



Tungsten TotalAgility

On-Premise Multi-Tenant Installation

Guide

Version: 8.1.0

Date: 2024-10-01

TUNGSTEN
AUTOMATION

© 2024 Tungsten Automation. All rights reserved.

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

Table of Contents

Preface.....	9
TotalAgility documentation.....	9
Full documentation set.....	9
Offline documentation.....	13
Training.....	16
Getting help with Tungsten Automation products.....	16
Chapter 1: Installation planning.....	17
System requirements.....	17
Prerequisites.....	17
SQL Server.....	17
Transformation Server.....	18
Tungsten TotalAgility Document converter.....	18
Reporting Server.....	18
Microsoft Dynamics CRM.....	18
Microsoft Dynamics 365 CRM.....	18
Tungsten Message Connector.....	18
Tungsten SignDoc.....	19
Tungsten VRS Elite.....	19
TCM Proxy.....	19
Tungsten TotalAgility Repository Browser.....	20
Tungsten Web Capture Service.....	20
Tungsten TotalAgility Scan Agent Service.....	20
Licensing.....	21
Concurrent user licenses.....	21
Reserved licenses.....	21
Activate a license in TotalAgility.....	21
Automatic recovery.....	22
Set up a non-administrator service account for Tungsten License Server service.....	22
Tungsten VRS Elite licenses.....	24
TotalAgility License Proxy.....	24
Use the Tungsten TotalAgility license for Tungsten VRS Elite.....	24
Utilities.....	25
Installation types.....	25
Database only.....	26
Upgrade databases.....	26

Web Server.....	26
Application Server.....	26
Web and Application Server.....	26
Real Time Transformation Service.....	26
Manual installation of databases.....	26
Capture binary data storage.....	28
Post-installation configurations.....	28
Chapter 2: TotalAgility On-Premise Multi-Tenancy installation.....	29
Silent installation of TotalAgility On-Premise Multi-Tenancy.....	29
Silent installation of database only.....	29
Silent installation for upgrading databases.....	31
Silent installation of Web and Application on the same server.....	33
Silent installation of Web and Application on different servers.....	40
Silent installation of Real Time Transformation Server.....	44
Standard installation of TotalAgility On-Premise Multi-Tenancy.....	50
Standard installation of Database Only.....	50
Standard installation for upgrading databases.....	52
Standard installation of Web and Application on the different servers.....	53
Standard installation of the Web and Application on the same server.....	59
Standard installation of Real Time Transformation Server (RTTS).....	64
Use Integration Server with on-premise multi-tenant server deployment.....	66
Language pack installation.....	66
Install the .NET Framework language packs.....	67
Chapter 3: TotalAgility installation in a Docker container.....	68
Overview.....	68
Limitations.....	68
Prerequisites.....	68
Install Docker on the Windows server.....	69
Use Image Quality Analysis, Mobile ID, and Mobile Card Capture on Docker.....	70
Create a TotalAgility Docker container image.....	71
Perform silent installation of TotalAgility in a Docker container.....	72
Demo server in a Docker container.....	72
Application Server (Core Services and Core Worker) in a Docker container.....	74
Web Server in a Docker container.....	76
Web Server and Application Server (Core Services and Core Worker) in a Docker container.....	76
Reporting Server in a Docker container.....	78
License Server in a Docker container.....	78

Transformation Server in a Docker container.....	79
Real Time Transformation Service in a Docker container.....	81
Run a Docker container.....	82
Access TotalAgility Tenant Management System.....	84
Access Message Connector.....	84
Useful Docker commands.....	85
Use secrets.....	86
Use Kubernetes secrets.....	86
Use Docker secrets.....	87
Use AWS secrets.....	88
Import SSL certificate on the container.....	92
Use Windows authentication with IIS and SQL server.....	93
Use Windows authentication with IIS and SQL Server.....	93
Chapter 4: Transformation Server bundle installation.....	97
Prerequisites.....	97
User Accounts for Transformation Server.....	98
Configure the user account.....	98
Silent installation of Transformation Server.....	99
TS_SETUP_CONFIG_FILE sample.....	99
Standard installation of Transformation Server.....	100
Encrypt and decrypt the configuration file.....	102
Use TotalAgility.EncryptConfig.exe.....	103
Decrypt the configuration file.....	105
Edit the configuration file.....	105
Install the NLP language packs manually.....	106
Upgrade Transformation Server using silent installation.....	106
Uninstall the Transformation Server.....	107
Chapter 5: Message Connector installation.....	108
Prerequisites.....	108
Deployment scenarios and advanced configuration.....	108
System limits.....	108
Install multiple instances of Message Connectors.....	108
Upgrade Message Connector instances.....	110
Chapter 6: Reporting Server installation.....	111
Prerequisites.....	111
Silent installation of the Reporting Server.....	111
Standard installation of the Reporting Server.....	113
Uninstall the Reporting Server.....	114

Chapter 7: TCM Proxy installation.....	115
Prerequisites.....	115
Silent installation of TCM Proxy.....	115
Standard installation of TCM Proxy.....	115
Docker installation of TCM Proxy.....	116
Update the TCM Server URL.....	116
Manually update the TCM Server URL.....	116
Use the Configuration Utility.....	117
Install TCM Proxy manually.....	117
Chapter 8: Tungsten VRS Elite Installation.....	118
VRS Elite Basic or Professional OEM installations.....	118
Install VRS Elite.....	118
Use VRS Elite with the TotalAgility Scan Client.....	119
Chapter 9: TotalAgility License Proxy installation.....	120
Prerequisites.....	120
Silent installation of License Proxy.....	120
Standard installation of License proxy.....	121
Chapter 10: Tungsten Web Capture Service installation.....	123
Install the Web Capture Service at the default location.....	123
Install the Web Capture Service at a custom location.....	123
Install the Web Capture Service as Windows Service.....	123
Use the Web Capture Service in a multiuser environment.....	124
Use the Web Capture Service on MS Terminal Server.....	124
Use the Web Capture Service on Citrix.....	124
Upgrade the Web Capture Service.....	124
Chapter 11: Tungsten TotalAgility Scan Agent Service installation.....	125
Prerequisites.....	125
Service account to use for Scan Agent Service.....	125
Standard installation of Scan Agent Service.....	125
Scanning with Scan Agent Service.....	126
Chapter 12: TotalAgility and Tungsten SignDoc integration.....	127
Set up the Tungsten SignDoc server.....	127
Chapter 13: TotalAgility and Microsoft Dynamics CRM integration.....	128
Prerequisites.....	128
Standard installation of Dynamics CRM.....	128
Update Web.config to support event handlers.....	128
Update Web.config for the CRM virtual directory.....	130
Update Web.config for Dynamics CRM.....	131

Update Web.config to support event handlers.....	131
Update Web.config for the CRM virtual directory.....	133
Chapter 14: TotalAgility configuration.....	134
Configure HTTPS communication.....	134
Create a single SSL certificate using a split Web-Application and Tenant Management system.....	134
Update Web.config.....	135
Import an SSL certificate.....	135
Configure TotalAgility for high availability.....	135
Generate a common machine key if using Federated Security.....	136
Encrypt and decrypt the configuration files.....	136
List of configuration files.....	137
Encrypt and decrypt web.config.....	138
Encrypt and decrypt the configuration files of executables.....	138
Encrypt the configuration files in a Docker container.....	141
Edit a configuration file.....	142
Edit the TotalAgility configuration settings.....	143
Configure the settings to record system tasks history.....	143
Configure the settings for system tasks threadpool size.....	144
Add custom job thread pools.....	144
Add a thread pool monitoring interval.....	145
Update the settings for a License Server.....	146
Update the settings for Anti-Cross Site Request Forgery (CSRF) measures.....	147
Edit the configuration files for safe scripting.....	148
Update settings for forcing HTTPS access with HSTS.....	149
Update the settings to enable consolidated logging.....	152
Secure cookies.....	155
Add performance monitoring counters.....	155
Exclude folders and files from the antivirus scan.....	156
Chapter 15: Log on to TotalAgility On-Premise Multi-Tenancy.....	159
Chapter 16: Uninstall TotalAgility.....	160
Use the silent mode.....	160
Use the installation wizard.....	160
Chapter 17: Upgrade TotalAgility On-Premise Multi-Tenant.....	161
Upgrade deployment servers.....	161
Silent upgrade process.....	162
Interactive upgrade process.....	164
Standard upgrade process.....	164

Use the Zero downtime upgrade process.....	165
Switch from SQL authentication to Windows authentication.....	167
Change Capture binary data storage.....	168
Chapter 18: Troubleshooting.....	169
TotalAgilityAppPool exists.....	169
Error on Linked servers page in TotalAgility Designer.....	169
Installation failure in IPv4 and IPv6 environment.....	169
Exception during Transformation Designer project import.....	170
Appendix A: Generic terms.....	172
Tungsten TotalAgility Core Worker service.....	172
Tungsten TotalAgility Reporting service.....	172
Tungsten License Server service.....	172
Tungsten TotalAgility Export Worker service.....	172
Tungsten Transformation Server service.....	172
Import Service.....	173
Tungsten TotalAgility Streaming Service.....	173
Capture Binary Data Storage.....	173
FILESTREAM.....	173
TungstenTotalAgilityInstallErrorLog.log.....	174
ETL.....	174
L2S.....	174
Staging database.....	174
wsa_messages table.....	174
wsa_message.....	174
Kofax.CEBPM.Reporting.AzureETL.exe.....	175
ETL iteration.....	175
Warehouse database.....	175
Completed batch session.....	175
TotalAgility.EncryptConfig.exe.....	175

Preface

This guide provides the instructions for installing Tungsten TotalAgility On-Premise Multi-Tenant 8.1.0.

Read this guide completely before installing the software.

Use the Tungsten TotalAgility On-Premise Multi-Tenant installation files to install:

- Tenant Management System (used to create and manage tenants)
- Live (production) environment
- Additional deployment environment


For on-premise multi-tenancy, the additional and production environments must be installed on separate servers to ensure the additional server workload does not affect the production 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 must 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 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 Tungsten TotalAgility On-Premise Multi-Tenant system, you must create a tenant to access the system.

TotalAgility documentation

To access the full documentation set online, see the Tungsten TotalAgility 8.1.0 [Product Documentation](#) page.

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

 When upgrading to TotalAgility 8.1.0 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.

You can access the TotalAgility documentation online as well as [offline mode](#).

Full documentation set

A complete set of TotalAgility documentation includes the following items.

Guide/Help	Description
Administrator's Guide	Provides information for administrators who are responsible for configuring and maintaining a TotalAgility installation.
API Documentation	Includes the details of the supported APIs (excludes deprecated methods), supported methods for each service, and all input and output including the required fields, field types, and enumerations, any special information about each method, coding examples, and related details.
Architecture Guide	Provides an overview of the TotalAgility architecture, covering various deployments for on-premise, on-premise multi-tenancy, and Azure environments.
Best Practices Guide	Describes the best practices to follow when using TotalAgility to improve performance, cost, maintenance, availability, and security.
Configuration Utility Guide	Provides instructions for using the Configuration Utility to update settings across various configuration files for different installation and deployment types.
Designer Help	Provides details about using TotalAgility Designer to design business jobs and cases, assign resources, create forms, integrate with external applications, and more.
Features Guide	Provides an overview of the TotalAgility features.
Installation Guide	Provides instructions on installing TotalAgility and integrating it with other products.
Integration Server Installation Guide	Provides instructions on installing TotalAgility Integration Server and integrating it with other products.
On-Premise Multi-Tenant Installation Guide	Provides instructions on installing and configuring a TotalAgility On-Premise Multi-Tenant system.
Prerequisites Utility Guide	Provides system requirements for installing TotalAgility, instructions for running the Pre-requisite Utility, and a software checklist for various installation types.
Reporting Tables	Describes the Dimension and Fact tables of the Reporting data warehouse that store information related to Capture client activities in TotalAgility.
Reporting Views	Describes the sample views provided with Reporting.
Tables for Analytics	Describes the TotalAgility tables and fields used by Analytics for TotalAgility.
Tenant Management System Help	Describes how to create and manage tenants using the TotalAgility On-Premise Multi-Tenant system.
Tenant Management System Installation Guide	Provides instructions for installing the TotalAgility Tenant Management System.

Guide/Help	Description
TotalAgility Apps Help	<p>Provides details about using the TotalAgility Apps application that allows citizen developers to configure the workflow and capture items with little or no training. The <i>TotalAgility Apps Help</i> encapsulates the help for the following applications.</p> <ul style="list-style-type: none"> • Business Data • Import • Tungsten Copilot • Quick Capture • Quick Classification • Quick RPA • Quick Rules • Quick Skins • Quick Workflow
Web Capture Control Help	<p>Provides details for 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.</p>
Workspace Help	<p>Provides details for using TotalAgility to design business jobs and cases, assign resources, create forms, integrate with external applications, and more.</p>
Other documentation	
Capture Client help for Capture activities	<p>Provides help for using Capture activities in TotalAgility. It includes the following help systems:</p> <ul style="list-style-type: none"> • Document Review Activity Help • Scan Activity Help • Scan Create New Job Form Help • Validation Activity Help • Verification Activity Help
Devices Help	<p>Provides details for managing devices connected to TotalAgility.</p>
Document Converter Help	<p>Provides instructions on how to configure the parameters that determine the tools to use for document conversion, connection to the Adobe Experience Manager output server that is used to convert XFA forms to PDF format, and log files and traces.</p>
Export Connector Help	<p>Provides instructions on managing an Export Connector and setting up an Export Connector for a document type.</p>
Transformation Converter Help	<p>Provides instructions on how to convert Tungsten Capture and Tungsten Transformation projects into the correct format so that they can be used in TotalAgility.</p>
Front Office Server .NET Restful Web Service API for the Device Client	<p>Provides documentation for the .NET Restful Web Service API for the Device Client.</p>

Guide/Help	Description
Front Office Server .NET Legacy API for the Device Client	Provides documentation for the .NET Legacy API for the Device Client.
Message Connector Help	Provides instructions on how to configure and use Message Connector.
MFP Starter Pack Getting Started Guide	Provides instructions on how to use TotalAgility to import and process the MFP Starter Pack.
MFP Administrator's Guides for Devices	<p>Describe how to prepare MFP devices to work with TotalAgility. The administrator's guides for the following devices are available:</p> <ul style="list-style-type: none"> • Canon MEAP • Canon ScanFront • Emulator • Fujitsu • HP • Konica Minolta • Kyocera • Lexmark • Ricoh • Xerox
MFP Web Services Connector SDK Developer's Guide	Provides an overview and instructions for developing inputs with the MFP Web Services Connector Software Developer Kit (SDK). Along with this guide, the SDK provides documentation for the Web services.
Repository Browser Help	Provides instructions on how to use the Repository Browser to view the extraction results for a set of folders and documents.
Search and Matching Server documentation	Provides documentation of the Tungsten Search and Matching Server, which handles search requests from various Tungsten Automation applications for large volumes of data located at a remote site.
Transformation Designer Help	Provides instructions on how to use Transformation Designer to set up, store, and test projects that contain all the necessary information for processing documents.
Transformation Designer Scripting Help	Provides an introduction to the WinWrap Basic Editor and an overview of the available scripting events.
XDoc Browser Help	Provides help on using the XDoc Browser, a program that provides direct access to the document representation that is used by TotalAgility. With XDoc Browser, you can open and display an XDoc along with any referenced images for testing, demonstration, and debugging purposes.
Documentation only available on the Product Documentation page (and not in the Offline documentation package)	
Federated Security in TotalAgility	Provides information about claims-based identity in TotalAgility.


Guide/Help	Description
Release Notes	Includes key details about the new and enhanced features and any changes in behavior in TotalAgility 8.1.0. It also lists any known and resolved issues in this version of TotalAgility.
Technical Specifications	Provides technical specifications for TotalAgility.
Tutorial for Capture Starter Pack	Lets you test drive a predefined TotalAgility solution that requires minimal configuration to create and process TotalAgility jobs right away.
Tutorial for Data Objects	Provides information about how to create a solution using Data objects and create and update data using Data objects and RESTful service.
Tutorial for Online Learning	Explains how to create a Machine Learning project that uses Online Learning for classification and extraction of documents.
Tutorial for Quick Workflow	Provides information about how to create a workflow quickly so you can start working with a fully functional TotalAgility solution.

Offline documentation

If you require offline documentation, you can download it from the [Tungsten Automation Fulfillment Site](#). For each language, a separate documentation package is available to download as a compressed file, such as TotalAgilityDocumentation_8.1.0_EN.zip for English or TotalAgilityDocumentation_8.1.0_FR.zip for French.

Following is the list of TotalAgility supported languages and the language codes used in the ZIP files.

Language	Code
Brazilian Portuguese	pt_BR
English	EN
French	FR
German	DE
Italian	IT
Japanese	JA
Spanish	ES

 The English and Japanese .zip files include both help and print folders. The print folder contains PDF guides, such as the installation guide and administrator's guide. The .zip files for other languages contain a limited set of localized files.

The following procedure describes accessing TotalAgility documentation offline for English.

1. From the [Tungsten Automation Fulfillment Site](#), download the documentation.zip file for the applicable language, such as English.
2. Extract the contents of the compressed documentation file to your local computer.

- In the TotalAgility product installation files, inside the `Agility.Server.Web\Help` folder, create a folder for the desired language. For example, for accessing TotalAgility documentation offline for English, create the EN folder for each item as given in the following table.


i In a distributed environment, copy files on the Web server, and apply the `Web.config` changes on the Application and Web servers.

