# Integrating SQL Server with File Access Manager

Version: 8.2 Revised: July 05, 2021

# Contents

# Capabilities

This connector enables you to use IdentityIQ File Access Manager to access and analyze data stored in SQL Server and do the following:

- Analyze the structure of your stored data.
- Monitor user activity in the resources.
- Verify user permissions on the resources, and compare them against requirements.

See the IdentityIQ File Access Manager documentation for a full description.

## Supported Versions

- SharePoint Server 2013, 2016, and 2019
- 32-bit and 64-bit

# Connector Overview

The SQL connector enables connection to an MS SQL resource. The connector supports crawling, permissions collection and activity monitoring.

## Supported Versions

The IdentityIQ File Access Manager SQL Connector supports the following versions of MS SQLServer:

- 2017 (14.0)
- 2016 (13.0)
- 2014 (12.0)
- 2012 (11.0)

## Limitations of the SQL Server Connector

The following features are not supported by the SQL Server Connector

- Nested Roles – Roles within other roles (Database roles and Server roles)
- SQL Server Permission Covering . See

  https://docs.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-2017#chart-of-sql-server-permissions
- Contained Users - SQL Server Database Contained Users . See

  https://docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable
- MS SQL Server for Azure
- The following SQL Server Resources
  - XML Schema Collections
  - Message Types
  - Contracts
  - Services
  - Remote Service Bindings
  - Routes
  - Full-text catalog and stoplists
  - Symmetric Key
  - Asymmetric Key
  - Certificate
  - Endpoints

- Availability Groups
- Database scoped credential

IdentityIQ File Access Manager features not supported by the SQL connector

- *What If* for local groups
- Access fulfillment
- Data Classification
- Effective Permissions are not calculated. The flag is always set to FALSE

## Activity Monitor Operation Principles

The activity monitor collects events from the SQL server using a query that is defined in the application configuration. Each row returned by the query is an activity, and stored in the IdentityIQ File Access Manager database.

> Just to clarify the point - IdentityIQ File Access Manager does not monitor database activity. It monitors a table supplied by you, analyzing the entries as activities, and entering them into the File Access Manager activity analysis engine.

***To configure activity monitoring in IdentityIQ File Access Manager:***

1. Identify or create a database activity table that contains the activities
2. Create a query defining user activities as you wish to monitor them, that points to this activity table
3. Add the query to the configuration panel described below, under Activities Query
4. Map the fields in the Activities Query to the IdentityIQ File Access Manager activity fields, on the same configuration panel

## Permissions Collector Operation Principles

IdentityIQ File Access Manager connects to the SQL Server through Microsoft ODBC driver, gathers local SQL Server principals and analyzes its objects and permissions on all the server's database instances.

## Local Principals Gathering

### Identity types

Before collecting all the permission-principal relations, three types of identities are collected:

- Server Logins – principals that might relate to a Windows user / active directory user or an SQL Server authentication user
- Server Roles – principals that act as SQL Server groups on the entire server scope
- Database Roles – principals that act as SQL Server groups on a database scope

### Principals Naming

SQL Server Login names stored by the Permission Collection have certain naming patterns, whereas "domain" fields might act as - domain name, special groups such as NT SERVICE, Computer name or the server instance name (i.e.

domain1\user2, NT SERVICE\MSSQLSERVER, machine45\user56)

SQL Server Database Role names stored as “database name\role name” (i.e. db1\public, db2\db_owner)

# Business Resource Full Path Conventions

## Tree node types

Resource tree nodes can be divided into two categories:

***A Real SQL Server object node***

A server instance, table, assembly, etc.

***A Virtual SQL Server node***

Tables, Databases, Security, etc.

## Characters encoding

As each real object might contain special characters such as a period (.) or back-slash (\), the node name is wrapped in brackets ‘[‘ and ‘]’

Examples: [TABLE1], [VIEW1], [sp_help]

> Virtual node names are not wrapped in brackets, since the name of virtual nodes are fixed and defined by IdentityIQ File Access Manager

## Root node

Each resource full path starts with an instance name [SERVER\INSTANCE NAME]

## Components

- Virtual components start with a colon ( ‘:’ )
  - [SERVER]:Databases
  - [SERVER]:Security:Users
- Real SQL Server objects start with a period, to separate them from other components
  - [Server].[DB1].[Schema2].[Table3]
  - [Server]:Security:Logins.[sa]

# Prerequisites

Make sure your system fits the descriptions below before starting the installation.

