

Kofax TotalAgility

Integration Server Installation Guide

Version: 7.6.0

Date: 2019-06-03

The KOFAX logo is displayed in a bold, blue, sans-serif font. The letters are thick and closely spaced, with a consistent weight throughout the word.

© 2019 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface.....	6
Related documentation.....	6
Training.....	7
Getting help with Kofax products.....	7
Chapter 1: Installation planning.....	8
Kofax Message Connector.....	8
Chapter 2: TotalAgility Integration Server installation.....	9
Perform a silent installation.....	9
Perform a standard installation.....	11
Perform TotalAgility installation in a Docker container.....	13
Docker installation on the Windows server.....	14
Create a TotalAgility docker container image.....	14
Run a docker container.....	16
Use Windows authentication with IIS and SQL server.....	18
Use Integration Server with on-premise multi-tenant server deployment.....	21
Encrypt and decrypt the configuration files.....	21
Encrypt and decrypt the web.config file.....	21
Encrypt and decrypt the Core Worker or Export Worker config file.....	21
Edit the TotalAgility server configuration file.....	24
Add a thread pool monitoring interval.....	25
Manually.....	25
Using Configuration Utility.....	26
Chapter 3: Integrate Microsoft SharePoint with TotalAgility Integration Server.....	27
Update the web configuration file.....	28
To get custom pages.....	28
To support event handlers.....	28
For a SharePoint site.....	30
Network authentication for SharePoint and TotalAgility.....	31
TotalAgility and SharePoint are on the same domain.....	31
TotalAgility and SharePoint are on different domains.....	32
Configure the TotalAgility custom web pages in SharePoint.....	32
Enable single sign-on.....	33
Add the TotalAgility Integration Server custom web pages to the SharePoint quick launch menu.....	33

Add the create TotalAgility workflow context menu item to a document library.....	34
Configure the custom web pages.....	35
Configure TotalAgility web parts in SharePoint server.....	36
Use web services.....	36
Enable session.....	36
Set up the Microsoft SharePoint server and TotalAgility server to provide fault tolerance.....	37
Set up the TotalAgility server.....	37
Set up the Microsoft SharePoint server.....	38
Chapter 4: Integrate Microsoft Dynamics CRM with TotalAgility Integration Server.....	39
Install Dynamics CRM.....	39
Update the web configuration file for Dynamics CRM.....	39
Update web.config for the CRM virtual directory.....	41
Chapter 5: Integrate Microsoft Dynamics AX with TotalAgility Integration Server.....	42
Create Dynamics AX service reference to the TotalAgility web service.....	43
Create Dynamics AX 09 service reference to the TotalAgility web service.....	43
Create Dynamics AX 12 service reference to the TotalAgility web service.....	43
Add a reference.....	44
In Dynamics AX 09.....	44
In Dynamics AX 12.....	44
Import the TotalAgility connector class into Dynamics AX.....	44
Edit Database X++ event methods.....	45
Verify the Application Pool account.....	45
Chapter 6: Integrate Micro Focus Content Manager server with TotalAgility Integration Server.....	46
Identify the Content Manager SDK version.....	46
Set up the Micro Focus Content Manager server.....	46
Install and configure TotalAgilityTrimCommunicatorService.....	46
Configure the event handler in Content Manager.....	47
Chapter 7: Integrate Kofax SignDoc with TotalAgility.....	50
Set up the Kofax SignDoc server.....	50
Chapter 8: Integrate Kofax Communication Manager with TotalAgility Integration Server.....	51
KCM proxy installation on the Web server.....	51
Silent installation.....	51
Standard installation.....	51
Chapter 9: Configure TotalAgility Integration Server for HTTPS communication.....	52
Change the bindings in Integration Server Web.config file.....	52
Chapter 10: KCM proxy installation on the Web server.....	53
Silent installation.....	53
Standard installation.....	53

Update the KCM Server URL in TotalAgility Web.config.....	53
Manually update the KCM Server URL in TotalAgility Web.config.....	54
Using the Configuration Utility.....	54
Install KCM Proxy manually.....	55
Chapter 11: Launch TotalAgility Integration Server.....	56
Chapter 12: Uninstall TotalAgility Integration Server.....	57
Uninstall using the wizard.....	57
Uninstall in silent mode.....	57
Chapter 13: Upgrade process.....	58
Upgrade TotalAgility Integration Server in silent mode.....	58
Chapter 14: Troubleshooting.....	59
TotalAgility Integration Server AppPool exists.....	59
Site location invalid error.....	59

Preface

This guide includes instructions for installing and upgrading to Kofax TotalAgility Integration Server 7.6.0, and integrating it with other products.

Read this guide completely before installing the software.

Related documentation

The product documentation set for Kofax TotalAgility is available at the following location.

<https://docshield.kofax.com/Portal/Products/KTA/7.6.0-d4fslp3xyr/KTA.htm>

In addition to this guide, the documentation set includes the following items:

- *Kofax TotalAgility Prerequisites Guide*: Provides system requirements for installing TotalAgility, instructions for running the prerequisite utility, and a software checklist for various installation types.
- *Kofax TotalAgility Installation Guide*: Describes how to install and configure TotalAgility.
- *Kofax TotalAgility On-Premise Multi-Tenancy Installation Guide*: Describes how to install and configure On- Premise Multi-Tenant system.
- *Kofax TotalAgility Configuration Utility Guide*: Explains how to use the Configuration Utility to update settings across various configuration files for different types of installation and deployment.
- *Kofax TotalAgility Administrator's Guide*: Provides information to the administrator on configuring and maintaining a TotalAgility installation.
- *Kofax TotalAgility Architecture Guide*: Provides an overview of the TotalAgility architecture, covering various deployments for on-premise, on-premise multi-tenancy and Azure environments.
- *Kofax TotalAgility Best Practices Guide*: Describes the best practices you must follow when using TotalAgility to improve performance, cost, maintenance, availability and security.
- *Kofax TotalAgility Features Guide*: Provides an overview of the TotalAgility features.
- *Kofax TotalAgility Migration Guide*: Provides information on TotalAgility upgrades from different versions and post upgrade configuration.
- *Kofax TotalAgility Help*: Provides details about using TotalAgility to design business jobs and cases, assign resources, create forms, integrate with external applications, and more. Access the help from the TotalAgility application by clicking the Help button.
- *Kofax TotalAgility Workspace Help*: Describes how to use the Workspace to manage activities, jobs, and resources. Access the help from the TotalAgility Workspace by clicking the Help button.
- *Kofax TotalAgility On-Premise Multi-Tenant System Help*: Describes how to create and manage tenants using the TotalAgility On-Premise Multi-Tenant system.
- *Kofax TotalAgility Web Capture Control Help*: Provides details on using a Web Capture control in creating multi-page documents, creating a new document in a new folder, deleting pages that have been incorrectly scanned, and more; also, describes the buttons available in a Web Capture control toolbar.

- *Kofax Analytics for TotalAgility Product Features Guide*: Provides an overview of the dashboards that help you track data through the workflow, analyze the effectiveness of the processes and resources, and address business problems.
- *Kofax TotalAgility Tables*: Describes the Kofax TotalAgility tables and fields used by Kofax Analytics for TotalAgility.
- *Migration From Kofax Products Guide*: Provides information about migrating TotalAgility files and Kofax Transformation Modules projects to TotalAgility.

Training

Kofax offers both classroom and computer-based training that will help you make the most of your Kofax TotalAgility solution. Visit the Kofax website at www.kofax.com for complete details about the available training options and schedules.

Getting help with Kofax products

The [Kofax Knowledge Base](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the Kofax [website](#) and select **Support** on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.
- Access to the Kofax Customer Portal (for eligible customers).
Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Kofax Partner Portal (for eligible partners).
Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Installation planning

TotalAgility is specifically designed to give organizations the flexibility to deploy either on-premise or in the cloud. The TotalAgility Integration Server enables customers to utilize on-premise LOB applications within TotalAgility Azure. You can configure various LOB Connectors within the Designer, similar to TotalAgility On-Premise and set the new nodes to execute either on the Azure tenant or the Integration Server.

The primary source of information about supported operating systems and other TotalAgility Integration Server requirements is the Technical Specifications document, which is available on the Kofax website at <http://www.kofax.com>.

Review these important notes before you proceed with the installation.

- For prerequisites, see the *Kofax TotalAgility Prerequisites Guide* available on the [Kofax Fulfillment Site](#).
- If your solution includes multiple Kofax products, review the Technical Specifications document.
- Obtain a license key for Integration Server either from your Account Manager or from Kofax Support.
- Before extracting TotalAgility installation .zip file, unblock the .zip file from the file properties window.
- After installing the Integration Server, you can update the configuration settings by modifying the configuration file or by running the configuration utility available on the installation media. You must manually copy the utility onto the server where the configuration settings are to be modified. See the *Kofax TotalAgility Configuration Utility Guide*.

Kofax Message Connector

Kofax Message Connector is a Windows service responsible for importing messages and files in many electronic formats. It retrieves documents from various sources and saves them in its internal storage making them available for retrieval through a web service interface. TotalAgility connects to the Message Connector web service interface and retrieves the documents for import.

Kofax Message Connector can import messages and files from a number of sources:

- Email messages including attachments using various email protocols (SMTP, POP3, IMAP).
- Fax messages (through internal fax over IP server or external fax servers: Kofax Communication Server, RightFax, Biscom).
- Files from a network folder.

For information on prerequisites for the Kofax Message Connector, see the *Kofax TotalAgility Prerequisites Guide* and for information on deployment scenarios and advanced configurations, see the *Kofax TotalAgility Administrator's Guide*.

Chapter 2

TotalAgility Integration Server installation

This chapter describes two methods for installing TotalAgility Integration Server:

- [Silent installation](#) for multiple servers that use the same configuration.
- [Standard installation](#) using the installation wizard.

Perform a silent installation

Use the Integration Server silent installation to install Integration Server without any user interaction. Once you edit the silent installation file and run the command from a command line or a batch file, the Integration Server installation proceeds automatically.

Note The user who will run Integration Server must have "Log on as Service" rights.

1. On the installation media, navigate to `\\IntegrationServerInstall` and open `SilentInstallConfig.xml` using a text editor.
2. In `SilentInstallConfig.xml`, update the following parameters.

Note Fix the line breaks if you copy and paste the code from this guide.

Parameter	Default Value	Description
PortNumber	3581	Keep default
SerialNumber	empty (false)	Keep default
ProductCode	empty (false)	Keep default
SkipLicense	true	Keep default
InstallDirectory	C:\Program Files\Kofax \TotalAgility\	Specify the Integration Server destination directory.
RunAsSystemAccount	true	Keep default Set to true to run Integration Server with LocalSystem account.
RunAsNetworkServiceAccount	false	If set to true, the AppPool and Kofax TotalAgility services are created with the NT Authority\Network Service username.
ValidOS	true	Set to true to check if the Operating System is valid.

Parameter	Default Value	Description
SQLServerInstalled	true	Set to true to check if the SQL Server is installed.
SQLClientInstalled	false	Set to true to check if the SQL Client is installed.
IISInstalled	true	Set to true to check if IIS is installed.
ImportSystemMaps	true	Keep default
InstallAction	IntegrationServerInstall	Accept the default.
InstallMode	Silent	Accept the default.
InstallType	Both	Select the install type. The Install Type can be ApplicationServer, WebServer or both.
IsIntegrationServer	false	Set to true to install Integration Server.
TenantId	Provide valid Tenant URL	Enter the valid Tenant URL. Note When a Tenant is created, the tenant URL is sent to the tenant through email.
SystemSessionId	Provide valid System Session Id	Enter the valid System Session ID. Note Log on to TotalAgility Designer. On the Home page click System Settings > Settings . The System Session ID is available on the General tab.
<SiteRoot>	Default Web Site	Install TotalAgility under a custom site that uses a non-standard port other than the standard ports (80 and 443). For example, create a custom site called "testsite" under IIS using the port number 85.