Copy the contents from the folder	Paste the contents to the folder
Designer	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \TotalAgility_designer\EN</code> <p>i The TotalAgility installer creates the <code>TotalAgility_designer</code> and <code>API</code> folders inside the <code>Help</code> folder. You must manually create other folders such as <code>Workspace</code> and <code>TotalAgilityApps</code> and then copy the contents into the respective folders.</p>
Devices	<code>\\TotalAgilityInstall\Agility.Server.Web\bin \Administrative\Help\Devices\EN</code>
DocumentConverter	<code>\\Tungsten\Document Converter\web\en\WebHelp</code>
ExportConnector	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \ExportConnector_help\EN</code>
KCKTM_Converter	<code><%ProgramData%>\Tungsten\Transformation\en_US\help \KCKTM_Converter</code>
MessageConnector	<code>\\Kofax\KIC-ED\MC\web\en\WebHelp</code>
RepositoryBrowser	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \RepositoryBrowser\EN</code>
SDK_Documentation	<code>\\TotalAgilityInstall\Agility.Server.Web\Help\API \EN</code>
TenantManagementSystem	<code>\\TotalAgilityInstall \Agility.Server.Web.TenantManagement \TenantManagement\Help\TenantManagementSystem\EN</code>
TotalAgilityApps	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \TotalAgilityApps\EN</code>
TransformationDesigner	<code><%ProgramData%>\Tungsten\Transformation\en_US\help \TransformationDesigner</code>
WebCaptureControl	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \WebCaptureControl\EN</code>
Workspace	<code>\\TotalAgilityInstall\Agility.Server.Web\Help \Workspace\EN</code>
XDocBrowser	<code><%ProgramData%>\Tungsten\Transformation\en_US\help \XDocBrowser</code>
Activity folder within CaptureClient Example: <code>DocumentReviewActivity</code>	<code>\\TotalAgilityInstall\Agility.Server.Web\Forms \Controls\Capture\Help\DocumentReviewActivity\EN</code>

4. Navigate to the installation folder.

For the help	Perform the following steps
<ul style="list-style-type: none"> TotalAgility Designer Devices Transformation Designer XDoc Browser Transformation Converter 	<p>a. Open TotalAgility Web.config in a text editor from the following location:</p> <pre>\\TotalAgilityInstall\Agility.Server.Web</pre> <p>b. Locate the <appSettings> section and remove http://docshield.tungstenautomation.com/KTA from the key value: <add key="OnlineHelpURL" value="http://docshield.tungstenautomation.com/KTA"/>.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p>i For the Transformation Designer, XDoc Browser, and Transformation Converter Help to work offline and 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.</p> </div>
TotalAgility Export Connector	<p>a. Open Agility.Server.ExportConnector.exe.config in a text editor from the following location:</p> <pre>\\TotalAgilityInstall\Agility.Server.Web\bin</pre> <p>b. Locate the <appSettings> section and remove http://docshield.tungstenautomation.com/KTA from the key value: <add key="OnlineHelpURL" value="http://docshield.tungstenautomation.com/KTA"/>.</p> <p>Alternatively, run TotalAgility.ConfigurationUtility.exe (available from the TotalAgility Product installation files at \\Tungsten TotalAgility-8.1.0\Utilities\ConfigurationUtility) and remove the URL for online help from the OnlinehelpURL setting.</p>
TotalAgility Message Connector	<p>a. Open configuration.xml in a text editor from the following location:</p> <pre>\\Kofax\KIC-ED\MC\web</pre> <p>b. Locate the <OnlineHelp>1</OnlineHelp> section and replace 1 with 0.</p>
TotalAgility Document Converter	<p>a. Open configuration.xml in a text editor from the following location:</p> <pre>\\Tungsten\Document Converter\web</pre> <p>b. Locate the <OnlineHelp>1</OnlineHelp> section and replace 1 with 0.</p>

5. Save and close the configuration file.

Clicking the Help icon  launches the help for the installed product.


Training

Tungsten Automation offers both on-demand and instructor-led training to help you make the most of your product. To learn more about training courses and schedules, visit the [Tungsten Automation Learning Cloud](#).

Getting help with Tungsten Automation products

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

To access the Tungsten Automation Knowledge Portal, go to <https://knowledge.tungstenautomation.com/>.

 The Tungsten Automation Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Tungsten Automation Knowledge Portal 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.
To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Tungsten Automation Community (for all customers).
On the Resources menu, click the **Community** link.
- Access the Tungsten Automation Customer Portal (for eligible customers).
Go to the [Support Portal Information](#) page and click **Log in to the Customer Portal**.
- Access the Tungsten Automation Partner Portal (for eligible partners).
Go to the [Support Portal Information](#) page and click **Log in to the Partner Portal**.
- Access Tungsten Automation support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Go to the [Support Details](#) page and select the appropriate article.

Chapter 1

Installation planning

This chapter describes the system requirements, prerequisites, licensing details, and various third-party and Tungsten Automation products that you can integrate to use with TotalAgility.

System requirements

See the *Tungsten TotalAgility Technical Specifications* document on the Product Documentation site.

- For supported operating systems and other system requirements.
- If your solution includes multiple Tungsten Automation products.

The document is updated regularly, and we recommend that you review it carefully to ensure success with your TotalAgility product.

Prerequisites

- Before extracting the TotalAgility installation ZIP file, unblock the file from the File Properties window.
- Run the Prerequisites Utility to ensure all the required software is installed on your computer before installing TotalAgility. For more information on prerequisites and the software checklist for various installation types, refer to the *Tungsten TotalAgility Prerequisites Guide*.
- You must have an administrator account to install TotalAgility.
- The user who will run TotalAgility must have "Log on as Service" rights.
- The user who will run TotalAgility with the IIS service account must have "Log on as a Batch Job" permission.

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

SQL Server

The SQL and TotalAgility servers must run in the same time zone; otherwise, unexpected issues such as activities resetting incorrectly may occur.

Transformation Server

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

Tungsten TotalAgility Document converter

The Document Converter is automatically installed when installing the Transformation Server.

Reporting Server

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

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

You cannot have two reporting services on the same server. However, you can install the reporting service on two servers and run them at the same time.

Microsoft Dynamics CRM

You can integrate Microsoft Dynamics CRM with TotalAgility.

Microsoft Dynamics 365 CRM

You can integrate Microsoft Dynamics 365 CRM with TotalAgility.

Tungsten Message Connector

Tungsten Message Connector is a Windows service responsible for importing messages and files in many electronic formats. It can retrieve documents using one of the following connection modes:

- **Storage mode:** Retrieves documents from various sources and saves them in internal storage, and they are available for retrieval using a web service interface. TotalAgility connects to the Message Connector web service interface and retrieves the documents for import.
- **Direct mode:** Retrieves documents from various sources and directly imports them to TotalAgility.

Tungsten Message Connector can import messages and files from many sources:

- Email messages including attachments using various email protocols (MS Graph, SMTP, POP3, IMAP, and EWS).
- Fax messages (via internal fax over IP server or external fax servers: Tungsten Communication Server, RightFax, and Biscom).
- Files from a local or network folder, or Cloud folders such as Azure Blob Storage and Azure File Share.

When you install TotalAgility from a network share, make sure the user has the Write permissions to the share; otherwise, the Message Connector will not be installed successfully.

If you want to install a Message Connector, then before installing TotalAgility, you must set the value of the `ImportService` parameter to true in `SilentInstallConfig.xml` available at the following location in your installation files:

```
\\Program Files (x86)\Kofax\KIC-ED\MC
```

You can install multiple instances of Message Connectors. See [Silent installation of multiple instances of Message Connectors](#).

Tungsten SignDoc

You can integrate Tungsten SignDoc with TotalAgility to allow a callback to occur when the signing is completed. See [TotalAgility and Tungsten SignDoc integration](#).

Tungsten VRS Elite

We highly recommend Tungsten VRS Elite, 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 Image processing technology included with TotalAgility. For information about licensing options, see Tungsten VRS Elite licenses.

TCM Proxy

TCM Proxy is required when you want to use the Tungsten Communications Manager (TCM) control on a TotalAgility form for interactive requests with Communications Manager. The proxy allows secure cross domain communication between the TotalAgility Web Server and Communications Manager.

 To use TCM functionality, you must run the TCM Proxy installer on every Web Server in use.

Tungsten TotalAgility Repository Browser

The Tungsten TotalAgility Repository Browser is a utility intended to aid in developing and testing TotalAgility projects and uses direct SQL access to the database. As such, you should not use the utility in a production environment, or against large datasets.

This utility is not installed by default. To install this utility, run the RepositoryBrowser.msi available in the TotalAgility installation files at \\Tungsten TotalAgility-8.1.0_OPMT\RepositoryBrowser.

Tungsten Web Capture Service

Install the Tungsten Web Capture Service to enable web scanning. You can install the Tungsten Web Capture Service either at default or custom location.

You must install the Web Capture Service only once, and web scanning is enabled across all the supported browsers. You must have administrative rights to complete the installation when installing through the browser.

Once you install the Web Capture Service, temporary files are created under the folder, "Interprocess". The user must have read/write access to this folder.

You can use the Web Capture Service in multiuser environments.

Tungsten TotalAgility Scan Agent Service

The Scan Agent Service is an asynchronous upload capability that allows a scan operator to continue to the next batch without needing to wait for the previous scan job to finish uploading.

This service is useful in remote scanning scenarios, where the scan station has limited network bandwidth to the main TotalAgility site. It allows a scan operator to keep up with physical scanning throughput, while the image upload is done in the background, thus enhancing the scan operator's 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 the 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 the 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.

Licensing

Obtain a license key for TotalAgility from your Account Manager or Tungsten Automation Support.

Concurrent user licenses

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 Firefox and Chrome, the user consumes two concurrent licenses. The license server automatically releases the applicable license when a user logs off from a session.

Reserved licenses

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. Consider the following policies 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 logins 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 activate the license when you are ready to use TotalAgility. If you log on to TotalAgility for the first time and the license is not activated, the License Activation window opens.

1. In the License Activation window, click **Next** to accept the default values for the **License Server** and **Port Number** or enter the new values.
2. Click **Set license server** to save the information.
3. For further instructions, see the Activate the License Server step in [Standard installation of the Web and Application on the same server](#).


 If you have issues activating your license, contact Tungsten Automation support at: <https://knowledge.tungstenautomation.com/category/support>

Automatic recovery

On installing TotalAgility, it is possible to manually configure the Tungsten 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 Tungsten 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 configure the license at the command line. Example: `sc.exe failure KSALicenseService reset= 86400 actions= restart/660`

Set up a non-administrator service account for Tungsten License Server service

You can set up a non-administrator service account for the Tungsten License Server service using either of the following ways:

- [Manually](#)
- [By uninstalling and re-installing Tungsten License Server service](#)

Manually

Use the following procedure to setup the non-admin user account manually.

1. Create the non-admin User account.
2. Add the user to the local policy of the machine to allow logon as a service.
3. At the netsh http prompt, run the `delete urlacl=<URL>` command to remove the registered URLs.
The existing URL reservations are removed.
4. At the netsh http prompt, run the `Add urlacl=<URL>` command to add the registered URLs.
5. Run the Add command for each URL.
6. Stop the Tungsten License Server service.
7. Add the non-admin user to the SQL Logins.
8. Give the following permissions to the non-admin user: datareader, datawriter and execute rights to the "Main" database of Tungsten TotalAgility.
9. Change the account running the Tungsten License Server service (Windows service) to the non-admin user account.
This will re-configure Tungsten License Server service to use the new user.

10. Start the Tungsten License Server service.
11. Launch TotalAgility Designer or TotalAgility Workspace to logon.
If the login fails, the errors are logged in the Event log. License related errors may be, for example, due to the following reasons:
 - The non-admin user does not have the datawriter rights.
 - HTTP could not register the URL.
 - The process does not access rights to the namespace, as the URL is not registered for the non-admin user.

Resolve the errors and restart the Tungsten License Server service.

By uninstalling and re-installing Tungsten License Server service

Use the following procedure to setup the non-admin user account by uninstalling and re-installing Tungsten License Server service.

1. Create the non-admin User account.
2. Add the user to the local policy of the machine to allow logon as a service.
3. Back up the service.exe configuration file.
This will backup the Tungsten TotalAgility database configuration used by the service.
4. Uninstall the Tungsten License Server service.
The existing URL reservations are removed.
5. Add the non-admin user to the SQL Logins.
6. Give the following permissions to the non-admin user: datareader, datawriter and execute rights to the Main Tungsten TotalAgility database.
7. Open the Command Prompt window and run the following command to re-install the Tungsten License Server service.

```
Msiexec /i "path to the KofaxLicenseServer-6.6.1.msi" SALSVCUSER="" SALSVCPWD="" /qn
```

8. Stop the Tungsten License Server service.
9. Restore the service.exe configuration backup from Step 3.
The database configuration to Tungsten TotalAgility is restored.
10. Start the Tungsten License Server service.
11. Launch TotalAgility Designer or TotalAgility Workspace to logon.
If the login fails, the errors are logged in the Event log. License related errors may be, for example, due to the following reasons:
 - The non-admin user does not have the datawriter rights.
 - HTTP could not register the URL.
 - The process does not access rights to the namespace, as the URL is not registered for the non-admin user.

Resolve the errors and restart the Tungsten License Server service.

Tungsten VRS Elite licenses

We highly recommend Tungsten VRS Elite, 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 Tungsten Automation image processing technology included with TotalAgility.

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

Several Tungsten VRS Elite licensing options are available:

- **VRS Elite Basic or Professional OEM:** Automatically activate a VRS Elite Basic or Professional OEM license that is included with many industry-standard scanners. License activation for these scanners is required only when upgrading to Tungsten 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. This configuration may be convenient if you have many scanners. For this configuration, make sure VRS Elite 5.1.2 or later is installed.

TotalAgility License Proxy

TotalAgility License Proxy enables unconnected Scan Workstations and/or other TotalAgility components to get licensing from the TotalAgility License server.

Use TotalAgility License Proxy when the license server is not directly accessible from VRS stations or the linked TotalAgility server. For example, the server may not be directly accessible if you use Azure or because of security restrictions. Using the License Proxy, you can use a TotalAgility license configuration through TotalAgility web services rather than by directly addressing the license server.

A License Proxy is also useful for network topologies where multiple networks are logically separate, such as Microsoft Azure Cloud. A License Proxy allows computers in Network A to use a TotalAgility license server in Network B. A License Proxy uses TotalAgility web services (over HTTP/HTTPS) to communicate with the license server. The License Proxy computer needs a working Internet connection to facilitate the HTTP/HTTPS traffic to the License server.

See [TotalAgility License Proxy installation](#).

Use the Tungsten TotalAgility license for Tungsten VRS Elite

The Tungsten TotalAgility license includes at least one Tungsten VRS Elite license.

To support tenant licensing for Tungsten VRS Elite, a new component replaces the Tungsten 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 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.

Utilities

The following utilities are available from your TotalAgility product installation files.

- **Prerequisite utility:** Run this utility to ensure all the required software is installed on your computer before installing TotalAgility. For more information, see the *Tungsten TotalAgility Prerequisites Guide*.
- **Configuration utility:** Run this utility after installing TotalAgility to modify or update the settings across multiple configuration files at the same time instead of editing each file separately. See the *Tungsten TotalAgility Configuration Utility Guide*.
- **Docker:** 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. See [TotalAgility installation in a Docker container](#).
- **EvrCheck utility:** Run this utility to test how an image will look once the eVRS setting is applied to it. For more information, see EvrCheck utility.
- **TotalAgility.EncryptConfig.exe:** Use this utility to encrypt and decrypt the configuration files of executables. See [Encrypt and decrypt the configuration files of executables](#).

Installation types

You can perform either standard or silent installation of TotalAgility. Install TotalAgility as one of the following types under standard or silent installation.

Database only

Installs only the database component of Tungsten TotalAgility on-premise multi-tenant; no other components are installed.

TotalAgility includes the following databases.

Database	Default Database Name	Purpose
MasterTenantDatabase	MasterTenant	Purpose?
DataCenterDatabase	DataCenterTenants	Purpose?

Upgrade databases

Upgrades all the 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 TotalAgility Designer and TotalAgility Workspace.

i TotalAgility does not support a Web server pointing to a combined Web/App server. A Web server must point to an App only server. While a Web server pointing to a combined Web/App server may still work, there are some areas that do not work. For example, the Streaming service on a Web tier does not work when pointing to a Streaming service on a combined Web/ App.

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 TotalAgility Designer and TotalAgility Workspace.

Web and Application Server

Installs the Web and Application servers on a single computer.

Real Time Transformation Service

Installs the Real Time Transformation Service.

Manual installation of databases

1. Create the MasterTenants and DataCenterTenants databases.

2. Run the following scripts on the MasterTenants database.

Example:

- Create_MasterTenants.sql
- Initialise_MasterTenants.sql

3. Run the following scripts on the 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.



- 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 the names given while creating databases manually.
- c. Click **Next**. Ensure the installation is completed 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 the 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.

i 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.

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.

Post-installation configurations

After installation, you can modify the configuration settings by editing each configuration file separately or running the Configuration Utility. The Configuration Utility is available from your TotalAgility installation files. You must manually copy the utility onto each server where the configuration settings are to be modified. See the *Tungsten TotalAgility Configuration Utility Guide*.

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.

Silent installation of TotalAgility On-Premise Multi-Tenancy


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.




This section describes the silent installation for the following installation types:

- [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. From your TotalAgility installation files, navigate to `\\OnPremiseMultiTenancyInstall` and open `SilentInstallConfig.xml` using a text editor.
2. In `SilentInstallConfig.xml`, update the following parameters.

Parameter	Default Value	Description
LiveHostName		<p>Enter the Production deployment host name. This should be the Production Web server machine name.</p> <p>When using the LiveHostName to access TotalAgility, the format of the name should be <code>hostname: port number</code>.</p> <p>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 <code>ta.app.com</code>; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed.</p> <p>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.</p>
DevHostName		<p>Enter the additional deployment host name. This should be the additional deployment Web server machine name.</p> <p>When using the DevHostName to access TotalAgility, the format of the name should be <code>hostname: port number</code>.</p> <p>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 <code>ta.app.com</code>; otherwise, the host name is the host name of the machine where TotalAgility Web server is installed.</p> <p>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.</p>
DatabaseInformation		
UpdateDatabases	true	Accept the default to automatically install the databases. Set to false to ignore installing databases.
ScriptsLocation	C:\Program Files\Tungsten\TotalAgility\DatabaseScripts\SQL Server	The path where the database scripts are located.
OverwriteIfExists	false	<p>Set to true to overwrite the existing databases.</p> <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p> If the existing database details are not valid, or if the databases do not exist, an error occurs, and the installation fails.</p> </div>
MasterTenantDatabase		
DatabaseName	MasterTenants	Accept the default.
Server	Server Name	Specify the name of your machine.
Security		



Parameter	Default Value	Description
WindowsAuthentication	true	Set to true to use Windows credentials for connecting to the database. If set to false, provide the username and password. (Default: empty)  Configure this setting for the DataCentre database also.
UserName	empty	
Password	empty	
NewDatabase	false	Set to true to create a new database.  Configure this setting for the DataCenter database also.
DataCenterDatabase		
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 the database, the services, such as Core Worker Service, Reporting Service, License Service, and Transformation Service are ignored and not installed.


- Run `Setup.exe /Silent`.
 - The databases are installed automatically.
 - The system generates a summary of log, `TungstenTotalAgilityMultiTenancySilentInstall.txt`, on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.
 - The success or failure of installation is indicated in the event log.
 - When automating the installation, if you run `setup.exe` from Command line, or as a silent installation, one of the codes returns to indicate the following:
 - 0=Success
 - 1=Success with warnings
 - 2=Failure

Silent installation for upgrading databases

- From your TotalAgility installation files, 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, and Transformation Service are ignored and not installed.
LiveHostName		Enter the Production deployment host name. This should be the Production Web Server machine name. When using the LiveHostName to access TotalAgility, the format of the name should be <code>hostname: port number</code> . 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 <code>ta.app.com</code> ; otherwise, the host name is the host name of the machine where the 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 additional deployment host name. This should be the Web Server machine name of the additional deployment. When using the DevHostName to access TotalAgility, the format of the name should be <code>hostname: port number</code> . 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 <code>ta.app.com</code> ; otherwise, the host name is the host name of the machine where the 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		
UpdateDatabases	true	Set to false to ignore installing databases. If set to true, installs the databases.
OverwriteIfExists	false	Set to true to overwrite the existing databases.  If the existing database details are not valid, or if the databases do not exist, an error occurs, and the installation fails.

Parameter	Default Value	Description
MasterTenantDatabase		
DatabaseName	MasterTenants	Accept the default.
Server	Server Name	Specify your machine name.
Security		
WindowsAuthentication	true	Set to true to use Windows credentials for connecting to the database. If set to false, provide the username and password. (Default: empty)  Configure this setting for the DataCentre database also.
UserName	empty	
Password	empty	
NewDatabase	false	Accept the default. If set to true, creates a new database.
DataCentreDatabase		
DatabaseName	DataCenterTenants	Accept the default.
Server	Server Name	Specify the your machine name.
InstallInfo		
InstallType	Both	Change the value to UpgradeDatabasesOnly to upgrade all the databases to the latest version of TotalAgility.


