



# Integrating Google Drive with File Access Manager

Version: 8.3 Revised: March 30, 2022

This document and the information contained herein is SailPoint Confidential Information

---

## Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

# Contents

---

|  |            |
|--|------------|
| <b>Contents</b> .....  | <b>iii</b> |
| <b>Capabilities</b> .....  | <b>5</b>   |
| <b>Connector Overview</b> .....  | <b>6</b>   |
| How is Google Drive Mapping Converted to a Business Resources Tree? .....        | 6          |
| Monitored Activities .....   | 7          |
| Permissions Collection Operation Principles .....                                | 7          |
| <b>Prerequisites</b> .....   | <b>8</b>   |
| Software Requirements .....  | 8          |
| Permissions .....  | 8          |
| Enabling Google SDKs (Google Drive API, Drive Activity API, Admin SDK API) ..... | 8          |
| Creating a Service Account and Assigning it Domain-wide Delegation .....         | 9          |
| Delegate Domain-wide Authority to the Service Account. ....                      | 10         |
| Limiting File Access Manager Permissions .....                                   | 10         |
| Communications Requirements .....  | 12         |
| <b>Google Drive Connector Installation Flow Overview</b> .....                   | <b>13</b>  |
| <b>Collecting Data Stored in an External Application</b> .....                   | <b>14</b>  |
| <b>Adding a Google Drive Application</b> .....                                   | <b>15</b>  |
| Select Wizard Type .....   | 15         |
| General Details .....  | 15         |
| Connection Details .....   | 15         |
| Configuring and Scheduling the Permissions Collection .....                      | 16         |
| Selecting and Scheduling the Data Classification Settings .....                  | 22         |
| Data Privacy .....   | 23         |
| Configuring Activity Monitoring .....  | 23         |
| Configuring Data Enrichment Connectors .....                                     | 23         |
| <b>Installing Services: Activity Monitor Collector</b> .....                     | <b>24</b>  |
| <b>Verifying the Google Drive Connector Installation</b> .....                   | <b>26</b>  |
| Installed Services .....   | 26         |

## Contents

---

|                              |    |
|------------------------------|----|
| Log Files .....              | 26 |
| Monitored Activities .....   | 26 |
| Permissions Collection ..... | 26 |

## Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in Google Drive and do the following:

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

See the File Access Manager documentation for a full description.

## Connector Overview

File Access Manager Connector for Google Drive uses the following Google APIs:

- Google Drive Activities API and Google Reports API for event monitoring
- Google Drive API for resource crawling and permissions collection
- Google Admin SDK (Directory API) for domain identities (users, groups, and so on)

Google APIs are accessed via a Service Account, defined within the scope of the customer's Google Apps Domain. The Service Account has Domain-wide delegation permission so that it can impersonate domain users and access their Google Drive activities and data.

### How is Google Drive Mapping Converted to a Business Resources Tree?

- Google Drive represents files and folders in a graph (a.k.a. map) data structure so that every node may have multiple parent and children nodes. In a tree structure, however, every node can have only one parent. For example, a folder shared by two users actually has two different parents – one in each of the user's personal drives.
- To maintain a recognizable structure for Google Drive resources, File Access Manager displays business resources in a tree, exactly as they are arranged from the user's perspective.
- When users share folders, flattening the graph structure into a tree results in duplicate resources, which are maintained to keep the structure recognizable.
- If external users (external to the company's Google Apps domain) share folders with domain users, a separate "External" tree root represents those resources.
- If shared drives exist in the domain and have members assigned to them, a separate "Shared Drives" tree root represents those resources.
- The following is a sample schematic of the File Access Manager Google Drive resource tree:
  - External
    - private@gmail.com
      - sharedFolder1
  - Shared Drives
    - Shared Drive 1
      - sharedDriveFolder1
      - sharedDriveFolder2
  - Users
    - u1@my-company.com
      - Folder1
      - Folder2

- u2@my-company.com
- u3@my-company.com

## Monitored Activities

Monitored Administrator audit events (Google Domain events) include:

- User Events and group events (USER\_SETTINGS and GROUP\_SETTINGS, respectively)

## Permissions Collection Operation Principles

The File Access Manager Google Drive Permissions Collection task uses Google Drive API to retrieve information From Google Drive.

