Kofax TotalAgility
On-Premise Multi-Tenant Installation Guide

Version: 7.10.0

Date: 2021-12-12

KOFAX

Table of Contents

Preface

This guide provides the instructions for installing Kofax TotalAgility On-Premise Multi-Tenant 7.10.0.

Read this guide completely before installing the software.

Use the Kofax TotalAgility On-Premise Multi-Tenant installation media to install:
- Tenant management system (used to create and manage tenants)
- Live (production) environment
- Development environment

For on-premise multi-tenancy, the development and live environments must be installed on separate servers to ensure the development server workload does not affect the live server workload. For Tenant Management System, we recommend that you do not create the Tenant Management site on the Application server because the Tenant Management System has to directly communicate with the on-premise multi-tenancy web server via SDK APIs to upgrade the tenants. The Tenant Management System should either be installed on the Web server or on another server. You can also install Tenant Management System on the Application server, only if the application server has direct access to the Web server.

After installing Kofax TotalAgility On-Premise Multi-Tenant system, you must create a tenant to access the system.

Related documentation

The full documentation set for Kofax TotalAgility is available at the Product documentation page.

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 Integration Server Installation Guide*: Describes how to install Kofax Integration Server and integrate it with other products.
- *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 KofaxTransformation Modules projects to TotalAgility.

Offline documentation

Customers who require offline documentation can download the individual zip files available on a per language basis, such as Kofax TotalAgilityDocumentation7.10.0_EN.zip and Kofax TotalAgilityDocumentation7.10.0_DE.zip from the Kofax Fulfillment Site.

See Access the TotalAgility documentation for more information

Training

Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the Kofax Education Portal on the Kofax website.

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:

1. Go to the Kofax website home page and select **Support**.

2. When the Support page appears, select **Customer Support** > **Knowledge Base**.

> ⓘ 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.

From the Knowledge Base home page, you can:
- Access the Kofax Community (for all customers).

  Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Installation planning

For information on supported operating systems and other system requirements, see the *Kofax TotalAgility Technical Specifications* document on the Product Documentation page site. The document is updated regularly, and we recommend that you review it carefully to ensure success with your TotalAgility product.

Review these important notes before you proceed with the installation.

- To view information on the system requirements for installing TotalAgility, instructions for running the prerequisite utility, and the software checklist for various installation types, download the Kofax TotalAgility Prerequisites Guide from the Kofax Fulfillment Site.

  For additional prerequisites for the Transformation Server, see Transformation Server prerequisites.

- If your solution includes multiple Kofax products, review the Kofax Technical Specifications document.

- Obtain a license key for TotalAgility from your Account Manager or Kofax Support.

- Before extracting the TotalAgility installation ZIP file, unblock the file from the file properties window.

- The TotalAgility servers should run on the same time zone, because issues may occur if they run on different time zones.

- Upgrade installations of Kofax Transformation Designer that connects to TotalAgility 7.10.0.

- TotalAgility includes a limited number of VRS Elite licenses. You may need to purchase additional licenses, depending on the number of scanners you plan to use with VRS. See the Kofax Scanner Configurator to verify VRS certification and licensing requirements for your scanner.

- The Transformation Designer does not come with the Kofax TotalAgility On-Premise Multi-Tenant installation. Please download it from the TotalAgility eDelivery site.

After installing TotalAgility On-Premise Multi-Tenancy, you can update the configuration settings by modifying each file separately or by running the configuration utility. The utility allows you to modify or update the settings across multiple configuration files at one go instead of editing each file separately. You must manually copy the utility onto each server where the configuration settings are to be modified. See the *TotalAgilityConfiguration Utility Guide*.

Transformation Server prerequisites

Transformation Server is installed on a different computer from TotalAgility.

The computer should have a multi-core processor. Other processor and memory-intensive processes should not run on the same computer as Transformation Server. The computer does not require IIS or a database. The .NET Framework is installed automatically with Transformation Server.

For prerequisites, see the *Kofax TotalAgility Prerequisites Guide* available on the Kofax Fulfillment Site. For additional prerequisites, see the following sections

Enable support for 8.3 short file names (sfn)

Before installing the Transformation Server, enable NTFS to generate 8.3 sfn for long file names and for file names that contain characters from the extended character set. Use one of the following methods:

Windows Server 2008 R2 or Later

1. Log in as Administrator and open a Command Prompt window.

2. Run **cmd.exe**.

3. Run **fsutil.exe 8dot3name set 0**.

Other Operating Systems

1. Run **regedit.exe** to open the registry editor.

2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem` and set the value of the `NtfsDisable8dot3NameCreation` key to **0**.

For more information on file names, see the Microsoft website.

Configure the user account

When installing Transformation Server, provide a user account for running the Transformation Server service. The user account used to run the service must be a member of the administrators group which allows creating a Windows user for each tenant that runs a transformation process, so that tenants cannot access each other's data. With administrator rights, Windows users can create other users.

For an on-premise installation with multi-tenancy, the account must have certain user rights and permissions:

1. Log on as Administrator and open a Command Prompt window.

2. Run **secpol.msc**.

3. Under **Security Settings**, navigate to **Local Policies**, click **User Rights Assignment**, and ensure the account has following permissions:
   - Adjust memory quotas for a process.
   - Create a token object.
   - Log on as a service.
   - Replace a process level token.
   - In addition to the preceding permissions, for Windows Server 2012, add the user to the Local Administrative group.

4. Add the account that Transformation Server will be using for each of these settings.

For security, Transformation Server uses a single user group per computer and a single user account per tenant. The first time Transformation Server receives activity for a tenant, the user group and account are created:

- User account: TU<GUID> (truncated to 20 characters)
- Local group: TenantUsers

The user account has all permissions except to execute files, and it uses the same database authentication mechanism as all Kofax TotalAgility components. These user account permissions prevent malicious scripts from running on the server. Other permissions, including bypassing traverse checking and the ability to use Web services, are necessary for operation.

The TenantUsers group also contains tenant users, which are created automatically as needed. These users do not have access to Transformation Server configuration files and cannot execute scripts. The tenant user accounts are deleted when the server stops.

Install databases manually

1. Create the MasterTenants and DataCenterTenants databases.
2. Run the following scripts on MasterTenants database.
   Example
   - Create_MasterTenants.sql
   - Initialise_MasterTenants.sql
3. Run the following scripts on DataCenterTenants database.
   Example
   - Create_DataCenterTenants.sql
   - Initialise_DataCenterTenants.sql
   - Create_KLS_OnPremiseTenants.sql
4. Run the MasterTenantsManScript.sql script after updating the server name and system session ID values inside the script.

   > ℹ️
   >
   > - The <servername> is the machine name.
   > - For [SYSTEM_SESSION_ID]: Get the value from [DataCenterTenants].[dbo].[SERVER_DATA] table of [SYSTEM_SESSION_ID] column value.

5. In the Installation wizard, in the Tenant Databases window, do the following:

   a. Clear the check box for "Overwrite Databases if they exist?".

   b. Rename the databases under **Database Name** to match with the names given while creating databases manually.

   c. Click **Next**. Ensure the installation completes before updating the configuration files.

6. You can edit the value of the database connections in the Web.config manually or run the Configuration Utility available on the installation media.

   - Open Web.config located in the `TotalAgility\Agility.Server.Web` directory in your installation location and change the following settings for the DataCenterTenants database.

     ```
     <add key="TenantDBConnectionString"
      value="Server=(local);Trusted_Connection=Yes;Database= DataCenterTenants ;"/>
     ```

     The server value is the database server name where the DataCenterTenants databases reside.

     > 🛈 Skip this step when you install databases on the same computer where TotalAgility is installed, as the setup.exe automatically updates Web.config with the machine name. However, check Web.config to ensure the DataCenterTenants database configuration is correct.

   - Run the Configuration Utility and modify the DataCenterTenants database connection value available on the Common settings tab.

7. To modify the value of MasterTenants database in Web.config, do either of the following:

   - Open Web.config located in AgilityServer.Web.TenantManagement and change the following settings for the MasterTenants database.

     ```
     <add key="MasterTenantDBConnectionString"
      value="Server=(local);Trusted_Connection=Yes;Database=MasterTenants;"/>
     ```

     The Server value is the database server name where the MasterTenants databases reside.

     > 🛈 Skip this step when you install databases on the same computer where TotalAgility is installed, as the setup.exe automatically updates Web.config with the machine name. However, check the Web.config file to ensure the MasterTenants database configuration is correct.

   - Run the Configuration Utility and modify the MasterTenantDBConnectionString value available on the TMS tab.

Configure 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.

Any SSL certificates being used must be fully trusted. If no certificates exist, obtain a wildcard certificate. Different certificates should be used for the live and development environments.

Wildcard SSL certificates secure the website URL and an unlimited number of its sub-domains. For example, a single wildcard certificate *.TotalAgility.com can secure tenant1.TotalAgility.com, tenant2.TotalAgility.com, and tenant3.TotalAgility.com.

Create a single SSL certificate using split Web-Application and Tenant Management system

Use Subject Alternative Names (SAN) to create a single SSL certificate to use for Kofax TotalAgility on-premise installation that is using split Web-Application and Tenant Management System on the same deployment.

For example, create a single SSL certificate if you have Web and Application servers as follows:
- web.kta.com is for Tenant Management System on the Web server.
- *.web.kta.com is for multiple tenants on the Web server .
- app.kta.com is for Tenant Management System on the Application server.
- *.app.Kofax.com for multiple tenants on the Application server.

1. Set the Subject Alternative Names section to the Fully Qualified Domain Names you wish to use in the certificate request.
   You can add as many entries as required.
2. Generate the SSL certificate request file and submit it to a Certificate Authority (CA) for signing.
3. Install the pfx certificate in the system and IIS by importing the pfx certificate file on both Web and Application servers.

> ⓘ To create a single SSL certificate for secure Web server and non-secure Application server, install the pfx certificate in the system and IIS by importing the pfx certificate file on the Web server, if you have Web and Application servers as follows:
> - web.kta.com (for Tenant Management System on the Web server)
> - *.web.kta.com (for multiple tenants on the Web server)

Update Web.config

1. Open **Web.config** located at your installed location. The default location is:

   `C:\Program Files\Kofax\TotalAgility\Agility.Server.Web`

2. In `<servicebehaviors>`, the `httpsGetEnabled` setting is as follows:

   ```
   <serviceBehaviors>
    <behavior name="Agility.Server.Web.Services.Behavior">
    <serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
   </serviceBehaviors>
   ```

3. By default, HTTPS mode is used with `<security mode="Transport">`. For the `BasicHttpBinding_SharepointReceiverService`, update the `<security>` setting as follows:

   If using HTTPS authentication, comment out the HTTP section:

   ```
   <!-- HTTPS SSL with application authentication-->
   <security mode="Transport">
   <transport clientCredentialType="None"/>
   ```

```
</security>
```

> ℹ️ For Windows or Manual authentication, the SharePoint Receiver Service must use anonymous binding for HTTPS authentication.

Import an SSL certificate

1. Open **Internet Information Services (IIS) Manager**.
2. On the **Features View**, double-click **Server Certificates**.
3. Under **Actions**, click **Import**.
4. Browse and select the certificate name.
5. Enter password.
6. Click **OK**.

Import a non-SSL certificate

1. Type inetmgr from the command prompt and press Enter.
2. Double-click **Server Certificates**.
3. Select **Create Self-Signed Certificate**.
4. Enter a **Certificate Name** and click **OK**.
5. Right-click **Default web site** and select **Enable Bindings**.
6. Click **Add**.
7. Select **Https** as **Type**.
8. Select **SSL Certificate** and then click **OK**.

You must secure cookies post installation. See Secure cookies.

Licensing information

This section provides information on licensing details.

Concurrent user licensing

In the Concurrent User model, many users can simultaneously log into the system. Each user session consumes a license. For example, if a single user logs into the TotalAgility Designer and the TotalAgility Workspace simultaneously or the user logs into the Designer in two browsers such as Internet Explorer and Chrome, the user consumes two concurrent licenses. When a user logs off from a session, the license server automatically releases the license.

When the number of concurrent users reaches the maximum, the system automatically checks for available reserved licenses. If any reserved license is available, a new user can log on and the count of available reserve licenses is reduced by 1. Keep the following items in mind when managing reserved licenses:

- A reserved license expires seven days after you begin using the license.
- You can use each reserved license only twice within 12 months.

If the user tries to log on after the number of concurrent logons reaches the limit and there are no reserved licenses, the system displays an error message and additional users cannot log on.

If a reserved license expires, an error message appears in the TotalAgility Designer and TotalAgility Workspace.

Activate a license in TotalAgility

The license period starts once the license is activated. So you can skip activation during installation and only activate it when you are ready to use TotalAgility.

Activate a license in TotalAgility On-Premise Multi-Tenancy

If you log on to TotalAgility On-Premise Multi-Tenancy and the license is not activated, the License Activation window appears.

1. In the **License Activation** window, do either of the following:
   - Click **Next** to accept the default values for the **License Server** and **Port Number**.
   - Enter the new values.
2. Click **Set license server** to save the information.
3. For further instructions, see Activate the License Server step in Install Application server

   ⓘ If you have issues activating your licence, contact Kofax support at: `http://www.Kofax.com/support/tools/`

Automatic recovery

After TotalAgility installation, it is possible to manually configure the Kofax License Server Service to automatically restart in the event of a service error.

1. Go to **Service Control Manager**.
2. Edit the properties for the Kofax License Server Service.
3. Go to the **Recovery** tab.
4. Configure options for how the service should respond after the first, second, and subsequent failures.

   You do not need to restart the service for the changes to take effect.

   ⓘ You can also do this configuration at the command line. Example:

   ```
   sc.exe failure KSALicenseService actions= restart/660000/
   restart/660000/""/660000 reset= 86400
   ```

Reporting Server

Kofax Reporting provides centralized storage of historical operational metrics and audit data. Kofax Reporting includes components, such as the reporting service and databases.

> ❗ Due to high process utilization by Transformation Server (99%), Reporting Server is known to produce **SQL Timeout** error when installed on the same machine as Transformation Server. Therefore, you must install Reporting Server separately from Transformation Server.

Kofax VRS Elite

We highly recommend Kofax VRS Elite, a patented image perfection software that dramatically improves scanning productivity and document capture efficiency when used with a VRS-certified scanner. If your scanner is not VRS-certified, you can use the Kofax image processing technology included with TotalAgility.

Several Kofax VRS licensing options are available:

Kofax VRS Basic or Professional OEM
Automatically activate a Kofax VRS Basic or Professional OEM license that is included with many industry-standard scanners. License activation for these scanners is required only when upgrading to Kofax VRS Elite.

Standalone workstation
Manually activate a standalone license, which stays on the workstation until it is deactivated. The standalone license can only be activated on one scan station at a time.

TotalAgility license server
Centrally manage concurrent VRS Elite licenses from the TotalAgility license server.

To centrally manage VRS licenses through the TotalAgility license server, each VRS station needs to communicate with the license server directly or through a license proxy.

Web Capture Service

To enable web scanning, you must install the Kofax Web Capture Service. When installing through the browser, you must have administrative rights to complete the installation.

Install the Kofax Web Capture Service either at the default location or to a custom location.

You must install the Web Capture Service only once, and web scanning is enabled across all the supported browsers.

Temporary files are created under the folder "Interprocess". The user must have read/write access to this folder.

You can also use the Web Capture Service on multiuser environments.

Scan Agent Service

The Scan Agent Service is an asynchronous upload capability, which allows scan operator to continue on to the next batch, without needing to wait for the previous scan job to complete upload.

This service is useful in remote scanning scenarios, where the scan station has limited network bandwidth to the main TotalAgility site.

The capability allows scan operator to keep up with physical scanning throughput, while image upload is done in the background, thus enhancing the scan operator efficiency.

This feature is only available for Scan Create New Job forms.

A Scan Create New Job form automatically uses the asynchronous image upload mode if it detects Scan Agent Service installed on the scan station. Otherwise, it uses the synchronous image upload mode if the Scan Agent Service is not detected.

For Device Create New Job form, a pre-condition of [SCANNED] > 0 must be added to the first activity in a process, to allow the process to wait for all images to be uploaded before moving on to the first activity.

Chapter 2

TotalAgility On-Premise Multi-Tenancy installation

This chapter describes two methods for installing TotalAgility on-premise multi-tenancy.

- Silent installation for multiple servers that use the same configuration.
- Standard installation using the standard installation wizard.

You can install TotalAgility on-premise multi-tenancy as one of the following types:

- **Database Only**: Installs only the database components of Kofax TotalAgility no other components are installed.
- **Upgrade Databases**: TotalAgility installer upgrades the MasterTenant and DataCenter databases to the latest version of TotalAgility when TotalAgility is not installed locally.
- **Web Server**: Installs a server to point to any Application server. In case you install TotalAgility on a computer other than the default port, you must enter the Application Server machine name and port number. For example, `<appserver_name:82>`. A Web server installs the SDK Services and user interfaces for the Designer and Workspace. See Install Web Server.
- **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. See Install Application Server or Web-Application Server.
- **Web and Application Server**: Installs the Web and Application servers on a single computer. See Install Application Server or Web-Application Server.

> ⓘ
> - You must have administrator account to install TotalAgility.
> - Ensure that the user who will run TotalAgility has "Log on as Service" rights.
> - You can use hotkeys to navigate to next screen.

Perform a silent installation

Use the silent installation to install TotalAgility On-Premise Multi-Tenancy automatically from a command line or a batch file. After you edit the silent installation file, the installation proceeds without any further user interaction. SSL is automatically set to True.

See also:

- Silent installation for Database only
- Silent installation for upgrading databases

- Silent installation of Web and Application on the same server
- Silent installation on a separate Web and Application Server
- Silent installation of Real Time Transformation Server

Silent installation of database only

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

Parameter	Default Value	Description
LiveHostName		Enter the Live deployment host name. This should be the Live Web Server machine name.
		When using the LiveHostName to access TotalAgility, the format of the name should be `hostname: port number`.
		Host Name: When you are using a load balancer and a public DNS, the Host name text should be the Fully Qualified Domain Name (FQDN), such as `kta.app.com`; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed.
		Port Number: Use port number when TotalAgility is installed on a non-standard TCP port. You can ignore the port number when TotalAgility is installed on a default port.
DevHostName		Enter the Dev deployment host name. This should be the Dev Web Server machine name.
		When using the DevHostName to access TotalAgility, the format of the name should be `hostname: port number`.
		Host Name: When you are using a load balancer and a public DNS, then Host name text should be the Fully Qualified Domain Name (FQDN), such as `kta.app.com`; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed.
		Port Number: Use port number when TotalAgility is installed on a non-standard TCP port. You can ignore the port number when TotalAgility is installed on a default port.
DatabaseInformation		
InstallDatabases	true	Accept the default to automatically install the databases. Set to false to ignore installing databases.
OverwriteIfExisting	false	Set to true to overwrite the existing databases. ⓘ If the existing database details are not valid, or if the databases does not exist, an errors occurs and the installation fails.
MasterTenantDatabase		

Parameter	Default Value	Description
DatabaseName	MasterTenants	Accept the default.
Server	Server Name	Specify the name of your machine.
Security		
WindowsAuthentication	true	Set to true to use Windows credentials for logging in. If set to false, provide the username and password. Otherwise, leave the username and password blank. ⓘ Configure this setting for the DataCentre database also.
UserName	empty	
Password	empty	
NewDatabase	false	Set to true to create new database. ⓘ Configure this setting for the DataCentre database also.
DataCentreDatabase		
DatabaseName	DataCenterTenants	Accept the default.
Server	Server Name	Specify the name of your machine.
Install Info		
InstallType	DatabaseOnly	Accept the default. ⓘ When you only install database, the services, such as Core Worker Service, Reporting Service, License Service, Transformation Server are ignored and not installed.
<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. Run `Setup.exe /Silent`.

   The databases are installed automatically.

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

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

   When automating the installation, if you run setup.exe from the 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

See also:

• Silent installation for upgrading databases

- Silent installation of Web and Application on the same server
- Silent installation on a separate Web and Application Server
- Silent installation of Real Time Transformation Server

Silent installation for upgrading databases

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

Parameter	Default Value	Description
<ServicesInstallOptions>		
	true for all the services.	Set to false for all the services. ⓘ When you upgrade TotalAgility databases, the services, such as Core Worker Service, Reporting Service, License Service, Transformation Server are ignored and not installed.
LiveHostName		Enter the Live deployment host name. This should be the Live Web Server machine name. When using the LiveHostName to access TotalAgility, the format of the name should be `hostname: port number`. **Host Name**: When you are using a load balancer and a public DNS, the Host name text should be the Fully Qualified Domain Name (FQDN), such as `kta.app.com`; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed. **Port Number**: Use port number when TotalAgility is installed on a non-standard TCP port. You can ignore the port number when TotalAgility is installed on a default port.
DevHostName		Enter the Dev deployment host name. This should be the Dev Web Server machine name. When using the DevHostName to access TotalAgility, the format of the name should be `hostname: port number`. **Host Name**: When you are using a load balancer and a public DNS, then Host name text should be the Fully Qualified Domain Name (FQDN), such as `kta.app.com`; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed. **Port Number**: Use port number when TotalAgility is installed on a non-standard TCP port. You can ignore the port number when TotalAgility is installed on a default port.
DatabaseInformation		

Parameter	Default Value	Description
InstallDatabases	true	Set to false to ignore installing databases. If set to true, installs the databases.
OverwriteIfExisting	false	Set to true to overwrite the existing databases. ⓘ If the existing database details are not valid, or if the databases does not exist, an errors occurs and the installation fails.
MasterTenantDatabase		
DatabaseName	MasterTenants	Accept the default.
Server	Server Name	Specify the your machine name.
Security		
WindowsAuthentication	true	Set to true to use Windows credentials for logging in. If set to false, provide the username and password. Otherwise, leave the username and password blank. ⓘ Configure this setting for the DataCentre database also.
UserName	empty	
Password	empty	
NewDatabase	false	Accept the default. If set to true, creates new database.
DataCentreDatabase		
DatabaseName	DataCenterTenants	Accept the default.
Server	Server Name	Specify the your machine name.
Install Info		
InstallType	Both	Change the value to UpgradeDatabasesOnly. ⓘ All the databases are upgraded to the latest version of TotalAgility. Upgrading databases prior to TotalAgility 7.3.0 is not supported when TotalAgility is not installed locally.
<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. Run `Setup.exe /Silent`.

The databases are installed automatically.

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

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

When automating the installation, if you run setup.exe from the 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

See also:

- Silent installation for Database only
- Silent installation of Web and Application on the same server
- Silent installation on a separate Web and Application Server
- Silent installation of Real Time Transformation Server

Silent installation of Web and Application on the same server

Update the following parameters for an Application or Web-Application server installation.

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` and open SilentInstallConfig.xml using a text editor.

2. In the SilentInstallConfig.xml, update the following parameters.

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

Parameter	Default Value	Description
ServicesInstallOptions		
CoreWorkerService	true	You can set it to true/false, as needed.
ReportingService	true	You can set it to true/false, as needed.
LicenseService	true	You can set it to true/false, as needed.
TransformationService	true	You can set it to true/false, as needed.
CoreServices	true	You can set it to true/false, as needed. Set to false to install only Transformation Server on the Application server so that IIS prerequisite is not needed. IIS is not required for standalone installation of the Transformation Server.
LicenseServer		
LicenseServerName	localhost	Enter the name of the license server.
PortNumber	3581	Do not change this value.
SerialNumber	no default	Enter your TotalAgility on-premise multi-tenancy serial number.

Parameter	Default Value	Description
ProductCode	no default	Enter your TotalAgility on-premise multi-tenancy product code.
SkipLicense	true	Use the default value to skip activating the license. ⓘ If SkipLicense is set to FALSE, you must enter the serial number and product code.
ServerId	1	Sets primary or backup license server: • `1`: The license server is set as a primary license server. • `2`: The license server is set as a backup license server.
IsDatabaseWindowsAuthentication	false	Set to true to use Windows authentication to connect to SQL Server.
InstallDirectory	C:\Program Files\ Kofax\TotalAgility	Specify the TotalAgility destination directory.
SsLEnabled	true	Accept the default.
InstallTenantManagementWebsite	true	Accept the default.
DatabaseInformation		
OverwriteIfExisting	false	Set to true to overwrite the existing databases. ⓘ If the existing database details are not valid, or if the databases does not exist, an errors occurs and the installation fails.
ScriptsLocation	C:\Program Files\Kofax\TotalAgility \DatabaseScripts\ SQL Server \	Specify the directory for installing scripts.
MasterTenantDatabase		
DatabaseName	MasterTenants	Accept the default.
Server	Server Name	Specify your machine name.
Security		
WindowsAuthentication	true	Set to true to use Windows credentials for logging in. If set to false, provide the username and password. Otherwise, leave the username and password blank. ⓘ Configure this setting for the DataCentre database also.

Parameter	Default Value	Description
UserName	empty	
Password	empty	
NewDatabase	false	Set to true to create new database. ⓘ Configure this setting for the DataCentre database also.
DataCentreDatabase		
DatabaseName	DataCenterTenants	Accept the default.
Server	Server Name	Specify the name of your machine.
IdentityInformation		
UserName	empty (false)	Enter the name of the user who will run TotalAgility. Only required if RunAsSystemAccount is false.
Password	empty (false)	Enter the password for the user. Only required if RunAsSystemAccount is false.
RunAsSystemAccount	false	If set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. ⓘ If you set this parameter to true, databases should be created using SQL authentication.
RunAsNetworkServiceAccount	false	If set to true, the AppPool and Kofax TotalAgility services are created with the NT Authority\Network Service username. ⓘ • Set RunAsNetworkServiceAccount to true only for Docker installations that want to make use of a Group Managed Service Account (gMSA). • If you set this parameter to true, databases should be created using SQL authentication.
InstallInfo		
InstallAction	MultiTenancyInstall	Accept the default.
InstallMode	Silent	Accept the default.
InstallType	Both	Accept the default.
MultiTenancyInstallMode	Live	Accept the default for Live environment or enter "Dev" for a Development environment.