3. If installing TotalAgility on a non-standard port, modify the <TenantServiceURL>Provide Valid Tenant URL</TenantServiceURL> parameter to include the non-standard port number as follows:

```
<TenantServiceURL>https://<tenantname.FQDN>:<non-standard port no></TenantServiceURL>
```

4. Save and close the file.
5. On the Command Prompt, change the command line to the root directory of the Setup.exe file.

6. Run `Setup.exe /Silent`.

The following items are installed automatically:

- Kofax TotalAgility Integration Server
- Utility for Kofax Export Connector
- Kofax Import Connector

The system generates a log file that reports errors (if any).

The success and failure of installation is indicated in the event log.

When automating installation, if you run `setup.exe` from command line, or run `setup.exe` as a silent installation, one of the codes returns to indicate the following:

- 0=Success
- 1=Success with warnings
- 2=Failure

Perform a standard installation

When you run the installation wizard, the following items are installed automatically:

- Kofax TotalAgility Integration Server
- Utility for Kofax Export Connector
- Kofax Import Connector

Note the following:

- You must have administrator account to install the Integration Server.
- The user who will run Integration Server must have "Log on as Service" rights.
- You can use hotkeys to navigate to next screen.

1. Navigate to `\\IntegrationServerInstall` on the installation media and run one of the following commands:

- If UAC (User Account Control) is enabled, right-click **Setup.exe** and select **Run As Administrator**.
- If UAC is not enabled, run **Setup.exe**.

The system starts the **Kofax TotalAgility Integration Server installation**.

Note To exit the setup, click **Cancel** or press Esc.

2. Click **Next**.

The **Kofax Inc. Software License Agreement** window opens.

3. In the **Kofax Inc. Software License Agreement** window, accept the terms in the License Agreement and click **Next**.

The **Type of Install** window opens.

4. Select the type of install:
 - **Web Server:** Installs a server to point to any Application server. A Web server installs the SDK Services and user interfaces for the Designer and Workspace.
 - **Application Server:** Installs a server to which remote clients will connect and sets up their web servers. An Application server only installs Core services and does not install user interfaces and any shortcuts for the Designer and Workspace.
 - **Web/Application Server:** Installs the Web and Application servers on a single machine.
5. Click **Next**.
The **Destination** window opens.
6. Use the default installation folder or click **Browse** to select a different path and click **Next**.
The **Credentials** window opens.
7. Enter the credentials for the user who will run Integration Server.

Note This user must be an existing Integration Server user.

8. On the **Root Website to host TotalAgility Application** list, select the website to host the Integration Server application. By default, the **Default Web Site** is selected. However, you can select any other site as required.

Note The websites added in IIS Manager appear on this list. To add a website in IIS Manager, click `Start > Run > IIS Manager > Sites > Add Web Site`.

9. To support SSL, select the **Support SSL** check box.

Note The SSL option is only available if you have configured the https binding in IIS. See [Configure Kofax TotalAgility Integration Server for HTTPS communication](#).

10. Click **Next**.
The **Software Checks** window opens. The system displays a list of required software and whether or not the software is installed.
11. Review the **Detected Software** list and proceed as follows:
 - If your system does not have all the required software, click **Cancel** to close the installer and install the software.
 - If your system has all the required software, click **Next**.

12. Click Next.

Depending on the type of install, the following window appears:

- If installing Web/Application server, the **Tenant Information** window opens: Enter the following information:
 - a. Tenant URL:** This URL is available in the email sent upon tenant creation. Using this URL the system will connect to the on-premise multi-tenancy tenant or Azure tenant.
Tenant URL examples: `https://TenantName.<fullyqualifieddomainname>/TotalAgility` for on-premise multi-tenancy and `https://tenantname.cloudserviceURL/` for Azure.
 - b. System Session Id:** This ID is used for Core Worker authentication with Kofax TotalAgility in Azure environment.
- If installing Web server, the **Choose Server Location with Options** window opens: Enter the Server name of your existing Integration Server machine in the following format: HW-ABC-W7, or provide the IP Address.

13. Click Next.

The **Installation Review** window opens and displays the settings.

14. Click Next.

The **Installation Progress** window opens. The setup installs the required files and other integrated products.

15. Click Finish.

Your installation is now complete.

Note If any errors occur during the installation, Integration Server creates a log file called **Kofax TotalAgilityInstallErrorLog.txt** on your desktop. Check this log file for error details. The success or failure of installation is indicated in the event log.

After installing, further configure Integration Server to:

- [Integrate with SharePoint.](#)
- [Integrate with Dynamics CRM.](#)
- [Integrate with Dynamics AX.](#)
- [Integrate with Micro Focus Content Manager.](#)
- [Integrate with Kofax Communication Manager](#)

Perform TotalAgility installation in a Docker container

A Docker is an open platform for developing, shipping, and running applications. Docker enables you to separate an application from its infrastructure. Using Docker, you can manage your infrastructure in the same way you manage your applications.

Docker provides the ability to package and run an application, such as TotalAgility in a loosely isolated environment called a Container. The isolation and security allows you to run many containers simultaneously on a given host using less resources than virtual machines.

You can deploy TotalAgility application into your production environment, as an independent container or an orchestrated set of containers. This works the same whether your production environment is a local datacenter, a cloud provider, or a hybrid of the two. This means you would not need to use the

TotalAgility installation program when TotalAgility is deployed in a Docker container. Instead the container would already have TotalAgility installed and only the relevant configuration settings (such as database connection strings) are required when the container runs.

By default, all TotalAgility containers do not have limits for memory or CPU. SQL Server runs either on another Windows container or another machine, it does not run in the TotalAgility container.

See also:

- [Docker installation on the Windows server](#)
- [Create a TotalAgility docker container image](#)
- [Run a docker container](#)
- [Use Windows authentication with IIS and SQL server](#)

Docker installation on the Windows server

Setup Docker on your Windows server.

1. Open an elevated PowerShell command prompt, and type the following commands.

```
Install-Module DockerMsftProvider -Force
Install-Package Docker -ProviderName DockerMsftProvider -Force
```

2. Check if a reboot is required. If required, restart your instance using the following command:

```
(Install-WindowsFeature Containers).RestartNeeded
```

If the output of this command is Yes, restart the server using the following command: `Restart-Computer`.

3. Test your Docker Engine - Enterprise installation by running the hello-world container.

```
docker run hello-world:nanoserver

Unable to find image 'hello-world:nanoserver' locally
nanoserver: Pulling from library/hello-world
bce2fbc256ea: Pull complete
3ac17e2e6106: Pull complete
8cac44e17f16: Pull complete
5e160e4d8db3: Pull complete
Digest: sha256:25eac12ba40f7591969085ab3fb9772e8a4307553c14ea72d0e6f98b2c8ced9d
Status: Downloaded newer image for hello-world:nanoserver
Hello from Docker!
```

This message shows that your installation appears to be working correctly.

Create a TotalAgility docker container image

A container is defined by its image as well as any configuration options you provide to it when you create or start it.

To create a docker image, you need internet connectivity because docker uses the Microsoft's "microsoft/aspnet" image as a base onto which the prerequisites get installed (from the base OS or from Internet when any feature is not available on the image).

1. Extract the Kofax TotalAgility 7.6 ZIP file and copy the TotalAgility directory to a local path such as `C:\Docker\Kofax TotalAgility7.6\TotalAgility`.
2. Create a new folder <workingdirectory>.

3. Extract the contents of "DockerFiles.zip" to the <workingdirectory>.

The file structure should be as follows:

```
<workingdirectory>\dockerfile
<workingdirectory>\TotalAgility\PowerShellScripts
<workingdirectory>\TotalAgility\Dependencies
```

4. Extract the contents of the TotalAgility installation archive to <workingdirectory>\TotalAgility.

The file structure should be as follows:

```
<workingdirectory>\TotalAgility\IntegrationServerInstall
<workingdirectory>\Licensing
```

5. On the installation media, navigate to \\TotalAgility\TotalAgility\IntegrationServerInstall and open SilentInstallConfig.xml using a text editor and update the parameters as needed for each container type. See [Perform a silent installation in a docker container](#) for more information.
6. To create the image, open a PowerShell window on the container host and run the following command:

```
docker build -t <imagenamegoeshere> "<fullpathtoworkingdirectory>"
```

Note Container host is the machine where docker server is installed. Performance of a build command depends on the number processors in the container host machine. Command may take approximately one hour to complete with quad core processors configuration.

Example The following command generates the image with the name "kofaxis" using the contents inside the C:\Docker\Kofax TotalAgility directory:

```
docker build -t kofaxis "C:\Docker\KofaxTotalAgility"
```

Perform a silent installation in a docker container

Note Only "ImportService" or only "ExportService" or a combination of "ExportService" and "ImportService" together, in any of the following container types below is not supported.

Parameter	Default value	Description
Identity Information		
UserName	KTA_admin	A user with name KTA_admin is created inside the docker image for installing Kofax TotalAgility. So you cannot modify the user name.
RunAsSystemAccount	TRUE	Accept the default. If set to true, the AppPool and Kofax TotalAgility services are created with LocalSystem account.
Install Info		
InstallType	Both	Accept the default.

Run a docker container

A Docker container runs on any machine that supports the container's runtime environment. Applications are not required to be tied to the host operating system, so both the application environment and the underlying operating environment can be kept clean and minimal.

Note When a running container is stopped, any changes to its state that are not stored in persistent storage disappear.

Before running a docker container, it is expected that databases are already setup (using Database only installation mode) before bringing the containers up and running.

1. Generate “dockersettings.env” using Configuration Utility in the docker mode. The file will be used later for the container initialization. Refer the *Kofax TotalAgility Configuration Utility Guide* for more information.
2. To run the TotalAgility container using Windows authentication:
 - a. Set up an account and create win.json using Windows authentication.
Win.json contains the credentials in the Json format which will be passed to the container during creation.
 - b. To bring the container up, use the settings provided inside the env file using the Windows authentication account with credentials specified under the win.json file.
To run the TotalAgility container using manual authentication, configuration is not needed.
3. Container access can be limited to the container host or can be port forwarded for the global access. Enable the required exposed port number in firewall settings of host machine.
4. Execution commands:
 - a. Container access can be limited to container host with windows authentication `"docker run --env-file <fullpathtoenvfile> --security-opt "credentialspec=file://win.json" <imagename>"`
Example The following command will bring a container up using the kofaxis image with the Kofax TotalAgility settings applied from dockersettings.env file using Windows authentication with the credentials specified in the win.json file.
`docker run --env-file "C:\Docker\TotalAgility\dockersettings.env" --security-opt "credentialspec=file://win.json" kofaxis,`
 - b. Container access can be limited to container host with client credentials: `"docker run --env-file <fullpathtoenvfile> <imagenamegoeshere>"`.
Example The following command will bring a container up using the kofaxis image with the Kofax TotalAgility settings applied from dockersettings.env file using client credentials.
`docker run --env-file "C:\Docker\TotalAgility\dockersettings.env"`
 - c. Port forwarded container access which is not limited to the container host with Windows authentication using the following command to bring the container up using the settings

provided inside the env file forwarding the site from within the container in port <portonimage> on to port <dockerserverexposedport> on the docker server.

```
"docker run --env-file <fullpathtoenvfile> --security-opt
"credentialspec=file://win.json" -p <dockerserverexposedport>:<portonimage>
<imagenamegoeshere>"
```

Example The following command will bring a container up using the kofaxis image with the Kofax TotalAgility settings applied from dockersettings.env file with the credentials for Windows authentication specified under the win.json file, and forwarding the port 80 from the container into the 5000 port on the container host:

```
docker run --env-file "C:\Docker\TotalAgility\dockersettings.env" --
security-opt "credentialspec=file://win.json" -p 5000:80 kofaxis
```

- d. Port forwarded container access which is not limited to the container host with client credentials, using the following command to bring the container up using the settings provided inside the env file forwarding the site from within the container in port <portonimage> onto port <dockerserverexposedport> on the docker server.

```
"docker run --env-file <fullpathtoenvfile> -p
<dockerserverexposedport>:<portonimage> <imagenamegoeshere>"
```

Example The following command will bring a container up using the kofaxis image with the Kofax TotalAgility settings applied from dockersettings.env file with the credentials and forwarding the port 80 from the container into the 5000 port on the container host:

```
docker run --env-file "C:\Docker\TotalAgility\dockersettings.env" -p
5000:80 kofaxis
```

- 5. To attach the current powershell session in the docker server to a command prompt one inside the container, you can use "docker attach <containerIDgoeshere>" or add "-it" parameter as part of the "docker run" command .