- Run `Setup.exe /Silent`.
 - The databases are installed automatically.
 - The system generates a summary of log, `TungstenTotalAgilityMultiTenancySilentUpgrade.txt`, on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.
 - The success or failure of installation is indicated in the event log.
 - When automating the installation, if you run `setup.exe` from Command line, or as a silent installation, one of the codes returns to indicate the following:
 - 0=Success
 - 1=Success with warnings
 - 2=Failure


Silent installation of Web and Application on the same server

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




- From your TotalAgility installation files, 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
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 the Transformation Server on the Application server so that the IIS prerequisite is not needed. IIS is not required for the 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.
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: <ul style="list-style-type: none"> • 1: The license server is set as a primary license server. • 2: The license server is set as a backup license server.
EnableSSL	false	You can set to true to enable https.
Certificate	Empty	If SSL is enabled, you must provide the certificate thumbprint of a correctly configured certificate on the computer on which you install TotalAgility. If you enable SSL and provide the certificate thumbprint, the port number for Licensing is automatically set to 3582.

Parameter	Default Value	Description
IsDatabaseWindowsAuthentication	false	Set to true to use Windows authentication to connect to SQL Server. The databases are created in the following format when tenants are created: <ul style="list-style-type: none"> TotalAgility_Main_Live_TenantName TotalAgility_Reporting_Live_TenantName TotalAgility_Reporting_staging_Live_TenantName TotalAgility_Documents_Live_TenantName
InstallDirectory	C:\Program Files\ Tungsten \TotalAgility	Specify the TotalAgility destination directory.
SSLEnabled	true	Accept the default.
InstallTenantManagement Website	false	Accept the default. Set to true to install the Tenant Management System. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i You must pre-configure the parameters in the SilentInstallConfig.xml for Tenant Management System before running the silent installation from on-premise multi-tenancy. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.</p> </div>
DatabaseInformation		
OverwriteIfExists	false	Set to true to overwrite the existing databases. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i If the existing database details are not valid, or if the databases do not exist, an error occurs, and the installation fails.</p> </div>
ScriptsLocation	C:\Program Files\Tungsten \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 connecting to database. If set to false, provide the username and password. (Default: empty) <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i Configure this setting for the DataCentre database also.</p> </div>

Parameter	Default Value	Description
UserName	empty	
Password	empty	
NewDatabase	false	Set to true to create a 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 Tungsten 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 Tungsten TotalAgility services are created with the NT Authority\Network Service username.  <ul style="list-style-type: none"> 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 Production environment or enter "Dev" for additional deployment 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 <code>smtp.office.com</code> .
PortNumber	port number	Enter the port number, such as 387.
UserName	username	Enter the username, such as <code>abc@tungsteautomation.com</code>
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered, such as <code>abc@tungsteautomation.com</code> .
TransformationServerInfo		
<p> Configure these settings if TransformationService is "true".</p>		
TSConfigFile	empty	Specify the path to the .ini file along with the name for Transformation Server to configure. <p> 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.</p>
LogFile	C:\Program Files\Tungsten\TotalAgility\Transformation Server\Tslog.txt	Set the location where the Transformation Server log file will be created. Make sure to include the filename (such as TSLog.txt) in the filepath. For example, <code>C:\Program Files\Tungsten\Transformation Server\TSLog.txt</code> If the log filepath is not valid, the Transformation Server installation fails.
InstallLocation	For example, <code>C:\Program Files (x86)\Tungsten\TotalAgility\Transformation Server</code>	Specify the Transformation Server destination directory.
WindowsServiceAccount	no default	Enter the name of the user who will run Transformation Server.
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 the Transformation Server process all activities regardless of the pool.


Parameter	Default Value	Description
PoolName	empty	<p>If UseSpecificPool is set to true, enter the Transformation Server pool name.</p> <p>i If you leave the pool name empty, all activities are processed regardless of their pools.</p>
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 A2iA recognition engine [unsupported].
EnableSyncCalls	true	Set to true to enable synchronous calls for a Transformation Server instance. false or any other value disables these calls.
TS_INSTALL_NLP_WESTERN	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
TS_INSTALL_NLP_ADDITIONALLANGUAGES1	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.
TS_INSTALL_NLP_ADDITIONALLANGUAGES2	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.
TS_INSTALL_NLP_ADDITIONALLANGUAGES3	false	If set to true, installs the Natural Language Processing language bundle for Swedish, Finnish, Danish, Norwegian, and Arabic.

Parameter	Default Value	Description
<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 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. A 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:

- Tungsten 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 summary of log, `TungstenTotalAgilityMultiTenancySilentInstall.txt`, on the desktop.
- The system generates a log file that reports any errors.

- If any errors occur, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt, on the desktop. Fix those errors and repeat the above steps.
- 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_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

```

Silent installation of Web and Application on different servers

Install TotalAgility on a separate Web or Application server.

This section describes the silent installation for the following installation types:

- [Silent installation of the Web Server](#)
- [Silent installation of the Application Server](#)

Silent installation of Web Server

1. From your installation files, 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 \Tungsten\ 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.

Parameter	Default Value	Description
InstallTenantManagement Website	false	<p>Accept the default. Set to true to install the Tenant Management System.</p> <p>i You must pre-configure the parameters in the SilentInstallConfig.xml for Tenant Management System before running the silent installation from on-premise multi-tenancy. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.</p>
ApplicationServerName	App server name	<p>Enter the Fully Qualified Domain Name (FQDN) of the Application server.</p> <p>i 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:</p> <pre><WebServerName> FQDN:portnumber </WebServerName></pre>
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	<p>If set to true, the IIS AppPool and Tungsten TotalAgility services run as the LocalSystem account.</p> <p>i If you set this parameter to true, databases should be created using SQL authentication.</p>

Parameter	Default Value	Description
RunAsNetworkServiceAccount	false	<p>If set to true, the AppPool and Tungsten TotalAgility services are created with the NT Authority\Network Service username.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i</p> <ul style="list-style-type: none"> 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. </div>
InstallInfo		
InstallAction	MultiTenancyInstall <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff; margin-top: 5px;"> <p>i For upgrade, specify InstallAction as MultiTenancyUpgrade.</p> </div>	Accept the default.
InstallMode	Silent	Accept the default.
InstallType	Both	Enter WebServer
MultiTenancyInstallMode	Live	Accept the default for Production environment or specify the additional environment.
DatabaseServerType	SQLServerNonSSL	Accept the default or enter Azure .
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 abc@tungstenautomation.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered, for example, abc@tungstenautomation.com.
UseSSL	false	Enter the SSL certificate to use HTTPS communication.

Parameter	Default Value	Description
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 port number 85.

3. Save and close the file.
4. On the Command Prompt, change the current directory to the root directory of Setup.exe.
5. Run `Setup.exe /Silent`.
 - Tungsten TotalAgility is installed automatically.
 - The system generates a summary of log, `TungstenTotalAgilityMultiTenancySilentInstall.txt`, on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.
 - The success or failure of installation is indicated in the event log.
 - When automating the installation, if you run `setup.exe` from Command line, or as a silent installation, one of the codes returns to indicate the following:
 - 0=Success
 - 1=Success with warnings
 - 2=Failure

Silent installation of an Application Server

Update the following parameters for an Application Server.

1. From your installation files, 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.

i 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](#).

i 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:

- Tungsten TotalAgility

i 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

i 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 summary of log, `TungstenTotalAgilityMultiTenancySilentInstall.txt`, on the desktop.
- If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.
- The success or failure of installation is indicated in the event log.
- When automating the installation, if you run `setup.exe` from Command line, or as a silent installation, one of the codes returns to indicate the following:
 - 0=Success
 - 1=Success with warnings
 - 2=Failure



Silent installation of Real Time Transformation Server

- From your installation files, navigate to `\\OnPremiseMultiTenancyInstall` and open `SilentInstallConfig.xml` using a text editor.
- In `SilentInstallConfig.xml`, update the following parameters.

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

Parameter	Default Value	Description
InstallDirectory	C:\Program Files\ Tungsten \TotalAgility	Specify the TotalAgility destination directory.
IsDatabaseWindowsAuthenticatio n	false	Set to true to use Windows authentication to connect to SQL Server.
DatabaseInformation		

Parameter	Default Value	Description
InstallDatabases	false	Set to false to ignore installing databases.
OverwriteIfExists	false	Set to true to overwrite the existing databases. i If the existing database details are not valid, or if the databases do not exist, an error occurs, and the installation fails.
DataCenterDatabase		
DatabaseName	TotalAgility tenant	Specify the name of the DataCenter database.
Server	server name	Specify the fully qualified domain name (FQDN) of the server.
Security		
WindowsAuthentication	false	Set to true to use Windows credentials for connecting to the database. If set to false, provide the username and password. (Default: empty)
UserName	empty	
Password	empty	
NewDatabase	false	Accept the default as the user connects to an existing datacenter database.
TenantDatabase		
DatabaseName	TotalAgility_tenant	Specify the name of the tenant database.
Server	server name	Specify the fully qualified domain name (FQDN) of the server. i 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		

Parameter	Default Value	Description
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.
IdentityInformation		
UserName	username	Enter the username of the Windows service account for the TotalAgility services.
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 Tungsten TotalAgility services are created with the 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 Tungsten TotalAgility services are created with the NT Authority \Network Service username. <ul style="list-style-type: none"> 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
InstallType	Both	Set to RTTS. i When you install RTTS, it ignores the services. The services such as CoreworkerService, ImportService, and ExportService are not installed.
SslEnabled	true	Accept the default.
Transformation ServerInfo		
TransformationService	true	Accept the default.
TsConfigFile	no default	Specify the path to .ini file along with the name for Transformation Server to configure. i 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\Tungsten\TotalAgility\Transformation Server\Tslog.txt	Set the location where the Transformation Server log file will be created. Make sure to include the filename (such as TSLog.txt) in the filepath. For example, C:\Program Files\Tungsten\TotalAgility\Transformation Server\TSLog.txt If the log filepath is not valid, the Transformation Server installation fails.
InstallLocation	For example, C:\Program Files (x86)\Tungsten\TotalAgility\Transformation Server	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 the Transformation Server process all activities regardless of the pool.

Parameter	Default Value	Description
PoolName	empty	<p>If you set UseSpecificPool=true, enter the Transformation Server pool name.</p> <p>i If you leave the pool name empty, all activities are processed regardless of their pools.</p>
OLEnabled	true	<p>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.</p> <p>i In cases where multiple instances of the 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.</p>
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 CPU_SERVER_OVERRIDE_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.

Parameter	Default Value	Description
TS_INSTALL_NLP_WESTERN	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
TS_INSTALL_NLP_ADDITIONALLANGUAGES1	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.
TS_INSTALL_NLP_ADDITIONALLANGUAGES2	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.
TS_INSTALL_NLP_ADDITIONALLANGUAGES3	false	If set to true, installs the Natural Language Processing language bundle for Swedish, Finnish, Danish, Norwegian, and Arabic.
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 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 the Transformation Server in a synchronous mode and configures the core and SDK APIs of TotalAgility which clients can invoke.
 - The system generates a summary of log, `TungstenTotalAgilityMultiTenancySilentInstall.txt`, on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.
 - 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 as a silent installation, one of the codes returns to indicate the following:
 - 0=Success
 - 1=Success with warnings
 - 2=Failure

Standard installation of TotalAgility On-Premise Multi-Tenancy

You can install TotalAgility On-Premise Multi-Tenancy using the standard installer wizard.

- [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 \(RTTS\)](#)

TotalAgility On-Premise Multi-Tenancy supports SQL Server authentication or Windows authentication. For higher security when deploying TotalAgility On-Premise Multi-Tenancy, SQL Server authentication can be used where separate users are created for each tenant database. If required, Windows authentication can be used but this means each tenant database will be accessed with the same Windows service account.


There are separate production, additional deployment and Reporting schemas per tenant database if using SQL Server authentication. There are separate production (Live), additional deployment and Reporting databases per tenant if using Windows authentication.

Standard installation of Database Only

1. From your TotalAgility installation files, 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 **Tungsten 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 **Software License Agreement** window, accept the terms in the License Agreement and click **Next**.
4. In the **Type of Install** window, select **Database Only** (default: Web/Application Server) and click **Next**.
The **Databases** window opens.
5. By default, **Install Databases** (read-only) option is selected. Do the following:
 - a. Enter the name of the MasterTenants database. The name should match the MasterTenants database created by the Tenant Management System installer.

i Make sure the Tenant Management System installer is already run to create the MasterTenants database.

- b. Enter the database name for the DataCenter database.
- c. Enter the **Production Deployment Hostname** in the following format: <Fully qualified domain name: port>. This should be the Production Web Server machine name.
- d. If the database with the same name already exists, and if you want to overwrite the existing database, select **Overwrite databases if they exist?**.
The **Test connections** option becomes available.
- e. 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.

- f. 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** to connect to the database, or select the **SQL Server Authentication** (default) providing the username and password, and then click **OK**. If all the databases reside on the same server, select **Apply these settings to all other Databases**.
6. Click **Next**.
The **DB Connection Results** window opens and displays the results of connecting to databases.

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

7. Click **Next**.
The **Capture Binary Data Storage** window opens.
8. By default, binary data such as Capture documents, .NET Store DLLs, and TCM 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 binary data. The cloud services helps reduce the SQL Server maintenance costs, delegate maintenance to external service and provide encryption.

i 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.

Storage type	Description
Windows Azure Blob Storage	<p>Stores Capture data in Azure Blob Storage service.</p> <p>Under Cloud Account Settings, enter the Account Connection String to connect to the Blob storage service.</p> <p>i The Container name for Capture data storage is automatically created by the installer.</p>
Amazon S3	<p>Configure the following Cloud Account Settings:</p> <ol style="list-style-type: none"> Enter the Access Key to connect to the Amazon S3 storage service. Enter the Secret Key. On the Region list, select a predefined S3 region, for example Asia Pacific (Sydney). (Default: US East (Ohio)) <p>i The Bucket name for data storage is automatically created. Bucket is a fundamental container in Amazon S3 for data storage.</p>

9. Click **Next**.

The **Installation Review** window opens and displays the installation type as Database Only Install.

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.

11. Click **Finish**.

Your installation is now complete.

i If any errors occur, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt, on the desktop. Fix those errors and repeat the above steps.

Standard installation for upgrading databases

1. From your TotalAgility installation files, 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 **Tungsten 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 **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) and click **Next**.
The **Databases** window opens.
5. 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 username and password, and then click **OK**. If all the databases reside on the same server, select **Apply these settings to all other Databases** and click **OK**.
6. Click **Next**.
The **Installation Review** window opens.
7. Review the settings and click **Next** to start the installation.
The **Installation Progress** window displays the progress of the installation. The setup upgrades TotalAgility databases.
If any errors occur, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt, on the desktop. Fix those errors and repeat the above steps.
8. Click **Finish**.
Your installation is now complete.

Standard installation of Web and Application on the different servers

Install TotalAgility on a separate Web or Application server.

This section describes the standard installation for the following installation types:

- [Standard installation of the Web Server](#)
- [Standard installation of the Application Server](#)

Standard installation of the Web server

Perform a standard installation on a Web Server.

1. From your installation files, 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 **Tungsten 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 **Software License Agreement** window, accept the terms in the License Agreement and click **Next**.
4. In the **Type of Install** window, select **Web Server** (default: Web/Application Server) and click **Next**.
The **Environment Type** window opens.

5. Select the mode of environment to setup. Available options are:
 - **Production deployment** (default): Installs the production environment. You can choose to install the Tenant Management System while installing On-Premise Multi-Tenancy or as a separate installation by running the setup from the `TenantManagementInstall` folder from your TotalAgility installation files. To install now, select **Install Tenant Management components** (default: Clear), click **Next** and follow the wizard instructions to install the Tenant Management components.
 - **Additional deployment (non-production)**: If selected, installs the additional deployment.
6. Click **Next**.

The **Software Checks** window opens. 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.

Tungsten TotalAgility will be installed into the selected folder path.
9. Click **Next**.

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

i 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 the Production environment, 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 additional deployment, 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.

i 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.

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`.
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.

If any errors occur, by default, TotalAgility creates a log file,

TungstenTotalAgilityInstallErrorLog.txt, 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)

The system automatically connects to the backup license server if the primary license fails.


- Transformation Server

1. From your TotalAgility installation files, 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 **Tungsten 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 **Software License Agreement** window, accept the terms in the License Agreement and click **Next**.

4. In the **Type of Install** window, select **Application Server** (default: Web/Application Server) and click **Next**.

The **Environment Type** window opens.

5. Select the mode of environment to setup. Available options are:

- **Production deployment** (default): Installs production environment. You can choose to install the Tenant Management System while installing On-Premise Multi-Tenancy or as a separate installation by running the setup from the `TenantManagementInstall` folder from your TotalAgility installation files. To install now, select **Install Tenant Management components** (default: Clear), click **Next** and follow the wizard instructions to install the Tenant Management components.
- **Additional deployment (non-production)**: If selected, installs the additional deployment. Enter a **Name** for the additional deployment. The additional deployment name should not exceed 10 characters and cannot contain special characters.

6. Click Next.

The **Application Server** window opens.

7. 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
- Transformation Service

i 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.

- Import Service
- License Service (Primary license server or Backup license server, and Enable SSL)
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 running the Configuration Utility post TotalAgility installation to automatically update the setting. See [Update the settings for a license server](#).
For the License service, enable SSL and provide the thumbprint of a correctly configured certificate on the computer on which you install TotalAgility. If you enable SSL and provide the certificate, the License server screen automatically displays the port as 3582.

The WCF Services include Core Services.

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.

Tungsten TotalAgility will be installed into the selected folder path.

11. Click Next.

The **Credentials** window opens.

12. In the Credentials window, enter the credentials for the user who will run TotalAgility On-Premise Multi-Tenancy.**13. Click Next.**

The **Databases** window opens.

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

For additional deployment environment mode, you must only provide data center databases.

- a. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**.
- b. If you are not using the local server, click the ellipsis and select the DataCenter databases.
- c. 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 username and password, and then click **OK**.

i 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.

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 *Tungsten TotalAgility Configuration Utility Guide*.

15. Once the databases are successfully pointed, click **Next**.
The **Install Options** window opens.
16. To automatically start the services, keep the **Automatically Start Services** check box selected.
17. Click **Next**.
The **Installation Review** window opens and displays the settings.
18. 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.
19. To connect to the License Server, do one of the following:
 - To use the existing licenses associated with the deployments of the on-premise multi-tenancy data center, select the **Use existing license** checkbox and select a license on the **License Server** list; enter the port number on which the License Server listens and then click **Next**.
The **Tungsten TotalAgility Multitenancy Installation Complete** window displays the summary of the installation.
 - 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. In the **Port Number** field, enter the port number on which the License Server listens and **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.
20. Enter your TotalAgility **Serial Number** and **Product Code**.

i 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.

21. 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 Tungsten Automation 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 **Tungsten 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 Tungsten Automation can send the information you need to activate the product license.
 - d. Click **Next** to proceed with the activation process.

i Ignore the **Version** selection field if you do not have Tungsten 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 the license. If you skip activating the license, a warning appears that you need to activate the license later.

i 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 **Tungsten TotalAgility Installation Complete** window displays the summary of the installation.

i If any errors occur, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt, on the desktop. Fix those errors and repeat the above steps.

22. 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.

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

23. Click **Yes** to install the Transformation Server.

The installation for Transformation Server is launched. See [Transformation Server Bundle installation](#).

Standard installation of the Web and Application on the same 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)

The system automatically connects to the backup license server if the primary license fails.


- Transformation Server

1. From your TotalAgility installation files, 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 **Tungsten 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 **Software License Agreement** window, accept the terms in the License Agreement and click **Next**.

4. In the **Type of Install** window, select **Application Server** (default: Web/Application Server) and click **Next**.

The **Environment Type** window opens.

5. Select the mode of environment to setup. Available options are:

- **Production deployment** (default): Installs production environment. You can choose to install the Tenant Management System while installing On-Premise Multi-Tenancy or as a separate installation by running the setup from the `TenantManagementInstall` folder from your TotalAgility installation files. To install now, select **Install Tenant Management components** (default: Clear), click **Next** and follow the wizard instructions to install the Tenant Management components.
- **Additional deployment (non-production)**: If selected, installs the additional deployment. Enter a **Name** for the additional deployment. The additional deployment name should not exceed 10 characters and cannot contain special characters.

6. 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
- Transformation Service
- Import Service (Instance 2 and Instance 3)

- License Service (Primary license server or Backup license server, and Enable SSL)

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.

For License service, enable SSL and provide the thumbprint of a correctly configured certificate on the computer on which you will install TotalAgility. If you enable SSL and provide the certificate, the License server screen will automatically display the port as 3582.

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 **Credentials** window opens.

10. 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.

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`.

11. Click **Next**.

The **Databases** window opens.

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

For an additional deployment environment, you must only provide Datacenter 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.

i 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**. The databases are created in the following format when tenants are created:
 - TotalAgility_Main_Live_TenantName
 - TotalAgility_Reporting_Live_TenantName
 - TotalAgility_Reporting_staging_Live_TenantName
 - TotalAgility_Documents_Live_TenantName

i This setting is not related to tenant users logging on to TotalAgility Designer or Workspace. Windows authentication is not supported in on-premise multi-tenant environment for end users unless it is via Federated security.

- 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 username 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 *Tungsten TotalAgility Configuration Utility Guide*.

13. Click Next.

The **DB Connection Results** window opens.

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

14. Click Next.

The **Capture Binary Data Storage** window opens.

- 15.** By default, binary data such as Capture documents, .NET Store DLLs, and TCM 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 binary data. The cloud services helps reduce the SQL Server maintenance costs, delegate maintenance to external service and provide encryption.

i 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. i The Container name for Capture data storage is automatically created by the installer.
Amazon S3	Configure the following Cloud Account Settings : <ul style="list-style-type: none"> 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)) i The Bucket name for data storage is automatically created. Bucket is a fundamental container in Amazon S3 for data storage.

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

i 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.

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

18. Click **Next**.

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

19. 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.

20. To connect to the License Server, do one of the following:

- To use the existing licenses associated with the deployments of the on-premise multi-tenancy data center, select the **Use existing license** checkbox and select a license on the **License Server** list; enter the port number on which the License Server listens and then click **Next**.


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

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

21. 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.

22. 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 Tungsten Automation 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 Tungsten Automation 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 Tungsten Automation 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 Tungsten Automation 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 **Tungsten TotalAgility Multitenancy Installation Complete** window displays the summary of the installation.

i If any errors occur, by default, TotalAgility creates a log file, `TungstenTotalAgilityInstallErrorLog.txt`, on the desktop. Fix those errors and repeat the above steps.

23. 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.

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

24. Click Yes to install the 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. From your TotalAgility installation files, 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 **Tungsten 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 **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 Service** (default: Web/ Application Server) and click **Next**.
The **Environment Type** window opens.
5. Select the mode of environment to setup. Available options are:
 - **Production deployment** (default): Installs production environment.
 - **Additional deployment (non-production)**: If selected, installs the additional deployment. Enter a **Name** for the additional deployment. The additional deployment name should not exceed 10 characters and it cannot contain special characters.
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.

i 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.

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`.

11. Click **Next**.

The **Databases** window opens.

12. Enter the database name for the **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 **Use SQL Server Authentication**, provide the username and password, and then click **OK**.

The user name and password credentials belong to the TenantName_schema user created by the Tenant Management System 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.

i 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.

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.


If any errors occur, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt, on the desktop. Fix those errors and repeat the above steps.

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 Tungsten 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}.OPMAppServerHostNameGoesHere/
TotalAgility/services/core/{R:1}" logRewrittenUrl="false" />
      <conditions trackAllCaptures="true">
        <add input="{HTTP_HOST}" pattern="([^.]*)(.*)" />
      </conditions>
    </rule>
  </rules>
</rewrite>
```

