



Kofax Insight Administrator's Guide for Azure

Version: 6.5.0

Date: 2022-09-20

© 2018–2022 Kofax. All rights reserved.

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

Table of Contents

Preface	4
Product documentation.....	4
Training.....	5
Getting help with Kofax products.....	5
Chapter 1: Install Kofax Insight on Azure	7
Prerequisites.....	7
Create storage, Key Vault and Virtual Network on Azure.....	7
Storage.....	8
Key Vault and Virtual Network.....	8
Update the configuration (.cscfg) file.....	8
HTTPS.....	8
SQL connection settings.....	8
Roles and instances count.....	9
Storage name, access key and virtual network.....	10
Cloud service and deployment of the Insight package on Azure.....	10
Chapter 2: Getting started with Kofax Insight on Azure	12
Distribution of Insight functionality.....	12
Configure roles.....	12
Resolve transient faults.....	13
Activate the license.....	13
Access to Insight applications.....	14
View mode.....	14
Edit mode.....	14
Log management.....	14
Use Azure Key Vault to store the connection settings.....	15

Preface

Use the information in this guide if you are the administrator who will configure and maintain Kofax Insight. This guide describes the recommended configuration and setup.

Product documentation

The Kofax Insight documentation set is available online at the following URL¹:

<https://docshield.kofax.com/Portal/Products/Insight/6.5.0-550o6u6oqu/Insight.htm>

The full documentation set includes the following items:

Kofax Insight Release Notes

Contains late-breaking product information not included in this guide.

Kofax Insight Technical Specifications

Contains information on supported operating systems and other system requirements.

Kofax Insight Administrator's Guide for Azure

Contains information for administrators who are responsible for configuring and maintaining Kofax Insight in an Azure environment.

Kofax Insight help systems

Context-sensitive online help is available directly from the following Kofax Insight applications.

Kofax Insight Admin Console Help

Describes the functions in the Admin Console application.

Kofax Insight Data Loader Help

Describes the functions in the Data Loader application.

Kofax Insight Multi-Tenant Console Help

Describes the functions in the Multi-Tenant Console application.

Kofax Insight Studio Help

Describes the functions in the Studio application, including the Dashboard Designer and the Viewer.

¹ You must be connected to the Internet to access the full documentation set online. For access without an Internet connection, see "Offline documentation."

Kofax Insight Themes and Formats Help

Describes the functions in the Themes and Formats application.

Kofax Insight Viewer Help

Describes the functions in the Viewer application.

Tutorial

The tutorial, which is intended for use with the Samples project in the Insight installation package, includes a Quick Start Guide.

Training


Insight offers computer-based training to help you make the most of your Insight solution. Visit the Kofax website at <http://www.kofax.com> for details.

Getting help with Kofax products

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

To access the Kofax Knowledge Base:

1. Go to the [Kofax website](#) home page and select **Support**.
2. When the Support page appears, select **Customer Support > Knowledge Base**.

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

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need. Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news. Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:

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

- Access the Kofax Partner Portal (for eligible partners).
Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Install Kofax Insight on Azure

This chapter contains step-by-step installation and configuration instructions for Kofax Insight 6.5.0 on Azure. Read the prerequisites before you get started.

Kofax Insight on Azure supports two configuration types:

- **Single-tenant:** Single tenant on Insight with a single Insight Administration database. The Administrator is responsible for all projects on Insight.
- **Multi-tenant:** Multiple tenants on Insight, where each tenant has a separate Insight Administrator with project databases. The Administrators are created per tenant and manage their own projects.

Prerequisites

You need to have access to the Azure portal account and create a [storage](#), a [Key Vault and Virtual Network](#), update a [configuration file](#), and create a [cloud service](#) for deploying and using Kofax Insight on Azure.

Most of the settings are common to both **single-tenant** and **multi-tenant** configurations. For a multi-tenant configuration, you should create a dedicated database and administrator account for each set of projects, and update the settings in the [configuration file](#). Follow the instructions in this guide, until you are prompted to select your type of configuration.

Ensure that you have access to the Azure portal account and the most current versions of the following files:

- Kofax Insight Azure package and configuration files, which are included in *KofaxInsight-6.5.0_ForAzure.ZIP*.
The ZIP file is available for download and listed under the Kofax Insight 6.5.0 package on the Kofax Fulfillment site.
- SSL certificate, which is required to initiate a secure session with cloud URLs. You can also use a self-signed certificate.