Additional information

This table includes some useful docker commands.

Docker Command	Description
docker images	Gets the list of all docker images currently available on the server.
docker ps -a	Gets the list of all containers available on the server.
docker start <containerID>	Starts the container with the ID <containerID> on the server.
docker attach <containerID>	Attaches the powershell session to the session inside the container with ID <containerID>.
docker stop <containerID>	Stops the container with the ID <containerID> on the server.
docker rm <containerID>	Deletes the container with the ID <containerID> on the server.
docker rmi <imagenamename>	Deletes the image with the ID <imagenamename> on the server; this is successful only if there are no child containers using this image.
docker inspect -f "{{ .NetworkSettings.Networks.nat.IPAddress }}" <containerID>	Gets the IP address of the container with the ID <containerID>.

Docker Command	Description
<code>docker cp "<containerID>:/<fullfilepathoncontainer>" "<pathtofolderonserver>"</code>	Copies a file from the container to the server.
<code>docker cp "<fullfilepathonserver>" "<containerID>:/<fullfilepathoncontainer>"</code>	Copies a file from the container to the server.

Use Windows authentication with IIS and SQL server

Docker containers cannot join an Active Directory domain. However, when running a container, you can specify that it should use a specific AD Group Managed Service Account (gMSA) for any local Windows services and IIS Application pool in the container that are configured to run as LocalSystem or NetworkService accounts.

When running as these accounts in the container, the services and App pool will automatically get the access rights of the gMSA to allow them to use Windows authentication to access other VMs/machines outside of the container.

When setting up a TotalAgility docker container to use Windows authentication, you must modify the SilentInstallConfig.xml file to specify LocalSystem as the account to use for all TotalAgility services and IIS App pool. This account will be used when the container is built.

Ensure the following prerequisites are met:

- Add docker server, SQL server machine and machines that will use gMSA under required domain controller.
- Add these machines in the Active Directory under "Computer" folder.
- Create a Global Security group, such as " ContainerHostName" in the Active Directory under "Builtin" folder.
- Add docker server, SQL server machine or machines that will use gMSA as members to the new group.

Perform the following steps to use Windows authentication with IIS and SQL server.

1. Create the KDS root key.

This key is used by the KDS service on DCs (along with other information) to generate passwords. You can generate this key only once per domain.

a. Login to domain controller and execute the following commands:

```
Import-module ActiveDirectory
Add-KdsRootKey -EffectiveImmediately
```

b. Verify your key using the following command:

```
Get-KdsRootKey
```

2. Create a gMSA account.

a. Login to domain controller and execute the following command:

```
GMSA account name : containerhost
Domain name: TotalAgilityexample.com
```

```
New-ADServiceAccount -Name containerhost -DNSHostName TotalAgilityexample.com
-PrincipalsAllowedToRetrieveManagedPassword "Domain Controllers",
"domain admins", "CN= ContainerHostGroupName,CN=Builtin, DC=
TotalAgilityexample, DC=COM" -KerberosEncryptionType RC4, AES128, AES256
```

- b. Verify the new gMSA account using the following command: .
Get - ADServiceAccount - Identity containerhost
 - c. A new gMSA object appears in your domain's Managed Service Account.
3. Add gMSA account to the servers you want to use.
 - a. Open the Active directory Admin Center and go to Managed service accounts.
 - b. Select the gMSA account and click **Properties**.
 - c. Select the security and click **Add**.
 - d. Select the computers where you want to use gMSA such as docker server and SQL server machine.
 - e. Reboot Domain controller for the changes to take effect.
 - f. Reboot the computers that will be using gMSA.
 4. Install gMSA Account on servers.

- a. Login to the machine that will be used as docker server.
- b. If Active Directory features are not available, execute the following command:
Enable-WindowsOptionalFeature -FeatureName ActiveDirectory-Powershell
-online -all
- c. To install and test gMSA, execute the following commands:

```
// check whether you are able to account
Get-ADServiceAccount -Identity containerhost //Name of GMSA

// install on machine
Install-ADServiceAccount -Identity containerhost

// test
Test-ADServiceAccount -Identity containerhost
```

If the output does not contain any errors, it will look like as follows:

```
Path :
Online : True
RestartNeeded : False
DistinguishedName : CN=containerhost,CN=Managed Service Accounts, DC=local
Enabled : True
Name: containerhost
objectClass : msDs-GroupManagedServiceAccount
ObjectGUID : containerhost$
SamAccountName : containerhost$
SID : S-1-5-21-3914853822-719528391-929614657-1606
UserPrincipalName :

True
```

5. Associate Service Principal Name with the gMSA:

- a. This step is required for kerberos authentication to work and for automatic login in Chrome and Internet Explorer browsers. If you skip this step, authentication still works but will always prompt for username/password since it will fallback to NTLM.

GMSA account : containerhost

Domain name: TotalAgilityexample .com

Container host machine: machine1

- b. Login to domain controller and execute the following command:

```
setspn -c -s HTTP/ machine1 TotalAgilityexample \ containerhost
setspn -c -s HTTP/ machine1.TotalAgilityexample.com TotalAgilityexample \
containerhost
```

6. To test Active Directory access on the container host, run the following command on the host machine: `nltest /parentdomain`

At this point, if no errors occurs, the LocalSystem account on the container will be a proxy for the configured gMSA account. Any process run as the LocalSystem principal on the container will appear to be the GMSA principal to all assets on the Active Directory domain.

- 7. Generate credential specifications file which must be passed to the docker during container creation to utilize this service account. Run the following commands to download module which will create this file from Microsoft github account and will create a JSON file containing required data.**

```
GMSA account : containerhost
Domain name: TotalAgilityexample.com

Invoke-WebRequest "https://raw.githubusercontent.com/Microsoft/Virtualization-
Documentation/live/windows-server-container-tools/ServiceAccounts/
CredentialSpec.psm1" -UseBasicParsing -OutFile $env:TEMP\cred.psm1

import-module $env:temp\cred.psm1

New-CredentialSpec -Name win -AccountName containerhost
#This will return location and name of JSON file
Get-CredentialSpec

Name Path
---- ----
win C:\ProgramData\docker\CredentialSpecs\win.json
```

- 8. For SQL server configuration to allow gMSA, enter the gMSA account as "containerhost" and domain name as "TotalAgilityexample.com" and run the following SQL commands on your SQL database:**

```
CREATE LOGIN " TotalAgilityexample \containerhost$"
FROM WINDOWS
GO
```

To create user for all the TotalAgility databases:

```
CREATE USER containerhost FOR LOGIN " TotalAgilityexample \ containerhost$"
GO

EXEC sp_addrolemember 'db_datareader', containerhost
EXEC sp_addrolemember 'db_datawriter', containerhost
```

- 9. If there are no errors, the LocalSystem account on the container will be a proxy for the configured gMSA account. Any process run as the LocalSystem principal on the container will appear to be the gMSA principal to all assets on the Active Directory domain. To test Active Directory access on the container, run the following command on the container: `nltest /parentdomain`**

Use Integration Server with on-premise multi-tenant server deployment

When installing the Integration Server with a separate Web-Application on-premise multi-tenant server deployment, the Integration Server is required to point to the on-premise multi-tenant Application server. This can cause an issue if the on-premise multi-tenant Application server is not directly accessible by the Integration Server. To avoid this, we recommend that you point the Integration Server to the on-premise multi-tenant Web server.

1. Navigate to the installation directory for the TotalAgility Integration Server.
2. Open Web.config in a text editor.
3. Locate the following section:

```
<appSettings>
  <add key="CoreIntegrationServicesLocation" value="<on-premise multi-tenant
  Web server machine name>"/>
</appSettings>
```

4. Save and close the configuration file.

Encrypt and decrypt the configuration files

The Integration Server configuration files include the DB Connection settings and sensitive information. Therefore, we recommend that you encrypt the following Integration Server files.

- **Web.config**
- **Core Worker config**
- **Export Worker config**

Encrypt and decrypt the web.config file

The Integration Server, **Web.config** file is located under <Kofax Install location>\TotalAgility\Agility.Server.Web.

Use the Microsoft ASP.NET IIS Registration Tool (aspnet_regiis) to encrypt or decrypt any section of the Web.config file. For more information, see [http://msdn.microsoft.com/en-us/library/zhhdckxy\(v=vs.100\).aspx](http://msdn.microsoft.com/en-us/library/zhhdckxy(v=vs.100).aspx).

At a minimum, encrypt the appSettings section that includes the Database connection information.

Encrypt and decrypt the Core Worker or Export Worker config file

The Integration Server **Core Worker config** and **Export Worker config** files are located under <Kofax Install location>\TotalAgility\CoreWorkerService.

The TotalAgility Server supports two encryption methods:

- [DPAPI encryption](#)

- [RSA encryption](#)

Use the `Kofax.CEBPM.Encryption.exe` utility to encrypt and decrypt files with either of these methods.

Use the `Kofax.CEBPM.Encryption.exe` utility

The `Kofax.CEBPM.EncryptConfig.exe` utility (located in the Integration Server installation directory) encrypts (-enc) or decrypts (-dec) any section of a configuration file.

At a minimum, encrypt the `appSettings` section of each config file that includes the user ID and password as well as other sensitive information. Use the optional `-h` flag to display help for the command.

`Kofax.CEBPM.EncryptConfig.exe` cannot work with `Web.config`, it can only work with configuration files or executables.

Important Add the following security provider to the configuration file before encrypting the file:

```
<configProtectedData>
  <providers>
    <add useMachineProtection="true"
        name="DPAPIProtection"
        type="System.Configuration.DpapiProtectedConfigurationProvider,
System.Configuration, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
    <add name="RSAProvider"
        type="System.Configuration.RsaProtectedConfigurationProvider,
System.Configuration, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a,
processorArchitecture=MSIL"
        keyContainerName="CPUserverKeys"
        useMachineContainer="true" />
  </providers>
</configProtectedData>
```

Use the DPAPI encryption method

Because you must decrypt the file on the same machine where it was encrypted, use this utility to encrypt one server at a time.