## Software Requirements

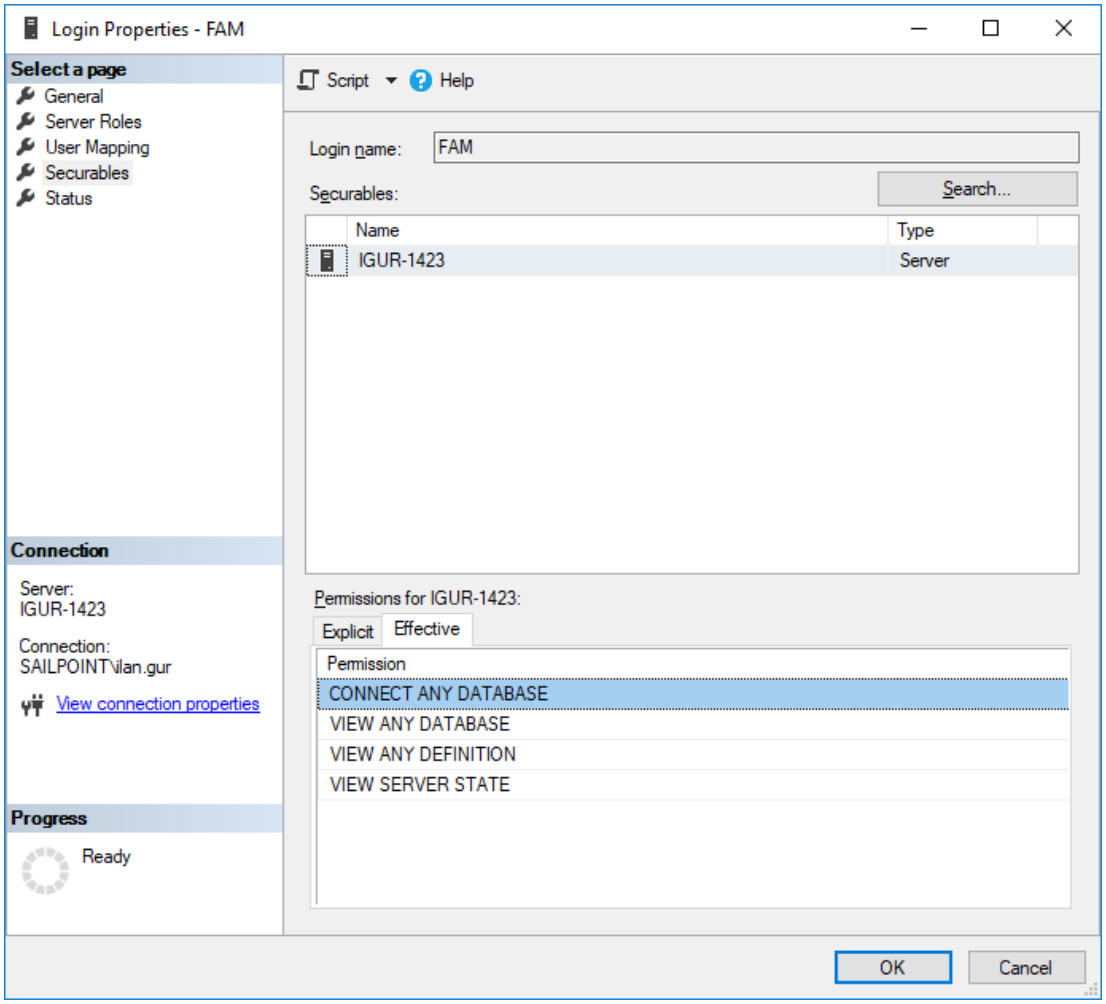
IdentityIQ File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 3.1.x Hosting Bundle version from here .

