



# Kofax Insight Installation Guide

Version: 6.5.0

Date: 2022-09-20

**KOFAX**

© 2013–2022 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

<b>Preface</b> .....	<b>5</b>
Product documentation.....	5
Offline documentation.....	6
<b>Chapter 1: Introduction</b> .....	<b>7</b>
Insight Web Applications.....	10
Insight Data Services.....	11
Insight Scheduler.....	12
<b>Chapter 2: System requirements</b> .....	<b>13</b>
Server software.....	13
Microsoft packages required.....	13
IIS web server.....	13
Metadata repository.....	15
Insight license.....	15
Databases.....	15
Administration database.....	16
Project databases.....	16
Multi-tenant database.....	16
Combine Administration, Meta, and Data databases.....	16
Database access rights.....	17
Port requirements.....	18
Multi-tenancy overview.....	19
<b>Chapter 3: Installation</b> .....	<b>21</b>
Install Kofax Insight.....	21
Run Insight Installation Manager.....	22
General settings.....	23
Insight Web Applications IIS Settings.....	24
Insight Data Services Settings.....	25
Scheduler Service Settings.....	26
Activate the product license.....	27
Change Insight configuration after installation.....	27
Change the encrypted key after installation.....	28
Run a silent installation.....	28
Silent installation sample configuration files.....	30
Set up Insight in a three-tier architecture.....	33

Web server layer.....	34
Application server layer.....	35
Upgrade Insight.....	35
Upgrade the Insight version and Admin database.....	36
Upgrade existing projects.....	36
Install Insight 6.5.0 alongside previous version.....	37
Install Kofax Insight on Docker.....	37
Set up Insight in high availability mode.....	39
Install Insight in high availability mode in two-tier architecture.....	40
Activate the product license.....	45
Install and configure Insight in high availability mode in three-tier architecture.....	46
Set up Insight in high availability mode on Azure Kubernetes.....	48
Set up Insight in high availability mode on Docker with Swarm on-premise environment.....	50
<b>Appendix A: Recover from a lockout.....</b>	<b>52</b>
Log in to an application as an Insight user.....	52
<b>Appendix B: Repair connection strings and apply a new encryption key.....</b>	<b>53</b>
<b>Appendix C: Set up and configure the load balancer.....</b>	<b>54</b>
Settings for the web farm.....	54
Insight-specific cookies.....	54
<b>Appendix D: Windows Active Directory authentication support.....</b>	<b>56</b>
Configure the IIS environment.....	56
Troubleshoot Windows Active Directory authentication.....	57
<b>Appendix E: Insight log files.....</b>	<b>58</b>

# Preface

This guide includes instructions for installing and upgrading Kofax Insight, and for activating the product license.

## Product documentation

The Kofax Insight documentation set is available online at the following URL<sup>1</sup>:

<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.

---

<sup>1</sup> 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.

## Offline documentation

To make the documentation available for use in offline mode (without an active Internet connection), obtain the documentation.zip file from the product package that you downloaded from the [Kofax Fulfillment Site](#). The product package includes the following documentation files for offline use:


- KofaxInsightDocumentation\_6.5.0\_EN.zip  
Contains the entire product documentation set in English.
- KofaxInsightDocumentation\_6.5.0\_JA.zip  
Contains the entire product documentation set in Japanese.

For each language, the .zip files include the following folders:

- The **print** folder contains the Kofax Insight Installation Guide and Kofax Insight Administrator's Guide for Azure.
- The **help** folder contains Kofax Insight Admin Console Help, Kofax Insight Studio Help, Kofax Insight Data Loader Help, Kofax Insight Multi-Tenant Console Help, Kofax Insight Viewer Help, Kofax Insight Themes and Formats Help, API Online Help, and Tutorial and Sample Project Help.

1. Obtain the compressed documentation package for the required language from the Kofax Insight 6.5.0 product package that you downloaded from the Downloads page on the Kofax Fulfillment Site.
2. Create the **Documentation** folder to extract the contents of the documentation .zip file to the following location:  
`[drive:]\Program Files\Kofax\Insight 6.5.0\HtmlInsight\Documentation`
3. Start any Insight application and click the Help icon to open the help in a separate browser window.

To use the PDF documentation offline, you can open it from the Documentation folder or from another location on your computer. When the offline documentation is installed for Kofax Insight according to these instructions, the product will use the offline version of the documentation by default, even if an active Internet connection exists.

 The Documentation folder is not removed automatically in case the product is uninstalled. You need to delete it manually.

## Chapter 1

# Introduction

This document describes the components and its technical architecture for Kofax Insight 6.5.0.

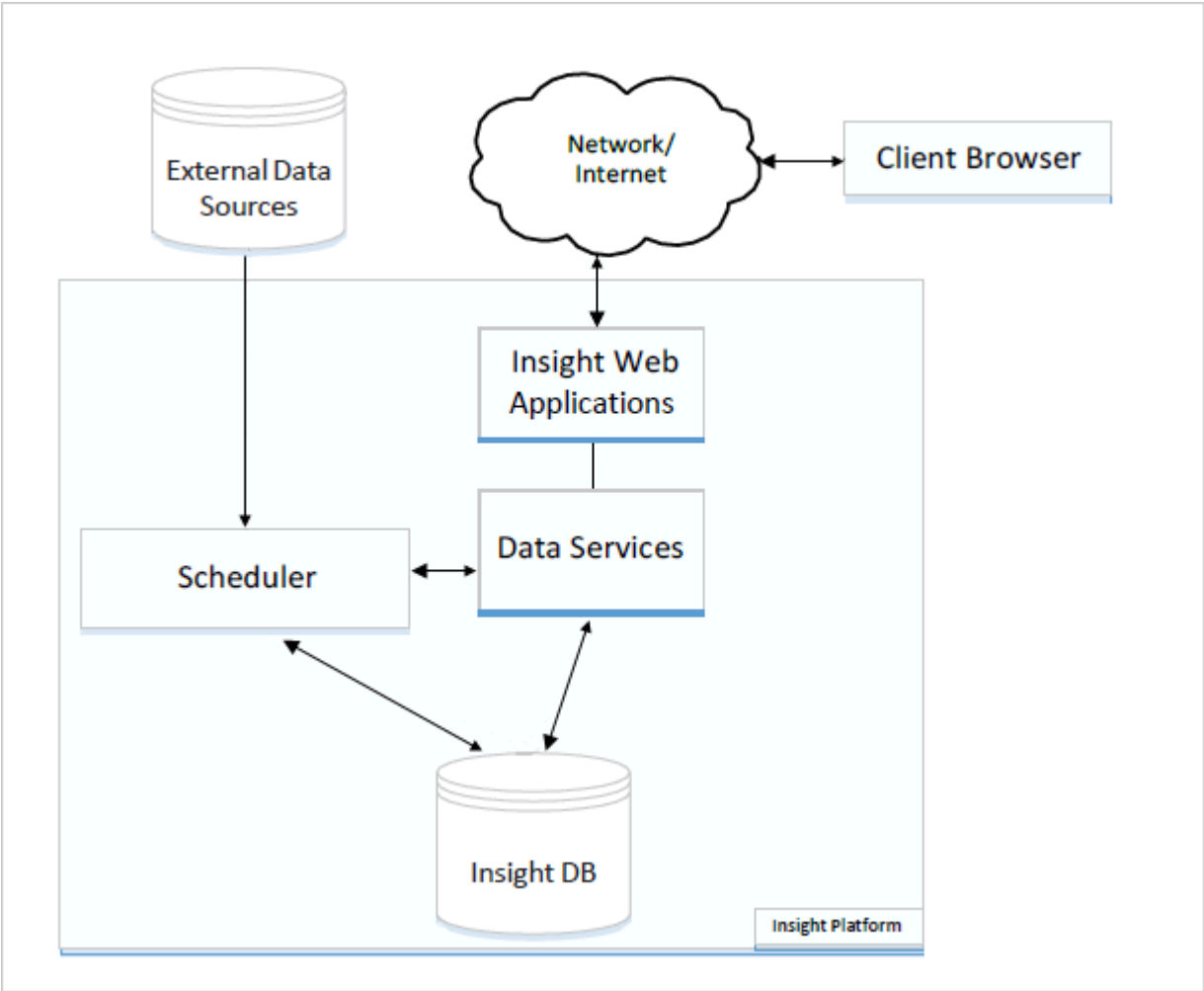
Kofax Insight is a browser-based system that runs on HTML5/JavaScript supported browsers. The server components are built on the Microsoft .NET Framework and run on Windows (64-bit)/IIS servers.

Kofax Insight consists of the following main components:

- Insight Web Applications
- Insight Data Services
- Scheduler
- Insight Database

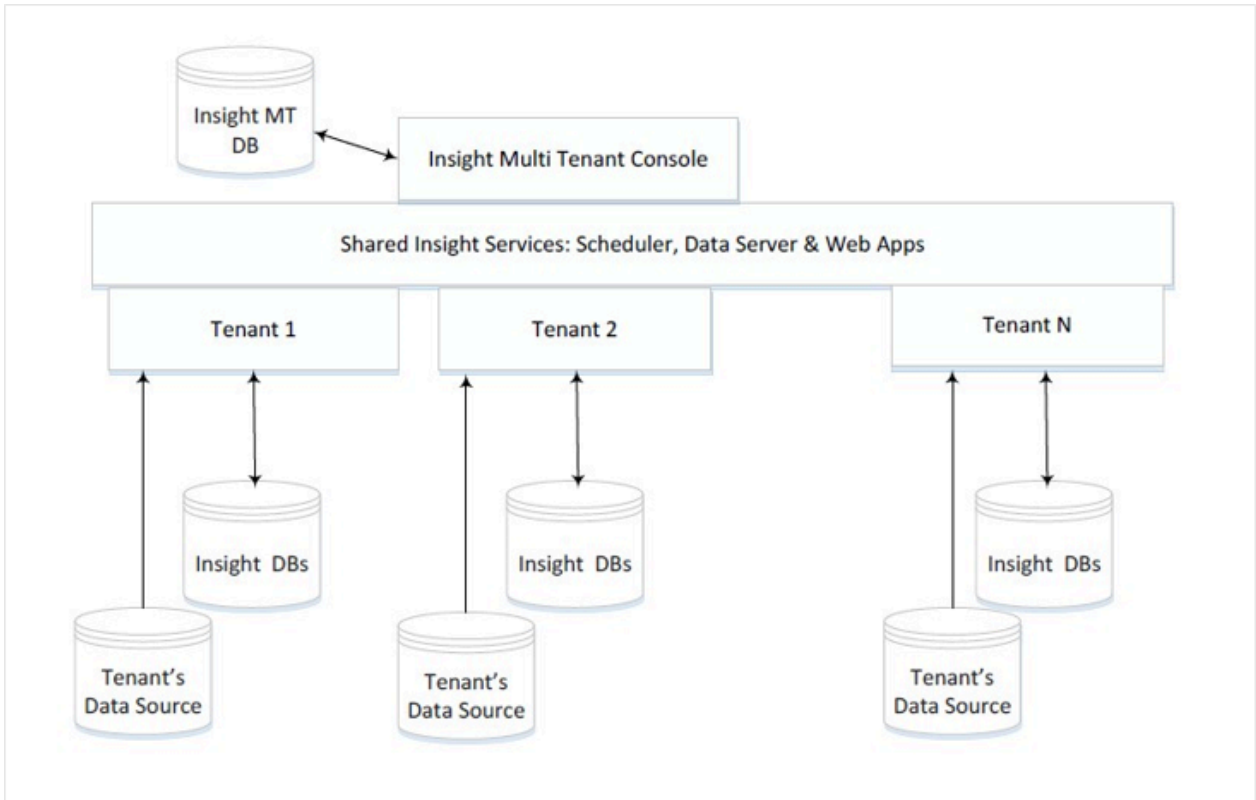
Kofax Insight can be deployed in a single-tenant or multi-tenant mode.

The following diagram displays the architecture of Insight deployed in a single-tenant mode. In this document, "DB" is used to denote "database."



The following diagram shows the architecture of Insight deployed in a multi-tenant mode.





Each tenant can be set up with the Kofax Insight Multi-Tenant Console application. Once a tenant is set up, use the following URL to access the Insight tenant environment:

```
http(s)://<tenant_id>.<host:port>/Insight/[Admin|Studio|View|Themes|DataLoader]
```

