Integrating OneDrive with File Access Manager

Version: 8.2 Revised: November 19, 2021

Contents

Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in OneDrive 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

Activity Monitor Operation Principles

- File Access Manager Activity Monitor for OneDrive uses the Microsoft Office365 Management Activity API.
- The Activity Monitor queries the API for OneDrive events.
- The Microsoft Office365 Management Activity API uses the OAuth 2.0 authorization protocol to authenticate and authorize API requests.
- Use of the API, File Access Manager for OneDrive Connector requires a short authorization process during the definition of the OneDrive for Business application.
- After the initial authorization process, File Access Manager will handle OAuth token management automatically and refresh the token if needed.

> It might take up to two hours for events to be received by the File Access Manager for OneDrive Activity Monitor (a current Microsoft limitation).

Monitored Activities

Monitored events and activities are as defined in the Office365 Management Activity API specification:

https://msdn.microsoft.com/en-us/library/office/mt607130.aspx#SharePointAuditOperations

Permissions Collection Operation Principles

- File Access Manager OneDrive for Business permissions collection task uses the Microsoft OneDrive REST API.
- The permissions collection task queries OneDrive for Business for the existing Role Assignments to determine object permissions.
- An Azure Identity Collector must be configured to map the permissions to users and groups from the Azure Active Directory.

> The section on Identity collection in the File Access Manager Installation Guide provides more information on how to define an Azure Identity Collector.

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 Required for OneDrive User

Granting Access to Office365

- Create a proprietary File Access Manager service account in Azure / Office365 administration portal (e.g. **fam-srv@example.com**).
- Assign the "SharePoint administrator" role and “Tenant Admin” privilege / "Global Administrator" Role to the new service account.This will allow the service account to enumerate the existing OneDrive accounts and query for audit information.

> The Tenant Admin privilege / "Global Administrator" Role is necessary for this service account in the initial stage of configuring the application and for granting the consent.
> After the initial configuration, and once the application is configured in File Access Manager, this privilege can be revoked from the service account. During the creation of the Application in the File Access Manager website – log in with the newly created service account and grant Consent to the File Access Manager Azure App.

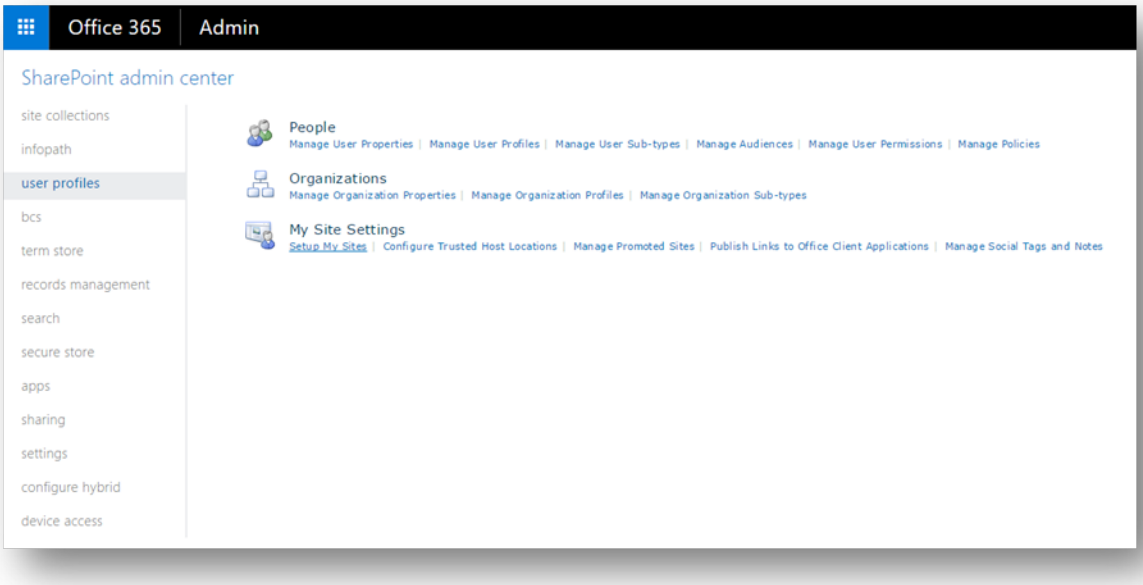
Granting Access to all Existing OneDrive Accounts