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


Language pack installation

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

```
\\OnPremiseMultiTenancyInstall\Agility.Server.Web\LocalizationFiles
```

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.

 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.

Chapter 3

TotalAgility installation in a Docker container

This chapter describes the prerequisites, limitations, procedure for creating and running a Docker container, and silent installation configuration.

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 allow you to run many containers simultaneously on a given host using fewer resources than virtual machines.

You can deploy the TotalAgility application into your production environment, as an independent container or orchestrated set of containers. This works the same whether your production environment is a local data center, 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, but it does not run in the TotalAgility container.

Limitations

The Export Connectors are not supported in a Docker environment.

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 are set up and remotely accessible (using either an IP address or a fully qualified domain name).

To use this setup, configure the following on the SQL Server being used:

- Firewall should allow remote access to SQL Server
- Configure SQL Server to allow remote access with Mixed mode since the user is also allowed to access without Windows Authentication.
- Enable TCP/IP protocols for SQL Server.

i The "Named Pipes" protocol does not work.

Install Docker on the Windows server

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

i 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 relevant command to install Docker on the Windows server.

i If you use the "Key Value Pairs" extraction feature in Quick Capture or use the Key Value Pairs locator in the Transformation Server, you must run the following command:

```
docker pull mcr.microsoft.com/windows
```

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 to resolve DNS for all the tenants to communicate with the App container. Resolving DNS can either be done by modifying the "hosts" file on the 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/dotnet/framework/aspnet` for all the TotalAgility container types (including RTTS and Transformation Server), where the "Image Quality Analysis, Mobile ID, and Mobile Card Capture" are required.

Make the following changes in the Docker file:

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



- Additionally, Mobile ID and Mobile Card Capture have a prerequisite for the VC++ 2013 x86 redistributable. This can be automatically downloaded and installed in the Docker file.
- Make sure that the 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 operating system 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.

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

1. Extract the contents of Tungsten TotalAgility-8.1.0_OPMT.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](#).

i When you create a Docker image for the Transformation Server, and use the "Key Value Pairs" extraction feature, you must update the Docker file as follows for the feature to work: Remove the first line `FROM mcr.microsoft.com/dotnet/framework/aspnet` from the Docker file and add `FROM mcr.microsoft.com/windows/server`.

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

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

i 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 "totalagilityopmt" using the contents inside `C:\Docker\TotalAgility`:

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


Perform silent installation of TotalAgility in a Docker container



1. From your TotalAgility installation files, 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](#)

i 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 server in a Docker container

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	
TransformationService	true	<p> If this parameter is set to true, you must copy the fonts by running the PowerShell script from the following path: <code><Working directory>/containerfiles/powershellscripts/copyfonts.ps1</code>. By running the script, the fonts are copied from <code>Windir/fonts</code> to <code><Working directory>/containerfiles/powershellscripts/fonts</code> on the Docker container for PDF generation.</p>
CoreServices	true	
InstallTenantManagement Web site	false	<p>Accept the default. Set to true to install the Tenant Management System.</p> <p> You must pre-configure the parameters in the <code>SilentInstallConfig.xml</code> for Tenant Management System. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.</p>
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten 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 Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA). <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p> </div>
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 Tungsten Automation@Tungsten Automationindiapvtlimited.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, Tungsten Automation@Tungsten Automationindiapvtlimited.com.
StartServices	false	Since we expect the services to be started only after the container is running.

Application Server (Core Services and Core Worker) in a Docker container



Update the following parameters for the Application server installation.

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

Parameter	Value	Description
InstallTenantManagement Website	false	Accept the default. Set to true to install the Tenant Management System. <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #cfe2f3;"> <p>i You must pre-configure the parameters in the SilentInstallConfig.xml for Tenant Management System. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.</p> </div>
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten 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 Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA). <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #cfe2f3;"> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p> </div>
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 abc@TungstenAutomation.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, abc@TungstenAutomation.com.
StartServices	false	Since we expect the services to be started only after the container is running.

Web Server in a Docker container

Update the following parameters for the Web Server installation.

Parameter	Value	Description
InstallTenantManagement Web site	false	Accept the default. Set to true to install the Tenant Management System.  You must pre-configure the parameters in the SilentInstallConfig.xml for Tenant Management System. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten TotalAgility services run as the LocalSystem account. This can also be used to run the container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	When set to true, the IIS AppPool and Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA).  If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the 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) in a Docker container

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

Parameter	Value	Description
ServicesInstallOptions		

Parameter	Value	Description
LicenseService	false	
CoreWorkerService	true	
ReportingService	false	
TransformationService	false	
CoreServices	true	
InstallTenantManagement Web siteUpdateDatabases	false	<p>Accept the default. Set to true to install the Tenant Management System.</p> <p>i You must pre-configure the parameters in the SilentInstallConfig.xml for Tenant Management System. See the <i>Tungsten TotalAgility Tenant Management System Installation Guide</i> for more information.</p>
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten TotalAgility services run as the LocalSystem account. This can also be used to run the container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	<p>When set to true, the IIS AppPool and Tungsten 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).</p> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p>
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 abc@Tungsten Automation.com.
Password	password	Enter the password.
FromAddress	from address	Enter the email address from which the email is triggered. For example, abc@Tungsten Automation.com.

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

Reporting Server in a Docker container

Update the following parameters for the Reporting Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	false	
ReportingService	true	
TransformationService	false	
CoreServices	false	
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten 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 Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA). <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p> </div>
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after the container is running.

License Server in a Docker container

Update the following parameters for a License Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	true	
CoreWorkerService	false	
ReportingService	false	
TransformationService	false	
CoreServices	false	
DatabaseInformation		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten 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 Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA). <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p> </div>
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after the container is running.

Transformation Server in a Docker container

Update the following parameters for a Transformation Server installation.

Parameter	Value	Description
ServicesInstallOptions		
LicenseService	false	
CoreWorkerService	false	
ReportingService	false	

Parameter	Value	Description
TransformationService	true	<p>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/powershellscripts/copyfonts.ps1. By running the script, the fonts are copied from Windir/fonts to <Working directory>/containerfiles/powershellscripts/fonts on the Docker container for PDF generation.</p>
CoreServices	false	
Database Information		
UpdateDatabases	false	Skips installing databases as part of the Docker image installation.
Identity Information		
RunAsSystemAccount	true	When set to true, the IIS AppPool and Tungsten TotalAgility services run as the LocalSystem account. This can also be used to run the container as a Group Managed Service Account (gMSA).
RunAsNetworkServiceAccount	false	<p>When set to true, the IIS AppPool and Tungsten TotalAgility services run as the NT Authority\Network Service account. This can also be used to run the container as a Group Managed Service Account (gMSA).</p> <p>i If RunAsSystemAccount or RunAsNetworkServiceAccount is true, this can be used to run the container as a Group Managed Service Account (gMSA).</p>
Install Info		
InstallType	ApplicationServer	
StartServices	false	Since we expect the services to be started only after the container is running.
TS_INSTALL_NLP_WESTERN	false	If set to true, installs the Natural Language Processing language bundle for English, Spanish, Portuguese, French, and German.
TS_INSTALL_NLP_ADDITIONALALLLANGUAGES1	false	If set to true, installs the Natural Language Processing language bundle for Italian, Romanian, and Dutch.
TS_INSTALL_NLP_ADDITIONALALLLANGUAGES2	false	If set to true, installs the Natural Language Processing language bundle for Japanese, Chinese, and Korean.
TS_INSTALL_NLP_ADDITIONALALLLANGUAGES3	false	If set to true, installs the Natural Language Processing language bundle for Swedish, Finnish, Danish, Norwegian, and Arabic.

i 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 in a Docker container

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

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

i 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 to the *Tungsten TotalAgility Configuration Utility Guide* for more information.

i 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 totalagilityopmt image. Tungsten TotalAgility settings are applied from the 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:\Dockers\TotalAgility\dockersettings.env" -p 5000:443 totalagilityopmt
```

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

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

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:\Dockers\TotalAgility\dockersettings.env" -p 5000:80 -p 3581:3581 totalagilityopmt
```

i If running the License Server in a container, the associated license serial number must be activated before the Tungsten 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 the 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:\Dockers\TotalAgility\dockersettings.env" -p 5000:80 -p 5003:25086 totalagilityopmt
```

i 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 hold 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-MC Stop-service KIC-ED-MC`

Useful Docker commands

This table includes some useful Docker commands.

Docker command	Purpose
<code>docker images</code>	Gets the list of all Docker images currently available on the server.
<code>docker ps -a</code>	Gets a list of all containers available on the server.
<code>docker start <containerID></code>	Starts the container with the ID <containerID> on the server.
<code>docker stop <containerID></code>	Stops the container with the ID <containerID> on the server.
<code>docker rm <containerID></code>	Deletes the container with the ID <containerID> on the server.
<code>docker rmi <imagename></code>	Deletes the image with the ID <imagename> on the server. Deletion is successful only if no child containers use this image.
<code>docker inspect -f "{{ .NetworkSettings.Networks.nat.IPAddress }}" <containerID></code>	Gets the IP address of the container with the ID <containerID>.
<code>docker cp "<containerID>:/<fullfilepath oncontainer>" "<pathtofolderonserver>"</code>	Copies a file from the container to the server.
<code>docker cp "<fullfilepathonserver>" "<containerID>:/ <fullfilepathoncontainer>"</code>	Copies a file from server to the container.
<code>docker logs <containerID></code>	Displays all logs for a particular container.
<code>docker logs - tail n <containerID></code>	Displays the last "n" logs for a particular container.
<code>type <FQDN of text file></code>	Displays the content of text file within powershell instance.
<code>Get-Process</code>	Gets the list of all processes.
<code>Get-Service</code>	Gets the list of all services (running and stopped).
<code>start-service <ServiceName></code>	Starts a particular service.
<code>Stop-service <ServiceName></code>	Stops a particular service.
<code>Get-WMIObject Win32_Service select starname, name, status</code>	Gets the list of all services with some additional columns.
<code>Get-EventLog -LogName Application -newest 10 format-table -auto -wrap</code>	Gets the last 10 application logs from event viewer.
<code>import-module webadministration</code>	Runs before the following commands.

Docker command	Purpose
get-iisappool	Gets the name of the Application pool.
get-itemProperty -path IIS:\APPPools \TotalAgilityAppPool -names	Gets the identity information of the Application pool.

Use secrets

You can use one of the following secrets to store sensitive information, such as database connection strings, passwords, and more.

- Kubernetes
- Docker
- AWS

Use Kubernetes secrets

If you are using Kubernetes secrets, you must make some changes before building the Docker images and deploying them to Kubernetes. For example, consider using the `MainDBConnectionString` application setting as the secret.

You can use Kubernetes secrets as volumes or environmental variables.

Use Kubernetes secrets as volumes

1. Create a secret `<maindbsecret>` in Kubernetes that contains the `MainDBConnectionString` details. Refer to the Kubernetes documentation to create a secret.
2. From the Docker container installation files, navigate to `\\Utilities\docker\ContainerFiles\PowershellScripts\`. Replace the line `"$appSetting.value = $_.Value;"` with the following lines which will check for the 'maindbconnectionstring' setting and update its value in all the Tungsten 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;
    }
}
```

i All the corresponding `MaindbConnectionString` values in the `DockerSettings.env` no longer need to be provide, as they are 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>`, such as `</ta/maindb/>` in the container. Refer to the Kubernetes documentation 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:\ta\maindb\` in the container and also updates the corresponding TotalAgility configuration file settings with the secret value.

Use Kubernetes 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`, such as `"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 to add as an environment variable.
3. Similarly, multiple environment variables can be added to the pod definition that needs the value from a secret. No changes are needed to the script files.

Use Docker secrets

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

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

1. Create a secret `<maindbsecret>` in the swarm that contains the `MainDBConnectionString` details. Refer to the Docker documentation to create a secret.
2. From the Docker container installation files, 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 check for the 'maindbconnectionstring' setting and update its value in all the Tungsten 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 need to be provided, as they are 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 the corresponding settings of the Tungsten TotalAgility configuration files with the secret value. Refer to the Docker documentation to create a service.

Use AWS secrets

If you are using AWS Secrets to store sensitive information, such as database connection string, and passwords, you can dynamically retrieve the secrets from the container 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.

Use AWS Tools for PowerShell

If using AWS secrets via AWS Tools for PowerShell, do the following changes.

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. From the Docker installation files, 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 update the contents of the `<mainsecret>` retrieved from the 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 following lines which check for the ‘maindbconnectionstring’ setting and update its value in all the Tungsten 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 following script lines before the 'Update-License-Config' function which cleans 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 the script above as environment variables. Docker commands mentioned in the Run a Docker container section must now also pass in these **--env** variables along with the **--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>
```

i All the corresponding MaindbConnectionString values in the DockerSettings.env no longer need to be provided, as they are 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 Tungsten 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.

Use Custom Library

If using AWS secrets via custom library, do the following changes.

1. Create a secret <mainsecret> in AWS Secret Manager that contains the MainDBConnectionString details.
Refer to the 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 awsSecretAccessKey,
string region , string awsSecretName)
{
    string secret = string.Empty;
    IAmazonSecretsManager client = new
AmazonSecretsManagerClient(awsAccessKeyId, awsSecretAccessKey,
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. From the Docker installation files, navigate to \\TungstenTotalAgility-8.1.0_OPMT\Utilities\Docker\ContainerFiles\PowershellScripts\ and copy the utility DLL files: AWSSecretManager.dll, AWSSDK.Core.dll and 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:\TA\PowershellScripts
\AWSSecretManager.dll")
$add = [Reflection.Assembly]::LoadFile("C:\TA\PowershellScripts
\AWSSDK.SecretsManager.dll")
$add = [Reflection.Assembly]::LoadFile("C:\TA\PowershellScripts\AWSSDK.Core.dll")

$sawsAccessKeyId = [Environment]::getEnvironmentVariable('KTA_AWS_ACCESSKEYID');
$sawsSecretAccessKey =
[Environment]::getEnvironmentVariable('KTA_AWS_SECRETACCESSKEY');
$sawsRegion = [Environment]::getEnvironmentVariable('KTA_AWS_REGION');
Set-AWSCredential -AccessKey $sawsAccessKeyId -SecretKey $sawsSecretAccessKey
Initialize-AWSDefaultConfiguration -Region $sawsRegion

$sawsMainSecretName =
[Environment]::getEnvironmentVariable('KTA_AWS_MAINSECRETNAME');
Try {
    $sawsMainSecret_response =
    [AWSSecretManager.AWSSecretManager]::GetAWSecret($sawsAccessKeyId,
    $sawsSecretAccessKey, $sawsMainSecretName)
}
Catch {
    Write-Host "Exception:."
    Write-Host $_.Exception
}
$mainSecretJsonobj = ConvertFrom-Json -inputObject
    $sawsMainSecret_response.SecretString

```

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

```

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

```

- 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);

```

- Save the changes.
- When running the Docker container, pass the `KTA_AWS` variables mentioned in the script above as environment variables. The Docker run commands mentioned in the Run a Docker container section must now also pass in these `--env` variables along with the `--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>

```

i All the corresponding `MaindbConnectionString` values in the `DockerSettings.env` no longer need to be provided, as they are pulled from the secrets.