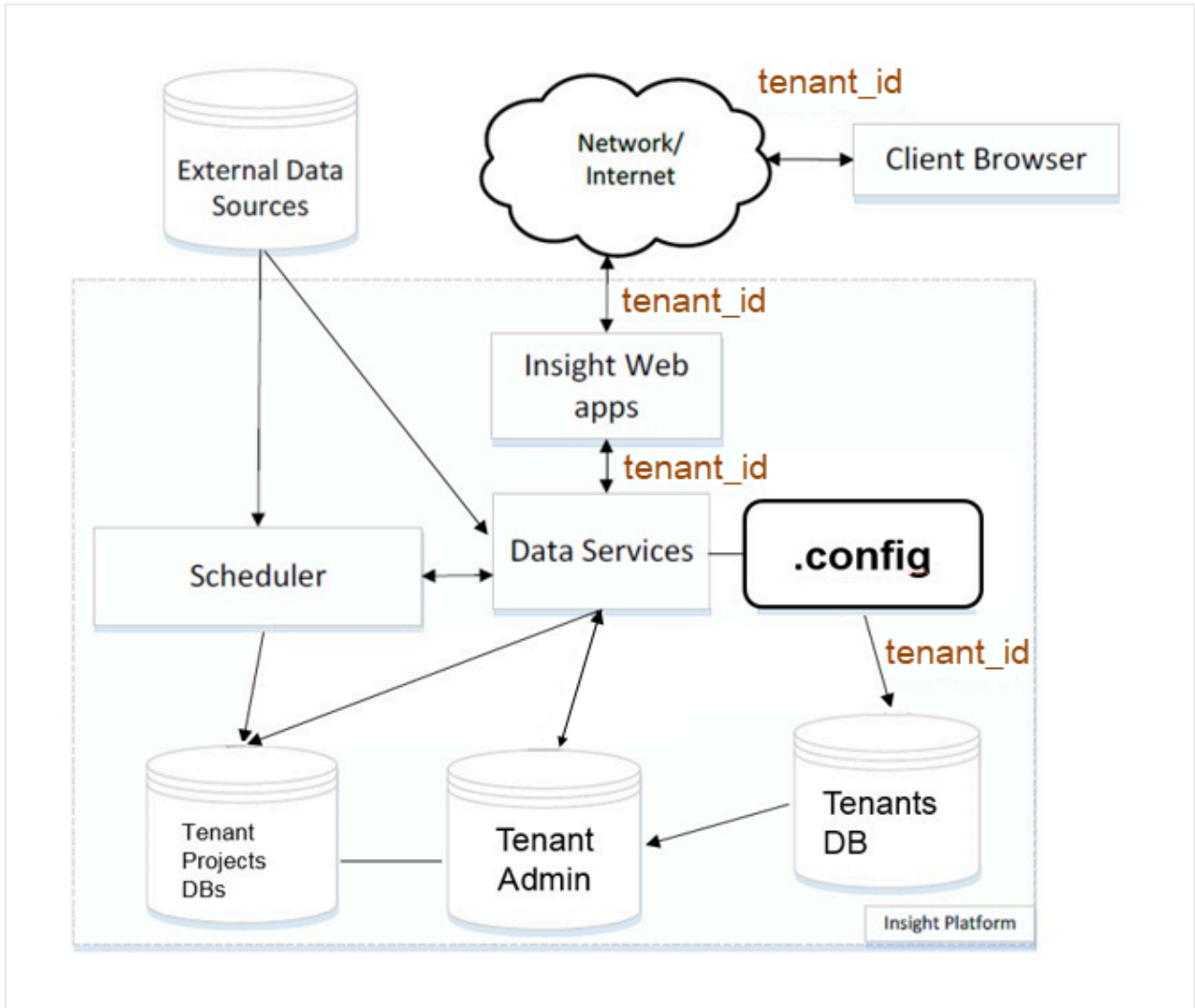
For example, if Insight is set up on a domain named *MyInsight* and a tenant with a tenant ID called *tenant2*, tenant2 can access Insight using the following URL:

```
http://tenant2.MyInsight.com/Admin
```

The Tenant (Customer) admin should have a record in the DNS for the subdomain that points to the same IP as the domain.

When an Insight application gets a request, Insight reads the tenant ID and sends it to the Data Service as an additional parameter.

Insight Data Service reads the tenant ID from parameters and then retrieves the connection string to the Admin DB of the tenant from the Insight MT database. Insight authenticates the user in the same way as in a single-tenant mode.



## Insight Web Applications

The Insight Web Applications provide the user interface to the Insight platform. The user interface, which serves as the presentation layer of the Insight system, consists of the following applications that allow a user to configure and manage Insight:

Name	Physical Name	Type	Description/Functions
Admin	Admin	Website	Provides access to Insight License Manager, along with configuration settings related to authentication, users, roles, and access rights. Also used to create and manage Insight projects and to import Analytics solutions.
Data Loader	DataLoad	Website	Logs, manages and schedules data loads from various data sources into Insight Data Mart.
Studio	Studio	Website	Manages Insight project documents such as metrics and records, views (dashboards), data sources, execution plans, file processor, reports, and audit.
View	View	Website	Provides access to the view (dashboard) for the end user.
Themes & Formats	Themes	Website	Manages all themes and formats used in the dashboards and Insight projects.

## Insight Data Services

Data Services, the application layer of the Insight system, provides authentication, data management, and Analytics services for Insight. The Data Services connect to the Insight databases and communicate with the Web applications and Scheduler. Data Services components are listed in the table.

Name	Physical Name	Type	Description/Functions
WCFData	WCFDataService	.NET WCF Service	Provides authentication, Insight document management and data analytics services.
Chart Snapshot	ChartSnapshotService	.NET WCF Service	Prints the reports.

## Insight Scheduler

The Insight Scheduler is a Windows service that launches a Scheduler-Data Loader EXE that loads the data from external data sources into the Insight Data Mart (Insight project data database). The default Insight Scheduler Service port is 13501. If you are upgrading a previously installed version of Insight to version 6.5.0, the port will be switched to default 13501 during the installation. You can specify any port in the Insight Installation Manager.

Name	Physical Name	Type	Description/Functions
Scheduler	InsightSchedulerServiceXYZ	Windows Service	Launches the EXE that loads the data. <i>The XYZ in the name is the version number (if a second version is installed in the same environment), for example, 650 is version 6.5.x. .</i>
Scheduler - Data Loader EXE	Altosoft.Insight.DashboardServer.exe	EXE	Performs the data load operation of a single execution plan.

## Chapter 2

# System requirements

The system requirements (hardware and software) for Kofax Insight are listed in the *Kofax Insight Technical Specifications* document, which is available from the Kofax Insight 6.5.0 [Support pages](#) on the Kofax website. We recommend that you review the document carefully before installing your product. This chapter is intended to supplement the *Technical Specifications* document and to offer details about databases, ports, and related requirements.

## Server software

See the *Kofax Insight 6.5.0 Technical Specifications* for information about requirements and supported versions for the following:

- Operating system
- .NET Framework
- HTML 5 Browser with enabled cookies
- IIS Web Server
- Database management system

## Microsoft packages required

The **Microsoft Visual C++ 2015 SP1 Redistributable** (x64) package or higher must be pre-installed on the server where you install Insight. If you plan to install Insight in a 3-tier environment, install the Microsoft package on the server that runs the WCF Data Services.

Also, the **Microsoft .NET Framework 4.7.2 or later** must be pre-installed on the server prior to installing Insight.

On the server where Insight is installed, you are encouraged to install **Microsoft Access Database Engine 2016 Redistributable** to work with Excel files (.xls or .xlsx) as a data source, create records on files as data sources, or to load and use custom shapes for the Map component.

You can obtain the Microsoft Access Database Engine from the Microsoft website and install it after Insight is set up.

## IIS web server

Before installing Insight, verify that Internet Information Server (IIS) is enabled and configured. While IIS is provided with all Windows servers, it is not installed by default; you must ensure that the installation is complete.

❗ When you configure Insight manually on IIS, the application pool (default or custom) must be .NET v4.x. For **Managed pipeline mode**, select **Integrated**.

When using a custom application pool, you must have a dedicated application pool that contains the ChartSnapshotService. If you use an Active Directory account for an application pool, it must have the same level of permissions as the NetworkService. We recommend that the application pool has the idle timeout set to zero, so that it always remains active.

## Configure IIS

1. Using Control Panel, navigate to **Administrative Tools > Server Manager**.
2. In **Server Manager**, select **Add roles and features**.
3. In the **Add roles and features** wizard, under **Server Roles**, select **Web Server (IIS)** and expand the list to select the following options.
  - Common HTTP features:
    - Static Content
    - Default Document
    - HTTP Errors
    - HTTP Redirection
  - Health and Diagnostics
    - HTTP Logging
  - Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - IIS Client Certificate Mapping Authentication
    - URL Authorization
    - Windows Authentication
  - Application Development
    - .NET Extensibility (use the latest version)
    - ASP.NET (use the latest version)
    - ISAPI Extensions
    - ISAPI Filters
  - Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
    - Management Service
4. Click **Next** to configure the **Features** and select the following options:
  - .NET Framework 4.x (select the latest version)
    - WCF Services
      - HTTP Activation
5. Click **Install** to install the selected roles and features.

❗ For IIS 10 on Windows 2016, when you add Role Services for the server, select all the features related to the IIS Web Server. Later, when IIS is installed, you may remove all unnecessary features.

## Configure IIS for Windows 7 and Windows 8

1. Using Control Panel, navigate to **Programs > Programs and Features**.
2. Click **Turn Windows features on or off** and select **Internet Information Services**.
3. Select the required options and click **OK**.

## Metadata repository

Kofax Insight stores its metadata and calculated data in either Oracle, Microsoft SQL Server, or MySQL databases. The database can be located on a dedicated server or on the same shared server with Insight.

If you want to use a separate server, install it prior to installing Insight.

## Insight license

Although you can perform a new Insight 6.5.0 installation without a license, you cannot use the product until the [license is activated](#). When upgrading to Insight 6.5.0 from version 5.x or 6.x, you can continue with the current license without reactivating it. If you need help to obtain an Insight license, contact the Insight Sales team.

To use multi-tenancy, you need to get a multi-tenant license, which is available separately.

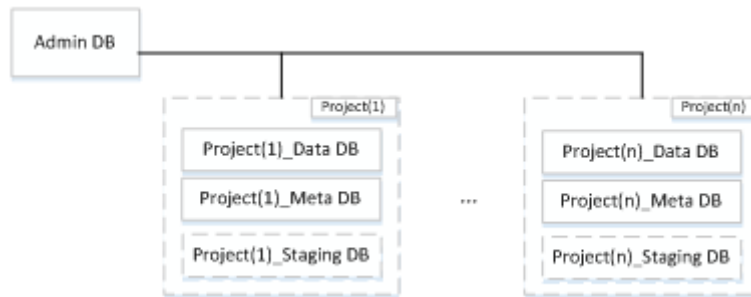
## Databases

The Insight Application server and Scheduler must be able to access the data to be analyzed. If the databases are accessed over a network connection, you must verify the necessary security/firewall settings and the availability of the drivers required for the target databases.

i The Insight uninstall procedure has no impact on the databases.

The Insight database structure consists of the following:

- Admin database
- Project databases
- Multi-tenant database (if applicable)



## Insight Database Structure

**i** The Staging database is optional.

## Administration database

The Administration database stores administrative data related to the Insight environment and projects, including users, roles, filtering, alert messages, logs, themes and formats. The Administration database contains connection to the Project Meta database, and information about other databases is stored in the Meta database of each project.

One Administration database exists per Insight server. You can use the MS SQL Server, Oracle, or MySQL for the Administration database.

## Project databases

Each Insight project consists of the following databases:

- **Meta database:** Stores configuration information about the documents that make up a project. The project documents include data sources, records, metrics, translation tables, view (dashboard), reports, execution plans, file processor, processes, parameters, constants, and accelerators.  
No data is stored in the Meta database, which stores localization strings for project documents.
- **Data database:** Stores the data related to processed records, metrics, and other project documents. A new table is created for each document, and the database schema is updated as documents are added, modified, or removed.
- **Staging database (optional):** Stores the data for external files parsed by the file processor. Examples include XML, CSV or Excel files.

## Multi-tenant database

If you have a Multi-tenant license, see [Multi-tenancy overview](#) in this guide for details.

## Combine Administration, Meta, and Data databases

In case of limited resources, all tables can be physically located in a single MS SQL database upon condition of using different schemes. To use this option, you can create multiple users with different



default database schemas, such as Meta, Data, and Admin. Later, when configuring the connection, you can use a single database and different users.

## Database access rights

Insight requires the rights to create, drop and modify index and tables for the Admin, Meta, Data or staging databases.

### MS SQL Server

The database administrator can create three databases. An SQL user should have privileges (or have a membership) in the following groups:

- db\_datareader
- db\_datawriter
- db\_ddladmin

Also, the database administrator can create an SQL user with the privilege of creating databases (or have a membership of the db\_creator role). In this case, Insight creates databases automatically and no additional assignment of rights is required.


#### Database Connectors

No additional drivers or connectors are required for Insight to connect to the MS SQL Server.

### Oracle

#### Database Connectors

Insight requires the Oracle Data Provider for .NET (ODP.NET), which is available in the Oracle Data Access Components (ODAC) for Windows Downloads pages on the Oracle website. Be sure to select the ODP.NET option when you perform the Oracle database installation.

 If you use "Xcopy," make sure that you complete all installation steps appropriately, including registering the libraries in .NET and the registry.

#### Access Rights to the Oracle Database

The user must have the following access rights:

- CREATE SESSION
- CREATE TABLE
- CREATE PROCEDURE
- CREATE SEQUENCE

The user must have an appropriate tablespace (also temporary tablespace) quota. Indexes will be stored in the same tablespace.

Example:

```
CREATE USER <USER NAME>
```

IDENTIFIED BY <PASSWORD>  
DEFAULT TABLESPACE <TABLESPACE NAME>  
QUOTA UNLIMITED ON <TABLESPACE NAME>  
GRANT  
CREATE SESSION  
CREATE TABLE  
CREATE PROCEDURE  
CREATE SEQUENCE  
TO <USER NAME>

### Register ODP.NET in Oracle client 18/19

Machine-wide configuration is no longer supported beginning with ODAC 18c. Administrators can still place ODP.NET in the GAC and add the configuration section handler and DbProviderFactory information to machine.config manually to override the ODP.NET settings for individual applications. For details, see the Oracle support website.

To register ODP.NET, perform the following actions:


1. Use the OraProvCfg file located at [drive]:\<app>\client\Administrator\product\19.0.0\<client\_1>\odp.net\bin\4
2. Run the following commands:  
oraprovcfg /action:gac  
/providerpath:[drive]:\<app>\client\Administrator\product  
\19.0.0\<client\_1>\odp.net\bin\4\Oracle.DataAccess.dll  
oraprovcfg /action:config /force /product:odp /frameworkversion:v4.0.30319  
/providerpath:[drive]:\<app>\client\Administrator\product  
\19.0.0\<client\_1>\odp.net\bin\4\Oracle.DataAccess.dll

## MySQL

MySQL Connector/NET is required only if you use MySQL. On the MySQL Connector/NET website, select a version that is compatible with your version of MySQL.

## Port requirements

Insight uses the ports listed in the table.