- Owner access for the proprietary File Access Manager user is required to crawl, gather permissions and perform classification of documents stored on OneDrive accounts.
- The built-in “SharePoint Service Administrator” group automatically contains any user that was assigned the "SharePoint administrator" role in Azure.
- To grant the required access, “SharePoint Service Administrator” must be defined as a Secondary Owner of each OneDrive account.
- If a user is wanting to share something, the user can either right-click and **Share** or you can grant permission through adding direct permissions or adding them as collaborators.
- In the installation package, you can find a script called **SIQUpdateOneDriveSecondaryOwners.ps1**. This script can be used to automatically update the Secondary Owners list of all existing OneDrive accounts so they to include “SharePoint Service Administrator”. To run the script:
    - Open the folder Scripts in the Collectors.zip installation package
    - Open the SharePoint Online Management Shell (install from here https://www.microsoft.com/en-us/-download/details.aspx?id=35588)
    - Run the script, you will be prompted to provide Credentials for Office365 Global Administrator, and The tenant name of your Office365 subscription.

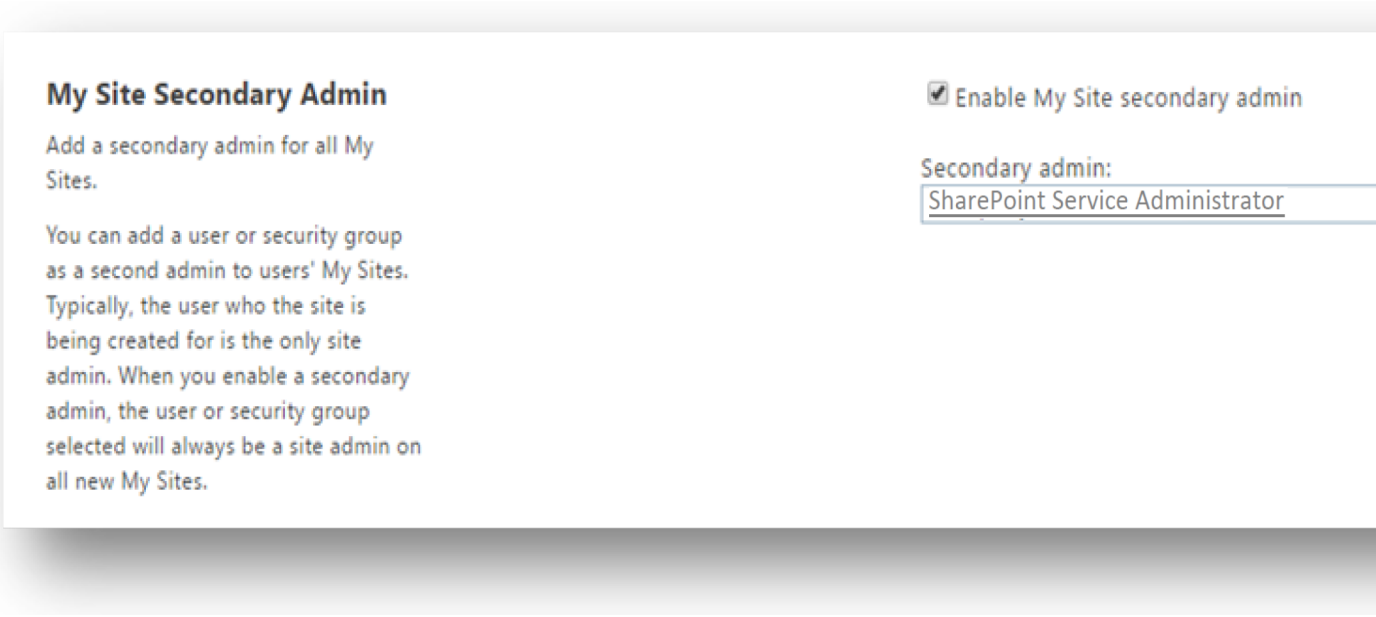
- File Access Manager will not be able to crawl, collect permissions or classify content on OneDrive accounts that are not assigned with the ‘Site Collection Administrator’ permissions for the File Access Manager user.

Granting Access to Future OneDrive Accounts

- SharePoint Online administration portal allows configuration of default members of the Secondary Owners list for newly created OneDrive accounts.
- Browse to the admin portal (e.g. https://my-company-admin.sharepoint.com).
- Go to the “User Profiles” section, then click “Setup My Sites” under “My Site Settings”.



- Scroll down to “My Site Secondary Admin”



- Click the "**Enable My Site secondary admin**" checkbox
- Type "SharePoint Service Administrator" in the text box, and click the resolve button (once successfully resolved, the text should be underlined).
- Scroll to the bottom of the page and click "**OK**".