Create storage, Key Vault and Virtual Network on Azure

This section describes how to create a storage account, Key Vault and Virtual Network, which are required to set up Kofax Insight projects on Azure.

Storage

Log in to the Azure portal and follow the instructions on the Microsoft Azure pages to [create a storage account](#).

Key Vault and Virtual Network

Review the [deployment prerequisites](#) for Azure Cloud Services (extended support) on the Microsoft Azure pages and complete the following steps.

- Create Key Vault and upload the SSL certificate.
- Create Virtual Network.

Update the configuration (.cscfg) file

Before proceeding, extract the following files from *KofaxInsight-6.5.0_ForAzure.ZIP*:

- AzureInsight.XXXX.cspkg - Insight Azure package
- ServiceDefenition_XXXX.csdef - service definition file
- ServiceConfiguration.Cloud.cscfg - configuration file

Open **ServiceConfiguration.Cloud.cscfg**. Make the changes described in the following subsections, according to your type of configuration.

HTTPS

The certificate thumbprint string appears after you upload the certificate. Copy the string and update the <Certificates> section of the configuration file for "InsightWebRole" and "SchedulerRole".

```
<Role name="InsightWebRole">
  <Instances count="2" />
  <ConfigurationSettings>
    <Certificates>
      <Certificate name="Altosoft.Azure.Https" thumbprint="2F1A604401EF4357639A2FF146346DB1ACEE7835" thumbprintAlgorithm="sha1" />
      <Certificate name="Insight.Application.ClientCert" thumbprint="2F1A600000EF4357639A2FF100086DB1ACEE7835" thumbprintAlgorithm="sha1" />
    </Certificates>
  </Role>
<Role name="SchedulerRole">
  <Instances count="2" />
  <ConfigurationSettings>
    <Certificates>
      <Certificate name="Insight.Application.ClientCert" thumbprint="2F1A600000EF4357639A2FF100086DB1ACEE7835" thumbprintAlgorithm="sha1" />
    </Certificates>
  </Role>
```

SQL connection settings

Create an SQL server on the Azure portal. Complete the following steps and set the configuration file according to your type of configuration.

For a **single-tenant** configuration:

Change the connection strings for the Insight Admin database in **ServiceConfiguration.Cloud.cscfg**.

1. Set the SQL server name, administration database name, SQL user ID, and password. If you specify an existing administration database name, it is updated to the most current version. If you specify a new administration database name, it is created automatically.
To get your SQL database credentials, navigate to **Azure > SQL Databases > Show connection strings**.
2. Leave the `Insight.TenantAdmin.MasterDBConnectionString` value blank.

```
<Setting name="Insight.Admin.MasterDBConnectionString" value="Server={ServerName};Database={DatabaseName};User ID={UserID};Password={Password};Trusted_Connection=False;Encrypt=True;Connection Timeout=30;" />
<Setting name="Insight.TenantAdmin.MasterDBConnectionString" value="" />
```

For a **multi-tenant** configuration:

Change the connection strings for the Insight multi-tenant admin database in **ServiceConfiguration.Cloud.cscfg**.

1. Set the SQL server name, SQL user ID, password, and multi-tenant administration database. If you specify an existing multi-tenant administration database name, it is updated to the most current version. If you specify a new multi-tenant administration database name, it is created automatically.
To get your SQL database credentials, navigate to **Azure > SQL Databases > Show connection strings**, and copy them to the configuration file.
2. Leave the `Insight.Admin.MasterDBConnectionString` value blank.

```
<Setting name="Insight.Admin.MasterDBConnectionString" value="" />
<Setting name="Insight.TenantAdmin.MasterDBConnectionString" value="Data Source={ServerName};Initial Catalog={MultitenantAdminDatabaseName}; User Id={userID};Password={password};" />
```

Conditionally, you may need to change the configuration settings for the data sources. For details, see the **Connection key** section in *Kofax Insight Studio Help*.