File Access Manager automatically creates a Google Drive Identity Collector (when the “Add New Application” wizard finishes) which collects the users and groups from the Google Apps Domain.

## Prerequisites

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

### Software Requirements

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

To enable File Access Manager to interact with Google Apps, the high level steps are:

1. Enable Google SDKs (Google Drive API, Drive Activity API, Admin SDK API)
2. Create a service account and assign it domain-wide delegation
3. Delegate domain-wide authority to the service account. This is required to capture activities.

### Enabling Google SDKs (Google Drive API, Drive Activity API, Admin SDK API)

#### *Creating a project:*

1. Go to your Google Apps developer console: <https://console.developers.google.com>
2. Make sure that you are using an administrator account for your Google Apps domain.
3. Click **Project** drop down from top bar (next to Google API logo), select “**New Project**”.
4. Name the project (e.g., “FAM”) and click “**Create**”.
5. Wait for the project to be created and then click “**Select Project**” from the top right Notification bar.
6. Using the previous drop-down selector, ensure the new project is selected, otherwise you may default to the previous project.

#### *Enabling Google APIs:*

1. Top left, click three lines > APIs & services
2. In the new project click “**+Enable APIs**” from the top bar
3. Using the Search box, find and enable the following APIs:
  - a. Google Drive API
  - b. Drive Activity API
  - c. Admin SDK API

## Creating a Service Account and Assigning it Domain-wide Delegation

1. On the top left (menu button) choose APIs & Services > Credentials.

This is an important step, failure to do so will mean you will create Credentials just for the last API you were in.

2. Click **"Create Credentials"**.
3. Select **"Service account"**.
4. Type in a name for the new service account in "Service account name" (e.g. "svc\_fam").

Note that the user, domain, and service account name are all case sensitive.

5. Click **Create** then **Done**.
6. Verify that the new account is listed under within Credentials, under the **Service Accounts** heading
7. Click on newly created account, or click the Edit icon
8. Click the **Show Domain-wide Delegation** drop down menu
9. click **Enable G Suite Domain-wide Delegation**

If you get a message 'To change domain wide delegation, a product name for the OAuth consent screen must be configured....', follow the prompts and create the Consent as instructed.

10. Click Add Key > Create new key
11. Select "P12" under "Key type".
12. Choose Project Owner as the role for this service account.
13. Click **Create**.
14. A certificate file (".p12") is then downloaded to your computer, this file is required when creating the Google Drive application in [Adding a Google Drive Application](#) in File Access Manager.
15. A popup window appears showing the password to the .p12 file. Save this password for future use within the *Add New Application Wizard*.

This popup is displayed only once. Copy the password, or you will have to define a new service account

16. Copy the svc account email address <email>@<project\_name>-123.iam.gserviceaccount.com this will be needed in the next step (authorizing the service account).
17. Click **Show Domain-wide delegation** and then **Enable G Suite Domain wide delegation**
18. Assign a Product Name as prompted (eg FAM).

19. Copy the Unique ID number (the Client ID) – this file will be needed in the next step (authorizing the service account)
20. Click **Save**.

## Delegate Domain-wide Authority to the Service Account.

This is required in order to capture activities.

1. Go to Google administrative console at: <https://admin.google.com>
2. Click **“Security”** . If it is not listed, click the **“More controls”** button at the bottom of the screen).
3. Click API Controls
4. Manage Domain Wide Delegation
5. Click “Add new”
6. Under **“Client ID”**, paste the “Unique ID” (this is the same as the Client ID) of the service account you created in the previous step.
7. Under **“Oath scopes (comma-delimited)”**, paste the following in its entirety:  
  
`https://www.googleapis.com/auth/activity, https://www.-  
googleapis.com/auth/admin.directory.group.member.readonly, https://www.-  
googleapis.com/auth/admin.directory.group.readonly,  
https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.-  
googleapis.com/auth/admin.reports.audit.readonly, https://www.googleapis.com/auth/drive.readonly,  
https://www.googleapis.com/auth/drive.activity`
8. Click **“Authorize”**

## Limiting File Access Manager Permissions

During the Application setup, you must provide a Domain Admin User for File Access Manager to collect data on the Google Drive domain.