Component name	Default port	Comments
Insight Web and Data applications and services	80 or 443 for https	<p>The ports can be reconfigured during installation. To reconfigure the port after Insight is installed, do the following.</p> <ol style="list-style-type: none"> <li>1. Open a Command Prompt window.</li> <li>2. Run <code>&lt;installation folder&gt;\Insight 6.5.0\InstallationManager\Altosoft.InsightInstallManager.exe /i.</code></li> </ol>
Insight Scheduler service (Windows service)	13501	<p>If you have a pre-installed version of Kofax Insight and are upgrading it to Insight 6.5.0, the port will be set to default 13501 during the installation. If the default port is already in use, the port will be switched to 13650.</p> <p>You can change the port in the Installation Manager.</p>
Insight Bridge service (Windows service)	15501	<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p> The Insight Bridge Service is an optional service. It is not installed by default.</p> </div> <p>If you have a pre-installed version of Kofax Insight and are upgrading it to Insight 6.5.0, the port will be set to default 15501 during the installation. If the default port is already in use, the port will be switched to 15650.</p> <p>To change the port, do the following.</p> <ol style="list-style-type: none"> <li>1. Navigate to the Insight installation folder at <code>\Program Files\Kofax\Insight 6.5.0\InsightBridgeService\</code> and in the <code>Altosoft.Insight.BridgeService.exe.config</code> file, change the port in the <code>InsightBridgeService</code> property.</li> <li>2. Navigate to the Insight installation folder at <code>\Program Files\Kofax\Insight 6.5.0\SchedulerServer\</code> and in the <code>AltoSoft.Insight.Scheduler.exe.config</code> file, change the port in the <code>BridgeServiceURL</code> property.</li> <li>3. Navigate to the Insight installation folder at <code>\Program Files\Kofax\Insight 6.5.0\Server\</code> and in the <code>AltoSoft.Insight.DashboardServer.exe.config</code> file, change the port in the <code>BridgeServiceURL</code> property.</li> </ol>

## Multi-tenancy overview

In Insight, you can use multi-tenancy to deploy multiple customers (tenants) on the same set of Insight servers where each tenant's data and configuration is protected from other tenants. At the same time, each tenant can configure its own projects, users, authentication, roles, themes, and other parameters.

Each tenant has its own Insight databases (Admin DB, Meta DB, Data DB), and information about all tenants is stored in the Insight MT (Multi-tenant) DB.

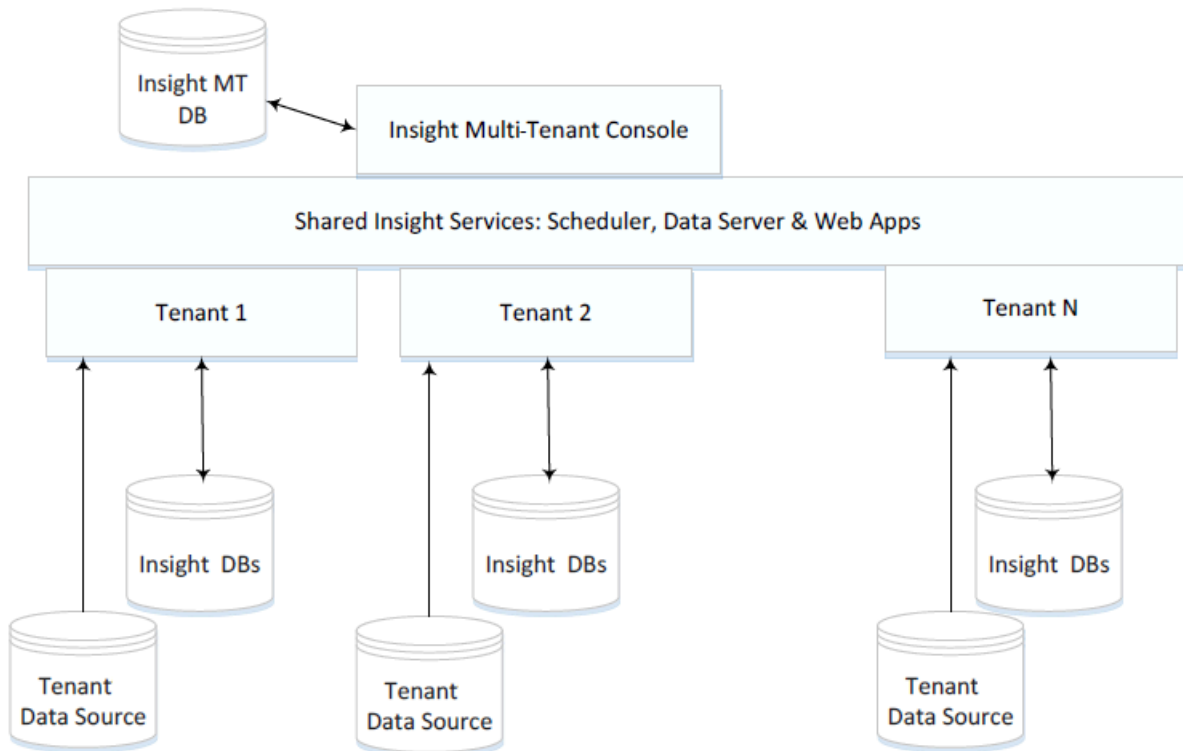
The Multi-tenant Administrator has the following rights:

- Access to the full Insight system and all the tenants
- Access to Multi-Tenant Console
- Ability to add/remove tenants
- Perform other actions with tenant's configuration (upgrade, password setup, and more).

A Tenant Administrator has the following rights:

- Access to all the Insight applications with the exception of Multi-Tenant Console.
- Full control over the projects, users, and data within a single given tenant.

The following overview diagram shows the basic principles of multi-tenancy in Insight.



## Chapter 3


# Installation

This chapter includes instructions for installing Kofax Insight. Installation is a two-part process:

1. Run the [Insight installer](#) to copy the necessary files to the server.
2. Run the [Insight Installation Manager](#) to create and configure the Insight database and Insight websites on IIS.

Insight includes a silent installer for performing an Insight installation without manual input. See [Run a silent installation](#).

Also, it is possible to [install Insight on Docker](#).

 If you reinstall or upgrade Insight, the procedure may overwrite existing configuration files. Therefore, before performing any of these procedures, be sure to back up any configuration files that contain custom settings. After completing the Insight upgrade, you need to manually reapply any required customization to the new configuration files.


## Install Kofax Insight

1. Download the Kofax Insight product files to the computer where you plan to install the product.
2. Extract KofaxInsight-6.5.0\_64-bit.ZIP.
3. Run the applicable .msi file, such as **KofaxInsightSetup\_6.5.0.0.0.<NNNN>\_x64.msi**, where <NNNN> is the Insight build number listed in the "Version information" section of the *Kofax Insight 6.5.0 Release Notes*.  
The installation wizard appears.
4. Click **Next**.
5. If the installer is not being run as the administrator, a notification window appears. In this situation, click **Restart** to run as the administrator.
6. Review the license agreement, select the check box to accept the terms, and click **Next**.
7. On the **Kofax Insight Setup** screen, select **Full environment** and click **Next**.  
If you are performing a custom installation, see [Set up Insight in a three-tier architecture](#).
8. On the **Custom setup** page, accept or change the default installation folder.
9. Specify a folder or browse to select the location for storing log files. Initially, permissions to the log folder are granted to everyone.
10. For the **Data root folder**, leave the default folder [drive:]\Temp\InsightData or browse to another location. You can change this folder later, after Insight is

installed, in the `Web.config` file located at `Program Files\Kofax\Insight 6.X.X\WcfDataService` and in the file `Program Files\Kofax\Insight 6.5.0\Server\Altosoft.Insight.DashboardServer.exe.config`. You need to set a new folder to the `Insight.DataService.FileRootDirectory` settings and assign required rights to the user. The Insight pool user and scheduler login user must have read/write permissions to this folder. The **Data root folder** is used for all files that you upload through Insight. Initially, access rights to this folder are assigned to everyone. This folder can contain the following sub-categories.

- **Solution:** Stores all ZIP files for solution import and creating a project.
- **ImportExport:** Stores all extracted project and solution files.
- **<ProjectName>:** Default subfolder that stores data for the project. You can create individual subfolders for your projects as required.
- **Encryption key:** You can store the encryption key used for security purposes.


11. Click **Next**.

 If you install multiple instances of Insight for high availability, share access to the Data root folder so that all Insight instances can access it.

12. On the **Ready to install Kofax Insight** page, click **Install** to begin the installation.

13. On the **Completed the Kofax Insight Setup Wizard** page, click **Finish**.

The Insight Installation Manager appears. For instructions, continue to the section *Run the Insight Installation Manager*.

 After a successful installation, all installation steps are logged to a file in the log folder specified previously on the "Custom setup" page. If the installation fails, you can check the respective log in the **Event Viewer**.

If you are new to Insight, we encourage you to review *Kofax Insight Tutorial* to get started with the product.

## Run Insight Installation Manager

Use the Insight Installation Manager to select single- or multi-tenant mode, specify the Insight database, type of connection, the Insight websites on IIS, and configure remote data services and scheduler authentication.

In most cases, the Insight Installation Manager is launched automatically after you run the Insight installer to copy files to the server. You can also launch the Insight Installation Manager from your Insight program folder. When you run the Installation Manager after the first successful configuration, you need to provide credentials for any Admin user. Also, you can use Windows authentication.

If you need to run the Insight Installation Manager to repair configuration settings or change IIS settings, start the Command Prompt and run the following command:

```
<installation folder>\Insight_6.X.X\InstallationManager  
\Altosoft.Insight.InstallManager.ui.exe /i
```

## General settings

When the Insight Installation Manager is launched, you are prompted to set up a database for Admin Console to store information.

Specify the following information:

1. Select the Insight mode: **Single** or **Multi-Tenant**.

**i** If you select to deploy Insight in multi-tenant mode, you need to add the license and configure tenants using the Multi-Tenant Console application. To log in as a Multi-tenant administrator, use the *MTAdmin* user name and enter the password.

2. Select the **High Availability** check box to turn the [high availability](#) mode on.
3. **Connection Type:** The server to use (Microsoft SQL, Oracle, or MySQL).
4. **SQL Server Name:** Enter the server name or the TNS name for the database server.  
If you use MySQL or Oracle, ensure that you have the necessary database drivers installed prior to installing Insight.  
For the Microsoft SQL server, you can use the **Windows authentication**.
5. **Login and Password:** Provide the login credentials for an Administration database.  
For the Oracle database, you need to create a user with privileges before installation. For the Microsoft SQL and MySQL databases, Insight creates new databases automatically if they do not exist, but the user must have required privileges for creating a database. As another option, you can create the Administration database before installation.
6. Select the **Administration Database Name** to assign a name.
7. Use **Additional Connection String** to define additional parameters for a connection string.
8. Select the **Use Custom Key** check box to encrypt the Insight connections for security purposes. Two options are available:
  - **Generate New Key:** In this case, the key is generated and stored in a local folder with Insight licenses. To save the key also in the Data Folder, select the respective check box.
  - **Use Existing Key:** Select this option and click **Open file** to specify the path to an existing encryption key. In this case, the key is copied to a local folder with Insight licenses.
9. Select the **Save to Data Folder** check box to save the key in the Data Folder. This is required for the purposes of high availability: If you change the key, you do not need to change it for each computer.

The following connections are encrypted:

- Connection to the Administration database
- Connection document from Admin Console
- Connection to the project meta and data databases
- Connection used in the Data Source document to the databases

**Important:** If the generated file in the Data Folder [gets lost](#), you will not be able to work with all of these connections.

You may later change the generated key by running the [Insight Installation Manager](#) or through the [silent installation](#).

10. Under the **Localization** group, use the drop-down lists to set **Insight Locale** and **Viewer Locale**. By default, English locale is selected.

11. Click **Next**.  
The Insight Web Applications IIS Settings page appears.


## Insight Web Applications IIS Settings

Define the following web application settings:

- Set the **Host** and **TCP Port** parameters, and the protocol that will be used for all URLs.
  - Host:** The default host address is **127.0.0.1**. You can enter the server domain name or the IP address where Insight is installed to access the website.
  - TCP Port:** The default TCP/IP port when using SSL (HTTPS) is 443, and the default non-secure (HTTP) port is 80.
  - Use TLS/SSL:** Select this check box to enable the encrypted connection.
- Under the **Application Pool** group, define the **Application Pool Name**: Select the created IIS pool name or enter the new pool name.



3. Optional. Click **Set Identity** to define the application pool identity.
  - a. Under the **Service account** group, click **Application Pool Identity**. In the displayed dialog box, select one of the following options:
    - **Network Service**
    - **This account:** Enter the Account Name or Domain\User name. If you plan to use Windows authentication to access a database, specify the account that has access to this database.
  - b. Set and confirm the password.
  - c. Click **OK** to save changes and quit the screen.
4. **Web Site Name:** If you already created an IIS website, select it from the list and make sure that the entered TCP port is assigned to this site. Otherwise, make sure that the entered TCP port is available and click **New** to create a new website.
  - a. In the **Add Website** dialog box, enter the **Site Name**.
  - b. In the **Binding** group, set the **Type**, **Port**, and **Host Name**.

 We strongly recommend that you use an SSL connection. Use IIS Manager to create or import SSL certificate before you continue with the Installation Manager. For information on how to set up SSL on IIS, see the Microsoft support website.

If you use HTTPS binding type, select the **SSL Certificate** from the list.

After you save the changes, the **Use TLS/SSL** check box is automatically selected. To change the SSL settings after the installation is finished, see the procedure in [Change Insight configuration after installation](#).

- c. Click **OK** to save the changes and close the dialog box.

## Insight Data Services Settings

1. Select the **Enable Windows authentication for Data Service** check box. It is required to enable this option if you are going to use [Windows authentication](#) for any Insight components.
2. Under the **Insight Data Services Settings** group, select the **Enforce password policy** check box to enforce the following requirements for the Administrator password:
  - Contains at least eight characters
  - Contains at least one alpha character (a-z; A-Z)
  - Contains at least one numeric character (0-9)
  - Contains at least one special character (Examples: @ & % \*)
3. Specify the Administrator or Multi-Tenant Administrator password and then type it again.
4. If you want to connect to Data Services on a remote server, select the **Use remote Insight Data Service** check box, set the **Host**, **TCP Port**, and enable the **Use TLS/SSL** option.
5. Optional. Select the **Use only for Scheduler service** check box to apply the remote service settings only for the Scheduler service.

Insight Installation Manager

# KOFAX

Insight Installation Manager  
Components Installation

## Insight Web Applications IIS Settings

Host:  TCP Port:   Use TLS/SSL

Application Pool Name:

Web Site Name:

Create a new application pool in IIS for Insight or use an existing pool.  
The selected pool must use .NET Framework 4.0 and have the Managed Pipeline Mode set to Integrated.  
Contact your system administrator for clarification regarding the properties of the existing pools.

## Insight Data Services Settings

Enable Windows authentication for Data Service  
Check this if you are going to use Windows authentication for Insight components

Enforce password policy

Administrator password:

Use remote Insight Data Service  
Use this option to install the Data Services on a remote server.