Run the utility on each TotalAgility Server individually.

1. Stop the Integration Server Core Worker Service service.
2. Navigate to the TotalAgility Integration Server Core Worker installation directory and open a command-line window.
3. Run the following command:

```
Kofax.CEBPM.EncryptConfig.exe -f Agility.Server.Core.WorkerService.exe.config -s
"appSettings" -p DPAPIProtection -enc
```

Use the RSA encryption method

RSA encryption is an algorithm for public key encryption and digital signatures that uses two separate keys. Create a key and encrypt the configuration file on one Server, and export the key to all the other Servers. All the TotalAgility Servers with the exported key installed can access the configuration file. Use this method if you have several Servers with the same configuration.

The following instructions differentiate between the source TotalAgility Server where you create the key and the target TotalAgility Servers onto which you import the key.

Prepare the key

Perform these steps on one source TotalAgility Integration Server.

1. Create the custom RSA key container:
 - a. Logon to the Integration Server with administrator rights.
 - b. Open a command-line window.
 - c. Navigate to the .NET Framework version 2.0 directory. For example, enter the following command:
cd \WINDOWS\Microsoft.Net\Framework\v2.0.*
 - d. Run the following command:
aspnet_regiis -pc "<KeysFile>" -exp
where:
 - <KeysFile> is the name of the key file.
 - The -exp option makes the key exportable.
2. Run the following command to grant the TotalAgility Integration Server Core Worker Server service user permission to read the <KeysFile> RSA container file.
aspnet_regiis -pa "<KeysFile>" "<TotalAgilityserviceuser>"
where:
 - <KeysFile> is the name of the key file you created in step 1d.
 - <TotalAgilityserviceuser> is the Integration Server Core Worker Server service user.
3. Encrypt the file:
 - a. Log on to the TotalAgility Server as the TotalAgility Integration Server Core Worker Server service user.
 - b. Navigate to the installation directory for the TotalAgility Server and open a command-line window.
 - c. Run the following command:
Kofax.CEBPM.EncryptConfig.exe -f Agility.Server.Core.WorkerService.exe.config -s "appSettings" -p RSAProvider -enc
This command encrypts the appSettings section of the configuration file. The appSettings section includes the user ID and password as well as other sensitive information.
4. Export the key by running the following command:
aspnet_regiis -px "<KeysFile>" "c:\keys.xml" -pri
where:
 - <KeysFile> is the default keystore keyContainerName.
 - <c:\keys.xml> is the path and file name of the exported key file.

Import the key

Perform these steps on every target TotalAgility Server.

1. Import the key:
 - a. Log on to the TotalAgility Server with administrator rights.
 - b. Copy the keys.xml file from the source TotalAgility Server to the root C:\ directory of the target TotalAgility Server.
 - c. Open a command-line window.
 - d. Run the following command:
aspnet_regiis -pi "<KeysFile>" "c:\keys.xml"
where:
 - <KeysFile> is the default name of the key file.
 - <c:\keys.xml> is the path and file name to the imported key file.
 - e. Delete the keys.xml file on the target Server because it contains the unprotected private key.
2. Run the following command to grant the TotalAgility Integration Server Core Worker Server service user permissions to use the <KeysFile> RSA container file:
aspnet_regiis -pa "<KeysFile>" "TotalAgilityserviceuser"
where:
 - <KeysFile> is the name of the key file you imported in step 1.
 - <TotalAgilityserviceuser> is the TotalAgility Integration Server Core Worker Server service user.
3. Repeat these steps on all remaining TotalAgility Servers.

Decrypt the configuration file

1. Stop the **Kofax TotalAgility Integration Server Core Worker Server** service.
2. Navigate to the TotalAgility Server installation directory and open a command-line window.
3. Run the following command:
Kofax.CEBPM.EncryptConfig.exe -f Agility.Server.Core.WorkerService.exe.config -s "appSettings" -p DPAPIProtection -dec

Repeat these steps to encrypt and decrypt the Export Worker configuration file.

Edit the TotalAgility server configuration file

When you install TotalAgility, the system stores the configuration settings in a .NET file, **Agility.Server.Core.WorkerService.exe.config**. To change the value of any parameter, edit the configuration file or run the configuration utility. The configuration utility is available on the installation media and must be manually copied to your Kofax TotalAgility server. See the *Kofax TotalAgility Configuration Utility Guide*.

See

1. If you encrypted the configuration file after you installed the TotalAgility Server, decrypt the file. See [Decrypt the configuration file](#) .

Note If you used RSA encryption, decrypt the configuration file only on the source TotalAgility Server where you initially encrypted the file.

2. Navigate to the installation directory for the TotalAgility Server.
3. Open the configuration file in a text editor.
4. Locate the following section:

```
<appSettings>
  <add key="KeyNameString" value="which may contain passwords;" />
</appSettings>
```

5. Edit the parameter values as needed.
6. Save and close the configuration file.
7. To re-encrypt the configuration file, run the encryption utility. See [Encrypt and decrypt the configuration files](#).

Note If you used RSA encryption, export the key and install the encryption key file on any target TotalAgility Servers onto which you imported the original encrypted configuration file.

8. Restart the Kofax TotalAgility Integration Server Core Worker Server service.

Add a thread pool monitoring interval

When long running automatic activities are processed by the Core Worker, the threads in the automatic activity thread pool are not freed up when the taken activity is reset due to timeout. Configure a thread pool monitoring interval to free up the threads for these long running taken activities to allow other activities to progress once they timeout.

You can configure the thread pool monitoring interval manually or use the Configuration Utility.

Manually

1. Navigate to the installation directory for the TotalAgility server.
2. In a text editor, open **Agility.Server.Core.WorkerService.exe.config** from the following directory:

```
\\TotalAgility\Agility.Server.Web
```

3. Locate the following section and add a thread pool monitoring interval (default:60).

```
<appSettings>
  <add key="CoreWorkerThreadPoolMonitoringIntervalInSeconds" value="60" />
</appSettings>
```

4. Save and close the configuration file.
5. Restart the Kofax TotalAgility Core Worker service.

Using Configuration Utility

Run the Configuration utility and add the thread pool monitoring interval. See the *Kofax TotalAgility Configuration utility Guide*.

Chapter 3

Integrate Microsoft SharePoint with TotalAgility Integration Server

Integrate Microsoft SharePoint 2010 or SharePoint 2013 with Integration server to use SharePoint in the Integration Server.

1. Navigate to `\\SharePointInstallation` on the installation media, and run **Setup.exe**.
The system opens the Kofax TotalAgility for SharePoint Setup wizard.
2. Click **Next**.
The system displays the TotalAgility SharePoint Components window.
3. Select the TotalAgility Integration Server SharePoint components to install:
 - a. To install the SharePoint web parts, select the **TotalAgility SharePoint WebParts** check box.
 - b. To install the SharePoint web service and event-handler dlls, select the **TotalAgility SharePoint Event-Handling Components** check box.
 - c. To install the TotalAgility SharePoint custom pages, select the **TotalAgility SharePoint Custom Pages** check box.
 - By default, the **Add Assembly To GAC** check box is selected. The files are automatically added to GAC.
 - If you do not have access to GAC, clear the **Add Assembly To GAC** check box and enter the SharePoint Site Port Number. The files are automatically added to the bin folder (default location is `C:\inetpub\wwwroot\wss\VirtualDirectories\[PortNumber]\bin`) within the site.
 - d. On the list of **Website to host TotalAgility SharePoint components**, select a website.

Note You must not select the SharePoint related websites.

Note You can rerun the setup at a later date to install the custom pages if you did not do it initially.

4. Click **Install**.
5. Update **Web.config** to get custom pages, support event handlers and configure SharePoint site. See [Update the Web configuration file](#).

Further configure:

- [TotalAgility Integration Server custom web pages in SharePoint](#).
- [TotalAgility Integration Server web parts in the SharePoint server](#).
- [Microsoft SharePoint Server and TotalAgility Integration Server to provide fault tolerance](#).

Update the web configuration file

Update the Web.config file for the TotalAgility Integration Server components.

To get custom pages

Add the following optional “appsettings” key values to the Web.config file in the target SharePoint web application folder. For example, C:\inetpub\wwwroot\wss\VirtualDirectories\<PortNumber> where <PortNumber> is the port number of the target SharePoint web application.

Appsetting	Description	If not specified
TAEmbeddedSolutionURL	Point to the Integration Server site URL to integrate into the SharePoint web application.	The TotalAgility Form site is available at the same location as the SharePoint web application.
TALogonUserIdentifier	Point to the identifier that passes the SharePoint logon user name into embedded forms in the TotalAgility Forms site.	The LOGON_USER is used as the identifier.
TAWorkqueueEmbeddedForm:	Point to the form in the Integration Server Form site to use in the Workqueue custom page.	The WorkQueue.form is used.
TAJobListEmbeddedForm	Point to the form in the Integration Server Form site to use in the JobList custom page.	The JobList.form is used.
TADocURLIdentifier	Point to the identifier that passes the SharePoint document URL into embedded CreateNewJob forms in Integration Server.	The DOC_URL is used.
TADocNameIdentifier	Point to the identifier that passes the SharePoint document name into embedded CreateNewJob forms in Integration Server.	The DOC_NAME is used.

Example: Settings in Web.config file to get custom pages

```
<appSettings>
<add key="TAEmbeddedSolutionURL" value="http://domainname1:80/Forms/SharepointSite" />
<add key="TALogonUserIdentifier" value="LOGON_USER" />
<add key="TAWorkqueueEmbeddedForm" value="WorkQueue.form" />
<add key="TAJobListEmbeddedForm" value="JobList.form"/>
<add key="TADocURLIdentifier" value="DOC_URL"/>
<add key="TADocNameIdentifier" value="DOC_NAME"/>
</appSettings>
```

To support event handlers

Note If you copy and paste the code from this guide, correct any incorrect line breaks.

```
<configSections>
```

```
<section name="exceptionHandling"
type="Microsoft.Practices.EnterpriseLibrary.
ExceptionHandling.Configuration.ExceptionHandlingSettings,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
requirePermission="true" />
<section name="loggingConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.
Logging.Configuration.LoggingSettings,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35" requirePermission="true" />
</configSections>

<loggingConfiguration
name=""
tracingEnabled="true"
defaultCategory="General">
<listeners>
<add name="Event Log Listener"
type="Microsoft.Practices.EnterpriseLibrary.Logging.
TraceListeners.FormattedEventLogTraceListener,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
listenerDataType="Microsoft.Practices.EnterpriseLibrary.
Logging.Configuration.FormattedEventLogTraceListenerData,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
source="Total Agility" formatter="Text Formatter"
log="" machineName="." traceOutputOptions="None" />
</listeners>
<formatters>
<add type="Microsoft.Practices.EnterpriseLibrary.Logging.
Formatters.TextFormatter,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
template="Timestamp: {timestamp}
{newline}&#xA;Message: {message}
{newline}&#xA;Category: {category}
{newline}&#xA;Priority: {priority}
{newline}&#xA;EventId: {eventid}
{newline}&#xA;Severity: {severity}
{newline}&#xA;Title: {title}
{newline}&#xA;Machine: {localMachine}
{newline}&#xA;App Domain: {localAppDomain}
{newline}&#xA;ProcessId: {localProcessId}
{newline}&#xA;Process Name: {localProcessName}
{newline}&#xA;Thread Name: {threadName}
{newline}&#xA;Win32 ThreadId: {win32ThreadId}
{newline}&#xA;Extended Properties:
{dictionary({key} - {value}{newline})}"
name="Text Formatter" />
</formatters>
<categorySources>
```

```

<add switchValue="All" name="General">
<listeners>
<add name="Event Log Listener" />
</listeners>
</add>
</categorySources>
<specialSources>
<allEvents switchValue="All" name="All Events" />
<notProcessed switchValue="All" name="Unprocessed Category" />
<errors switchValue="All" name="Logging Errors & Warnings">
<listeners>
<add name="Event Log Listener" />
</listeners>
</errors>
</specialSources>
</loggingConfiguration>
<exceptionHandling>
<exceptionPolicies>
<add name="Agility Exception Policy">
<exceptionTypes>
<add name="All Exceptions" type="System.Exception,
mscorlib,
Version=4.0.0.0,
Culture=neutral,
PublicKeyToken=b77a5c561934e089"
postHandlingAction="NotifyRethrow">
<exceptionHandlers>
<add name="Logging Exception Handler"
type="Microsoft.Practices.EnterpriseLibrary.
ExceptionHandling.Logging.LoggingExceptionHandler,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
logCategory="General" eventId="100" severity="Error"
title="Total Agility"
formatterType="Microsoft.Practices.EnterpriseLibrary.
ExceptionHandling.TextExceptionHandler,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=5.0.505.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" priority="0" />
</exceptionHandlers></add>
</exceptionTypes>
</add>
</exceptionPolicies>
</exceptionHandling>

```

Note SharePoint event handler executes in the context of the user who initiated the action.