## Permissions

File Access Manager requires the following permissions on an SQL Server's login:

- GRANT CONNECT ANY DATABASE ON SERVER LEVEL
- GRANT VIEW ANY DEFINITION ON SERVER LEVEL

  This covers the permission: VIEW ANY DATABASE ON SERVER LEVEL
- GRANT VIEW SERVER STATE ON SERVER LEVEL




***Why do we need this access?***

The SQL connector uses these privileges in order to define the last access date of object in the SQL Server for use by the stale data feature.

File Access Manager uses "The principle of least privilege".

**CONNECT ANY DATABASE** is a simple server-level permission that provides access to all current and future databases. On its own, there is no further functionality provided, but when combined with other permissions, it can allow business security needs to be met with ease.

Combined with **VIEW SERVER STATE**, a login can now monitor server and database metrics via a host of dynamic management views.

File Access Manager collects **last_access** properties from database metrics and use them to define stale data.

## Communications Requirements

| Requirement | Source | Destination | Port |
|---|---|---|---|
| File Access Manager Message Broker | Permissions Collector | RabbitMQ | 5671 |
| IdentityIQ File Access Manager Access | Activity Monitor | IdentityIQ File Access Manager Servers | 8000-8008 |
| Permissions Collection/ Activity Audit | Permissions Collector services / Activity Monitor | SQL Server Instance | As Configured in SQL Server Configuration Manager (usually TCP port 1433, Or port 0 to connect to SQL Server Browser) |

# Connector Installation Flow Overview

To install the SQL Server connector:

1. Configure all the prerequisites.
2. Add a new SQL Server application in the Business Website.
3. Install the relevant services:
    - Activity Monitor
    - Permissions Collector

# Collecting Data Stored in an External Application

### Connector / Collector terminology:

***Connector***

The collection of features, components and capabilities that comprise IdentityIQ File Access Manager support for an endpoint.

***Collector***

The “Agent” component or service in a Permission Collection architecture.

***Engine***

The core service counterpart of this architecture.

***Identity Collector***

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your IdentityIQ File Access Manager installation. See the server Installation guide for further details.

***Install a Permission Collection central engine***

One or more central engines, installed using the server installer

***Create an Application in File Access Manager***

From the Business Website. The application is linked to central engines listed above.

***Add an Activity Monitor***

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

***Install Permission Collectors (optional)***

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

> For further details, see section **Application > Central Service > Collector Relations** in the IdentityIQ File Access Manager Administrator Guide

# Adding an SQL Server Application

In order to integrate with SQL Server, we must first create an application entry in IdentityIQ File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin* > *Applications*
2. Click **Add New** to open the wizard.

## Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

## General Details

***Application Type***

SQL Server

***Application Name***

Logical name of the application

***Description***

Description of the application

***Tags***

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

> The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

***Event Manager Server***

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu

***Identity Collector***

Select from the Identity Collector dropdown menu.

- You can create identity collectors in the administrative client. *Applications* > *Configuration* > *Permissions Management* > *Identity Collectors*

  See section "OOTB Identity Collection" in the Collector Installation ManagerIdentityIQ File Access Manager Administrator Guide for further details.
- If adding a new identity collector, press the **Refresh** button to update the Identity Collector dropdown list.

Click **Next**.

## Connection Details

***Server / Instance Path***

The name of the SQL Server Instance

***Port***

The port of the instance, or 0 - for SQL browser connectivity. Default is set to 1433

***Authentication Type***

Choosing Windows authentication will use AD Credentials to re-authenticate for the given user/password. SQL Authentication is used by default.

***Domain Name***

For Windows authentication only. For SQL Authentication this field should remain empty

***User Name / password***

Windows user name without domain, or SQL login for SQL authentication

> Do not use the format domain\username.

***Query Timeout (min)***

In minutes. The default timeout is 0, which means 'wait indefinitely'.

***Activities Query***

This query will periodically run to fetch new activities from the table(s) defined as containing activity records (See Activity Monitor Operation Principles)

***Activity ID Column Name***

The column name in the Activities Query which identifies the unique id of the activity. This column is used to query for new activities periodically

***Business Resource Column Name***

The column name in the Activities Query which will be displayed to the user as the Business Resource Full Path in the Activities Forensics

***Domain Column Name***

The column name in the Activities Query which will be displayed to the user as the Domain in the Activities Forensics. This field is optional

***Username Column Name***

The column name in the Activities Query which will be displayed to the user as the User Name in the Activities Forensics

***Activity Timestamp Column Name***

The column name in the Activities Query which represents the time the activity occurred

***Activity Action Column Name***

The column name in the Activities Query which represents the action of the activity – not mandatory

***Sample Event Column Name***

Either by Event ID or by Date

> The SQL Server connector adds a condition to fetch only new events for each query. This condition is created with the Sample Event Column.