Roles and instances count

Use roles to manage the functionality of Insight on Azure. In the configuration file, find and set the scheduler role. Enter a corresponding user login. The following examples use the default user login:

- For a single-tenant configuration, specify
`<Setting name="Insight.Scheduler.Login" value="Administrator"/>`.
- For a multi-tenant configuration, specify
`<Setting name="Insight.Scheduler.Login" value="MTAdmin"/>`.

i When Insight is installed on Azure, you can [configure other role settings](#) in the interface.

Next, proceed with the role instances, which ensure uninterrupted performance: if one of the role instances fails for a reason, such as an error or disconnection, then the second instance takes over the tasks and continues the processing. The role switch doesn't affect the performance.

The minimum number of instances for the role is one. For more information, see the Microsoft documentation on cloud service specifications.

For high availability purposes, we recommend to specify two instances for each role.

Find and set `<Instances count="2"/>` and specify the number of instances. This value applies to the `InsightWebRole` and the `SchedulerRole`, and is set individually for each role in the relevant section of the configuration file.

```
<Role name="InsightWebRole" >
  <Instances count="2" />
  <ConfigurationSettings>

<Role name="SchedulerRole" >
  <Instances count="2" />
  <ConfigurationSettings>
```

Storage name, access key and virtual network

The Storage is used for Insight logs and for importing and exporting Insight files (projects).

To copy the primary access key, navigate to **Azure > Storage > Manage Access keys**. The access key provides access to the storage account. It is generated by Azure and can be regenerated if necessary.

You need to update the **ServiceConfiguration.Cloud.cscfg** file with the name and key of your storage account, and with the name of your virtual network.

1. Update the name and change the account key for `InsightWebRole`.
2. Change the account key and name for the `SchedulerRole`.
3. In the `NetworkConfiguration` section enter the name of the virtual network that you have created.
4. Save the configuration file.


Cloud service and deployment of the Insight package on Azure

After updating the configuration file, create a cloud service and upload the configuration package.

1. Navigate to **Azure portal > Cloud service (extended support)**. In the Cloud Service (extended support) pane, select **Create**.
The creation window opens in the **Basics** tab.
2. Complete the fields on the **Basics** tab.
 - a. Set the **Cloud service name** and select the **Region**.
 - b. Select **From local** for the **Package/configuration/service definition location**.
 - c. Select the **Storage account** and upload the **.cspkg** and **.csdef** files included in the `KofaxInsight-6.5.0_ForAzure.zip` package and the updated **.cscfg** file.

3. Proceed to the **Configuration** tab and complete the fields.
 - a. Select the existing **Public IP address** or create a new one.
 - b. Select **None** for **Swappable cloud service**.
 - c. Select the **Start cloud service** check box.
 - d. Select the **Key Vault** that you have created.
 - e. Click **Review + create**.

The deployment process may take about 20-30 minutes. After the deployment is complete, open Insight in a browser: [https://\[cloud service IP\]/insight/admin](https://[cloud service IP]/insight/admin). If you configure Insight in multi-tenant mode, you need to log in to the Multi-Tenant Console: [https://\[cloud service IP\]/insight/admin/MTConsole](https://[cloud service IP]/insight/admin/MTConsole).

 For details, see *Insight Admin Console Help* or *Insight Multi-Tenant Console Help*.

Chapter 2

Getting started with Kofax Insight on Azure

Kofax Insight on Azure is similar to Insight on-premises, with the exceptions noted below.

- Windows authentication is not supported.
- The Scheduler cannot be used on the client side. It is assumed that the source databases are available from within the Azure environment (from the Scheduler server instance).
- File Processor is not allowed.

For details about using Kofax Insight features, see the online help.

Distribution of Insight functionality

An Azure instance of Insight includes the following functionality.

