



Integrating SharePoint Online 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

Contents	iii
Capabilities	5
Supported Versions	5
Connector Overview	6
Activity Monitor Operation Principles	6
Monitored Activities	6
Permissions Collection Operation Principles	6
Microsoft Teams Support	7
Prerequisites	8
Software Requirements	8
OAuth Support	8
Permissions	9
Communications Requirements	10
Azure Active Directory Connectivity Requirements	10
SharePoint Online Connector Installation Flow Overview	11
Collecting Data Stored in an External Application	12
Adding a SharePoint Online Application	13
Select Wizard Type	13
General Details	13
Connection Details	14
Configuring and Scheduling the Permissions Collection	14
Configuring Activity Monitoring	21
Configuring Data Enrichment Connectors	22
Installing Services: Activity Monitor Collector	23
Verifying the SharePoint Online Connector Installation	25
Installed Services	25
Log Files	25
Monitored Activities	25

Permissions Collection25

Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in SharePoint Online 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.

Supported Versions

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

Connector Overview

Activity Monitor Operation Principles

- File Access Manager Activity Monitor for SharePoint Online uses the Microsoft Office365 Management Activity API.
- The Activity Monitor queries the API for SharePoint events, which discards OneDrive for Business related 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 SharePoint Online 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 SharePoint Online Activity Monitor (This is due to 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

CSOM

File Access Manager SharePoint Online permissions collection and crawling uses SharePoint Client-Side Object Model (CSOM).

Azure Identity Collector

The permissions collection task queries SharePoint Online 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.

Crawl level: Folder vs File

By default, permissions are analyzed to the folder level, but they can also be analyzed on the file level. If permissions are analyzed on the file level, the system will only display uniquely managed files in the Business Resource Tree.

[Adding a NetApp Application](#) describes how to analyze file level permissions.

The section on “Identity collection” in the *File Access Manager Administrator Guide* provides more information on how to define an Azure Identity Collector.

Microsoft Teams Support

The SharePoint Online connector supports gathering permissions, monitoring activities, and classifying information being stored in Teams sites and channels.

Files transferred through Teams chats are viewable under the Team site > **Shared Documents** > **General**.

Files transferred through private chats are placed under the initiating user's OneDrive for Business Personal Drive and are managed by the File Access Manager OneDrive for Business Application.

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](#).

OAuth Support

File Access Manager offers full support of standard OAuth 2.0 Authentication for the SharePoint Online connector.

The new authorization sequence will direct the user through a standard Microsoft O365 consent flow, to grant the File Access Manager SharePoint Online Connector application the privileges to acquire and refresh access tokens.

- The SharePoint Online Connector now uses only fully modern authentication methods, and does not require Legacy Authentication methods be enabled, tenant-wide, or otherwise.
- The SharePoint Online Connector supports any user as a delegated account (the granting account), including users with Multi-Factor Authentication requirements enabled, and is no longer limited by Microsoft's restrictions on Federated Accounts.
- The SharePoint Online Connector supports internal token management and will be responsible for managing and renewing its own tokens.
- The SharePoint Online Connector now supports the use of multiple service accounts, for the Permission Collection, Data Classification and Activity Monitoring modules, to utilize larger API access quotas and minimize delays caused by Microsoft O365 Rest APIs quotas, throttling and back-off algorithms.
- As part of this change, the OneDrive Connector's support for file-level permissions analysis, no longer requires user and password credentials and will be using the existing OneDrive OAuth token instead.

This enhancement brings full OAuth support to the SharePoint Online Connector, instead of the legacy user and password approach.

File Access Manager uses the Authorization Code Token Acquisition flow, to generate and refresh OAuth tokens.

This means the configuration will resemble other connectors for cloud applications such as OneDrive.

- Configuring the SharePoint Online Application, instead of providing a user-name and a password, you will first fill in the tenant domain name, and then click on the plus sign next to the relevant token you would like to generate. You will then be directed to a Microsoft login page.
- Enter the relevant user credentials and give your consent for the File Access Manager SharePoint Online O365 Application to access your tenant's SharePoint Online data.
- You will then be redirected to receive a new Authorization Code.
- Copy the resulting authorization code, paste it to the Authorization Code pop-up, and click Done.
- The access token will be used in all requests to the tenant's SharePoint Online environment and will be automatically refreshed when needed.
- There are four (4) required Access Tokens, and you must follow the token acquisition process for each.