- When the container is running, it should get the secret `<mainsecret>` which contains the connection string value and also updates the corresponding Tungsten TotalAgility configuration file settings with the secret value.
- Similarly, you can update the `UpdateConfigAppSettings.ps1` script file and the Docker run command to get other application settings from the AWS secret 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 exporting certificates.

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 the password file using a mapped volume, do the following:
 - a. Create a new text file, such as password.txt in 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 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:
 - `docker run --env-file "C:\Docker\TotalAgility\dockersettings.env" -e KTA_SSL_CERT_PASSWORD="password" -e KTA_SSL_CERT_PATH="HostMachineFolder\CertificateName.pfx" -v "HostMachineFolder:ContainerFolder" -p 5000:443 -d tungsten/ta_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 tungsten/ta_771`
 - d. Replace HostMachineFolder with the actual certificate path on the host machine.
 - e. Replace CertificateName with the actual certificate name.
 - f. Replace ContainerFolder with the actual folder path 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 is configured to run as LocalSystem or NetworkService accounts.

When running as LocalSystem or NetworkService 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 pools. This account will be used when the container is built.

Ensure the following prerequisites are met:

- Add the Docker server, SQL Server machine, and machines that will use gMSA under the required domain controller.
- Add these machines to the Active Directory under the Computer folder.
- Create a Global Security group, such as ContainerHostGroupName in the Active Directory under the Builtin folder.
- Add the Docker server, SQL Server machine, or machines that will use gMSA as members of 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 the 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. Log in to the domain controller and execute the following command:

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

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

b. Verify the new gMSA account using the following command:

```
Get - ADServiceAccount - Identity containerhost
```

c. A new gMSA object appears in your domain's Managed Service Account.

3. Add a 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 security and click **Add**.

- d. Select the computers where you want to use gMSA, such as the Docker server and the SQL Server machine.
- e. Reboot the Domain controller for the changes to take effect.
- f. Reboot the computers that will be using gMSA.

4. Install gMSA Account on servers.

- a. Log in to the machine that will be used as the 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 similar to the following:

```
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 the Chrome browser. If you skip this step, authentication still works but will always prompt for username/password since it will fall back to NTLM.

GMSA account: containerhost

Domain name: TotalAgilityexample .com

Container host machine: machine1

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

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

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

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

7. Generate a credential specifications file that must be passed to Docker during container creation to use this service account. Run the following commands to download the module which creates this file from a Microsoft GitHub account and creates a JSON file containing the required data.

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

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

import-module $env:temp\cred.psml

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 the domain name as "TotalAgilityexample.com" and run the following SQL commands on your SQL database:

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

To create a user for all the TotalAgility databases:

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

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

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

Chapter 4

Transformation Server bundle installation

The Transformation Server bundle includes:

- Transformation Server
- Transformation Core modules

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

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

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 *Tungsten TotalAgility Configuration Utility Guide*.


Prerequisites

For prerequisites, see the *Tungsten TotalAgility Prerequisites Guide*. For additional prerequisites, see the following sections.

Before installing the Transformation Server Bundle, make sure to do the following:

- Install the USERTrust Certificate and the DigiCert Assured ID Root CA Certificate in your environment. The installation may fail if these certificates are missing.
- For additional environments, install the Transformation Server Bundle where you installed TotalAgility. For production environments, install the Transformation Server Bundle on a separate computer.
- If you are using Oracle, install the Oracle Data Provider on every server where the Transformation Server is installed. You can get the Oracle Data Provider from the Oracle website.
- If you install the Transformation Server 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 administrative privileges and "Log on as Service" rights. This user 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.
- A user can run Transformation Server as a non-admin if the user account is part of Windows Group: Users, and has the following privileges:
 - Local Security Policy rights: Log on as Service.
 - Full access to the log file folder configured for logging. By default, this folder is the installation folder.

- Full access to the following folders:
 - C:\ProgramData\Tungsten
 - C:\Program Files\Tungsten\TotalAgility\Transformation Server

 This folder contains "Transformation.ServiceHost.exe.config."

- The following rights to the database:
 - db_reader
 - db_writer
 - Execute permission

User Accounts for Transformation Server

For security, Transformation Server uses a single user group per computer and a single user account per tenant. The first time the 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 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.

Configure the user account

For an on-premise multi-tenant installation, 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 the 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 the Transformation Server will be using for each of these settings.

Silent installation of Transformation Server

This section describes the steps to silently install the Transformation Server bundle without any interaction with TotalAgility. For additional deployment 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.

i 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_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% TS_INSTALL_OCR_ADDONS=1%
TS_INSTALL_NLP_WESTERN=1 %TS_INSTALL_NLP_ADDITIONALLANGUAGES1=1%
TS_INSTALL_NLP_ADDITIONALLANGUAGES2=1%
TS_INSTALL_NLP_ADDITIONALLANGUAGES3=1% (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](#).

i 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;
TS_INSTALL_OCR_ADDONS=1
```

```

TS_INSTALL_NLP_WESTERN=1
TS_INSTALL_NLP_ADDITIONALLANGUAGES1=1
TS_INSTALL_NLP_ADDITIONALLANGUAGES2=1
TS_INSTALL_NLP_ADDITIONALLANGUAGES3=1

```

Standard installation of Transformation Server

Use the Installation Wizard to install and configure Transformation Server for a multi-tenant configuration. Before you start the installation, ensure that all requirements including the access permissions and privileges required to run Transformation Server service are fulfilled. [Configure the user account](#).

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

You must have administrator privileges to run the Transformation Server on-premise multi-tenancy on all Windows (Server) operating system.

i When running Transformation Server as a non-admin account, certain protections meant to sandbox tenant processes that run user-submitted scripts are not used.

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 \\TungstenTotalAgility-8.1.0\TransformationServer from the installation files and run **TransformationServerSetup.exe**.

The Transformation Server is installed and the log file is available in the temp folder.

i To install the Transformation Server with the log file at a specific location 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 installer opens automatically.

The Tungsten Automation Transformation Server bundle window appears

i 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 **Tungsten Transformation Server 8.1.0** Setup window, click **Options** and do the following:

The following settings are available:


Setup Options

Multitenant installation	If selected, installs Transformation Server in an on-premise multi-tenant environment. (Default: Clear)
Additional A2iA engines [unsupported]	If selected, installs the A2iA recognition engine. (Default: Clear)
Natural Language Processing language bundles	
Western (en, es, pt, fr, de) (default: selected)	If selected, installs the natural language processing language bundles.
Additional Languages 1 (it, ro, nl)	
Additional Languages 2 (ja, zh, ko)	
Additional Languages 3 (ar, da, fi, no, sv)	

3. Select **Multitenant installation** and click **OK**.
You return to the first window.
4. 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.

5. In the welcome screen, click **Next**.
The **Welcome to the Tungsten Transformation Server 8.1 Setup Wizard** window appears.
6. Click **Next**.
The **End-User License Agreement** window appears.
7. In the license agreement window, accept the terms in the license agreement and click **Next**.

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

The **Destination Folder** window appears where you select the folder where Transformation Server is installed.

8. 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**.
The **Service account setup** window appears where you can enter the user credentials to run the Transformation Server service.
9. On the **Service account setup** window, 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**.
The **Setting up connection data** window appears where you can configure your connection to the TotalAgility tenant.
10. Enter the **Connection string for the tenants database** for your tenant if you are installing Transformation Server separately from TotalAgility.
If you are installing Transformation Server as part of the TotalAgility installation, the connection string for the tenant database is automatically displayed.
11. Optionally select **Use Windows authentication for tenant databases** if you want to use Windows authentication to connect to your tenant.
12. From the **Select environment** list, choose which environment to use.

If you select **Additional deployment (non-production)** then a **Name** field is displayed where you can enter the name of another non-production deployment.

13. Click Next.

The **Connection options to TotalAgility Server** window appears so you choose whether or not to use online learning.

14. If you do not want to use online learning for this Transformation Server instance, clear **Enable Online Learning processing by this Transformation Server instance. Otherwise, leave the field selected. Click Next.**

The **Advanced execution options** window appears.

15. In the **Advanced execution options window, configure the following advanced execution options:**

- **Enable support for Quick Capture** (Default: Selected):
- **Enable synchronous calls processing** (Default: Selected): 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.
- **Override default number of processing slots** (Default: Clear): To specify a number of slots other than the default.

Click **Next**.

The **Ready to install Tungsten Transformation Server 8.1.0** window appears.

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

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

17. Click **Finish.**

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

18. 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 TotalAgilty.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 TotalAgility.EncryptConfig.exe

The TotalAgility.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 TotalAgility.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:

```
TotalAgility.EncryptConfig.exe -f Transformation.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 (TASession 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:

- Log on to the Transformation Server as the Transformation Server service user.
- Navigate to the installation directory for the Transformation Server and open a Command Prompt window.

c. Run the following command:

```
TotalAgility.EncryptConfig.exe -f
Transformationh.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:

- Log on to the Transformation Server with administrator rights.
- Copy the keys.xml file from the source Transformation Server to the root directory of the target Transformation Server.
- Open a Command Prompt window.
- 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.
- 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:

```
TotalAgility.EncryptConfig.exe -f Transformation.ServiceHost.exe.config -s
"appSettings" -p DPAPIProtection -deC
```

Edit the configuration file

Modify the Transformation Server configuration file, **Transformation.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 **Transformation.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="TransformationServerLog.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](#).

i 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 Tungsten Automation 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 Tungsten NLP engine language packs on the machine where Transformation Designer is installed. This is because the Tungsten NLP engine language packs are installed by the Transformation Server bundle only, and these languages are required to use the Tungsten NLP functionality in Transformation Designer and in production.

1. From your TotalAgility installation directory, navigate to `C:\Program Files (x86)\Common Files\Tungsten\Salience7.0`.
2. Double-click on one of the following `.msi` files depending on the languages you are supporting.

TungstenTransformation_Salience7.0_LanguageBundle_western-default.	Installs English, German, French, Spanish, and Portuguese language support.
TungstenTransformation_Salience7.0_LanguageBundle_additionalLanguages1.	Installs Italian, Dutch, and Romanian language support.
TungstenTransformation_Salience7.0_LanguageBundle_additionalLanguages2.	Installs Japanese, Korean, and Mandarin language support.
TungstenTransformation_Salience7.0_LanguageBundle_additionalLanguages3	Installs Swedish, Finnish, Danish, Norwegian, and Arabic language support.

A Windows Installer window appears and then installs the selected Tungsten NLP languages automatically.

The installer window closes when the installation is complete.

3. Follow the same procedure if you want to support additional languages.

Upgrade Transformation Server using silent installation

To upgrade the Transformation Server in silent mode, use the following command, replacing the example content with your environment.

```
setup.exe /quiet /Upgrade /log installation.log TS_SERVER_SERVICE_URL=http://<Server>/TotalAgility/Services/Core/ServerService.svc TS_INSTALLLOCATION="<Program Files>\Tungsten\TotalAgility\Transformation Server"
TS_MAIN_DB_CONNECTION_STRING="Server=servername;Database=databasename;User Id=sa;Password=password" TS_SERVICE_ACCOUNT=serviceAccountName
TS_SERVICE_PASSWORD=password TS_STARTSERVICE=TRUE
```

Uninstall the Transformation Server

Uninstall the Transformation Server depending on how you have installed it.

- When you install Transformation Server as part of Tungsten 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 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.

Chapter 5

Message Connector installation

This chapter provides the instructions for installing the Message Connector.

Prerequisites

For information on prerequisites for the Message Connector, see the *Tungsten TotalAgility Prerequisites Guide*.

Deployment scenarios and advanced configuration

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

System limits

The following are the system limits that apply to 64-bit installations. For 32-bit installations, the limits might be lower.

Maximum size of a message in Message Connector storage	250 GB
Maximum number of Message Connector instances on a single computer	3
Maximum usage limit for Kofax Converter system memory. However, while processing an input file, the memory usage may vary depending upon the following factors: <ul style="list-style-type: none">• Number of pages in the document• Document type• Conversion type	4 GB

Install multiple instances of Message Connectors

You can install up to three instances of Message Connector on a computer in a Silent mode. The first instance of Message Connector is installed automatically with Tungsten TotalAgility setup.

However, depending on the TotalAgility version installed or upgraded from, use the MSI and MSP files to install Message Connector second and third instances:

- For new installation of Tungsten TotalAgility 8.1 use both MSI and MSP files.
- While upgrading from Tungsten TotalAgility 8.0, use only MSP file.
- While upgrading from Tungsten TotalAgility 7.11 or lower, use both MSI and MSP files.

1. To install the first instance of Message Connector, before installing TotalAgility, set the value of the `ImportService` parameter to true in `SilentInstallConfig.xml`.

Alternatively, to install first instance from Command Prompt, run the following:

```
C:\Share\export>msiexec /i C:\share\export\MC\MC.msi -l*v
KOFAXPRODUCTVERSION=2.11.0.0.0.219 /qn
msiexec /update MC-9.8.3.756.msp KOFAXPRODUCTVERSION=2.11.0.3.756 /qb /
l*v MC-2.11.0.3.756-Inst1.log /n {ED3A11FC-AEED-43E3-ACB9-346251589F42}
```

2. To install the second instance of Message Connector, run the following commands on the Command Prompt:

- `msiexec /i <\\TotalAgility\KIC\Export\MC\MC.msi> TRANSFORMS=:I02 MSINewInstance=1 Kofax="<path>" <options>`

Where `<\\TotalAgility\KIC\Export\MC\MC.msi>` is the path of the TotalAgility setup folder.

In `<path>`, specify the installation path for the second instance of Message Connector. `\KIC-ED\MC02` is appended to this path at the time of installation.

- `msiexec /update MC-9.8.3.756.msp KOFAXPRODUCTVERSION=2.11.0.3.756 /qb /l*v MC-2.11.0.3.756-Inst2.log /n {BECAC22C-F193-4D6F-BE5D-99AD080E776F}`

3. To install the third instance of Message Connector, run the following commands on the Command Prompt:

- `msiexec /i <\\TotalAgility\KIC\Export\MC\MC.msi> TRANSFORMS=:I03 MSINewInstance=1 Kofax="<path>" <options>`

Where `<\\TotalAgility\KIC\Export\MC\MC.msi>` is the path of the TotalAgility setup folder.

In `<path>`, specify the installation path for the third instance of Message Connector. `\KIC-ED\MC03` is appended to this path at the time of installation.

- `msiexec /update MC-9.8.3.756.msp KOFAXPRODUCTVERSION=2.11.0.3.756 /qb /l*v MC-2.11.0.3.756-Inst3.log /n {F6C1303A-7A09-4F2E-AF46-F063E03331F9}`

For the second and third instances of Message Connector, optionally, in `<options>` use the following commands:

- `/qn` - silent installation
- `/qb` - silent installation with elementary user interface (progress bar)
- `ALLUSERS=1` - install for all users

The following command assumes that the TotalAgility setup folder is in the C: drive and the Message Connector's second instance will be installed at `C:\Program Files (x86)\Kofax`.

```
msiexec /i C:\TotalAgility\KIC\Export\MC\MC.msi TRANSFORMS=:I02
MSINewInstance=1 Kofax="C:\Program Files (x86)\Kofax" /qn /norestart
ALLUSERS=1
```

Upgrade Message Connector instances

If you have installed more than one instance of Message Connector, you must upgrade all the instances of Message Connector at the time of upgrading TotalAgility.

1. To upgrade the first instance of Message Connector, before upgrading TotalAgility, set the value of the `ImportService` parameter to true in `SilentInstallConfig.xml`. See [Silent upgrade process](#).

2. To upgrade the second instance of Message Connector, run the following command on the Command Prompt:

```
<\\TotalAgility\KIC\Export\MC\MC.msi> TRANSFORMS=:I02 MSINewInstance=1
Kofax="<path>" <options>
```

Where, `<\\TotalAgility\KIC\Export\MC\MC.msi>` is the path of TotalAgility setup folder.

In `<path>`, specify the upgrade path for the second instance of Message Connector. `\KIC-ED\MC02` is appended to this path at the time of upgrade.

3. To upgrade the third instance of Message Connector, run the following command on the Command Prompt:

```
<\\TotalAgility\KIC\Export\MC\MC.msi> TRANSFORMS=:I03 MSINewInstance=1
Kofax="<path>" <options>
```

Where, `<\\TotalAgility\KIC\Export\MC\MC.msi>` is the path of TotalAgility setup folder.

In `<path>`, specify the upgrade path for the third instance of Message Connector. `\KIC-ED\MC03` is appended to this path at the time of upgrade.

For the second and third instances of Message Connector, you can use the following command in `<options>`:

- `/qn` - silent installation
- `/qb` - silent installation with elementary user interface (progress bar)
- `ALLUSERS=1` - install for all users

i On upgrading to Tungsten Import Connector 2.11, by default, the '[Deny]' attribute is added to the **Folder input base directory** setting under **Security options** in Message Connector Configuration. This attribute disables access to the local watch folder.

To enable access, remove the '[Deny]' attribute from the **Folder input base directory** box and save the Message Connector Configuration.

Chapter 6

Reporting Server installation

This chapter describes the Tungsten Reporting Server installation procedure.

- Silent installation of Reporting Server independent of TotalAgility
- Standard installation using the installation wizard.

Prerequisites

For the additional environments, install the Reporting Server where you installed TotalAgility.

i If you choose to install the Reporting Server on a separate system in the same domain where you installed TotalAgility, then you must assign the following roles to service account:

- For the Staging database: kfx_staging
- For the data warehouse: kfx_etl, kfx_reader, kfx_advanced_reader

The service account must be able to perform bulk operations in database. To do so, run the following command:

```
USE master GRANT ADMINISTER BULK OPERATIONS TO  
[<service_account_running_reporting_server>];
```

Silent installation of the Reporting Server

This section describes the silent installation of 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.

See the following table for the silent installation parameters required to install the Reporting Server.

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

Parameter	Default Value	Description
INSTALLLOCATION	C:\Program Files\Tungsten \TotalAgility\Reporting\	Specify the Reporting Server destination directory.

Parameter	Default Value	Description
WINSERV_ACCOUNT	no default	Enter the name of the user who will run the Reporting Server. To specify a domain user, enter the username 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 runs 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.
TENANT_DB_CONNECTION_STRING	Server=localhost; Trusted_Connection=Yes; Database=DataCenterTenants;	Enter a connection string to the TotalAgility tenants database (DataCenterTenants).
IS_DATABASE_WINDOWS_AUTH	false	Use the Windows database authentication for SQL Server connections in an on-premise multi-tenant environment.
DEPLOYMENT_TYPE	Additional	Specify the deployment type as production or additional.
DEPLOYMENT_NAME	Development	Specify the deployment name in case of additional deployment.

 Parameter names are case-sensitive.