Host:  TCP Port:   Use TLS/SSL

Use only for Scheduler service


6. Click **Next**.  
The **Scheduler Service Settings** screen appears.

## Scheduler Service Settings

Define the following Scheduler Service settings:

1. Under the **Service account** group, select one of these options:
  - **Network Service**
  - **This account:** Enter the login and password and then confirm the password. If you plan to use Windows authentication to access databases, specify the account that has access to these databases.
2. Under **Insight Authentication method**, specify the credentials for Scheduler to access the Data service. Use one of the following options:
  - **Insight User:** Enter the Insight user login, type and confirm the password.
  - **Windows authentication**

3. The default Insight Scheduler Service port is 13501. If the default port is already in use, and you are upgrading a previously installed version of Insight to version 6.5.0, the port will be switched to 13650 during the installation. You can specify any port in the Installation Manager.
4. Click **Next** and review the setup details. After reviewing, click **Next**. To make changes, click **PREVIOUS** to return to the previous pages.  
A list of installed components appears while the installation is in progress.
5. When notified that the Insight 6.5.0 installation is complete, click **Next**. Select **Admin Console** to activate the product license. Also, you can select one of the following options.
  - Use **Manage Settings** to update the Insight IIS settings or the Insight Admin database.
  - Use **Admin Console** to activate the product license and configure the projects, users, roles, and rights.
  - **Setup Kofax Analytics Project** to start the Kofax Analytics installation wizard. For details, see *Insight Admin Console Help*.
  - Use **Exit** to clear the notification message and return to the desktop.

 Before proceeding to the next section, we recommend that you check for and apply any fix packs that may be available for Insight 6.5.0.

## Activate the product license

Verify that you have the Insight license file provided at the time of your product purchase, and then use Admin Console to activate it. When upgrading from a previous release, a new license is not required.

1. Copy your product license file to a location that is accessible from your Insight installation.
2. In the Insight 6.5.0 program folder, select **Administration > Admin Console**.
3. Enter the Admin Console login credentials.
4. In the **Documents Tree**, select **License manager**.
5. In the right pane, click **Add new data**.
6. Navigate to the license file, select it, and then click **Open**.

The license is added to the License Manager list, and the Components section displays the components provided with the license.

The **Documents Tree** is refreshed.

## Change Insight configuration after installation

Use the procedure in this section to change Insight configuration after the installation. For example, change your credentials to the Admin database or enable TLS/SSL mode.

1. Open a Command Prompt window.
2. Navigate to the folder where Insight is installed by typing:  

```
cd C:\Program Files\Kofax\Insight 6.X.X
```
3. From the installation folder, type the following:

```
cd InstallManager
```

4. Run the following command:

```
Altosoft.Insight.InstallManager.ui.exe /i
```

The Installation Manager is launched.

5. Follow the procedure to update the settings as described in [Run the Insight Installation Manager](#).

## Change the encrypted key after installation

Make sure that Insight databases (Administration and Project Meta) are available and use the procedure in this section to change the generated key after the installation.

1. In the Insight Installation Manager, in the **Security** group, click **Change Key**.
2. On the **Confirm** screen, select the **Generate new** radio button. By default, the generated key is located at `[drive]:\ProgramData\Altosoft.Insight.Licenses`. Also, you can select the **Use existing key** radio button and click **Open file** to specify the path.
3. Optional. Select the **Save to Data Folder** check box to duplicate the key and keep it in the Data folder.
4. Click **OK** to save changes.

## Run a silent installation

As an alternative to the standard Insight installation process, you can achieve the same results by performing a silent installation from a Command Prompt window. During a silent installation, no manual entries are required.

1. Open a Command Prompt window and change to the folder where you extracted the Insight product files.
2. Run the following command:

```
msiexec /i KofaxInsightSetup_6.5.0.NNNN_x64.msi /q
```

where `NNNN` is the build number listed in the "Version information" section of the *Kofax Insight Release Notes*.

 The `/q` runs the Insight installer in silent mode (no user interface).

3. To specify the data folder, add the argument `DATAFOLDER="<folder>"` to the command.

Example:

```
msiexec /i KofaxInsightSetup_6.5.0.0.0.NNNN_x64.msi /quiet DATAFOLDER="D:\Temp"
```

where `"D:\Temp"` is the folder where the data files will be stored.

To specify the log folder, add the argument `LOGFOLDER="<folder>"` to the command.

Example:

```
msiexec /i KofaxInsightSetup_6.5.0.0.0.NNNN_x64.msi /quiet LOGFOLDER="D:\Temp"
```

where "D:\Temp" is the folder where the log files will be stored.

Alternatively, you can use a non-default location when installing Insight.

Example:

```
msiexec /i KofaxInsightSetup_6.5.0.0.0.NNNN_x64.msi /q DATAFOLDER="D:\temp\insightdata"
```

```
INSTALLLOCATION="D:\Program Files\Kofax\Insight 6.5.0\"
```

4. To define the Insight components for installation, use the following arguments.
  - a. Set the installation type parameter as follows: `INSTALLATION_TYPE="Custom"`
  - b. Define the component for installation:
    - `INSTALLATION_TYPE_I: Web Application`
    - `INSTALLATION_TYPE_S: Scheduler`
    - `INSTALLATION_TYPE_W: WcfDataService`

To install the component, set the value to 1. Otherwise, set the value to 0.

For example, to install the Web Application and the Scheduler, run the following command:

```
msiexec /i KofaxInsightSetup_6.5.0.NNNN_x64.msi /q
INSTALLATION_TYPE="Custom" INSTALLATION_TYPE_I="1" INSTALLATION_TYPE_S="1"
INSTALLATION_TYPE_W="0"
```

**i** When you install WcfDataService, the Web Application is also installed, even though the value for Web Application is set to 0. This exception provides a means for printing the reports in PDF.

5. Create a file named **InstallManagerSettings.xml** for the configuration settings.
  - a. Review the samples in [Silent installation sample configuration files](#). Optionally, add the following commands to the configuration file:
    - `<Security UseCustomKey="True" GenerateNewKey="True"></Security>`: Applies the new generated encryption key.
    - `<Security UseCustomKey="True" KeyPath="c:\temp\CSEncrypt.key" SaveToDataFolder="true"/>`: Applies the existing custom key and saves data to the Data Folder.
    - `<HighAvailability>True</HighAvailability>`: Enables the High Availability mode.
    - `<MultiTenant>True</MultiTenant>`: Installs Insight in multi-tenant mode.
  - b. Base your file on the sample that corresponds to your database type (SQL Server, Oracle, or MySQL), and update the user name, password, and other values as applicable.
6. Save your configuration file in a separate folder, such as:
 

```
C:\Insight
```

**i** In silent mode, the installer uses InstallManagerSettings.xml to obtain the configuration settings that otherwise would be entered from the Installation Manager user interface.

7. Run the following command.

```
<installation folder>/InstallationManager/
Altosoft.Insight.InstallManager.exe /i /a /f "<ConfigurationFilePath>"
```

## Silent installation sample configuration files

This section lists sample configuration files to use as a starting point for creating your own configuration file (**InstallManagerSettings.xml**) for the silent installation. Update the user name, password, and other values as applicable.

### Microsoft SQL Server

```
<?xml version="1.0" encoding="UTF-8"?>
<InstallSettings>
  <InstallDirectory>C:\Program Files\Kofax\Insight 6.5.0</InstallDirectory>
  <HighAvailability>True</HighAvailability>
  <DBSettings>
    <ConnectionType>MSSQL</ConnectionType>
    <AuthDBName>AuthDBName</AuthDBName>
    <ServerName IsSQLAuthorisation="True"></ServerName>
    <User>User</User>
    <Password>Password</Password>
    <AdditionalConnectionString>AdditionalConnectionString</AdditionalConnectionString>
  </DBSettings>
  <WebDirContext CreateAppPool="True" CreateWebSite="False" Port="80" Host="hostname"
  UseSSL="False" EnableWindowsAuthentication="True">
    <ApplicationPoolName>InsightPool</ApplicationPoolName>
    <AppPool NetworkService="True" Identity=".\administrator" Password="password"/>
    <WebSiteName>Default Web Site</WebSiteName>
  </WebDirContext>
  <Security UseCustomKey="True" KeyPath="c:\temp\CSEncrypt.key"
  SaveToDataFolder="True"/>
  <Projects UpdateAll="False">
  </Projects>
  <AuthSettings Login="Administrator" Password="password">
  </AuthSettings>
  <InsightLocale>en-us</InsightLocale>
  <ViewerLocale></ViewerLocale>
  <SchedulerSettings LogOnAsNetworkService="True" LogOnAsAccount=".\UserName"
  LogOnAsPassword="password"
  UseWindowsAuthentication="False" UserName="Administrator" Password="password"
  ServiceName="InsightSchedulerService" Port="13501" BridgeServicePort="15501">
  </SchedulerSettings>
  <!--Uncomment RemoteInsightDataseviceSettings for remote application service-->
  <!--<RemoteInsightDataseviceSettings Host="Host" Port="Port" UseSSL="False"
  UseOnlyForScheduler="False|True">
  </RemoteInsightDataseviceSettings-->
</InstallSettings>
```

### Microsoft SQL Server with SSL connection

```
<?xml version="1.0" encoding="UTF-8"?>
<InstallSettings>
  <InstallDirectory>C:\Program Files\Kofax\Insight 6.5.0</InstallDirectory>
  <HighAvailability>True</HighAvailability>
  <DBSettings>
    <ConnectionType>MSSQL</ConnectionType>
    <AuthDBName>AuthDBName</AuthDBName>
    <ServerName IsSQLAuthorisation="True"></ServerName>
    <User>User</User>
    <Password>Password</Password>
    <AdditionalConnectionString>AdditionalConnectionString</AdditionalConnectionString>
```

```

</DBSettings>
  <WebDirContext Port="443" Host="hostname" CreateWebSite="True"
CreateAppPool="False" UseSSL="True">
  <AppPool NetworkService="True" Identity=".\\administrator" Password="password"/>
  <ApplicationPoolName>ASP.NET v4.0</ApplicationPoolName>
  <WebSiteName>Default Web Site</WebSiteName>
  <Certificate Thumbprint="{certificate thumbprint}" Name="IIS Development
Certificate"/>
</WebDirContext>
  <AppPool NetworkService="True" Identity=".\\administrator" Password="password"/>
  <Security UseCustomKey="True" KeyPath="c:\\temp\\CSEncrypt.key"
SaveToDataFolder="True"/>
  <Projects UpdateAll="False">
</Projects>
  <AuthSettings Login="Administrator" Password="password">
</AuthSettings>
  <InsightLocale>en-us</InsightLocale>
  <ViewerLocale></ViewerLocale>
  <SchedulerSettings LogOnAsNetworkService="True" LogOnAsAccount=".\\UserName"
LogOnAsPassword="password"
  UseWindowsAuthentication="False" UserName="Administrator" Password="password">
</SchedulerSettings>
  <!--Uncomment RemoteInsightDataseviceSettings for remote application service-->
  <!--<RemoteInsightDataseviceSettings Host="Host" Port="Port" UseSSL="False"
UseOnlyForScheduler="False|True">
</RemoteInsightDataseviceSettings-->
</InstallSettings>

```

## Microsoft SQL Server with Windows Authentication

```

<?xml version="1.0" encoding="UTF-8"?>
<InstallSettings>
  <InstallDirectory>C:\\Program Files\\Kofax\\Insight 6.5.0</InstallDirectory>
  <HighAvailability>True</HighAvailability>
  <DBSettings>
    <ConnectionType>MSSQL</ConnectionType>
    <AuthDBName>InsightDB</AuthDBName>
    <ServerName IsSQLAuthorisation="False">localhost</ServerName>
    <AdditionalConnectionString>AdditionalConnectionString</AdditionalConnectionString>
  </DBSettings>
  <WebDirContext CreateAppPool="True" CreateWebSite="False" Port="80" Host="hostname"
UseSSL="False">
  <AppPool NetworkService="True" Identity=".\\administrator" Password="password"/>
  <ApplicationPoolName>ASP.NET v4.0</ApplicationPoolName>
  <WebSiteName>Default Web Site</WebSiteName>
</WebDirContext>
  <Security UseCustomKey="True" KeyPath="c:\\temp\\CSEncrypt.key"
SaveToDataFolder="True"/>
  <Projects UpdateAll="False">
</Projects>
  <AuthSettings Login="Administrator" Password="password">
</AuthSettings>
  <InsightLocale>en-us</InsightLocale>
  <ViewerLocale></ViewerLocale>
  <SchedulerSettings LogOnAsNetworkService="True" LogOnAsAccount=".\\UserName"
LogOnAsPassword="password"
  UseWindowsAuthentication="False" UserName="Administrator" Password="password">
</SchedulerSettings>
  <!--Uncomment RemoteInsightDataseviceSettings for remote application service-->
  <!--<RemoteInsightDataseviceSettings Host="Host" Port="Port" UseSSL="False"
UseOnlyForScheduler="False|True">
</RemoteInsightDataseviceSettings-->
</InstallSettings>

```

**Oracle**

```
<?xml version="1.0" encoding="UTF-8"?>
<InstallSettings>
  <InstallDirectory>C:\Program Files\Kofax\Insight 6.5.0</InstallDirectory>
  <HighAvailability>True</HighAvailability>
  <DBSettings>
    <ConnectionType>Oracle</ConnectionType>
    <AuthTNS>AuthTNS</AuthTNS>
    <AuthUser>AuthUser</AuthUser>
    <AuthPassword>AuthPassword</AuthPassword>
    <AdditionalConnectionString>AdditionalConnectionString</AdditionalConnectionString>
  </DBSettings>
  <WebDirContext CreateAppPool="True" CreateWebSite="False" Port="80" Host="hostname"
  UseSSL="False">
    <AppPool NetworkService="True" Identity=". \administrator" Password="password"/>
    <ApplicationPoolName>InsightPool</ApplicationPoolName>
    <WebSiteName>Default Web Site</WebSiteName>
  </WebDirContext>
  <Security UseCustomKey="True" KeyPath="c:\temp\CSEncrypt.key"
  SaveToDataFolder="True"/>
  <Projects UpdateAll="False">
  </Projects>
  <AuthSettings Login="Administrator" Password="password">
  </AuthSettings>
  <InsightLocale>en-us</InsightLocale>
  <ViewerLocale></ViewerLocale>
  <SchedulerSettings LogOnAsNetworkService="True" LogOnAsAccount=". \UserName"
  LogOnAsPassword="password"
  UseWindowsAuthentication="False" UserName="Administrator" Password="password">
  </SchedulerSettings>
  <!--Uncomment RemoteInsightDataseviceSettings for remote application service-->
  <!--<RemoteInsightDataseviceSettings Host="Host" Port="Port" UseSSL="False"
  UseOnlyForScheduler="False|True">
  </RemoteInsightDataseviceSettings-->
</InstallSettings>
```