Parameter	Default Value	Description
DatabaseServerType	SQLServerNonSSL	Accept the default, or use the SQL Azure database, enter **SQLAzure**.
CacheType	InMemory	InMemory cache
EmailConfig		
HostName	host name	Enter the host name, such as `smtp.office.com`.
PortNumber	port number	Enter the port number, such as 387.
UserName	username	Enter the username, such as Kofax@kofaxindiapvtlimited.com
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, Kofax@kofaxindiapvtlimited.com.
TransformationServerInfo		
ℹ Configure these settings if TransformationService is "true".		
TSConfigFile	empty	Specify the path to .ini file along with the name for Transformation Server to configure. ❗ If you provide the .ini file, the TransformationServerInfo settings are taken from the .ini file; the parameters (with their default values) mentioned in the SilentMultiTenancyInstallConfig are ignored. See .INI file sample for the parameters.
LogFile	`C:\Program Files \Kofax\TotalAgility \Transformation Server \Tslog.txt`	Specify the location where the Transformation Server log file will be created. If the log file path is not valid, the Transformation Server installation fails. Example: `C:\Program Files \Kofax\TotalAgility \TransformationServer`
InstallLocation	For example, `C:\Program Files (x86)\Kofax\ TotalAgility\ TransformationServer`	Specify the Transformation Server destination directory.
WindowsServiceAccount	no default	Enter the name of the user who will run Transformation Server.

Parameter	Default Value	Description
WindowsServicePassword	no default	Enter the password for the user who will run Transformation Server.
UseSpecificPool	false	Set to true to add this Transformation Server to a pool. Set to false (or leave blank or assign any other value) to have Transformation Server process all activities regardless of pool.
PoolName	empty	If UseSpecificPool is set to true, enter the Transformation Server pool name. ℹ If you leave the pool name empty, all activities are processed regardless of their pools.
OLEnabled	true	Set to true to enable online learning.
WcfPort	9001	Enter the port used by TotalAgility to communicate with the Transformation Server during synchronous calls (such as fuzzy searches and pushed activities).
ReservedSlots	0	Enter the number of slots on this Transformation Server that are reserved for pushed activities and high-priority activities.
OverrideDefSlots	empty	To override the default number of processing slots for this Transformation Server, set this parameter to true. Any other value, including empty, is treated as false and the system automatically sets the default number of processing slots based on the system configuration.
MaxSlots	0	If you set OverrideDefSlots to true, enter the number of processing slots for this Transformation Server.
InstallOCRAddons	1	Installs additional OCR engines (A2iA CheckReader and A2iA FieldReader).
EnableSyncCalls	true	Set to true to enable synchronous calls for a Transformation Server instance. false or any other value disables these calls.
NlpWestern	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
NlpWesternExtended	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.

Parameter	Default Value	Description
NlpExtended	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.
<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.
CaptureConfiguration		
CloudStorageType	SQLServer	By default, the capture data is stored in the SQL Server. Change the Cloud Storage Type to "Azure" for Windows Azure Blob Storage, "AWS" for Amazon S3 storage and "SqlFileStream" for SQL Server and File System.
AzureBlobStorageConnectionString	empty	The Account Connection String to connect to the Blob storage service.
AzureBlobStorageContainerName	empty	The Container Name of the storage service.
AmazonS3AccessKey	empty	The access key to connect to the Amazon S3 storage service.
AmazonS3SecretKey	empty	The secret key to the Amazon S3 storage service.
AmazonS3BucketName	empty	The bucket name of the storage service. Bucket is a fundamental container in Amazon S3 for data storage.
AmazonS3RegionName	empty	The S3 region name.
TenantFileStorageRootPath	empty	The path for tenant file storage

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

5. Run `Setup.exe /Silent`.

Based on the parameters set to **True** in the silent configuration file, the following items are installed:

- Kofax TotalAgility

> ⓘ TotalAgility services will be installed but the tenant databases will not be created until a tenant is created.

- Core Worker Service
- Reporting Service
- Licensing Service
- Transformation Server, if the TransformationService parameter is set to true, and the WindowsServiceAccount and WindowsServicePassword parameters are set for Transformation Server.

The system generates a log file that reports any errors.

When automating the installation, if you run setup.exe from the 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

.INI file sample

```
TS_INSTALLLOCATION= C:\Program Files\Kofax\TotalAgility\Transformation Server
TS_SERVICE_ACCOUNT=username
TS_SERVICE_PASSWORD=password
TS_SERVER_SERVICE_URL=http://servername/TotalAgility/Services/Core/ServerService.svc
TS_USE_SPECIFIC_POOL=FALSE
TS_POOL_NAME=
TS_OL_ENABLED=TRUE
TS_WCF_PORT=9001
TS_RESERVED_SLOTS=0
TS_OVERRIDE_DEF_SLOTS=
TS_MAX_SLOTS=0
TS_ENABLE_SYNC_CALLS=TRUE
TS_MAIN_DB_CONNECTION_STRING=Server=servername;Trusted_Connection=Yes;
Database=totalagility;
TS_STARTSERVICE=TRUE
TS_SYNCHRONOUS_ONLY=false
TS_TENANT_DB_CONNECTION_STRING=Server=servername;Trusted_Connection=Yes;
Database=datacentername;
TS_MULTITENANT_INSTALL=1
```

See also:
- Silent installation for Database only
- Silent installation for upgrading databases
- Silent installation on a separate Web and Application Server
- Silent installation of Real Time Transformation Server

Silent installation on a separate Web and Application Server

Install TotalAgility on a separate Web and Application server.

Silent installation on an Application server

Update the following parameters for an Application Server.

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` and open SilentInstallConfig.xml using a text editor.
2. In SilentInstallConfig.xml, update the following parameters.
   - InstallType = ApplicationServer.
   - WebServerName = Enter the name of the web server.

     > ⓘ If the Web server is installed on a non-standard port, you must modify the <WebServerName> parameter in the SilentInstallConfig.xml on the Application server as follows:
     >
     > `<WebServerName>FQDN:portnumber</WebServerName>`

   - For other parameters, see Silent installation of Web and Application on the same server.

     > ⓘ You can choose to install or not to install certain components by setting the values to True/False in the ServicesInstallOptions section of the Silent Configuration file.

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

5. Run `Setup.exe /Silent`.

Based on the parameters set to **True** in the silent configuration file, the following items are installed:

- Kofax TotalAgility

  ⓘ TotalAgility services will be installed but the tenant databases will not be created until a tenant is created.

- Core Worker Service
- Reporting Service
- Licensing Service
- Transformation Service

  ⓘ When you choose to install only Transformation service on the Application server, set Transformation Service to true and Core Worker Service to false. If you do not exclude Core Services, TotalAgility will prompt for IIS requirement, and IIS is not required for installing the Transformation service on an Application Server.

The system generates a log file that reports any errors.

When automating the installation, if you run setup.exe from the 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

Silent installation on a Web server

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

Parameter	Default Value	Description
InstallDirectory	`C:\Program Files\ Kofax\ TotalAgility`	Specify the TotalAgility destination directory.
IsDatabaseWindowsAuthentication	false	Set to true to use Windows authentication to connect to SQL Server.
SSLEnabled	true	Accept the default.
InstallTenantManagement Website	true	Accept the default.

Parameter	Default Value	Description

ApplicationServerName	App server name	Enter the Fully Qualified Domain Name (FQDN) of the Application server.
		
		🛈 If the Application server is installed on a non-standard port, you must modify the <ApplicationServerName> parameter in the SilentInstallConfig.xml on the Web server as follows:
		`<WebServerName>`
		`FQDN:portnumber`
		`</WebServerName>`

IdentityInformation		
UserName	empty (false)	Enter the name of the user who will run TotalAgility.
Password	empty (false)	Enter the password for the user.
RunAsSystemAccount	false	If set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. 🛈 If you set this parameter to true, databases should be created using SQL authentication.
RunAsNetworkServiceAccount	false	If set to true, the AppPool and Kofax TotalAgility services are created with the NT Authority\Network Service username. 🛈 • Set RunAsNetworkServiceAccount to true only for Docker installations that want to make use of a Group Managed Service Account (gMSA). • If you set this parameter to true, databases should be created using SQL authentication.
InstallInfo		

Parameter	Default Value	Description
InstallAction	MultiTenancyInstall ⓘ For upgrade, specify InstallAction as MultiTenancyUpgrade.	Accept the default.
InstallMode	Silent	Accept the default.
InstallType	Both	Enter WebServer
MultiTenancyInstallMode	Live	Accept the default for Live environment or enter "Dev" for a Development environment.
DatabaseServerType	SQLServerNonSSL	Accept the default or enter **Azure**.
CacheType	InMemory	InMemory Cache
EmailConfig		
HostName	host name	Enter the host name, for example, `smtp.office.com`.
PortNumber	port number	Enter the port number, for example, 387.
UserName	username	Enter the username, for example, `kofax@kofaxindiapvtlimited.com`.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered, for example, `kofax@kofaxindiapvtlimited.com`.
UseSSL	false	Enter the SSL certificate to use HTTPS communication.
SupportInternationalCharacters	false	Enter the email address in which international characters are used.
<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. Save and close the file.
4. On the Command Prompt, change the command line to the root directory of the Setup.exe file.

5. Run `Setup.exe /Silent.`

    The system generates a log file that reports any errors.

    When automating the installation, if you run setup.exe from the 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

See also:

- Silent installation for Database only
- Silent installation for upgrading databases
- Silent installation of Web and Application on the same server
- Silent installation of Real Time Transformation Server

Silent installation of Real Time Transformation Server

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

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

Parameter	Default Value	Description
InstallDirectory	`C:\Program Files\ Kofax\ TotalAgility`	Specify the TotalAgility destination directory.
IsDatabaseWindowsAuthentication	false	Set to true to use Windows authentication to connect to SQL Server.
DatabaseInformation		
InstallDatabases	false	Set to false to ignore installing databases.
OverwriteIfExisting	false	Set to true to overwrite the existing databases. > ⓘ If the existing database details are not valid, or if the databases does not exist, an errors occurs and the installation fails.
DataCenter Database		
DatabaseName	TotalAgility tenant	Specify the name of the DataCenter database.
Server	server name	Specify the fully qualified domain name (FQDN) of the server.
Security		

Parameter	Default Value	Description
WindowsAuthentication	false	Set to true to use Windows credentials for logging in.
		If set to false, provide the username and password. Otherwise, leave the username and password blank.
UserName	empty	
Password	empty	
NewDatabase	false	Accept the default as the user connects to an existing datacenter database.
Tenant Database		
DatabaseName	TotalAgility tenant	Specify the name of the tenant database.
Server	server name	Specify the fully qualified domain name (FQDN) of the server.
		ⓘ When installing TotalAgility with a remote database, update SilentInstallConfig.xml with the server name (<Server>servername</Server>) of the machine on which the database resides. The account used to connect to the database during the installation requires rights to create databases.
Security		
WindowsAuthentication	false	Accept the default.
UserName	empty	Provide the username and password specified when creating the tenant.
Password	empty	
NewDatabase	false	Accept the default as the user connects to an existing tenant.
KofaxHostedTenant	false	Set to true when you point to existing azure databases.
Identity Information		
UserName	username	Enter the user name of the Windows service account for the TotalAgility services.

Parameter	Default Value	Description
Password	password	Enter the password of the windows service account for the TotalAgility services. ⓘ If the service account name ends with a $ (dollar), do not specify the password.
RunAsSystemAccount	false	If set to true, the AppPool and Kofax TotalAgility services are created with LocalSystem account. ⓘ When you set this parameter to true, databases should be created using SQL authentication.
RunAsNetworkServiceAccount	false	If set to true, the AppPool and Kofax TotalAgility services are created with the NT Authority\Network Service username. • Set RunAsNetworkServiceAccount to true only for Docker installations that want to make use of a Group Managed Service Account (gMSA). • If you set this parameter to true, databases should be created using SQL authentication.
Install Info		
InstallType	Both	Set to RTTS. ⓘ When you install RTTS, it ignores the services. The services such as CoreworkerService, ImportService, ExportService are not installed.
SslEnabled	true	Accept the default.
Transformation Server Info		
TransformationService	true	Accept the default.

Parameter	Default Value	Description
TSConfigFile	no default	Specify the path to .ini file along with the name for Transformation Server to configure. ❗ If you provide the .ini file, the TransformationServerInfo settings are taken from the .ini file; the parameters mentioned in the SilentInstallConfig are ignored. See the .INI file Sample for the parameters.

LogFile	`C:\Program Files`
	`\Kofax\TotalAgility`
	`\Transformation Server`
	`\Tslog.txt`
		Specify the location where the Transformation Server log file will be created. If the log file path is not valid, the Transformation Server installation fails.
		Example:
		`C:\Program Files`
		`\Kofax\TotalAgility`
		`\TransformationServer`
		`\TSLog.txt`

InstallLocation	For example, `C:\Program Files (x86)\Kofax\ TotalAgility\ TransformationServer`	Specify the Transformation Server destination directory.
WindowsServiceAccount	username	Enter the name of the user who will run the Transformation Server.
WindowsServicePassword	password	Enter the password for the user.
UseSpecificPool	false	Set true to add this Transformation Server to a pool. Set false (or leave blank or assign any other value) to have Transformation Server process all activities regardless of pool.
PoolName	empty	If you set UseSpecificPool=true, enter the Transformation Server pool name. ℹ If you leave the pool name empty, all activities are processed regardless of their pools.

Parameter	Default Value	Description
OLEnabled	true	Set to true to enable online learning tasks on this Transformation Server instance. Set to false or any other value to disable online learning tasks. ⓘ In case where multiple instances of Transformation Server are installed for improving the throughput of the capture activities, online learning should be enabled only on a single transformation server instance in the cluster.
WcfPort	9001	Enter the port that is used by TotalAgility to communicate with Transformation Server during synchronous calls (such as fuzzy searches and pushed activities).
ReservedSlots	0	Enter the number of slots on this Transformation Server that are reserved for pushed activities and high-priority activities.
OverrideDefSlots	empty (false)	To override the default number of processing slots for this Transformation Server, set this parameter to true. Any other value, including empty, is treated as false and the system automatically sets the default number of processing slots based on the system configuration.
MaxSlots	0	If you set CPUSERVER_OVERRI DE_DEF_ SLOTS to true, enter the number of processing slots for this Transformation Server.
EnableSyncCalls	true	Set to true to enable synchronous calls or false to disable these calls.
NlpWestern	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
NlpWesternExtended	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.

Parameter	Default Value	Description
NlpExtended	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.
StartServices	true	
<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. Save and close the file.
4. On the Command Prompt, change the command line to the root directory of the Setup.exe file.
5. Run `Setup.exe /Silent`.
   The Real Time Transformation Server is installed. The Real Time Transformation Service sets up Transformation Server in a synchronous mode and configures the core and SDK APIs of TotalAgility which clients can invoke.

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

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

   When automating the installation, if you run setup.exe from the 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

See also:
- Silent installation for Database only
- Silent installation for upgrading databases
- Silent installation of Web and Application on the same server
- Silent installation on a separate Web and Application Server

Perform a standard installation

You can install TotalAgility on-premise multi-tenancy using the standard installer wizard.

See also:
- Standard installation of database only
- Standard installation for upgrading databases
- Standard installation of the Web server
- Standard installation of the Application server
- Standard installation of the Web and Application server

- Standard installation of Real Time Transformation Server (RTTS)

Standard installation of Database Only

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.

2. In the **Kofax TotalAgility Multitenancy Installation** window, click **Next** or press Enter to move to the next window.

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

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

4. In the **Type of Install** window, select **Database Only**.

5. Click **Next**.
   The **Software Checks** window opens. The system displays a list of required software and whether the software is installed.

6. 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**.
     The **Databases** window opens.

7. Enter the database name for Master and DataCenter databases.

   a. If the database with the same name already exists, and if you want to overwrite the existing database, select the **Overwrite databases if they exist?** check box.
      The **Test connections** option becomes available.

   b. To test the database connections, click **Test connections**. Once the database connections are successfully established, click **Next**. On confirmation to overwrite, the databases will be re-initialized and the existing data will be lost.

      > ⓘ If the database details are not valid, or if the database does not exist, connection to database fails.

   c. If you are not using the local server and want to create databases on a different machine, enter a name for the databases; click ellipsis for **Server**; select the database server where the databases reside; in the **Security** group, either use **Windows Authentication**, or select the **SQL Server Authentication** (default) providing the user name and password, and then click **OK**. If all the databases reside on the same server, select the **Apply these settings to all other Databases** check box.

8. Enter the **Live Deployment Hostname** and **Dev Deployment Hostname** in the following format: `<Fully qualified domain name: port>`.
   These should be the Live and Dev Web Server machine names.

9. Click **Next**.
   The **DB Connection Results** window opens and displays the results of connecting to databases.

   > ⓘ If the connection to database fails, the installation cannot be progressed. Click **Back** and make changes as needed.

10. Once the databases are successfully connected, click **Next**.
    The **Installation Progress** window opens. The setup installs the required files, databases, and other integrated products.
    The **Licensing** window opens.

11. To connect to the license server, do the following:

    a. In the **License Server** field, enter the location of the License Server.

       > ⓘ To connect to the shared License Server, enter the name or the IP address of the shared License Server.

    b. In the **Port Number** field, enter the port number on which the License Server listens.

12. Click **Next**.
    Alternatively, click **Skip** if you want to skip connecting to the License Server now but connect when launching TotalAgility.

13. Click **Finish**.
    Your installation is now complete.

    > ⓘ Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

Standard installation for upgrading databases

1. On the TotalAgility installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.

2. In the **Kofax TotalAgility Multitenancy Installation** window, click **Next** or press Enter to move to the next window.

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

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

4. In the **Type of Install** window, select **Upgrade Databases**. (Default: Web/Application Server)

5. Click **Next**.

    The **Databases** window opens.

6. To specify the lower version databases to upgrade, do the following for the Master and DataCenter databases as needed: enter the database name to upgrade; click ellipsis for **Server** and select the **Database Server** where the databases reside; in the **Security** group, either use **Windows Authentication**, or select the **SQL Server Authentication** (default) providing the user name and password, and then click **OK**. If all the databases reside on the same server, select the **Apply these settings to all other Databases** check box and click **OK**.

7. Click **Next**.

    The **Installation Review** window opens.

8. Review the settings and click **Next** to start the installation.

    The **Installation Progress** window displays the progress of installation. The setup upgrades TotalAgility databases.

    Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

9. Click **Finish**.
    Your installation is now complete.

Standard installation of the Web server

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.

2. In the **Kofax TotalAgility Multitenancy Installation** window, click **Next** or press Enter to move to the next window. Click **Cancel** or press Esc to exit setup.

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

4. In the **Type of Install** window, select **Web Server** and click **Next**.

5. In the **Environment Type** window, select either environment type from the following and click **Next**:

    -   **Live**: Installs the production environment.
    -   **Dev**: Installs the development environment.

    The **Software Checks** window opens. The system displays a list of required software and whether the software is installed.

6. 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**.

      The **Destination** window opens.
7. Use the default installation folder or click **Browse** to select a different path and click **Next**.

    The **Tenant Management website** window opens.
8. If you choose not to deploy the Tenant Management system as a separate installation, select the **Install Tenant Management components** check box to install the Tenant Management components. (Default: Clear)
9. Click **Next**.

    The **Choose Server Location with Options** window opens.
10. Enter the **Server Name** or provide the IP Address.

    > ⓘ You must enter the name of the TotalAgility Multi Tenant Server machine. You must provide the server name (port number, if it is other than the default port) in the following format: `<machinename>.<fullyqualifieddomainname>:<portnumber>`.

    - If installing Live, open the Application server's Web.config file, copy the TotalAgilityHostNameLive app setting value and paste it into the Server Name box in the wizard.
    - If installing Dev, open the Application server's Web.config file, copy the TotalAgilityHostNameDev app setting value and paste it into the Server Name box in the wizard.
11. Click **Next**.

    The **Credentials** window opens.
12. Enter the credentials for the user who will run the TotalAgility On-Premise Multi-Tenancy.

    > ⓘ If the service account name ends with a $ (dollar), do not specify the password.

13. On the **Root Website to host TotalAgility Application** list, select the website to host the TotalAgility application. By default, the **Default Web Site** is selected.

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

14. Click **Next**.

    The **Installation Review** window opens and displays the settings.
15. Review the settings and click **Next**.

    The **Installation Progress** window opens. The setup installs the required files, databases, and other integrated products.
16. Click **Finish**.

    Your installation is now complete for the Web Server.

    Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog"

type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

Standard installation of the Application server

On performing standard installation for the Application Server, based on the install type selected, the following items are installed automatically:

- TotalAgility
- Core Worker Server
- Reporting Server
- License Server (Primary and Backup)

  If the primary license fails, the system automatically connects to the backup license server.
- Transformation Server

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.
2. In the **Kofax TotalAgility Multitenancy Installation** window, click **Next** or press Enter to move to the next window.

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

3. In the **Kofax Inc. Software License Agreement** window, accept the terms in the License Agreement and click **Next**.
4. In the **Type of Install** window, select **Application Server** and click **Next**.
5. In the **Environment Type** window, select either of the following:
   - **Live**: Installs the production environment.
   - **Dev**: Installs the development environment.

   The **Application Server** window opens.
6. By default, all Windows Services and WCF Services are selected and installed. If you do not want to install any service, clear the check box for the service.

   The Windows Services include:
   - Core Services
   - Reporting Service
   - License Service (Primary license server or Backup license server)

     By default, the Primary server is selected. If the primary license server fails to connect, you can connect to the backup server by manually updating the license server configuration file, or run the Configuration Utility post TotalAgility installation to automatically update the setting. Also, after upgrading TotalAgility from versions prior to 7.7.0, you must reconfigure

the license server by updating the settings to use the new licensing behavior. See Update the settings for a license server.

- Transformation Service

> ⓘ When you choose to install only Transformation service on the Application server by excluding all other Windows services, you must also clear the check box for WCF Core Services. If you do not exclude WCF Core Services, TotalAgility setup.exe will prompt for IIS requirement, and IIS is not required for installing the Transformation service on an Application Server.

The WCF Services include Core Services.

7. Click **Next**.

   The **Software Checks** window appears. The system displays a list of required software and whether the software is installed.

8. 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**.

     The **Destination** window opens.

9. Use the default installation folder or click **Browse** to select a different path and click **Next**.

   The **Tenant Management website** window opens.

10. If you choose not to deploy the Tenant Management system as a separate installation, select the **Install Tenant Management components** check box to install the Tenant Management components. (Default: Clear)

11. Click **Next**.
    The **Email Configuration** window opens.

12. Enter the details for the SMTP configuration.

    a. **Host Name**, such as smtp.office.com

    b. **Port Number**, such as 587

    c. **User Name**, such as Kofax@kofaxindiapvtlimited.com

    d. **Password**

    e. **From Address**: Email address from where the email is sent. For example, Kofax@kofaxindiapvtlimited.com

    f. **BCC**: Email addresses of the users who need to receive the copy of the email.

    g. Select **Enable SSL** to use HTTPS communication.

    h. Select **Enable Support International Characters** to enable the support for international characters in the email address.

    An email is triggered from the configured SMTP server when the tenant is created.

13. Click **Next**.
    The **Credentials** window opens.

14. In the **Credentials** window, enter the credentials for the user who will run TotalAgility On-Premise Multi-Tenancy.

    > ℹ If the service account name ends with a $ (dollar), do not specify the password.

15. On the **Root Website to host TotalAgility Application** list, select the website to host the TotalAgility application. By default, the **Default Web Site** is selected.

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

16. Click **Next**.
    The **Tenant Databases** window opens.

17. Enter the database name for the Master and DataCentre databases.

    a. If the database with the same name already exists, and if you want to overwrite the existing database, select the **Overwrite databases if they exist?** check box.

       The **Test connections** option becomes available.

    b. To test the database connections, click **Test connections**. Once the database connections are successfully established, click **Next**. On confirmation to overwrite, the databases will be re-initialized and the existing data will be lost.

       > ℹ If the database details are not valid, or if the database does not exist, connection to database fails.

    c. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**.

    d. If you are not using the local server, click the ellipsis and select the Master and DataCentre databases.

    e. If you want to manually install the databases, see Install databases manually. For a clean installation, run the setup.exe wizard to this screen, and do not select the **Overwrite databases if they exist?** check box.

    f. If you want to point to existing databases in a different machine, enter a name for the databases; click ellipsis for **Server**; select the database server where the databases reside; in the **Security** group, either use **Windows Authentication**, or select the SQL Server authentication providing the user name and password, and then click **OK**. If all the databases reside on the same server, select the **Apply these settings to all other Databases** check box.

       > ℹ If you have already selected the check box for Windows authentication for databases in the Tenant Databases window, you can only use the Windows Authentication in the Security group.

    > ℹ If you install TotalAgility without any databases, you can use the Configuration Utility to point to the databases when they are available at a later a stage. See the *Kofax TotalAgility Configuration Utility Guide*.

18. Once the databases are successfully connected, click **Next**.
    The **Capture Binary Data Storage** window opens.

19. By default, the binary data such as capture documents, .NET Store DLLs and CCM Packs are stored in the TotalAgility database. You can use the preconfigured external cloud data storage services such as Amazon S3 or Windows Azure Blob Storage for saving and processing the binary data. The cloud services helps to reduce the SQL Server maintenance costs, delegate maintenance to external service and provide encryption.

    ⓘ If you change the storage type to Azure/Amazon blob storage, the binary data is saved in the selected storage type. Once the cloud storage is enabled, you cannot turn it off later.