For a SharePoint site

Note If you copy and paste the code from this guide, correct any incorrect line breaks.

- Update the <system.serviceModel> section:

```

<system.serviceModel>
<bindings>
<basicHttpBinding>
<binding name="BasicHttpBinding_Service" openTimeout="00:10:00"
closeTimeout="00:10:00" sendTimeout="00:10:00" receiveTimeout="00:10:00"
allowCookies="true"

```

```

maxBufferSize="2147483647" maxReceivedMessageSize="2147483647"
maxBufferPoolSize="524288">
<readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
<security mode="TransportCredentialOnly">
<transport clientCredentialType="None" />
</security>
</binding>
</basicHttpBinding>
</bindings>
<client>
<endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://[TotalAgility server name or IP Address]/TotalAgility/Services/Core/
IntegrationEventService.svc"/>
</client>
</system.serviceModel>

```

Replace <TotalAgility server name or IP Address> with the IP Address of the Integration Server.

Note Point the endpoint address to the integration service URL for Integration Server.

Network authentication for SharePoint and TotalAgility

TotalAgility and SharePoint are on the same domain

1. Ensure that TotalAgility site has Windows Authentication in Internet Information Services (IIS) and the required SharePoint users are added to the TotalAgility server. Perform the following in the TotalAgility server:
 - a. Open **Internet Information Services (IIS) Manager**.
 - b. Click **Sites > Default Web Site > TotalAgility**.
 - c. On the **Features View** tab, double-click **Authentication**.
 - d. Right-click **Windows Authentication** and click **Providers....**
 - e. Check if, **Negotiate** and **NTLM** are available as providers. If not, add them from the **Available Providers** list.
2. Ensure that TotalAgility SharePoint Communicator site has windows authentication in Internet Information Services (IIS). Perform the following in the SharePoint server:
 - a. Open **Internet Information Services (IIS) Manager**.
 - b. Click **Sites > Default Web Site > TotalAgilitySharepointCommunicator**.
 - c. On the **Features View** tab, double-click **Authentication**.
 - d. Right-click **Windows Authentication** and click **Providers....**
 - e. Check if, **Negotiate** and **NTLM** are available as providers. If not, add them from the **Available Providers** list.
 - f. Ensure that Site App pool is changed to SharePoint site App pool.

TotalAgility and SharePoint are on different domains

Ensure that TotalAgility and SharePoint domains are trusted. If domains are not trusted, Windows authentication will not work, so it must be disabled and Anonymous authentication must be enabled in IIS. The Web.config files must also be updated. The steps to modify the Web.config files are given in the sub section.

Perform the following steps in the TotalAgility server and SharePoint server:

1. Open **Internet Information Services (IIS) Manager**.
2. Click **Sites > Default Web Site > TotalAgility**.
For SharePoint server, click **Sites > Default Web Site > TotalAgilitySharePointCommunicator**
3. On the **Features View** tab, double-click **Authentication**.
4. Right-click **Windows Authentication** and click **Disable**.
5. Right-click **Anonymous Authentication** and click **Enable**.

Update the web.config files

Update the Web.config files if TotalAgility and SharePoint are on different domains.

1. In the **Web.config** file for TotalAgility, replace `<transport clientCredentialType="Windows" />` with `<transport clientCredentialType="None" />` in the following bindings:
 - BasicHttpBinding_SharepointCommunicatorService
 - BasicHttpBinding_Service
 - BasicHttpBinding_CoreService
 - WebHttpBinding_Service
2. In the **Web.config** file for TotalAgilitySharePointCommunicator site on SharePoint server, replace `<transport clientCredentialType="Windows" />` with `<transport clientCredentialType="None" />` for `BasicHttpBinding_SharepointCommunicatorService` binding.
3. In the **Web.config** file for SharePoint site (C:\inetpub\wwwroot\wss\VirtualDirectories\<site port>), replace `<transport clientCredentialType="Windows" />` with `<transport clientCredentialType="None" />` for `BasicHttpBinding_SharepointCommunicatorService` binding.

Configure the TotalAgility custom web pages in SharePoint

Integrate a TotalAgility site directly into the SharePoint web interfaces to add the following TotalAgility forms to SharePoint:

- Create new job/workflow
- Work queue
- Take activities (displaying TotalAgility Integration Server take activity forms)
- Job/workflow list and job properties

TotalAgility site forms are hosted within custom ASPX web pages that are added to the target SharePoint web application.

Enable single sign-on

Provide single sign-on to access the SharePoint website and the Integration Server site.

Note Disable the Header Form option while creating the custom pages.

Use the default username initialization variable called "LOGON_USER" in the "top level" forms (CreateNewJob, WorkQueue and JobList) in the Integration Server site.

Note You can modify the name in the "LOGON_USER" if needed.

When implementing these forms, SharePoint passes the "LOGON_USER" variable into the embedded TotalAgility Integration Server forms to call the Integration Server API "UserService::GetSessionId()".

1. Map form variable, LOGON_USER to userId.
2. Provide 7 to logOnProtocol.
3. Map global variable, SESSION_ID to SessionId.
4. Map global variable, RESOURCE_ID to ResourceId.

The GetSessionId() API gets Integration Server session ID for the user if they are already logged on, otherwise it just logs the user. This avoids the need to provide a separate logon to the Integration Server forms that are integrated into SharePoint.

Note The SharePoint user *must* also be a user in Integration Server for single log on to work.

Add links to the "top level" Integration Server custom web pages in the SharePoint Quick Launch menu.

Add the TotalAgility Integration Server custom web pages to the SharePoint quick launch menu

1. Go to **Site Actions > Site Settings**.
2. Under Look and Feel category, click **Quick Launch**.
3. Add the following new headings and rename the headings if needed.

Heading	Web Address
TotalAgility Workqueue	/_layouts/WorkQueue.aspx?EmbeddedForm=WorkQueue.form Note Rename WorkQueue.form to point to your TotalAgility work queue form; do not change the name if the form is called WorkQueue.form. If the Quick Launch menu is on a subsite, prefix the subsite name in the link as follows: /SubSiteName/_layouts/WorkQueue.aspx?EmbeddedForm=WorkQueue.form

Heading	Web Address
TotalAgility Create Workflows	/_layouts/CreateJob.aspx?EmbeddedForm=Create%20Jobs.form Note Rename Create%20Jobs.form to point to your TotalAgility CreateNewJob form; do not change the name if the form is called Create Jobs.form. You can create multiple TotalAgility Create Workflow headings to point to different TotalAgility CreateNewJob embedded forms. If the Quick Launch menu is on a subsite, prefix the URL with SubSiteName as explained for TotalAgility Workqueue .
TotalAgility Workflows	/_layouts/JobList.aspx?EmbeddedForm=JobList.form Note Rename JobsList.form to point to your TotalAgility JobList form; do not change the name if the form is called JobList.form. If the Quick Launch menu is on a subsite, prefix the URL with SubSiteName as explained for TotalAgility Workqueue.

Add the create TotalAgility workflow context menu item to a document library

Provide context menu links in SharePoint document libraries to launch the TotalAgility Create Workflow custom page. Pass in the selected SharePoint document URL as an initialization variable to the new TotalAgility workflow or job so it can be used in Activity forms to provide hyperlinks to the document.

Before you add a new context menu item to a document library, complete the following steps:

1. Create a process with two initialization parameters, DOC_URL and DOC_NAME.
2. Build a Create New Job form and add these initialization parameters:
 - DOC_URL
 - DOC_NAME
 - LOGON_USER
3. Modify the Getinitvarlist action to clear the DOC_URL and DOC_NAME parameters to retain values from the query string.

Add the new context menu item:

1. Create a text file with the following JavaScript:

```
<script>
function Custom_AddDocLibMenuItems(m, ctx)
{
// parse the URL out of the itemTable
var URL = "";
var DocName = "";
var index = itemTable.innerHTML.indexOf("href=");
if (index > 0)
{
var str = itemTable.innerHTML.substr(index + 6);
index = str.indexOf('"');
if (index > 0)
{
URL = str.substr(0, index);
index = str.indexOf('>');
}
}
}

```

```

    var index2 = str.indexOf('<');
    DocName = str.substr(index + 1, index2 - index - 1);
  }
}
if (URL != "")
{
strAction = 'window.location = "http://[domainname]:
[Port Number]/[SubSiteName]/_layouts/CreateJob.aspx?DocUrl='
+ URL + '&DocName=' + DocName +
'&EmbeddedForm=[CreateNewJobFormName.form]";

    var strDisplayText = "Create workflow in TA";
    var strAction;
    var strImagePath = "";

    // Add menu item
    CAMOpt(m, strDisplayText, strAction, strImagePath);

    // add a separator to the menu
    CAMSep(m);
}
return false;
}
</script>

```

2. Replace [domainname] with the location of the SharePoint web application that contains the TotalAgility custom web pages.
3. If required, specify the SharePoint subsite name in [SubSiteName].
4. Replace the [CreateNewJobFormName.form] text with the name of your TotalAgility CreateNewJob form.
5. If required, rename the menu item display text "Create workflow in TA" in the script.
6. Upload this file to SharePoint Shared Documents.
7. Provide the link to this file in Content Editor Web Part:
 - a. Go to **Site Actions > Edit page**.
 - b. Click **Add a Web Part**.
 - c. In the **Media and Content** group, select **Content Editor Web Part**.
This mechanism injects JavaScript into the SharePoint page.
8. Save the changes to the SharePoint page and exit Edit mode.
A new menu item called "Create Workflow in TA" becomes available from the Context list for a document in this document library. Select the menu item to go to the CreateJob.aspx TotalAgility custom web page and pass in the document URL and name.
9. Add more context menu items to use multiple Create Workflow pages.

Configure the custom web pages

Perform the following steps if you configure the TotalAgility custom web pages in SharePoint.

1. Download a copy of existing Seattle.master from the Master Page gallery and rename it to KTA.master.
2. Open the KTA.master file in the editor.