**MySQL Server**

```
<?xml version="1.0" encoding="UTF-8"?>
<InstallSettings>
<InstallDirectory>C:\Program Files\Kofax\Insight 6.5.0</InstallDirectory>
<HighAvailability>True</HighAvailability>
<DBSettings>
  <ConnectionType>MySQL</ConnectionType>
  <AuthDBName>Insight_DB</AuthDBName>
  <ServerName>Insight_Server</ServerName>
  <User>sa</User>
  <Password>sa</Password>
  <AdditionalConnectionString>AdditionalConnectionString</AdditionalConnectionString>
</DBSettings>
  <WebDirContext CreateAppPool="True" CreateWebSite="False" Port="80" Host="hostname"
  UseSSL="False">
    <AppPool NetworkService="True" Identity=". \administrator" Password="password"/>
    <ApplicationPoolName>ASP.NET v4.0</ApplicationPoolName>
    <WebSiteName>Default Web Site</WebSiteName>
  </WebDirContext>
  <Security UseCustomKey="True" KeyPath="c:\temp\CSEncrypt.key"
  SaveToDataFolder="True"/>
  <Projects UpdateAll="False">
  </Projects>
  <AuthSettings Login="Administrator" Password="password">
  </AuthSettings>
  <InsightLocale>en-us</InsightLocale>
```



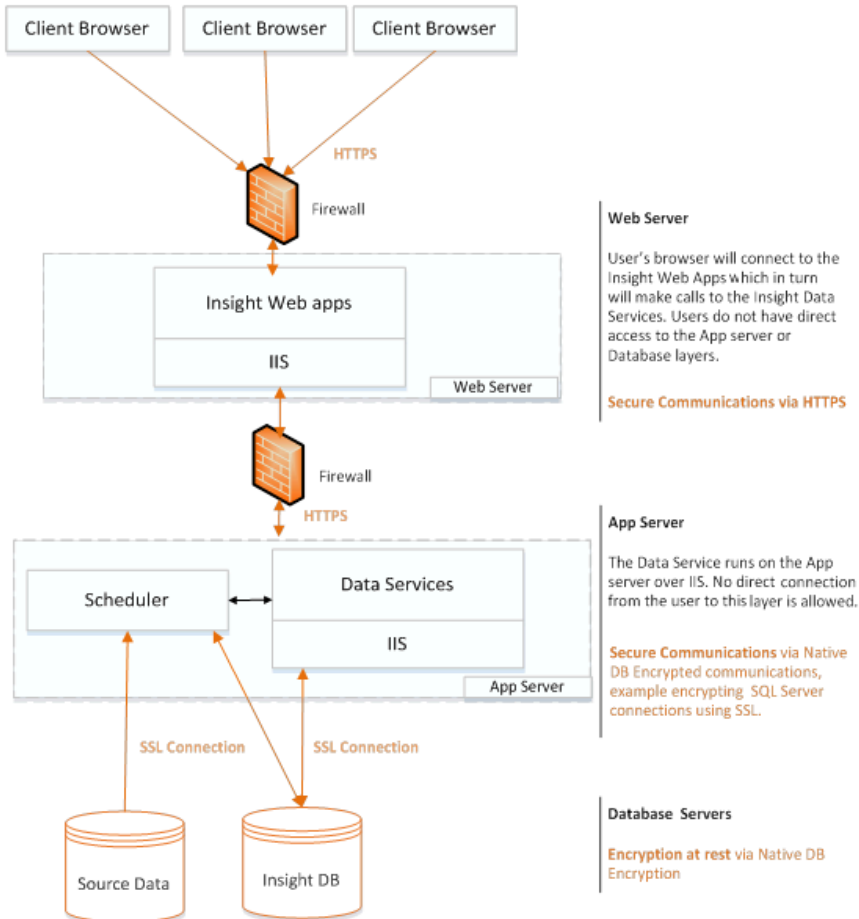
```

<ViewerLocale></ViewerLocale>
<SchedulerSettings LogOnAsNetworkService="True" LogOnAsAccount=".\UserName"
LogOnAsPassword="password"
  UseWindowsAuthentication="False" UserName="Administrator" Password="password">
</SchedulerSettings>
<!--Uncomment RemoteInsightDataseviceSettings for remote application service-->
<!--<RemoteInsightDataseviceSettings Host="Host" Port="Port" UseSSL="False"
UseOnlyForScheduler="False|True">
</RemoteInsightDataseviceSettings-->
</InstallSettings>

```

## Set up Insight in a three-tier architecture

You can set up Insight in a three-tier architecture, where the Web Application is installed on the Web Server layer and the Insight Data Services and Insight Scheduler Services are installed on the App Server layer. This approach may be useful in a large-scale deployment (banking, financial, healthcare or other) that calls for balanced and secure distribution of the workload.



## Web server layer

1. Run the Insight installer on the web server, and follow the procedure in [Install Kofax Insight](#) with this exception: When you get to the Kofax Insight Setup screen, select **Custom**, and click **Next**.

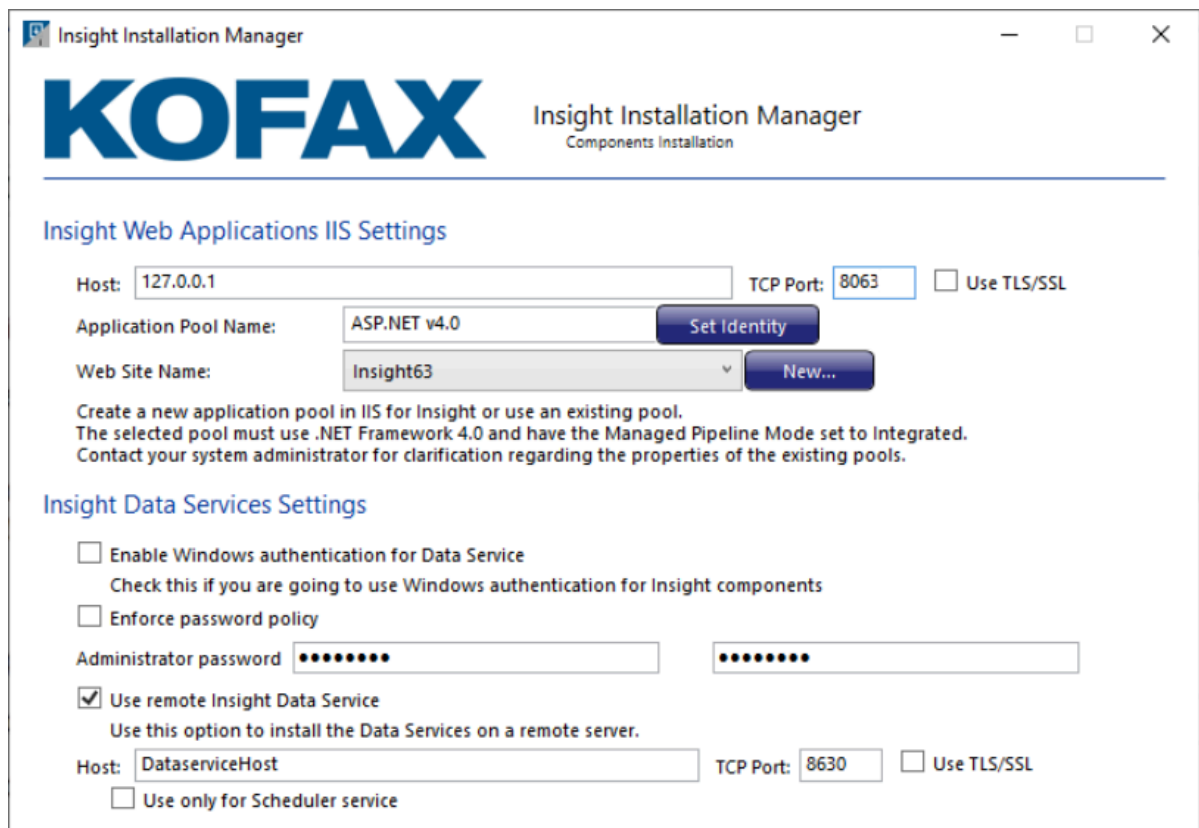
The component selection screen appears.

2. Select **Insight Web Applications**, and click **Next**.
3. Browse to the installation folder, and click **Next**.  
You are prompted to begin the installation.
4. Click **Install**.

The installer copies the files to the selected folder and a completion message appears when the process is finished.

5. Click **Finish** to close the installer and launch the Insight Installation Manager.
6. Enter the necessary information about the IIS server on the Web Server layer.
7. Select the **Use remote Insight Data Service** check box, enter the Host and TCP port for the app server layer, and click **Next**.

These settings are necessary to ensure that the web server is able to access the app server.



**Insight Web Applications IIS Settings**

Host:  TCP Port:   Use TLS/SSL

Application Pool Name:

Web Site Name:

Create a new application pool in IIS for Insight or use an existing pool.  
The selected pool must use .NET Framework 4.0 and have the Managed Pipeline Mode set to Integrated.  
Contact your system administrator for clarification regarding the properties of the existing pools.

**Insight Data Services Settings**

Enable Windows authentication for Data Service  
Check this if you are going to use Windows authentication for Insight components

Enforce password policy

Administrator password

Use remote Insight Data Service  
Use this option to install the Data Services on a remote server.

Host:  TCP Port:   Use TLS/SSL

Use only for Scheduler service

8. Review and confirm the IIS settings, and click **Next**.  
The Insight Web Application components are installed.

9. When notified that the Insight 6.5.0 installation is complete, click **Next**, and then click **Exit**. Proceed to install the Data Service and Scheduler on the App Server.

## Application server layer

1. Run the Insight installer on the web server, and follow the procedure in [Install Kofax Insight](#) with this exception: When you get to the Kofax Insight Setup screen, select **Custom**, and click **Next**.  
The component selection screen appears.
2. Select **Insight Data Services** and **Insight Scheduler Service** and click **Next**.
3. Select the folder where the installer should copy the files and click **Next**.
4. Click **Install**.  
The installer copies the files to the selected folder and a completion message appears when the process is finished.
5. Click **Finish** to close the installer and launch the Insight Installation Manager.
6. Enter the Database Connection information.
7. Enter the IIS information for the Insight Data Services.
8. Enter the Insight Administrator login credentials and select the **Windows authentication** check box as applicable.
9. Review the IIS settings and click **Next**.
10. Configure the Scheduler settings and click **Next**.  
The Insight app server components are installed.
11. When notified that the Insight 6.5.0 installation is complete, click **Next**, and then click **Exit**.  
The three-tier installation is completed.


## Upgrade Insight

If you reinstall or upgrade Insight, the procedure may overwrite existing configuration files. Therefore, before performing any of these procedures, be sure to back up any configuration files that contain custom settings. After completing the Insight upgrade, you need to manually reapply any required customization to the new configuration files.

When upgrading to Insight 6.5.0 from an earlier version, do the following:

1. [Upgrade the Insight version and Admin database](#)
2. [Upgrade existing Insight projects](#)

Before starting the upgrade process, we strongly recommend that you back up the Insight [Admin](#) and [project](#) databases.

 To perform a direct upgrade to Insight 6.5.0, you must have version 6.0 or later. To upgrade from a version earlier than 6.0, you must first upgrade to version 6.4, and then to 6.5.0.

## Upgrade the Insight version and Admin database

This section explains how to upgrade the Insight version and Admin database.

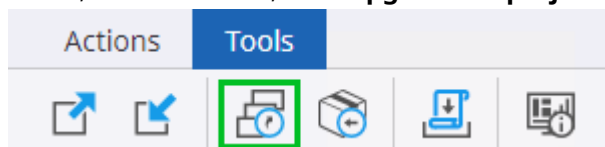
1. Keep your existing Insight 6.X installation in place.
2. Run the installer for Insight 6.5.0, and follow the procedure described in [Install Kofax Insight](#). The installer sequence is the same with one exception: After you accept the license agreement, you are prompted to upgrade the existing version or install Insight as a separate installation.
3. Select **Upgrade ver. 5.X** or **Upgrade ver. 6.X**, and click **Next**.
4. Finish the installation and launch the Installation Manager.
5. Follow the procedure described in [Run the Insight Installation Manager](#), and make sure to do the following:
  - a. Under **Insight Engine Database Configuration**, specify the connection and authentication information for the existing Insight Admin database.
  - b. Under **Databases**, specify the name of the existing Insight Admin database.
  - c. Provide configuration settings. Under **Insight Data Services Settings**, you must specify the Insight Administrator password (even if you plan to retain the same password from the previous version).
  - d. Finish the installation.  
The Admin database is upgraded to the format required for Insight 6.5.0. Once the upgrade is finished, your existing Insight projects are available in Admin Console and Studio. To upgrade your projects, see the next section.
  - e. Check for the latest fix pack for Insight 6.5.0 and apply it if it is available.

## Upgrade existing projects

Use Admin Console to upgrade projects created in earlier versions of Insight. You can upgrade all existing projects at the same time, or upgrade them individually.

**i** As another option, you can upgrade an existing project in Studio. When you select a project created in an earlier version of Insight, Studio automatically prompts you to convert the project for use in the current version.

1. Start **Admin Console** and provide your credentials.
2. On the **Tools** tab, on the toolbar, click **Upgrade all projects**.



The **Select projects to update** dialog box appears.

3. On the list, select the projects to update for use in the new Insight version. Select the check box at the top to select all projects, or select individual check boxes, and then click **OK**.  
Your projects are upgraded.

