Kofax Insight

Administrator's Guide

Version: 5.4.0

Date: 2016-08-30

KOFAX
from Lexmark

Table of Contents

Preface

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

Getting help for Kofax products

Kofax regularly updates the Kofax Support site with the latest information about Kofax products.

To access some resources, you must have a valid Support Agreement with an authorized Kofax Reseller/Partner or with Kofax directly.

Use the tools that Kofax provides for researching and identifying issues. For example, use the Kofax Support site to search for answers about messages, keywords, and product issues. To access the Kofax Support page, go to www.kofax.com/support.

The Kofax Support page provides:

- Product information and release news

  Click a product family, select a product, and select a version number.
- Downloadable product documentation

  Click a product family, select a product, and click **Documentation**.
- Access to product knowledge bases

  Click **Knowledge Base**.
- Access to the Kofax Customer Portal (for eligible customers)

  Click **Account Management** and log in.

  To optimize your use of the portal, go to the Kofax Customer Portal login page and click the link to open the *Guide to the Kofax Support Portal*. This guide describes how to access the support site, what to do before contacting the support team, how to open a new case or view an open case, and what information to collect before opening a case.
- Access to support tools

  Click **Tools** and select the tool to use.
- Information about the support commitment for Kofax products

  Click **Support Details** and select **Kofax Support Commitment**.

Use these tools to find answers to questions that you have, to learn about new functionality, and to research possible solutions to current issues.

Chapter 1

Admin Console

Use the Admin Console to configure and administer Kofax Insight to activate and manage your Insight licenses, define user mapping and authentication, and specify a language. You can also define users, roles, and calendars, create view filters, view logs and alerts, and define global SQL functions.

Configuration Settings

- License Manager: Add and manage Insight licenses. Obtain the product license from your Kofax sales representative or from Kofax Support.
- Authentication: Configure Insight to use HTTP (custom) or Windows Active Directory to authenticate the user. Insight user authentication is the default.
- User mapping: Use to map (identify) a user from a non-Insight source, such as from Windows Active Directory.
- Localization (under Options): Configure the Insight applications to display in any of the supported languages. US English is the default language.

Administration Settings

- Admin dashboard: View an overview of activity and access rights.
- Users: Create and manage users.
- Roles: Create, remove, or modify roles, which provide access rights to projects and views (dashboards).
- Calendars: Define custom calendars to incorporate in your dashboards.
- Filters: Create global and non-global filters that can be used in Insight views (dashboards).
- Alerts: View all alerts that are configured in InsightStudio.
- Map Aggregate: Add, remove, and administer map aggregate node servers.
- Logs: View audit logs.
- SQL Functions: Define global SQL function that can be used when building a dashboard.

Access Admin Console

1. In the Insight program folder, select **Administration** > **Admin Console**.
   The Insight Admin Console login window appears.
2. Enter a valid username and password, and click **Log in**.
   The login credentials are set during the installation. See the *Kofax Insight Installation Guide*.
   The Admin Console appears.
3. Activate the product license.
   See License manager.

4. Select an option from the **Documents Tree**:
   - Admin dashboard
   - Authentication
   - Projects
   - Connectors
   - Users
   - User mapping
   - Roles
   - User filters
   - Filter group
   - Alerts
   - Distribution
   - Calendars
   - Map-Aggregate
   - Logs
   - Options
   - License manager
   - SQL Functions

Chapter 2

Configuration Settings

License manager

License management is available within the Admin Console application. If the license is expired, the following behavior applies:

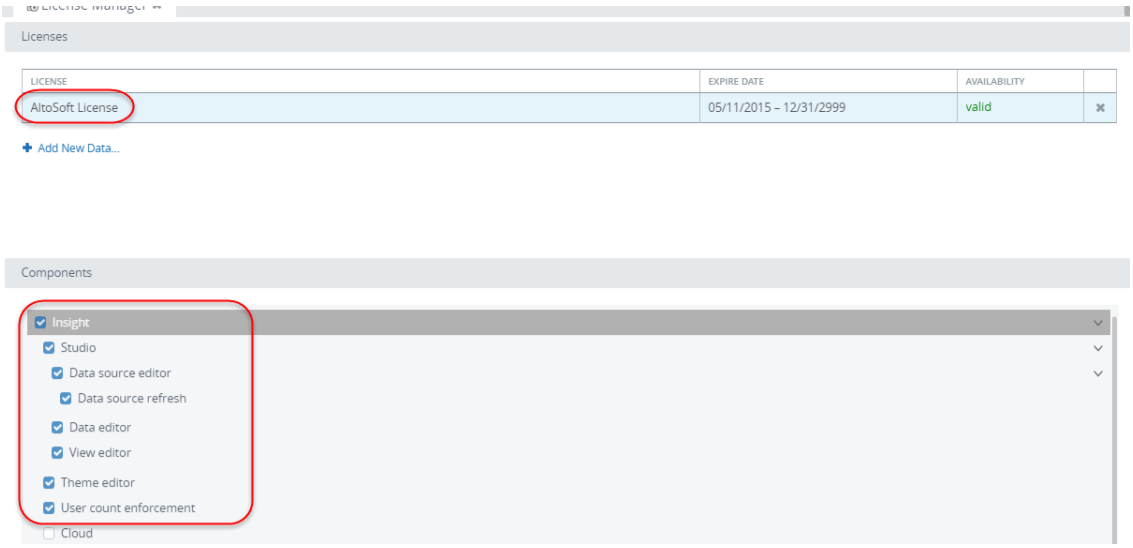
- You can still access Admin Console if you are authorized for this application.
- If you try to access Studio, Data Loader, or Themes and Formats, you are prompted with the message "The license has expired. Please contact your administrator." After this message is cleared, you are redirected to the **License Manager** tab within the Admin Console, if you are authorized to access it.
- If you try to access the Viewer, you are only prompted with the message "The license has expired. Please contact your administrator." (without any redirection to the License Manager window).

Use the following steps within **License Manager** to add and maintain licenses.

1. In **Admin Console**, on the Documents Tree, click **License manager**.
   The License Manager window appears.
2. The **License** section shows all active licenses. To upload a new license, click the **Add New Data** link and navigate to the location of the license file.

   Note Licenses are XML files. If your license is delivered in a compressed file format (such as ZIP), you must extract and store the XML on the computer before you select **Add New Data**.

3. Select a license to view **Components** affected by the license.



The following rules apply.

For the Studio application:

- **Data source editor**: If this check box is not selected, you cannot edit data sources.
- **Data source refresh**: If this check box selected, you can edit data sources with the following limitations: the list of tables is fixed and cannot be refreshed, and you cannot create or delete data sources. This option is disabled if the previous **Data source editor** option is disabled.
- **Data editor**: If this check box is not selected, you cannot open, create or edit records, metrics, or translation tables.
- **View editor**: If this check box is not selected, you cannot create or edit Views.

For the Themes and Formats application:

- **Theme editor**: If this check box is not selected, the **Themes and Formats** application is hidden.

For user count:

- **User count enforcement**: If this check box is selected, the system checks for the **Maximum Named Users** or **Maximum Concurrent Users** every time you start the Insight WCF service (see the section **Options** below).

  If this option is enabled, and the numbers for **Maximum Named Users** and **Maximum Concurrent Users** are exceeded, the user is not granted an access to the Insight applications. A license violation message is shown to the administrator.

  If this option is disabled, and the numbers are exceeded, the user can still log in to the Insight applications. A license violation message is shown to the administrator.

4. In the **Options** section, you can see how many data sources and concurrent users are allowed by the license.
   - **Maximum Data Sources**: If the value is zero, it means you can use an unlimited number of data sources. If this box displays a positive number, it specifies how many Excel files and web service data sources you can create and save. If you attempt to enter an invalid number, you are prompted with the message "Could not save the document." This option is disabled if **Data source editor** is not selected.

Note Data DB data sources and Staging DB data sources are not counted with this option.

- **Maximum Named Users**: If the value is zero, an unlimited number of unique users are allowed. If this box displays a positive number, it specifies how many users you can create in Admin Console with the rights to log in to any application.

  Note The number of distinct values in the User column is counted in the dbo.LOGINLOGS table in the Admin database. This number is checked every time you launch Admin Console, and if it exceeds the limitation, you are prompted with the message "The number of unique users <X> exceeds the license value of <Y>. Please contact your administrator."

- **Maximum Concurrent Users**: If the value is zero, an unlimited number of concurrent sessions are allowed. IIf this box displays a positive number, it specifies how many concurrent sessions are allowed.

  Note Sessions are counted from memory (in case High Availability is disabled). The administrator can monitor the number of sessions on the Admin Dashboard or in the db.SESSIONS table in the Admin database (if High Availability mode is enabled). If the number is invalid, you are prompted with the message "The number of concurrent users at <date/time> <X> exceeds the license value of <Y>. Please contact your administrator."

Email notifications

If you set up the SMTP server, all license violations related to unique and concurrent users and license expiration are sent to the specified email of the administrator.

Authentication

You can set up authentication to allow users to see a dashboard, require user names and passwords, and allow individual levels of access and roles associated with a specific login.

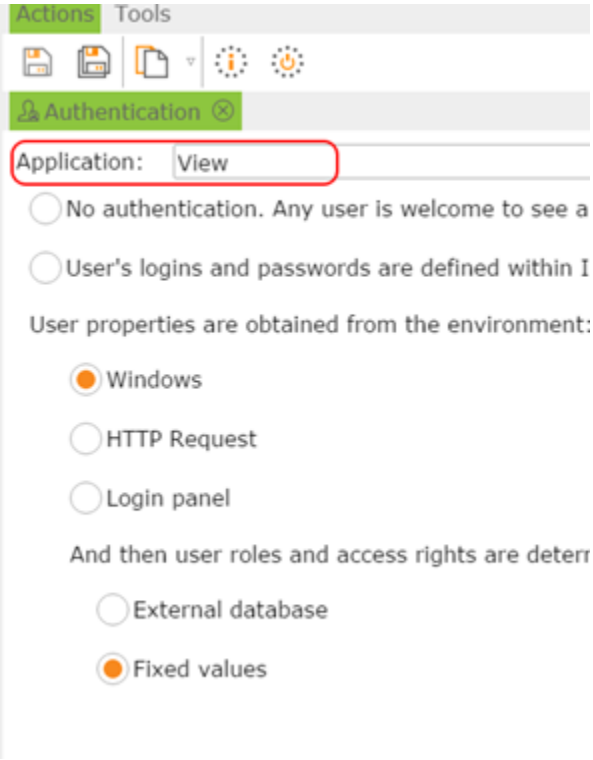
Use the Authentication tab to set authentication preferences that affect access to the following Insight components and applications: View (dashboards), Studio, Admin Console, Themes and Formats, and Data Loader.

Configure authentication to allow any user to access any Insight application, or you can limit access levels based on login credentials and user roles.

You can define authentication for each Insight application. The table lists the default authentication types.

Insight application	Default authentication type
Admin Console	Insight
Studio	None
Themes and Formats	Insight
Data Loader	Insight
View (Dashboards)	No authentication

Select the application from the list.

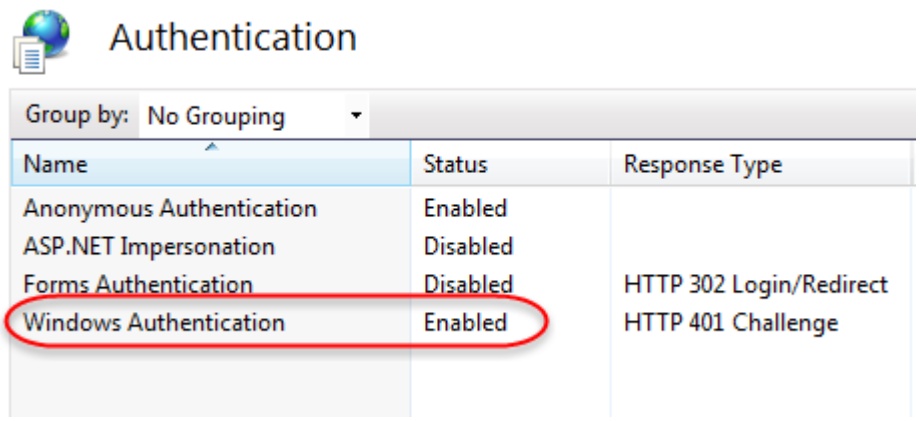


Windows authentication

For all Insight applications, you can use Windows Active Directory authentication, which is checked only once when the user logs in.