    Select one of the following capture data storage types:

Storage type	Description
SQL Server (default)	Stores capture data in the SQL Server.
SQL Server and File System	Stores the tenant FILESTREAM groups that are created when creating a tenant. Under **File storage settings**, specify the root folder on the SQL machine to store these FILESTREAM groups.
Windows Azure Blob Storage	Stores capture data in Azure Blob Storage service. Under **Cloud Account Settings**, enter the **Account Connection String** to connect to the Blob storage service. ⓘ The Container name for capture data storage is automatically created by the installer.
Amazon S3	Configure the following **Cloud Account Settings**: a. Enter the **Access Key** to connect to the Amazon S3 storage service. b. Enter the **Secret Key**. c. On the **Region** list, select a predefined S3 region, for example Asia Pacific (Sydney). (Default: US East (Ohio) ⓘ The Bucket name for data storage is automatically created. Bucket is a fundamental container in Amazon S3 for data storage.

20. Click **Next**.

    ⓘ The FILESTREAM is only supported with Windows authentication if the storage type is SQL Server and File System. If you do not select the check box for "Use Windows authentication for tenant databases" in the Databases window, a warning appears stating FILESTREAM is not supported with SQL authentication or when databases do not exist.

    The **DB Connection Results** window opens.

    ⓘ If the connection to database fails, the installation cannot be progressed. Click **Back** and make changes as needed.

21. Once the databases are successfully connected, click **Next**.
22. On-Premise Multi-Tenant runs on a single data center, therefore you must provide the Web server location to connect to the On-Premise Multi-Tenant data center. In the **Choose WebServer Location** box, enter the **Server Name** in the following format: `<machinename>.<fullyqualifieddomainname>:<portnumber>` where <servername> is the name of the On-Premise Multi-Tenant Web Server machine. Alternatively, you can provide the port number if it is other than the default port.

   > ⓘ You can modify the name of the Web Server if you want to point to another Web Server machine later by running the following SQL command:
   >
   > ```
   > UPDATE [MasterTenants].[dbo].[DATA_CENTER] SET [LIVE_HOST_NAME] =
   >  '<WebServerName>/ TotalAgility ',
   > [DEV_HOST_NAME] ='<WebServerName>/TotalAgility'
   > ```
   >
   > Running the SQL command is not required if you are pointing the application to the existing database by running the Configuration tool.

23. Click **Next**.
    The **Install Options** window opens.
24. To automatically start the services, keep the **Automatically Start Services** check box selected.
25. Click **Next**.
    The **Installation Review** window opens and displays the settings.
26. Review the settings and click **Next**.
    The **Installation Progress** window appears. The setup installs the required files, databases, and other integrated products. The **Licensing** window opens.
27. To connect to the License Server, perform the following steps:

    a. In the **License Server** field, enter the location of the License Server.

       > ⓘ To connect to the shared License Server, enter the name or the IP address of the shared License Server.

    b. In the **Port Number** field, enter the port number on which the License Server listens.

    c. Click **Next**. The second Licensing window opens.

       > ⓘ To skip connecting to the License Server now but connect when launching TotalAgility, click **Skip** and proceed to the next step.

28. Enter your TotalAgility **Serial Number** and **Product Code**.

    > ⓘ The ID of the selected License Server appears in the **Machine ID** field. The **Serial Number** and **Product Code** appear by default if the License Server is shared.

29. To activate the license, select the license activation method:
    - **Automatic**: Use this option when Internet connectivity is available. The license is activated online.

- **Manual**: Use this option when there is no Internet connectivity or if automatic activation is not successful from the installer or license utility for your Kofax product. The Activation Code box is displayed. To obtain the activation code:

  a. Enter the following URL in your browser:

     `http://activatelegacy.Kofax.com/support/Activation/manual.aspx`.
     The Kofax Product License Activation page appears.

  b. Enter the **Serial Number** issued to you at the time of purchase. If you have a hardware key, the serial number (usually 7 characters) is printed on the key.

  c. Enter the email address where Kofax can send the information you need to activate the product license.

  d. Click **Next** to proceed with the activation process.

     > ⓘ Ignore the **Version** selection field if you do not have Kofax Capture or Ascent Capture.

  e. Copy and paste the **Activation Code** into the field on the **Licensing** window.

  f. Either click **Activate** to activate the license or click **Skip** to skip activating license. If you skip activating the license, a warning informs that you need to activate the license later.

     > ⓘ The license period starts once the license is activated. You can skip activation during installation and only activate it when you are ready to use TotalAgility. You must activate the license when you log in to TotalAgility for the first time.

The **Kofax TotalAgility Installation Complete** window displays the summary of the installation.

> ⓘ Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

30. Click **Finish**.
    - Your installation is now complete. See Log on to TotalAgility On-Premise Multi-Tenancy for more information.
    - The Transformation Server installation window appears.

      > ⓘ The Transformation Server installation window only appears if you have selected the transformation service option in the **Application Server** window.

31. Click **Yes** to install Transformation Server.
    The installation for Transformation Server is launched. See Transformation Server Bundle installation.

Standard installation of the Web and Application server

On performing standard installation for the Web-Application Server, based on the installation type selected, the following items are automatically installed:

- TotalAgility
- Core Worker Server
- Reporting Server
- License Server (Primary and Backup)

  If the primary license fails, the system automatically connects to the backup license server.

- Transformation Server

  1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.

  2. In the **Kofax TotalAgility Multitenancy Installation** window, click **Next** or press Enter to move to the next window.

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

  3. In the **Kofax Inc. Software License Agreement** window, accept the terms in the License Agreement and click **Next**.
  4. In the **Type of Install** window, select **Application Server** or **Web/Application Server** and click **Next**.
  5. In the **Environment Type** window, select either of the following:

     - **Live**: Installs the production environment.
     - **Dev**: Installs the development environment.

  6. Click **Next**.

     The **Application Server** window opens.

  7. By default, all the Windows Services are selected and installed. If you do not want to install any service, clear the check box for the service.

     The Windows Services include:

     - Core Services
     - Reporting Service
     - License Service (Primary license server or Backup license server)

       By default, the Primary server is selected. If the primary license server fails to connect, you can connect to the backup server by manually updating the license server configuration file, or run the Configuration Utility post TotalAgility installation to automatically update the setting. Also, after upgrading TotalAgility from versions prior to 7.7.0, you must reconfigure the license server by updating the settings to use the new licensing behavior. See Update the settings for a license server.

     - Transformation Service

8. Click **Next**.
    The **Software Checks** window appears. The system displays a list of required software and whether the software is installed.
9. 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**.
        The **Destination** window opens.
10. Use the default installation folder or click **Browse** to select a different path and click **Next**.
    The **Tenant Management website** window opens.
11. In the **Tenant Management website** window, select the checkbox for **Setup Tenant Management website**.

    > ℹ This website helps you to launch the Tenant Management website in the browser.

12. Click **Next**.
    The **Email Configuration** window opens.
13. Enter the details for the SMTP configuration.
    a. **Host name**, such as smtp.office.com
    b. **Port Number**, such as 587
    c. **User Name**, such as kofax@kofaxindiapvtlimited.com
    d. **Password**
    e. **From Address**: Email address from where the email is sent. For example, Kofax@Kofax indiapvtlimited.com
    f. **BCC**: Email addresses of the users who need to receive the copy of the email.
    g. Select **Enable SSL** to use HTTPS communication.

       > ℹ If HTTPS is being used in TotalAgility Designer, when you link TotalAgility servers in some browser a prompt appears for you to select a client certificate and authenticate yourself. Ignore the prompt as TotalAgility will automatically pass any specified client certificate when required.

    h. Select **Enable Support International Characters** to enable support of international characters in the email address.
    An email is triggered from the configured SMTP server when the tenant is created.
14. Click **Next**.
    The **Credentials** window opens.
15. Provide the credentials for the user:
    a. Enter the **Username** for the user who will run TotalAgility On-Premise Multi-Tenancy.
    b. Enter the **Password** and **Confirm** password.

       > ℹ If the service account name ends with a $ (dollar), do not specify the password.

    c.   On the **Root Website to host TotalAgility Application** list, select the website to host the TotalAgility application. By default, the **Default Web Site** is selected.

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

16. Click **Next**.
    The **Databases** window opens.

17. Enter the database name for **Master** and **DataCentre** databases.
    - If the database with the same name already exists, and if you want to overwrite the existing database, select the **Overwrite databases if they exist?** check box.

      The **Test connections** option becomes available.
    - To test the database connections, click **Test connections**. Once the database connections are successfully established, click **Next**. On confirmation to overwrite, the databases will be re-initialized and the existing data will be lost.

      > ⓘ If the database details are not valid, or if the database does not exist, connection to database fails.

    - To use Windows authentication to connect to SQL Server, select the check box for **Use Windows authentication for tenant databases**.
    - If you are not using the local server, click the ellipsis and select the Master and DataCentre databases.
    - If you want to manually install the databases, see Install databases manually. For a clean installation, run the setup.exe wizard to this screen, and do not select the **Overwrite databases if they exist?** check box.
    - If you want to point to existing databases in a different machine, enter a name for the databases; click ellipsis for **Server**; select the database server where the databases reside; in the **Security** group, either use **Windows Authentication**, or select the SQL Server authentication providing the user name and password, and then click **OK**. If all the databases reside on the same server, select the **Apply these settings to all other Databases** check box.

      > ⓘ If you have already selected the check box for "Windows authentication for databases" in the Tenant Databases window, you can only use the Windows Authentication in the Security group.

    > ⓘ If you install TotalAgility without any databases, you can use the Configuration Utility to point to the databases when they are available at a later a stage. See the *Kofax TotalAgility Configuration Utility Guide*.

18. Click **Next**.
    The **DB Connection Results** window opens.

    > ⓘ If the connection to database fails, the installation cannot be progressed. Click **Back** and make changes as needed.

19. Click **Next**.
    The **Capture Binary Data Storage** window opens.

20. By default, the binary data such as capture documents, .NET Store DLLs and CCM Packs are stored in the TotalAgility database. You can use the preconfigured external cloud data storage services such as Amazon S3 or Windows Azure Blob Storage for saving and processing the binary data. The cloud services helps to reduce the SQL Server maintenance costs, delegate maintenance to external service and provide encryption.

    > ⓘ If you change the storage type to Azure/Amazon blob storage or SQL Server and File System, the binary data is saved in the selected storage type. Once the storage type is changed, you cannot turn it off later.

    Select one of the following capture data storage types:

Storage type	Description
SQL Server (default)	Stores capture data in the SQL Server.
SQL Server and File System	Stores the tenant FILESTREAM groups that are created when creating a tenant. Under **File storage settings**, specify the root folder on the SQL machine to store these FILESTREAM groups.
Windows Azure Blob Storage	Stores capture data in Azure Blob Storage service. Under **Cloud Account Settings**, enter the **Account Connection String** to connect to the Blob storage service. > ⓘ The Container name for capture data storage is automatically created by the installer.
Amazon S3	Configure the following **Cloud Account Settings**: a. Enter the **Access Key** to connect to the Amazon S3 storage service. b. Enter the **Secret Key**. c. On the **Region** list, select a predefined S3 region, for example Asia Pacific (Sydney). (Default: US East (Ohio) > ⓘ The Bucket name for data storage is automatically created. Bucket is a fundamental container in Amazon S3 for data storage.

21. If you wish to make any changes, click **Back** and make your changes, otherwise, click **Next**.

    > ⓘ The FILESTREAM is only supported with Windows authentication if the storage type is SQL Server and File System. If you do not select the check box for "Use Windows authentication for tenant databases" in the Databases window, a warning appears stating FILESTREAM is not supported with SQL authentication or when databases do not exist.

    The **Install Options** window opens.

22. To automatically start the services, keep the **Automatically Start Services** check box selected.

23. Click **Next**.
    The **Installation Review** window opens and displays the settings.

24. Review the settings and click **Next**.
The **Installation Progress** window appears. The setup installs the required files, databases, and other integrated products. The **Licensing** window opens.

25. To connect to the License Server, perform the following steps:

    a. In the **License Server** field, enter the location of the License Server.

    > ⓘ To connect to the shared License Server, enter the name or the IP address of the shared License Server.

    b. In the **Port Number** field, enter the port number on which the License Server listens.

    c. Click **Next**. The second Licensing window opens.

    > ⓘ To skip connecting to the License Server now but connect when launching TotalAgility, click **Skip** and proceed to the next step.

26. Enter your TotalAgility **Serial Number** and **Product Code**.

    > ⓘ The ID of the selected License Server appears in the **Machine ID** field. The **Serial Number** and **Product Code** appear by default if the License Server is shared.

27. To activate the license, select the license activation method:
    - **Automatic**: Use this option when Internet connectivity is available. The license is activated online.

- **Manual**: Use this option when there is no Internet connectivity or if automatic activation is not successful from the installer or license utility for your Kofax product. The Activation Code box is displayed. To obtain the activation code:

  a. Enter the following URL in your browser:

  `http://activatelegacy.Kofax.com/support/Activation/manual.aspx`.
  The Kofax Product License Activation page appears.

  b. Enter the **Serial Number** issued to you at the time of purchase. If you have a hardware key, the serial number (usually 7 characters) is printed on the key.

  c. Enter the email address where Kofax can send the information you need to activate the product license.

  d. Click **Next** to proceed with the activation process.

    ⓘ Ignore the **Version** selection field if you do not have Kofax Capture or Ascent Capture.

  e. Copy and paste the **Activation Code** into the field on the **Licensing** window.

  f. Either click **Activate** to activate the license or click **Skip** to skip activating license. If you skip activating the license, a warning informs that you need to activate the license later.

    ⓘ The license period starts once the license is activated. You can skip activation during installation and only activate it when you are ready to use TotalAgility. You must activate the license when you log in to TotalAgility for the first time.

The **Kofax TotalAgility Installation Complete** window displays the summary of the installation.

ⓘ Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

28. Click **Finish**.

    - Your installation is now complete. See Log on to TotalAgility On-Premise Multi-Tenancy for more information.
    - The **Transformation Server Installation** window appears.

      ⓘ The Transformation Server installation window only appears if you have selected the transformation service option in the Application Server window.

29. Click **Yes** to install Transformation Server.
    The installation for Transformation Server is launched. See Transformation Server Bundle installation.

Standard installation of Real Time Transformation Server (RTTS)

RTTS is supported in a multi tenant environment. However, each tenant must have their own setup. These RTTS tenant specific installations should be done in the same deployment as the TotalAgility multi-tenanted installation containing the tenant(s).

1. On the installation media, navigate to `\\OnPremiseMultiTenancyInstall` 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 installation.
2. In the **Kofax TotalAgiltiy Multitenancy Installation** window, click **Next** or press Enter to move to the next window.

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

3. In the **Kofax Inc. Software License Agreement** window, accept the terms in the License Agreement and click **Next**.
4. In the **Type of Install** window, select **Real Time Transformation Server** and click **Next**.
5. In the **Environment Type** window, select either of the following:
    *   **Live**: Installs the production environment.
    *   **Dev**: Installs the development environment.
6. Click **Next**.
    The **Software Checks** window appears. The system displays a list of required software and whether the software is installed.
7. 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**.

    The **Destination** window opens.
8. Use the default installation folder or click **Browse** to select a different path and click **Next**.
    The **Credentials** window opens.
9. Enter the credentials for the user who will run TotalAgility On-Premise Multi-Tenancy.

    > ⓘ If the service account name ends with a $ (dollar), do not specify the password.

10. On the **Root Website to host TotalAgility Application** list, select the website to host the TotalAgility application. By default, the **Default Web Site** is selected.

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

11. Click **Next**.
    The **Databases** window opens.

12. Enter the database name for **Tenant** and **DataCenter** databases.

   a. For the **Tenant** database, enter the tenant database name, click ellipsis for **Server** and point to an existing tenant database on an existing TotalAgility environment. In the **Security** group, select **SQL Server authentication**, provide the user name and password, and then click **OK**.

   The user name and password credentials belong to the TenantName_schema user created by on-premise multi-tenant when creating the tenant. For example, <Tenant1>_live | <Tenant1>_reportingstaginglive, where <Tenant1> is the name of the tenant. These credentials can be found in the Database Connection field in the Tenant Management System.

   b. For the **DataCenter** database, enter the name for the database, click ellipsis for **Server** and select the database server where the databases reside. In the **Security** group, either use **Windows Authentication**, or select the SQL Server authentication providing the user name and password, and then click **OK**. If all the databases reside on the same server, select the **Apply these settings to all other Databases** check box.

   > ❶ If you have already selected the check box for "Windows authentication for databases" in the Databases window, you can only use the Windows authentication in the Security group for a datacenter database.

   c. Select the check box for **Kofax hosted tenant** when you point to existing azure databases.

13. Review the settings. If you wish to make any changes, click **Back** and make your changes, otherwise, click **Next**.
   The **Installation Progress** window opens. The setup installs the required files, databases, and other integrated products.

14. Click **Finish**.
   Your installation is now complete. See Log on to TotalAgility On-Premise Multi-Tenancy for more information.
   Ensure that no error log is created. If any errors occur, by default, TotalAgility creates a log file at the same location where setup.exe exists if the path in the System diagnostics section of the `Setup.exe.config` is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>". The log file is also created on the desktop. Fix those errors and repeat the above steps.

See also:
- Standard installation of database only
- Standard installation for upgrading databases
- Standard installation of the Web server
- Standard installation of the Application server
- Standard installation of the Web and Application server

Perform TotalAgility installation in a Docker container

Overview

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 fewer 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. You do not need to use the TotalAgility installation program when TotalAgility is deployed in a Docker container. Instead, TotalAgility is already 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.

Limitations

The following are the limitations:

- Currently, Microsoft does not officially support MSDTC on the Docker Windows containers. Due to this limitation, TotalAgility cannot have out-of-box support for split databases (main and archive). As a workaround, enable Active Directory support for the containers by making use of Globally Managed Service Accounts (GMSA). Once the container is in the same domain as host machine and SQL server machine, MSDTC will be able to execute distributed transaction among live and archive databases by resolving machine names using Active Directory.
- Export Connectors are not supported in a container.

Prerequisites

We recommend using a standalone server for your database (not a container). Therefore before running TotalAgility inside a container, make sure the TotalAgility databases is setup and remotely accessible (using either IP address or fully qualified domain name).

To use this setup, you need the following configuration on the SQL server being used:

- Firewall should allow remote access to SQL Server.
- SQL Server itself should be configured to allow remote access with Mixed mode since the user is also allowed to access without Windows Authentication.
- TCP/IP protocols should be enabled for SQL Server. Note Named pipes protocol does not work.

Install Docker on the Windows server 2016 and higher

Set up Docker on your Windows server. This requires Windows Server 2016 or higher to support running a TotalAgility Windows container.

> ⓘ Image Quality Analysis, Mobile ID and Mobile Card Capture are not supported when you set up Docker on Windows Server 2016.

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

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

2. If a reboot is 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 "docker info" command.

   ```
   docker info
   Containers: 1
    Running: 0
    Paused: 0
    Stopped: 1
   Images: 26
   Server Version: 18.09.3
   Storage Driver: windowsfilter
    Windows:
   Execution Driver: <not supported>
   Logging Driver: json-file
   Plugins:
    Volume: local
    Network: ics l2bridge l2tunnel nat null overlay transparent
   Kernel Version: 10.0 14393 (14393.2828.amd64fre.rs1_release_inmarket.190216-1457)
   Operating System: Windows Server 2016 Standard Version 1607 (OS Build 14393.2828)
   OSType: windows
   Architecture: x86_64
   CPUs: 4
   Total Memory: 10.04 GiB
   Name: HV-Docker-QA
   ID: HI53:GJSY:3BWT:Z3S5:3NWU:DEFN:6D3X:KCXO:2EMJ:ITZR:QAVY:VXFK
   Docker Root Dir: C:\ProgramData\docker
   Debug Mode (client): false
   Debug Mode (server): false
   Registry: https://index.docker.io/v1/
   Labels:
   Insecure Registries:
    127.0.0.0/8
   ```

4. Optional. NLP support for Transformation Server within Docker is not enabled by default. To make Docker work with NLP within the Transformation server, and to increase the default maximum size for the Docker container images, perform the following steps:

   a. Open **daemon.json** available at "`C:\ProgramData\docker\config`". If the file does not exist at that location, create the file.

   b. Append the following text to daemon.json:

   ```
   {
   ```

```
"storage-opts": ["size=50GB"]
}
```

   c. Restart the Docker Engine service.

5. If using split Web/App containers, the Web and App containers should be able to resolve DNS for the host machine. The Web container should also be able resolve DNS for all the tenants to communicate with the App container. Resolving DNS can either be done by modifying the hosts file on container during or after startup, or by using a DNS server. It is recommended to use a DNS server.

If modifying the hosts file, perform the following steps:

   a. Create a new hosts file and add the following entries:

```
HostMachineIP HostMachineName
HostMachineIP tenantname.HostMachineName
```

   b. Copy the hosts file to the web container on startup and after each tenant is created.

Use Image Quality Analysis, Mobile ID and Mobile Card Capture on Docker

To use Image Quality Analysis, Mobile ID and Mobile Card Capture in a container, Windows Server 2019 or higher must be used as a container host with the following Docker base container specified in the Docker file: `mcr.microsoft.com/windows:1809`

Make the following changes in the Docker file:

- Add the following line: `RUN powershell "Set-ExecutionPolicy -ExecutionPolicy RemoteSigned"` before the line, `RUN powershell C:\KTA\PowershellScripts \ConfigureContainer.ps1`

Make the following changes in the InstallWindowsFeatures.ps1 powershell script:

- Identify the following line:

```
Install-WindowsFeature -Name NET-Framework-Features -Source C:\kta\NET-Framework35-
Features -Verbose
(Install-WindowsFeature cmdlet is not supported in Windows 1809 image)
```

- Replace the preceding line with the following:

  - ```
    dism /Online /Add-Package /PackagePath:c:\kta\NET-Framework35-Features\Microsoft-
    Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~en-US~.cab
    dism /Online /Add-Package /PackagePath:c:\kta\NET-Framework35-Features\microsoft-
    windows-internetexplorer-optional-package~31bf3856ad364e35~amd64~~.cab

    dism /Online /Add-Package /PackagePath:c:\kta\NET-Framework35-Features\Microsoft-
    Windows-NetFx3-OnDemand-Package~31bf3856ad364e35~amd64~en-US~.cab
    dism /Online /Add-Package /PackagePath:c:\kta\NET-Framework35-Features\microsoft-
    windows-netfx3-ondemand-package~31bf3856ad364e35~amd64~~.cab
    ```

> ⓘ
> - Additionally, Mobile ID and Mobile Card Capture has a prerequisite for the VC++ 2013 x86 redistributable. This can be automatically downloaded and installed in the Docker file.
> - Make sure that following dlls are present when you run Image Quality Analysis, Mobile ID and Mobile Card Capture applications (32 bit dll dependency) on Windows server 2016 or 2019. Copy the 32-bit version of DLLs (avicap32.dll, avifil32.dll, msacm32.dll, msvfw32.dll) from the host's `C:\Windows\SysWOW64` and paste the DLLs in the Docker container's `C:\Windows\SysWOW64 folder`. You must copy these DLLs to all containers running the Transformation Service.

Create a TotalAgility Docker container image

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

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

> ⓘ For a TotalAgility Docker container to be successfully built, approximately 100 GB of free disk space is needed.

On-premise multi-tenancy

To create a TotalAgility Docker image in an on-premise multi-tenant environment, perform the following steps.

1. Extract the contents of Kofax TotalAgility-7.10.0.ZIP to a `<source directory>`.
2. Create a new folder, `<workingdirectory>`.
   Your Docker commands will be run from this directory.
3. Copy the contents of `<source directory>\Utilities\Docker` to `<working directory>`.
4. Move the contents from `<source directory>` to `<working directory>\ContainerFiles`.
   The file structure should be as follows:
   ```
   <working directory>\Dockerfile
   <working directory>\ContainerFiles\KCMProxyInstallation
   <working directory>\ContainerFiles\Licensing
   <working directory>\ContainerFiles\OnPremiseMultiTenancyInstall
   <working directory>\ContainerFiles\Reporting
   <working directory>\ContainerFiles\RepositoryBrowser
   <working directory>\ContainerFiles\ScanAgentService
   <working directory>\ContainerFiles\TenantManagementInstall
   <working directory>\ContainerFiles\TransformationServer
   <working directory>\ContainerFiles\Utilities
   <working directory>\ContainerFiles\PowerShellScripts
   ```
5. Update the parameters as needed for each container type. See Silent installation configuration.

6. To create the image, open a PowerShell window on the container host and run the following command:

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

ⓘ 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. The command may take approximately one hour to complete with a quad core processor configuration.

Example The following command generates the image with the name "kofaxopmt" using the contents inside `C:\Docker\TotalAgility`:

```
docker build -t kofaxopmt "C:\Docker\ TotalAgility "
```

Silent installation configuration

1. On the installation media, navigate to \\OnPremiseMultiTenancyInstall and open SilentInstallConfig.xml using a text editor.
2. The following are the supported Docker container types for this deployment and the required configuration parameters to be updated in SilentInstallConfig.xml.
   - Demo
   - Application Server (Core Services and Core Worker)
   - Web Server
   - Web Server and Application Server (Core Services and Core Worker)
   - Reporting Server
   - License Server
   - Transformation Server
   - Real Time Transformation Service

   ⓘ You can create a Docker container with any combinations of App server, Web server, Reporting Server, Licensing Server and Transformation Server. Real Time Transformation Server (RTTS) is supported only in a dedicated Docker container.

Demo

Update the following parameters for a Demo server installation.

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

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	true	
CoreWorkerService	true	
ReportingService	true	

Parameter	Value	Description
TransformationService	true	ℹ If the TransformationService is set to true, you must copy the fonts by running the powershell script from the following path: `<Working directory>/containerfiles/ poweshellscripts/copyfonts.ps1`. By running the script, the fonts are copied from `Windir/fonts` to `<Working directory>/containerfiles/ poweshellscripts/fonts` on the Docker container for PDF generation.
CoreServices	true	
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ℹ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	Both	
EmailConfig		
HostName	host name	Enter the host name, such as smtp.office.com.
PortNumber	port number	Enter the port number, such as 387.
UserName	username	Enter the username, such as Kofax@Kofaxindiapvtlimited.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, Kofax@Kofaxindiapvtlimited.com.
StartServices	false	Since we expect the services to be started only after container is running.

Application Server (Core Services and Core Worker)

Update the following parameters for the Application server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	false	
ReportingService	false	
TransformationService	false	
CoreServices	true	
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ℹ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	ApplicationServer	
EmailConfig		
HostName	host name	Enter the host name, such as smtp.office.com.
PortNumber	port number	Enter the port number, such as 387.
UserName	username	Enter the username, such as Kofax@Kofaxindiapvtlimited.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, Kofax@Kofaxindiapvtlimited.com.

Parameter	Value	Description
StartServices	false	Since we expect the services to be started only after container is running.

Web Server

Update the following parameters for the Web Server installation.

Parameter	Value	Description
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	WebServer	
StartServices	false	Since we expect the services to be started only after container is running.

Web Server and Application Server (Core Services and Core Worker)

Update the following parameters for both Web and Application Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	true	
ReportingService	false	
TransformationService	false	
CoreServices	true	
DatabaseInformation		

Parameter	Value	Description
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	Both	
EmailConfig		
HostName	host name	Enter the host name, such as smtp.office.com.
PortNumber	port number	Enter the port number, such as 387.
UserName	username	Enter the username, such as Kofax@Kofaxindiapvtlimited.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, Kofax@Kofaxindiapvtlimited.com.
StartServices	false	Since we expect the services to be started only after container is running.

Reporting Server

Update the following parameters for the Reporting Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	false	
ReportingService	true	
TransformationService	false	
CoreServices	false	

Parameter	Value	Description
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after container is running.

License Server

Update the following parameters for a License Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	true	
CoreWorkerService	false	
ReportingService	false	
TransformationService	false	
CoreServices	false	
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).

Parameter	Value	Description
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after container is running.

Transformation Server

Update the following parameters for a Transformation Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	false	
ReportingService	false	
TransformationService	true	ⓘ If the TransformationService is set to true, you must copy the fonts by running the powershell script from the following path: `<Working directory>/containerfiles/poweshellscripts/copyfonts.ps1`. By running the script, the fonts are copied from `Windir/fonts` to `<Working directory>/containerfiles/poweshellscripts/fonts` on the Docker container for PDF generation.
CoreServices	false	
DatabaseInformation		
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).

Parameter	Value	Description
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after container is running.
NlpWestern	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
NlpWesternExtended	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.
NlpExtended	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.

ⓘ NLP support for Transformation Server within Docker is not enabled by default. To make Docker work with NLP within the Transformation server, and to increase the default maximum size for the Docker container images, perform the following steps:

1. Open **daemon.json** available at "`C:\ProgramData\docker\config`". If the file does not exist at that location, create the file.

2. Append the following text to daemon.json:

   ```
   {
   "storage-opts": ["size=50GB"]
   }
   ```

3. Restart the Docker Engine service.

Real Time Transformation Service

Update the following parameters for a Real Time Transformation service installation.

Parameter	Value	Description
ServicesInstallOptions		
CoreServices	true	
DatabaseInformation		

Parameter	Value	Description
InstallDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Kofax TotalAgility services run as the LocalSystem account. This can also be used to run container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Kofax TotalAgility services run as the NT Authority\Network Service account. This can also be used to run container as a Group Managed Service Account (gMSA). ⓘ If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run container as a Group Managed Service Account (gMSA).
Install Info		
InstallType	RTTS	
StartServices	false	Since we expect the services to be started only after container is running.

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.

When a container stops running, changes to its state are not lost unless they are saved in persistent storage.

Before running a Docker container, the database server must be installed and the databases must already be set up (using Database only installation mode).

Enter the hostname (machine name) of the container that you intend to use for the "on-premise multi-tenant demo" or "on-premise multi-tenant APP" container when prompted for Live Host Name and Dev Host Name.

When using Live Host Name and Dev Host Name to access the TotalAgility containers, the text format should be as follows: `host name : any TCP port number open for the incoming connection on the host machine`.

To get the host name, do the following:

1. On the host name, go to the Command Prompt.

2. Enter the host name.
   Command returns the hostname, such as 'MyHostMachine'.

To get the port number, use any TCP port number where incoming connections are allowed. However, ensure to use same port number for the port forwarding while creating the container. For example, if you have given live\dev host names as MyHostMachine :5000. Port forwarding should be done at port 5000 using switch -p in the run command: `docker run --env-file "DockerSettings.env " -p 5000:443 -it ` Kofax`kofax/ kta_771`.

If you are using a load balancer and a public DNS, then Host name text should be the Fully Qualified Domain Name (FQDN)", such as kta.app.com.

To use this setup, you need the following configuration on the SQL Server being used:
- Firewall should allow remote access to SQL Server.
- SQL Server itself should be configured to allow remote access with Mixed mode since the user is also allowed to access without Windows Authentication.
- TCP/IP protocols should be enabled for SQL Server.

> ⓘ Named pipes protocol does not work.

- To use split databases, the Main and Finished Jobs databases must point to the same database and reside on the same database server. Microsoft does not support MSDTC on Docker containers.

> ⓘ Verify that you are able to remotely connect to the database server where the databases were set up using SQL Server Management Studio that uses the IP address. The verification ensures that the Docker containers are connected to the database server without any issues.

1. Generate "dockersettings.env" using Configuration Utility in the Docker mode. The file will be used later for the container initialization. Refer the *Kofax TotalAgilityConfiguration Utility Guide* for more information.

   > ⓘ The authentication mode for accessing TotalAgility can be set using the Configuration Utility.

2. Container access can be limited to the container host or can be port forwarded for global access. Enable the required exposed port number in the firewall settings of the host machine.

3. For non-Windows authentication:

   a. The following command brings up a container using the kofaxopmt image. Kofax TotalAgility settings are applied from dockersettings.env without Windows authentication. Port 80 from the container is forwarded to port 5000 on the container host.

      ```
      docker run -d --hostname "opmtdemo2" --name "opmtdemo2" --env-file "C:
      \Docker\TotalAgility\dockersettings.env" -p 5000:443 kofaxopmt
      ```

   b. The following command will bring up a container using the kofaxopmt image. Kofax TotalAgility settings applied from dockersettings.env file without Windows authentication.

      ```
      docker run -d --hostname "opmtdemo1" --name "opmtdemo1" --env-file "C:
      \Docker\TotalAgility\dockersettings.env" kofaxopmt
      ```

4. To enable licensing in a container, you must add "-p 3581:3581" to the "docker run" command. For example:

```
docker run -d --hostname "opmtdemo2" --name "opmtdemo2" --env-file "C:
\Docker\TotalAgility\dockersettings.env" -p 5000:80 -p 3581:3581 kofaxopmt
```

> ⓘ If running the License Server in a container, the associated license serial number must be activated before the Kofax TotalAgility Core Worker service can be started.

5. Use `"docker exec -it <container id\name goes here> powershell"` to attach to a powershell session on the created container.

   The docker exec -it opmtdemo3 powershell will bring up a powershell session inside the container with opmtdemo3 as container name.

6. To open port number required for Message Connector, you must add " -p 5003:25086" to the "docker run" command. For example:

```
docker run -d --hostname "opmtdemo2" --name "opmtdemo2" --env-file
"C:\Docker\TotalAgility\dockersettings.env" -p 5000:80 -p 5003:25086
kofaxopmt
```

> ⓘ 5003 is an example forwarded port number for Message Connector. Use the port number that you have configured for Message Connector. Similarly, you can configure port numbers for other instances of Message Connector.

If running TotalAgility containers on multiple hosts, we recommend that you use Docker Swarm or Kubernetes orchestrators that have a built-in DNS server to resolve container DNSs across multiple hosts.

If not using a container orchestrator and using Transformation Server synchronous processing, the TRANS_SERVER_INSTANCE database table should be manually updated to contain the IP URL of the host running the Transformation Server container. Transformation Server service runs on port 9001 by default; however, the port can be reconfigured using the Configuration utility. This port needs to be exposed in order to be used by App container hosted on the different host machine. Use additional switch `-p TS Port :9001` while running a Transformation Server container.

Access TotalAgility Tenant Management System

After you connect to the Docker container and verify that all services are in their expected state, use the following URL to access the TotalAgility Tenant Management System outside the container host with the port forwarded setup:

```
https://<ipaddressofthecontainerhost>:<exposedportofthecontainerhost>/
TenantManagementWebSite/TenantManagement/TenantLogon.html
```

For containers hosting IIS – TotalAgility Website

Due to different default behavior with case-insensitive URL resolution within Docker containers, it is necessary to perform extra configuration to ensure the TotalAgility website can be resolved in a case-insensitive way.

When you configure the container for the Designer / Workspace, we recommend that you use a VirtualHost file to configure the port and URL exposure through the host OS before you access the

URI. You may also consider using a rewrite rule to ensure that any URL access is redirected to a lowercase representation.

As per RFC 2616, "…a client SHOULD use a case-sensitive octet-by-octet comparison of the entire URIs…Comparisons of host names MUST be case-insensitive."

The Docker daemon and cache holds case-sensitive resolutions of the URL, which can cause issues if the case of the URL is changed prior to first access. This caching issue occurs as a result of Docker's use of WSL v1 and should be resolved in WSL v2. Within Docker, you cannot expose the same container port for multiple protocols, and having previously cached a case-sensitive URL, the cache must be cleared to replace with the lowercase URL.

Access Message Connector

To access the Message Connector within the container host or from outside the host, perform the following steps.

1. Use the following URL: `http:DockerServerIP:5003/en/file/index.html`

   Where DockerServerIP is the IP of the Docker Container host and 5003 is the configured forwarded port number to access Message Connector. Use the forwarded port number you have configured for Message Connector.

   The Message Connector Monitor appears.

2. To access Message Connector configuration, click the **Configuration Tool**.
   The Message Connector Configuration tool appears.

3. Make the necessary configuration changes and save.

4. Optionally, to restart the Message Connector service, click the **Restart service** button.

   To stop and restart Message Connector service from the Docker Container, use the following commands:`Start-service KIC-ED-MCStop-service KIC-ED-MC`

Additional information

This table includes some useful Docker commands.

Docker command	Purpose
docker images	Gets the list of all Docker images currently available on the server.
docker ps -a	Gets a list of all containers available on the server.
docker start <containerID>	Starts the container with the ID <containerID> on the server.
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 <imagename>	Deletes the image with the ID <imagename> on the server. Deletion is successful only if no child containers use this image.
docker inspect -f "{{ .NetworkSettings.Networks.nat.IPAddress }}" <containerID>	Gets the IP address of the container with the ID <containerID>.
docker cp "<containerID>:/<fullfilepath oncontainer>" "<pathtofolderonserver>"	Copies a file from the container to the server.
docker cp "<fullfilepathonserver>" "<con tainerID>:/ <fullfilepathoncontainer>"	Copies a file from server to the container.

Docker command	Purpose
docker logs <containerID>	Displays all logs for a particular container.
docker logs - tail n <containerID>	Displays the last "n" logs for a particular container.
type <FQDN of text file>	Displays the content of text file within powershell instance.
Get-Process	Gets the list of all processes.
Get-Service	Gets the list of all services (running and stopped).
start-service <ServiceName>	Starts a particular service.
Stop-service <ServiceName>	Stops a particular service.
Get-WMIObject Win32_Service | select startname, name, status	Gets the list of all services with some additional columns.
Get-EventLog -LogName Application -newest 10 | format-table -auto -wrap	Gets the last 10 application logs from event viewer.
import-module webadministration	Runs before the following commands.
get-iisapppool	Gets the name of the Application pool.
get-itemProperty -path IIS:\APPPOOLS\TotalAgilityAppPool -names	Gets the identity information of the Application pool.

Using secrets

If you are using Kubernetes secrets to store sensitive information, such as database connection string, passwords and more, you must do the following changes before building the Docker images and deploying to Kubernetes. For example, consider using the MainDBConnectionString application setting as the secret.

Kubernetes secrets

If using secrets as volumes

1. Create a secret `<maindbsecret>` in Kubernetes that contains the MainDBConnectionString details. Refer to the Kubernetes documentation on secrets to create a secret.

2. On the Docker container installation media, navigate to `\\Utilities\Docker \ContainerFiles\PowershellScripts\`. Replace the line "`$appSetting.value = $_.Value;`" with the following lines which will check for 'maindbconnectionstring' setting and update its value in all the Kofax TotalAgility configuration files with the contents of the <maindbsecret> file mounted in a <target path>.

```
if($appSetting.key -eq "<MainDBConnectionString>")
               {
  $dbconnstring = (Get-Content "<target path>\<maindbsecret>") -as [string];
  if($dbconnstring -ne $null)
  {
   $appSetting.value = $dbconnstring;
  }
               }
               else
               {
                   $appSetting.value = $_.Value;
               }
```

> ⓘ All the corresponding MaindbConnectionString values in the DockerSettings.env no longer needs to be provided as it is pulled from the secrets.

3. Save the Changes.

4. Similarly, update the `UpdateConfigAppSettings.ps1` script file for other application settings, as needed.

5. Modify the Pod definition to add a volume <maindbvol> along with the <maindbsecret> to a chosen <target path>, for example, `</kta/maindb/>` in the container. Refer to the Kubernetes documentation on secrets to add a volume.

6. When the pod is deployed, this should create a secret file <maindbsecret> which contains the connection string value under the path `c:\kta\maindb\` in the container and also update the corresponding TotalAgility configuration file settings with the secret value.

If using secrets as environmental variables

1. Create a secret <maindbsecret> in Kubernetes that contains the MainDBConnectionString details. Refer to the Kubernetes documentation on secrets to create a secret.

2. Modify the Pod definition to add an environmental variable <env variable name> for the secret <maindbsecret>. The <env variable name> must be same as in dockerSettings.env, for example, "KTA_Agility.Server.Web--web.config_MainDBConnectionString". This should set the environment variable "KTA_Agility.Server.Web--web.config_MainDBConnectionString" with the value of the secret <maindbsecret> which contains the connection string value, once the pod is deployed. Refer to Kubernetes documentation on secrets to add as environment variable.

3. Similarly multiple environment variables can be added to the pod definition that needs to get the value form a secret. No changes are needed to the script files.

Docker Secrets

If you are using Docker secrets to store sensitive information, it is only available in the Swarm mode; so the standalone containers cannot use this feature.

> ⓘ The following changes need to be made before building the Docker images and deploying to swarm.

1. Create a secret <maindbsecret> in the swarm that contains the MainDBConnectionString details. Refer to the Docker documentation on Docker secrets to create a secret.

2. On the Docker container installation media, navigate to `\\Utilities\Docker \ContainerFiles\PowershellScripts` and update the *UpdateConfigAppSettings.ps1* Powershell script file. Replace the line " `$appSetting.value = $_.Value;` " with the following lines which will check for 'maindbconnectionstring' setting and update its value in all the Kofax TotalAgility configuration files with the contents of the <maindbsecret> file located in a default target location (For windows containers, the default target is under 'C:\ProgramData \Docker\secrets') :

```
if($appSetting.key -eq "<MainDBConnectionString>")
                {
  $dbconnstring = (Get-Content "<target location>\<maindbsecret>") -as [string];
  if($dbconnstring -ne $null)
  {
```

```
  $appSetting.value = $dbconnstring;
 }
              }
              else
              {
                  $appSetting.value = $_.Value;
              }
```

> ℹ All the corresponding MaindbConnectionString values in the DockerSettings.env no longer needs to be provided as it is pulled from the secrets.

3. Save the Changes. Similarly, you can update the `UpdateConfigAppSettings.ps1` script file for other application settings as needed.

4. Create/update a Docker service and provide access to the <maindbsecret> secret along with the Docker environment file. This should create a secret file <maindbsecret> in the container and also update corresponding settings of theKofax TotalAgilityconfiguration files with the secret value. Refer to the Docker documentation on Docker secrets to create a service.

AWS Secrets

If you are using AWS Secrets to store sensitive information, such as database connection string, passwords, do the following changes to dynamically retrieve the secrets from the container. You can do this via AWS tools for powershell or via a custom .Net library. (For example, consider using the MainDBConnectionString application setting as the secret.)

> ℹ Make the following changes before building the docker images

Using AWS Tools for Powershell

1. Create a secret <mainsecret> in AWS Secret Manager that contains the MainDBConnectionString details.

   Refer to AWS documentation to create a secret.

2. Install NuGet provider and AWS.Tools.SecretsManager in the container to retrieve secrets from AWS.

3. On the docker installation media, navigate to `\\TotalAgility\Utilities\Docker\ContainerFiles\PowershellScripts\` and update the UpdateConfigAppSettings.ps1 Powershell script file. In the 'Update-ConfigFile' Function, add the following script lines before the line "Get-ChildItem env:*| ...." which will install the required AWS tools for powershell and updates the contents of the <mainsecret> retrieved from AWS secret:

```
Set-PSRepository -Name 'PSGallery' -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
If(-not(Get-InstalledModule AWS.Tools.SecretsManager -ErrorAction
 silentlycontinue))
{
    Install-Module AWS.Tools.SecretsManager -RequiredVersion 4.1.4.0 -Confirm:
$False -Force
}
$awsAccessKeyId = [Environment]::getEnvironmentVariable('KTA_AWS_ACCESSKEYID');
$awsSecretAccessKey =
 [Environment]::getEnvironmentVariable('KTA_AWS_SECRETACCESSKEY');
$awsRegion = [Environment]::getEnvironmentVariable('KTA_AWS_REGION');
Set-AWSCredential -AccessKey $awsAccessKeyId -SecretKey $awsSecretAccessKey
Initialize-AWSDefaultConfiguration -Region $awsRegion
```

```
$awsMainSecretName =
 [Environment]::getEnvironmentVariable('KTA_AWS_MAINSECRETNAME');
$awsMainSecret_response = Get-SECSecretValue -SecretId $awsMainSecretName
$mainSecretJsonobj = ConvertFrom-Json -inputObject
 $awsMainSecret_response.SecretString
```

4. Replace the line "$appSetting.value = $_.Value;" with the below lines which will check for 'maindbconnectionstring' setting and update its value in all the Kofax TotalAgility configuration files with the contents of the <mainsecret> retrieved from AWS secret:

```
              if($appSetting.key -eq "<MainDBConnectionString>")
              {
 $dbconnstring = $mainSecretJsonobj.$awsMainSecretName;
 if($dbconnstring -ne $null)
 {
  $appSetting.value = $dbconnstring;
 }
              }
              else
              {
                  $appSetting.value = $_.Value;
              }
```

5. Add the below script lines before the 'Update-License-Config' Function which will clean up the AWS environment variables.

```
$awsAccessKeyId = [Environment]::setEnvironmentVariable('KTA_AWS_ACCESSKEYID',
$null);
$awsSecretAccessKey =
 [Environment]::setEnvironmentVariable('KTA_AWS_SECRETACCESSKEY',$null);
$awsRegion = [Environment]::setEnvironmentVariable('KTA_AWS_REGION',$null);
$awsMainSecretName =
 [Environment]::setEnvironmentVariable('KTA_AWS_MAINSECRETNAME',$null);
```

6. Save the Changes.

7. When running the docker container, pass the KTA_AWS variables mentioned in above script as environment variables. The docker run commands as mentioned in 'Run a Docker Container' section must now also pass in these **--env** variables along with **--env-file**.

```
docker run -d --hostname "<host>" --name "<name>" --env
 KTA_AWS_ACCESSKEYID=<access id> --env KTA_AWS_SECRETACCESSKEY=<key> --env
 KTA_AWS_REGION=<region> --env KTA_AWS_MAINSECRETNAME=<mainsecret> -env-file
 "dockersettings.env" -p <port> <image>
```

> ⓘ All the corresponding 'MaindbConnectionString' values in the DockerSettings.env no longer needs to be provided as it is pulled from the secrets.

8. When the container is running, get the secret <mainsecret> which contains the connection string value and also update the corresponding Kofax TotalAgility configuration file settings with the secret value.

9. Similarly, you can update the UpdateConfigAppSettings.ps1 script file and docker run command to get other application settings from AWSsecret by adding new variables similar to `$ awsMainSecretName` and `KTA_AWS_MAINSECRETNAME` respectively .

Using Custom Library

1. Create a secret <mainsecret> in AWS Secret Manager that contains the MainDBConnectionString details.

   Refer to AWS documentation to create a secret.

2. Create a .Net custom library 'AWSSecretManager.dll' with a GetAWSSecret() method that will retrieve the AWS secret. This will need `AWSSDK.Core & AWSSDK.SecretsManager SDK` for .Net installed. The method code will be as follows:

```
class AWSSecretManager::
public static string GetAWSSecret(string awsAccessKeyId, string awsSecretAcessKey,
 string region , string awsSecretName)
        {
            string secret = string.Empty;
            IAmazonSecretsManager client = new
 AmazonSecretsManagerClient(awsAccessKeyId, awsSecretAcessKey,
 RegionEndpoint.GetBySystemName(region));
            GetSecretValueRequest request = new GetSecretValueRequest();
            request.SecretId = awsSecretName;
            request.VersionStage = "AWSCURRENT"; // VersionStage defaults to
 AWSCURRENT if unspecified.
            GetSecretValueResponse response = null;
            // In this sample we only handle the specific exceptions for the
 'GetSecretValue' API.
            // See https://docs.aws.amazon.com/secretsmanager/latest/apireference/
API_GetSecretValue.html
            // We rethrow the exception by default.
            try
            {
                response = client.GetSecretValueAsync(request).Result;
            }
            catch (DecryptionFailureException e)
            {
                // Secrets Manager can't decrypt the protected secret text using
 the provided KMS key.
                // Deal with the exception here, and/or rethrow at your
 discretion.
                throw;
            }
            catch (InternalServiceErrorException e)
            {
                // An error occurred on the server side.
                // Deal with the exception here, and/or rethrow at your
 discretion.
                throw;
            }
            catch (InvalidParameterException e)
            {
                // You provided an invalid value for a parameter.
                // Deal with the exception here, and/or rethrow at your discretion
                throw;
            }
            catch (InvalidRequestException e)
            {
                // You provided a parameter value that is not valid for the
 current state of the resource.
                // Deal with the exception here, and/or rethrow at your
 discretion.
                throw;
            }
            catch (ResourceNotFoundException e)
            {
                // We can't find the resource that you asked for.
                // Deal with the exception here, and/or rethrow at your
 discretion.
                throw;
            }
            catch (System.AggregateException ae)
```

```
            {
                // More than one of the above exceptions were triggered.
                // Deal with the exception here, and/or rethrow at your
 discretion.
                throw;
            }

            // Decrypts secret using the associated KMS CMK.
            // Depending on whether the secret is a string or binary, one of these
 fields will be populated.
            if (response.SecretString != null)
            {
                secret = response.SecretString;
            }
            else
            {
                MemoryStream memoryStream = new MemoryStream();
                memoryStream = response.SecretBinary;
                StreamReader reader = new StreamReader(memoryStream);
                secret =
 System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(reader.ReadToEnd()));
            }

            return secret;
        }
```

3. On the docker installation media, navigate to `\\TotalAgility\Utilities\Docker \ContainerFiles\PowershellScripts\` and copy the utility Dlls - AWSSecretManager.dll, AWSSDK.Core.dll & AWSSDK.SecretsManager.dll

4. Update the UpdateConfigAppSettings.ps1 Powershell script file. In the 'Update-ConfigFile' Function, add the following script lines before the line "Get-ChildItem env:*| ...." which will Load the custom library and update the contents of the <mainsecret> retrieved from AWS secret into :

```
$add = [Reflection.Assembly]::LoadFile("C:\KTA\PowershellScripts
\AWSSecretManager.dll")
$add = [Reflection.Assembly]::LoadFile("C:\KTA\PowershellScripts
 \AWSSDK.SecretsManager.dll")
$add = [Reflection.Assembly]::LoadFile("C:\KTA\PowershellScripts\AWSSDK.Core.dll")

$awsAccessKeyId = [Environment]::getEnvironmentVariable('KTA_AWS_ACCESSKEYID');
$awsSecretAccessKey =
 [Environment]::getEnvironmentVariable('KTA_AWS_SECRETACCESSKEY');
$awsRegion = [Environment]::getEnvironmentVariable('KTA_AWS_REGION');
Set-AWSCredential -AccessKey $awsAccessKeyId -SecretKey $awsSecretAccessKey
Initialize-AWSDefaultConfiguration -Region $awsRegion

$awsMainSecretName =
 [Environment]::getEnvironmentVariable('KTA_AWS_MAINSECRETNAME');
Try {
    $awsMainSecret_response =
 [AWSSecretManager.AWSSecretManager]::GetAWSSecret($awsAccessKeyId,
$awsSecretAccessKey,$awsMainSecretName)
}
Catch {
   Write-Host "Exception::"
    Write-Host $_.Exception
}
$mainSecretJsonobj = ConvertFrom-Json -inputObject
 $awsMainSecret_response.SecretString
```

5. Replace the line " $appSetting.value = $_.Value; " with the following lines which will check for 'maindbconnectionstring' setting and update its value in all the TotalAgility configuration files with the contents of the <mainsecret> retrieved from AWS secret:

```
            if($appSetting.key -eq "<MainDBConnectionString>")
            {
  $dbconnstring = $mainSecretJsonobj.$awsMainSecretName;
  if($dbconnstring -ne $null)
  {
   $appSetting.value = $dbconnstring;
  }
            }
            else
            {
                $appSetting.value = $_.Value;
            }
```

6. Add the following script lines before the 'Update-License-Config' Function which will clean up the AWS environment variables.