4. Click **Close**.

## Install Insight 6.5.0 alongside previous version

You can install Insight 6.5.0 alongside an earlier version. This approach is useful if you decide to run both versions in parallel for a period of time before removing the earlier version.

Perform the Insight 6.5.0 installation according to the instructions in [Install Kofax Insight](#) and [Run the Installation Manager](#), but with the exceptions noted in this section.

1. Before starting the installation:
  - a. Use IIS Manager to create a new web site, which is available for selection when you run the Insight 6.5.0 Installation Manager. Select the new port. Or you can skip this step and create the site from the Installation Manager.
  - b. Use the current version of Insight to export your existing projects and admin settings.

**i** Also, you can clone databases and use existing clones for the new Insight version. In this case the databases are updated automatically to the new version. But in this case you should open each project in the Admin database, do not update the existing project, but click **Change** and then provide the credentials to the copied project databases.

2. When you run the Insight 6.5.0 installer, select Install separately on the screen that appears after the license agreement.
3. Run the [Installation Manager](#) but use the new Admin database for the new Insight version.
4. Start Insight 6.5.0 Admin Console, create a new project, and then import the projects and Admin settings that were exported from the earlier version of Insight.

## Install Kofax Insight on Docker

This section includes instructions for installing Kofax Insight on Docker.

1. Download the Kofax Insight product files to the computer where you plan to install the product.
2. Extract **KofaxInsight-6.5.0\_64-bit.ZIP**.
3. Create the **DockerFolder** folder and extract the **KofaxInsight-6.5.0\_Docker.zip** into it. The extracted **KofaxInsight-6.5.0\_Docker.zip** contains the followings files:
  - The **Insight** folder with the **InstallConfig.xml** file and **Install\_fonts.ps** file. Copy the **.msi** installer from the extracted **KofaxInsight-6.5.0\_64-bit.ZIP** into it.
  - The configuration files: **InsightWeb.Dockerfile**, **Docker-compose.yml**, **Scheduler.Dockerfile**. Each configuration file contains settings that can be extended as necessary.
4. Install the latest version of Docker for Windows and run it as a Windows container.
5. Open the **InsightWeb.Dockerfile** and **Scheduler.Dockerfile** for editing and define the full name of the applicable .msi file, such as **KofaxInsightSetup\_6.5.0.0.0.<NNNN>\_x64.msi**,

where <NNNN> is the Insight build number listed in the "Version information" section in the *Kofax Insight Release Notes 6.5.0*.

To install the Fix Pack, copy the **.msp** file in the **Insight** folder, then open the **InsightWeb.Dockerfile** and **Scheduler.Dockerfile** for editing and uncomment the following line:

```
#RUN Start-Process msiexec.exe -ArgumentList '/update', 'C:\Insight\KofaxInsightSetup_FixPack.msp', '/qn' -NoNewWindow -Wait, where X is the fix pack number, and YYYY stands for the build number.
```

If you use Windows 2016, in **InsightWeb.Dockerfile**, comment the `RUN C:\\Insight\\install_fonts.ps1` line as follows: `#RUN C:\\Insight\\install_fonts.ps1`

6. Optional. Insight on Docker is supported only on Microsoft SQL Server. To use a new database, you should create a new Administration database.
7. Open the **Docker-compose.yml** file for editing to define the database and user settings.
  - For a single tenant environment:

- a. Define the connection for

`DataService_Insight.Admin.MasterDBConnectionString` in the following format:

```
Data Source=<datasource>; Initial Catalog=<DBName>; Password=<userpassword>; User Id=<username>
```

- b. For a new Administration database, define the Administrator password in the `DataService_Insight.Password` setting.

- c. Specify the Administrator password for the Scheduler in the `Scheduler_Password` setting.

**i** If you created a new database, the Administrator password for the Scheduler is the same as defined above for the Dataservice.

- For a multitenant environment:

- a. Define the connection for

`DataService_Insight.TenantAdmin.MasterDBConnectionString` in the following format:

```
Data Source=<datasource>; Initial Catalog=<DBName>; Password=<userpassword>; User Id=<username>
```

- b. For a new Administration database, define the password for the MTAdmin user in the `DataService_Insight.Password` setting.

- c. Change the login for a Scheduler user to MTAdmin: `Scheduler_Login=MTAdmin`

- d. Specify the MTAdmin password for the Scheduler in the `Scheduler_Password` setting.

**i** If you created a new database, the MTAdmin password for the Scheduler is the same as defined above for the Dataservice.

8. Start **PowerShell** as an Administrator user and navigate to the **DockerFolder** using the following command:

```
cd <DockerFolder>
```

9. To build the Insight image on Docker, run the following command:

```
docker-compose build
```

The first time, it may take up to two hours to download the basic Windows image.

10. To start the containers, run the command:

```
docker-compose up
```

11. After two containers are launched, you can start Insight in a browser using this URL:

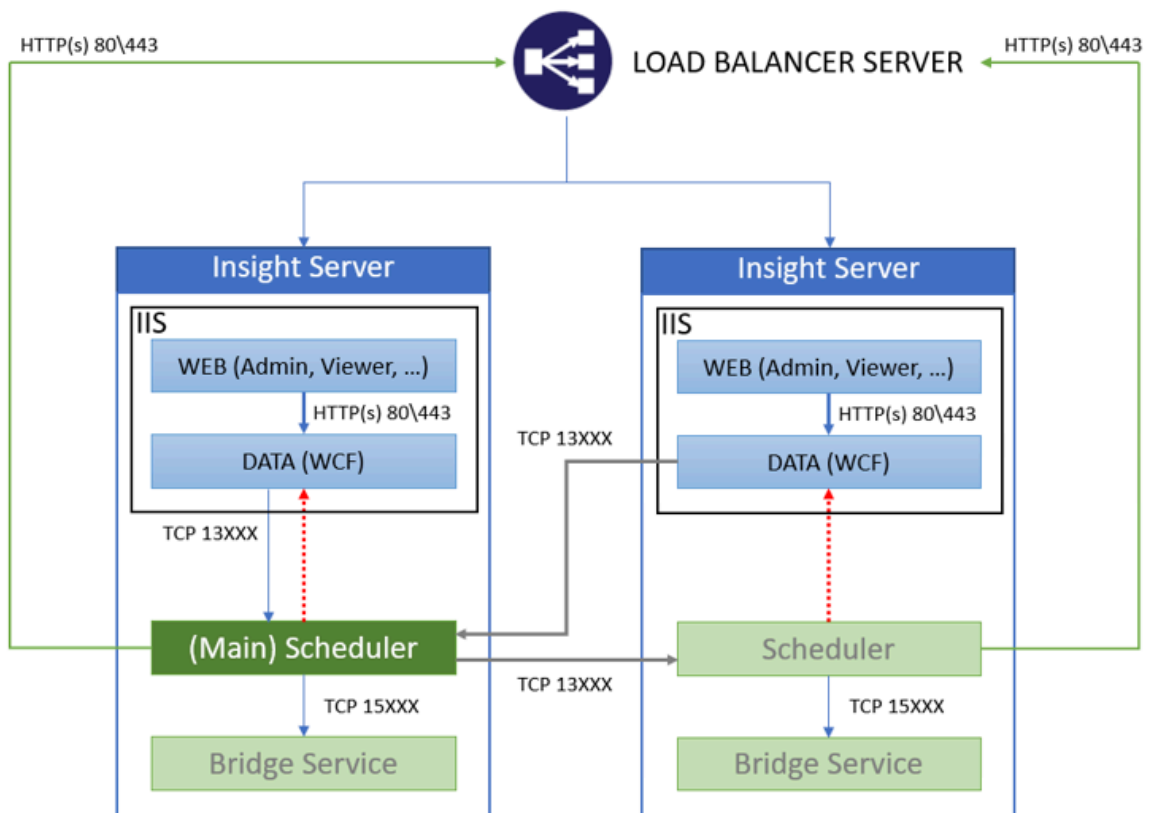
```
http://servername:8080/insight/admin
```

**i** You can specify any alternative port in the **Docker-compose.yml** file.

## Set up Insight in high availability mode

This section describes how to make Insight dashboards highly available by running multiple Insight environments on a [Load Balancer](#).

In the following diagram, the Insight environment consists of two Insight servers with Web Application, Data Service, and Scheduler. Data Service URLs for all Schedulers are set up to the Load Balancer entry point, and Data Service URLs for Web Application are configured to use the local Data Service.




The Web Application on each server must have a connection to Data Service. It is possible to use the connection with Load Balancer or connect to the local Data Service (on the same server). In case of two-tier architecture, where Web Application and Data Service are installed on the same server, we recommend that you use a local Data Service because traffic from the client is balanced upon requests to the Web Application, which functions as proxy between the client and the Data Service. Also, each Data Service must have a connection to another service, which is required for Data Services synchronization.

The Scheduler service must also have access to the Data Service. It is recommended to use the Load Balancer as an entry point from a Scheduler to a Data Service (green arrow), instead of connecting to the local Data Service on the same server (red arrow). With this configuration, if the IIS service on the local server fails, the Scheduler remains available as it is a Windows service. In this case, the Load Balancer redirects the requests from the Scheduler to another available Data Service and continues processing the requests from Scheduler. This option allows to achieve high availability for the Scheduler.

The Scheduler can be installed on the same Insight servers with Data Service or on separate machines.

After Insight servers are configured to run in high availability mode, Insight assigns one Scheduler as the "Main" Scheduler. The Main Scheduler executes plans and tasks and assigns the tasks to the other Schedulers using TCP connection. Also, the Main Scheduler must be available from all Data Services (WCF) to allow execution of various tasks, such as manual data load, tests, schedule plans, and more. If the Main Scheduler fails, another Scheduler takes its role and becomes the Main Scheduler. If the failed Scheduler is back online, it starts executing the tasks received from the Main Scheduler.

 All Insight servers running the Scheduler should use the same set of database drivers and time zone settings. Also, the system time should be synchronized.

After the configuration is completed, to improve the performance, set the View mode by clicking the Stop icon in Admin Console. In View mode, no updates can be made to Admin Console or projects, and the Viewer application functions as usual. To update the project in Admin Console or Studio, set Insight to the Edit mode by clicking the Play icon in Admin Console. When the system is in Edit mode, Viewer is available with reduced performance.

## Install Insight in high availability mode in two-tier architecture

This section gives an example of how to install and set up Insight in high availability mode in two-tier architecture, when all Insight components (Web applications, Data service, and Scheduler) are installed on each Insight server.

The following are high-level steps:

1. Identify the load balancer entry point server.
2. Set up Insight on a server and configure the Load balancer as the entry point server.
3. Repeat Step 2 for other Insight servers (for high availability, at least two Insight servers must exist).



**Prerequisites:**

- Servers: In this example, three Windows servers are used: One server is the load balancer entry point, and the other two are the Insight servers.
- You must have administrator rights to access all computers or virtual machines that run the Windows Server 2012 or higher.

Follow the procedure below to install Insight on each server. Also, you can perform a silent installation on each server.

1. Download the Kofax Insight product files to the computer where you plan to install the product.
2. Extract **KofaxInsight-6.5.0\_64-bit.ZIP**.
3. Run the applicable .msi file, such as **KofaxInsightSetup\_6.5.0.0.<NNNN>\_x64.msi**, where <NNNN> is the Insight build number listed in the "Version information" section of the *Kofax Insight 6.5.0 Release Notes*.  
The installation wizard appears.
4. Click **Next**.
5. If the installer is not being run as administrator, a notification window appears. In this situation, click **Restart** to run as administrator.
6. Review the license agreement, select the check box to accept the terms, and click **Next**.
7. On the **Kofax Insight Setup** screen, select **Full environment** and click **Next**.
8. On the **Custom setup** page, accept or change the default installation folder.
9. Specify a folder or browse to select the location for storing log files. Initially, permissions to the log folder are granted to everyone. We recommend that you use a local folder to improve the performance and split the logs from different servers. Also, you can use a shared folder, but in this case, it is recommended to create individual subfolders for each Insight server to split the logs.
10. Set up the **Data root folder**. We recommend that you use a shared drive for the **Data root folder**: This approach allows all instances of Insight to access the **Data root folder** used for uploading files and projects to Insight. The Insight pool user and Scheduler login user must have read/write permissions to this folder.  
The **Data root folder** is used for all files that you upload through Insight. Initially, access rights to this folder are assigned to everyone. This folder can contain the following subcategories.
  - Solution: Stores all ZIP files for solution import and creating a project.
  - ImportExport: Stores all extracted project and solution files.
  - <ProjectName>: Default subfolder that stores data for the project. You can create individual subfolders for your projects as required.
  - Encryption key: You can store the encryption key used for security purposes.
11. Click **Next**.
12. On the **Ready to install Kofax Insight** page, click **Install** to begin the installation.
13. On the **Completed the Kofax Insight Setup Wizard** page, click **Finish**.  
The Insight Installation Manager appears. For instructions, continue to the section *Configure Insight in the Installation Manager*.

**i** After a successful installation, all installation steps are logged to a file in the log folder specified previously on the "Custom setup" page. If the installation fails, you can check the respective log in the **Event Viewer**.

## Configure Insight in the Installation Manager

In most cases, the Insight Installation Manager is launched automatically after you run the Insight installer to copy files to the server. You can also launch the Insight Installation Manager from your Insight program folder.

**i** When you run the Installation Manager after the first successful configuration, you need to provide credentials for any Insight Administrator user. Also, you can use Windows authentication. If you need to run the Insight Installation Manager to repair configuration settings or change IIS settings after installation, start the Command Prompt and run the following command:

```
[drive:]\Insight_6.X.X\InstallationManager  
\Altosoft.Insight.InstallManager.ui.exe /i
```

## General settings

When the Insight Installation Manager is launched, you are prompted to set up Administration database for Admin Console to store information.

Specify the following information:

1. Select the Insight mode: **Single** or **Multi-Tenant**.

**i** If you select to deploy Insight in multi-tenant mode, you need to add the license and configure tenants using the Multi-Tenant Console application. To log in as a Multi-tenant administrator, use the *MTAdmin* user name and enter the password.

2. Select the **High Availability** check box to turn the high availability mode on.
3. **Connection Type**: The server to use (Microsoft SQL, Oracle, or MySQL).
4. **SQL Server Name**: Enter the server name or the TNS name for the database server.  
If you use MySQL or Oracle, ensure that you have the necessary database drivers installed prior to installing Insight.  
For the Microsoft SQL server, you can use the **Windows authentication**.