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor	File Access Manager Servers	8000-8008
Permissions Collection / Data Classification	Permissions Collector / Data Classification services	OneDrive REST API	https
Activity Audit	Activity Monitor	Office365 Activity API	https

Access to the following over HTTPS

https://{tenant-name}.sharepoint.com/*

https://{tenant-name}-admin.sharepoint.com/*

https://{tenant-name}-my.sharepoint.com/*

https://{tenant-name}-my.sharepoint.com/Personal/*

https://{tenant-name}-my.sharepoint.com/_api/v2.0/drive/*

https://{tenant-name}-my.sharepoint.com/_api/web/*

https://{tenant-name}-my.sharepoint.com/_api/web/siteusers

https://{tenant-name}-my.sharepoint.com/_api/web/sitegroups

https://manage.office.com/* - to monitor and collect event data, using the Microsoft Management API

https://oauth.whiteboxsecurity.com/* - SailPoint OAuth service site

Azure Active Directory Connectivity Requirements

The OneDrive Connector requires an AzureAD Identity Collector.

File Access Manager uses the AzureAD graph API – which works exclusively in HTTPS.

The API base path is : "https://graph.windows.net/{tenant_domain_name}Where the tenant domain name is the customer assigned domain name on Microsoft cloud. It is usually in the format of domain_name.onmicrosoft.com, but might be changed in your configuration.

A list of resources that are accessed by File Access Manager using the REST graph API include:

https://graph.windows.net/{tenant_domain_name}/tenantDetails

https://graph.windows.net/{tenant_domain_name}/ users

https://graph.windows.net/{tenant_domain_name}/ users/{user_id}

https://graph.windows.net/{tenant_domain_name}/ groups/{group_id}

https://graph.windows.net/{tenant_domain_name}/ directoryRoles

https://graph.windows.net/{tenant_domain_name}/ directoryRoles/{role_id}

OneDrive Connector Installation Flow Overview

To install the OneDrive connector:

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

> OneDrive 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.

Adding a New OneDrive Application

In order to integrate with OneDrive, 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

OneDrive for Business

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 ManagerFile 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**. to open the Connection Details page.

Connection Details

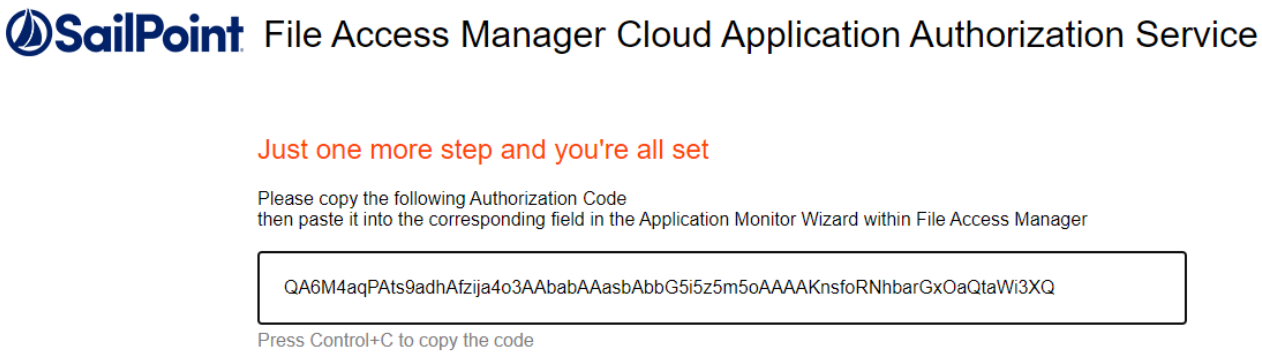
OneDrive access requires an authorization code from OneDrive. Follow the link provided to receive a fresh code and paste it in the OneDrive authorization code field.

Tenant Domain Name

The name of the Azure domain is typically part of the OneDrive URL address

OneDrive Authorization Page

Click this link to open the OneDrive Authorization page. Log in to open the File Access Manager Cloud Application Authorization Service page. Copy the authorization code.



OneDrive Authorization Code

Paste in the authorization code from the previous step

O365 Management Authorization Page

Click this link to get the O365 Management Authorization Code

O365 Management Authorization Code

Paste in the authorization code from the previous step

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 File Access Manager Administrator Guide for further details.