```
$awsAccessKeyId =
[Environment]::setEnvironmentVariable('KTA_AWS_ACCESSKEYID',$null);
$awsSecretAccessKey =
[Environment]::setEnvironmentVariable('KTA_AWS_SECRETACCESSKEY',$null);
$awsRegion = [Environment]::setEnvironmentVariable('KTA_AWS_REGION',
$null); $awsMainSecretName =
[Environment]::setEnvironmentVariable('KTA_AWS_MAINSECRETNAME',$null);
```

7. Save the Changes.

8. When running the docker container, pass the KTA_AWS variables mentioned in above script as environment variables. The docker run commands as mentioned in 'Run a Docker Container' section must now also pass in these **--env** variables along with **--env-**file.

```
docker run -d --hostname "<host>" --name "<name>" --env
KTA_AWS_ACCESSKEYID=<access id> --env KTA_AWS_SECRETACCESSKEY=<key> --env
KTA_AWS_REGION=<region>--env KTA_AWS_MAINSECRETNAME=<mainsecret> -env-file
"dockersettings.env" -p <port> <image>
```

> ⓘ All the corresponding 'MaindbConnectionString' values in the DockerSettings.env no longer needs to be provided as it is pulled from the secrets.

9. When the container is running, this should get the secret <mainsecret> which contains the connection string value and also update the corresponding Kofax TotalAgility configuration file settings with the secret value.

10. Similarly, you can update the `UpdateConfigAppSettings.ps1` script file and docker run command to get other application settings from AWSsecret by adding new variables similar to `$ awsMainSecretName` and `KTA_AWS_MAINSECRETNAME` respectively .

Import SSL certificate on the container

You can import a custom SSL certificate for use by TotalAgility on a Docker container.

You can import password-protected certificates with a private key. See SSL Support Desk for more information on certificate export.

1. Create a new folder, such as "HostMachineFolder" on the host machine.

2. Copy the certificate file, such as CertificateName.pfx to the newly created folder (HostMachineFolder).

3. You can pass the certificate password to the container as text or in a file. The file can be passed to the container as a secret (if using Docker compose, Kubernetes, and so on) or as a mapped volume. To pass password file using mapped volume, do the following:

   a. Create new text file, such as password.txt in the HostMachineFolder.

   b. Open the newly created file and enter the certificate's password in the first line of the file.

   c. Save the file and ensure to that you change the file attribute to hidden.

4. Create a Docker container using the "docker run" command as documented in previous sections with two additional switches, "-v" and "-e".

   a. -v: Container can access contents of HostMachineFolder via mapped ContainerFolder.

   b. -e: additional environment variables are created to store SSL certificate path "KTA_SSL_CERT_PATH" and password ("KTA_SSL_CERT_PASSWORD" or password "KTA_SSL_CERT_PASSWORD_PATH)".

   c. Following are the examples of the "docker run" command with new -v and -e:

   For on-premise multi-tenancy:
   - ```
     docker run --env-file "C:\Docker\TotalAgility\dockersettings.env" -
     e SSL_CERT_PASSWORD="password" -e SSL_CERT_PATH="HostMachineFolder
     \CertificateName.pfx" -v "HostMachineFolder:ContainerFolder" -p
     5000:443 -d kofax/kta_771
     ```
   - ```
     docker run --env-file "C:\Docker\TotalAgility\dockersettings.env"
     -e KTA_SSL_CERT_PASSWORD_PATH="C:\folder\password.txt" -e
     KTA_SSL_CERT_PATH="C:\folder\Cert.pfx" -v "C:\folder:C:\folder2" -p
     5000:443 -d kofax/kta_771
     ```

   d. Replace HostMachineFolder with the actual certificate path on the host machine.

   e. Replace the CertificateName with the actual certificate name.

   f. Replace the ContainerFolder with the actual folderpath and name on the container (folder will be created).

   > ⓘ Ensure that folder paths or names do not have spaces.

Use Windows authentication with IIS and SQL server

Use GSMA to configure Windows authentication for Docker containers.

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 " ContainerHostGroupName" 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:  TotalAgility example.com

      New-ADServiceAccount -Name containerhost -DNSHostName  TotalAgility
       example.com -PrincipalsAllowedToRetrieveManagedPassword "Domain Controllers",
      "domain admins", "CN= ContainerHostGroupName,CN=Builtin, DC=  TotalAgility
       example,  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   TotalAgility example \ containerhost
  setspn -c -s HTTP/ machine1.  TotalAgility example.com   TotalAgility example
   \ 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 downloads module

which will create this file from Microsoft github account and will create a JSON file containing required data.

```
GMSA account : containerhost
Domain name:  TotalAgility example.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 "  TotalAgility example \containerhost$"
 FROM WINDOWS
 GO
```

To create user for all the TotalAgility databases:

```
CREATE USER containerhost FOR LOGIN "  TotalAgility example \ 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, it is required to point the Integration Server 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, perform the following steps on the on-premise multi-tenant Web server.

1. Either install IIS URL Rewrite 2.0 and Microsoft Application Request Routing (2.5 or higher) for IIS, or install the Microsoft plugin - Web Platform from the Microsoft website.

2. 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**.

3. Configure a URL rewrite rule in Kofax TotalAgility Web.config on the on-premise multi-tenant Web server to redirect /Services/Core requests to the on-premise multi-tenant Application Server.

```
<rewrite>
  <rules>
    <rule name="CoreServicesRule" enabled="true" stopProcessing="true">
      <match url="Services/Core/(.*)" />
        <action type="Rewrite" url="https://{C:1}.OPMTAppServerHostNameGoesHere/
TotalAgility /services/core/{R:1}" logRewrittenUrl="false" />
        <conditions trackAllCaptures="true">
          <add input="{HTTP_HOST}" pattern="([^.]*)(.*)" />
        </conditions>
      </rule>
  </rules>
</rewrite>
```

> ⓘ Replace the `<OPMTAppServerHostNameGoesHere>` with the host name of the on-premise multi-tenant Application Server.

Encrypt and decrypt the configuration files

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

- Web.config (Use Microsoft ASP.NET IIS Registration Tool)
- Configuration files of executables (Use the Kofax.CEBPM.EncryptConfig.exe utility)

> ⓘ Kofax.CEBPM.EncryptConfig.exe cannot work with Web.config; it can only work with configurations of executables.

Encrypt and decrypt web.config

Use the Microsoft ASP.NET IIS Registration Tool to encrypt or decrypt any sections of Web.Config. Refer to the Encrypting and Decrypting Configuration sections on the Microsoft website.

1. Navigate to the location of TotalAgility Web.config:

   `<Kofax Install location>\TotalAgility\Agility.Server.Web`

2. Run the Microsoft ASP.NET IIS Registration Tool (aspnet_regiis).

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

Encrypt and decrypt the configuration files of executables

Use the Kofax.CEBPM.EncryptConfig.exe utility (located in the TotalAgility installation_folder) to encrypt (-enc) or decrypt (-dec) the configuration files of executables.

Before encrypting the configuration files of executables, you must add a security provider.

List of configuration files of executables that can be encrypted

The following table includes the list of configuration files of executables that can be encrypted.

Configuration file name	Location

• Agility.Server.ExportConnector.exe.config
• Agility.Server.StreamingService.exe.config
	Agility.Server.Web files:
	`<Kofax Install location>\TotalAgility`
	`\Agility.Server.Web`

• Agility.Server.Core.WorkerService.exe.config
• Agility.Server.Core.Executor.exe.config
• Agility.Server.Core.ExportService.exe.config
• Agility.Server.Core.ExportWorker.Host.exe.config
	Core Worker Service files:
	`<Kofax Install location>\TotalAgility`
	`\CoreWorkerService`

• Kofax.CEBPM.Reporting.TAService.exe.config	Reporting Server Service file: `<Kofax Install location>\TotalAgility\Reporting`
• Kofax.CEBPM.CPUServer.ServiceHost.exe.config	Transformation Server Service file: `<Kofax Install location>\TotalAgility\Transformation Server`
• KSALicenseService.exe.config	License Server Service file: `<Kofax Install location>\TotalAgility\LicenseServer`
• ExtractionProcess.exe.config	`C:ProgramFiles (x86)\Common Files\Kofax\Server\`
• RegAscSc.exe.config	`<Kofax Install location>\TotalAgility\ExportConnectors\bin\`

Add a security provider

Add the following security provider in the configuration file before encrypting them:

```
<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>
```

Encrypt the configuration files of executables

The Kofax.CEBPM.EncryptConfig.exe utility encrypts (-enc) or decrypts (-dec) any section of the configuration file.

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

The TotalAgility Server supports two encryption methods depending on command line parameters using the Kofax.CEBPM.EncryptConfig.exe utility:

- DPAPI encryption
- RSA encryption

Use the DPAPI encryption method

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

Run the utility on each TotalAgility Server individually.

1. Stop the TotalAgility Core Worker Server service.

2. Navigate to the TotalAgility Core Worker installation directory.

3. Copy the **Kofax.CEBPM.EncryptConfig.exe** to the same folder where **Agility.Server.Core.WorkerService.exe.config** resides.

4. Open a Command Prompt window and 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

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 Server.

1. Create the custom RSA key container:

   a. Log on to the TotalAgility Server with administrator rights.

   b. Open a command-line window.

   c. Navigate to the .NET Framework version 4.0 directory. For example, enter the following command:

      cd \WINDOWS\Microsoft.Net\Framework\v4.0.*

     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 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.
- • <TAserviceuser> is the TotalAgility Core Worker Server service user.

3. Encrypt the file:

     a. Log on to the TotalAgility Server as the TotalAgility 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 `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, password and other 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 because it contains the unprotected private key.

2. Run the following command to grant the TotalAgility 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 Core Worker Server service user.

3. Repeat these steps on all remaining TotalAgility Servers.

Decrypt the configuration file

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

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

   > 🛑 Repeat the encrypt and decrypt procedures for Export configuration file also.

Encrypt the configuration files in a Docker container

You can encrypt the Web.config files and all executable configuration files using the "DPAPI" or "RSA" methods.

Encrypting the configuration files using "DPAPI"

Add the following to your Docker run command.

```
-e KTA_CONFIG_ENCRYPTION_PROVIDER_TYPE="DPAPI"
```

For example, "`docker run -d --hostname "opdemo2" --name "opdemo2" --`
`env-file "C: \Docker\TotalAgility\dockersettings.env" -p 5000:80 -e`
`KTA_CONFIG_ENCRYPTION_PROVIDER_TYPE="DPAPI" kofaxop"`

Encrypting the configuration files using "RSA"

Add the following to your docker run command.

```
-e KTA_CONFIG_ENCRYPTION_PROVIDER_TYPE="RSA"
```

For example, "`docker run -d --hostname "opdemo2" --name "opdemo2" --`
`env-file "C: \Docker\TotalAgility\dockersettings.env" -p 5000:80 -e`
`KTA_CONFIG_ENCRYPTION_PROVIDER_TYPE="RSA" kofaxop"`

Edit a configuration file

When you install TotalAgility On-Premise Multi-Tenancy, the system stores the configuration settings in a .NET file, Agility.Server.Core.WorkerService.exe.config. To change the value for any parameter, you can edit the Agility.Server.Core.WorkerService.exe.config file or run the TotalAgility

configuration utility to modify the settings. 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*.

1. If you encrypted the configuration file after you installed the TotalAgility Server, decrypt the file. See Decrypt a configuration file.

   ⓘ 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 On-Premise Multi-Tenancy configuration files.

   ⓘ 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 Core Worker Server service.

Edit the configuration files for safe scripting

Using the Safe Scripting option, you can configure TotalAgility to prevent malicious scripts and code from being executed on a multi-tenant environment without affecting the execution of other tenant's assemblies and ensure that tenant's data is isolated and cannot be accessed in any way by another tenant.

For example, you can configure C# scripts, VB .NET scripts, Expressions, .NET assemblies, or .NET Form actions, which when run into TotalAgility on a multi-tenant environment, allow or restrict certain actions.

Restrict:
- Accessing data from different tenants such as reading memory, file system or database.
- Breaking or affecting the process execution from the current or other tenants.
- Modifying operating system systems, update registry or reboot the machine.
- Reading or writing to file system outside of its allocated sandbox for its tenant.
- Executing non-CLR managed code.
- Running external OS process.
- Crashing hosted application.

Allow:

- Executing .NET managed code.
- Reading and writing to allocated sandbox folder for its tenant.
- Accessing internet (call web services using http protocol).
- Accessing a public database, if they have the credentials.
- Invoking APIs exposed by the TotalAgility SDK.

On installing TotalAgility, the safe scripting option is set to true by default. To set this option to false do the following:

1. Locate the setting, `<add key="SafeScripting" value="true"` in the following files:
   - Web.config available at `\\TotalAgility\Agility.Server.Web`
   - Agility.Server.Core.Executor.exe available at `\\TotalAgility\CoreWorkerService`
   - Agility.Server.StreamingService.exe available at `\\TotalAgility\CoreWorkerService`
   - Agility.Server.Core.WorkerService.exe available at `\\TotalAgility\CoreWorkerService`
2. Replace the value with "false".

Update the settings for a license server

When installing TotalAgility, by default, the primary license server is used. If the primary license server fails, you can connect to the backup server post installation manually, or run the Configuration utility.

Manually

After installing TotalAgility, you can update the license server parameters in the KSALicenseService.exe available in the installation directory.

1. Stop the Kofax Licenser Server service.
2. Navigate to the installation directory for the TotalAgility server.
3. In a text editor, open KSALicenseService.exe.config from the following directory: `\\Kofax\TotalAgility\LicenseServer`.
4. Locate the following section and update the serverID and connectionStrings parameters. By default, serverId value is "1", which means primary license server is connected.

```
<appSettings>
  <!-- Specify "1" for a primary license server or "2" for a backup license
  server. -->
  <add key="serverId" value="1"/>
</appSettings>
<connectionStrings>
  <add name="LicensingDatabase"
  connectionString="Server=<machinename>;Trusted_Connection=Yes;Database='
  TotalAgility ';"/>
</connectionStrings>
```

   a. To connect to the backup license server, modify the serverId value as "2".

   b. Update the LicensingDatabase connection string to point to Data Center Tenants for on-premise multi-tenant environment.

5. Save and close the configuration file.

Use the Configuration Utility

Run the Configuration utility and select **Backup** license server setting on the **Licensing** tab. See the *Kofax TotalAgility Configuration Utility Guide*.

Add custom job thread pools

A job thread performs multiple operations at a time, such as job evaluation, raising an exception job or ingestion through Kofax Import Connector. Multiple operations can lead to bottlenecks in the production systems. For example, when there are thousands of jobs to be archived, ingestion and job evaluation take longer time because the job threads are busy archiving jobs. Adding custom job thread pools, helps in achieving better throughput and prioritizing the background tasks.

You can add custom job thread pools, specify the number of threads in the thread pool and assign the worker task to a thread pool 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:

   ```
   \\OnPremiseMultiTenancyInstall\Agility.Server.Web
   ```
3. Locate the following section:

   ```
   <configSections>
       <section name="CoreWorker" type="Agility.Server.Core.Worker.Configuration,
   Agility.Server.Core.Worker"/>
     </configSections>
   ```

4. Add one or more job thread pools within the `CoreWorker` section and add worker tasks, as required. The following is a sample from the configuration file.
   Example

   ```
   <CoreWorker>
       <JobThreadPools>
         <add Id ="1" Size ="16" WorkerTasks ="ArchiveJobTask, DeleteItemTask,
   CreateExceptionTask, CreateJobTask, EvaluateJobTask,
       ProcessStateActionTask, IngestSystemTask, CaptureBatchTask "/>
       </JobThreadPools>
     </CoreWorker>
   ```

> ⓘ You must assign the following worker tasks to some thread pool, otherwise, an error message is displayed and the Core Worker Service stops working. You cannot assign the same worker task to more than one thread pool.
>   - ArchiveJobTask
>   - EvaluateJob Task
>   - CreateException Task
>   - CreateJob Task
>   - IngestSystem Task
>   - CaptureBatch Task
>   - DeleteItem Task
>   - ProcessStateAction Task

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

Use the Configuration Utility

Run the Configuration utility and add or update the custom job thread pools, specify the number of threads in the thread pool and assign the worker task to a thread pool.

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:

   ```
   \\OnPremiseMultiTenancyInstall\Agility.Server.Web
   ```
3. Locate the following section and add a thread pool monitoring interval (default:60).

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

   The default value is 60.
4. Save and close the configuration file.
5. Restart the TotalAgility Core Worker service.

Use the Configuration Utility

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

Add performance monitoring counters

Use the performance counters to record application states and activities.

The following categories for TotalAgility performance monitoring counters are automatically installed on the target machine when the Core Worker Service and the Export Service are installed:

- TotalAgility Core Worker: Locked Activities
- TotalAgility Core Worker: System Tasks
- TotalAgility Core Worker: Threads
- TotalAgility Core Worker: Worker Tasks
- TotalAgility Export Service
- TotalAgility Child Export Processes

Each category is associated with the performance counters. When the performance monitor is launched, you can select the installed counters and add to the current monitoring session. Each instance is recorded for a performance counter. For example, the Active Threads Per Thread pool performance counter records an instance per thread pool as shown in the image below.
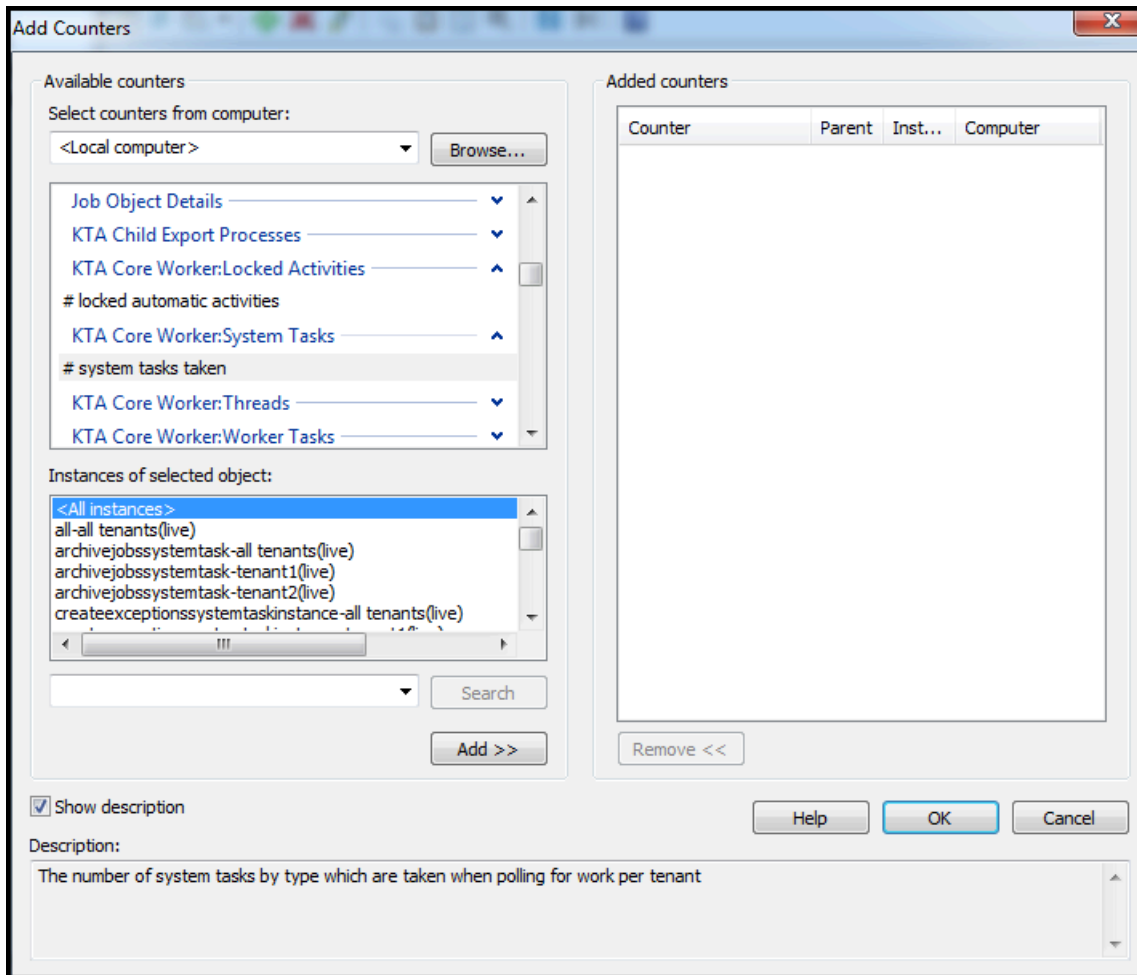
You can log each performance counter to the TotalAgility log file by enabling the logging function. For more information on performance monitoring counters, see the *Kofax TotalAgilityAdministrator's Guide*.

Anti-Cross Site Request Forgery (CSRF) measures

Use the following anti-CSRF measures to protect the site against Cross-site Request Forgery attacks.

- Configure the Anti-CSRF tokens
- Specify the Samesite attribute with value as Strict or Lax in the <hostCookies> tag of the web.config to prevent CSRF attacks. See the Microsoft website for more information.
- Enable Host prefix for cookies

Anti-Cross Site Request Forgery (CSRF) tokens

A CSRF attack relies on a user being authenticated on a website. The attack usually comes as an email or website hyperlink on which the user clicks while still authenticated. This URL then points back to the user's website and attempts to perform a privileged action (such as add an administrator account) without the user's knowledge. In TotalAgility, the TargetHostName and TargetPortNo settings are added as Anti-CSRF tokens in the Web.config file. The TargetHostName is the fully qualified domain name of the webserver and the TargetPortNo is the website port number. When you provide for these settings, the Anti-CSRF origin and referrer validations are performed on the request URL. If the validation fails, the request will be terminated considering it as a potentially dangerous request.

You can configure the Anti-CSRF tokens in the Web.config manually or using the Configuration Utility.

Manually

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

   `\\OnPremiseMultiTenancyInstall\Agility.Server.Web`
3. Locate the following section and specify the target host name and target port number.

   ```
   <appSettings>
                 <add key= "TargetHostName" value="<hostnamegoeshere"/>
    <add key= "TargetPortNo" value="443"
                 </appSettings>
   ```
4. Save and close the configuration file.

Use the Configuration Utility

Run the Configuration utility and specify the TargetHostName and TargetPortNo settings. See the *Kofax TotalAgility Configuration Utility Guide*.

Enable Host prefix for cookies

Use the "Host Prefix for Cookies", a browser functionality which makes the cookies more secure by prefixing the TotalAgility cookie names with "__HOST-". When a cookie name starts with this flag, it triggers additional browser policy on the cookie in supporting browsers. A __Host--prefixed cookie is only accessible by the same domain it is set on, which means a subdomain can no longer overwrite the cookie value. It also makes a cookie accessible from HTTPS sites only. This protects the cookie even if an attacker uses a forged insecure site to overwrite a secure cookie.

Edit the setting manually or use the Configuration Utility for enabling or disabling the cookies security.

Perform the following steps on the Web or combined Web/Application server.

1. On theKofax TotalAgility installation media, navigate to `\\OnPremiseMultiTenancyInstall\Agility.Server.Web`.
2. Open web.config in a text editor.

3. Locate the **<appSettings>** section and make sure the value of "UseHostPrefixForCookies" value="true".

```
<appSettings>
      <add key="UseHostPrefixForCookies" value="true"/>
</appSettings>
```

Use the Configuration Utility

Run the Configuration Utility and change the Host Prefix for Cookies setting on the Web settings tab as needed.

Update settings to prevent stored Cross-Site Scripting vulnerabilities

You can provide enhanced security to prevent stored Cross Site Scripting vulnerabilities in TotalAgility.

If TotalAgility is on https protocol and needs to prevent stored Cross Site Scripting vulnerabilities and enable additional security layer so that data remains secure.

Make sure URL redirect module is installed on your computer where TotalAgility is installed.