1. Launch a Command Prompt window and from your TungstenTotalAgility-8.1.0_OPMT installation files, navigate to \Reporting\TAReportingService\.
2. Run the following command:

```
msiexec.exe /i Tungsten.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.

Standard installation of the Reporting Server

1. From your TotalAgility installation files, navigate to `TungstenTotalAgility-8.1.0_OPMT\Reporting\TAReportingService` and click `Tungsten.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\Tungsten\TotalAgility\Reporting\`) 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 Tungsten 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, do the following:
 - a. Enter the URL of the Reporting Server service where the configuration settings reside.
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.
 - b. Enter the Tenants DB connection string and click **Test connection** to test the connection.
 - c. To use Windows authentication, select **Use Windows authentication for tenant databases** and provide the Windows credentials.
 - d. Select the **Deployment Type** as **Production deployment** or **Additional deployment (non-production)** (default).
 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.

- If the Reporting Server is installed as part of the Tungsten TotalAgility standard installation, uninstalling TotalAgility automatically uninstalls the Reporting Server.
- If the Reporting Server is installed on a separate system using Wizard, uninstall the Reporting Server from the Control Panel.
- If the Reporting Server is installed in silent mode, you must do the following to uninstall the Reporting Server in silent mode:
 1. On the Command Prompt, change the command line to the root directory of `Tungsten.Reporting.TAService.msi`.
 2. Run `msiexec.exe /quiet /x Tungsten.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 installation and logging.

Chapter 7

TCM Proxy installation

This chapter describes how to install the TCM Proxy on a Web Server. TCM Proxy is required when you want to use the Tungsten Communications Manager (TCM) control on a TotalAgility form for interactive requests with Communications Manager. The proxy allows secure cross domain communication between the TotalAgility Web Server and Tungsten Communications Manager.

Prerequisites

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

Silent installation of TCM Proxy

1. From your TotalAgility installation directory, navigate to `\\TCMProxyInstallation`.
2. Launch a Command Prompt window and run **Setup.exe** and enter the TCM Server URL in the following format: `http(s)://<TCMServer>:<Portnumber>`.
Provide the IP address and port number of the TCM server. The installer updates the Web.config with TCM server details and enables the proxy rewrite rules on the web server (IIS).
3. Press **Enter**.
The TCM Proxy is installed in silent mode.
The system generates a log file at the same location where **Setup.exe** exists.

Standard installation of TCM Proxy

1. From your TotalAgility installation directory, navigate to `\\TCMProxyInstallation` and double-click **Setup.exe**.
The **TCM Proxy Configuration** window appears.
2. Enter the **TCM Server URL** in the following format: `http(s)://<TCMServer>:<Portnumber>`.
The Web.config file is automatically updated with the TCM Server IP and the Port number.
3. Click **Configure**.
4. Click **OK**.

Docker installation of TCM Proxy

While generating the "dockersetting.env" file, if the URL is specified in the "TCM Server URL" setting in the Configuration Utility tool, the same URL is used to install TCM Proxy and configure the deployment in the container.

Update the TCM Server URL

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

Manually update the TCM Server URL

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

```
\\<OnPremiseMultiTenancy installation directory>\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/
kcmcomposerui.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>
</rewrite>
```

```
</rules>
```

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

Use the Configuration Utility

Run the Configuration Utility and on the **Configuration Editor Tool**, select the **App** tab and update the configuration settings. See the *Tungsten TotalAgility Configuration Utility Guide*.

Install TCM Proxy manually

You can install the TCM proxy without using the Web platform installer and TCM 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 a server level, double-click the **Application** request routing cache.
 - b. Click **Server Proxy Settings**.
 - c. Select **Enable Proxy**.
 - d. Click **Apply**.
4. In TotalAgility Web.config, find `{http://cmmserver:port}` and replace it with `http://servername:port`, where **servername** is the host name of the TCM machine and **port** is the port TCM listed as (default 8081). See the previous section for manually updating the TCM Server URL in TotalAgility Web.config.
5. Uncomment the `<rewrite>` section.
6. Save and close the configuration file.

Chapter 8

Tungsten VRS Elite Installation

This chapter describes how to install and configure Tungsten VRS Elite for TotalAgility. For detailed information on Tungsten VRS Elite installation, refer to the Tungsten VRS Elite Installation Guide from the Tungsten Automation support site.

VRS Elite 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.

Install VRS Elite

Install VRS Elite depending on the licensing options:

- If your scanner includes an OEM version of VRS Basic or Professional, run setup.exe on the scan station. The VRS software is automatically activated based on the attached scanner model.
- If you purchased a standalone VRS license, run 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.
- If you want to manage VRS licenses through the TotalAgility License Server while also enabling VRS Elite shared profiles and auto-profile training data, do the following:
 1. Run setup.exe from the VRS Elite installation media.
 2. When prompted, select Server as the setup type.
 3. Confirm the TotalAgility license server information.

i 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. Use the generated deployment Kofax VRS.msi to install VRS on the scan stations. Refer to the *Tungsten VRS Elite Installation Guide* for details.

Use VRS Elite with the TotalAgility Scan Client

After you install VRS Elite, Kofax Software VRS - TWAIN appears in the list of scanners when you scan a document in TotalAgility. See the *TotalAgility Scan Client Help* for more information.

Chapter 9

TotalAgility License Proxy installation

You can install the License Proxy manually or when installing TotalAgility.

This chapter describes the License Proxy installation procedure.

- [Silent installation of License Proxy](#)
- [Standard installation of License Proxy](#)

For information on installing the License Proxy when installing TotalAgility, see the Step for License Proxy installation in Standard installation of TotalAgility.

Prerequisites

Make sure the system meets the following prerequisites:

1. Install License Proxy on the machine where the VRS Elite server is installed (recommended). Otherwise, you will need to run the license utility on each workstation and configure the server to point to the proxy machine.
2. Install the License Proxy on a different computer from the License server (a computer running the Tungsten License Server service) because the License Proxy needs to route traffic to the License 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".

Silent installation of License Proxy

Use the License Proxy silent installation to install the License Proxy automatically from a command line or a batch file. After you edit the silent installation file, the installation proceeds without any user interaction.

1. From your TotalAgility installation files, navigate to \\TungstenTotalAgility-8.1.0_OPMT\Licensing\Installs.
2. On the Command prompt, run the following command.

```
"msiexec /i KofaxLicenseServer.TotalAgility.Proxy-6.6.1.msi  
INSTALLLOCATION="C:\Program Files\Tungsten\TotalAgility License Proxy\  
WINSERV_ACCOUNT="<user>" WINSERV_PASSWORD="<pwd>"  
TOTAL_AGILITY_URL=http://<TA_SERVER>/TotalAgility/Services/SDK/  
LicenseServerService.svc  
SYSTEM_SESSION_ID="<SYSTEM_SESSION_ID>" /qn"
```

See the following table for a description of parameters.


Parameter	Description
InstallLocation	Location where the TotalAgility License Proxy is installed.
WINSERV_ACCOUNT	The name of the user running the service.
WINSERV_PASSWORD	The password of the user running the service. <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p>i Make sure the user running the service has "log on as service" rights and other requirements appropriate to the environment.</p> </div>
TOTAL_AGILITY_URL	The Tungsten TotalAgility server to connect (replace '<TA SERVER>' with your server).
SYSTEM_SESSION_ID	The system session ID from Tungsten TotalAgility (replace '<SYSTEM_SESSION_ID>' with your system session ID).

Standard installation of License proxy

You can install TotalAgility License Proxy using the standard installer wizard.

1. From your TotalAgility installation files, navigate to `\\TungstenTotalAgility-8.1.0_OPMT\Licensing\Installs` and run `KofaxLicenseServer.TotalAgility.Proxy-6.6.1.msi`. The Tungsten 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\Kofax\TotalAgility License Proxy\`) where the Tungsten 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 username.
To specify a domain user, enter the username in the format `Domain\User`.
 - b. Enter and confirm the password.

i This account must have access to the specified TotalAgility URL. These credentials are used for Tungsten Automation 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 System session ID value from the TotalAgility Designer (**System > System settings > Logon and authentication > User sessions**).

c. Click **Next**.

The system downloads the settings.

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

9. Click **Finish**.



The Tungsten TotalAgility License Proxy for VRS Server is installed. To verify if the proxy is working properly, navigate to `C:\Program Files\Kofax\Imgctl\bin` (for Windows 32-bit) or `C:\Program Files (x86)\Kofax\Imgctl\bin` (Windows 64-bit) and run `KSALicenseUtility`. If the proxy is configured properly, the license information appears in the Tungsten Automation License Utility user interface; otherwise, an error appears. You may need to reconfigure the System session ID to match with the TotalAgility Server.

Chapter 10

Tungsten Web Capture Service installation

This chapter describes how to Install the Tungsten Web Capture Service at the default location or a custom location.

Install the Web Capture Service 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 Designer 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 the installation is complete.
5. The View and Change Settings icon  on the Scan Create New Job form becomes available after the page refresh.
6. The Tungsten Web Capture Service icon  in the System Tray icons indicates if the service is running.

Install the Web Capture Service at a custom location

For enterprise deployment scenarios where a custom Web Capture Service installation location is required, install the Web Capture Service as follows.

On the Command Prompt, type the following command:

```
msiexec /i Tungsten.WebCapture.Installer.msi INSTALLFOLDER=<Installation Folder>
```

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 Tungsten.WebCapture.Installer.msi INSTALLSERVICE=1
```

The MSI installation package is available in the TotalAgility installation folder at:

```
\\TungstenTotalAgility-8.1.0_OPMT\OnPremiseMultiTenancyInstall  
\Agility.Server.Web\Forms\Controls\Capture\external\webcapture
```

Use the Web Capture Service in a multiuser environment

You can use the Web Capture Service in 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.

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 can't be installed because you already have Web Capture Service installed as Windows service.`

However, you can upgrade from the standalone installation to Windows Service.

Chapter 11

Tungsten TotalAgility 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.

Prerequisites

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 specify the Active Directory account that can authenticate within TotalAgility. Otherwise, use the LocalSystem account.
- As Scan Agent Service needs access to user profile-specific folders (to access scanned images), the service account used for Scan Agent Service must have administrative privileges to access different user profiles. For example, when Scan Agent Service is installed on the terminal server and/or different users (scan operators) use the same computer.
- If Scan Agent Service is going to be deployed to the end-user computer, for example, to upload images only for a particular user, then you may not require administrator privileges. You can install Scan Agent Service under the end user's account.

Standard installation of Scan Agent Service

1. Navigate to `\\TungstenTotalAgility-8.1.0_OPMT\ScanAgentService`.
2. Double-click **Tungsten.TotalAgility.ScanAgentService.Installer.msi**.
The **Tungsten TotalAgility Scan Agent Service 8.1.0 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 Scan Agent service.
9. Click **Next**.
10. Click **Install** to begin the installation.
Once installed, a local service, "Tungsten 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 the 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 the 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:** The job is being prepared for upload.
- **In Progress:** The job is currently being uploaded.
- **Finished:** The job has successfully been uploaded.
- **Error:** The job encountered an error and has been stopped.
- **Paused:** The 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.

Chapter 12

TotalAgility and Tungsten SignDoc integration

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

Set up the Tungsten SignDoc server

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

Refer to the "Integrate TotalAgility with SignDoc" topic in the *Tungsten TotalAgility Designer Help* to know how to set up the SignDoc server to point to the TotalAgility server.

Chapter 13

TotalAgility and Microsoft Dynamics CRM integration

You can integrate Microsoft Dynamics CRM and Microsoft Dynamics 365 CRM with TotalAgility.

Prerequisites

You must have administrator rights to install Microsoft Dynamics CRM and Microsoft Dynamics 365 CRM.

Standard installation of Dynamics CRM

Follow the same steps to install Dynamics CRM and Dynamic 365 CRM.

1. **Navigate to** \\TungstenTotalAgility-8.1.0_OPMT\DynamicsCRMInstall, and double-click **Setup.exe**.

For Dynamics 365 CRM, navigate to \\\TungstenTotalAgility-8.1.0\Dynamics365CRMInstall_OPMT, 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 the Event Handler in CRM and places necessary files in Global Assembly Cache (GAC).

Update Web.config to support event handlers

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 & Warnings">
<listeners> <add name="Event Log Listener" />
</listeners>
</errors>
</specialSources>
</loggingConfiguration>

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

```

Update Web.config for the CRM virtual directory

```

<system.serviceModel>
<bindings>
  <basicHttpBinding>
    <binding name="BasicHttpBinding_Service" openTimeout="00:10:00"
closeTimeout="00:10:00"
sendTimeout="00:10:00" receiveTimeout="00:10:00" allowCookies="true"
maxBufferSize="2147483647"
maxReceivedMessageSize="2147483647" maxBufferPoolSize="524288">
      <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
    <security mode="TransportCredentialOnly">

```

```

        <transport clientCredentialType="None" />
    </security>
</binding>
</basicHttpBinding>
</bindings>
<client>
    <endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"
contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://<TotalAgility server name or IP Address>/TotalAgility/Services/Core/
IntegrationEventService.svc"/>
</client>
</system.serviceModel>

```


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

Update Web.config for Dynamics CRM

Update Web.config for Dynamics CRM to support event handlers and for the CRM virtual directory.

Update Web.config to support event handlers

Add the following script for the TotalAgility components to support event handlers in Dynamics CRM and Dynamics 365 CRM:

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

```

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

<loggingConfiguration
name=""
tracingEnabled="true"
defaultCategory="General">
<listeners>
<add name="Event Log Listener"
type="Microsoft.Practices.EnterpriseLibrary.Logging.TraceListeners.
FormattedEventLogTraceListener,
Microsoft.Practices.EnterpriseLibrary.Logging,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
listenerDataType="Microsoft.Practices.EnterpriseLibrary.Logging.

```

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

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

```

        ExceptionHandling.TextExceptionFormatter,
Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=5.0.505.0,
Culture=neutral,
PublicKeyToken=31bf3856ad364e35"
priority="0" />
</exceptionHandlers>
</add>
</exceptionTypes>
</add>
</exceptionPolicies>
</exceptionHandling>


```

Update Web.config for the CRM virtual directory

```

<system.serviceModel>
<bindings>
  <basicHttpBinding>
    <binding name="BasicHttpBinding_Service" openTimeout="00:10:00"
closeTimeout="00:10:00"
  sendTimeout="00:10:00" receiveTimeout="00:10:00" allowCookies="true"
maxBufferSize="2147483647"
maxReceivedMessageSize="2147483647" maxBufferPoolSize="524288">
    <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647"
maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
    <security mode="TransportCredentialOnly">
      <transport clientCredentialType="None" />
    </security>
  </binding>
</basicHttpBinding>
</bindings>
<client>
  <endpoint name="CoreIntegrationEventServiceEndpoint"
binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_Service"
  contract="Agility.Server.Core.Model.Interfaces.Services.IIntegrationEventService"
address="http://<TotalAgility server name or IP Address>/TotalAgility/Services/Core/
IntegrationEventService.svc"/>
</client>
</system.serviceModel>

```

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

Chapter 14

TotalAgility configuration


This chapter provides the instructions for configuring TotalAgility such as changing or updating any installation parameters post TotalAgility installation, encrypting and decrypting the TotalAgility configuration files, and more.

Configure HTTPS communication

Enable SSL (Secure Sockets Layer) communication for the TotalAgility web layer and TotalAgility Core Worker to communicate with core services and the Tungsten Automation 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 Production and additional 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.

 Any SSL certificates being used must be fully trusted and publicly signed.

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

Use Subject Alternative Names (SAN) to create a single SSL certificate to use for Tungsten 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.ta.com is for Tenant Management System on the Web server.
 - *.web.ta.com is for multiple tenants on the Web server .
 - app.ta.com is for Tenant Management System on the Application server.
 - *.app.Tungsten.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.

i 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.ta.com (for Tenant Management System on the Web server)
- *.web.ta.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\Tungsten\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>
```

i 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 a password.
6. Click **OK**.

You must secure cookies post-installation. See [Secure cookies](#).

Configure TotalAgility for high availability

You can install a second License Server on a different computer and use it as a backup server for TotalAgility.

1. Navigate to \\TungstenTotalAgility-8.1.0_OPMT\Licensing\Installs.

2. Click **KofaxLicenseServer-xxx.msi**.
The **Tungsten License Server - InstallShield Wizard** opens.
3. Click **Next**.
The **Destination Folder** window opens.
4. Select the default folder (C:\ProgramFiles (x86)\Tungsten\TotalAgility\LicenseServer) for the License Server or click **Change** to select a different folder.
5. Click **Next** and follow the instructions to complete the installation.

Generate a common machine key if using Federated Security

When using Federated Security with TotalAgility in a load-balance environment, TotalAgility cannot consistently decrypt the encrypted token passed from an Identity Provider using WsFed tokens. This is because, by default, each load-balanced server has a unique machine key identifier used for token encryption/decryption.

We recommend that you generate a common machine key and propagate it to all servers in the load-balanced environment. For example, if you generate a machine key for the TotalAgility application, the Web.config file gets automatically updated with the machine key element. The configuration of a machine key can be done at the web server, site, or application level.

To generate a machine key, perform the following steps:

1. Open Internet Information Services (IIS) manager.
2. Select the TotalAgility application, website, or web server from the left panel to generate a machine key.
3. In **Features View**, right-click **Machine Key**, and then click **Open Feature**.
4. On the **Machine Key** page, select an encryption method from the **Encryption method** drop-down list.
5. Select a decryption method from the **Decryption method** drop-down list.
6. Optionally, configure settings for **Validation** and **Decryption** keys.
7. In the **Actions** panel, click **Generate Keys**, and then click **Apply**.
When you click apply, the changes are automatically saved in the Web.config file.
To encrypt and decrypt the machine key, see [Encrypt and decrypt the TotalAgility configuration files](#).

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 TotalAgility.EncryptConfig.exe utility)

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

You can encrypt or decrypt all configuration files.

List of configuration files

List of configuration files of executables

Configuration filename	Default location
<ul style="list-style-type: none"> Agility.Server.ExportConnector.exe.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web
<ul style="list-style-type: none"> Agility.Installation.Server.Upgrade.exe.config Agility.Server.Core.Executor.exe.config Agility.Server.ExportConnector.exe.config Agility.Server.StreamingService.exe.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\bin\
<ul style="list-style-type: none"> Agility.Server.Core.Executor.exe.config Agility Server.Core.ExportService.exe.config Agility.Server.Core.ExportWorker.Host.exe.config Agility.Server.Core.WorkerService.exe.config Agility.Server.StreamingService.exe.config 	C:\Program Files\Tungsten\TotalAgility\CoreWorkerService
<ul style="list-style-type: none"> Kofax.CEBPM.Reporting.AzureETL.exe.config Kofax.CEBPM.Reporting.TAService.exe.config 	C:\Program Files\Tungsten\TotalAgility\Reporting
<ul style="list-style-type: none"> KSALicenseService.exe.config 	C:\Program Files (x86)\Tungsten\TotalAgility\LicenseServer
<ul style="list-style-type: none"> ExtractionProcess.exe.config 	C:\Program Files (x86)\Common Files\Kofax\Server\
<ul style="list-style-type: none"> RegAscSc.exe.config 	C:\Program Files (x86)\Tungsten\TotalAgility\ExportConnectors\bin\
<ul style="list-style-type: none"> Setup.exe.config 	C:\Program Files\Tungsten\TotalAgility\TCMProxyInstallation
<ul style="list-style-type: none"> Agility.Server.Core.Executor.exe.config Transformation.ServiceHost.exe.config DocumentConversionService.Host.exe.config ProcessingService.Host.exe.config 	C:\Program Files\Tungsten\TotalAgility\Transformation Server
<ul style="list-style-type: none"> csc.exe.config 	C:\Program Files\Tungsten\TotalAgility\Transformation Server\roslyn

List of Web configuration files

<ul style="list-style-type: none"> • Web.config • App.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\DeviceManager
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\KFS
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\Kofax\BrowserDevice
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\Kofax\BrowserDevice\Static
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\MobileServices
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\Services\Core
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\Services\Core\Integration
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web\Services\Sdk
<ul style="list-style-type: none"> • Web.config 	C:\Program Files\Tungsten\TotalAgility\OpenAPI

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. The default location is:

```
C:\Program Files\Tungsten\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.

For encryption, use the following command:

```
aspnet_regiis -pef "Section of file" "Path excluding web.config without trailing slash"
```

For decryption, use the following command:

```
aspnet_regiis -pdf "Section of file" "Path excluding web.config without trailing slash"
```

Encrypt and decrypt the configuration files of executables

Use the TotalAgility.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.

Add a security provider

Before encrypting the configuration file, add the following `<configProtectedData>` section in the file:

i The `<configSections>` element must be the first child element of the configuration in the configuration file. This is enforced by .NET configuration manager.