Click **Next**.

## Configuring and Scheduling the Permissions Collection

Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the “IdentityIQ FAM Central Permission Collector” wasn’t installed during the installation of the server, this configuration setting will be disabled.

***To configure the Permission Collection***

- Open the edit screen of the required application
  a. Navigate to **Admin > Applications**
  b. Scroll through the list, or use the filter to find the application
  c. Click the edit icon on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

***Central Permissions Collection Service***

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section "Services Configuration" in the IdentityIQ File Access Manager Administrator Guide for further details.

***Skip Identities Sync during Permission Collection***

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connectors.

> This option is checked by default.

## Scheduling a Task

***Create a Schedule***

Click on this option to view the schedule setting parameters.

***Schedule Task Name***

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

***Schedule***

Select a scheduling frequency from the dropdown menu.

- ***Schedule Types and Intervals***

  ***Once***

  Single execution task runs.

  ***Run After***

  Create dependency of tasks. The task starts running only upon successful completion of the first task.

  ***Hourly***

  Set the start time.

  ***Daily***

  Set the start date and time.

  ***Weekly***

  Set the day(s) of the week on which to run.

  ***Monthly***

  The start date defines the day of the month on which to run a task.

  ***Quarterly***

  A monthly schedule with an interval of 3 months.

  ***Half Yearly***

  A monthly schedule with an interval of 6 months.

  ***Yearly***

  A monthly schedule with an interval of 12 months.

***Date and time fields***

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.

***Active check box***

Check this to activate the schedule.

Click **Next**.

# Configuring and Scheduling the Crawler

***To set or edit the Crawler configuration and scheduling***

- Open the edit screen of the required application
  a. Navigate to **Admin > Applications**
  b. Scroll through the list, or use the filter to find the application
  c. Click the edit icon on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type

***Create a Schedule***

Click to open the schedule panel. See Scheduling a Task

## Setting the Crawl Scope

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

### *Including and Excluding Paths by List*

***To set the paths to include or exclude in the crawl process for an application***

- Open the edit screen of the required application
  a. Navigate to **Admin > Applications**
  b. Scroll through the list, or use the filter to find the application
  c. Click the edit icon on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type

1. Scroll down to the Crawl configuration settings.
2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
3. Click Include / Exclude Resources to open the input fields.
4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.
5. To remove a resource from a list, find the resource from the list, and click the *x* icon on the resource row.

When creating exclusion lists, excludes take precedence over includes.

## *Excluding Paths by Regex*

***To set filters of paths to exclude in the crawl process for an application using regex***

- Open the edit screen of the required application
  a. Navigate to **Admin > Applications**
  b. Scroll through the list, or use the filter to find the application
  c. Click the edit icon on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions. See the example below in section Business Resource Structure to better understand the business resource full path structure.

**Crawler Regex Exclusion Examples**

The following are examples of crawler Regex exclusions:

**Exclude all shares which start with one or more shares names:**

| |
|---|
| Starting with \\server_name*shareName* |
| Regex: `\\\\server_name\\`*shareName*`$` |
| Starting with \\server_name\shareName or \\server_name*OtherShareName* |
| Regex: `\\\\server_name\\(`*shareName*`|`*OtherShareName*`)$` |

**Include ONLY shares which start with one or more shares names:**

| |
|---|
| Starting with \\server_name*shareName* |
| Regex: `^(?!\\\\server_name\\`*shareName*`($|\\.*)).*` |
| Starting with \\server_name*shareName* or \\server_name*OtherShareName* |
| Regex: `^(?!\\\\server_name\\(`*shareName*`|`*OtherShareName*`)($|\\.*)).*` |

**Narrow down the selection:**

*Include ONLY* the C$ drive shares: \\server_name*C$*

```
Regex: ^(?!\\\\server_name\\C\$($|\\.*)).*
```