1. Navigate to the installation directory for the TotalAgility server.

2. In a text editor, open Web.config from the following directory:

   `\\TotalAgilityInstall\Agility.Server.Web`

3. Do one of the following:
   - If KCM is not installed, locate the rule: **"HTTP to HTTPS redirect"** and uncomment the `rewrite` section where this rule is available.
   - If KCM is installed and if you need additional layer of security, do the following:

     a. Locate the **"HTTP to HTTPS redirect"** rule (shown in bold) and copy it.

```
<rewrite>
      <rules>
        <rule name="HTTP to HTTPS redirect" stopProcessing="true">
         <match url="(.*)" />
         <conditions>
           <add input="{HTTPS}" pattern="off" ignoreCase="true" />
         </conditions>
         <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
redirectType="Permanent" />
        </rule>
      </rules>
      <outboundRules>
        <rule name="Add Strict-Transport-Security when HTTPS"
enabled="true">
        <match serverVariable="RESPONSE_Strict_Transport_Security"
pattern=".*" />
        <conditions>
          <add input="{HTTPS}" pattern="on" ignoreCase="true" />
        </conditions>
```

```
              <action type="Rewrite" value="max-age=31536000;
 includeSubDomains" />
          </rule>
      </outboundRules>
    </rewrite>
```

b. Locate the following section and paste the copied rule (as displayed in bold).

```
<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="ComposerTinyMCEProxyRule" stopProcessing="true">
          <match url="CCM/Proxy/tinymce/(.*)" />
          <action type="Rewrite" url="{http://ccmserver:port}/proxy/tinymce/
{R:1}" />
        </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>
         <rule name="HTTP to HTTPS redirect" stopProcessing="true">
          <match url="(.*)" />
          <conditions>
            <add input="{HTTPS}" pattern="off" ignoreCase="true" />
          </conditions>
          <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
 redirectType="Permanent" />
        </rule>
      </rules>
```

c. Locate the following outbound rule: **"Add Strict-Transport-Security when HTTPS"** (shown in bold) and copy it.

```
<rule name="Add Strict-Transport-Security when HTTPS" enabled="true">
```

```
              <match serverVariable="RESPONSE_Strict_Transport_Security"
pattern=".*" />
            <conditions>
              <add input="{HTTPS}" pattern="on" ignoreCase="true" />
            </conditions>
            <action type="Rewrite" value="max-age=31536000;
includeSubDomains" />
          </rule>
<rewrite>
      <rules>
        <rule name="HTTP to HTTPS redirect" stopProcessing="true">
          <match url="(.*)" />
          <conditions>
            <add input="{HTTPS}" pattern="off" ignoreCase="true" />
          </conditions>
          <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
redirectType="Permanent" />
        </rule>
      </rules>
      <outboundRules>
         <rule name="Add Strict-Transport-Security when HTTPS"
enabled="true">
          <match serverVariable="RESPONSE_Strict_Transport_Security"
pattern=".*" />
          <conditions>
            <add input="{HTTPS}" pattern="on" ignoreCase="true" />
          </conditions>
          <action type="Rewrite" value="max-age=31536000;
includeSubDomains" />
        </rule>
      </outboundRules>
    </rewrite>
```

   d. Paste it before the closing bracket of outbound rules of CCM (as displayed in bold).

```
<outboundRules>
          <rule name="HTTPCookie" preCondition="IncomingNoSSLSecureCookie">
            <match serverVariable="RESPONSE_Set_Cookie" pattern="(.*);
Secure(.*)" />
            <action type="Rewrite" value="{R:1}{R:2}" />
          </rule>
          <rule name="HTTPSCookie" preCondition="IncomingSSLNoSecureCookie">
            <match serverVariable="RESPONSE_Set_Cookie" pattern="(.*);
HttpOnly" />
            <action type="Rewrite" value="{R:1}; Secure; HttpOnly" />
          </rule>
          <preConditions>
            <preCondition name="IncomingNoSSLSecureCookie">
              <add input="{CACHE_URL}" pattern="^http://" />
              <add input="{RESPONSE_Set_Cookie}" pattern=".*; Secure.*" />
          </preCondition>
          <preCondition name="IncomingSSLNoSecureCookie">
            <add input="{CACHE_URL}" pattern="^https://" /><add
input="{RESPONSE_Set_Cookie}" pattern=".*; Secure.*" negate="true"/>
          </preCondition>
        </preConditions>
<rule name="Add Strict-Transport-Security when HTTPS" enabled="true">
        <match serverVariable="RESPONSE_Strict_Transport_Security"
pattern=".*" />
        <conditions>
          <add input="{HTTPS}" pattern="on" ignoreCase="true" />
        </conditions>
        <action type="Rewrite" value="max-age=31536000;
includeSubDomains" />
```

```
                          </rule>
                  </outboundRules>
```

4. Save and close the configuration file.

Log on to TotalAgility On-Premise Multi-Tenancy

After you install TotalAgility Tenant Management application, it will create a shortcut in All Programs.

1. On the **Start** menu, navigate to **Kofax TotalAgility Tenant Management** > **TenantAdmin**. Alternatively, enter the following URL in the browser:

    ```
    http://<TA server hostname or IP>/TenantManagementWebSite/
    TenantManagement/TenantLogon.html
    ```

    The TotalAgility Tenant Management application is started.

2. Enter the **Username** and the **Password**.

    Kofax TotalAgility On-Premise Multi-Tenancy is launched in the browser.

    > ⓘ The default username and password is **Administrator**. Change the username and password for security reasons. See "Manage Users" in the *Help for Tenant Management System*.

3. To access TotalAgility Designer, you must create a tenant. See "Create a tenant" in the *Help for Tenant Management System*.

    > ⓘ You need to update both DB accounts (Database Creator and Login Creator) when adding tenants. The Database Creator must have rights to create tenant database and Login Creator must have rights to create logins for tenants.

4. After creating a tenant, an email is sent to the tenant's email address with login credentials. Based on the tenant's permissions, links are sent for the TotalAgility Designer, Kofax TotalAgility Quick Start and TotalAgility Workspace for production and development environments.

    > ⓘ A Wildcard DNS must be used along with the Wildcard SSL certificate to resolve the tenant URL. You can update the Windows hosts file (`%windir%\System32\drivers\etc\hosts`) to allow the URLs to be resolved for demo testing purposes. Updating the Windows hosts file approach must not be used in a production environment.

Secure cookies

The Secure attribute for sensitive cookies in HTTPS sessions is not set by default. This allows a browser to send these cookies in plain text over an HTTP session.

To secure the cookies, uncomment the `httpCookies` tag, `<httpCookies requireSSL="true"/>` in the Kofax TotalAgility Web.config file.

Install the language pack

The languages files are available at the following location in the installation directory:

`\\OnPremiseMultiTenancyInstall\Agility.Server.Web`

After installing TotalAgility, import <Language>.zip using the "Import Languages" feature of the TotalAgility menu.

When you change your browser to one of the supported languages, the corresponding translation is displayed.

> ❶ Only the Workspace is localized according to the browser display language after installing the language pack.

Install the .NET Framework language packs

To localize the system error messages from .NET, you must install the .NET Framework language packs on both the Web and Application servers.

You can download the .NET Framework language pack from the Microsoft website.

Install the .NET Framework language packs

To localize the system error messages from .NET, you must install the .NET Framework language packs on both the Web and Application servers.

You can download the .NET Framework language pack from the Microsoft website.

Exclude folders from antivirus scan

In your antivirus application, add the following TotalAgility folders to the list of items which are excluded from scanning:

- `\\ProgramData\Kofax`
- `\\Program Files (x86)\Common Files\Kofax`
- `\\Program Files\Kofax\TotalAgility\`

Access TotalAgility documentation

You can access help online as well as in offline mode.

Online documentation

The product documentation for Kofax TotalAgility 7.10.0 is now available at the following location:

https://docshield.kofax.com/Portal/Products/KTA/7.10.0-vmhad0mru4/KTA.htm

To launch the online help for the installed version of the product, click the Help icon on the application.

> ⓘ
>
> - On upgrading to TotalAgility 7.10.0 from an earlier version, to view the TotalAgility Workspace help, you must import the WorkspaceHeader form from the TotalAgility Workspace package.
> - When upgrading to TotalAgility 7.10.0 from an earlier version, ensure that the check box for "Import system Workspace package" is selected to view the Workspace help online; otherwise, you must import the WorkspaceHeader form from the TotalAgility Workspace package.

Offline documentation

To access the documentation offline, you can download it from the Kofax Fulfillment Site. For each language, a separate documentation package is available to download as a compressed file, such as Kofax TotalAgilityDocumentation7.10.0_EN.zip for English or Kofax TotalAgilityDocumentation7.10.0_FR.zip for French.

The English .zip file includes both help and print folders. The print folder contains all guides, such as installation guide and administrator's guide. The .zip files for other languages contain only the localized files as applicable.

The following procedure describes accessing TotalAgility documentation offline for English.

1. From the Kofax Fulfillment Site, download the documentation.zip file for the applicable language.
2. Extract the contents of the compressed documentation file to your local machine.

3. On the TotalAgility installation media, inside the `Agility.Server.Web\Help` folder, create a folder for the desired language. For example, for accessing TotalAgility documentation offline for English, create EN folder as follows:

> ❶ In a distributed environment, perform copying files on the Web server, and the Web.config changes on the Application and Web servers.

- Copy the contents from Designer folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\TotalAgility_designer\EN`

  > ❶ TotalAgility installer creates the TotalAgility_designer and API folders inside the Help folder. You must manually create other folders such as Workspace and TotalAgilityApps and then copy the contents into the respective folders.

- Copy the contents from Workspace folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\Workspace\EN`

- Copy the contents from WebCaptureControl folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\WebCaptureControl\EN`

- Copy the contents from TransformationDesigner folder to:

  `<%ProgramData%>\Kofax\Transformation\en_US\help\TransformationDesigner`

- Copy the contents from KCKTM_Converter folder to:

  `<%ProgramData%>\Kofax\Transformation\en_US\help\KCKTM_Converter`

- Copy the contents from XDocBrowser folder to:

  `<%ProgramData%>\Kofax\Transformation\en_US\help\XDocBrowser`

- Copy the contents from TenantManagementSystem folder to:

  `\\TotalAgilityInstall\Agility.Server.Web.TenantManagement`
  `\TenantManagement\Help\TenantManagementSystem\EN`

- Copy the contents from TotalAgilityApps folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\TotalAgilityApps\EN`

- Copy the contents from ExportConnector folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\ExportConnector_help\EN`

- Copy the contents from the activity (such as DocumentReviewActivity) folder within CaptureClient folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Forms\Controls\Capture\Help`
  `\DocumentReviewActivity\EN`

- Copy the contents from Devices folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\bin\Administrative\Help\Devices`
  `\EN`

- Copy the contents from RepositoryBrowser folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\RepositoryBrowser\EN`

- Copy the contents from SDK_Documentation folder to:

  `\\TotalAgilityInstall\Agility.Server.Web\Help\API\EN`

- Copy the contents from DocumentConverter folder to:

  `\\Kofax\Document Converter\web\en\WebHelp`

- Copy the contents from MessageConnector folder to:

  `\\Kofax\KIC-ED\MC\web\en\WebHelp`

4. Navigate to the installation folder and do the following:
   - For TotalAgility Designer help, Devices help, Transformation Designer help, XDoc Browser help and KC_KTM Converter help:
     a. Open TotalAgility Web.config in a text editor from the following location:

        `\\TotalAgilityInstall\Agility.Server.Web`

     b. Locate the <appSettings> section and remove `http://docshield.kofax.com/KTA` from the key value: `<add key="OnlineHelpURL" value="http://docshield.kofax.com/KTA"/>`.

        Alternatively, run the Configuration Utility (available from the Installation media at `\\TotalAgilityInstall\Utilities\ConfigurationUtility`) and remove the URL for online help from the OnlinehelpURL setting.

     > ⓘ For Transformation Designer, XDoc Browser and KC_KTM Converter Help to work offline, make sure that TotalAgility is actively connected to Transformation Designer. To connect TotalAgility to Transformation Designer, log in to Transformation Designer and click **File > Connections** and provide the connection path.

   - For TotalAgility Export Connector help:
     a. Open Agility.Server.ExportConnector.exe.config in a text editor from the following location:

        `\\TotalAgilityInstall\Agility.Server.Web\bin`

     b. Locate the <appSettings> section and remove `http://docshield.Kofax.com/KTA` from the key value: `<add key="OnlineHelpURL" value="http://docshield.kofax.com/KTA"/>`.

   - For TotalAgility Message Connector help:
     a. Open configuration.xml in a text editor from the following location:

        `\\Kofax\KIC-ED\MC\web`

     b. Locate the <OnlineHelp>1</OnlineHelp> section and replace 1 with 0.

   - For TotalAgility Document Converter help:
     a. Open configuration.xml in a text editor from the following location:

        `\\Kofax\Document Converter\web`

     b. Locate the <OnlineHelp>1</OnlineHelp> section and replace 1 with 0.

5. Save and close the configuration file.
   Clicking the Help icon will launch the help for the installed product.

Chapter 3

Transformation Server Bundle installation

The Transformation Server Bundle includes:

- Transformation Server
- Transformation Core modules

To install any component, you must install the entire Transformation Server Bundle.

You can install the Transformation Server Bundle when you install TotalAgility, or install the Transformation Server Bundle separately.

> ⓘ
>
> - For development environments, install the Transformation Server Bundle where you installed TotalAgility. For production environments, install the Transformation Server Bundle on a separate computer.
> - If you install the Transformation Server or Transformation Designer independent of TotalAgility, make sure the supported version of .NET Framework is already installed on that machine.
> - The user who will run the Transformation Server must have "Log on as Service" rights. Also, the user who is running Transformation Server will be used for all communication channels where Windows authentication is used. For example, if Windows authentication is being used for SQL Server, this user must have rights on this server, otherwise Transformation Server does not work.
> - The user who will run the Transformation Server must have the rights described in Configure the user account.
> - After installing the Transformation Server, you can modify the configuration settings by editing the Transformation Server configuration file or by running the configuration utility. See the *Kofax TotalAgility Configuration Utility Guide*.

Perform a silent installation

This section describes the steps to silently install the Transformation Server Bundle without any interaction with TotalAgility. For development environments, install the Transformation Server Bundle where you installed TotalAgility. Otherwise, install the Transformation Server Bundle on a separate system in the same domain where you installed TotalAgility.

> ⓘ If you copy and paste the code from this guide, fix any incorrect line breaks.

1. Launch a Command Prompt window and navigate to `\\TotalAgility\Transformation Server\`.

2. Run the following command:

```
TransformationServerSetup.exe /quiet /log %LogFile% TS_INSTALLLOCATION=
%InstallLocation% TS_SERVICE_ACCOUNT=%WindowsServiceAccount%
TS_SERVICE_PASSWORD=%WindowsServicePassword% TS_USE_SPECIFIC_POOL=
%UseSpecificPool%TS_POOL_NAME=%PoolName% TS_OL_ENABLED=%OLEnabled
% TS_WCF_PORT=%WcfPort% TS_RESERVED_SLOTS=%ReservedSlots%
TS_OVERRIDE_DEF_SLOTS=%OverrideDefSlots% TS_MAX_SLOTS=%MaxSlots
% TS_ENABLE_SYNC_CALLS=%EnableSyncCalls% TS_STARTSERVICE=TRUE
TS_MULTITENANT_INSTALL=1 TS_TENANT_DB_CONNECTION_STRING=
%DataCentreDatabase% TS_INSTALL_OCR_ADDONS=% TS_DEPLOYMENT_TYPE=
%MultiTenancyInstallMode%
```
(deployment type is case sensitive and should be in lower case only)

For description of these parameters, see Silent installation of Web and Application on the same server.

> ⓘ Enter more parameter values as necessary. If the value of a parameter has spaces, enclose the value in quotation marks.

Example: Silent installation command

```
TransformationServerSetup.exe /quiet /log TSinstallationLog.log
TS_USE_SPECIFIC_POOL=true
TS_POOL_NAME=Pool1
TS_OVERRIDE_DEF_SLOTS=true
TS_MAX_SLOTS=2
TS_INSTALL_OCR_ADDONS=1
TS_TENANT_DB_CONNECTION_STRING="Server=dbserver;Database=TotalAgility;User ID=dbo_id;
 Password=dbopassword;
```

TS_SETUP_CONFIG_FILE sample

```
TS_SERVICE_ACCOUNT=.\serviceUser
TS_SERVICE_PASSWORD=secretPwd
TS_TENANT_DB_CONNECTION_STRING=Server=localhost;Trusted_Connection=Yes;
Database=DataCenter_Tenants;
```

Perform a standard installation

Use the Installation Wizard to install and configure Transformation Server for a multi-tenant configuration. This approach provides different options than a non-tenant configuration. Before you start the installation, ensure that you have fulfilled all of the requirements, which include granting the user who will run the Transformation Server service the rights described in Configure the user account.

> ⓘ If you install Transformation Server for a multi-tenant installation and you later need to switch to a non-tenant configuration, reinstall Transformation Server.

1. Start the Installation Wizard. Use the appropriate method for your type of system.
   - **Production systems**: Install the Transformation Server Bundle separately from TotalAgility. Navigate to the `TransformationServer` folder and do either of the following:
     - To install without creating a log file, run **TransformationServerSetup.exe**.
     - To install and create a log file, open a Command Prompt window and enter the following command:
       ```
       TransformationServerSetup.exe \log <path\install_log.txt>
       ```
       Where `<path\install_log.txt>` is the path and name of the log file.
   - **Development systems**: If you are installing the Transformation Server Bundle as part of the TotalAgility installation, the Transformation Server Bundle installer opens automatically.

   The Kofax Transformation Server Bundle window appears.

   > ⓘ Perform steps 2, 3 and 5 only if you are installing Transformation Server Bundle separately from TotalAgility. If you are installing Transformation Server Bundle as part of the TotalAgility installation, you are directly taken to step 4.

2. In the **Kofax Transformation Server 7.10** window, click **Options** and do the following:

Setup Options	
Multitenant installation	If selected, installs the Transformation Server on an on-premise multi-tenancy environment. (Default: Clear)
Additional A2iA engines [unsupported]	If selected, installs additional OCR engines (A2iA CheckReader and A2iA FieldReader). (Default: Selected)
Natural Language Processing language bundles	
Western (en, es, pt, fr, de) (default: selected)	If selected, installs natural processing language bundles.
Western extended (it, ro, nl)	
Extended (ja, zh, ko)	

3. Click **Options**.
   The Setup Options window appears.
4. Select **Multitenant Installation** and click **OK**.
   You return to the first window.
5. Click **Install**. When the welcome screen appears, click **Next**.
   The license agreement window appears.

   > ⓘ The license agreement window does not appear if you are installing Transformation server as part of TotalAgility installation.

6. Accept the terms in the license agreement and click **Next**.
   A window appears where you select the folder where Transformation Server is installed.

7. Use the default installation path or change it by typing it in the field or selecting it from the window by clicking **Change**. To continue with the installation, click **Next**.

8. Type the name and password of the user account used to run the Transformation Server service. To specify a domain user, enter the user name in the format Domain\User. Click **Next**.

> ⓘ Perform Step 8 only if you are installing Transformation Server Bundle separately from TotalAgility. If you are installing Transformation Server Bundle as part of the TotalAgility installation, the connection string for the tenant database is automatically displayed.

9. Set up data to connect to the tenant database.

    a. Select either Dev or Live.

    b. Enter the connection string to connect to and authenticate with the tenant database. Use the following syntax:

    - SQL authentication:

    ```
    Server=<server address or name>;Database=DataCenterTenants;User
     ID=<user_name>; Password=<password>;
    ```

    Specify the address of the database server and the user name and password to authenticate with database where indicated. Example:

    ```
    Server=dbserver;Database=DataCenterTenants;User ID=dbo_id;
     Password=dbopassword;
    ```

    - Windows authentication:

    ```
    Server=<server address or
     name>;Trusted_Connection=Yes;Database=DataCenterTenants;
    ```

    Example:

    ```
    Server=dbserver;Trusted_Connection=Yes;Database=DataCenterTenants;
    ```

    c. Click **Next**.

10. Select either advanced execution option:

    - **Enable synchronous calls processing**: To select the TCP/IP port and number of reserved processing slots. The default TCP/IP port is 9001, and the number of reserved processing slots is 0.

    > ⓘ If you are upgrading Transformation Server from version 7.0, "Enable synchronous calls processing" is disabled if the number of reserved processing slots is zero and enabled if there are one or more reserved processing slots.

    - **Override default number of processing slots**: To specify a number of slots other than the default.

    Click **Next**.

11. Click **Install** to install the Transformation Server.

    The system displays the installation status and a message when Transformation Server setup is complete.

12. Click **Finish**.

    The system displays the Transformation Server Bundle setup status and a message when the Transformation Server Bundle installation is successful.

13. Click **Close** to close the success message window.

Encrypt and decrypt the configuration file

The configuration file includes the Transformation Server settings, including sensitive information. Therefore, we recommend that you encrypt this file. The Transformation Server supports two encryption methods depending on command line parameters:

- **DPAPI encryption**: Because you must decrypt the file on the same machine where it was encrypted, use this utility to encrypt one server at a time. See Use Kofax.CEBPM.EncryptConfig.exe.
- **RSA encryption**: An algorithm for public key encryption and digital signatures that uses two separate keys. Create a key and encrypt the configuration file on one Transformation Server, and export the key to all the other Transformation Servers. All the Transformation Servers with the exported key installed can access the configuration file. Use this method if you have several Transformation Servers with the same configuration (TAService ID, pool name, and so on). See Use RSA Encryption.

To decrypt the configuration file, see Decrypt the configuration file.

Use Kofax.CEBPM.EncryptConfig.exe

The Kofax.CEBPM.EncryptConfig.exe utility encrypts (-enc) or decrypts (-dec) the CPUServer and appSettings sections of the configuration file. The CPUServer section includes the TotalAgility Session ID. The AppSettings section includes the user ID and password as well as other information. Use the optional -h flag to display help for the command.

Encrypt a File with Kofax.CEBPM.EncryptConfig.exe

Run the utility on each Transformation Server individually.
1. Stop the Transformation Server service.
2. Navigate to the Transformation Server installation directory and open a command Prompt window.
3. Run the following command:

   Kofax.CEBPM.EncryptConfig.exe -f Kofax.CEBPM.CPUServer.ServiceHost.exe.config -s "appSettings" -p DPAPIProtection -enc

Use RSA encryption

Use RSA encryption to encrypt the configuration file, export the encryption key, and install the encryption key file on multiple Transformation Servers. Use this method if you have several Transformation Servers with the same configuration (TAService ID, pool name, and so on).

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

Prepare the key

Perform these steps on one source Transformation Server.

1. Create the custom RSA key container:

    a. Log on to the Transformation Server with administrator rights.

    b. Open a Command Prompt window.

    c. Navigate to the .NET Framework version 4.5 directory. For example, enter the following command:

        ```
        cd \WINDOWS\Microsoft.Net\Framework\v4.5.*
        ```

    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 Transformation Server service user permission to read the <KeysFile> RSA container file.

    aspnet_regiis -pa "<KeysFile>" "<TSserviceuser>"

    where:

    - **<KeysFile>** is the name of the key file you created in Step 1d.
    - **<TSserviceuser>** is the Transformation Server service user.

3. Encrypt the file:

    a. Log on to the Transformation Server as the Transformation Server service user.

    b. Navigate to the installation directory for the Transformation Server and open a Command Prompt window.

    c. Run the following command:

        ```
        Kofax.CEBPM.EncryptConfig.exe -f
        Kofax.CEBPM.CPUServer.ServiceHost.exe.config -s "appSettings" -p
        RSAProvider -enc
        ```

        This command encrypts the CPUServer and AppSettings sections of the configuration file. The CPUServer section includes the TotalAgility Session ID. The AppSettings section includes the user ID, password and other 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 Transformation Server.

1. Import the key:

    a. Log on to the Transformation Server with administrator rights.

    b. Copy the keys.xml file from the source Transformation Server to the root directory of the target Transformation Server.

    c. Open a Command Prompt 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 because it contains the unprotected private key.

2. Run the following command to grant the Transformation Server service user permissions to use the <KeysFile> RSA container file:

    ```
    aspnet_regiis -pa "<KeysFile>" "TSserviceuser"
    ```
    where:
    - **<KeysFile>** is the name of the key file you imported in step 1.
    - **<TSserviceuser>** is the Transformation Server service user.

3. Repeat these steps on all remaining Transformation Servers.

Decrypt the configuration file

1. Stop the Transformation Server service.
2. Navigate to the Transformation Server installation directory and open a command-line window.
3. Run the following command:

    ```
    Kofax.CEBPM.EncryptConfig.exe -f
    Kofax.CEBPM.CPUServer.ServiceHost.exe.config -s "appSettings" -p
    DPAPIProtection -dec
    ```

Edit the configuration file

Modify the Transformation Server configuration file, **Kofax.CEBPM.CPUServer.ServiceHost.exe.config** if the system configuration has changed, or when you need to resolve a technical or performance issue.

1. If you encrypted the configuration file after you installed the Transformation Server, decrypt the file. See Decrypt the configuration file.

    > ℹ If RSA encryption is used, decrypt the configuration file only on the source Transformation Server where you initially encrypted the file.

2. Navigate to the installation directory for the Transformation Server and locate **Kofax.CEBPM.CPUServer.ServiceHost.exe.config**.

3. Back up the file and save it in a secure location.

4. Open the configuration file in a text editor.

5. To change the system configuration options, modify the keys in the `<appSettings>` section.

   The section contains a list of keys for setting configuration options. The ones that can be modified have comments that describe the setting and supported values, as in this example.

   ```
   <!-- Maximum number of instances allowed for Executor Process -->
        <add key="MaxNumberOfTenantProcesses" value="1"/>
   ```

6. Change the value within the quotation marks to a supported value, as indicated in the comments.

7. To change how errors are reported in the application event log, which can be viewed in the Event Viewer, modify the **<system.diagnostics>** section as follows:

   a. Under **<switches>**, locate the following element:

   ```
   <add name="TraceLevelSwitch" value="Warning"/>
   ```

   By default, the value is set to Warning, which reports error and warning messages. Change the value to any of the options listed in the comment to change the type of messages reported.

   b. Under <sharedListeners>, locate the following line:

   ```
   <add name="CPUServerLogTxt" type="
    Kofax .CEBPM.CPUServer.Common.Diagnostics.DateTimeTaggedTraceListener,
    Kofax .CEBPM.CPUServer.Common" initializeData=" Kofax CPUServerLog.log" >
   ```

   To specify a different log file or change the format for **timestamps**, change the value of **initializeData** as shown in the comments in the file.

8. Save and close the configuration file.

9. To re-encrypt the configuration file, run the encryption utility. See Encrypt and Decrypt the configuration file.

   > ⓘ If you used RSA encryption, export the key, and install the encryption key file on any target Transformation Servers imported the original encrypted configuration file.

10. Restart the Kofax Transformation Server service.

Install the NLP language packs manually

If the Transformation Designer is installed on a separate server than the Transformation Server Bundle in your solution, then you need to install the Kofax NLP engine language packs on the machine where Transformation Designer is installed. This is because the Kofax NLP engine language packs are installed by the Transformation Server Bundle only, and these languages are required to use the Kofax NLP functionality in Transformation Designer and in production.

To install the Kofax NLP engine language packs, you need access to the original Kofax TotalAgility installation zip file.

You can install the Kofax NLP engine language packs by following these steps.

1. Navigate to the `TotalAgility\TransformationServer`
   `\KofaxTransformation_Salience6.4` path inside the extracted Kofax TotalAgility
   installation zip file.