These tokens are used to access different resources on the tenant's SharePoint Online environment.

- **The General SharePoint Online token** – is used for accessing all site collections and contained data.
- **The SharePoint Online Admin token** – is used for accessing the administrative site collection ({TenantDomain}-admin.sharepoint.com) and fetching the list of top-level site-collections.
- **The SharePoint Online “My” token** – is used for accessing the site-collections underlying the OneDrive environment ({TenantDomain}-my.sharepoint.com).
- **The O365 Management API token**– is used for Activity Monitoring and fetching activity data from the O365 Management API. All Tokens are required.

Multiple service accounts can be used to generate tokens for all token categories.

- The same service accounts can be used for all modules. However, it is important to note that API call quotas are user/service-account based and will be shared.
- To reduce the likelihood of exceeding the API call quotas and encountering throttling issues, it is recommended to use multiple service-accounts (at least 4) in each token category and use a separate set of service-accounts for Activity Monitoring.

Existing SharePoint Online applications will need to be reconfigured and go through the configuration wizard to generate access tokens to switch over to the modern authentication flow.

This will not recreate the SharePoint Online application, and all current SharePoint Online information will remain intact.

Permissions

Activity Monitor

To access to the Office365 Management Activity API, configure a user by going through the OAuth authorization process.

The OAuth authorization process must be executed by the Tenant Administrator of the Azure/Office365 domain. The user needs to grant consent to the SailPoint SecurityIQ Office365 Application to access the domain’s activity data.

The global Tenant Administrator is needed only for the activity monitoring service.

Permissions Collection

To perform crawl and permissions collection, the user must be assigned a “SharePoint administrator” role.

It is a built-in role for any Azure domain that includes any SharePoint online plan. This role grants the permission to list all existing Site Collections.

The configured user must also be assigned as a Site Collection Owner for each Site Collection that needs to be analyzed for permissions.

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	SharePoint Online	https
Activity Monitoring	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://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 SharePoint Online 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}`

SharePoint Online Connector Installation Flow Overview

To install the SharePoint Online connector:

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

SharePoint Online 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 SharePoint Online Application

In order to integrate with SharePoint Online, 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

SharePoint Online

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 Manager 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**. to open the Connection Details page.

Connection Details

Tenant Name

The name of the Azure domain. Typically, this is the first part of the DNS name (e.g. http://my-company.sharepoint.com).

Fill in the tenant name, and save it by pressing the Save button to enable the authorization fields in the rest of this configuration page.

Fill in only the “my-company” part, do not include “sharepoint.com” or “onmicrosoft.com”.

SharePoint Online Authorization Code

Click the + to open OAuth authorization window. Log in to open the File Access Manager Cloud Application Authorization Service page. Copy the authorization code into the authorization code window.



Just one more step and you're all set

Please copy the following Authorization Code then paste it into the corresponding field in the Application Monitor Wizard within File Access Manager

QA6M4aqPAts9adhAfzija4o3AAbabAAasbAbbG5i5z5m5oAAAAKnsfoRNhbarGxOaQtaWi3XQ

Press Control+C to copy the code

Repeat with the appropriate accounts and access for the following authorization codes:

- **SharePoint Online Admin Authorization Code**
- **SharePoint Online My Authorization Code**
- **Management Authorization Code**

Analyze permissions on files?

This determines whether to display files that break permissions inheritance in the Business Resource Tree and analyze the permissions of those files.

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.