3. To change the page logo to Kofax, update the LogoImageUrl as follows.
LogoImageUrl= <SharePoint:SiteLogoImage CssClass="ms-siteicon-img" name="onetidHeadbnnr0" id="onetidHeadbnnr2" LogoImageUrl="/_layouts/15/images/<Image>?rev=23" runat="server">
Replace <image> with the Kofax image name.
4. If using Internet Explorer, update the content attribute value of <meta> tag to "IE=Edge" in the KTA.master file as follows:
<meta http-equiv="X-UA-Compatible" content="IE=Edge"/>.
5. Upload the new KTA.master in the Master Page gallery as ASP NET Master Page file.
6. Publish the new KTA.master as a major version.
7. Set the new Master Page as Primary master page of your site.
8. Navigate to Site settings > Master Page and select the KTA.master page.
9. Update custom pages to use KTA.master.

Configure TotalAgility web parts in SharePoint server

Configure the SharePoint site that contains the Integration Server web parts to communicate with the Integration Server either using web services or enabling session.

Use web services

1. Open the `Web.config` file.
2. Add the key: <add key="SPPServerName" value="<TotalAgility server name><:port>/<SiteName>"/>. For example, <add key="SPPServerName" value="DL-WDEML-32:85">

Note the following:

- If you do not add the key, a message informs you that the web services communications layer to Integration Server is not configured.
- In the key do not mention the Port if running under port 80.

Enable session

1. Navigate to the `C:\Inetpub\wwwroot\VirtualDirectories\<Port>` folder.

Note Get the <Port> from address bar in Internet Explorer.

2. Open the `Web.config` file and do the following:
 - a. Search for "`<add name="Session">`" and uncomment this line.
 - b. Search for the "`<pages enableSessionState`" tag and change the "`enableSessionState`" attribute value from "`false`" to "`true`".

Set up the Microsoft SharePoint server and TotalAgility server to provide fault tolerance

Set up the TotalAgility server

Install MSMQ support:

1. Open Server Manager on the SharePoint Server.
2. Select to add Message Queuing feature.
3. Select the Message Queuing Server, Directory Service Integration and HTTP Support.

To set up the TotalAgility server:

1. Create a physical MSMQ queue on the TotalAgility Server:
 - a. Go to **Computer Management\Message Queuing\Private Queues**.
 - b. Create a Transactional private queue called: **TotalAgility/Services/Core/IntegrationEventService.svc**.

Note You must select the Transactional check box when creating the queue.

2. Enter the following two commands to configure IIS 7 to enable WAS to listen to the message queue and activate your service when new messages arrive:

```
appcmd set site "Default Web Site" -+bindings.
[protocol='net.msmq',bindingInformation='localhost']
appcmd set app "Default Web Site/TotalAgility" /
enabledProtocols:net.msmq,http
```

3. Open the Web.config file located in the TotalAgility\Agility.Server.Web folder in your install location, for example, C:\Program Files\Kofax\TotalAgility\Agility.Server.Web.
4. Add the following msmq binding in the <bindings> section:

```
<netMsmqBinding>
  <binding name="MsmqBindingTransactionalNoSecurity" maxRetryCycles="3"
receiveErrorHandling="Move" receiveRetryCount="3" retryCycleDelay="00:01:00">
  <security mode="None"/>
  </binding>
</netMsmqBinding>
```

5. Open the Web.config file located in the Core folder in your install location, for example, C:\Program Files\Kofax\TotalAgility\Agility.Server.Web\Services\Core, locate for <service name="Agility.Server.Core.Services.IntegrationEventService" behaviorConfiguration="Agility.Server.Web.Services.Behavior">.
6. Add the following endpoint below this service tag:

```
<endpoint address=
"net.msmq://localhost/private/TotalAgility/Services/Core/
IntegrationEventService.svc"
binding="netMsmqBinding" bindingConfiguration="MsmqBindingTransactionalNoSecurity"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService" /
>
```

7. Verify that the Microsoft Windows net.msmq Listener Adapter service is started.

Set up the Microsoft SharePoint server

1. Open the Web.config file for a SharePoint site.
2. Add the following tags under <bindings> section:

```
<netMsmqBinding>
  <binding name="MsmqBindingTransactionalNoSecurity" maxRetryCycles="3"
receiveErrorHandling="Move" receiveRetryCount="3" retryCycleDelay="00:30:00">
  <security mode="None"/>
  </binding>
</netMsmqBinding>
```

3. Add the following tags under <client> section:

```
<endpoint address=
"net.msmq://<TA_MACHINENAME>/private/TotalAgility/Services/Core/
IntegrationEventService.svc"
behaviorConfiguration="MsmqBindingTransactionalTransportSecurity"
binding="netMsmqBinding"
  bindingConfiguration="MsmqBindingTransactionalNoSecurity"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
name="Agility.Server.Core.Services.IntegrationEventService" />
```

4. Remove or comment out the following tag under <appSettings> section:

```
<add key="SPP_EventHandler_WebServiceURL" value="" />
```

5. Replace <TA_MACHINENAME> with the TotalAgility server name.

Chapter 4

Integrate Microsoft Dynamics CRM with TotalAgility Integration Server

To install and work with Dynamics CRM, users must have administrator rights.

Install Dynamics CRM

1. Navigate to `\\DynamicsCRMInstall` on the installation media, and double-click **Setup.exe**. The installation wizard appears.
2. Click **Next**.
3. In the **CRM Server URL** box, replace the `<ServerName>` with the CRM server name and replace `<Port>` with the port number on which CRM is running.
4. In the **CRM Service URL** box, replace the `<ServiceName>` with the CRM service name.
5. In the **Metadata Service URL** box, replace the `<MetaDataServiceName>` with the CRM metadata service name.
6. In the **Domain** box, enter the domain name.
7. Enter the **Username** and **Password**.
8. Click **Finish**. The installation starts and registers Event Handler in CRM and places necessary files in Global Assembly Cache (GAC).

Update the web configuration file for Dynamics CRM

Add the following script for the Integration Server components to support event handlers:

Note If you copy and paste the code from this guide, correct any incorrect line breaks.

```
<configSections>
<section name="exceptionHandling"
type="Microsoft.Practices.EnterpriseLibrary.
ExceptionHandling.Configuration.ExceptionHandlingSettings,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35" requirePermission="true" />
<section name="loggingConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.Logging.Configuration.LoggingSettings,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" requirePermission="true" />
```

```
</configSections>

<loggingConfiguration
name=""
tracingEnabled="true"
defaultCategory="General">
<listeners>
<add name="Event Log Listener"
type="Microsoft.Practices.EnterpriseLibrary.Logging.TraceListeners.
FormattedEventLogTraceListener,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
listenerDataType="Microsoft.Practices.EnterpriseLibrary.Logging.
Configuration.FormattedEventLogTraceListenerData,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
source="Total Agility" formatter="Text Formatter"
log="" machineName="." traceOutputOptions="None" />
</listeners>
<formatters>
<add type="Microsoft.Practices.EnterpriseLibrary.Logging.Formatters.TextFormatter,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
template="Timestamp: {timestamp}{newline}&#xA;Message: {message}
{newline}&#xA;Category: {category}{newline}&#xA;Priority:
{priority}{newline}&#xA;EventId: {eventid}
{newline}&#xA;Severity: {severity}{newline}&#xA;Title:
{title}{newline}&#xA;Machine: {localMachine}
{newline}&#xA;App Domain: {localAppDomain}
{newline}&#xA;ProcessId: {localProcessId}
{newline}&#xA;Process Name: {localProcessName}
{newline}&#xA;Thread Name: {threadName}
{newline}&#xA;Win32 ThreadId:{win32ThreadId}
{newline}&#xA;Extended Properties:
{dictionary({key} - {value}{newline})}"
name="Text Formatter" />
</formatters>
<categorySources>
<add switchValue="All" name="General">
<listeners> <add name="Event Log Listener" />
</listeners>
</add>
</categorySources>
<specialSources>
<allEvents switchValue="All" name="All Events" />
<notProcessed switchValue="All" name="Unprocessed Category" />
<errors switchValue="All" name="Logging Errors & Warnings">
<listeners> <add name="Event Log Listener" />
</listeners>
</errors>
</specialSources>
</loggingConfiguration>

<exceptionHandling>
<exceptionPolicies>
<add name="Agility Exception Policy">
<exceptionTypes>
<add name="All Exceptions" type="System.Exception, mscorlib,
```



```

Version=4.0.0.0,
Culture=neutral,
PublicKeyToken=b77a5c561934e089"
postHandlingAction="NotifyRethrow">
<exceptionHandlers>
<add name="Logging Exception Handler"
type="Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.
    Logging.LoggingExceptionHandler,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
logCategory="General" eventId="100" severity="Error"
    title="Total Agility"
formatterType="Microsoft.Practices.EnterpriseLibrary.
    ExceptionHandling.TextExceptionFormatter,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
priority="0" />
</exceptionHandlers>
</add>
</exceptionTypes>
</add>
</exceptionPolicies>
</exceptionHandling>

```

Update web.config for the CRM virtual directory

```

<system.serviceModel>
<bindings>
    <basicHttpBinding>
        <binding name="BasicHttpBinding_Service" openTimeout="00:10:00"
closeTimeout="00:10:00"
sendTimeout="00:10:00" receiveTimeout="00:10:00" allowCookies="true"
maxBufferSize="2147483647"
maxReceivedMessageSize="2147483647" maxBufferPoolSize="524288">
            <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
            <security mode="TransportCredentialOnly">
                <transport clientCredentialType="None" />
            </security>
        </binding>
    </basicHttpBinding>
</bindings>
<client>
    <endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"

    contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://<TotalAgility server name or IP Address>/TotalAgility/Services/Core/
IntegrationEventService.svc"/>
</client>
</system.serviceModel>

```

Note Replace <TotalAgility server name or IP Address> with the IP Address of the Integration Server.

Chapter 5

Integrate Microsoft Dynamics AX with TotalAgility Integration Server

To install and work with Dynamics AX,

- Users created in TotalAgility must have Deployment Administrator rights.
- If a user does not use the *default Deployment Administrator* to install the TotalAgility Dynamics AX integration, the user must meet the following conditions:
 - Be the system administrator in AX.
 - Have full CAL access.

Failure to meet the preceding criteria generates the following error message during installation: "System unable to process request error."

1. Navigate to the `//DynamicsAXInstall` on the installation media, and double-click **Setup.exe**. The Kofax TotalAgility for Dynamics AX Setup wizard appears.
2. Click **Next**.

The window displays a list of prerequisite software for Dynamics AX.

Note If the required software is not installed, you must first install the software and then install Dynamics AX. If using Dynamics AX 2009, install .NETFramework 3.5. If using Dynamics AX 2012, install .NETFramework 4.6.1.

3. Click **Next**.
The Destination window appears.
4. Use the information in the following table to specify file paths in the Destination Folder:

Destination Folder	Sample Path for Dynamics AX 2009	Sample Path for Dynamics AX 2012
DAX website Physical Location	C:\inetpub\wwwroot \MicrosoftDynamicsAXAif50\	C:\inetpub\wwwroot \MicrosoftDynamicsAXAif60
DAX website URL	Default Web Site/ MicrosoftDynamicsAXAif50/	Default Web Site/ MicrosoftDynamicsAXAif60/
DAX Client Physical Location	C:\Program Files\Microsoft Dynamics AX\50\Client\Bin\	C:\Program Files (x86)\Microsoft Dynamics AX\60\Client\Bin
DAX Server Physical Location	C:\Program Files\Microsoft Dynamics AX\50\Server \DynamicsAx1\Bin	-NA-

5. Click **Next**.
The Credentials window appears.

6. Enter your **Username** and **Password** to associate with DAX Application pool.
7. Click **Next**.
The system displays the installation status and a summary of installation report when installation is complete.
8. Click **Finish**.