2. Double-click on one of the following `.MSP` files depending on what languages you are
   supporting.
   - KofaxTransformation_SalienceV6.4.0_LanguageBundle_western-default.

     Run to install English, Spanish, Portuguese, French, and German support.
   - KofaxTransformation_SalienceV6.4.0_LanguageBundle_western-extended.

     Run to install Italian, Romanian, and Dutch support.
   - KofaxTransformation_SalienceV6.4.0_LanguageBundle_extended.

     Run this to install Japanese, Chinese, and Korean support.

   A Windows Installer window appears and then installs the selected Kofax NLP languages
   automatically.

   The installer window closes when the installation is complete.

3. Optionally, double-click on another language installer if you want to support additional
   languages.

Uninstall the Transformation Server

Uninstall Transformation Server depending on how you have installed it.

- When you install Transformation Server as part of Kofax TotalAgility standard installation,
  uninstalling TotalAgility will automatically uninstall Transformation Server.
- When you install Transformation Server on a separate system, uninstall the Transformation
  Server Bundle from the Control Panel.
- To uninstall in a silent mode, do the following:
  - Navigate to the root directory of TransformationServerSetup.exe.
  - Run `TransformationServerSetup.exe / uninstall / quiet`.

    The system uninstalls the Transformation Server and automatically creates a log file in the
    temporary files folder. This log file contains information on errors, if any.

Reporting Server installation

This chapter describes two methods for installing the Kofax Reporting Server:
- Silent installation of Reporting Server independent of TotalAgility
- Standard installation using the installation wizard.

Perform a silent installation

The following table describes the parameters to set when you silently install the Reporting Server independent of TotalAgility. For development environments, install the Reporting Server where you installed TotalAgility. Otherwise, install the Reporting Server on a separate system in the same domain where you installed TotalAgility.

> ⓘ If you copy and paste the code from this guide, fix any incorrect line breaks.

Parameter	Default Value	Description
`INSTALLLOCATION`	`C:\Program Files\Kofax \TotalAgility\Reporting Server\`	Specify the Reporting Server destination directory.
`WINSERV_ACCOUNT`	no default	Enter the name of the user who will run the Reporting Server. To specify a domain user, enter the user name in the format Domain\User.
		Ensure that the account details are correct, as under this account Reporting Server authenticates in all places where Windows authentication is used. Example: TA database.
		All communication and resource access is run under this account. Therefore, the account under which Reporting Server is running must not be a dummy account.
`WINSERV_PASSWORD`	no default	Enter the password for the user.

Parameter	Default Value	Description
DEPLOYMENT_TYPE	live or dev	Specify the deployment type as live or dev.
TENANT_DB_CONNECTION_STRING	Server=localhost; Trusted_Connection=Yes; Database=DataCenterTenants;	Enter a connection string to the TotalAgility tenants database (DataCenterTenants).

ⓘ Parameter names are case-sensitive.

1. Launch a Command Prompt window and on the installation media, navigate to `\\Reporting\`.
2. Run the following command:

```
msiexec.exe /i Kofax.Reporting.TAService.msi /q MULTITENANT_INSTALL=1
WINSERV_ACCOUNT=%WindowsServiceAccount% WINSERV_PASSWORD=
%WindowsServicePassword%TENANT_DB_CONNECTION_STRING="%DataCentreDatabase
%" INSTALLLOCATION="%InstallDirectory%" DEPLOYMENT_TYPE=
%MultiTenancyInstallMode% (deployment type is case sensitive and should be
lower case only)
```

ⓘ Enter more parameter values as necessary. If the value of a parameter has spaces, enclose the value in quotation marks.

Perform a standard installation

1. On the TotalAgility installation media, navigate to `TotalAgility > Reporting > TAReportingService > Kofax.Reporting.TAService.msi`.
   The TotalAgility Reporting Server Setup window opens.
2. Click **Next**.
3. In the End-User License Agreement window, accept the terms in the License Agreement and click **Next**.
4. In the Destination Folder window, select the default folder (`C:\Program Files (x86)\Kofax\TotalAgility\Reporting Server\`) for the Reporting server or click **Change** to choose another folder.
5. Click **Next**.
6. In the Service Account Setup window, enter the credentials for the user who will run the Kofax TotalAgility Reporting Server service:

   a. In the **Username** field, enter the username.

      ⓘ To specify a domain user, enter the username in the format Domain\User.

   b. Enter and confirm the **Password**.

   c. Click **Next**.

7. In the Obtaining TotalAgility Configuration window, enter the URL of the Reporting Server service where the configuration settings reside and click **Next**.

   Use the following format: `http://<server_name>/TotalAgility/Services/Core/TenantService.svc`

   where `<server_name>` is the TotalAgility server name

   The system downloads the settings.

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

9. Click **Finish**.

Uninstall the Reporting Server

Uninstall the Reporting Server depending on how you have installed it.

- When you install the Reporting Server as part of Kofax TotalAgility standard installation, uninstalling TotalAgility will automatically uninstall the Reporting Server.

- When you install the Reporting Server on a separate system using the Wizard, uninstall the Reporting Server from the Control Panel.

- If you install the Reporting Server in a silent mode, you must do the following to uninstall the Reporting Server in a silent mode:

   1. On the Command Prompt, change the command line to the root directory of the `Kofax.Reporting.TAService.msi` file.

   2. Run `msiexec.exe/quiet/x Kofax.Reporting.TAService.msi/L*V"%LogFileName%"`.

      The system uninstalls the Reporting Server and automatically creates a log file in the temporary files folder. This log file contains information on errors, if any. You can use `"msiexec/help"` (Windows installer help) to check options for the installation and logging.

Integrate Microsoft Dynamics CRM with TotalAgility

You can integrate Microsoft Dynamics CRM and Microsoft Dynamics 365 CRM with TotalAgility . To install both, the users must have the administrator rights.

See also:
- Dynamics CRM installation
- Update the Web configuration file for Dynamics CRM

Install Dynamics CRM

Follow the same steps to install Dynamics CRM and Dynamic 365 CRM.

1. Navigate to `\\DynamicsCRMInstall` on the installation media, and double-click **Setup.exe**.
   For Dynamics 365 CRM, navigate to `\\Dynamics365CRMInstallation` on the installation media, and double-click `Dynamics365CRM_Setup.exe`.
   The installation wizard appears.
2. Click **Next**.
3. In the **CRM Server** field, enter the IP address or machine name of the CRM server.
4. In the **CRM Port** field, enter the port on which CRM is running.
5. To enable SSL (Secure Sockets Layer), select **Use SSL** (default: Clear).
6. In the **Domain** field, 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 Web.config for Dynamics CRM

Add the following script for the TotalAgility components to support event handlers in Dynamics CRM and Dynamics 365 CRM:

> ℹ 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 &amp; 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://<TotaAgility 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 TotalAgility.

Integrate Microsoft Dynamics AX with TotalAgility

To install 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 `\\DynamicsAXInstall` on the installation media and double-click **Setup.exe**.

   The TotalAgility for Dynamics AX Setup wizard appears.

2. Click **Next**.

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

   > ❶ If the required software is not installed, 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 4.0.

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:\Program Files\Microsoft` `Dynamics AX\60\AifWebServices`
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`
		Not Applicable

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**.

   > ❗ 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 following URL for instructions: `http://msdn.microsoft.com/en-us/library/gg846350.aspx`.

Create Dynamics AX 09 service reference to the TotalAgility web service

1. Start Dynamics AX 09.
2. Click **AOT** (Application Object Tree) and press **Ctrl+D**.
3. In the application object tree, Right-click **References** and select **Add service reference**.
4. 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.

5. Click **OK**.

Create Dynamics AX 12 service reference to the TotalAgility web service

1. Start Dynamics AX 12.
2. Click **AOT** (Application Object Tree) and press **Ctrl+Shift+W**.
3. In the application object tree, right-click **References** and select **Add Reference**.
4. Browse to the TotalAgility assembly, KtaEvents.Services.dll which was installed previously. For example,

   `C:\Program Files (x86)\Microsoft Dynamics AX\60\Client\Bin`

5. Click **OK**.

Add a reference in Dynamics AX

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. Click **Browse** and navigate to the Dynamics AX Setup installation folder (in the Program
    Files(x86) or Program Files 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.

> ⓘ Once the class is imported, the Status tab in the compiler output page displays any errors.

Edit database X++ event methods

You can edit the database X++ event methods in the DAX Development Workspace under Classes and Application folders.

1. To alter the Application CUD (create, update and delete) class event methods, call the custom class method EventChangeNotifyKtaWebService when a CUD event has been 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:

   - Insertlog method: `new ktaController().EventChangeNotifyKtaWebService("Create", recordInserted, null, conNull(), recordInserted.RecId);`

   - Deletelog method: `new ktaController().EventChangeNotifyKtaWebService("Delete", recordDeleted, null, conNull(), recordDeleted.RecId);`

   - Updatelog method: `new ktaController().EventChangeNotifyKtaWebService("Update", recordOrig, recordUpdated, changedFields, recordUpdated.RecId);`

   > ⓘ 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 Application pool account is using the correct Business Connecter.NET (BC.NET) Windows credentials.

1. On the Start menu, select **All Programs** > **Accessories** and click **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, do the following:

   a. On the Actions panel, click **Advanced Settings**.

   b. 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. (The Kofax WCF service uses the BC.NET account to connect to Dynamics AX).

9. Click **OK**.

Integrate Micro Focus Content Manager with TotalAgility

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

Prior to installing Content Manager server, install the following software:

- IIS
- .NET Framework 4.6.1
- TotalAgility (optional)

Identify the Content Manager SDK Version

These instructions only apply to Content Manager version below 8.

1. Navigate to the **C:\Program Files\Kofax\TotalAgility** directory.
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. For example, 7.3.0.

   > ⓘ For TRIM SDK 7.3.0 and later, you will require to enter this number in the <assemblyBinding> section of the Web.config (see Set up the Micro Focus 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 Content Manager system.

Install and configure TotalAgilityTrimCommunicatorService

To install and work with Micro Focus Content Manager with version 9.4 or higher, do the following.

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

3. Click **Yes**.

   The installation wizard appears.

4. Click **Next**.

   The setup is ready to install the TotalAgility integration components.

   > ⓘ
   >
   > • If the Trim SDK already exists in your system, the **Trim SDK Detected** checkbox is by selected by default. Click **Finish**.
   >
   > • If the Trim SDK does not exist in your system, the **Trim SDK Detected** checkbox is clear by default and an error message appears. Also, the **Finish** button is not enabled. To resolve this error, click **Cancel** and run Install CM_COMComponents_x64.msi from the Content Manager installation media to get the Trim SDK. Rerun the Micro Focus Content Manager server setup.

5. Configure the Web configuration file as follows:

   a. In `C:\Program Files\Kofax\TotalAgility \TotalAgilityTrimCommunicatorService`, open the **Web.config** file in the 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 Integrate Content Manager with TotalAgility.

   c. Edit the <appsettings> as follows:

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

      • Replace the DocumentRecordType with the value taken from the Content Manager server by checking the record type of Document.

      • Replace the FolderRecordType with the value taken from the Content Manager server by checking record type of Folder.

- 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.

> ⊘ When you first install the TotalAgility Micro Focus Content Manager, a TrimIntegrationAppPool with a local system identity is created. This causes an error if the Content Manager server is remote.
>
> To resolve this error, you must update the TrimIntegrationAppPool identity to account with Administrator permission.

Configure the event handler in Content Manager

Configure TotalAgility events for actions in the Content Manager System.

1. Copy the following DLLs.
   - If using Content Manager version below 8, copy the following DLLs to the TRIM binaries directory (usually c:\Program Files\Hewlett-Packard\HP Records Manager.)
     - **Agility.Server.Integration.Trim.dll**
     - **Agility.Server.Integration.Model.dll**
     - **Agility.Server.Integration.Common**
   - If using Content Manager version 8 and above, copy **Agility.Server.Integration.Trim.dll** to the TRIM directory.
2. For Content Manager to fire events in TotalAgility, register the **Agility.Server.Integration.Trim.dll** file using RegAsm (`regasm /codebase Agility.Server.Integration.Trim.dll`).
3. To register the dll:

   a. Open **Content Manager**.

   b. Select **Tools** > **Context Administration** > **External Links**.
   The Content Manager 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** field, enter the ProgId, **Agility.Server.Integration.Trim.TrimIntegrationEventHandler**.

   f. Select **Add-In supports a multi-threaded environment**.

   g. Click **OK**.
   The Content Manager Context External Links window displays the new link.

   h. Select the link and click **Properties**.
   The Record AddIn Properties window appears.

   i. Click the **Used By** tab.

    j. Check the Document and File Folder under Record list and click **OK**.

       This configures the Event handler on Content Manager.

4. In the Explorer, find **trim.exe.config** file, open it in a text editor and add or replace the following tags:

> ⓘ If you cut and paste code from this guide, correct any incorrect line breaks.

```xml
<?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="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>
<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="Windows" />
```

```
</security>
</binding>
</basicHttpBinding>
</bindings>
<client>
<endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://<TotaAgility 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.

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.

KCM Proxy installation on the Web server

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

- **Silent installation**
- **Standard installation**
- **Docker 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 `\\KCMProxyInstallation`.
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 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 at the same location where **Setup.exe** exists.

Standard installation

1. On the installation media, navigate to `\\KCMProxyInstallation` and double-click **Setup.exe**.

   The **KCM Proxy Configuration** window appears.
2. Enter the **KCM Server URL** in the following format: `http(s)://<CCMServer>:<Portnumber>`.

   The Web.config file is automatically updated with the KCM Server IP and the Port number.
3. Click **Configure**.
4. Click **OK**.

Docker installation

While generating the `"dockersetting.env"` file, if the URL is specified in the "KCM Server URL" setting in the Configuration Utility tool, the same URL is used to install KCM Proxy and configure the deployment in the container.

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:

   `\\OnPremiseMultiTenancyInstall\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://<kcmserver>:<port>` with the kcmserver URL.
5. Save and close the configuration file.

Use 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 the previous section for manually updating the KCM Server URL in TotalAgility Web.config.
5. Uncomment the `<rewrite>` section.
6. Save and close the configuration file.

Configure VRS Elite for TotalAgility

Install KofaxVRS and configure the VRS license server. Refer to the *KofaxVRS Elite Installation Guide* for more details.

Kofax VRS Basic or Professional OEM installations

If your scanner includes an OEM version of VRS Basic or Professional, install VRS by running **setup.exe** on the scan station. The VRS software is automatically activated based on the attached scanner model.

Standalone installations

If you purchased a standalone VRS license, install VRS by running **setup.exe** and select **Standalone** as the setup type. When prompted, specify the part number (such as VP-P005-0001), product code, and serial number to activate the software.

> ⓘ VRS remains activated on the workstation unless you manually deactivate it.

Kofax VRS Elite licensing managed by the TotalAgility License Server

Use this configuration to manage VRS licenses through the TotalAgility License Server while also enabling VRS Elite shared profiles and auto profile training data.

This configuration requires installation of the VRS Elite 5.1.2 or higher.

Install VRS Elite Server

1. Run **setup.exe** from the VRS Elite installation media.
2. When prompted, select **Server** as the setup type.
3. Confirm the KTA license server information.

   > ⓘ If the VRS Server does not have a direct connection to the TotalAgility license server, you need to install a license proxy.

4. Complete the steps in the installation wizard.

5. When prompted to activate the license during VRS Elite server installation, click Cancel as you will be using the license proxy instead.

6. Use the generated deployment Kofax VRS.msi to install VRS on the scan stations. Refer to the *Kofax VRS Elite Installation Guide* for details.

Use Kofax VRS Elite with the TotalAgility Scan Client

After you install VRS Elite, KofaxSoftware VRS - TWAIN appears in the list of scanners when you scan a document in TotalAgility. See the *TotalAgility Scan Client help* for more information.

Use the Kofax TotalAgility license for VRS Elite

The Kofax TotalAgility license includes at least one VRS Elite license.

To support tenant licensing for VRS Elite, a new component replaces the VRS Elite license server in TotalAgility environments and communicates with TotalAgility for tenant-specific licensing.

Servers are linked to either Azure or On-Premise tenant deployment. In such cases, the linked server licensing needs to come from Azure.

Shared Licensing for On-Premise Linked Servers

This is the standard on-premise linked server configuration. In this scenario, the license server is deployed at a single site. The other sites share the license server deployed at one of the sites.

Shared Licensing for On-Premise Multi-Tenant Linked Servers

This scenario includes multiple sites to improve performance. The license server is deployed at one of the sites. The other sites share this existing shared license server. TotalAgility user-interactive runtime license requests are optimized.

Tenant Licensing for On-Premise Multi-Tenant with a Linked Server for One Tenant

This scenario includes a tenant using a local instance to improve performance. The license server is deployed at the main location, but the linked server must use the tenant-specific licensing.

Tenant Licensing for SaaS with a Linked Server for One Tenant

The linked server feature can be combined with SaaS deployments. This scenario includes a tenant using a local instance to improve performance.

Install TotalAgility License Proxy

TotalAgility License Proxy enables unconnected Scan Workstations and/or other TotalAgility components to get licensing from the TotalAgility Licence server.

We recommend that you install TotalAgility License Proxy on the machine where VRS Elite server is installed. Otherwise, you will need to run the license utility on each workstation and configure the server to point to the proxy machine.

Do not install the Licence Proxy on the same computer as the Licence server (computer running the 'Kofax License Server' service). The Licence Proxy must run on a separate computer, because it needs to route traffic to the licence server. As part of the License Proxy setup, the installer checks the local computer for the TotalAgility License Server, stops the service and sets the startup type to "Disabled".

You can install the License Proxy manually or when installing TotalAgility.

1. To install manually, on the Installation media, navigate to `\ \TotalAgilityInstall\ Licensing\Installs` and run Kofax`Kofax.Licensing.TotalAgility.Proxy.Installer.msi`TotalAgility. TheKofax TotalAgility License Proxy Setup wizard opens.

2. Click **Next**.

3. In the **End-User License Agreement** window, accept the terms in the License Agreement and click **Next**.

4. In the **Destination Folder** window, select the default path (`C:\Program Files (x86)\Kofax \TotalAgility License Proxy\`) where the Kofax TotalAgility License Proxy will be installed or click **Change** to choose another folder.

5. Click **Next**.

6. In the **Service account setup** window, enter the credentials for the user who will run the TotalAgility License Server service:

   a. In the **Username** field, enter the user name.

   To specify a domain user, enter the user name in the format Domain\User.

   b. Enter and confirm the password.

   > ⓘ This account must have access to the specified TotalAgility URL. These credentials are used for Kofax License Proxy service.

   c. Click **Next**.

7. In the **TotalAgility connection setup** window:

   a. Enter the URL of the License Server where the configuration settings reside.

   Use the following format: `http://<server_name>/TotalAgility/Services/Core/ LicenseServerService.svc` where `<server_name>` is the TotalAgility server name.

   > ⓘ If using SSL, you must have a trusted, valid certificate.

   b. Enter the System Session ID.

   Obtain the Session ID value from the TotalAgility Designer(System Settings>Settings page).

   c. Click **Next**.

   The system downloads the settings.

8. Click **Install** to begin installation.

9. Click **Finish**.

   Once the Kofax TotalAgility License Proxy for VRS Server is installed, you can verify if the proxy is working properly by navigating to `C:\Program Files\Kofax\Imgctls\bin \Application` and running `KSALicenseUtility`. If the proxy is configured properly, the

license information appears in the KofaxLicense Utility user interface; otherwise, an error appears. You may need to reconfigure the System Session ID to match with the TotalAgility Server.

Kofax Web Capture Service installation

Install the Kofax Web Capture Service either at the default location or to a custom location.

Install at the default location

1. When opening a scan-enabled form for the first time, a prompt appears asking you to install the new Web Capture Service. See *Build a Scan Create New Job form in TotalAgility Help*.
2. Click **Run**.
3. Select **Save As** if you want to keep a copy of the msi installer. The msi installer can be used for Enterprise central deployment scenarios.
4. Refresh the page once installation completes.
5. The View and Change Settings icon ⬙ on the Scan Create New Job form becomes available after page refresh.
6. The Kofax Web Capture Service icon ⬚ in the System Tray icons indicates if the service is running.

Install at custom location

For enterprise deployment scenarios where a custom Web Capture service installation location is required, install Web Capture service as follows.

On the Command Prompt, type the following command:

```
msiexec /i Kofax.WebCapture.Installer.msi INSTALLFOLDER=<Installation Folder>
```

Use the Web Capture Service on multiuser environment

You can use the Web Capture Service on multiuser environments, such as MS Terminal Server and Citrix. Multiple users can work with Web Capture Service at the same time from different Windows logon sessions.

Use the Web Capture Service on MS Terminal Server

When using a Terminal Server, users can connect to the scan server simultaneously and perform scanning tasks or import files in parallel. The Web Capture Service Host determines who exactly has

made the request and forwards the request to the appropriate Web Capture Service Worker. The Web Capture Service Worker then works with devices and files that are available to the specific user.

> ℹ The Web Capture Service can only work with scanners attached to a remote Terminal Server; it cannot work with locally connected scanners.

Similarly, for file import, the Web Capture Service provides access to files on a Terminal Server.

Use the Web Capture Service on Citrix

When both the Browser app and Web Capture Service are installed on the Citrix Server, the Web Capture Service physically runs on a remote Citrix server, while a scanner is connected to the client user's computer. This works transparently for Web Capture Service when Citrix TWAIN Redirection is enabled.

> ℹ The number of simultaneously active user sessions for one Citrix Server is limited to 50 sessions.

Install the Web Capture Service as Windows Service

To deploy and upgrade the Web Capture Service installed as Windows Service, you must have Administrator rights.

To install the Web Capture Service as a Windows Service, enable the multiuser support features by using the INSTALLASSERVICE command line option as follows:

```
msiexec /I Kofax.WebCapture.Installer.msi INSTALLASSERVICE=1
```

The MSI installation package is available in the TotalAgility installation folder at:

```
\\TotalAgilityInstall\Agility.Server.Web\Forms\Controls\Capture\external
\webcapture
```

Upgrade the Web Capture Service

To upgrade the Web Capture Service installed as Windows Service, use the same command line parameter that you used for installing the Web Capture Service.

> ℹ You cannot upgrade the Web Capture Service installed as a Windows Service to the standalone version. If you try to do so, the following message appears: This application cannot be installed because you already have Web Capture Service installed as Windows service.

However, you can upgrade from the standalone installation to Windows.

Scan Agent Service installation

The Scan Agent Service is offered through lightweight local agents that can be deployed through an msi file included in the TotalAgility installation media.

You must have sufficient privileges to install system services, otherwise the Scan Agent Service (ScanAgentService) cannot be installed.

Service account to use for Scan Agent Service:

If TotalAgility is configured to use Windows authentication then Active Directory account must be specified that can authenticate within TotalAgility. Otherwise, the LocalSystem account can be used.

As Scan Agent Service needs access to user profile specific folders (to access scanned images) then service account that is used for Scan Agent Service must have access to different user profiles. This means that this account must have administrative privileges. For example, when Scan Agent Service is installed on terminal server and/or different users (scan operators) use the same computer.

If Scan Agent Service is going to be deployed to end user computer then you may not require administrator privileges. For example, if Scan Agent Service is going to upload images only for a particular user then you can install Scan Agent Service under this user account.

Standard installation

1. On the installation media, navigate to `\\ScanAgentService`.
2. Double-click **Kofax.TotalAgility.ScanAgentService.Installer.msi**.
   The Kofax TotalAgility Scan Agent Service Setup wizard starts.
3. Click **Next**.
4. In the **End-user License Agreement** window, select **I accept the terms in the License Agreement**.
5. Click **Next**.
6. In the **Destination Folder** window, either accept the default location where the Scan Agent Service must be installed, or click **Change** to choose another folder.
7. Click **Next**.
8. In the **Service account setup** window, specify the logon account (Windows account) for the Kofax TotalAgility Scan Agent service.
9. Click **Next**.
10. Click **Install** to begin installation.
    Once installed, a local service, "Kofax TotalAgility Scan Agent Service", is created on the workstation. A companion "Scan Agent Monitor" is available, which can be used to monitor job upload status.

Scanning with Scan Agent Service

The status bar of the Scan Create New Job form indicates if the session is connected to Scan Agent Service.

The Scan create new job form offloads actual upload of images to Scan Agent Service. However if image enhancement is enabled, the Scan create new job form performs image processing in a regular way.

Once image processing operation (if any) is done, the "Create Job" button becomes available, even if images have not been completely uploaded to the server. When you click "Create Job", the job appears in the Scan Agent Monitor.

The Scan Agent Monitor can be used to monitor job upload status. The job upload statuses include:

- **Pending**: Job is being prepared for upload.
- **In Progress**: Job is currently being uploaded.
- **Finished**: Job has successfully being uploaded.
- **Error**: Job encountered an error and has been stopped.
- **Paused**: Job has been paused.

Depending on the job status, the following actions are available.

- **Abort**: Aborts and cancels the corresponding job, and prompts you for a TotalAgility user account to cancel the job with.

  > ⓘ This action uses a separate TotalAgility user session; if "Allow Multiple Logon" is not enabled, the abort action ends any other session using the same user account.

- **Pause**: Pauses the upload session for the job. You must explicitly resume a paused job.
- **Retry**: Queues uploading job again if the job encounters an error. This action helps in recovering from an upload error.
- **Resume**: Resumes a paused job.
- **Clear Completed**: Removes all uploaded complete jobs from the list.

Uninstall TotalAgility

Uninstalling TotalAgility only removes the application and not the database.

Use the installation wizard

1. Click **Start > All Programs >TotalAgility** and select **Uninstall or Repair TotalAgility**.
   The **Repair/Uninstall** window opens.
2. Select **Uninstall** and click **Next**.
3. Follow the prompts until you are informed that the product is uninstalled, and then click **Finish**.

   The summary report lists the components, servers, applications and services uninstalled.

   Ensure that no error log is created. If any errors occur, by default, a log file **KofaxTotalAgilityInstallErrorLog.log** is created at the same location where setup.exe exists if the path in the System diagnoatics is not defined. However, you can define the path for the log file by specifying the path in the <add name="KTALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>" />. Fix those errors and repeat the above steps.

Use the silent mode

1. On the Command Prompt, change the command line to the root directory of the Setup.exe file.
2. Run `Setup.exe /Silent /U`.

   The system uninstalls TotalAgility and automatically creates a log file at the same location where setup.exe exists. This log file contains information on errors, if any. The removal of the product is indicated in the event log.

   > ⓘ Uninstalling TotalAgility in silent mode not only removes the applied fix pack or service pack but also removes the TotalAgility application completely. To reinstall TotalAgility, you must install its base version and then apply any patches.

Upgrade TotalAgility On-Premise Multi-Tenancy

Upgrade TotalAgility On-Premise Multi-Tenancy from 7.4.0 (or any interim patches), 7.5.0 (or any interim patches), 7.6.0 (or any interim patches), 7.7.0 (or any interim patches), 7.8.0 (or any interim patches) or 7.9.0 (or any interim patches) to 7.10.0. Tenants must be updated through the Tenant Management system.

When upgrading TotalAgility On-Premise Multi-tenancy from previous versions to 7.10.0, the capture data migration is performed when upgrading a tenant. See Capture data migration.

You can upgrade TotalAgility components and databases independent of each other or upgrade TotalAgility components including databases. You can also upgrade databases manually using database scripts. See Upgrade process.

You can choose to upgrade TotalAgility using the non-zero downtime upgrade process, which involves application being down for a while or upgrade using zero down time, where you can upgrade by introducing a new version of your application to production during the upgrade process, and the application is never completely down or in an unstable state until all tenants are upgraded.

ⓘ Before upgrading TotalAgility, ensure TotalAgility App Pool and all the TotalAgility Services are stopped, and the databases are backed up. Once upgrade is complete, you must start the TotalAgility Services.

Upon upgrading, TotalAgility installer restores the following configuration settings:
* All existing AppSettings
* All existing Security Bindings
* All HTTP URL Rewrites to be done for TotalAgility

ⓘ After upgrading TotalAgility from versions prior to 7.7.0, you must reconfigure the license server by updating the settings to use the new licensing behavior. See Update the settings for a license server.

You can upgrade TotalAgility on-premise multi-tenancy in a silent mode.

Upgrade to Windows authentication

When upgrading TotalAgility On-Premise Multi-tenancy, you can choose to switch from SQL Authentication to Windows Authentication to connect tenant databases. The upgrade will not

automatically create the separate tenants database; the databases must be created manually by the database administrator using SQL Server management tools.

The databases created should be in the following format

- TotalAgility_Main_Live_TenantName
- TotalAgility_Reporting_Live_TenantName
- TotalAgility_Reporting_Staging_Live_TenantName
- TotalAgility_Documents _Live_TenantName

Before changing the mode of authentication from SQL authentication to Windows, do the following:

1. Create the tables for Main, Reporting, Reporting Staging and Documents databases.

2. Copy all the data from live and reporting live databases to the newly created databases to work with the tenant.

3. Open the CEBPM_Settings.xml from the SERVER_DATA table and update the RepositoryDBConnectionString for DataLayerConfiguration.