To use Windows (Active Directory) authentication in Insight, follow these steps.

1. Verify that Windows authentication is enabled in IIS for the Insight application.
    1. Open IIS Manager on your computer and select the Insight application.
    2. Click the **Authentication** icon.
    3. Verify that **Windows Authentication** is enabled.



2. In the **Admin Console**, in the **Documents Tree**, click **Authentication**.
   The **Authentication Method** window appears.
3. Select **Windows** and **Fixed values**.

   Note Selecting **Windows** changes the authentication type of the web application in the corresponding **Web.config** file the next time a user launches the application. If Windows authentication is not defined properly, the user may be locked out from the application. In this case, you need to change **Web.config** manually. See Recover from a lockout.

   To add additional or multiple Active Directory domains/subdomains, use this procedure.

   1. Open **Web.config** at `<Insight installation folder>\HtmlInsight\View`.
   2. Add the LDAPPath key and value for each subdomain.
      The key name must start with `LDAPPath`, such as:
      `LDAPPath`
      `LDAPPath-1`
      `LDAPPathAnyPath`
      String examples:

```
<add key="LDAPPath-US1" value="LDAP://US1.kofax.com:8668/DC=kofax,DC=com" />
<add key="LDAPPath-US2" value="LDAP://US2.kofax.com:8668/DC=kofax,DC=com" />
```

      Note LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information on a server.

Enter the user identifier

Define user identifier settings. This identifier should be constant for a specific user logon. Usually, it is session property - *Identity* and looks to the Active Directory domain/user.name.

1. Navigate to **Admin Console** > **User mapping**.
2. Select an application from the drop-down list:
   - Admin Console

- Data Loader
- Themes and Formats
- View
- Studio

3. Navigate to the **User Identifier (UID)** tab and select an option.
   - Use User Name. The display name of a user account.
   - Session property
   - Database query

   Note User Name and Email are optional parameters.

4. Select **User Name** and then select from the available options.
   - Deny authentication for users with undefined name
   - Use Email
   - Session property. This is typically one of the Active Directory properties such as *Identity*, *FullName*, or *display/Name*.
   - Database query and database source.
5. Select **Email** to enter the user's email.

   This email is used for self-subscriptions only. This is typically the Active Directory *EmailAddress* property.

Define role mapping

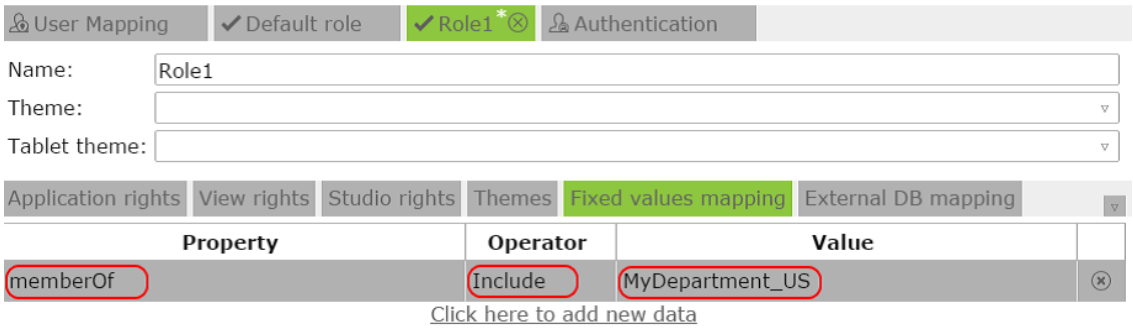
Roles define a set of predefined Admin Console settings, such as the theme and date format. Roles also define specific access rights to projects and dashboard views. You must describe mapping rules for each role. Typically, the Active Directory property *memberOf* is used for this purpose.

Each row in the mapping grid uses the AND operand. If more than one role matches conditions for a user account, the access rights are merged from all matching roles. Other settings, such as theme and date format, are assigned by the top matching role in the list.

1. In **Admin Console**, in the **Documents Tree**, select **Roles**, and click **New**.

   The **New Role** window appears.
2. In the **Name** field, enter a role name.

   The Role editing window appears.
3. Define the elements for the role such as Application rights, View rights, Studio rights, Themes, Fixed values mapping, or External DB mapping.
4. Select **Click here to add new data**.

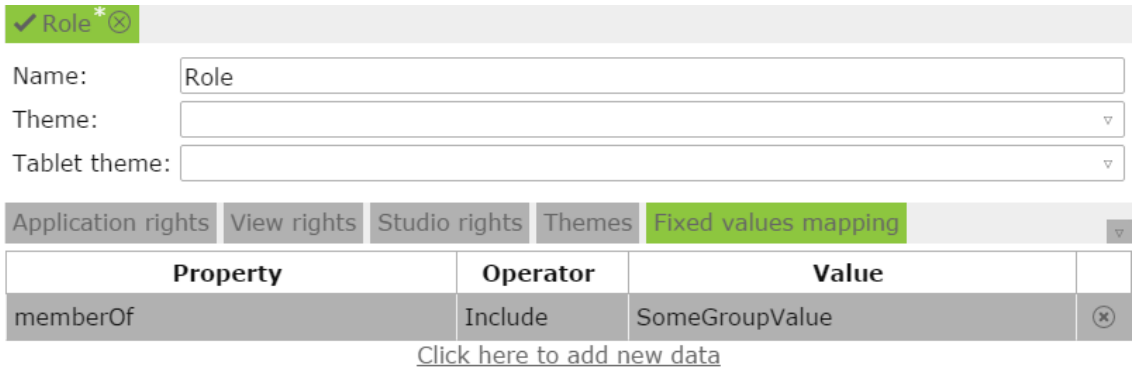


Where "MyDepartment_US" is an Active Directory group that the users are members of.

Note It is important to use the operator *Include* rather than *Equal*, because the property *memberOf* is a list of items for which you can specify only one item.

Sample flow for Active Directory authentication setup

1. Verify that **Windows authentication** is enabled under the IIS settings for the Insight application (View, Studio, Admin Console or other).
2. Select **Admin Console** > **Authentication** , and select **Admin Console** from the applications list.
3. Select **Windows** and **Fixed Values**, and save the changes.
4. In the **Documents Tree**, select **User mapping** and select **Admin Console** from the applications list.
5. Open the **User Identifier (UID)** tab and select the **Session property** check box. Enter *Identity* as the session property and save the changes.
6. In the **Documents Tree**, select **User mapping** > **Roles**. Right-click and then select **New**.
7. For the role, select the **Fixed values mapping** tab and enter *memberOf* as the Property, select **Include** as the Operator, and then enter the group the user belongs to. Save the changes.



8. Assign the role to the user.
   Now the user can log in to Admin Console as a Windows user.

Troubleshoot Windows Active Directory authentication

In case of a login failure, use the following steps to troubleshoot the issue.