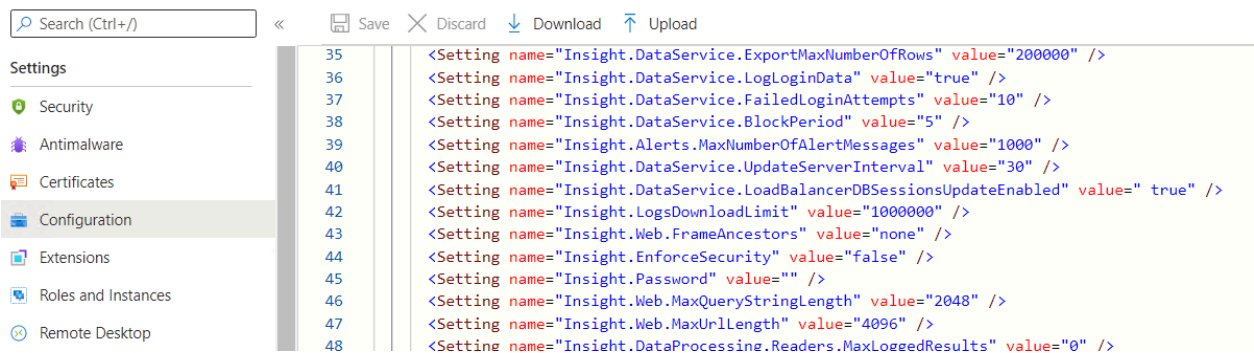
- **InsightWebRole:** Contains the Viewer, Studio, Data Loader, Themes and Formats, WCF data service, and Multi-Tenant Admin Console service.
- **SchedulerRole:** Contains the Scheduler service, such as the manual and automatic data load, alerts, and reports distribution.

Configure roles

When Insight is installed on Azure, you can configure the Insight role settings on the Azure portal.

Navigate to **Cloud Service (extended support) > Settings > Configuration**.

The configuration settings open in XML format.



The screenshot shows the Azure portal configuration page for Insight. The left sidebar lists various settings categories: Settings, Security, Antimalware, Certificates, Configuration (selected), Extensions, Roles and Instances, and Remote Desktop. The main content area displays XML configuration settings for the Insight role. The settings are listed in a table with line numbers 35 through 48. The XML settings include:

```
35 <Setting name="Insight.DataService.ExportMaxNumberOfRows" value="200000" />
36 <Setting name="Insight.DataService.LogLoginData" value="true" />
37 <Setting name="Insight.DataService.FailedLoginAttempts" value="10" />
38 <Setting name="Insight.DataService.BlockPeriod" value="5" />
39 <Setting name="Insight.Alerts.MaxNumberOfAlertMessages" value="1000" />
40 <Setting name="Insight.DataService.UpdateServerInterval" value="30" />
41 <Setting name="Insight.DataService.LoadBalancerDBSessionsUpdateEnabled" value="true" />
42 <Setting name="Insight.LogsDownloadLimit" value="1000000" />
43 <Setting name="Insight.Web.FrameAncestors" value="none" />
44 <Setting name="Insight.EnforceSecurity" value="false" />
45 <Setting name="Insight.Password" value="" />
46 <Setting name="Insight.Web.MaxQueryStringLength" value="2048" />
47 <Setting name="Insight.Web.MaxUrlLength" value="4096" />
48 <Setting name="Insight.DataProcessing.Readers.MaxLoggedResults" value="0" />
```

Configure the settings for the Web Role and the Scheduler Role. Save the changes.

i Ensure that you specify a valid user login and password for the Scheduler Role; otherwise the data load fails.

Resolve transient faults

When running a query that uses a connection string to select data from a source on the Azure SQL server, a transient fault may occur. A transient fault is typically resolved when the query is retried successfully after the connection is restored.

If a transient fault occurs, all temporary data already collected is deleted, and the data collection process is restarted when the connection to the data source is restored successfully.

Use the following procedure to set preferences for handling a transient fault situation. You can define the timing and number of attempts that are made to connect to the Administration database or a data source if a transient fault occurs.

i These settings are applied to resolve SQL server deadlocks as well. See *Insight Admin Console Help* for details.

1. Log in to the Azure portal and navigate to **Cloud Service (extended support) > Settings > Configuration**.

In the InsightWebRole configuration section, enter the values and save the changes.

- **Insight.TriesCount** (Default value is 3): Specify the number of attempts to make to connect to the data source if a deadlock or other transient fault occurs.
- **Insight.TimeBetweenTries** (Default value is 20): Set the number of seconds to elapse between each attempt to establish a connection to the data source if a transient fault occurs.

2. After the Insight package is deployed, you can define custom settings to connect to the data source. In Studio and Admin Console navigate to **Documents tree > Data Sources**, and select a data source. The connection string appears for the selected data source.


- a. In the **Property panel**, in the **Other** group, adjust these settings:

- **Time between tries**
- **Tries count**

- b. To roll back to the default settings, in the **Property panel**, in the **Other** group, set the **Tries count** parameter to **0**.