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 resources which start with one or more resource names:

Example: Starting with `https://www.mysharepoint.com/resourceName`

Regex: `https:\\www.mysharepoint.com\\resourceName$`

Example: Starting with `https://www.mysharepoint.com\\resourceName` or `//www.mysharepoint.com/OtherResourceName`

Regex: `https:\\www.mysharepoint.com\\(resourceName|OtherResourceName)$`

Example: SharePoint resources starting with `https://www.mysharepoint.com/sites/mySiteCollection`

Regex: `https:\\www.mysharepoint.com\\sites\\mySiteCollection$`

Example: SharePoint resources starting with

`http://www.mysharepoint.com/sites/mySiteCollection` or
`http://www.mysharepoint.com/other site/Different Site`

Regex: `https:\\www.mysharepoint.com\\(sites\\mySiteCollection|other_site\\Different_Site)$`

Include ONLY resources which start with one or more resources names:

Example: Starting with `https://www.mysharepoint.com/resourceName`

Regex: `^(?!https:\\www.mysharepoint.com\\resourceName($|V.*)).*`

Example: Starting with `https://www.mysharepoint.com/resourceName` or `https://www.mysharepoint.com/OtherResourceName`

Regex: `^(?!https:\\www.mysharepoint.com\\(resourceName|OtherResourceName)($|V.*)).*`

Example: SharePoint resources starting with `https://www.my-sharepoint.com/sites/mySiteCollection`

Regex: `^(?!https:\\\\www.mysharepoint.com\\sites\\mySiteCollection($|\\.*)).*`

Example: SharePoint resources starting with

`https://www.mysharepoint.com/sites/mySiteCollection` or

`https://www.mysharepoint.com/other site/Different_Site`

Regex: `^(?!https:\\\\www.mysharepoint.com\\(sites\\mySiteCollection|other_ site\\Different_Site)($|\\.*)).*`

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

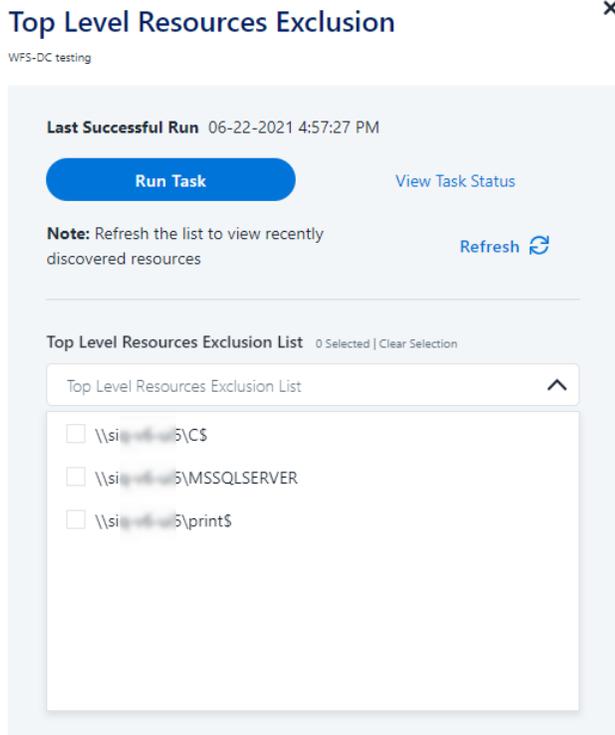
Settings > Task Management > Tasks

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.

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.

Mailbox Crawl Interval (min)

The interval for checking for newly created mailboxes in minutes, if working in Auto Learning Mode.

Monitor Admin Audit Activities

Admin audit activities on defined resources, such as mailboxes or public folders, will be associated with the resource. Other admin audit activities will be associated with a special resource named `'_Admin Audit'`.

Monitoring Exclusions

- To add an exclusion
 - Click the dropdown list
 - Type in an exclusion (file extension, user, folder, etc. as relevant)
 - Click the **+** icon to add this item to the list
 - After completing the list, click **Next** or **Cancel** to close the panel

- To edit or remove an exclusion from the list

Click the dropdown list

On the extension to edit or remove click the delete or edit icon

click **Next** or **Cancel** to close the panel

- Click **Clear Selection** to clear the entire list

Excluded File Extensions

List of file extensions that are not monitored. e.g. : txt, exe

Enter one value at a time as described above

Exclude Folders

List of folders that are not monitored

Exclude Users

List of users whose activities are not monitored

Each excluded user must be in the form of Domain\User.

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.