Include ONLY one folder under a share: \\server\share*folderA*

Regex: `^(?!\\\\server_name\\share\$($|\\folderA$|\\folderA\\.*)).*`

Include ONLY all administrative shares

Regex: ^(?!\\\\server_name\\[a-zA-Z]\$($|)).*

**Exclude one or more databases (For MS SQL Server):**

Exclude one or more databases by name

```
[SampleDatabase3]|[SampleDatabase1]
```

**Exclude parts of a database (For MS SQL Server):**

Exclude an object in a database, such as a table, view etc.:

```
[Database Name].[Schema Name].[Table Name]
```

For Virtual Objects propitiatory format with ":"

```
[Database Name]:Virtual Schema Name
```

> To write a backslash or a Dollar sign, add a backslash before it as an escape character.

> To add a condition in a single command, use a pipe character “|” .

## *Excluding Top Level Resources*

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

***To exclude top level resources from the crawl process***

1. Open the application screen

   *Admin* > *Applications*

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.
3. ***Run Task***

   The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

   Before running the task for the first time, the message above this button is:

   **"Note: Run task to detect the top-level resources"**

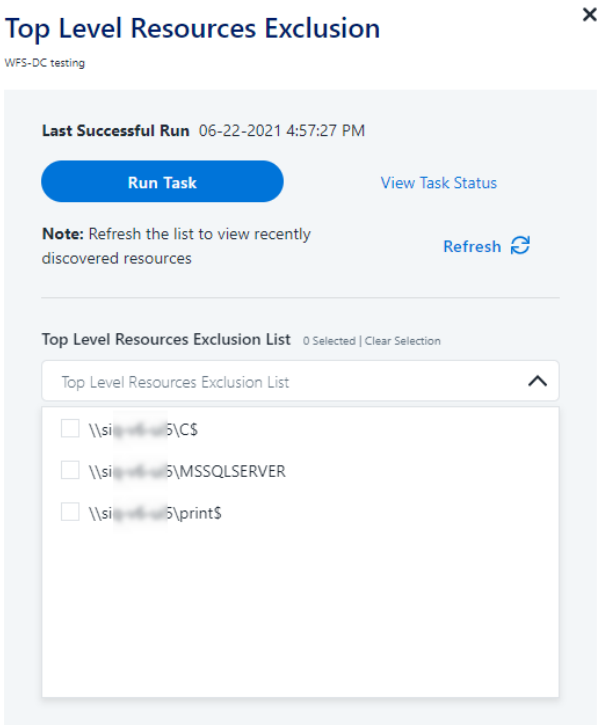
   If the top level resource list has changed in the application while yo u are on this screen, press this button to retrieve the updated structure.

   Once triggered, you can see the task status in

   *Settings* > *Task Management* > *Tasks*

   > This will only work if the user has access to the task page

   When the task has completed, press **Refresh** to update the page with the list of top level resources.
4. Click the top level resource list, and select top level resources to exclude.
5. Click *Save* to save the change.
6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.



### *Special Consideration for Long File Paths in Crawl*

If you need to support long file paths above 4,000 characters for the crawl, set the flag

**`excludeVeryLongResourcePaths`**

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

> You should not enable exclusion of long paths, unless you experience an issue.

#### *Background*

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

#### *Identifying the Problem*

When using an SQL Server database version 2014 and ealier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

#### *Setting the Long Resource Path Key*

The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\

Search for the key **excludeVeryLongResourcePaths** and correct it as described above.

## Configuring Activity Monitoring

Configure the activity monitoring process frequency.

#### *Polling Interval (sec)*

Activity fetching interval [in seconds]). Default is set to 60 seconds,

#### *Report Interval (sec)*

Activity Monitor Health reporting interval [in seconds]). Default is set yo 60 seconds.

***Local Buffer Size (MB)***

Local buffer size for activities [ in MB]). Default is set to 200MB.

This cyclic buffer is used to store activities on the Application Monitor's machine in case of network errors that prevent the activities from being sent.

## Configuring Data Enrichment Connectors

The Data Enrichment Connectors (DEC) configuration enables us to select data enrichment sources. These can be used to add information from other sources about identities.

An enrichment source could be a local HR database that is used to combine users' job descriptions or departments to the information stored in the identity store.