You can provide the Super Admin, or create a dedicated File Access Manager Google account with fewer permissions.

The File Access Manager Google account requires the following permissions:

### ***On the desired OU (Organizational Unit) level***

Organizational Units -> Read

Users -> Read

### ***Domain-wide***

Groups -> Read

Reports

Note the following regarding crawling, permissions collections, and activities:

### ***Crawling***

The resource tree contains only OU users and folders for which a File Access Manager user has permissions.

### **Permissions Collection**

File Access Manager only analyzes resources for permissions under scoped OUs.

Since groups are defined on a domain-wide basis, rather than by OU, File Access Manager collects all domain groups.

If users from OUs (for which a File Access Manager user lacks permission) have permissions on resources under the analyzed OU, those users are considered File Access Manager External Accounts, since File Access Manager cannot collect information on those users.

### **Activities**

File Access Manager only collects activities for users for which a File Access Manager user has permissions.

File Access Manager collects administrator activities (such as changing users or passwords) on a domain-wide basis, rather than by user/OU.

### **Data Classification**

File Access Manager only indexes and classifies resources collected during a crawl (only resources to which a File Access Manager user has permissions).

To create, and grant permissions to, a File Access Manager Google Administrator account perform the following steps:

1. Sign in to the Google Administrator console ([admin.google.com](https://admin.google.com)) using the Super Admin account (or any account that can create and grant Administrator roles and create users).

2. Click **Users**

If you cannot see Users, click the More Controls bar at the bottom of the screen.

3. Choose an OU on which to create a File Access Manager account by hovering over the plus (+) sign at the bottom right corner of the screen.

4. Click **Add User**.

5. Fill in a name and primary email address and password for the user, Ensure you note down the password for future reference.(for example, IdentityIQfam\_reader).

6. Click **Create**.

7. Click **Admin Roles** on the Google Admin console.

To see the Admin Roles, click the More Controls bar at the bottom of the screen.

8. Click **Create a New Role**. (This will be the OU targeted role.)

9. Type a role name and description (for example, File Access Manager OU Reader).

10. Click **Create**.

11. Check the following checkboxes under the *Privileges* tab > *Admin Console Privileges*:

## Prerequisites

---

- a. *Organizational Units > Read*
- b. *Users > Read*

12. Click **Save**.
13. Select the newly created role, and click **Assign Admins** under the **Admins** tab.
14. Select the desired OU from the drop-down list and type the name of the File Access Manager account.
15. Click **Confirm Assignment**.

The role applies to the OU and all its descendants. You can assign the role to the same user on another OU later.

16. Click **Create a New Role**. (This will be a domain-wide role.)
17. Type a role name and description (for example, File Access Manager Domain Reader).
18. Click **Create**.
19. Check the **Reports** checkbox under the *Privileges* tab > *Admin Console Privileges*.
20. Check the *Groups > Read* checkbox under the *Privileges* tab > *Admin API Privileges*.
21. Click **Save**.
22. Select the newly created role, and click **Assign Admins** under the **Admins** tab.
23. Type the File Access Manager account.
24. Click **Confirm Assignment**.

## Communications Requirements

| Requirement   | Source   | Destination                 | Port      |
|---|--|-----------------------------|-----------|
| File Access Manager Message Broker                    | Permission Collector / Data Classification Collector | RabbitMQ                    | 5671      |
| File Access Manager Access                            | Activity Monitor                                     | File Access Manager Servers | 8000-8008 |
| Permissions Collector / Data Classification Collector | Permissions Collector / Data Classification          | Google APIs                 | https     |
| Activity Monitoring                                   | Activity Monitor                                     | Google APIs                 | https     |

## Google Drive Connector Installation Flow Overview

To install the Google Drive connector:

1. Configure all the prerequisites.
2. Add a new Google Drive application in the File Access Manager website.
3. Install the relevant services:
  - Activity Monitor

Google Drive currently does not support the Cloud-Ready architecture for permissions collection and data classification. Permission collection and data classification tasks will run on the central engine services associated with the application, regardless of whether these services have one or more collectors associated with the central engine.

## Collecting Data Stored in an External Application

### Terminology:

#### **Connector**

The collection of features, components and capabilities that comprise File Access Manager support for an end-point.