```
<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 `TotalAgility.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 `TotalAgility.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 **TotalAgility.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:


```
TotalAgility.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:

```
TotalAgility.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:

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

i Also repeat the encrypt and decrypt procedures for the Export configuration file.

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" ta"

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" ta"

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, do the following:

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

i 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](#).

i 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 Tungsten TotalAgility Core Worker Server service.

Edit the TotalAgility configuration settings

After installing TotalAgility, to change or update any parameters, edit the following configuration files available in the installation directory.

- Agility.Server.Core.WorkerService.exe.config
- Agility.Server.Core.ExportService.exe.config
- Web.config
- KSALicenseService.exe.config

You can either edit each of these files separately or run the TotalAgility Configuration Utility to modify all the settings in one go. The Configuration Utility is available from the TotalAgility installation files and must be manually copied to your TotalAgility server. See the *Tungsten TotalAgility Configuration Utility Guide*.

Configure the settings to record system tasks history

The system task history is recorded to identify the performance issues on deployments. The history is recorded for all the system tasks or a specific task in On-Premise Multi-Tenant or Azure server using the SystemTasksHistoryToRecord setting. This is an optional setting.

The history of the system tasks includes:

- Time Taken In Seconds = Completed Date Time (Taken Date Time)
- Time Pending In Seconds = Taken Date Time (Pending or Creation Date Time)
- Time Spent In Seconds = Completed Date Time (Execution Started Date Time)
- Next Due Date Time
- Machine Name
- Completed Date Time
- Task Type And Name
- Status
- Due Date Time
- Taken Date Time
- Pending Date Time
- Tenant code
- Environment Name

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\CoreWorkerService
```

3. Locate the **<appSettings>** section and change the settings as required.

```
<appSettings>  
  <add key="SystemTasksHistoryToRecord" value="" />  
</appSettings>
```

The system task history is recorded based on the value:

- Empty or setting not found: The system does not record the task history.
- "-1": Records The system records history for all system task types.
- "0,1,2,3": The system records history for the specific system task types.

4. Save and close the configuration file.

Use the Configuration Utility

Run the Configuration utility and configure the **SystemTasksHistoryToRecord** setting on the **Core Worker** tab of TotalAgility on-premise multi-tenant in Configuration Utility. See the *Tungsten TotalAgility Configuration Utility Guide*.

Configure the settings for system tasks threadpool size

This setting is used to configure the threadpool size of the system task in On-Premise Multi-Tenant or Azure server.

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\CoreWorkerService
```

3. Locate the **<appSettings>** section and change the value in the setting if required (default: 4).

```
<appSettings>  
  <add key="SystemTaskThreadPoolSize" value="4" />  
</appSettings>
```

If the configuration setting is not found, or no value is provided, the system takes the default size.

4. Save and close the configuration file.

Use the Configuration Utility

Run the Configuration utility and configure the **SystemTaskThreadPoolSize** setting on the **Core Worker** tab of TotalAgility on-premise multi-tenant in Configuration Utility. See the *Tungsten 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 Tungsten 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 takes a 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>
```

i 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 on the **Job Thread Pool** tab. See the *Tungsten TotalAgility Configuration Utility Guide*.

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 time out.

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

Manually

1. Navigate to the installed location (default: C:\Program Files\Tungsten\TotalAgility\CoreWorkerService) of the TotalAgility server .
2. In a text editor, open **Agility.Server.Core.WorkerService.exe.config** from the following directory: \\OnPremiseMultiTenancyInstall\CoreWorkerService
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 configure the **Thread Pool Monitoring Interval** setting on the **Core Worker** tab. See the *TotalAgility Configuration Utility Guide*.

Update the settings for a License Server

You can update the settings for a License Server either manually or using the Configuration utility.

Manually

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.

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

1. Stop the Tungsten License Server service.
2. Navigate to C:\Program Files (x86)\Tungsten\TotalAgility\LicenseServer of the TotalAgility server.
3. Open KSALicenseService.exe.config in a text editor .
4. Locate the following section and update the serverId and connectionStrings parameters. By default, the serverId value is "1", which means the 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 the **Backup** license server setting on the **Licensing** tab. See the *Tungsten TotalAgility Configuration Utility Guide*.

Update the settings for 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 Web.config to prevent CSRF attacks. See the Microsoft website for more information.
- [Enable Host prefix for cookies](#)

Configure the 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 adding 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. TargetHostName is the fully qualified domain name of the Web server and TargetPortNo is the website port number. When you provide these settings, the Anti-CSRF origin and referrer validations are performed on the request URL. If the validation fails, the request are terminated considering it a potentially dangerous request.

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

Manually

1. Navigate to the installed location of the TotalAgility server. The default location is: `C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web`.
2. In a text editor, open **Web.config** from the following directory (default):
3. Locate the `<appSettings>` 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 **Anti-CSRF Target Host Name** and **Anti-CSRF Target Port Number** settings. See the *Tungsten TotalAgility Configuration Utility Guide*.

Enable Host prefix for cookies

Use "Host Prefix for Cookies", a browser functionality that makes the cookies more secure by prefixing the TotalAgility cookie names with "__HOST-". When a cookie name starts with this flag, it triggers an 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. Navigate to the installed location of the TotalAgility server. The default location is: C:\Program Files\Tungsten\TotalAgility\Agility.Server.Web.
2. Open **Web.config** in a text editor.
3. Locate the <appSettings> section and make sure the value of UseHostPrefixForCookies is true.

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

Use the Configuration Utility

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

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

Update settings for forcing HTTPS access with HSTS

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 an additional security layer so that data remains secure, make sure the 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:
`\\OnPremiseMultiTenancyInstall\Agility.Server.Web`
3. Do one of the following:
 - If TCM is not installed, locate the rule: **"HTTP to HTTPS redirect"** and uncomment the `rewrite` section where this rule is available.
 - If TCM is installed and if you need an 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>
</rewrite>
```

```

    </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 TCM (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.

Update the settings to enable consolidated logging

Every component has its own logging ecosystem, and the log files can be output to various locations. In TotalAgility, there are multiple diagnostics logs for different components.

Following are the examples of logging across Tungsten TotalAgility components:

- BPM trace log
- Transformation Server trace log
- Transformation Configuration trace log
- Capture Data Layer trace log
- Capture Document Services trace log
- Reporting trace log

By default, logging is not enabled (except for Reporting). When issues occur in any of the TotalAgility components, to get the log data you must manually enable each of these logs separately by updating the relevant configuration file for that component. These logs can be configured to output to log files or other destinations. It is cumbersome to find each log file that is scattered across drives and folders. With consolidated logging, you can get the log data from various TotalAgility components to a central location and single file. Consolidated logging makes log management and analysis easier in identifying, troubleshooting, and resolving the issues as the output for all logs are visible in a central location.

For consolidated logging, TotalAgility supports the trace sources and trace levels. You can use a combination of trace sources and trace filter levels to perform the search and get the log data.

See the following for a list of supported trace sources and their description.

Trace source name	Description
BPM	BPM log (includes Licensing and Tungsten Front Office Server (TFS) log)
TransServer	Transformation Server default log
TransServer_Perf	Transformation Server performance log
TransConfig	Transformation Configuration log
CaptureDL	Capture Data Layer default log
CaptureDL_Imaging	Capture Data Layer Imaging log

Trace source name	Description
CaptureDL_Ext	Capture Data Layer Extensions log
CaptureDL_LogExt	Capture Data Layer Logical Extensions log
CaptureDL_LogExt	Capture Data Layer Logical Extensions log
CaptureDS	Capture Document Services log
Reporting	Reporting log

See the following table for supported trace filter levels and their description.

Trace filter level	Description
All	Records all the critical errors, errors, warnings, information, and verbose.
Critical	Records only critical errors.
Error	Records critical errors and errors.
Warning	Records critical errors, errors, and warnings.
Information	Records critical errors, errors, warnings, and information.
Verbose	Records critical errors, errors, warnings, information, and verbose.

TRACE_LOGGING setting

The "TRACE_LOGGING" setting is available in Web.config, Agility.Server.Core.WorkerService.exe.config, and all other configuration files, and the value is empty by default. The TRACE_LOGGING setting contains a JSON string that includes:

- Log output type ('file')
- Log output filename (if using 'file' output type)
- Log file type ('text' or 'xml')
- Multiple output files ('use-multiple-files')
- append-pid-to-filename
- Maximum file size ('max-file-size-kb')
- Maximum number of files 'max-number-of-files)
- Trace source [ComponentTraceSourceName]:[TraceFilter]

To enable consolidated logging and output to a file, you can provide the following JSON string in the value attribute in the <appsettings> section of the configuration file:

```
{
  'log-type': 'file',
  'file-location': 'Trace_Logging.log',
  'file-type': 'text',
  'use-multiple-files': false,
  'append-pid-to-filename': false,
  'max-file-size-kb': 5120,
  'max-number-of-files': 10,
  'sources': ['<TraceSourceName>:<TraceLevelFilter>', '<[TraceSourceName]:
[TraceLevelFilter]>']
}
```

}



- The 'text' and 'xml' are supported values for 'file-type'. By default, the log file types are created as text files with log data written as plain text. To get the log file as an XML, specify the 'log-type' as 'xml' and 'file-location' as 'Trace_Logging.xml'.
- For both the file-types ('text' or 'xml'), the log file is appended with the process name as <filename.processname.extension> because multiple processes cannot be written to the same log file. See the following examples:
 - If the process name is "Agility.Server.Core.WorkerService", file name is 'Trace.txt', and the file type is text, the log file name is created as "Trace.Agility.Server.Core.WorkerService.txt".
 - If the process name is 'Coreworker', file name is 'Trace.xml', and the file type is xml, the log file name is created as 'Trace.Coreworker.xml'.
- You can optionally set the following attributes:
 - **use-multiple-files:** (Default: false). If set to true, multiple log files are created.
 - **max-file-size-kb:** (Default: 5120). If the original log file reaches this threshold, the log file copies itself and creates a new log file with a sequence number appended to it. The sub log files are numbered sequentially as Trace1.txt, Trace2.txt, Trace3.txt, and so on.
 - **max-number-of-files:** (Default: 10). The maximum number of files to create. If the file reaches the threshold, the log files gets deleted sequentially from 1, 2, 3, and so on.
 - **append-pid-to-filename:** (Default: false): If set to true, appends the Windows OS executable process ID to the file name. You must set this attribute to true if "use-multiple-files" is set to true when using consolidated logging with the TotalAgility website application. This is because IIS uses multiple Windows OS executables with the same name when recycling web applications and "use-multiple-files" requires uniqueness in the log file name for each executable.

The following is a sample from the configuration file with JSON string to create a log file with name, "Trace_Logging.log" in the current folder and write the log entries for the trace source as Transformation Server with trace filter level as All, and also for the trace source as BPM and trace level as Warning.

```
{
  'log-type': 'file',
  'file-location': 'Trace_Logging.log',
  'file-type': 'text'
  'sources': ['TransServer:All', 'BPM:Error']
}
```

Enable consolidated logging

Use the following procedure to enable consolidated logging, for example, for Transformation Server:

1. Stop the Tungsten Transformation Service.
2. Navigate to the installation directory for the TotalAgility server.
3. In a text editor, open **Transformation.ServiceHost.exe.config** from the following directory:
C:\Program Files\Tungsten\TotalAgility\Transformation Server

4. Locate the **<appsettings>** section and update the value of "TRACE_LOGGING" setting accordingly. For example, if you want to trace the logging of **TransServer** and BPM sources with trace level as **Warning**, provide the key value as follows:

```
<add key='TRACE_LOGGING' value='{ "log-type": "file", "file-location":
"d:\\logs\\mylog.log", "file-type": "text", "sources": ["TransServer:All",
"BPM:Error"] }' />
```

In 'd:\\logs\\mylog.log', 'file-type', <mylog> is the log file name to be generated.

The log file is generated in the following format:

<Logfilename>.processname.processID.extension provided (.log or .txt). For example, if the process name is Transformation.ServiceHost, process ID is 21784, and the extension is .log, the log file generated is mylog.Transformation.ServiceHost.21784.log.

i If a supported component trace source is not specified, then logging is disabled for it. Additionally, if an invalid trace source or level is specified, an error is written to the event log.

5. Start the Tungsten Transformation Server Service.
All the critical errors, errors, information, warnings, information, and verbose are logged for the Transformation Server, and all the critical errors and errors are logged for BPM.

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 `Web.config`.

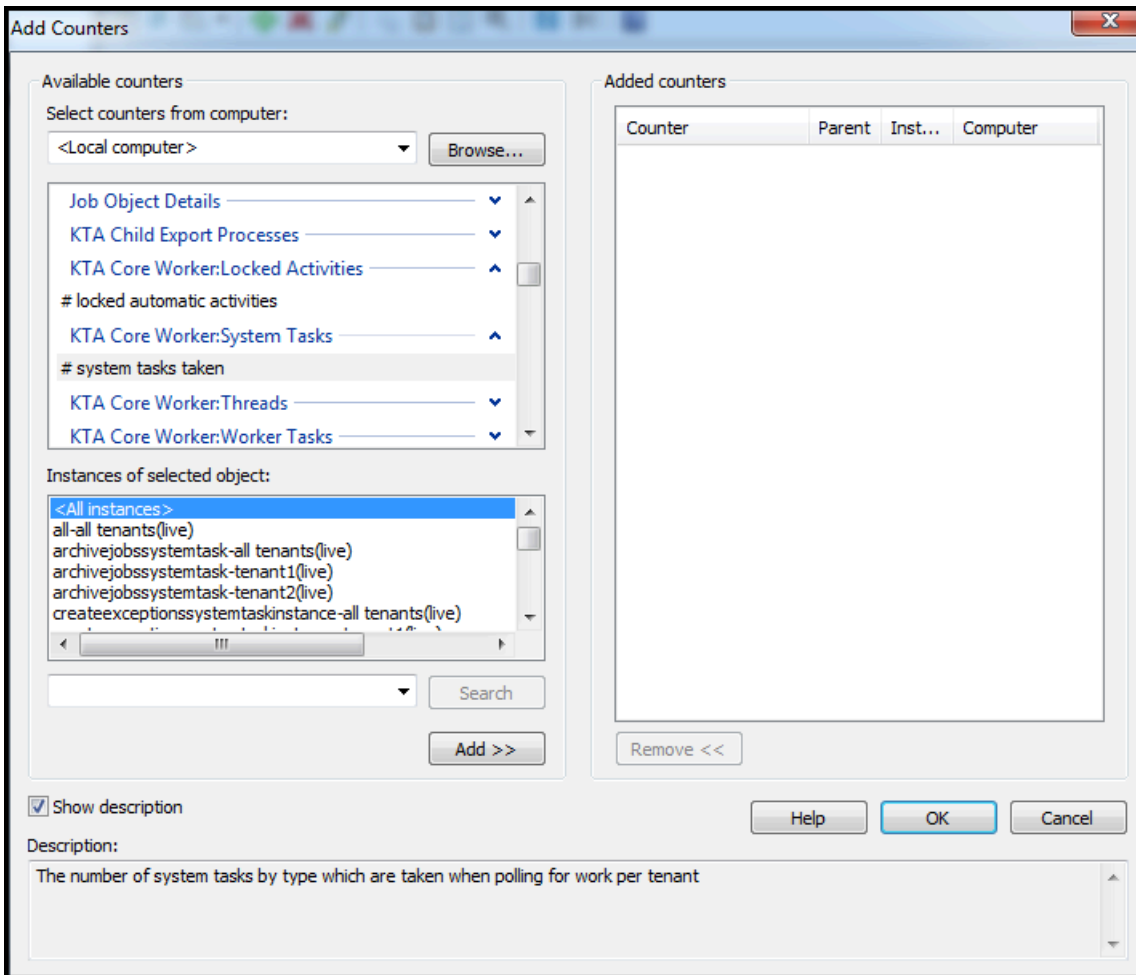
Add performance monitoring counters

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 them 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 *Tungsten TotalAgility Administrator's Guide*.

Exclude folders and files from the antivirus scan

In your antivirus application, add the following TotalAgility folders or files to the list of items that are excluded from scanning. See the following table for the TotalAgility folders and files that are excluded from antivirus scan.

Folders and files	Default path
KSALicenseService.EXE	C:\Program Files (x86)\Tungsten\TotalAgility \LicenseServer

Folders and files	Default path
Agility.Server.Core.Executor.exe Agility.Server.Core.ExportService.exe Agility.Server.Core.ExportWorker.Host.exe Agility.Server.Core.WorkerService.exe	C:\Program Files\Tungsten\TotalAgility \CoreWorkerService
Kofax.CEBPM.Reporting.AzureETL.exe Kofax.CEBPM.Reporting.TAService.exe	C:\Program Files\Tungsten\TotalAgility\Reporting
Agility.Server.Core.Executor.exe Transformation.ServiceHost.exe DocumentConversionService.Host.exe TotalAgility.EncryptConfig.exe ProcessingService.Host.exe PdfGenerator.exe	C:\Program Files\Tungsten\TotalAgility \Transformation Server
Agility.Installation.Server.Upgrade.exe Agility.Server.Core.Executor.exe Agility.Server.ExportConnector.exe Agility.Server.StreamingService.exe	C:\Program Files\Tungsten\TotalAgility \Agility.Server.Web\bin
Files within the bin folder	C:\Program Files (x86)\Kofax\KIC-ED\MC\bin <div style="background-color: #e0f2f7; padding: 5px;"> <p>i If you have multiple instances of Message Connector, you need to exclude the files from the bin folder of each Message Connector:</p> <ul style="list-style-type: none"> C:\Program Files (x86)\Kofax\KIC-ED\MC02\bin C:\Program Files (x86)\Kofax\KIC-ED\MC03\bin </div>
Runtime folders	
AppLogging KIC-ED KSALic KTT Licensing TotalAgility Vrs WebCapture	C:\ProgramData\Kofax
Telemetry TotalAgility TotalAgility Tenant Management	C:\Program Files\Tungsten <div style="background-color: #e0f2f7; padding: 5px;"> <p>i The Telemetry folder is only available if you install Telemetry.</p> </div>
Miscellaneous folders	

Folders and files	Default path
BWE CheckPlus7.3 CheckPlusInternational CheckRecognition1.2 CheckUltra CheckUsability1.7.4 Components DocumentConverter DetectHpMp3.0 FormXtra8.4 KetValuePrector NLP OmniPage22.2 Pdf Compressor Salience7.0 Server TableExtraction2.1	C:\Program Files (x86)\Common Files\Tungsten

Chapter 15

Log on to TotalAgility On-Premise Multi-Tenancy

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

1. On the **Start** menu, navigate to **Tungsten 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**.

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

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

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

i 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, TotalAgility Apps, and TotalAgility Workspace for production and additional deployment environments.

i 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.


Chapter 16

Uninstall TotalAgility

Uninstalling TotalAgility only removes the application and not the databases.

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.
 - The system generates a summary of log, `TungstenTotalAgilitySilentUnInstallLog.txt`, on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file `TungstenTotalAgilityInstallErrorLog.txt` on the desktop. Fix those errors and repeat the above steps.
 - 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.

Use the installation wizard

1. Click **Start > Tungsten TotalAgility** and select **Uninstall or Repair Tungsten 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. If any errors occur, by default, TotalAgility creates a log file `TungstenTotalAgilityInstallErrorLog.txt` on the desktop. Fix those errors and repeat the above steps.

Chapter 17

Upgrade TotalAgility On-Premise Multi-Tenant

To upgrade the TotalAgility On-Premise Multi-Tenant system:

- Upgrade the Tenant Management System servers to the latest version. When you do this, only MasterTenants databases are upgraded and not the DataCenterTenants or the tenant databases. See the *Tungsten TotalAgility Tenant Management System Installation guide*.
- Upgrade the Deployment servers using installer. When you do this, only MasterTenants databases are upgraded and not the DataCenterTenants or the tenant databases.
- Upgrade the tenants. You must upgrade the Tenants via the Tenant Management system or the Zero downtime utility, based on the upgrade process you choose. See the *Tungsten TotalAgility Tenant Management System Help* for more information.

i Before upgrading TotalAgility, ensure that all the databases are backed up.

Upgrade deployment servers

Upgrade TotalAgility deployments using the following methods:

- [Silent upgrade process](#)
- [Interactive upgrade process](#)
 - [Standard upgrade process](#)
 - [Zero downtime upgrade process](#)

i All the deployments need not be upgraded to the latest version. For example, you can choose to upgrade only an additional deployment and make sure it is working fine before you decide to upgrade the production. But you must upgrade the Tenant Management System servers to the latest version.

When upgrading via the installer, you can choose one of the following options:

- Upgrade only TotalAgility components.
- Upgrade only TotalAgility databases, that is the Datacenter databases.
- Upgrade TotalAgility components including databases.
- Switch from SQL authentication to Windows authentication for connection to tenant databases.

Upon upgrading, the TotalAgility installer restores the following configuration settings:

- All existing AppSettings.
- All existing Security Bindings.
- All HTTP URL Rewrites to be done for TotalAgility.

You can also upgrade the tenant databases manually using database scripts. See the *Tungsten TotalAgility Tenant Management System Help*.

Silent upgrade process

For a silent upgrade of TotalAgility on-premise multi-tenancy to version 8.1.0, 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 the Tenant Management system, the production and additional deployment environments are installed independently of each other, to upgrade the additional environment and production 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.

Parameter	Default value	Description
	upgrademultitenant databases	Use this setting only if you are upgrading the databases before upgrading TotalAgility components. <div style="background-color: #e6f2ff; padding: 10px;"> <p>i If you upgrade TotalAgility components and then upgrade databases, you must do the following:</p> <ol style="list-style-type: none"> a. Open SilentInstallConfig.xml available at the following location: \\TotalAgility Installation Information\Tungsten TotalAgility b. Update the <InstallAction> section with the following parameter: <InstallAction> =Upgradedatabasesforexistingmul titenancy c. Run Setup.exe /Silent /U from the above-mentioned path. </div>
	upgrademultitenant components	Use this setting to upgrade only TotalAgility components.
TransformationService	true	Set to true to install the Transformation Server.
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 the 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 and change the command line to the root directory of the Setup.exe file.
5. Run `Setup.exe /Silent /Upgrade`.
 - Based on the parameters set to true in the silent configuration file, the following items are upgraded automatically:
 - Tungsten TotalAgility
 - Tungsten Automation Import Connector (KIC)
 - Tungsten Automation Transformation Designer
 - Utility for Tungsten Automation Export Connector

- The system generates a summary of log, TungstenTotalAgilityMultiTenancySilentUpgrade.txt on the desktop.
 - If any errors occur, by default, TotalAgility creates a log file TungstenTotalAgilityInstallErrorLog.txt on the desktop. Fix those errors and repeat the above steps.
 - The success or failure of the installation is indicated in the event log.
6. Save and close the file.

Interactive upgrade process

You can choose to upgrade TotalAgility using the interactive upgrade process in either ways:

- [Standard upgrade process](#) (non-zero downtime)
- [Zero downtime upgrade process](#)

Standard upgrade process

In a standard upgrade process, you must close the current-running application for all the tenants, install the newer version on all the servers of a deployment, and then start the newer version of the application after all the tenants are upgraded. This upgrade process involves the application being down for a while.

Do the following to upgrade all the servers of a deployment:

1. From your TotalAgility 8.1.0 installation files, navigate to `\\OnPremiseMultiTenancyInstall` and double-click **Setup.exe**.
The **User Account Control** window opens.
2. In the **Tungsten TotalAgility MultiTenancy Upgrade** window, select one of the following options:
 - **TotalAgility components**: Upgrades only the components and not the datacenter database.
 - **TotalAgility databases**: Upgrades only the datacenter database.
 - **TotalAgility components including databases**: Upgrades both the components and the datacenter database.
3. To use Windows authentication to connect to SQL Server, select the check box for **Windows authentication for databases**. (Default: Clear)
4. By default, the services are automatically started. To start services manually, clear the check box for **Automatically start services**.
5. If the Tenant Management System is already installed on the same deployment server you are upgrading, the check box for **Tenant Management System** appears and is selected by default. If you do not want to upgrade Tenant Management System, you must clear the check box and proceed with the upgrade process.

Additionally, If you are upgrading from a version earlier than TotalAgility 7.11.0, the check box, **Please provide the additional environment host name to update in datacenter. If the additional environment does not exist, please uncheck and proceed.** appears and is selected by default. If the additional environment does not exist, you must clear the check box and proceed with the upgrade process. If the additional environment does not exist, you must clear the check box and proceed with the upgrade process.

6. Click Next.

The following things happen based on the selection of **Tenant Management System** option:

- If the checkbox is clear, the **Credentials** window opens.
- If the checkbox is selected, the Tenant Management System upgrade Installer is launched. For more information, see the *Tungsten TotalAgility Tenant Management System Installation Guide*. On upgrading the Tenant Management System, the **Credentials** window opens.

7. Enter the credentials(password and confirm password) and click Next.

The **Installation Progress** window opens. The setup upgrades the required components/database.

8. Click Finish to complete the upgrade process.

If any errors occur during the upgrade, by default, TotalAgility creates a log file, TungstenTotalAgilityInstallErrorLog.txt on the desktop. Fix the errors and complete the process.

Use the Zero downtime upgrade process

The zero-downtime upgrade of TotalAgility is only supported for upgrades from the previously released version which has a database change. For example, TotalAgility 8.1.0 only supports the zero-downtime upgrade from TotalAgility 8.0.0, as 8.0.0 is the last released version that has a database change. The zero-downtime upgrade from version earlier to 8.0.0 is not supported.

With a zero-downtime upgrade, you can upgrade TotalAgility by introducing a newer 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.

In a zero-downtime upgrade, the tenants are upgraded using the **OPMTDBUpgrader** utility and not via the Tenant Management System and without the need to install the newer version of TotalAgility on extra servers. The TotalAgility On-Premise Multi-Tenant system is always available during the upgrade, but individual tenants are deactivated while their data is being upgraded. This is due to the performance concern of upgrading tenant data while the tenant is still active.

The TotalAgility Designer is disabled for all tenants to prevent usage of new TotalAgility features during the upgrade of TotalAgility servers to the next version, as there may still be TotalAgility servers running using the earlier version.

If any issues occur during the zero-downtime upgrade, you can only roll back to the pre-upgrade backup, that is, the backup of the tenant databases done before the upgrade starts, as the tenant's system will still be running during the upgrade.

To upgrade TotalAgility On-Premise Multi-Tenant system using zero-downtime, do the following:


1. From your TotalAgility installation files, navigate to `\\TungstenTotalAgility-8.1.0_OPMT\Utilities\OPMTDBUpgrader` and run `TotalAgility.Install.OPMTDBUpgrader` on any Application server as an administrator.

The upgrader connects to the default DataCenter databases using the connection details from the Application server configuration files. If you run this utility from any server other than the Application Server, you must manually enter the database details.

The **Tungsten TotalAgility Multitenancy Tenant upgrader** window opens.

2. Click **Next** to continue with the setup.

The **Databases** window opens.

3. Specify the MasterTenants database connection string along with the DataCenter database connection string to upgrade. These connection strings are used to pre-upgrade the Master/ datacenter tables.
 4. Click **Next** and then click **Yes** to confirm.
The **Upgrade Tenants** window displays the list of tenants.
 5. On the **Select deployment to upgrade** list, select the deployment type.
The list of tenants that belong to the selected deployment type appears in the table. The following tenant information is displayed: Tenant name, database server, status, upgrade status, and result.
 6. Select a single tenant, multiple tenants, or all tenants to upgrade and click **Pre Upgrade**.
A confirmation message appears.
 7. Click **Yes**.
All the selected tenants are upgraded to the latest version. Each of the selected tenant is deactivated for a short period during the data upgrade. Once the upgrade process starts, TotalAgility Designer access for all the tenants is deactivated until the completion of the upgrade process.
 8. Click **Refresh**.
The **Status** column for the tenant displays the status of the selected tenant as **Upgrading**. The status of remaining tenants under the selected deployment is displayed as Active.
 9. Select the tenant and click **View Results**.
The **Tenant Upgrade Result** window displays the upgrade result.
 10. Click **Close** to return to the **Upgrade Tenants** window.
Upon upgrading successfully, the **Upgrade Status** column for the tenant displays the status as **Post Upgrade Pending**.
-  TotalAgility 8.1.0 only supports zero-downtime upgrade from TotalAgility 8.0.0. If a tenant being upgraded is using a version other than 8.0.0, an error appears
11. Once all the tenants are pre-upgraded, the databases are now backward compatible. You can close the utility.
 12. From your TungstenTotalAgility-8.1.0_OPMT installation files, navigate to `OnPremiseMultiTenancyInstall`, run **Setup.exe** and start upgrading all the on-premise multi-tenant TotalAgility deployment servers to the latest version via the TotalAgility installer. See *Tungsten TotalAgility On-Premise Multi Tenancy Installation Guide* for more information.
 13. Similarly, upgrade the Tenant Management System deployment server to the latest version via the Tenant Management System installer.
 - a. From your TungstenTotalAgility-8.1.0_OPMT installation files, navigate to `OnPremiseMultiTenancyInstall\TenantManagementInstall`.
 - b. Run **Setup.exe**.
Once the Tenant Management System and datacenter databases are upgraded to the latest version, the databases are now backward compatible. See the *Tungsten TotalAgility Tenant Management System Help* for more information.
 14. Make sure the tenants are working. To test, you can activate TotalAgility Designer access to a single tenant via the Tenant Management System tenant update screen and perform all tests.
 15. Make sure all the required deployment servers have been upgraded to the newer version.

16. Open the OPMTDBUpgrader utility, in the **Upgrade Tenants** window, click **Post Upgrade** to run the post upgrade database scripts for all the selected tenant databases. This is to cleanup the old data and complete the upgrade process.

i Ensure all the related deployment servers have been upgraded to the newer version before running post upgrade scripts .

Running the post-upgrade database scripts also executes the postscripts for master and datacenter tables and activates TotalAgility Designer access for all these tenants. During this process, each tenant is deactivated during the data upgrade.

All the tenants are now upgraded to the latest version and are no longer backward compatible with the previous Tungsten TotalAgility version.

Switch from SQL authentication to Windows authentication

When upgrading TotalAgility On-Premise Multi-Tenancy, you can choose to switch from SQL Authentication to Windows Authentication for connection to tenant databases.

Prerequisites:

- Make sure the databases created is in the following format:
 - TotalAgility_Main_Live_TenantName
 - TotalAgility_Reporting_Live_TenantName
 - TotalAgility_Reporting_Staging_Live_TenantName
 - TotalAgility_Documents_Live_TenantName
- Create the tables for Main, Reporting, Reporting Staging, and Documents databases.
- Copy all the data from production and Reporting Live databases to the newly created databases to work with the tenant.

To change the mode of authentication from SQL authentication to Windows, do the following:

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>
```

Change Capture binary data storage

By default, the Capture data is stored in the SQL Server. You can use 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 8.1.0, 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 on the **Capture Storage** tab of the Configuration Utility. See the *Tungsten TotalAgility Configuration Utility Guide*.

Chapter 18

Troubleshooting

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

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.

Error on Linked servers page in TotalAgility Designer

When you click **Integrations > Linked servers** in TotalAgility Designer, an unknown error occurs instead of displaying the Linked Servers page. This is because client certificates are not supported when using TLS 1.3 with IIS, and only TLS 1.2 or lower can be used.

To resolve this issue, disable **TLS 1.3 over TCP** in the IIS Manager by doing the following:

1. Click **Start > Run > InetMgr > Sites > Default Web Site**.
By default, the Default Web Site is selected.
2. Right-click on the **Default Website** and click **Edit Bindings**.
The **Site Bindings** dialog box is displayed.
3. Select **https** and then click **Edit**.
The **Edit Site Bindings** dialog box is displayed.
4. Select **Disable TLS 1.3 over TCP** and click **OK**.

Installation failure in IPv4 and IPv6 environment

If the SQL server is configured to listen only on IPv6 addresses on a dual-stack (IPV46), client connection attempts using IPv4 address will fail and it may take longer than default timeout, contributed by default TCP timeout logic during connection establishment handshakes. Even though the subsequent IPv6 connection can succeed immediately, the connection may still fail.

To resolve this issue, disable IPv4 in SQL Server Configuration Manager.

1. Start **SQL Server Configuration Manager**.
2. Open the **Properties** for the TotalAgility server instance TCP/IP protocol.
3. Set **Listen All** to **No**.

i This setting allows fine control over which interfaces the TAsServerSQLInstance 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. Select **OK** to commit changes and **OK** at the service restart dialog.
7. Restart the SQL Server (<TAsServerInstance>) service where TAsServerInstance is the actual instance used by TotalAgility (for example, Tungsten TotalAgility).

Exception during Transformation Designer project import

An exception is generated while importing projects using Transformation Designer which 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. On the Section list, expand **system.webServer** and select **serverRuntime**.
 - c. On the From list, select **ApplicationHost.config** <location path='Default Web Site/TotalAgility'/>.
 - 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**.

Appendix A

Generic terms

This topic describes the generic terms used in the TotalAgility Installation Guide.

Tungsten TotalAgility Core Worker service

The Core Worker Service is responsible for executing the background system tasks, such as performing automatic activities, message import, job creation, and other scheduled tasks for TotalAgility.

Tungsten TotalAgility Reporting service

The Reporting service processes reporting data created by different Tungsten TotalAgility components. This service extracts the capture data from the Reporting Staging database, transforms it and then loads it into the Reporting Main database. You must run this service on a dedicated server, as it performs CPU-intensive translation of data.

Tungsten License Server service

The License Server service decrements user and volume license counts.

Tungsten TotalAgility Export Worker service

The Export Worker service exports documents to the customer's choice of store. Once exported, the documents can be removed from the main TotalAgility database. In a Docker container, the Export service cannot run inside a container and must be run directly on a host server, because the export connectors have multiple dependencies which are not available in the container.

Tungsten Transformation Server service

The Transformation Server service polls the database for automatic capture activities to perform Image Processing, Separation, Classification, Extraction, and PDF Generation. As these operations are CPU intensive, this service must run on a dedicated server to perform its work when not running in Real Time Transformation Service mode. If running in Real Time Transformation Service

mode, where it provides customers with enhanced features aimed at mobile/capture APIs, it works with in-memory documents to improve performance.

Import Service

Use this service to install multiple instances of the Message Connector. When you uninstall TotalAgility, all the instances of Message Connector are also uninstalled.

Tungsten TotalAgility Streaming Service

Used to import and export packages in the TotalAgility Designer. You must use a Windows service as IIS only supports a maximum of 2 GB for a stream. This service runs on the Web Server. In a separate Web/Application, it runs on both the web tier and the application tier.

Capture Binary Data Storage

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

FILESTREAM

A FILESTREAM is a specific file group in the database where the Capture documents are stored. You can perform actions on the documents using the SQL Server database.

The Administrator creates these file groups. For these file groups to appear under the File storage settings, you must enable the FILESTREAM feature.

1. Select Start > Programs > SQL Server Configuration Manager > SQL Server properties > 'FILESTREAM'. The file groups configured in the SQL Server configuration manager are listed under the File storage settings.
2. Select a file group to store the Capture binaries.

FILESTREAM is not supported with SQL Server authentication or when the databases do not exist.

TungstenTotalAgilityInstallErrorLog.log

TungstenTotalAgilityInstallErrorLog.log is the log file created if any errors occur during installation. This file is created at the same location where setup.exe exists if the path in the System diagnostics section of the Setup.exe.config is not defined. You can define the name and the path to the log file in the `<add name="TALog" type="System.Diagnostics.TextWriterTraceListener" initializeData="<logfile path> <log file name>"`. The log file is also created on the desktop.

ETL


ETL (Extract, Transform, Load) is the main part of the TotalAgility Reporting Service. It is the general procedure of copying data from one or more sources into a destination system that represents the data differently from the source(s) or in a different context than the source(s).

L2S

L2S is a version of ETL implementation. It uses only three tables from this database: wsa_messages, kfx_db_version, and existing_id_values.

Staging database

The Staging database contains the wsa_messages table. Each row of this table represents a separate wsa_message.

 Other tables of the Staging database are used by the Reporting Service 7.9 and earlier for pre-processing information from the wsa_messages table.

wsa_messages table

wsa_messages table is the main table of the Staging database. Reporting Service periodically starts Kofax.CEBPM.Reporting.AzureETL.exe to extract rows from this table, process them, and load the result into the Warehouse database.

wsa_message

wsa_message is a structure containing reporting data that is generated by activity during job data processing. The activity writes wsa_message into the wsa_messages table of the Reporting Staging database during and after the TotalAgility activity completion (batch session). Each wsa_message corresponds to a separate row in the wsa_messages table.

Kofax.CEBPM.Reporting.AzureETL.exe

Kofax.CEBPM.Reporting.AzureETL.exe is an executable that is run by Reporting Service. It starts ETL iterations and interrupts ETL iterations by request from Reporting Service.

ETL iteration

ETL iteration is responsible for the creation and initialization of classes supporting ETL. The number of iterations performed by Kofax.CEBPM.Reporting.AzureETL.exe is defined by the environment variable, MaxMQ2StagingIterationsNum.

Warehouse database

The Warehouse database contains a set of tables collecting wsa_messages processing results.

Completed batch session

The completed batch session is a collection of wsa_messages generated by the activity at runtime. It contains several BatchEdit wsa_message that are written to the database throughout the session and one KCBatchAction wsa_message that is written at the end of the activity execution.

TotalAgility.EncryptConfig.exe

TotalAgility.EncryptConfig.exe is a utility that is used to encrypt or decrypt the configuration files of executables.