```
<Common_Settings>
    <ReportingSettings />
    <DataLayerConfiguration RepositoryDBConnectionString=";Data
 Source=<MachineName>;Initial Catalog=TotalAgility_Documents;User
 ID=;Password=;Integrated Security=True;Connect
 Timeout=30;Encrypt=False;TrustServerCertificate=False"
 RepositoryBlobStorageAccountConnectionString="{DATA_LAYER_BLOB_CONNSTRING}"
 RepositoryBlobStorageContainerName="{DATA_LAYER_BLOB_CONTAINER}"
 RepositoryBlobStorageEncryptionKey="{DATA_LAYER_BLOB_ENCRYPTION_KEY}" />
  </Common_Settings>
```

Capture data migration

In on-premise multi-tenancy, when upgrading from TotalAgility 7.7.0 or previous versions to 7.8.0 and higher, the capture data migration process is performed during the tenant upgrade process. The migration process of each tenant database is done from the Tenant Management System.

The migration process can migrate only consistent data. If for some reason (due to custom scripts or TotalAgility failures) some folders in database are in not in a consistent state, these folders cannot be migrated and appear as broken folders. If any broken root folders are found during tenant's upgrade, a "Complete with Warnings" is displayed for that tenant's status. You can review the warnings and associated broken root folder IDs. You can acknowledge each tenant individually, or acknowledge all tenants at once. Acknowledging a tenant in this case will mark the tenant's upgrade as complete. For more information on capture data migration, see Upgrading a tenant in the *Help for Tenant Management System*

We recommend that you leave enough free memory on the SQL server for better migration performance. See the following recommendations for faster capture data migration:

- It is highly recommended to have at least 4-6Gb of free memory available before migration is running.
- Make sure that no CPU consuming processes are running on machine where migration is running.
- If possible, run migration on machine where SQL Server is running.

- If you run migration on SQL Server's machine, make sure that 'Maximum Server Memory' option is reduced to have 50% or more free memory on the machine (database server restart may be needed to free up memory). This can significantly reduce the migration time.
- It is highly recommended to store SQL Server data files on SSD (solid-state drive) disks.

Capture binary data storage

By default, the capture data is stored in the SQL Server. You can use the preconfigured external data storage services such as Amazon S3, Windows Azure Blob Storage or SQL Server and File System for saving and processing the capture data. When upgrading TotalAgility On-Premise Multi-Tenancy to 7.10.0, the existing SQL Server binary data is not moved to the new storage. Post upgrade, you can change the storage type to Amazon S3, Windows Azure Blob Storage or SQL Server and File System from the **Capture Storage** tab by running the Configuration Utility. See the *Kofax TotalAgility Configuration Utility Guide*.

Upgrade TotalAgility in silent mode

See Upgrade TotalAgility in silent mode.

Upgrade process

You can choose to upgrade TotalAgility components and databases independent of each other or upgrade TotalAgility components including databases.

1. Navigate to TotalAgility Installation media and install a base version of TotalAgility on-premise multi-tenancy.
2. Launch Tenant Management System and create at least one tenant.
3. Navigate to TotalAgility 7.10.0 Installation media and double-click **Setup.exe**.
   The User Account control window opens.
4. In the **TotalAgility MultiTenancy Upgrade** window, you can do the following:
   - Upgrade TotalAgility components
   - Upgrade TotalAgility databases
   - Upgrade TotalAgility components including databases

   If any errors occur during upgrade, by default, TotalAgility creates a log file (Kofax TotalAgilityMultitenancyInstallErrorLog) at the following path on the TotalAgility installation media: `\\OnPremiseMultiTenancyInstall\Kofax TotalAgilityMultitenancyInstallErrorLog`. The log file is also created on the desktop. Fix the errors.
5. Launch the Tenant Management System.
   The tenants created in the base version of TotalAgility are displayed. You can upgrade the tenants to work in the upgraded version of TotalAgility or create new tenants in the upgraded

version. For more information, see Upgrading a tenant in the *Help for Tenant Management System*.

Upgrade TotalAgility components

To upgrade TotalAgility components such as License Proxy, Transformation Designer and Transformation Server, perform the following steps.

1. In the **Kofax TotalAgility MultiTenancy Upgrade** window, select **TotalAgility components**.
2. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**. (Default: Clear)
3. By default, the services are automatically started. To start services manually, clear the check box for **Automatically start services** and click **Next**.
   The **Credentials** window opens.
4. Enter the credentials (password and confirm password) and click **Next**.
   The Installation Progress window opens. The setup installs the required components.
5. Click **Finish** to complete the installation.

   If any errors occur during upgrade, by default, TotalAgility creates a log file (KofaxTotalAgilityMultitenancyInstallErrorLog) at the following path on the TotalAgility installation media: `\\OnPremiseMultiTenancyInstall\Kofax TotalAgility MultitenancyInstallErrorLog`. The log file is also created on the desktop. Fix the errors.

   After upgrading TotalAgility components, if you also want to upgrade Kofax TotalAgility databases, do the following:

   a. Navigate to TotalAgility Installation media and double-click **Setup.exe**.

      The Repair/Uninstall/Upgrade Databases window opens.

      > ⓘ Alternatively, you can select the Upgrade Databases option from the Repair/Uninstall/Upgrade Databases window by clicking Start > All Programs > Kofax TotalAgility and select Uninstall or Repair Kofax TotalAgility.

   b. Select **Upgrade Databases**.

   c. Click **Next** and follow the instructions.

Upgrade TotalAgility databases

Follow the steps to upgrade only TotalAgility databases.

1. In the Kofax TotalAgility MultiTenancy Upgrade window, select **TotalAgility databases**.
2. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**.
3. By default, the services are automatically started. To start services manually, clear the check box for **Automatically start services** and click **Next**.

   When upgrading TotalAgility from version lower than 7.8.0 to 7.9.0, clicking **Next** will display a pop-up message recommending to check for latest updates to perform capture data migration.

   The Credentials window opens.

4. Enter the credentials (password and confirm password) and click **Next**.

    The Installation Progress window opens. The setup installs the databases.

5. Click **Finish** to complete the installation.

    If any errors occur during upgrade, by default, TotalAgility creates a log file (KofaxTotalAgilityMultitenancyInstallErrorLog) at the following path on the TotalAgility installation media: `\\\OnPremiseMultiTenancyInstall\Kofax TotalAgilityMultitenancyInstallErrorLog`. The log file is also created on the desktop. Fix the errors.

Upgrade TotalAgility components including databases

Follow the steps to upgrade TotalAgility components including databases.

1. Navigate to TotalAgility Installation media and double-click **Setup.exe**.

    The User Account control window opens.

2. Click **Next**.

3. In the Kofax TotalAgility MultiTenancy Upgrade window, select TotalAgility components including databases.

4. If Tenant Management system, Development environment and Live environment are installed independent of each other, to upgrade Development environment and Live environment, provide MasterTenants database name in the **Master** field.

5. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**.

6. By default, the services are automatically started. To start services manually, clear the check box for **Automatically start services** and click **Next**.

    When upgrading TotalAgility from version lower than 7.8.0 to 7.9.0, clicking **Next** will display a pop-up message recommending to check for latest updates to perform capture data migration.

    The Credentials window opens.

7. Click **Next**.

    The Credentials window opens.

8. Enter the credentials (password and confirm password) and click **Next**.

    The **Installation Progress** window opens. The setup installs the required components and databases.

9. Click **Finish** to complete the installation.

    If any errors occur during upgrade, by default, TotalAgility creates a log file (KofaxTotalAgilityMultitenancyInstallErrorLog) at the following path on the TotalAgility installation media: `\\\OnPremiseMultiTenancyInstall \KofaxTotalAgilityMultitenancyInstallErrorLog`. The log file is also created on the desktop. Fix the errors.

Check for latest updates to perform capture data migration

When upgrading TotalAgility databases and TotalAgility components including databases from version lower than 7.8.0 to 7.9.0, perform the following steps.

1. In the **Kofax TotalAgility Upgrade** window, select **TotalAgility databases**.

2. By default, the services are automatically started. To start services manually, clear the check box for **Automatically start services**.

3. To import the Workspace package, select the check box for **Import system Workspace Package** and click **Next**.

   A pop-up message appears recommending to check for latest updates to perform capture data migration.

4. Click **Yes**.

   The **Installation Review** dialog box displays the following link for downloading the precheck updates for capture data migration.

   https://edelivery.kofax.com/TotalAgility/7.9.0/MigrationPreCheck.ZIP

5. Click the link to automatically download the MigrationPreCheck.zip to your local machine.

6. Click **Finish** in the **Installation Review** dialog box.

7. Run the utility, `Agility.Install.ApplyCaptureMigrationUpdates.exe` located at the installation directory to replace the DLLs and script files.

   The **Capture Migration** pop-up appears.

8. Click **Browse** and select the **Zip file location** where the MigrationPreCheck.zip is downloaded and click **OK**.

   The Capture Migration Updates Tool automatically extracts the zip and applies the updates into TotalAgility installer.

9. Click **OK** in the message.

10. Navigate to TotalAgility 7.10.0 Installation media and double-click **Setup.exe** to run the installation again

11. Click **No** when prompted to check for the updates to perform capture data migration..

    The **Credentials** window opens.

12. Enter the credentials and continue with the upgrade.

    If any errors occur during upgrade, by default, TotalAgility creates a log file (KofaxTotalAgilityInstallErrorLog) at the following path on the TotalAgility installation media: `\ \TotalAgilityInstall\KoaxTotalAgilityInstallErrorLog`. The log file is also created on the desktop. Fix the errors.

Zero downtime upgrade

In the non-zero downtime upgrade process, you must close the current running application for all the tenants, install new version and upgrade all the tenant databases and start the new version of the application after all the tenants are upgraded. This involves application being down for a while. With zero down time upgrade, you can upgrade TotalAgility by introducing a new version of your application to production during the upgrade process, the application is never completely down or in an unstable state and the system need not be down until all tenants to be upgraded.

Prerequisites to consider before a zero downtime upgrade:

1. The zero downtime upgrade of TotalAgility is only supported for upgrades from a last released version which has a database change. For example, TotalAgility 7.9.0 will only support upgrade from TotalAgility 7.8.0 as TotalAgility 7.8.0 is the last released version which has a Database change. Upgrade from version 7.7 or earlier is not supported.

2. The upgrade of tenants should be done using the Zero Down Time upgrade utility and not via Tenant Management System as this avoids the need to install newer version of TotalAgility on extra servers to facilitate upgrade.

3. The TotalAgility Designer is disabled for all tenants to prevent usage of new TotalAgility features during upgrade of TotalAgility servers to next version. This is needed while there are still TotalAgility servers running using the previous version.

4. In case of any issues, you will only be able to rollback to the pre-upgrade backup, that is, backup of the tenant databases will be done before upgrade starts and as the tenant system will still be running during the upgrade, up until the tenant is deactivated for upgrade.

Upgrade process

The TotalAgility on-premise multi-tenancy system will always be available during upgrade, but individual tenants will be deactivated while their data is being upgraded. This is due to performance concern of upgrading tenant data while the tenant is still active.

1. On the installation media of TotalAgility, navigate to `TotalAgility\Utilities\OPMTDBUpgrader`.

2. Open the `OPMTDBUpgrader` folder and run `Kofax.TotalAgility.Install.OPMTDBUpgrader.exe` as an administrator. The upgrader will connect to the default Datacenter database using the connection details from the Application server configuration files.

   ❶ You must run the upgrade utility on the Application server.

   The Kofax TotalAgility Multi Tenancy Tenant Upgrader window opens.

3. Click **Next** to continue with the setup.
   The **Databases** window opens.

4. Specify the MasterTenants database connection string along with the Datacenter database connection string to upgrade and click **Next** and then click **Yes** to confirm.
   These connection strings are used to pre upgrade the Master/datacenter tables.

5. The **Upgrade Tenants** window displays the list of tenants.

   a. Select the environment to upgrade as **Development**, **Production** or **Both**.

   b. Select single tenant, multiple tenants or all tenants to upgrade and click **Pre Upgrade**.
      All the selected tenants will be upgraded to the latest version. Each of the selected tenant will be deactivated during this data upgrade. Designer access to the tenants being upgraded will also be deactivated.

      ❶ If any tenant is not using a version of TotalAgility that supports zero down time upgrade, an error is displayed. For example, TotalAgility 7.9 will only support zero down time upgrade from TotalAgility 7.8.0.

6. Upgrade all the on-premise multi-tenant TotalAgility deployment servers to the latest version via the installer.

   ❶ You can only start upgrading on-premise multi-tenant deployments to latest version after all the tenant databases are pre upgraded.

7. Similarly, upgrade the Tenant Management System deployments to the latest version via the Tenant Management System installer. Once the Tenant Management System and datacenter databases are upgraded to latest version, the databases are now backward compatible. See the *Tenant Management help* for more information.

8. Make sure the tenants are working fine and activate TotalAgility Designer access to any one tenant via the Tenant Management System tenant update screen and perform all tests.

9. Open the OPMTDBUpgrader utility and go to the **Upgrade Tenants** window. For all the selected tenant databases, run the Post Upgrade DB scripts by clicking the **Post Upgrade** option to cleanup old data. This will also execute the post scripts for master and datacenter tables and also activates the Designer access for these tenants. Each tenant will be deactivated during this data upgrade.
All the tenants are now upgraded to the latest version.

Upgrade TotalAgility databases manually using database scripts

To run scripts manually, do the following:

ℹ On upgrading TotalAgility to 7.10.0, the connections to the Simulator database are removed.

1. Go to `\OnPremiseMultiTenancyInstall\DatabaseScripts\SQL Server\Upgrade Database Scripts`.

2. Run the conversion scripts (if exist) for all releases and patches starting from the version upgrading from to the version being upgraded to.
Example: If upgrading from 7.2.0.0 to 7.9.0, run the following conversion scripts.
   - 7.2.0.0 to 7.2.1.0 Conversion Scripts
   - 7.2.1.0 to 7.2.2.1 Conversion Scripts
   - 7.2.2.1 to 7.3.0.0 Conversion Scripts
   - 7.3.0.0 to 7.3.0.2 Conversion Scripts
   - 7.3.0.2 to 7.3.1.0 Conversion Scripts
   - 7.3.1.0 to 7.3.1.2 Conversion Scripts
   - 7.3.1.2 to 7.4.0.0 Conversion Scripts
   - 7.4.0.0 to 7.4.0.1 Conversion Scripts
   - 7.4.0.1 to 7.4.1.0 Conversion Scripts
   - 7.4.1.0 to 7.4.1.1 Conversion Scripts
   - 7.4.1.1 to 7.5.0.0 Conversion Scripts
   - 7.5.0.0 to 7.5.0.5 Conversion Scripts
   - 7.5.0.5 to 7.5.0.10 Conversion Scripts
   - 7.5.0.10 to 7.6.0.0 Conversion Scripts
   - 7.6.0.0 to 7.7.0.0 Conversion Scripts
   - 7.7.0.0 to 7.8.0.0 Conversion Scripts
   - 7.8.0.0 to 7.9.0.0 Conversion Scripts

3. Navigate to `\\TotalAgility\Agility.Server.Web\bin>` and open
   Agility.Installation.Server.Upgrade.exe.config. In the <appSettings> section, update the
   value for the following settings.
   - `<add key="UserName" value="" />` where the user name is the currently logged on
     user's name.
   - `<add key="TenantDBConnectionString"value="Server=(local);Trusted_Connec`
     `tion=Yes;Database=DataCenterTenants;" />`
   - `<add key="MasterTenantDBConnectionString"value="Server=(local);Truste`
     `d_Connection=Yes;Database=<MasterTenants database>;" />`

     Point the connection strings to where the databases are installed.
4. From the command prompt, run `Agility.Installation.Server.Upgrade.exe`
   by passing the parameters, "UpgradeMasterTenants" and "UpgradeDataCenter", such
   as `Agility.Installation.Server.Upgrade.exe "UpgradeMasterTenants"`
   and Agility.Installation.Server.Upgrade.exe "UpgradeDataCenter".
5. Ensure that no error log is created. If any errors occur, a log file called
   KofaxUpgradeDatabaseUtilityError.txt is created on your desktop. Fix those errors and
   repeat the above steps.
6. Start the Kofax TotalAgility Core Worker service manually:

   a. At Run, type **Services.msc** and press **Enter**.

   b. Right-click **Kofax TotalAgility Core Worker** and click **Start**.

Reset passwords

When upgrading TotalAgility On-Premise Multi-tenancy, all passwords are set to **password** and
encrypted using the new hashing algorithm.

On creating a new dev environment for a tenant:
- If the live instance has Scrypt as its hashing algorithm, the dev instance will have the same
  password as the live instance.
- If the live instance has SHA1 as its hashing algorithm, the dev instance will have the default
  password as password.

By default, any new (live or Dev) instance will have Scrypt as its hashing algorithm.

Upgrade TotalAgility in silent mode

Before upgrading TotalAgility from version 7.7.0 to 7.9.0 (any upgrade which includes databases,
and components including databases) in silent mode, you must click the following link for
downloading the precheck updates for capture data migration.

`https://edelivery.kofax.com/TotalAgility/7.9.0/MigrationPrecheck.ZIP`

After downloading the zip, run the utility Agility.Install.ApplyCaptureMigrationUpdates.exe which is
located at the installation directory to replace the DLLs and scripts.

For a silent upgrade of TotalAgility to version 7.10.0, do the following.

1. Go to the root directory of setup.exe.
2. Navigate to `\\OnPremiseMultiTenancyInstall` and open SilentInstallConfig.xml using a text editor.
3. In SilentInstallConfig.xml, update the following parameters.

Parameter	Default value	Description
IsDatabaseWindowsAuthentication	false	Set to true to use Windows authentication to connect to SQL Server.
MasterTenants	MasterTenants	If Tenant Management system, Development environment and Live environment are installed independent of each other, to upgrade Development environment and Live environment, provide MasterTenants database name.
Identity Information		
UserName	username	Enter the name of the user who will run TotalAgility.
Password	password	Enter the password for the user who will run TotalAgility.
Install Info		
InstallAction	MultiTenancyUpgrade	Use this setting to upgrade Multi-Tenant components including tenant databases.
	upgrademultitenant databases	Use this setting only if you are upgrading the databases before upgrading TotalAgility components. ⓘ If you upgrade TotalAgility components and then upgrade databases, you must do the following: a. Open SilentInstallConfig.xml available at the following location: \\TotalAgility Installation Information\Kofax TotalAgility b. Update the \<InstallAction> section with the following parameter: \<InstallAction> =Upgradedatabasesforexistingmultitenancy c. Run Setup.exe /Silent /U from the above mentioned path.
	upgrademultitenant components	Use this setting to upgrade only TotalAgility components.
TransformationService	true	Set to true to install the Transformation Server.

Parameter	Default value	Description
Transformation Server Info		
LogFile	no default	Set the location where the Transformation Server log file will be created. You can also keep the default.
WindowsServiceAccount	no default	Enter the name of the user who will run Transformation Server.
WindowsServicePassword	no default	Enter the password for the user.
StartServices	true	To start the services manually after the upgrade installation, set the StartServices parameter to false.

4. Open the Command Prompt window as an Administrator, change the command line to the root directory of the Setup.exe file.
5. Run `Setup.exe /Silent /Upgrade`.
   The following items are upgraded automatically:
   - Kofax TotalAgility
   - Kofax Import Connector (KIC)
   - Kofax Transformation Designer
   - Utility for Kofax Export Connector

   The system generates a log file which reports errors (if any).
   The success or failure of installation is indicated in the event log.
6. Save and close the file.

Troubleshooting

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

Installation failure in IPv6 environment

If SQL server is configured to listen only on IPv6 addresses on a dual-stack (IPV46), client connection attempts using IPv4 addresses will fail. These failures may take longer than the default TCP timeout established during connection handshakes. Even though the subsequent IPv6 connection may succeed immediately, the connection may still fail.

To resolve this issue, disable IPv4 in the SQL Server Configuration Manager.

1. Start **SQL Server Configuration Manager**.
2. Open the Properties for the TAServerInstance TCP/IP protocol.
3. Set **Listen All** to **No**.

   ⓘ This setting allows fine control over which interfaces the TAServerSQLInstance will listen for connections.

4. Click the **IP Address** tab.
5. Set **Enabled** to **No** for all entries except for ::1 which is the IPv6 local host address.
6. Click **OK** to commit changes and click **OK** at the service restart dialog box.
7. Restart the SQL Server (<TAServerInstance>) service where TAServerInstance is the actual instance used by TotalAgility. Example: Kofax TotalAgility.

TotalAgilityAppPool exists

TotalAgility Tenant Management creates an application pool called TotalAgilityAppPool. If an application pool with the same name exists, it is deleted and a new one is created.

String argument is empty error

When you update the Web.config settings manually, apply the same settings in the streaming service configuration file before you restart the streaming server service. Otherwise the following error occurs:

```
String argument is empty Parameter name: cacheName.
```

For example, if deployment type value is updated to Live in the Web.config file, and the deployment type value is Dev in the streaming service configuration file, the error occurs.

Exception during Transformation Designer project import

An exception is generated while importing projects using Transformation Designer that is connected to a TotalAgility web service that uses SSL.

1. If you run your server using SSL, set the **Client certificates** option to **Ignore** under SSL Settings.

2. To use Client certificates for authentication (Accept or Require), set the value for uploadReadAheadSize in IIS in one of the following ways:

   • In the IIS Manager:

     a. Open the Configuration Editor of the TotalAgility site.

     b. In the Section list, expand **system.webServer** and select **serverRuntime**.

     c. In the From list, select **ApplicationHost.config <location path='Default Web Site/ Totalgility'/>**.

     d. Set an appropriate value in bytes for **uploadReadAheadSize**.

Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site/TotalAgility	
alternateHostName	
appConcurrentRequestLimit	5000
authenticatedUserOverride	UseAuthenticatedUser
enabled	True
enableNagling	False
frequentHitThreshold	2
frequentHitTimePeriod	00:00:10
maxRequestEntityAllowed	4294967295
uploadReadAheadSize	83886080

   • Modify the IIS main configuration file:

     a. Open the **applicationHost.config** file located in the `C:\Windows\System32\inetsrv\config\` directory.

     b. If the <serverRuntime> node does not exist, add the node below the <security> node in the <system.webServer> section.

```
<location path="Default Web Site">
    <system.webServer>
        <security>
…
        </security>
        <serverRuntime uploadReadAheadSize="10485760" />
    </system.webServer>
</location>
```

     c. Set an appropriate value in bytes for **uploadReadAheadSize**.