Important If you are using 64 bit operating system and Dynamics AX 2009 32 bit application, enable the application pool account associated with the DAX Communicator site. In the IIS Manager, click Application Pools > DAXAppPool > Advanced Settings and set True for Enable 32-Bit Applications.

Create Dynamics AX service reference to the TotalAgility web service

As AOT (Application Object Tree) is in the Development Workspace, ensure to deploy the Development Workspace to add in references. Otherwise, you cannot integrate TotalAgility with Dynamics AX. See the Microsoft website for more information.

Create Dynamics AX 09 service reference to the TotalAgility web service

1. Click **AOT** (Application Object Tree) and press **Ctrl+D**.
2. In the application object tree, Right-click **References** and select **Add service reference**.
3. Complete the **Add service reference** window with the following information:
 - a. WSDL URL: Enter the web URL of the DynamicsAxIntegrationService within the Agility IIS web application. For example,
`http://Server/Agility.Server.Web/Services/SDK/DynamicsAxIntegrationService.svc`
 - b. .Net code namespace: **KtaEventsService**.
 - c. Reference name: **KtaEventsService**.
 - d. Service description: Description of the service reference.
4. Click **OK**.

Create Dynamics AX 12 service reference to the TotalAgility web service

1. Click **AOT** (Application Object Tree) and press **Ctrl+Shift+W**.
2. In the application object tree, right-click **References** and select **Add Reference**.
3. Browse to the TotalAgility assembly, KtaEvents.Services.dll that was installed previously. For example,
`C:\Program Files (x86)\Microsoft Dynamics AX\60\Client\Bin`
4. Click **OK**.

Add a reference

Add a reference to the `Agility.Server.Integration.Common.dll` assembly in Dynamics AX.

In Dynamics AX 09

1. Right-click **References** and select **Add reference**.
The assembly browsing form opens.
2. Browse to the **client\bin** directory of the Dynamics AX 09 installation. For example,
`C:\Program Files (x86)\Microsoft Dynamics AX\50\Client\Bin`
3. Select the **Agility.Server.Integration.Common.dll** assembly and click **OK**.
The newly added assembly appears under references.

In Dynamics AX 12

1. Right-click **References** and select **Add reference**.
2. Browse to the TotalAgility assembly, *Agility.Server.Integration.Common.dll*, that was installed previously. For example,
`C:\Program Files (x86)\Microsoft Dynamics AX\60\Client\Bin`
The newly added assembly appears under references.
3. Click **OK**.

Edit the service configuration file for Dynamics AX 12

1. Browse to the **client\bin** directory of the Dynamics AX where the WCF service configurations file, `KtaEvents.Services.dll.config` was copied by the installer.
2. Edit the endpoint to point to the valid TotalAgility Service for Dynamics AX notifications (`...Services/SDK/DynamicsAxIntegrationService.svc`).

Import the TotalAgility connector class into Dynamics AX

1. In the AOT, click **Import** or press **Ctrl+Shift+I**.
2. Browse to the Dynamics AX Setup installation directory. For example,
`C:\Program Files\Dynamics AX Setup\`
3. Select the XPO class, such as `Class_KtaController.xpo`.
4. Click **OK** to initiate the import or compilation process.

Note Once the class is imported, the status tab in the compiler output page displays any errors.

Edit Database X++ event methods

1. To alter the Application CUD (create, update and delete) class event methods, call the custom class method `EventChangeNotifyKtaWebService` when a CUD event is performed within Dynamics AX.
2. Edit the Application class methods (**InsertLog**, **DeleteLog** & **UpdateLog**) by adding a single line to the appropriate location within each method:
 - a. **Insertlog method:** `new ktaController().EventChangeNotifyKtaWebService("Create", recordInserted, null, conNull(), recordInserted.RecId);`
 - b. **Deletelog method:** `new ktaController().EventChangeNotifyKtaWebService("Delete", recordDeleted, null, conNull(), recordDeleted.RecId);`
 - c. **Updatelog method:** `new ktaController().EventChangeNotifyKtaWebService("Update", recordOrig, recordUpdated, changedFields, recordUpdated.RecId);`

Note The onsite AX administrator registers the `Databaselog` events for various AX documents. For example, if the *Customer*, *SalesOrder* and *Purchase Requisition* documents have the Insert, Update and Delete events registered against them, and when one of these events execute for one of these documents, TotalAgility is informed through a WCF call.

Verify the Application Pool account

Verify that the App Pool account is using the correct Business Connector.NET (BC.NET) Windows credentials.

1. On the Start menu, select **All Programs > Accessories > Run**.
2. Enter `inetmgr` and click **OK**.
The IIS Manager appears.
3. Navigate to Application Pool accounts.
4. Select the **DAXKTA** account and verify that the identity is the same as the BC.NET Windows credentials.
5. If the credentials differ, on the Actions panel, click **Advanced Settings**, select the identity and click **Edit**.
6. Click **OK**.
The Application Pool Identity window appears.
7. Click **Set**.
The Set Credentials window appears.
8. Enter the user credentials that are associated with the BC.NET account within Dynamics AX and click **OK**.

Note The Kofax WCF service uses the BC.NET account to connect to Dynamics AX.

Chapter 6

Integrate Micro Focus Content Manager server with TotalAgility Integration Server

This chapter provides the instructions for integrating Content Manager with the TotalAgility Integration Server.

Identify the Content Manager SDK version

1. Navigate to the `C:\Program Files\Kofax\TotalAgility\` folder.
2. Right-click **TrimSDKPIA20.dll** and select **Properties**.
The TrimSDKPIA20.dll properties window appears.
3. On the properties window, select the **Version** tab.
The File Version displays the current Content Manager version, such as 7.3.0.

Note For TRIM SDK 7.3.0 and later, you will require to enter this number in the <assemblyBinding> section of the Web.config file (See [Set up the Content Manager server](#)).

Set up the Micro Focus Content Manager server

To set up the Content Manager server, install and configure TotalAgilitytrimCommunicatorService and then configure the event handler in Micro Focus Content Manager.

Install and configure TotalAgilityTrimCommunicatorService

To install and work with Content Manager, users must have administrator rights.

1. Log on to the Content Manager server with an account with Local Administrator privilege.
2. Navigate to `\\ContentManagerInstallation` on the installation media, right click on the executable **Setup.exe** and **Run as administrator**.
The User Account Control window appears.
3. Click **Yes**.
The installation wizard appears.
4. Click **Next**.
5. Click **Finish**.

6. Configure **Web.config**:

- a. In `C:\Program Files\Kofax\TotalAgility\TotalAgilityTrimCommunicatorService`, open **Web.config** in a text editor.
- b. Locate the configuration > runtime tag and edit the <assemblyBinding> section as follows:

```
<assemblyBinding>
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
<dependentAssembly>
<assemblyIdentity name="TrimSdkPIA20"
publicKeyToken="533fc65e30e543fa" />
<bindingRedirect oldVersion="6.2.2.8614"
newVersion="<latest version>" />
</dependentAssembly>
</assemblyBinding>
```

Replace the <latest version> with the version of **TRIM SDK**. See [Identify the TRIM SDK version](#).

- c. Edit the <appSettings> section as follows:

```
<appSettings>
<add key="TrimDocumentRecordType"
value="DocumentRecordType" />
<add key="TrimFolderRecordType"
value="FolderRecordType" />
<add key="WorkGroupServerName" value="ServerName" />
</appSettings>
```

- Replace the DocumentRecordType with the document URI value. If you do not know the document URI value, enter **4**.
- Replace the FolderRecordType with the folder URI value. If you do not know the folder URI value, enter **3**.
- Replace the ServerName with the computer name of the Server.
To identify the computer name of the server, open **Windows Explorer**, right-click **Computer** and click **Properties**. In the Computer name, domain, and workgroup settings group, click **Change Settings**. Copy the computer name.

Important When you first install the TotalAgility Content Manager integration, a TrimIntegrationAppPool with a local system identity is created. This causes an error if the Content Manager server is remote.

To resolve this error, update the TrimIntegrationAppPool identity to an account with administrator permissions.

Configure the event handler in Content Manager

Configure TotalAgility events for actions in the Content Manager System.

1. Copy the following DLLs to the TRIM binaries directory (usually `C:\Program Files\Hewlett-Packard\HP TRIM`):
 - **Agility.Server.Integration.Trim.dll**
 - **Agility.Server.Integration.Model.dll**
 - **Agility.Server.Integration.Common**

2. To register the dll:
 - a. Open **Content Manager**.
 - b. Select **Tools > Context Administration > External Links**.
The TRIM Context External Links window appears.
 - c. Click **New Record AddIn**.
The Record AddIn Properties window appears.
 - d. Enter a Link Name.
 - e. In the COM Add-In PROGID box, enter the
ProgId,**Agility.Server.Integration.Trim.TrimIntegrationEventHandler**
 - f. Click **OK**.
The TRIM Context External Links window displays the new link.
 - g. Select the link and click **Properties**.
The Record AddIn Properties window appears.
 - h. Click the **Used By** tab.
 - i. Check the Document and File Folder under Record list and click **OK**.
This configures the Event handler on TRIM.
3. In C:\Program Files\Hewlett-Packard\HP TRIM\, open the **trim.exe.config** file in a text editor and add or replace the following tags:

Note If you cut and paste from this guide, correct any incorrect line breaks.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<configSections>
<section name="LoggingConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.Logging.Configuration.LoggingSettings,
Microsoft.Practices.EnterpriseLibrary.Logging, Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35" requirePermission="true" />
<section name="exceptionHandling"
type="Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Configuration.
ExceptionHandlingSettings,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling, Version=5.0.505.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="true" />
</configSections>
<exceptionHandling>
<exceptionPolicies>
<add name="Agility Exception Policy">
<exceptionTypes>
<add name="All Exceptions" type="System.Exception, mscorlib, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"
postHandlingAction="NotifyRethrow">
<exceptionHandlers>
<add name="Loggng Exception Handler"
type=
"Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging.LoggingExceptionHandler,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging,
Version=5.0.505.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35"
logCategory="General" eventId="100" severity="Error" title="Total Agility"
formatterType=
"Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.TextExceptionHandler,
```