1. Navigate to `C:\Temp\Insight_5.x.x`.
2. Open **WcfDataService.log**.
3. Search for "WcfDataService.Code.InsightService.LoginProvider."
4. Scroll to the Active Directory properties list.
5. 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, MyDeptarement_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
```

HTTP authentication

When you access an Insight dashboard from another application, you are not required to log in again to access the Insight dashboard. To avoid the duplicate login, the calling application can open the dashboard via an HTTP request. In this case, the calling application passes a parameter such as `sessionid` to the dashboard.

Complete the initial settings

Define connections to external databases to look up user properties including name, role, and filtering.

1. In the **Admin Console**, in the **Documents Tree,** right-click **Connections** and click **New**.
2. Enter a name for the new connection and click **OK**.
3. Enter the information for the connection.
4. Return to the **Admin Console** and select **Authentication**.
5. In the **Authentication Method** window, in the **User properties are obtained from the environment** section, click **HTTP Request**.
6. Select the **User Mapping** tab and specify a way to obtain the **User Identifier**. The User Identifier should be unique and constant for each user across different sessions. This identifier is used to detect ownership of views, alerts, and so on.

Important Within HTTP requests, you must always include a **User Identifier** parameter. Additional parameters are optional.

Possible options include:

- **Use User Name**: from the `User name` property
- **Session property**: directly from a special parameter of HTTP requests
- **Database query**: from user DB using a parameter of an HTTP request in a database query. Specify an SQL script that will return the user identifier. The query can use any parameters from the HTTP request string.

Note The property name is case-sensitive. Ensure you use the correct property name in an SQL statement.

Within SQL statements, each URL property should be placed within «**<**» and «**>**» characters for numeric values, and within angle brackets (**<** and **>**) for strings.

Example

Select Identifier from Users where Staff_ID = < UserID>

Where:

Staff_ID and **Identifier** are fields from the User table.

UserID is a URL parameter.

7. Select the **User Name** tab. (Optional)

   Select from the available options.

   - **Deny authentication for users with undefined name**
   - **Use Email**.
   - **Session property**. Example: UserName.

     Through a parameter within an HTTP request (**Session property**) where UserName is a variable to be passed in the HTTP header.
   - **Database query**. Enter the **Source** and the query. For example, select FullName from Users where Staff_ID=<UserID>

8. Select the **Email** tab. (Optional)
   - **Session property**. Through the URL parameter such as UserEmail.
   - **Database query**. Enter the Source and the query. For example, select Email from Users where Staff_ID=<UserID>.

9. On the toolbar, click **Save**  .

Map users to roles

You can map users to roles in two ways.

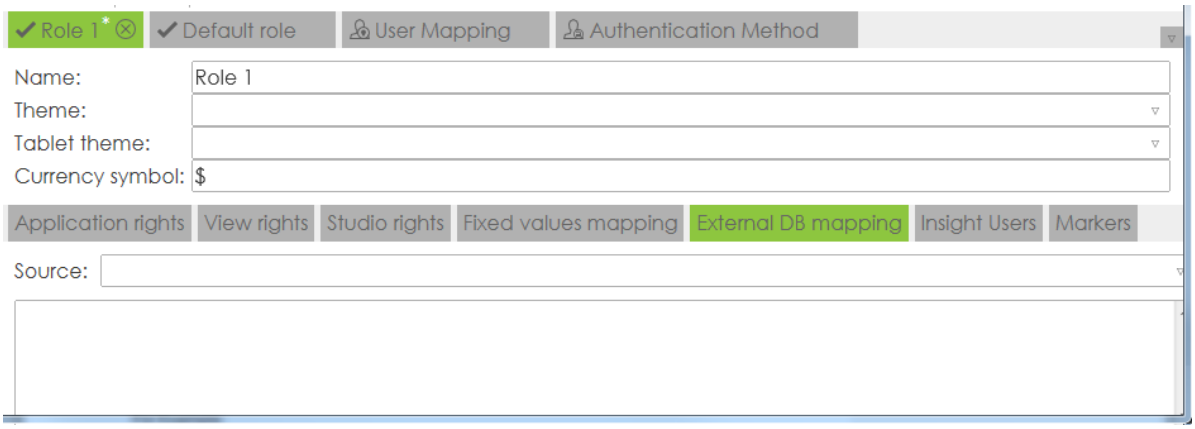
- Custom database query
- Fixed value

Custom Database Query

1. In **Admin Console**, in the **Documents Tree**, click **Authentication**.
2. Select **HTTP Request** and **External database**.

   Note Use this option to configure user roles from a custom query to an external database.

3. In **Admin Console**, right-click **Roles** and click **New**. Name the new role and click **OK**.
4. On the **External DB mapping** tab, **Source** field, enter the database connection string. In the area below the **Source** field, enter the SQL query.



Note Within an SQL statement, each URL property should be placed within «**<**» and «**>**» characters for numeric values, and within «**'<**» and «**>'**» for strings.

Any parameters from HTTP request string can be used within a query.

Example
Select *from Roles_Mapping
where Staff_ID='<UserID>' and Group_ID = 'Role'
Where:
Staff_ID and **Group_ID** are fields of Roles_Mapping table.
UserID is a parameter from an HTTP request.
'**Role**' is an identifier/name of a particular role.

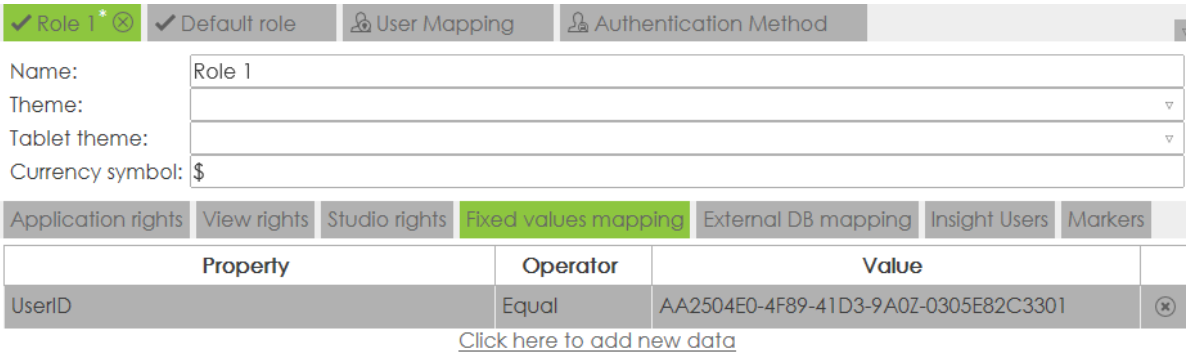
If the query returns at least one value, the user will get the rights of the selected role.

Fixed Values

1. In the **Admin Console**, in the **Documents Tree**, click **Authentication**.
2. Select **HTTP Request** and **Fixed values**.

   Note In this case, the parameters sent via HTTP request are compared to a fixed value.

3. In the **Admin Console**, right-click **Roles**, and click **New**. Name the new role and click **OK**.
4. In the **Fixed values mapping** tab, define the property that needs to be compared.



1. Select **Click here to add new data**.
2. Add the property to compare, such as *UserID*.

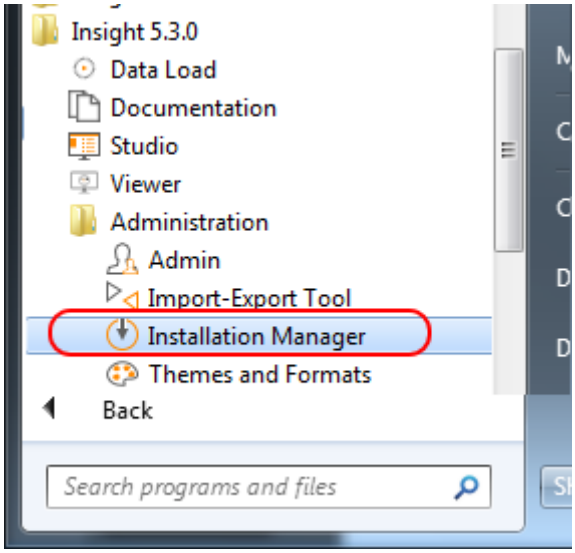
   Note This parameter is passed in the URL.

3. For the **Operator**, select **Equal** from the list, and add the fixed value.

Multiple authentication forms

You can configure different authentications for each Viewer instance and for Insight. Each instance has its own URL to access Insight.

1. Run the Insight Installation Manager.



2. In the **Insight Installation Manager**, click **Virtual Directories** > **Edit** > **Add New View** to add a new **Viewer** .

   Note Each added Viewer can be assigned a different type of authentication.

   All added Viewer instances are listed in the **Insight Installation Manager**.

3. Log in to **Admin Console** and in the **Documents Tree**, select the **Authentication** tab.

   All Viewer instances appear in the list under **Application**.

4. Set the required type of authentication for each application on the list.

   Examples

   - To only accept Insight users, select the **Login panel** and **Fixed values** for the Viewer instance such as "View1."
   - To access the Viewer instance *View1*, by the link, add "View1" to the end of the string in place of <Viewer instance name> : <server name>/Insight/<Viewer instance name>.
   - To only accept Windows authentication for "View2," select **Windows** authentication for the Viewer instance "View2."

   In this case, all Insight users access Insight via a specific URL and all Windows Active Directory users access Insight via a different URL.

   In this way, `https://myserver.com/Insight/View1` authenticates only Insight users, while `https://myserver.com/Insight/View2` authenticates only Windows Active Directory users.

Data authorization or Data access control (optional)

Data authorization or data access control is defined with user filters, which are used to restrict data based on a parameter such as a UserID or DepartmentID. You can use URL parameters to filter data. For example, you can use the UserID passed from the HTTP authentication request to identify the user, and filter all data that is based on that user's group. If you have a dashboard but only want users to see data filtered by their group_id, you can create the filter here for use in a record or metric.

You can also use user filters to define the financial year for time dimensions, when the year needs to be broken down by years and quarters.

1. In **Admin Console**, right-click **User filters** and click **New**. Name the filter and click **OK**.
2. Enter the following filter details.
   1. In the **Name** field, enter the name of the filter.
   2. In the **Source** field, define a connection source to a database from the **Admin Console** > **Connection** tab. This connects to a database that the Query (filter) runs against.
   3. In the **Query** field, enter the query to execute on the database specified in the **Source** field. For example, select Clients from Clients_mapping where Staff_ID = '<UserID>' .

      Note Within an SQL statement, each of the URL properties should be placed within «**<**» and «**>**» characters for numeric values, and within «**'<**» and «**>'**» for strings.

Example

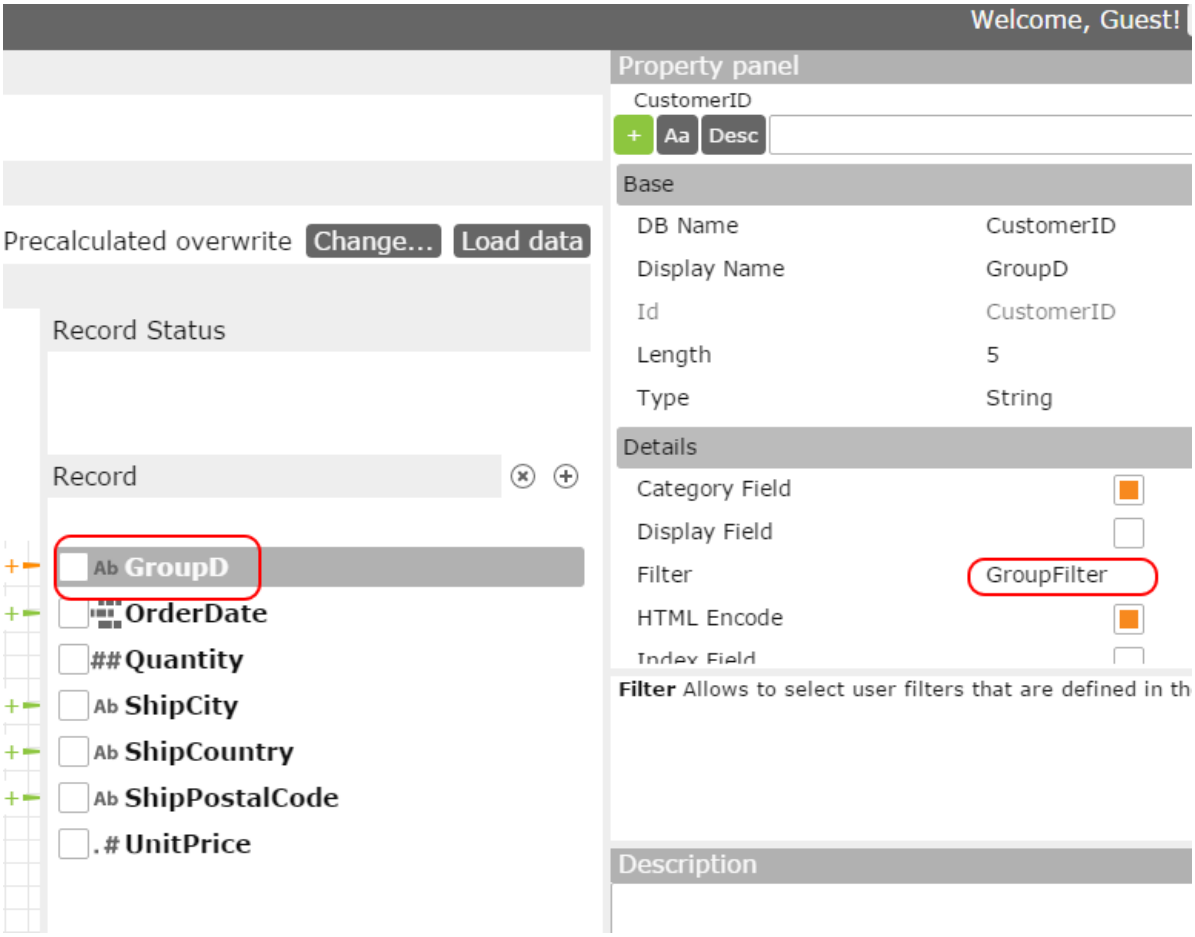
Select Clients from Clients_mapping where Staff_ID = '<UserID>'

Where:

Clients, Staff_ID - are fields of Clients_Mapping table

UserID - is a parameter from an HTTP request

3. Specify that filter for needed dimensions of records or metrics within Insight Studio.
   1. Log in to Insight Studio.
   2. Open a metric or a record to which the filter will be applied.
   3. Select the field that needs to be filtered. On the Property Panel, select **Filter**. From the list of filters, select the filter created above.

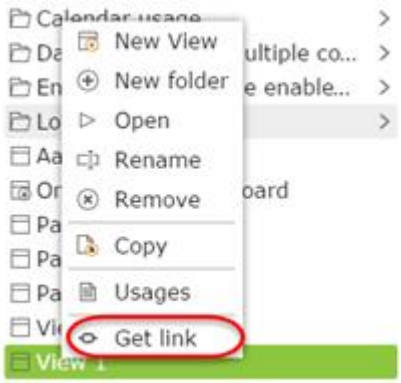


4. To define the beginning of the financial year, create a user filer with the following query: select 'MM/DD/YYYY'. Insight takes the month from this date as the first month of the financial year. For example, if you use the query 'select 06/01/2016,' the first quarter always starts with June.

Log in using HTTP request

You can use an HTTP request to log in to the Insight View (dashboard). For this purpose, configure an Insight View to use HTTP authentication (see HTTP authentication) and get the URL from the Studio.

1. In **Studio**, in the **Documents Tree**, expand **Views**.
2. Right-click the applicable View, and select **Get link**.



The full URL appears for the View.

Example:

```
http://127.0.0.1/viewer/?ProjectId=11e172c2-
fa42-40b6-9bad-4c2157e37ae6&ViewId=4ee45163-7092-4379-985a-48eb816a771f&ViewName=Chart_BreakDown
```

3. Copy the URL and add the *UID* parameter specified under the **User mapping** > **User Identifier (UID)**.

   For example, if you have *UserID* as the UID parameter, add *UserID* as a URL parameter and specify the value.

   ```
   http://127.0.0.1/viewer/?ProjectId=11e172c2-
   fa42-40b6-9bad-4c2157e37ae6&ViewId=4ee45163-7092-4379-985a-48eb816a771f&ViewName=Chart_BreakDown
   ```

   Use this URL to log in to the *Chart_BreakDown* View.

Send filter values through URL strings

You can provide filter parameters for a View via a URL, which is used to launch the Viewer in a ceratin state. For example, the filters can be passed as parameters in the URL. Insight uses the following prefixes for parameters.

- "Gr": for a Group
- "Dim": for a Dimension
- "Val": for a Value

As an example, you can configure a View to use the following>

- "MyGroup1" as a Group
- "ShipCountry" as a Dimension
- "USA" as a Value
- "MyGroup2" as a Group
- "Boise" as a Value

1. In the parameter name, specify the group using the *Gr* prefix.
   Example: `Gr1st=MyGroup1`
2. To specify the dimension, use the group key name `Gr1st` and the prefix *Dim*.
   Example: `Gr1stDimCity=ShipCountry`
3. To enter the value, use the group name, dimension key name, and the prefix *Val*.
   Example: `Gr1stDimCityValspec=USA`.
   The full URL for a View with parameters may look similar to this example:
   `http://127.0.0.1/viewer/?ProjectId=11e172c2-fa42-40b6-9bad-4c2157e37ae6&ViewId=4ee45163-7092-4379-985a48eb816a771f&ViewName=Chart_BreakDown&(`**View URL**`)UserID=User1&RoleID=Role1&(`**HTTP authorization parameters**`)Gr1st=MyGroup1&Gr1stDim1=ShipCity&Gr1stDim1Val1=Boise&Gr2nd=MyGroup2&Gr2ndDim1=ShipCountry&Gr2Dim1Val1=USA(`**six filter parameters**`).`

Connect to an external database

Use the Connections window to establish a connection between Insight and an external database.

1. In **Admin Console**, on the Property Panel, right-click **Connections** and click **New**.
   The New Shared DB window appears.
2. Enter a name for the new shared database and click **OK**.
   The **Connection Option** window appears.
3. Enter database information such as **Database type**, **Server Name**, **Provider Name**, and **Database Name**.
4. Enter the **User Name** and **Password**, or select **Windows Authentication**.
5. On the toolbar, click **Save** .

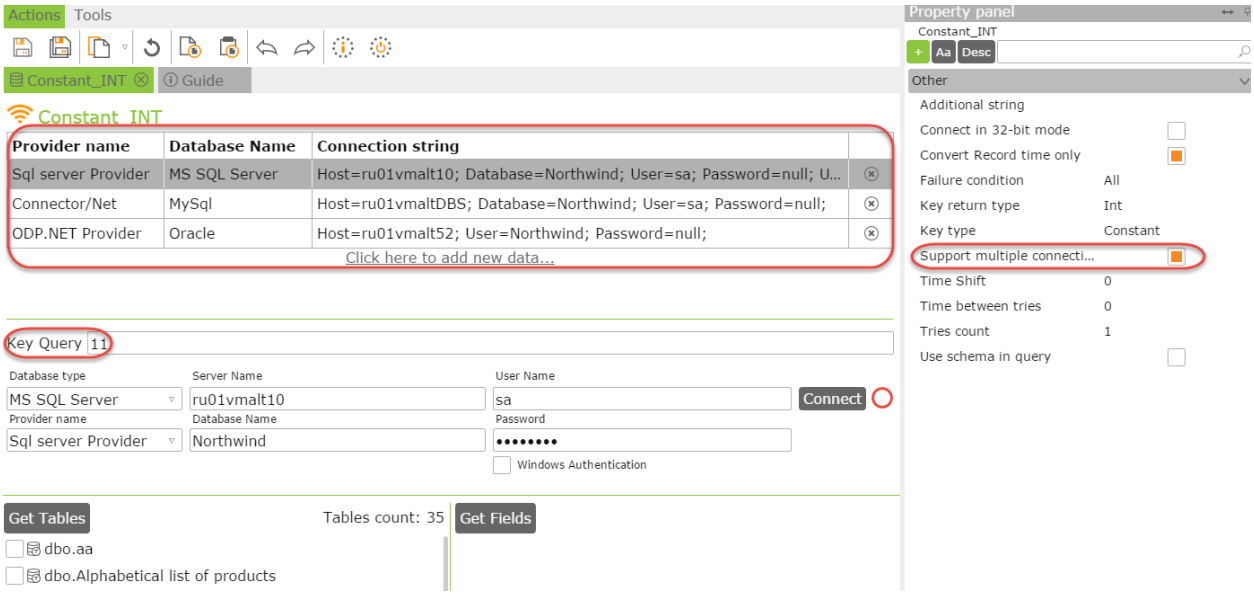
Multiple connection strings

A single data source may connect to multiple databases. For example, if you need to authenticate using Kofax Total Agility with multiple instances (database deployments), a single data source may contain multiple databases and queries at the same time.

You can use the data source both in **Admin Console** > **Connections**, and in Studio, within a project. Please note the following when using multiple connections strings:

- Only tables with the same structure (field names and types) can be used from multiple connection data sources.
- When the data is loaded from multiple databases, the data is combined from all connections of the data source.
- To enable multiple connection strings, the **Support multiple connections property** must be selected.
- It is possible to add a connection identifier to the loaded data. This data connection identifier can be defined in the **Key Query**.

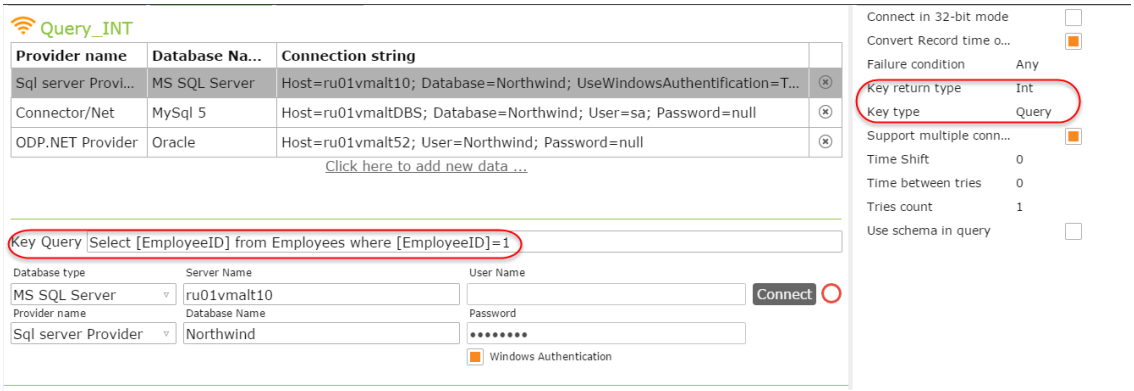
> **Note** **Key Query** can be defined in Studio for project data sources. Connections do not have any Key Query.



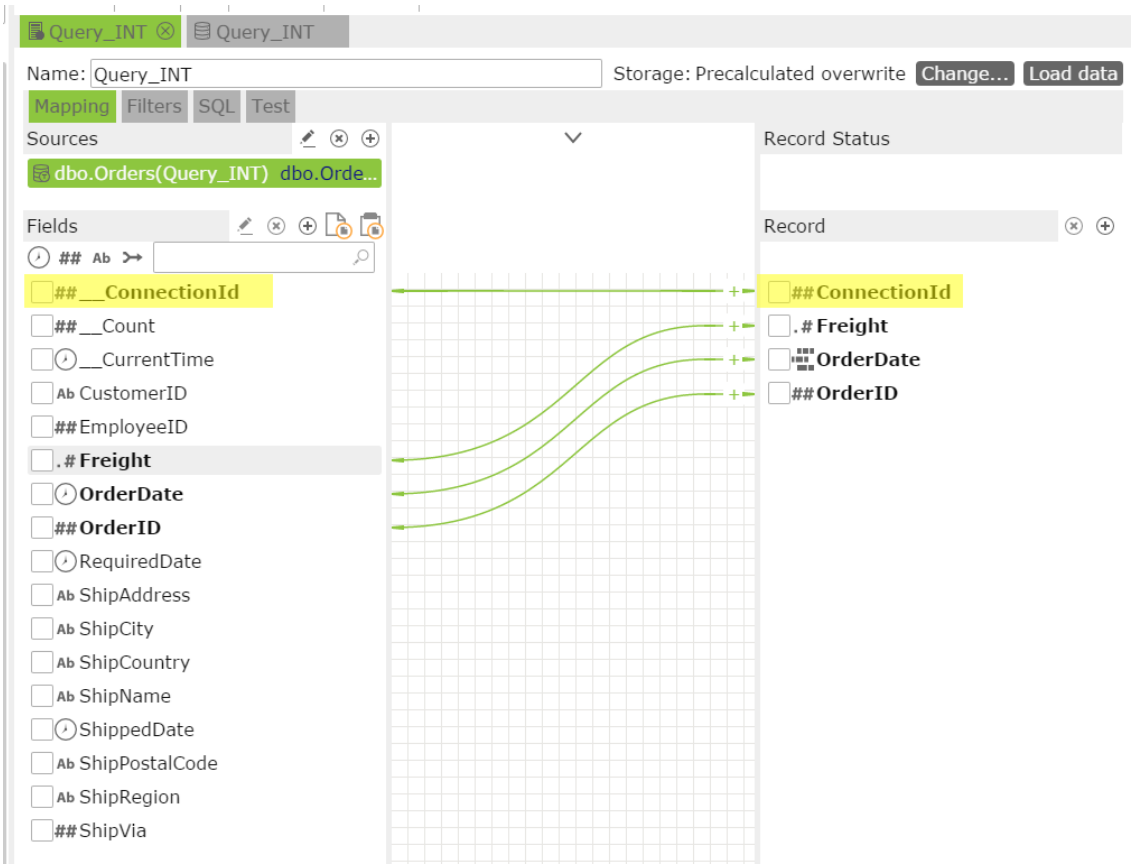
The **Key Query** has two parameters:

- Key type: None, Constant, or Query
- Key return type: String or Integer

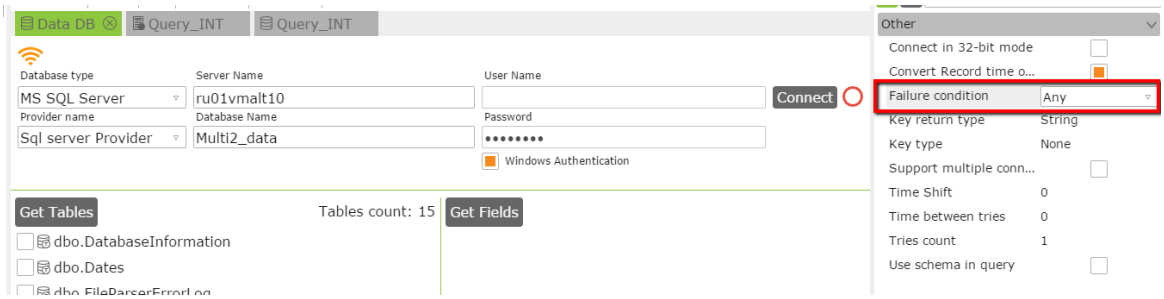
1. Use the **Key Query** string to identify the connection source, which is added to the data during the data load.



2. If the **Key type** is *Constant* or *Query*, then **Connection_Id** field appears in the Metric or Record. This field must be mapped in the Record/Metric for multiple connections to work correctly.



3. For the **Failure condition** parameter, select one of the following options from the list:
   - Any: If any of the multiple connections fails, all data loaded is considered as failed.
   - All: If all connections fail, then all data loaded is considered as failed. If only one connection fails, the others are loaded anyway.


Data DB
Query_INT
Query_INT
Database type
MS SQL Server
Server Name
ru01vmalt10
User Name
Connect
Provider name
Sql server Provider
Database Name
Multi2_data
Password
Windows Authentication
Get Tables
Tables count: 15
Get Fields
dbo.DatabaseInformation
dbo.Dates
Other
Connect in 32-bit mode
Convert Record time o...
Failure condition
Any
Key return type
String
Key type
None
Support multiple conn...
Time Shift
0
Time between tries
0
Tries count
1
Use schema in query

Chapter 3

Administration Settings

Admin Dashboard

The **Admin Dashboard** lists information about the current activity and access rights.

Activity

- Current sessions
- Projects (list of projects sorted by time, since the last activity from a Viewer)
- Total Insight Project Database size
- Admin Console Database size

View access rights

- By project: View access rights per project per role.
- By data source name: View the access rights per data source per role.

1. Double-click the project or data source name to view the access rights.

   The Project Details dialog box appears and lists the project name, DataMart data source, and database details.

   Details include the project and database names, data sources, records, metrics, and views.
2. Select one of the following options:
   - Data sources
   - Records
   - Metrics
   - Views

Projects

A project is a set of objects (documents) containing metadata and data related to data sources, metrics, records, the Insight DataMart and dashboards.

You can create a project in Admin Console and specify the databases to be used, and then add and modify the project in Studio.

Use the **Projects** pane to manage projects. You can also create new projects and access existing projects in this pane.

Create a new project

1. In **Admin Console**, in the **DocumentsTree,** right-click **Projects** and click **New**.
2. Enter a name for the new project and click **OK**.
3. Select an option for the project.
    1. **Create blank project**: Creates a new blank project.
    2. **Add Existing**: Adds an existing project to your current version of Insight.
    3. **Import from file**: Imports a project from a file.
       This file is a previously exported Insight project file (from Studio) in ZIP format (do not extract the project file). If importing from a file, select the file to import.

       Note You can import an Analytics project file (such as **KAFTA.zip** or **KAFC.zip**) here. See Create a solution in Studio to import.

       When creating a new project, we recommend that the Meta database be named as <ProjectName>_meta (without any spaces) and the Data database as <ProjectName>_data (again, without spaces), such as **Test_meta** and **Test_data.**
    4. Use the **Same server as the meta database** check box to copy the same server connection credentials (server name, User name and password) to the Data database section.

       Note You cannot connect to these databases until the tables are created. Tables are created when you save the project.

    5. To use a staging database, select **Staging DB** and fill in the information. Optional.
4. Click **OK**.
   The databases are created.

View and edit projects

You can edit the data source for a project for the cases when the server name, database name, or credentials change.

1. In the **Admin Console**, click **Projects**.
2. Click the name of the data source.
   A window with the basic data source information appears.
3. View data source information, or edit the data to change.
4. On the **Actions** toolbar, click **Save** .

Note Switch between projects by selecting **Documents Tree** > **Projects** > **<Project name>**.

Users

On the **Users** panel, define and configure users and user roles.

Work with users

Use this procedure to define and edit users, and associate a user with one ore more roles.

1. In the **Admin Console**, select **Documents Tree** > **Users**.
   All users currently established within the system are listed.
2. Click a user name to view related information.
   The User Details pane appears.
3. Edit the user information, as applicable.
   You can change login information, including user names and passwords. You can also specify the frequency of password changes and set or clear administrator rights for a user.

Add a user

1. In the **Admin Console**, on the **Documents Tree**, right-click **Users** and click **New**.
2. Enter a name for the new user and click **OK**.
3. Complete the user details such as **Login**, **User name**, **Email**, **Password**, and password policies.
4. Select **Enforce password policy** to enable the password strength check.
   In this case, the password must comply with the following rules:
   - Contain at least 8 characters
   - Contain at least one alpha character (a-z; A-Z)
   - Contain at least one numeric character (0-9)
   - Contain at least one special character. Example: @&%"

Define user mapping

On the **User mapping** tab, you can assign an identifier to a user, or set preferences related to the user name or email settings.

1. In the **Admin Console**, click **User mapping**.
   The User Identifier (UID) tab appears.
2. Specify a way to get the user's identifier.
   This identifier should be constant for a specific user login. Typically, this identifier is a session property such as an identify that looks to the Active Directory domain/user.name.

   Note **User Name** and **Email** fields are not mandatory.

3. On the **User Name** tab, define the display name for a user account.

This is typically one of the Active Directory properties such as *Identity*, *FullName*, *display/Name*, or other convenient property.

4. On the **Email** tab, define the email address for the user account.
   This is typically one of the Active Directory properties such as *EmailAddress*.

Roles

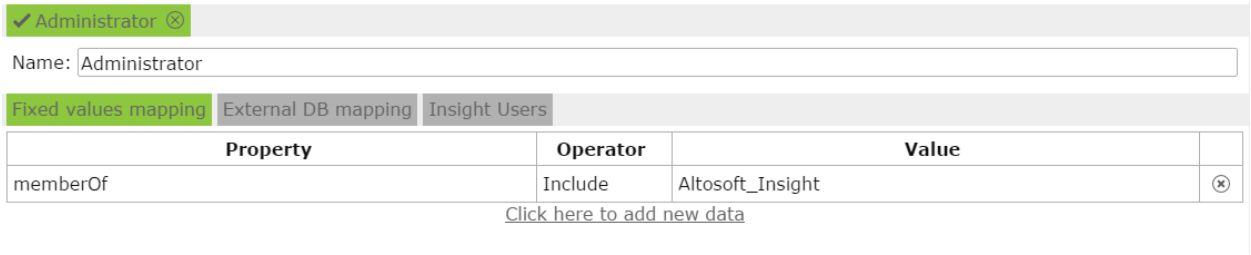
Use Roles to set and adjust the specific roles for each user, including access, editing abilities, default views, themes and styling, and functionality.

Default Administrator role

When you create an Administrative database, an Administrator user and Administrator role are created automatically. The default Administrator role is automatically assigned to the Administrator user.

The Administrator role gives the access rights to all the Insight applications (Studio, Data Loader, Themes and Formats), along with projects, data sources and project documents (metrics, records, translation tables, Views, reports, and more).

To open the Administrator role, select **Admin Console** > **Documents Tree,** expand **Roles**, and then click **Administrator**. This is the default Administrator role.



Create an Administrator role

You can create multiple Administrator roles.

1. In Admin Console, select **Documents Tree** > **Roles**.
2. Right-click **Roles** and select **New administrator role**.
   The "New Administrator role" dialog box appears.
3. Type a name for the new role and click **OK**.
   The "Administrator role" settings appear in the right pane.
4. Set the reference of the following tab, depending on the authentication method to use for this role. See the Authentication section.
   - Fixed values mapping

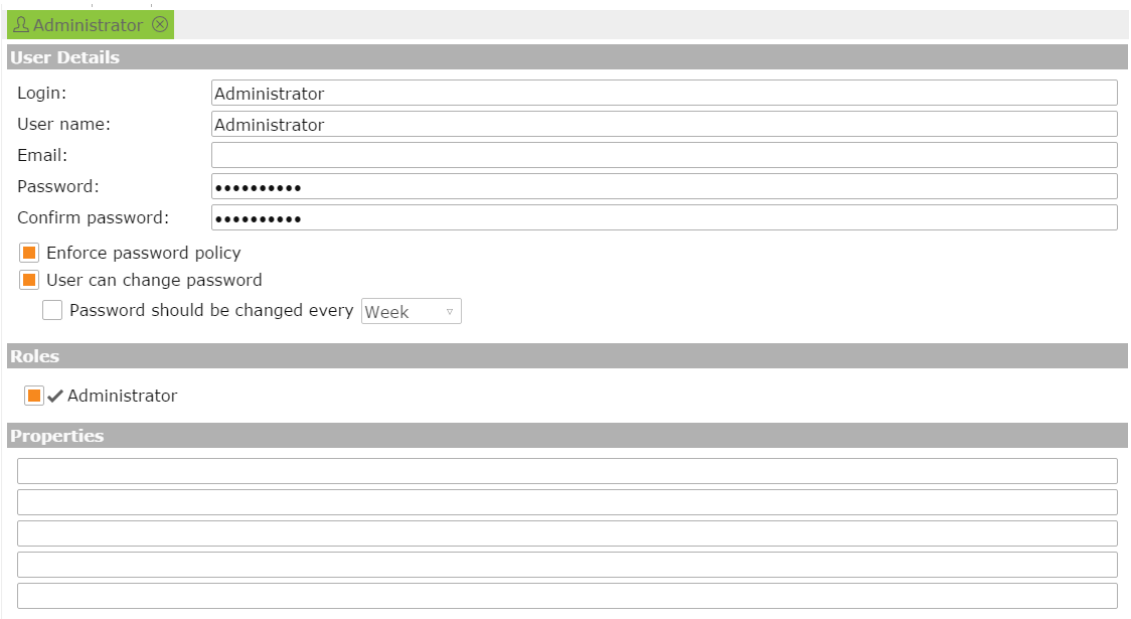
- External DB mapping
- Insight Users

5. On the **Actions** toolbar, click **Save**.
   The new Administrator role is created.

Assign an Administrator role to the user

After the Administrator role is created (either by you or by the default fole), you can assign it to a user.

1. Select **Admin Console** > **Documents Tree** > **Users**.
2. Select the user to be assigned an Administrator role.
3. In the right pane, in the **Roles** section, select the **Administrator** check box.



Note If the user is not assigned an Administrator role, the rights associated with the default role are granted.

4. On the **Actions** toolbar, click **Save**.

Non-Admin role

1. In the **Documents Tree**, right-click **Roles** and click **New user role**.
   The New Role window appears.
2. Type a name for the new role and click **OK**.
   The Role settings appear in the right pane.
3. Define a **Theme** and **Tablet Theme** for the role. Select a theme from the list.

4. In the **Application rights** tab, select which Insight components to access from this role. Options include **Admin Console**, **Themes and Formats**, **Data Loader**, and **Studio**.
5. In the **View Rights** tab, select which project and which portion of each project to be viewable by this role.

   Click each project to expand each into subparts.
6. In the **Studio rights** tab, select editing options to allow.