Select the data enrichment connectors to enrich monitored activities from the Available DECs text box.

Use the > or >> arrows to move the selected DECs to the Current DECs text box.

The user can select multiple DECs. Simply select each desired DEC.

You can create a new DEC in the Administrative Client (*Applications* > *Configuration* > *Activity Monitoring* > *Data Enrichment Connectors*). After creating a new DEC, Click **Refresh** to refresh the dropdown list.

The chapter **Connectors** of the IdentityIQ File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

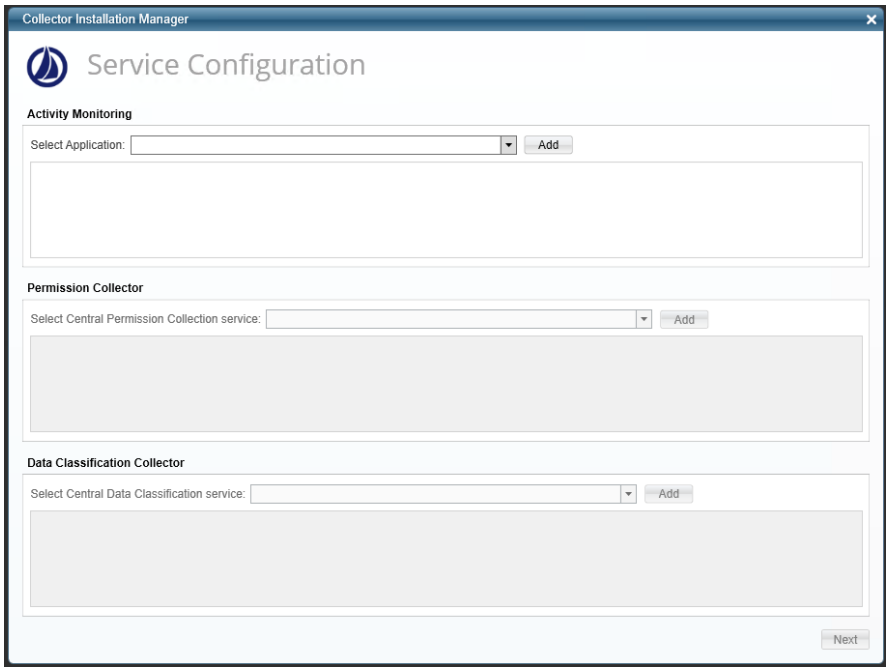
# Installing Services: Collector Installation

1. Run the **Collector Installation Manager** as an Administrator.
   The installation files are in the installation package under the folder **Collectors**.

   The Collector Installation Manager window displays.


2. Enter the credentials to connect to IdentityIQ File Access Manager.
   a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
   b. An IdentityIQ File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click **Next**.

   The Service Configuration window displays.




4. If you are installing the Activity Monitoring collector, select the application, and click **Add.**

   > In some applications, additional credentials may be required to allow granting elevated permission for activity monitoring collection.

5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**
6. Click **Next**.

   The Installation Folder window displays.

   > If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

7. Browse and select the location of the target folder for installation.
8. Browse and select the location of the folder for system logs.
9. Click **Next**.
10. The system begins installing the selected components.
11. Click **Finish**

    The Finish button is displayed after all the selected components have been installed.

> The *IdentityIQ File Access Manager Administrator Guide* provides more information on the collector services.

# Verifying the SQL Server Connector Installation

## Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the IdentityIQ File Access Manager services, and see that they are running.

for example:

- File Access Manager Activity Monitor - <Application_Name>
- File Access Manager Permissions Collection - <Application_Name>

## Log Files

Check the log files listed below for errors

- “%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"

## Monitored Activities

1. Simulate activities on SQL Server.
2. Wait a minute (approximately).
3. Verify that the activities display in the IdentityIQ File Access Manager website under

   *Forensics* > *Activities*

## Permissions Collection

1. Run the Crawler and Permissions Collector tasks (*Settings* > *Task Management* > *Scheduled Tasks*)
2. Verify that:
   - The tasks completed successfully
   - Business resources were created in the resource explorer (*Admin* > *Applications* > [application column] > *Manage Resources*)
   - Permissions display in the Permission Forensics page (*Forensics* > *Permissions*)