Activate the license

Obtain the product license from your Kofax sales representative or from Kofax Support. Follow the same procedure to activate the product license as described for on-premises Insight. See *Kofax Insight Admin Console Help* for more information.

 Ensure that you activate the Multi-Tenant Cloud license for Multi-tenant configuration.

Access to Insight applications

You can access all Insight web applications and services, such as the Viewer, Studio, Data Loader, Admin Console, Themes and Formats, Multi-Tenant Admin Console and WCF data service through SSL (HTTPS) only. Ensure that you use the HTTPS according to your type of configuration.

- **Single-tenant:** [cloud service IP]/insight/admin
- **Multi-tenant:** [cloud service IP]/insight/admin/MTCConsole

Kofax Insight deployed on Azure operates in two modes: View mode and Edit mode. In View mode, you can only work with the Viewer and Data Load site. To work with the other Insight applications, such as the Admin Console, Themes and Formats, Multi-Tenant Admin Console or Studio, you must enable Edit mode.


Navigate to **Admin Console** > **Actions** tab to switch modes. Depending on the current state, the **Turn on Edit mode** or **Turn off Edit mode** button is available. Clicking this button changes the mode and forces you to log in to the Admin Console again.

View mode

In view mode, when the Data Loader schedules the plans, a user can only check the logs for executed plans.

- If you try to access the other Insight applications (such as Studio or Themes and Formats), an error appears in red on the login screen: "Enter in the edit mode."
- If you try to access the Admin Console, it is opened with reduced functionality. The Actions tab only contains the Turn on Edit mode, About, and Logout buttons. The Tools tab contains the Download Logs icon.

Click **Turn on Edit mode** to enable Edit mode and to access the Studio, Data Loader, Themes and Formats, and Admin Console with full functionality, except for the restrictions described [here](#).

 In a multi-tenant configuration, Edit mode is defined for each tenant individually.

Edit mode

In Edit mode, all Insight applications are available with reduced performance.

Log management

Log management is available in any mode. Use the following procedure to download or delete log files for Insight deployed on Azure.

1. Open the Admin Console and navigate to the **Tools** tab.

2. Click the **Download Logs** button.
The **Download logs** window appears.
3. Select the log type from the list and set the interval as required.
4. Select the **Remove only** check box to delete all the selected logs. Clear the **Remove only** check box to download the selected logs. Click **OK**.
A progress indicator appears on the screen.
5. If you selected to remove the log files, you are returned to the Admin Console with the **Tools** tab selected. If you selected to download the log files, they are downloaded to your device in a file named **ExportLogArchive.zip**.

Use Azure Key Vault to store the connection settings

Insight uses service principal with a certificate authentication to access the Azure Key Vault. The certificate is assigned to the cloud service and to service principal, which allows you to authenticate using the Key Vault.

Complete the following steps to store your connection settings in the Key Vault and use them for authentication.

1. Review the instructions on the Microsoft Azure pages and complete the following steps.
 - a. [Create service principal in the Azure Active Directory](#).
 - b. [Get the Azure tenant and app ID values for signing in](#).
 - c. [Upload a certificate](#).
2. Save the app ID values and certificate settings in the .cscfg file. For example,

```
<Setting name="Insight.Application.ClientId" value="3ce0f0b2-6d41-4dac-aa71-5fa6bfb33d23"/>
<Setting name="Insight.Application.TenantId" value="f6acd565-bf47-4dfc-b17b-8d6fec7718ff"/>
<Setting name="Insight.Application.CertThumbprint"
value="B51D77FC2700000B4BC85845AF8040ECA41C30D"/>

<Certificate name="Insight.Application.ClientCert"
thumbprint="B51D77FC2700000B4BC85845AF8040ECA41C30D"
thumbprintAlgorithm="sha1" />
```

3. Assign the appropriate access policy to service principal in the Key Vault.
4. To use Secrets, add them to the Key Vault and copy the Secret's URL.
5. Add the Secret's URL to the .cscfg file as setting value. For example,

```
<Setting name="Insight.Admin.MasterDBConnectionString"
value="https://insightdkvault.vault.azure.net/secrets/adminconnection/82fd348adc3a46b4b41d3979e00e20c2" />
```