#### **Collector**

The “Agent” component or service in a Data Classification and or 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 File Access Manager installation. See the server Installation guide for further details.

#### **Install a Data Classification central engine**

One or more central engines, installed using the server installer

#### **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.

## Adding a Google Drive Application

In order to integrate with Google Drive, we must first create an application entry in 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**

Google Drive

#### **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.

Click **Next**. to open the Connection Details page.

### Connection Details

#### **Domain Admin User**

The full user name of an admin user in your Google domain.

Write the username as a UPN: User@Domain.com

Note that the user, domain, and service account name are all case sensitive.

### **Domain Name**

Your Google primary domain name

### **Service Account**

The full name of service account created in the [Permissions](#) section of this guide

e.g.: <email>@<project\_name>-123.iam.gserviceaccount.com

### **Certificate File**

The certificate file created during the Prerequisites section of this guide. Upload a certificate by dragging it onto the certificate field, or clicking to open a file manager dialogue

### **Certificate Password**

The password for the certificate file created in the Prerequisites section of this guide

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 “File Access Manager 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 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 connector.

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.

### **Calculate Resource Size**

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never
- Always
- Second crawl and on (This is the default)

### **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.

### Crawler Regex Exclusion Example

The following are examples of crawler Regex exclusions:

**Exclude all drives that start with one or more user names:**

Example: Starting with John.Doe

Regex: ^Users\John\.Doe@.\*

Example: Starting with John.Doe or Jane.Doe

Regex: ^Users\(John|Jane\)\.Doe@.\*

**Exclude users specific drives:**

Example: Exclude bin & debug drives under Service drive

Regex: `^Users\John\.Doe@.*\Service\bin|debug)$`

**Include ONLY drives that start with one or more user names:**

Example: Starting with John.Doe

Regex: `^(?!Users\John\.Doe@.*)*`

Example: Starting with John.Doe or Jane.Doe

Regex: `^(?!Users\John|Jane)\.Doe@.*)*`

Example: Include ONLY Service drive resources

Regex: `^(?!Users\John\.Doe@my_organization.com($|\Service($|V.*)))*`

**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 you are on this screen, press this button to retrieve the updated structure.

Once triggered, you can see the task status in

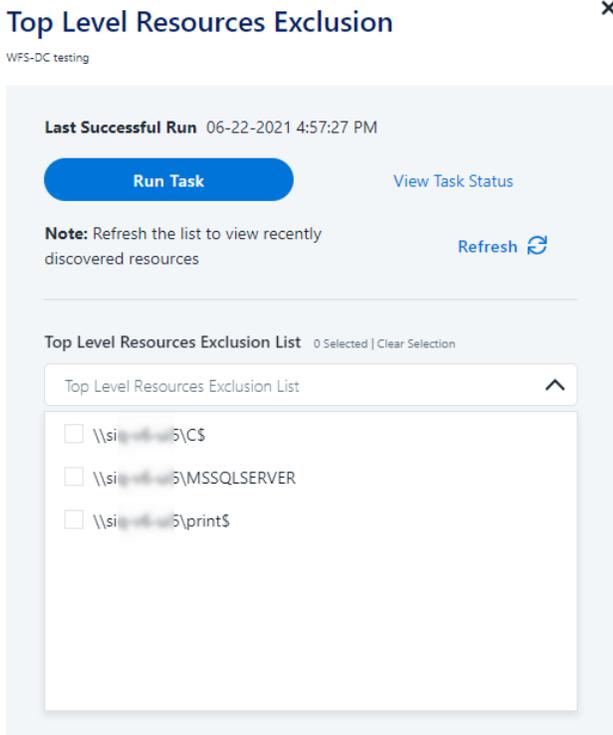
*Settings > Task Management > Tasks*

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.

- 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 earlier

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.

## **Selecting and Scheduling the Data Classification Settings**

### **To associate an application with a data classification service, and set the schedule**

- 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 **Data Classification** settings page.

The actual entry fields vary according to the application type

### **Central Data Classification Service**

Associate the application with a Central Data Classification Service. This service is responsible for running the Data Classification tasks.

If the “Central Data Classification” wasn’t installed during the installation of the server, this field is disabled.

### **Disabling Data Classification**

To disable data classification, delete the entry from the central data classification field.