   If **View rights** is the only option selected for the documents (records, metrics, views, execution plans, or other), the user is only allowed to view the document. If you select **Studio rights**, the user can view and change the document.
7. Select options on the **Themes** tab to allow or restrict themes for the user.
8. Use the **Fixed values mapping** tab to define mapping rules for each role. This is typically the Active Directory *memberOf* property.

   Each row in the mapping grid uses the AND operand. If more than one role listed matches conditions for a user account, the access rights are merged from all matching roles, while other settings (theme, date format, etc.) are assigned by the top matching role in the list.
9. Use the **External DB mapping** tab to map a database type to the role. See Authentication for details.
10. Select **Source** to select a source database.
11. In the **Insight Users** tab, click **Administrator** to define this user as an administrator.
12. Select options on the **Markers** tab to allow full customization of the role by creating markers throughout Insight. See Markers.

Markers

You can tag data by adding markers. Set on data points, markers allow a data point to be tagged and dragged, for the purpose of sharing analytics with other users across various pages, charts, and grids.

Typically, an annotation is set for a data point, but a marker can also launch a new View or a link to an external website.

A marker can have three levels of visibility with different types. These parameters are set for the roles overall and can be changed for a particular marker in the Viewer, but only within the limits defined by a role. For example, if a role restricts markers to either "Info" or "Alert," in the Viewer you can only use these two types (and not the "Issue" type).

You can also disable the function of creating markers for a role or define the lowest level of marker importance to be visible for the user within a role.

1. Navigate to **Admin Console** > **Roles**, select the required role, and select the **Markers** tab.
2. Select the **Can create markers** check box to enable "Markers" functionality.
3. Select **Roll up markers** if you want the markers to be visible only if the marker filters fully intersect with element filters. On the list, select the lowest level of marker importance that will be available to the role:
   - High
   - Low

- Medium

For example, if you select "Medium," the user assigned to this role can only see markers of Medium and High level importance on the dashboard.

4. Select the marker types available for the role.
   - Info
   - Issue
   - Alert
5. Select the marker visibility levels available for the role.
   - Personal
   - Selected
   - Public
6. On the **Actions** toolbar, click save .

Calendars

Use the Calendars functionality to customize the format for work days and times, which allows for accurate data time tracking for your organization. For example, if a mortgage was submitted by 4 pm on Friday and approved by 10 am on Monday, weekend hours are typically excluded (not tracked). For example, in a 9 to 5 work day with weekend hours excluded, the duration from submission to approval would typically be two hours (rather than 50 hours).

A calendar defines business hours for any given day.

1. Main schedule: Start and end time for each day of the week

   Example

   S: 10-2, M: 9-5, T: 9-5, W: 9-5, T: 9-5, F: 9-5, S: 10-3
2. Day-specific exceptions

   Examples

   1/1/2016 - Closed

   5/27/2016 - Closed

   7/3/2016 - 9-12

   7/4/2016 - Closed

   12/25/2016 - Closed
3. Temporary overwrite: List of temporary schedule overwrites. Each item in the list is a separate schedule, such as, #1 plus Start and End date.

   Examples

   Acton Memorial Library Calendar

   5/28/2017 - 9/08/2017

   S: Closed, M: 9-12, T: 9-12, W: 9-5, T: 9-12, F: 12, S: 10-12

Add a calendar

1. In the **Admin Console**, right-click **Calendars** and click **New**.
2. Enter a name for the calendar and click **OK**.
   The **Main schedule** window appears.
3. Define the main schedule for the calendar. and save the changes.
4. On the **Actions** toolbar, click **Save** .

Edit a calendar

1. In the **Admin Console**, click **Calendars** and click the name of the calendar to edit.
2. Make modifications to the calendar and click **Save**.

Define calendar exceptions

You can define exceptions for a calendar to exclude time calculations such as holidays or weekends.

1. In the **Admin Console**, on the **Documents Tree**, click **Calendars**.
2. Select the calendar to define an exception.
3. Select **Exceptions**, and click **Add** .
   The "Define exception" window appears.
4. Enter the **Date** and **Hours** for the exception, and click **OK**.
   The exception appears in the exception list.
5. Click **Delete** to delete a schedule exception.
6. Click **Edit** to make modifications to a schedule exception.
7. Save your changes.

Map-Aggregate

Use the Map-Aggregate profiler to generate a recommended manifest. This is a set of plans used for the Map-Aggregate based on database readers to request profiling of how your data is being used.

Before you use the profiler to recommend a plan, you must do the following:

1. Ensure that you have one or more nodes defined and running. Please see the *Kofax Insight Installation Guide* to install map aggregate nodes (by default, they are not installed).
2. Define one or more nodes in **Admin Console**.
3. Test the node connection.

Create a manifest

Use a manifest to define the memory node (Server) for your data. A manifiest is a list of all objects (with descriptions) that need to be downloaded to nodes. The map aggregation cannot function without a manifest. It sends information to the master node about which objects are present on a specific node. Also, it specifies the objects to be downloaded to nodes.

Note This functionality is only used if you have installed a node server.

Using the Insight **Map-Aggregate**, you can add and configure multiple node servers and specify which data to load into the memory of a node server. For more information on how to install a **Node Server**, see the *Kofax Insight Installation Guide*.

1. In Admin Console, on the Documents Tree, select **Map-Aggregate** > **Manifests**, and then right-click and select **New**.
2. Assign a unique descriptive name to the manifest, and click **OK**.
   The new manifest appears in the list under the **Manifests**. The default manifest is displayed in bold.
   If you have several manifests, set any of them as the default by right-clicking and selecting **Set default manifest**. Only one manifest can be active at a given time.

Create a plan

You need to create a plan or plans to be downloaded to nodes.

1. Right-click the new manifest and select **New Plan**.
   Name the plan and click **OK**.
2. On the plan editing window, for the **Object** field, select the required document.

   Note If you select a metric to be processed on nodes, verify that it has the Precalculated overwrite type of storage. See the *Kofax Insight Studio Help*.

3. Set the time frame for the aggregation to process a particular time interval of the data, if required.
4. Set **Frequency**. It defines how the data is grouped on the node. For example, to reload data on top of already existing data, the data is overwritten for one month if the frequency is set to *Months*. The frequency depends on the load of data that arrives daily, monthly, etc.
   We recommend setting this parameter according to the amount of your data:
   - Seconds: A hundred thousand rows of data or more per second.
   - Minutes: A hundred thousand rows of data or more per minute.
   - Hours: A hundred thousand rows of data or more per hour.
   - Days: A hundred thousand rows of data or more per day.
   - Months: A hundred thousand rows of data or more per month.

   Currently there is a constant value of 1,000,000 lines in the database related to the data. If your metric has 50 dimensions and you decide to assign only three of them to the node, the number of lines after aggregation is taken into consideration.

For example, suppose you set frequency to *Months*. In this case, a data array of 1 000 0000 is allocated for one month on the node. It is expected that this size will never be exceeded during the given period of one month. If it exceeds this number, a new array is created with the size of a double constant (2 000 000), old data is copied to this new array, and new data is downloaded. Such an operation demands an extra memory allocation and extra time to organize this memory and copy the data. If it becomes impossible to allocate the required memory, the node becomes non-working.

For example, if you download the data on USA on one node and set the frequency to *Months*, the other node contains all other data without any country filters. In the latter case, the amount of data is bigger and we recommend setting the interval to *Days*.

5. Set the **Indexing depth**.

   Use this setting to define how fast an element can be found by filters. To quickly find elements, we recommend indexing them. This parameter defines how far the indexing goes down the list of selected dimensions (the order of the dimensions in this list is important). The bigger the value is on the list, the more memory is used for storing the indexes and the more time is spent by the system while uploading new data. Filtration of dimensions is faster for items that are higher on the list.

   For example, suppose the parameter is set as Country = USA. If we don't have an index for the Country dimension, we should sort the data and find all strings where the country dimension is set to USA. If we set the index for this dimension, sorting is simplified to find this index, without sorting out all the existing strings.

   The user defines which dimensions are stored in a plan (by selecting/unselecting the check box on the right). The user can also change the order by dragging a dimension to another position.

   For example, suppose the plan has the following dimensions selected:

   1. Employee
   2. Customer
   3. Country
   4. City

   If we set Indexing depth to "3," then only the first three dimensions are indexed (Employee, Customer, and Country) and if the Indexing depth = 1, only the first dimension (Employee) is indexed.

   The order of dimensions influences the search speed. The index in the plan can be considered as data sorting among the indexed fields. For example, we have a plan with the indexing depth = 2 and the following data:

	Employee	Customer	Country	City
1	1	A	USA	New York
2	1	B	France	Paris
3	2	A	USA	Los Angeles
4	3	B	United Kingdom	London
5	3	C	Germany	Berlin

   In this case, the indexing is run in the following way.

The data is sorted at each level, which allows the required values to be found quickly. For instance, for Employee we can quickly define the numbers for the required lines 1 and 2. If the filer is set for the Customer, then it is necessary to check each Employee and find the needed Customer to get the string number. For the Customer B, we find string#2 under Employee 1 and string#4 under Employee 3.

6. Use the **Values** tab to select which values to download for the dimension. Select all those that apply and click **OK**; or select the **Exclude** check box to exclude the selected values from the download.

Define node optimization plan

It is essential to run a node optimization plan, which optimizes the memory use in the node.

1. Open **Map-Aggregate**, and click **Node optimization plan**.
2. In the **Node optimization plan** pane, in the **Type** field, select **Analyze manifest** from the list.
3. In the **Project** field, select a project, and then select the **Objects**.

   Note Select the same project that contains Object Plans for the documents included in the Manifest. Object Plans are rules for storing and processing data on nodes.

   Items selected in the **Documents Tree** appear in the plan list.
4. Click **Analyze** to run the manifest analysis for the project.
5. Save the **Node optimization plan**.

Use the profiler

1. In **Admin Console**, click **Map-Aggregate** > **Manifests**, and click **Profiler**.

   Once started, the profiler begins to analyze the data usage from the dashboards (Views).
2. In the **Client requests** window, notice that the **Requests #** increases.
3. Allow the profiler to run during a time when you have the optimal amount of users, such as two weeks.
4. Click **Stop** to end the profiling session.

Options

Use Options on the Documents Tree to configure settings related to email notifications, localization, high availability, and more.

Configure email settings

Use Email settings to set the email server configuration required to support sending email notifications. You can define alerts by a dashboard user. An email is sent to the dashboard user when the specified conditions are met.

You can configure an SMTP server to send emails because Insight has no predefined mail server.

1. In **Admin Console**, select **Options**.
   The **Options** editor appears.