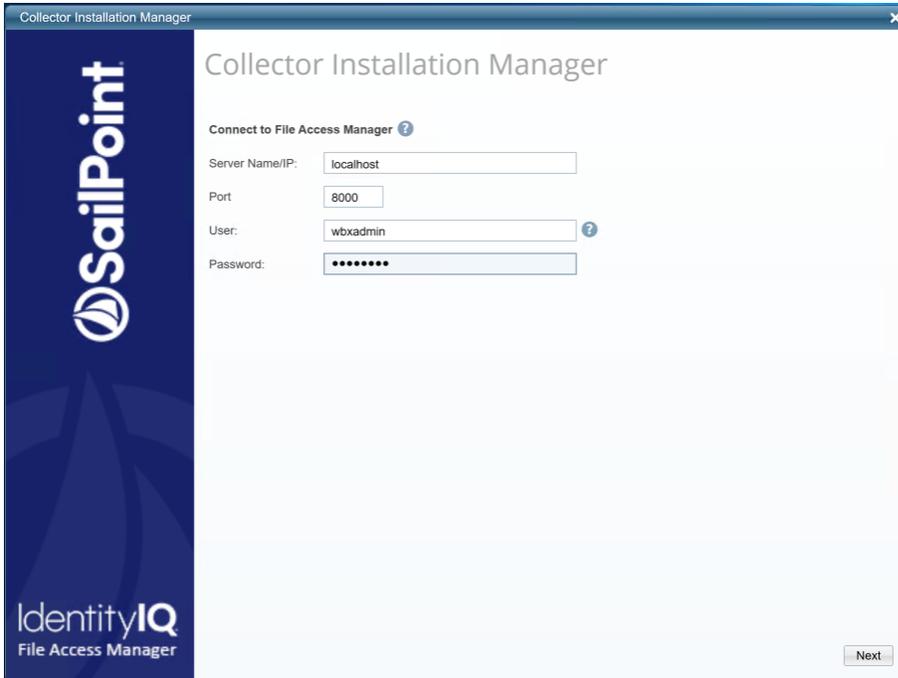
Installing Services: Activity Monitor Collector

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

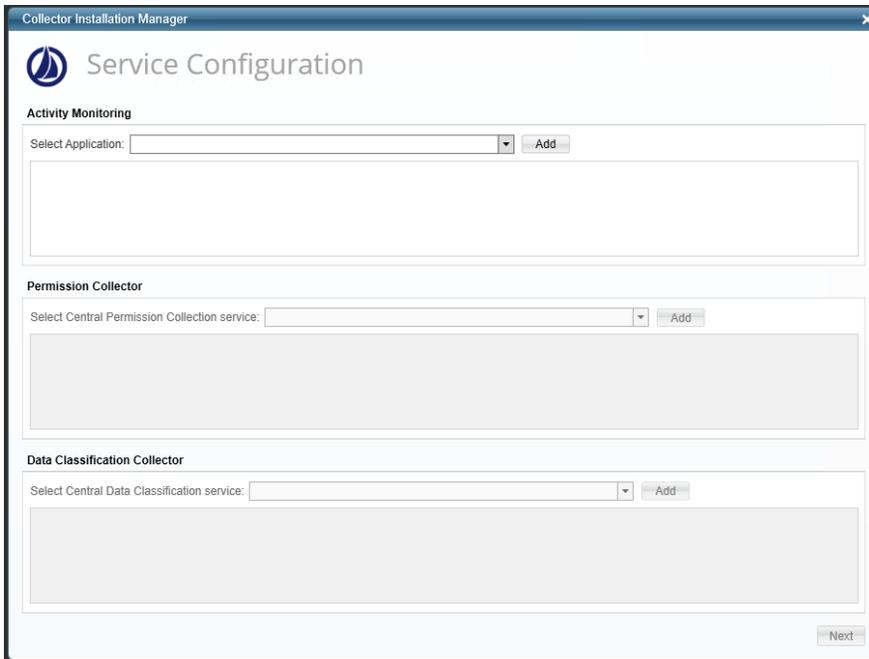
Install the activity monitor using the Collector Installation Manager. This tool is part of the File Access Manager installation package.

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 SharePoint Online 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 Activity Monitor - <Application_Name>
- File Access Manager Central Permissions Collection - <Application_Name>
- File Access Manager Central Data Classification - <Application_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%\SharePointOnline-<Application_Name>.log"

Monitored Activities

1. Simulate activities on SharePoint Online.
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*)