**i** Database connection should be the same for all servers.

5. **Login and Password**: Provide the login credentials for an Administration database.  
For the Oracle database, you need to create a user with privileges before installation. For the Microsoft SQL and MySQL databases, Insight creates new databases automatically if they do not exist, but the user must have required privileges for creating a database. As another option, you can create the Administration database before installation.
6. Select the **Administration Database Name** to assign a name.
7. Use **Additional Connection String** to define additional parameters for a connection string.

8. Select the **Use Custom Key** check box to encrypt the Insight connections for security purposes. Two options are available:

- **Generate New Key:** In this case, the key is generated and stored in a local folder with Insight licenses. To save the key also in the Data Folder, select the respective check box.
- **Use Existing Key:** Select this option and click **Open file** to specify the path to an existing encryption key. In this case, the key is copied to a local folder with Insight licenses.

Make sure that you use the same key on each server. If you already have the key file, copy the file to a shared folder and select the **Use Existing Key** option, and then specify the path to the shared folder. If you do not have the file, select **Generate New Key** and **Save to Data folder** during the first installation. For the next installation, select **Use Existing Key** and specify the path to shared Data folder.

 For silent installation, you can select **Use Existing Key** and specify the path to shared Data folder. In this case, if the file does not exist, a new file will be generated. If you decide to change the key, you should restart all Insight services (Web Application/IIS and Scheduler) on all nodes after the change.

9. Select the **Save to Data Folder** check box to save the key in the Data Folder: If you change the key, you do not need to change it for each computer.

The following connections are encrypted:

- Connection to the Administration database
- Connection document from Admin Console
- Connection to the project meta and data databases
- Connection used in the Data Source document to the databases

**Important:** If the generated file in the Data Folder [gets lost](#), you will not be able to work with all of these connections.

You may later change the generated key by running the [Insight Installation Manager](#) or through the [silent installation](#).


10. Under the **Localization** group, use the drop-down lists to set **Insight Locale** and **Viewer Locale**. By default, English locale is selected.
11. Click **Next**.  
The Insight Web Applications IIS Settings page appears.

## Insight Web Applications IIS Settings

Define the following Web Application settings:

1. Set the **Host** and **TCP Port** parameters, and the protocol that will be used for all URLs.
  - **Host:** The default host address is **127.0.0.1**. You can enter the server domain name or the IP address where Insight is installed to access the website.
  - **TCP Port:** The default TCP/IP port when using SSL (HTTPS) is 443, and the default non-secure (HTTP) port is 80.
  - **Use TLS/SSL:** Select this check box to enable the encrypted connection.
2. Under the **Application Pool** group, define the **Application Pool Name**: Select the created IIS pool name or enter the new pool name.

3. Optional. Click **Set Identity** to define the application pool identity.
  - a. Under the **Service Account** group, click **Application Pool Identity**. In the displayed dialog box, select one of the following options:
    - **Network Service**
    - **This account:** Enter the Account Name or Domain\User name. If you plan to use Windows authentication to access a database, specify the account that has access to this database.
  - b. Set and confirm the password.
  - c. Click **OK** to save changes and quit the screen.
4. **Web Site Name:** If you already created an IIS website, select it from the list and make sure that the entered TCP port is assigned to this site. Otherwise, make sure that the entered TCP port is available and click **New** to create a new website.
  - a. In the **Add Website** dialog box, enter the **Site Name**.
  - b. In the **Binding** group, set the **Type**, **Port**, and **Host Name**.

 We strongly recommend that you use an SSL connection. Use IIS Manager to create or import SSL certificate before you continue with the Installation Manager. For information on how to set up SSL on IIS, see the Microsoft support website.

If you use **Https** binding type, select the **SSL Certificate** from the list.

After you save the changes, the **Use TLS/SSL** check box is automatically selected. To change the SSL settings after the installation is finished, see the procedure in [Change Insight configuration after installation](#).

- c. Click **OK** to save the changes and close the dialog box.

## Insight Data Services Settings

1. Select the **Enable Windows authentication for Data Service** check box. It is required to enable this option if you are going to use Windows authentication for any Insight components.
2. Under the **Insight Data Services Settings** group, select the **Enforce password policy** check box to enforce the following requirements for the Administrator password:
  - Contains at least eight characters
  - Contains at least one alpha character (a-z; A-Z)
  - Contains at least one numeric character (0-9)
  - Contains at least one special character (Examples: @ & % \*)
3. Specify the Administrator or Multi-Tenant Administrator password and then type it again.
4. Select the **Use remote Insight Data Service** check box, set the **Host**, **TCP Port** for the load balancer, and enable the **Use TLS/SSL** option.
5. Select the **Use only for Scheduler service** check box to apply the remote service settings only for the Scheduler service. In this case, the Web Application will use local Data Service and Scheduler will use the load balancer.
6. Click **Next**.  
The **Scheduler Service Settings** screen appears.

## Scheduler Service Settings

Define the following Scheduler settings:

1. Under the **Service account** group, select one of these options:

- **Network Service**
- **This account:** Enter the login and password and then confirm the password. If you plan to use Windows authentication to access databases, specify the account that has access to these databases.

 As the Scheduler uses the shared Data folder, we recommend that you use Windows account for Scheduler instead of default Network service.

2. Under **Insight Authentication method**, specify the credentials for Scheduler to access the Data service. Use one of the following options:

- **Insight User:** Enter the Insight user login, type and confirm the password.
- **Windows authentication**

3. The default Insight Scheduler Service port is 13501. If the default port is already in use, and you are upgrading a previously installed version of Insight to version 6.5.0, the port will be switched to 13650 during the installation. You can specify any port in the Installation Manager.

4. Click **Next** and review the setup details. After reviewing, click **Next**. To make changes, click **PREVIOUS** to return to the previous pages.


A list of installed components appears while the installation is in progress.

5. When notified that the Insight 6.5.0 installation is complete, click **Next**. To make changes, click **Previous** to return to the previous pages. A list of installed components appears while the installation is in progress.

6. When notified that the Insight 6.5.0 installation is complete, click **Next**.

7. Select **Admin Console** to activate the product license. Also, you can select one of the following options.

- Use **Manage Settings** to update the Insight IIS settings or the Insight Admin database.
- Use **Admin Console** to activate the product license and configure the projects, users, roles, and rights.
- **Setup Kofax Analytics Project** to start the Kofax Analytics installation wizard. For details, see *Insight Admin Console Help*.
- Use **Exit** to clear the notification message and return to the desktop.

 Before proceeding to the next section, we recommend that you check for and apply any fix packs that may be available for Insight 6.5.0.

## Activate the product license

Verify that you have the Insight license file provided at the time of your product purchase and use one of the following options to store it.

**i** When upgrading from a previous release, a new license is not required.

- Use a shared folder.
  - To use the shared folder, add the `DataService_Insight.LicenseFolder` key to environment variables for each Insight instance and define path to the shared folder (for example, shared Data folder).
  - In the `WCFDataService.web.config` file, define the path:

```
<add key="Insight.LicenseFolder" value="Path_to_shared_folder"/>
```

**i** This folder should be shared for all Insight servers. Insight pool user should have read access to this folder.

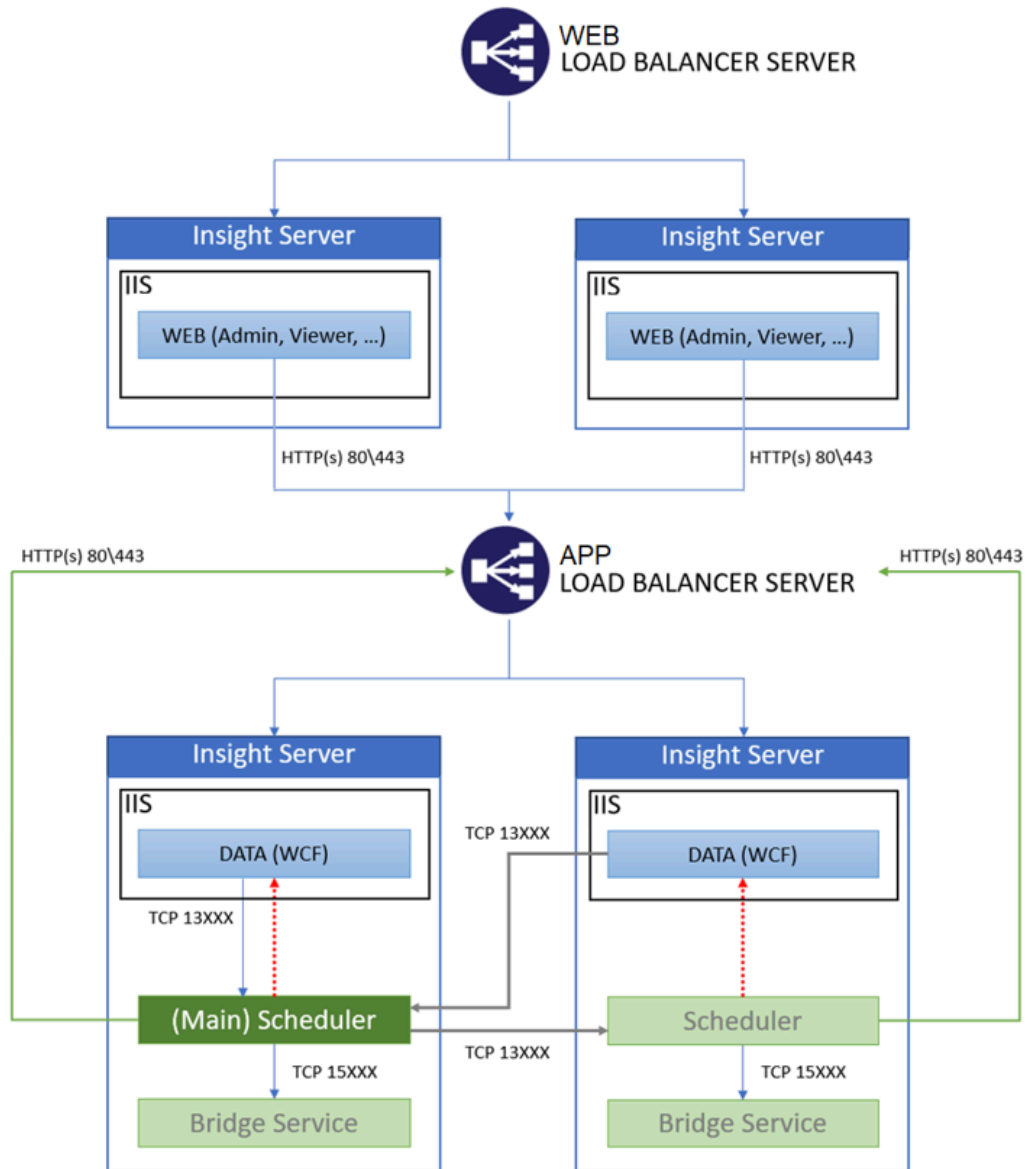
- Use a local folder.
  - Copy the license to "Altosoft.Insight.Licenses" folder in Program data.
  - Open Insight Admin Console directly on Insight server (not through Load Balancer) and upload the license. This option is available only if Web Application uses local Data Service.

Follow the procedure below to activate the license.

1. Copy your product license file to a location that is accessible from your Insight installation.
2. In the Insight 6.5 program folder, select **Administration > Admin Console**.
3. Enter the Admin Console login credentials.
4. In the **Documents Tree**, select **License manager**.
5. In the right pane, click **Add new data**.
6. Navigate to the license file, select it, and then click **Open**. The license is added to the **License Manager** list, and the **Components** section displays the components provided with the license. The **Documents Tree** is refreshed.

## Install and configure Insight in high availability mode in three-tier architecture

The following diagram represents Insight installation in High availability mode in 3-tier architecture.



Use the **Custom installation** option to install and configure Insight servers in 3-tier architecture following the same recommendations as for 2-tier architecture.

For all servers select the **Use remote Insight Data service** option and specify the Application Load Balancer server.

For Insight servers with Web applications, leave the **Use only for Scheduler service** check box unselected. In this case, Web Application uses the Application Load Balancer as entry point.

## Set up Insight in high availability mode on Azure Kubernetes

1. Build the Insight Web and Scheduler images on the [on-premise](#) server.
2. Run **Azure Cloud Shell** on the Azure portal.
3. Upload the following files to the **Azure Cloud Shell**. The files are available from the Insight product package:
  - kubernetes\azure-file-pvc.yaml
  - kubernetes\azure-file-sc.yaml
4. Run the following commands to create a new container registry if the registry does not already exist.

```
RESOURCE_GROUP="Kofax"
CONTAINER_REGISTRY="insight-registry"
az acr create -n $CONTAINER_REGISTRY -g $RESOURCE_GROUP --sku Basic --admin-enabled true
az acr credential show -n $CONTAINER_REGISTRY
```

5. On the computer where images were prepared, run the following commands to push the images to the Azure container registry.

```
docker login <CONTAINER_REGISTRY>.azurecr.io -u <CONTAINER_REGISTRY> --password <registry password>
docker tag insight-web <CONTAINER_REGISTRY>.azurecr.io/insight-web:v1
docker tag insight-scheduler <CONTAINER_REGISTRY>.azurecr.io/insight-scheduler:v1
docker push <CONTAINER_REGISTRY>.azurecr.io/insight-web:v1
docker push <CONTAINER_REGISTRY>.azurecr.io/insight-scheduler:v1
```

where <CONTAINER\_REGISTRY> is the registry name from the previous step.

To copy the registry password from the Azure portal container registry and fill in the <registry\_password> parameter, navigate to **Azure > Storage > Container registries > Access keys**.