2. In the **Email settings** section, select options such as **Enable SSL**, **Use authentication**, and **Send email at alert**.

   Note Select **Use authentication** if your email server requires authentication for connecting and sending emails.
3. Complete the data fields with the information for the email server you want Insight to use to send emails.
4. Fill in the **User** and **Password** information used for authentication.
5. Enter the email address for **Administrator email**.
   In the Insight dashboard tool, alerts can be sent to different people via email. When people reply to an alert email, those replies will be sent to the administrator email address.
6. Enter the email address for **License notification email**.
7. Enter the URL for **Viewer URL**.
8. Click **Send test** to ensure your settings are correct before saving your email settings.

Create filter groups

Use filter Groups in the View (dashboard) to filter a component you want to broadcast to a group, and apply the filter to the component that will listen to a group.

1. In the **Admin Console**, on the **Documents Tree,** click **Filter Groups**.
2. Select **Click here to add new data**.
3. Select the **Local** check box to only allow the filter group within one View.
   Clear the Local check box to allow Global access to the filter group. When the Local box is cleared, it is available for any Insight view.
4. To use these groups in a component, open the component **Data Wizard** and select **Action**.
5. In **Incoming Actions**, select the filter group this component will listen to.
6. In **Outgoing Actions**, specify the filter group to which the component will broadcast.

   Note You must select **Use the value of the dimension as filter** before specifying the filter group.

Logs

You can view and adjust log levels and in **Logs** window.

1. In **Admin Console**, on the Documents Tree, click **Logs**.
   The Logs window appears.
2. In the **Log level** section, check the options to log. Options include **Login/Logout activity** and **Open view, Print view, Print report, Export to Excel**.
3. In the **Statistics** section, you can include the number of records in the log, and select the first and last records.
4. In the **Cleanup** section, set a date and time to Permanently remove records from the log. Records older than this date are purged from the logs.
5. Click **Delete**.

Define custom SQL functions

Define a custom SQL function to execute on a specific database type, such as SQL Server, Oracle, or MySQL if there is no appropriate Insight logarithm function. The function may also be common to all databases.

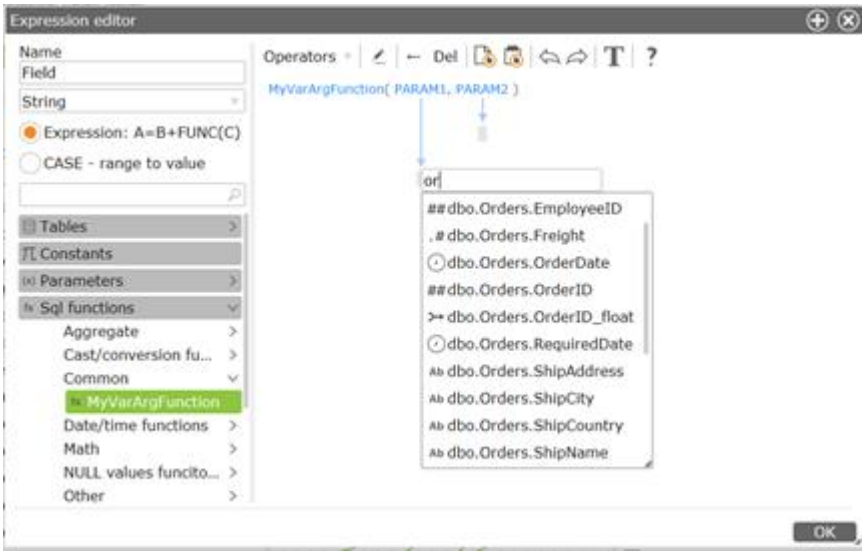
The custom SQL function can then be used in a derived field in a metric or record.

1. In Admin Console, on the Documents Tree, right-click **SQL Functions** and click **New**.
   The **New SQL Functions** window appears.
2. In the **Name** field, enter a name for the SQL function and click **OK**.
   The SQL Function editor appears.
3. Complete the following details:
   - **Name**: Name of the SQL function.
   - **Function Type**: Standard or Aggregate.
   - **Category**: Assign a category to this function so that it will be listed and saved under the category group. To use this function, it must be retrieved from this group in the expression editor.
   - **Variable number of arguments**: Select this option if the function accepts a variable number of arguments.
   - **Parameters**: List the input parameters to this function. The format is comma delimited without spaces. If the function accepts a variable number of arguments, enter "ListItem..."
   - **Description**: The function description.
   - **DB Type**: Use "Default DBMS Template" if you would like this function to work across all databases; otherwise, pick a specific database type and the function will only appear if the record or matrix fields are from the specific database type.
   - **Representation**: Use this space to enter the formula for the SQL function.
4. To use these functions, go to Studio and open a metric or record.
   You can now, for example, create a derived field.

5. In the **SQL Functions** section, select **Common**. Next, click and drag the function to the editor.

   Note You can also use smart input in the field. Type something in the field. The system will prompt you with the possible variants.

6. In the **Expression editor**, enter the number of parameters for the expression and click **OK**.
   The function appears in the expression editor. You can use this function to define the field.



Customize report distribution

Use the Distribution option to customize reports and alerts. You can allow or deny sending reports (defined in Studio) specify the conditions for sending.

Define report distribution options

1. In Admin Console, on the Documents Tree, click **Distribution**.
2. In the **Report distribution options** pane, define the following options:
   - Maximum number of simultaneously generated reports.
   - Reports saving path.
   - Reports distribution projects. This is which projects have reports generated according to this interval.

Define alert distribution options

1. In **Admin Console**, click **Distribution**.
2. In the **Alerts distribution option** pane, define the following options:
   - Alerts distribution interval
   - Alerts distribution projects. This is which projects the alerts are distributed.

Alerts

This section in Admin Console displays all the alerts defined in Insight Studio.

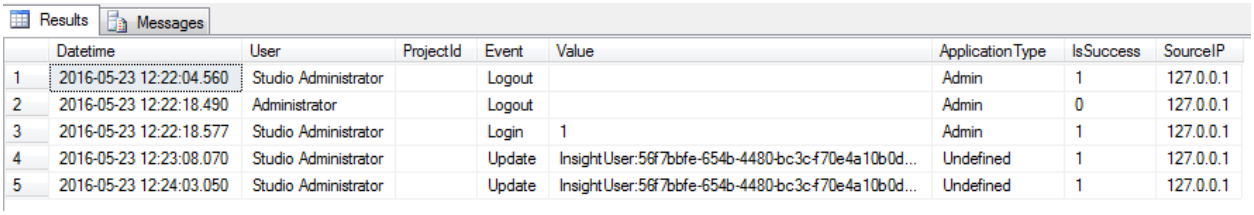
1. In **Admin Console**, in the **Documents Tree,** click **Alerts**.
2. View **Alerts**.
   Alerts can be defined based on a **Record**, **Metric** or a **Process**. Alerts are defined in Studio in the **View in Alerts** grid.

Security event logs

Insight generates and stores the following security events in the Admin database:

- User's successful login
- User's attempt to log in with incorrect credentials
- User's logout
- Adding/updating/deleting roles in Admin Console
- Adding/updating/deleting users in Admin Console
- Changing the expired password for the user

To view these logs, on the SQL server, navigate to the dbo.INSIGHTLOG table in the Administration database.



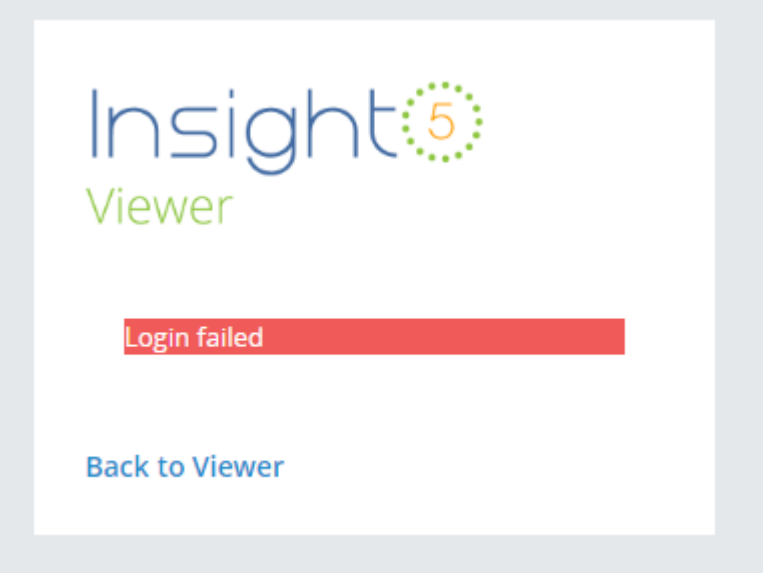
Results | Messages

	Datetime	User	ProjectId	Event	Value	ApplicationType	IsSuccess	SourceIP
1	2016-05-23 12:22:04.560	Studio Administrator		Logout		Admin	1	127.0.0.1
2	2016-05-23 12:22:18.490	Administrator		Logout		Admin	0	127.0.0.1
3	2016-05-23 12:22:18.577	Studio Administrator		Login	1	Admin	1	127.0.0.1
4	2016-05-23 12:23:08.070	Studio Administrator		Update	InsightUser:56f7bbfe-654b-4480-bc3c-f70e4a10b0d...	Undefined	1	127.0.0.1
5	2016-05-23 12:24:03.050	Studio Administrator		Update	InsightUser:56f7bbfe-654b-4480-bc3c-f70e4a10b0d...	Undefined	1	127.0.0.1

Customize return page for the Viewer

You can customize the page where the user returns in case of a login error from the Viewer. For example, this may be necessary if application access is denied due to incorrect login parameters. By default, the user is redirected at `http://<servername>/Insight/view/Default.aspx`. To change this link, use the following procedure.

1. Navigate to **web.config** file at `C:\Program Files\Kofax\Insight 5.4.0\HtmlInsight\View`.
2. Add `<add key="BackToURL" value="<website address>"/>` where <value> is a link to any custom page. Save the file.
   The next time the user gets a "Login failed" message, clicking the **Back to Viewer** link redirects the browser to the link specified above.



Note If you reinstall Insight, the preceding steps must be repeated.

Chapter 4

Import or export Insight projects and settings

You can use Admin Console to import or export Insight projects and settings, or you can use one of the following import methods:

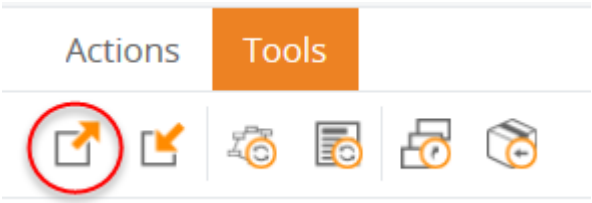
- Command prompt
- Batch file

You can import or export data from Kofax Analytics for TotalAgility, Kofax Analytics for Capture, or other Kofax Analytics applications; you can also selectively import or export Admin Console settings (related to users, authentication, user filters, and others) to an XML file.

Export project settings

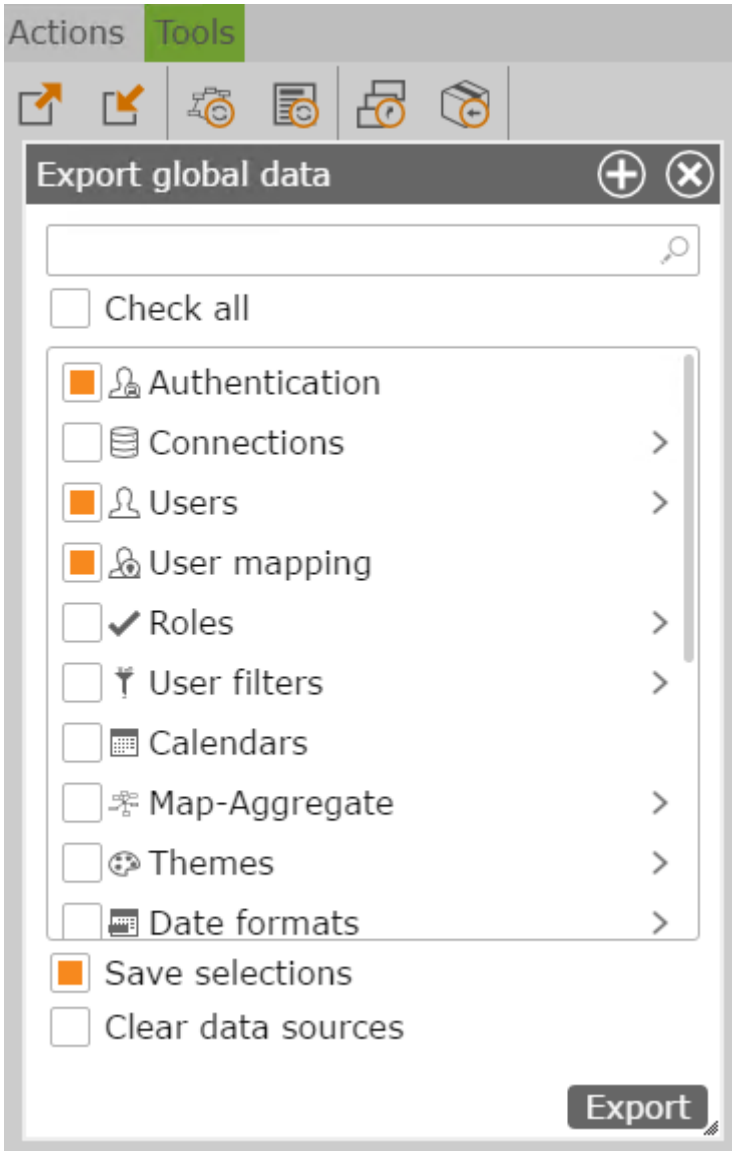
Use this option to export Admin Console project settings in an XML file format.

1. Navigate to **Admin Console** > **Tools** > **Export**.



The "Export global data" window appears.

2. Select the Admin Console documents to export, or select the **Check all** check box to select all of them, and then click **Export**.



Note Select the **Clear data sources** check box to exclude the paths to the data sources from the exported file. When the user imports this project, the data sources must be specified.

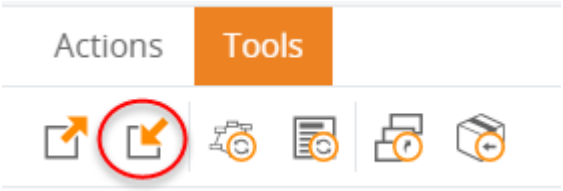
Note If you select the **Save selections** check box, the selected documents are overwritten if the import is performed using a Command Prompt window. See Overwrite saved selections. If the import is performed through the Insight interface or a batch file, the check box has no effect.

3. Click **OK** to clear the message confirming successful data export.
An XML file is downloaded with the file name **ExportAdminDatabase.xml**. The file is saved to the default download directory for your browser.

Import project settings

Use this procedure to import Admin Console settings (such as Roles, Users, Connection, and others). See Export Project Settings for the information on how to create the AdminSettings.xml file.

1. Navigate to **Admin Console** > **Tools**, and click **Import** .



2. Select the **AdminSettings.xml** file to import.
   The "Importing global data <file name>" window appears.
3. Select the documents to import.
4. Select **Overwrite** or **Preserve existing** and click **Import**.
   With **Overwrite**, the imported files overwrite any existing files with the same name. With **Preserve existing**, existing file names are preserved and the imported files have numbers appended to them.
5. Click **Yes** when prompted to refresh the page.

Import a solution

Use this option to import a solution from Kofax Analytics for Capture, Kofax Analytics for TotalAgility, or other Kofax Analytics product. A solution contains a project file (ZIP file) from Insight Studio and Admin Console settings (XML file) packed into a single ZIP file.

You can also use a command promptto import a solution.

1. Navigate to **Admin Console** > **Tools**, and click **Import solution**.
   Import a Kofax Analytics Project window appears.
2. Click the ellipsis button for the **Select a Kofax Analytics Project file** tab and select the location of the ZIP file (solution).

   Important Do not unzip the bundle.

3. Select a project where the solution will be imported to or click **Create new project**.
   If required, create a new project and save it.
4. Click **Import**.
5. When the import is complete:
   - Click **OK** to clear the message confirming successful data import.

- Click **Yes** when prompted to refresh the page.

Import or export via command prompt

Import or export Admin Console settings via command prompt

You can import or export all Admin Console settings, such as authentication type, users, user role settings, user filters separately from the project. You can also import or export from a command prompt.

1. Open a Command Prompt window.
2. At the command prompt, open the directory: `C:\Program Files\Kofax\Insight 5.X.X \ImportExport`.
3. Open Help where all the commands are listed:

   ```
   Altosoft.Insight.ImportExport.EntryPoint.exe -h
   ```

4. Execute the following:
   1. Export Admin Console settings:

      ```
      Altosoft.Insight.ImportExport.EntryPoint.exe -export -Admin -path="C:\Temp\ImportExports \FILENAME.xml"
      ```

      Change the path and file name.
   2. Import Admin Console settings:

      ```
      Altosoft.Insight.ImportExport.EntryPoint.exe -import -Admin -path="C:\Temp\ImportExports \FILENAME.xml"
      ```

      Change the path and file name.

Import solution via command prompt

Use this option to import a solution from Kofax Analytics for Capture, Kofax Analytics for TotalAgility, or other Kofax Analytics product. A solution contains a project file (ZIP file) from Insight Studio and Admin Console settings (XML file) packed into a single ZIP file.

1. Open a Command Prompt window.
2. Navigate to the `ImportExport` directory: `C:\Program Files\Kofax\Insight 5.X.X \ImportExport`.
3. Open Help where all the commands are listed:

   ```
   Altosoft.Insight.ImportExport.EntryPoint.exe -h
   ```

4. Execute the following:
   1. Import the bundle to a new project (it will be created during import execution):

      ```
      Altosoft.Insight.ImportExport.EntryPoint.exe -import -projectName="TestBundle1" -
      bundlePath="C:\temp\ImportExports\TestBundle.zip" -metaConnection="Data Source=<server
       name>;Initial Catalog= TestBundle1_meta; User Id=<User ID>;Password=<password>;" -
      metaProvider="sql" -metaDbType="MS SQL Server" -dataConnection="Data Source=<server
      ```