Disabling data classification can also be achieved by setting the scheduler to be inactive (which is the default setting for data classification).

### **Create a Schedule**

This option is enabled only if a central data classification service is selected.

See [Scheduling a Task](#)

See the chapter “Data Classification” in the File Access Manager Administrator Guide for more information

Click **Next** or **Finish**.

## Data Privacy

A user can associate the application with a Central Data Classification Engine Service. This engine will be responsible for executed Data Privacy tasks.

Though using different processes for each, the Data Classification engine service is in charge for both Data Privacy and Data Classification discovery tasks.

You may choose the same service for both, or use a different one for each, to run them in parallel.

The fields on the Data Privacy step are the same as the Data Classification step.

## 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 to 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 DEC's text box.

Use the > or >> arrows to move the selected DEC's to the Current DEC's text box.

The user can select multiple DEC's. Simply select each desired DEC.

You can create a new DEC in the Administrative Client (Applications>Configuration>ActivityMonitoring>DataEnrichmentConnectors).

After creating a new DEC, click **Refresh** to refresh the dropdown list.

The chapter Connectors of the 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: Activity Monitor Collector

The activity monitor is installed per application, collecting activity logs.

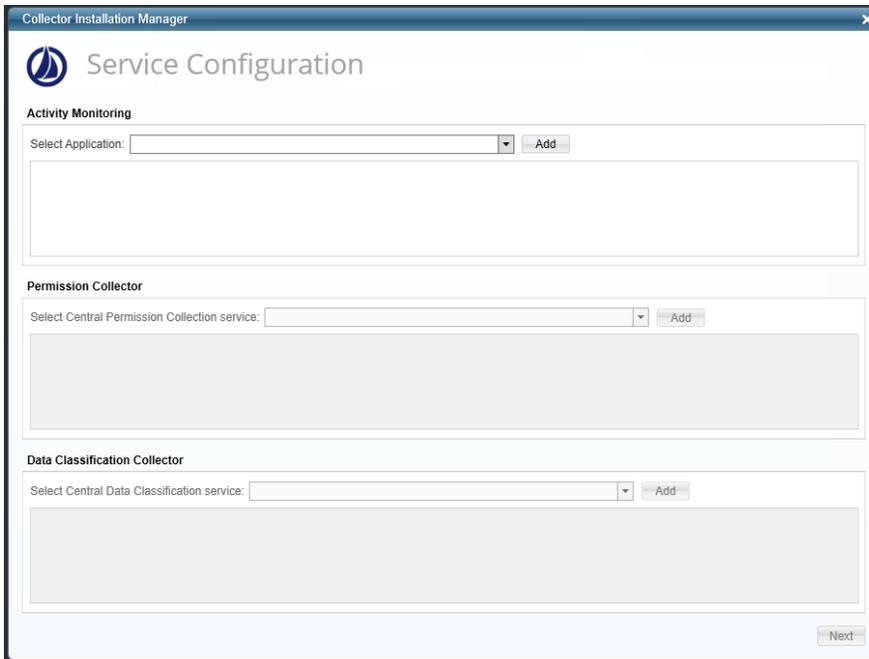
Install the activity monitor using the Collector Installation Manager. This tool is part of the File Access Manager installation package.

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



4. Select the appropriate application, and click **Add**.
5. 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. All future collectors will be installed in this folder.

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

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

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

# Verifying the Google Drive 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 File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Permissions Collection.
- File Access Manager Central Data Classification.
- File Access Manager Central Activity Monitor.

## Log Files

Check the log files listed below for errors

- "%SAILPOINT\_HOME\_LOGS%\PermissionCollection\_<Service\_Name>.log"
- "%SAILPOINT\_HOME\_LOGS%\DataClassification\_<Service\_Name>.log"
- "%SAILPOINT\_HOME\_LOGS%\GDrive-<Application\_Name>.log"
- **On the server which contains the central permissions collection service**  
PermissionsCollection\_[Service Name]
- **If a collector exists, then you can check the collector log**  
PermissionsCollection\_[Central Service Name] Collector [Running Number]

## Monitored Activities

1. Simulate activities on Google Drive.
2. Wait a minute (approximately).
3. Verify that the activities display in the 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*)