```
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling, Version=5.0.505.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35"
priority="0" />
</exceptionHandlers>
</add>
</exceptionTypes>
</add>
</exceptionPolicies>
</exceptionHandling>
<system.serviceModel>
<bindings>
<basicHttpBinding>
<binding name="BasicHttpBinding_Service" openTimeout="00:10:00"
closeTimeout="00:10:00"
sendTimeout="00:10:00" receiveTimeout="00:10:00" allowCookies="true"
maxBufferSize="2147483647" maxReceivedMessageSize="2147483647"
maxBufferPoolSize="524288">
<readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
<security mode="TransportCredentialOnly">
<transport clientCredentialType="None" />
</security>
</binding>
</basicHttpBinding>
</bindings>
<client>
<endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://<TotalAgility server name or IP Address>/TotalAgility/Services/
Core/IntegrationEventService.svc"/>
</client>
</system.serviceModel>
</configuration>
```

Replace <TotalAgility server name or IP Address> with the IP Address of the TotalAgility server.

Chapter 7

Integrate Kofax SignDoc with TotalAgility

This chapter provides the instructions for integrating Kofax SignDoc with TotalAgility.

Set up the Kofax SignDoc server

Configure the Kofax SignDoc server to point to the relevant TotalAgility server to allow callback to occur when the signing is completed. The SignDoc server can be configured per SignDoc account to allow the same SignDoc server to callback to multiple TotalAgility servers.

Refer to the section on integration with TotalAgility in SignDoc documentation to know how to set up the SignDoc server to point to the TotalAgility server.

Chapter 8

Integrate Kofax Communication Manager with TotalAgility Integration Server

To integrate Kofax Communication Manager (KCM) server with TotalAgility Integration server, manually replace the placeholder, {http://ccmserver:port} in the following format-`http(s)://<CCMServer>:<Portnum>` in the Web.config file which is available in Agility.Server.Web.

KCM proxy installation on the Web server

This chapter describes two methods for installing the KCM Proxy Web server:

- [Silent installation](#)
- [Standard installation](#)

Ensure that the Microsoft plugin, Web Platform Installer is installed before installing the KCM Proxy Web server. You can install the Microsoft Web Platform from the Microsoft website.

Silent installation

1. On the installation media, navigate to `\\CCMProxyInstallation`.
2. Launch a Command Prompt window and run **Setup.exe** and enter the KCM Server URL in the following format: `http(s)://<CCMServer>:<Portnumber>`.
Provide the IP address and port number of the KCM server. The installer updates the Web.config file with KCM server details and enables the proxy rewrite rules on the web server (IIS).
3. Press **Enter**.
The KCM Proxy is installed in the silent mode.
The system generates a log file on the desktop which reports errors (if any).

Standard installation

1. On the installation media, navigate to `\\CCMProxyInstallation` and double-click **Setup.exe**. The **KCM Proxy Configuration** window appears.
2. Enter the **KCM Server URL** in the following format: `http(s)://<CCMServer>:<Portnum>`. The Web.config file is automatically updated with the KCM Server IP and the Port number.
3. Click **Configure**.
4. Click **OK**.

Chapter 9

Configure TotalAgility Integration Server for HTTPS communication

Enable SSL (Secure Sockets Layer) communication for the TotalAgility web layer and TotalAgility Core Worker to communicate with core services and Kofax Transformation Server.

To enable SSL for TotalAgility Application:

1. Open **Internet Information Services (IIS) Manager**.
2. Right-click the **Default Web Site** and click **Edit Bindings**.
3. Click **Add**.
 - a. On the **Type** list, select **HTTPS**.
 - b. On the **SSL certificate** list, select the certificate.
 - c. Click **OK**.
4. Click TotalAgility and click **SSL settings** on the Features tab.
 - a. Click **Require SSL**.
 - b. **Accept** the Client Certificates.
 - c. Click **Apply**.

Change the bindings in Integration Server Web.config file

1. Open `C:\Program Files\Kofax\TotalAgility\Agility.Server.Web\Web.config` file.
2. Uncomment the HTTPS SSL with application logon for all bindings.
3. Comment the HTTP with Windows authentication sections for all bindings.
4. Update `httpGetEnabled="false"` and `httpsGetEnabled="true"`.
5. Save the file.

Update the Kofax TotalAgility Core Worker

`Agility.Server.Core.WorkerService.exe.config` located in the `C:\Program Files\Kofax\TotalAgility\CoreWorkerService` directory for all client endpoints `BasicHttpsBinding_Service` and restart the TotalAgility CoreWorker service. The Kofax Transformation Designer can be updated to use SDK SVC accessed through SSL, by updating the connection within Kofax Transformation Designer options.

Chapter 10

KCM proxy installation on the Web server

This chapter describes two methods for installing the KCM Proxy Web server:

- [Silent installation](#)
- [Standard installation](#)

Ensure that the Microsoft plugin, Web Platform Installer is installed before installing the KCM Proxy Web server. You can install the Microsoft Web Platform from the Microsoft website.

Silent installation

1. On the installation media, navigate to `\\CCMProxyInstallation`.
2. Launch a Command Prompt window and run **Setup.exe** and enter the KCM Server URL in the following format: `http(s)://<CCMServer>:<Portnumber>`.
Provide the IP address and port number of the KCM server. The installer updates the Web.config file with KCM server details and enables the proxy rewrite rules on the web server (IIS).
3. Press **Enter**.
The KCM Proxy is installed in the silent mode.
The system generates a log file on the desktop which reports errors (if any).

Standard installation

1. On the installation media, navigate to `\\CCMProxyInstallation` and double-click **Setup.exe**. The **KCM Proxy Configuration** window appears.
2. Enter the **KCM Server URL** in the following format: `http(s)://<CCMServer>:<Portnum>`. The Web.config file is automatically updated with the KCM Server IP and the Port number.
3. Click **Configure**.
4. Click **OK**.

Update the KCM Server URL in TotalAgility Web.config

You can manually update the KCM Server URL in TotalAgility Web.config or run the Configuration tool and update the settings before setting up the integration to KCM.

Manually update the KCM Server URL in TotalAgility Web.config

1. Navigate to the installation directory for the TotalAgility server.
2. In a text editor, open **TotalAgility Web.config** from the following directory:

```
\\TotalAgility\Agility.Server.Web
```

3. Locate the following section:

```
<rewrite>
  <rules>
    <rule name="CCMInteractiveProxy" stopProcessing="true">
      <match url="CCM/Proxy/Interactive/(.*)" />
      <action type="Rewrite" url="{http://ccmserver:port}/ccm/Interactive/
{R:1}" />
    </rule>
    <rule name="CCMDesignerProxy" stopProcessing="true">
      <match url="CCM/Proxy/Repository/(.*)" />
      <action type="Rewrite" url="{http://ccmserver:port}/ccm/Repository/
{R:1}" />
    </rule>
    <rule name="ComposerUIJavascriptProxyRule" stopProcessing="true">
      <match url="CCM/Proxy/ccmcomposerui.js" />
      <action type="Rewrite" url="{http://ccmserver:port}/proxy/
ccmcomposerui.js" />
    </rule>
    <rule name="ComposerUICssProxyRule" stopProcessing="true">
      <match url="CCM/Proxy/ccmcomposerui.css" />
      <action type="Rewrite" url="{http://ccmserver:port}/proxy/
ccmcomposerui.css" />
    </rule>
    <rule name="ComposerUIImgProxyRule" stopProcessing="true">
      <match url="CCM/Proxy/img/(.*)" />
      <action type="Rewrite" url="{http://ccmserver:port}/proxy/img/{R:1}" />
    </rule>
    <rule name="CCMDesignerStaticProxyRule" stopProcessing="true">
      <match url="CCM/Proxy/static/(.*)" />
      <action type="Rewrite" url="{http://ccmserver:port}/ccm/static/
{R:1}" />
    </rule>
    <rule name="ComposerUIFontProxyRule" stopProcessing="true">
      <match url="CCM/Proxy/fonts/(.*)" />
      <action type="Rewrite" url="http://{ccmserver:port}/proxy/fonts/
{R:1}" />
    </rule>
  </rules>
```

4. Replace the `http://<ccmserver>:<port>` with the ccmserver URL.
5. Save and close the configuration file.

Using the Configuration Utility

Run the Configuration Utility and update the configuration settings. See the *Kofax TotalAgility Configuration Utility Guide*. (Navigate to Configuration settings >On-premise >App section).

Install KCM Proxy manually

You can install KCM proxy without using Web platform installer and KCM proxy installer.

1. Install IIS URL Rewrite 2.0.
2. Install Microsoft Application Request Routing 2.5 or higher for IIS.
3. In the IIS Manager, do the following:
 - a. On server level, double-click **Application request routing cache**.
 - b. Click **Server Proxy Settings**.
 - c. Select **Enable Proxy**.
 - d. Click **Apply**.
4. In TotalAgility web.config, find `{http://ccmserver:port}` and replace with `http://servername:port` where `servername` is the host name of the KCM machine and `port` is the port KCM listed as (default 8081). See [Manually update the KCM Server URL in TotalAgility Web.config](#).
5. Uncomment the `<rewrite>` section.
6. Save and close the configuration file.

Chapter 11

Launch TotalAgility Integration Server

1. Enter `http://[TotalAgility server hostname or IP]/TotalAgility/Designer/default.htm` URL in the browser.
2. Enter the login credentials of the tenant used during installation.
TotalAgility Designer is launched in the browser.
3. Alternatively, click **Start > All Programs > Kofax TotalAgility > Designer**.

Uninstall TotalAgility Integration Server

Uninstall using the wizard

1. Click **Start > All Programs > Kofax TotalAgility** and select **Uninstall or Repair Kofax TotalAgility**. The **Repair/Uninstall** window opens.
2. Select **Uninstall** and click **Next**. The **Uninstall** window opens.
3. Click **Next**. The **Uninstalling** window opens. When the uninstall is complete, the **Uninstallation Complete** window opens. The summary report lists the components, servers, applications and services uninstalled.
4. Click **Finish**.

Note If there are any errors during uninstall, Integration Server automatically creates a log file called **Kofax TotalAgilityInstallationErrorLog.txt** on your desktop. This log file contains information on errors.

Uninstall in silent mode

1. Navigate to the root directory of the **Setup.exe** file.
2. Run `Setup.exe /Silent/U`. The system uninstalls Integration Server and automatically creates a log file on your desktop. This log file contains information on errors, if any.

Note Uninstalling in silent mode will not only remove the applied fix pack or service pack but it will remove Kofax TotalAgility application completely. To install TotalAgility again, you must install its base version and then apply any patches again.

Chapter 13

Upgrade process

Navigate to TotalAgility Installation media and double-click **Setup.exe** and follow the upgrade instructions.

If any errors occur during upgrade, TotalAgility creates a log file called **Kofax TotalAgilityInstallErrorLog.txt** on your desktop. Fix the errors.

Important To upgrade TotalAgility from any version below 7.0.2. to 7.6.0, you must migrate to 7.0.2 first, and then upgrade 7.0.2 to 7.6.0. See the *Kofax TotalAgility Migration Guide*.

On upgrade, the TotalAgility Integration Server installer restores the following configuration settings:

- All existing AppSettings
- All existing Security Bindings

Upgrade TotalAgility Integration Server in silent mode

1. Go to the root directory of setup.exe.
2. Open the Command Prompt window as an Administrator and change the command line to the root directory of Setup.exe.
3. Run `Setup.exe /Silent /Upgrade`.

The system generates a log file which reports errors (if any).

The success or failure of installation is indicated in the event log.

Troubleshooting

This section describes the issues you may encounter and their resolution.

TotalAgility Integration Server AppPool exists

Integration Server creates an application pool called TotalAgilityAppPool. Ensure you do not have an existing application pool of the same name as it may cause issues when installing or upgrading.

Site location invalid error

SharePoint security issues can occur when the TotalAgilitySharePointCommunicator web service hosted in IIS does not have permission to access the SharePoint site in IIS. This can cause a "Site location is invalid" error when integrating TotalAgility with SharePoint.

To resolve this issue:

1. Ensure the TotalAgilitySharePointCommunicator web service is running under the same application pool as your SharePoint site. Depending on the security trust level within SharePoint, TotalAgility can cause communication failures between TotalAgilitySharePointCommunicator and SharePoint due to permissions.
2. Turn off ASP impersonation on the TotalAgilitySharePointCommunicator web service in IIS (if enabled); ASP impersonation is not supported by the SharePoint application pool and may cause permission issues with remote SharePoint and TotalAgility servers.