6. Create a cluster and the nodes. Replace the placeholders for the following settings, copy the command to the **Azure Cloud Shell**, and run it.

```
USER_NAME="azureuser"
PASSWORD_WIN="userpassword"
RESOURCE_GROUP="Kofax"
CLUSTER_NAME="insight-cluster"
NODES_COUNT=1
CONTAINER_REGISTRY="insight-registry"
WIN_NODEPOOL_NAME="npwin"
```

### #cluster

```
az aks create \
  --resource-group $RESOURCE_GROUP \
  --name $CLUSTER_NAME \
  --node-count 1 \
  --enable-addons monitoring \
  --generate-ssh-keys \
  --windows-admin-password $PASSWORD_WIN \
  --windows-admin-username $USER_NAME \
  --vm-set-type VirtualMachineScaleSets \
  --network-plugin azure
```

```
az aks nodepool add \
  --resource-group $RESOURCE_GROUP \
  --cluster-name $CLUSTER_NAME \
```



```
--os-type Windows \
--name $WIN_NODEPOOL_NAME \
--node-count $NODES_COUNT
```

```
az aks get-credentials --resource-group $RESOURCE_GROUP --name $CLUSTER_NAME
```

### #storage

```
kubectl apply -f azure-file-sc.yaml
kubectl apply -f azure-file-pvc.yaml
kubectl get pvc
```

### #Log in to the container registry


```
kubectl create secret docker-registry regcred \
--docker-server=$CONTAINER_REGISTRY.azurecr.io \
--docker-username=$CONTAINER_REGISTRY \
--docker-password=<registry_password>
```

7. Replace the paths in the `kubernetes/insight-k8s-deployment.yml` file with the published Insight images paths.

<INSIGHT WEB IMAGE URL> should be replaced with <CONTAINER\_REGISTRY>.azurecr.io/insight-web:v1

<SCHEDULER IMAGE URL> should be replaced with <CONTAINER\_REGISTRY>.azurecr.io/insight-scheduler:v1

8. Define the databases.

 The databases should already exist.

9. Upload the `kubernetes/insight-k8s-deployment.yml` file to the **Azure Cloud Shell**.

10. Run the following command in the Azure Cloud Shell to publish Insight.

```
kubectl apply -f insight-k8s-deployment.yml
```

11. Wait until all pods are available. Use the following command to check the state.

```
kubectl get pod
```

12. Log in to Insight.

Use the following command to get an External IP for the cluster.

```
kubectl get services
```

To get an External IP and log in to Insight Admin Console.

```
http://externalIP/insight/admin
```

13. Optional. Enable the cluster autoscaler.

### #Node pools autoscaler

```
az aks nodepool update \
--enable-cluster-autoscaler \
--min-count 1 \
--max-count 5 \
--resource-group $RESOURCE_GROUP \
--name $WIN_NODEPOOL_NAME \
--cluster-name $CLUSTER_NAME
```

### #Pods autoscaler

```
kubectl autoscale deployment insight-web --cpu-percent=50 --min=1 --max=10
kubectl autoscale deployment insight-scheduler --cpu-percent=50 --min=1 --max=10
```

### #Getting autoscaler logs

```
kubectl get configmap -n kube-system cluster-autoscaler-status -o yaml
```

## Set up Insight in high availability mode on Docker with Swarm on-premise environment

1. Build the Insight Web and Scheduler images on the [on-premise](#) server.
2. Push the Insight images to a container registry such as an Azure container registry or DockerHub registry.

Use the following commands.

```
docker login [docker_rep_url] -u [user] --password [password]
docker tag insight-web [docker_rep_url]/insight-web:v1
docker tag insight-scheduler [docker_rep_url]/insight-scheduler:v1
docker push [docker_rep_url]/insight-web:v1
docker push [docker_rep_url]/insight-scheduler:v1
```

3. Create an SMB shared folder and map it to the G:\ drive on all nodes where a Docker container with Insight will be running.

For details, see documentation on the Microsoft [website](#).

4. Copy the Insight license file to the G:\ drive.
5. Install the Docker engine on all nodes.
6. Open the ports required for Swarm and Docker on all nodes. By default, the following ports should be available: 4789, 2377, 7946. For details, see the Swarm tutorial on the Docker [website](#).
7. Initialize the Docker Swarm environment on the primary node.  
Run the following command on the command line.

```
docker swarm init --advertise-addr [master node IP]
```


8. After the initialization is over, the console returns the following string. Copy the string to the other nodes and run the command to join the nodes to the cluster.

```
docker swarm join --token [Token-id] [ip:port]
```

9. To create an overlay network, run the following command.

```
docker network create --driver=overlay --attachable core-infra
```

10. Replace the paths in the Swarm/docker-compose.yml file:  
<INSIGHT WEB IMAGE URL> should be replaced with [docker\_rep\_url]/insight-web  
<SCHEDULER IMAGE URL> should be replaced with [docker\_rep\_url]/insight-scheduler
11. Define the databases.

 The databases should already exist.

12. Navigate to the Swarm folder and log in to the registry.  

```
docker login [docker_rep_url] -u [user] --password [password]
```
13. Deploy Insight in the Docker Swarm environment using the following command on the command line.  

```
docker stack deploy --compose-file docker-compose.yml --with-registry-auth insight
```
14. Open the /G drive properties and click OK on all nodes. Otherwise, Insight cannot be deployed.

**i** It is impossible to access Insight in the Swarm environment through the localhost URL. To access Insight in the Swarm environment, define the IP address and the host name on the primary node.

## Appendix A

# Recover from a lockout

A lockout may occur in the event that the administrator configures Windows authentication for Insight applications (Admin Console, Multi-Tenant Console, Viewer, Studio, Themes and Formats, or Data Loader) incorrectly and cannot log in. Use this procedure to recover from a lockout and restore the Authentication setting to None.

1. Locate **Web.config** at [drive:]\Program Files\Kofax\Insight 6.x.x\HtmlInsight\Admin.
2. Verify that the `PreventConfigChange` key is *True* under the `<appSettings>`. If not, add the following:

```
<add key="PreventConfigChange" value="true"/>
```

3. Change the authorization to the following:

```
<authorization>  
  <allow users="*" />  
</authorization>
```

4. Change the authentication mode to None.  

```
<authentication mode="None">
```
5. Repeat the procedure for other Insight applications, such as the Viewer, Studio, Themes and Formats, or Data Loader.

## Log in to an application as an Insight user

1. Locate the **Web.config** file at [drive:]\Program Files\Kofax\Insight 6.x.x\WcfDataService.
2. Verify that `<add key="Insight.DataService.TryInsightUsers" value="True" />` is *True*.
3. Access the application which has an incorrect login setup. In the address line, add `Login.aspx` at the end of the address.
4. Log in to the application as an Insight user.

## Appendix B

# Repair connection strings and apply a new encryption key

Use this section if the encryption keys are not available any more.

- To re-enter credentials for the Admin DB, run the Installation Manager in the *Install* mode (with the /i key).
- To re-enter credentials for the admin connection, launch Admin Console, open all connections and provide the credentials.
- To re-enter project credentials, open each project in Admin Console and provide the credentials.
- To re-enter data source credentials, expand a project, open each data source, and provide the credentials.

## Appendix C

# Set up and configure the load balancer

This section introduces an example of an entry point configuration. You can follow the recommended steps or use any load balancer as an entry point at your own responsibility. In the following example procedure, IIS Manager is used to configure load balancing. We recommend that you follow these steps to set up your own entry point. If you use a different load balancer as an entry point, refer to its respective documentation.

1. In **IIS Manager**, select **Get New Web Platform Components**.
2. In the browser window, download **Microsoft Web Platform Installer Download**, find **Application Request Routing**, and then install it.
3. A new menu item **Server Farms** is now present in **IIS Manager**. Right-click **Server Farms** and select **Create Server Farm**.
4. Enter the farm name.
5. On the **Add Server** screen, enter IP addresses for the computers with Insight and click **Finish**.
6. On the **Rewrite Rules** screen, click **Yes**.

## Settings for the web farm

1. On the **Server Affinity**, select **Client Affinity** and click **Apply**.
2. On the **Load Balance**, set the applicable load balance algorithm and click **Apply**.

## Insight-specific cookies

Although additional configuration is usually not required to set up sessions, you may take into account the following Insight-specific cookies:

```
<ApplicationType>__Insight_SessionId_<FullVersion>
```

where <ApplicationType> is one of the following applications:

- "Admin" for Admin Console
- "ThemeManager" for Themes and Formats
- "Studio" for Studio
- "Data Loader" for Data Load Manager

and <FullVersion> is the Insight build number listed in the "Version information" section in the *Kofax Insight Release Notes 6.5.0*.

For Viewer, the following cookies are used:

Viewer\_<ApplicationName>\_Insight\_SessionId\_<FullVersion>

where <ApplicationName> is the name for a Viewer application (you can add custom viewers), default application name is "View",

and <FullVersion> is the Insight build number listed in the "Version information" section in the *Kofax Insight Release Notes 6.5.0*.

## Appendix D

# Windows Active Directory authentication support

In Insight, Active Directory authentication is available for all Insight components, including Installation Manager, Scheduler service, Import and Export utilities. For Installation Manager and Import and Export utilities, the user mapping for the Admin application is used. For Scheduler, the user mapping for the Data Loader application is used. Only users with the administrator role can log in to Installation Manager, Scheduler service, and the Import and Export applications.

To enable Active Directory authentication, select **Enable Windows authentication for Data Service** in Installation Manager.

The LDAP path is defined in the WCF data service web.config. To use LDAPS, define the LDAP path in the following way: LDAP://ldap.domain.com:636

If a self-signed certificate is used, obtain the root certificate and install it as a Trusted Root Certificate. The fully-qualified domain name that you use to connect to Active Directory must match the SSL certificate exactly.

## Configure the IIS environment

1. Verify that Windows Authentication is enabled in IIS for the Insight application.
  - a. Open the IIS manager on the server where Insight is installed and select the Insight application.
  - b. Click the **Authentication** icon.
  - c. Verify that **Windows Authentication** is enabled.
2. The IIS Application Pool where the WCFDataService is located (ASP.NET v.4.0 by default) must be changed to run under the user that can be authenticated to the Windows Active Directory configured for Insight.
  - a. Open the IIS manager on the server where Insight is installed.
  - b. In the **Connection** pane, expand the server node and click **Application Pools**.
  - c. On the **Application Pools** page, select the Application Pool that contains the WCFDataService. **Note:** To view all the applications in the Application Pool, click **View Applications** in the **Actions** pane.
  - d. Click **Advanced Settings** in the **Actions** pane.
  - e. Under the **Process Model**, change the identity to the account that has access to the Windows Active Directory.




- f. Restart the Application Pool.

## Troubleshoot Windows Active Directory authentication

In case of a login failure, use the following steps to troubleshoot the issue. Perform an attempt to log in to the Viewer or Insight to capture the HTTP session parameters and values from the Windows Active Directory into the log file.

1. Verify that Authentication and User mapping settings are configured properly.

 For example, if you set up Windows authentication for the Viewer, make sure that under Authentication and User mapping settings the application is set as "Viewer."

2. Check the log files: Navigate to C:\Temp\Insight\_6.x.x.
3. Open WcfDataService.log.
4. Search for "WcfDataService.Code.InsightService.LoginProvider."
5. Scroll to the Active Directory properties list. If you use *Identity* as the session parameter in the user Identifier, search for the "Identity" key word and verify it passes the correct value as expected. Also, search for *memberOf* and verify that the value is correct.
6. Verify that you have specified the property being returned. Also, if the list is separated by commas, verify that you specified *Include* in your Fixed values mapping for the role:

```
givenName: John distinguishedName: CN=John
Doe,OU=Users,OU=US05,OU=US,OU=Countries,DC=MyCompany,DC=com instanceType: 4
whenCreated: 5/7/2014 8:52:59 PM whenChanged: 1/25/2016 8:37:08 PM
displayName:
John Doe otherTelephone: 2154446666 uSNCreated: System.__ComObject memberOf:
MyCompany.MyDept, CRMReportingGroup, CRMReportingGroupDev, MyDepartment_US,
MyDept_Media, All MyDept, Products_users, ProjectServer, ProjectManagers, VPN
Users uSNChanged: System.__ComObject co: United States department: MyDept -
Products company: MyCompany Inc. proxyAddresses: SMTP:John.Doe@MyCompany.com,
smtp:hDoe@MyDept.com, SIP:John.Doe@MyCompany.com, smtp:John.Doe@MyDept.com
countryCode: 840 employeeID: 5648 homeDirectory: \\us05401\users$\John.Doe
homeDrive: U: badPasswordTime: System.__ComObject lastLogoff:
System.__ComObject lastLogon: System.__ComObject pwdLastSet:
System.__ComObject
primaryGroupID: 513 objectSid: System.Byte[] accountExpires:
System.__ComObject
logonCount: 1368 sAMAccountName: John.Doe
```

## Appendix E

# Insight log files

This section gives you an overview of the information that is available in the Insight log files, which are located in the folder specified during installation:

C:\Temp\Insight\_6.x.x where 6.x.x is the version number.

Full access (read/write) to C:\Temp is required for logging.

### **AlertDistribution**

Information related to the Alert generation/distribution feature.

### **Altosoft.Insight.InstallManager**

Information on Insight software installation and other activities related to the Insight Installation Manager.

### **BridgeService**

Information related to the Insight Bridge Service, which is used to communicate with 32-bit data sources on 64-bit operating systems. This might be used with Excel or a 32-bit ODBC driver on a 64-bit computer.

### **ChartSnapshot**

Information related to the Chart Snapshot (report printing) functionality.

### **DataLoad**

Information related to the Data Loader web application.

### **DataProcessing**

Information related to dashboard queries (to the Data database/Data mart) to get data for dashboard display at runtime (View application) and design time (Studio application).

### **ImportExport**

Information related to import and export activity of the standalone Import/Export tool.

### **InsightAdmin**

Information related to the Admin Console web application.

### **InsightInstallation**

Information related to the main MSI installer for Insight software.

### **InsightServer\_WinApp**

Information and execution details for data loading (execution plans).

### **InsightStudio**

Information related to Studio web application.

### **InsightThemes**

Information related to the Themes and Formats web application.

### **InsightViewer**

Information related to the Viewer web application.

### **ProcessManager**

Information related to data loading of processes.

### **ReportDistribution**

Information related to the scheduled report generation/distribution feature.

### **Scheduler**

Information on the Insight Scheduler Service, which is used to update and launch scheduled tasks (as defined in execution plans).

### **UpdateTable**

Information related to database and table schema changes, typically due to Studio project development and Import/Export activity.

### **WcfDataService**

Information related to the WcfDataService web service. Includes database (Admin, Meta, and Data) queries for all Insight web applications; and user authentication and login activity for all the web applications.