Analyze Files with Unique Permissions

Application type(s): OneDrive

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 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]\$($|)).*

> 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*

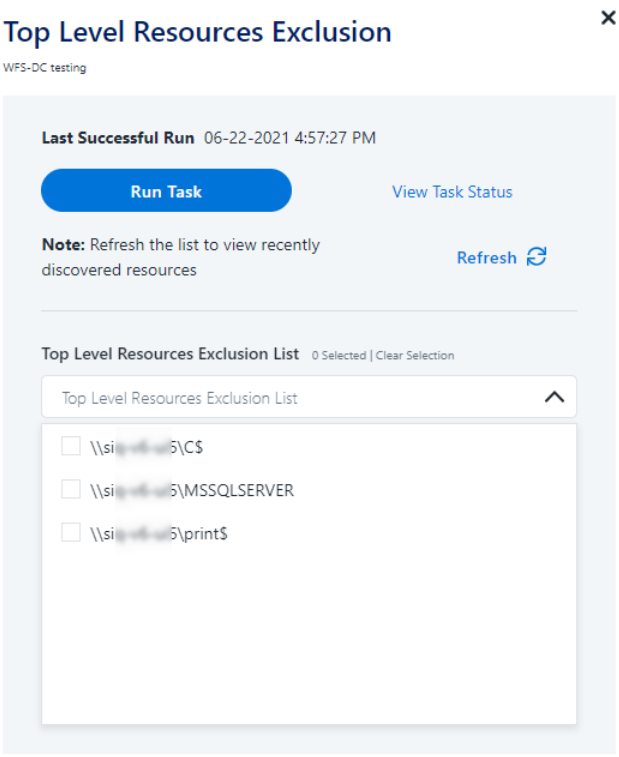
   > This will only work if the user has access to the task page

   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.

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**.

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>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

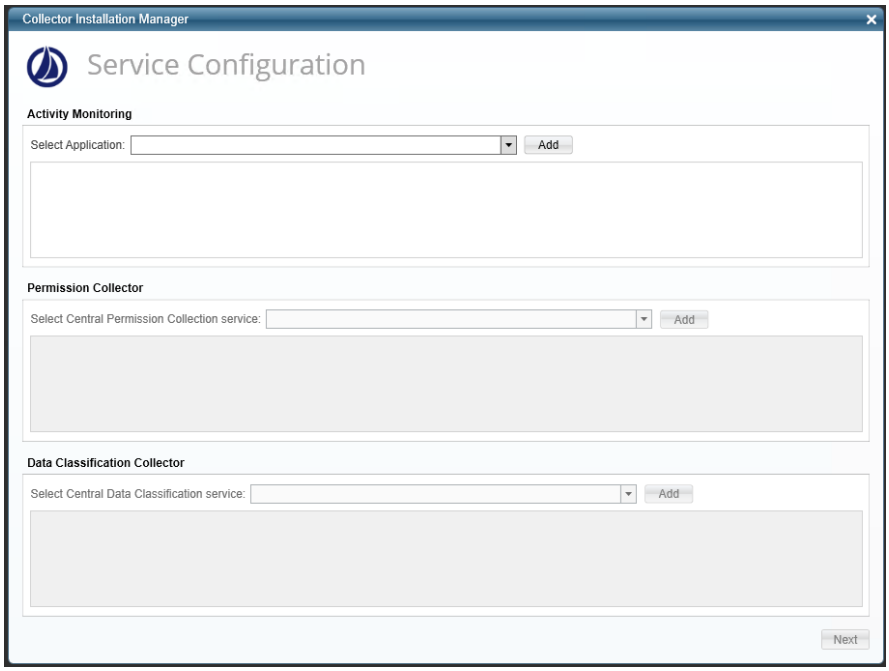
The activity monitor is installed per application, collecting activity logs.

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 OneDrive 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 Application - <Service Name>
- File Access Manager Central Data Classification - <Service Name>

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%\OneDrive-<Application_Name>.log"

Monitored Activities

1. Simulate activities on OneDrive.
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*)

Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

Accounts do not Appear in the Resources Tree

There are several reasons why the crawler might not identify all or part of the accounts, which would cause OneDrive accounts to either not appear in the resources tree, or appear only partially:

Uninitialized OneDrive accounts

These are accounts which were never accessed and activated.

These accounts can't be crawled, nor will they appear in the resources tree.

In the Crawl task details, you will see the following summary message :

Not initialized accounts: X (see logs for details)

(X stands for the number of uninitialized accounts)

Inaccessible OneDrive accounts

These are accounts which were not granted the prerequisites Site Collection Administrator permissions and cannot be accessed.

In the Crawl task details, you will see the following summary message

Not accessible accounts: X (see logs for details)

(X stands for the number of uninitialized accounts)

Partial Folder Structure For a OneDrive Account.

These are the hardest problem to troubleshoot.

It can happen when there is at least 1 publicly shared object (either a folder or file) under the OneDrive account, which makes it possible for external users to crawl it, but only the publicly shared objects will be returned. No error message is logged for these accounts, and you should verify that the required Site Collector Administrator permissions were granted.