```
 name>;Initial Catalog= TestBundle1_data; User Id=<user ID>;Password=<password>;" -
dataProvider="sql" -dataDbType="MS SQL Server"
```

Change the file name and path, and also specify data and meta database names, along with the server name and associated connection strings.

2. Import the solution to an existing project (already created in Insight, see Create a new project):

```
Altosoft.Insight.ImportExport.EntryPoint.exe -import -projectName="TestBundle" -
bundlePath="C:\temp\ImportExports\TestBundle.zip"
```

Change the file name and path for the bundle.

5. After the import is complete, check your project data in Admin Console or Studio.

Import or export a database via command prompt

Import a database

You can import a database through a command prompt.

1. Create an empty database on the SQL server.
2. Execute the following:

```
Altosoft.Insight.ImportExport.EntryPoint.exe
-import -path="C:\ImportExport\ExportDB_TestBundle_data"
-connection="Data Source=<server name>;Initial Catalog=ImportDBtest;
User Id=<User ID>;Password=<password>;" -provider="sql" -dbType="MS SQL
Server"
```

3. Define the connection strings.

Note In the sample above, the command is shown for MS SQL Server. Define the user name, password, database provider, and database.

4. Execute the command.
The new database contains the imported data.

Export a database

You can export a database through a command prompt.

1. Create a folder, where the database will be exported.
2. Open Help to list all available commands:
Altosoft.Insight.ImportExport.EntryPoint.exe -h
3. Execute the following:

```
 Altosoft.Insight.ImportExport.EntryPoint.exe
-export -path="C:\ImportExport\ExportDB_TestBundle_data"
-connection="Data Source=<server name>;Initial
Catalog=TestBundle_data; User Id=<User ID>;Password=<password>;" -provider="sql"
-dbType="MS SQL Server"
```

4. Define the connection strings.

Note In the sample above the command is shown for the MS SQL server. Define user name, password, database provider and database.

All the data is exported to the specified directory in XML files.

Overwrite saved selections

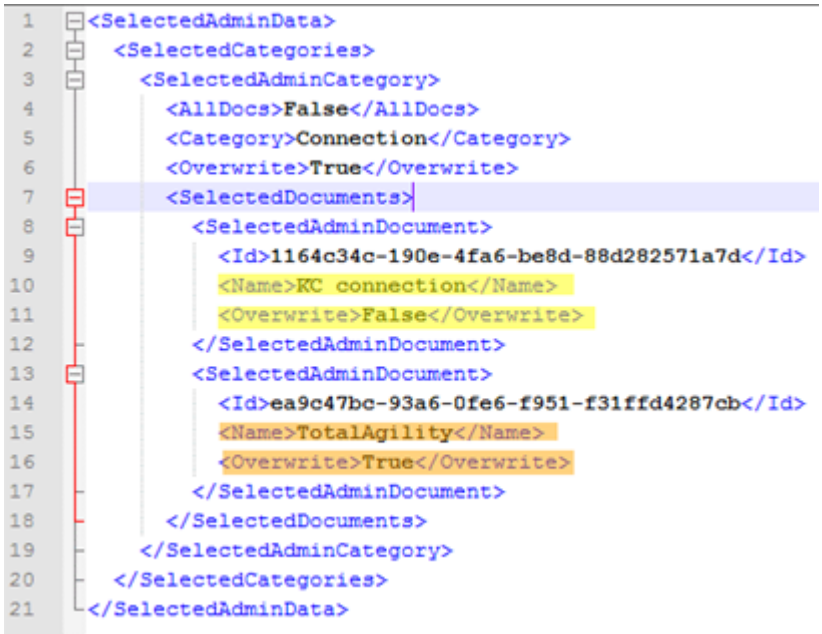
The Import/Export command line utility can be parameterized by an XML configuration file. This file may contain any number of documents or whole sections you want to import.

You can also pass a separate configuration file that contains data source connection properties for the update of data sources in the Insight project after it is imported.

When you export data, it is possible to filter out unnecessary settings.

Create a configuration file

1. Navigate to **Admin Console** > **Tools** > **Export**.
   Export global data window appears.
2. Select all the Admin Console documents as you need to export or select **Check all** check box.
3. Select **Save selections**, and click **Export**.
4. Click **OK** to clear the confirmation window.
5. Open the exported **SelectedAdminDocuments.xml** file, use `True` or `False` to indicate which documents are overwritten during import of settings. A value of `True` means that a document is overwritten; a value of `False` means that a document is not overwritten during import of settings.



6. To import selected documents via the command prompt, you must have the following:
   - **AdminDocuments.xml** (lists all exported documents)
   - **SelectedAdminDocuments.xml** (lists only selected documents)
7. Execute the following:

   Note Make sure all paths are valid XML files.

   ```
   Altosoft.Insight.ImportExport.EntryPoint.exe
   -import -Admin
   -selectedAdminDocuments="C:\Temp\SelectedAdmin Documents1.xml"
   -path="C:\Temp\ExportAdmin
   ConsoleDatabases\ExportAdminDatabase1.xml"
   ```

   Where `-selectedAdminDocuments` specifies the path to the **SelectedAdminDocuments.xml** file and `-path` specifies the path to the **AdminDocuments.xml** file.

Import or export an Analytics project

You can import projects into Kofax Insight from Kofax Analytics for TotalAgility or Kofax Analytics for Capture, and export Admin Console settings to an XML file.

The import or export command line method can be parameterized by an XML configuration file. This file may contain any number of documents or sections that the user wants to import. To generate the configuration file, select **Save selections** and click **Export** during project export through the Admin Console. See ???.

You can also pass a separate configuration file that contains data source connection properties for the update of data sources in the Insight project after it is imported.

Import or export using a batch file

You can modify a batch file to import or export the data.

1. Create a batch file or open an existing file.
   1. To create a new batch file, create a TXT file that includes the code.
   2. Change the file extension to .bat.
   3. Run the file with Windows administrator rights.
2. To export project with data, add the following command after changing the file name and path:
   `Altosoft.Insight.ImportExport.EntryPoint.exe -export - projectName="PROJECT PATH \PROJECT_NAME" –data`.
3. To export project without data, add the following command after changing the file name and path:
   `Altosoft.Insight.ImportExport.EntryPoint.exe -export - projectName="PROJECT PATH \PROJECT_NAME"`.
4. Save and execute the batch file with Administrator rights.
   The data is imported/exported accordingly.

Note The file may contain other commands, depending on the scenario. For example, the commands may be used for Insight installation, solution import, Admin settings import, connection strings, or data source updates. See Import or export via command prompt.

Chapter 5

Recover from a lockout

A lockout may occur in the event that the administrator configures Windows authentication for Insight applications (Admin 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 `Program Files\Kofax\Insight\HtmlInsight\Admin`.
2. Verify that the key `PreventConfigChange` 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 `Program Files\Kofax\Insight\HtmlInsight\Admin`.
2. Verify that `<add key="Insight.DataService.TryInsightUsers` 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 A

Import-Export Tool

Use the guidelines in this appendix to use the Windows user interface to import or export Insight databases.

Import a database

You can import a database by using the Import-Export tool in the Insight program folder.

1. In the Windows start menu, navigate to **Insight 5.4.0** > **Administration** > **Import-Export Tool**.
   Import/Export window appears.
2. Select **Import**.
3. Click the ellipsis button to select the folder where the database files are located.
4. Create an empty database for the SQL server.
5. On the **Import/Export** window, specify the configuration parameters and credentials for the newly created database. You can click **Test Connection** to check the connection.
6. Click **Import**.
   The data from database is imported to the specified empty database.

   Note You can use an SQL client to verify that the new database contains tables filled with data.

Export a database

You can export a database by using the Import-Export Tool in the Insight program folder.

1. In the Windows start menu, navigate to **Insight 5.4.0** > **Administration** > **Import-Export Tool**.
   Import/Export window appears.
2. Select **Export**.
3. Click the ellipsis button and select the destination folder where the database will be exported.
4. Specify configuration parameters and credentials for the database. You can click **Connect** to check the connection.
5. Click **Export**.
   The database is exported to the specified folder as an XML file.