Integrating OneDrive with File Access Manager

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 6.0.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 6.0.x Hosting Bundle version from here .

Creating an Azure Application for OneDrive

A new Azure Active Directory application must be created and configured to support the File Access Manager OneDrive functionality.

This configuration can be performed either by running the automated PowerShell script supplied with the SailPoint distribution pack, or by creating and configuring the application through the Azure portal.

Creating and Configuring the Application Automatically

There is a PowerShell script named **CreateSharePointOnlineAndOneDriveApp.ps1** provided in the **Collectors.zip** under the extracted scripts sub-folder. This script will perform all the Azure application creation and configuration steps required for OneDrive.

To run this script, the Azure AD PowerShell module must be installed.

```
Install-Module -Name AzureAD
```

Before running the script, open the file in a text editor to review the default parameters. The parameters can be edited in the file or passed as parameters when running the script.

To run the script with the default parameters:

```
.\CreateSharePointOnlineAndOneDriveApp.ps1
```

To run the script while overriding some of the default parameters:

```
.\CreateSharePointOnlineAndOneDriveApp.ps1 -AppName "OneDrive FAM App" -CertDnsName
"contoso.com" -CertYearsValid 15
```

When prompted, log in with administrator credentials to create and configure Azure applications. The last step of the script will launch a URL to grant admin consent for the application. After granting consent, the page will redirect to a missing localhost URL. The operation is successful if the URL for that page contains **admin_consent=True**.

> If you experience an access denied error or other error in the web browser when granting admin consent, this might be a timing issue. This can be resolved by either manually granting admin consent through the Azure portal (see section Grant admin consent manually), or by copying and pasting the consent URL (represented in the line from the script output that starts in "Consent URL: ") into your browser.
>
> The following output should be gathered or noted when running the script. This information will be used to configure the OneDrive application in File Access Manager:
>
> 1. The App ID value in the console output.
> 2. The created certificate file <AppName>.pfx located in your working directory.
> 3. The certificate password that was entered when prompted.

Creating and Configuring the Application Manually

The following steps will create and configure an Azure application for OneDrive authentication through the Azure portal.

These steps are adapted from the following online Microsoft documentation:

https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/security-apponly-azuread

Step 1: Register the Application in Azure AD

1. Open the Azure AD portal at https://portal.azure.com

2. Under Manage Azure Active Directory, select **View**.

3. On the Overview page that opens, under Manage, select **App registrations**.

4. On the App registrations page that opens, select **New registration**.

5. On the Register an application page that opens, configure the following settings:

   Name

     Enter something descriptive. For example, OneDrive FAM App

   Supported account types

     Verify that Accounts in this organizational directory only (<YourOrganizationName> only - Single tenant) is selected.

Redirect URI (optional)

Leave empty

6. When you're finished, click **Register**.

> Leave the app page open. You'll use it in the next step.

Step 2: Assign API Permissions to the Application

1. On the app page under Manage, select **Manifest**.

2. On the Manifest page that opens, find the requiredResourceAccess entry.

3. Replace the entire requiredResourceAccess entry with the following:

```
"requiredResourceAccess": [
    {
        "resourceAppId": "c5393580-f805-4401-95e8-94b7a6ef2fc2",
        "resourceAccess": [
            {
                "id": "594c1fb6-4f81-4475-ae41-0c394909246c",
                "type": "Role"
            }
        ]
    },
    {
        "resourceAppId": "00000003-0000-0ff1-ce00-000000000000",
        "resourceAccess": [
            {
                "id": "678536fe-1083-478a-9c59-b99265e6b0d3",
                "type": "Role"
            }
        ]
    }
],
```

4. Click **Save**.

5. On the Manifest page, under Manage, select **API permissions**.

6. On the API permissions page that opens, verify that both Sites.FullControl.All and ActivityFeed.Read appear on the list.

7. Select **Grant admin consent for <Organization>**, read the confirmation dialog that opens.

8. Click **Yes**. The Status value should now be Granted for <Organization> on both entries.

9. Close the current API permissions page (not the browser tab) to return to the App registrations page. You will use it in an upcoming step.

Step 3: Generate a Self-Signed Certificate

Create a self-signed x.509 certificate using the following PowerShell commands.

Edit parameters such as DnsName, Certificate expiration, and password as appropriate:

Create certificate

$mycert = New-SelfSignedCertificate -DnsName "contoso.org" -CertStoreLocation "cert:\LocalMachine\My" - NotAfter (Get-Date).AddYears(15) -KeySpec KeyExchange

Export certificate to .pfx file

$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $(ConvertTo-SecureString -String "P@ss- w0Rd1234" -AsPlainText -Force)

Export certificate to .cer file

$mycert | Export-Certificate -FilePath mycert.cer

Step 4: Assign the Certificate to the Azure Active Directory Application

After you register the certificate with your application, you can use the private key (.pfx file) for authentication.

1. If you need to get back to the Apps registration page:

    a. Open the Azure AD portal at https://portal.azure.com/

    b. Under Manage Azure Active Directory, select View.

    c. On the Overview page that opens, under Manage, select **App registrations**.

2. On the Apps registration page from the end of Step 2, select your application.

3. On the application page that opens, under Manage, select **Certificates & secrets**.

4. Click **Upload Certificate**.

5. Browse to the self-signed certificate (.cer file) that you created in Step 3.

6. Click **Add**. The certificate is now shown in the Certificates section.

7. Close the current Certificates & secrets page, and then the App registrations page to return to the main https://-portal.azure.com page. You'll use it in the next step.

Permissions

Activity Monitor

To perform Activity Monitoring, the Azure AD application for SharePoint Online requires the ActivityFeed.Read permission to access the Office 365 Management APIs.

Permissions Collection

To perform crawl and permissions collection, the Azure AD application for SharePoint Online requires the Sites.FullControl.All permission to access the SharePoint APIs.

Communications Requirements

Requirement	Source	Destination	Port
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
OAuth Access Token Acquisition	Permission Collector/Data Classification Collector/Activity Monitor	Microsoft Token Endpoint	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://login.microsoftonline.com/* - for OAuth access token acquisition.

Azure Active Directory Connectivity Requirements

The OneDrive Connector requires an AzureAD Identity Collector.

File Access Manager uses the Microsoft Graph REST API – which works exclusively in HTTPS.

The API base path is: https://graph.microsoft.com/v1.0/, 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 different 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

Complete the Connection Details fields:

Initial Domain Name

The Initial Domain Name that was given when the Azure tenant was initially created can be found in **Microsoft 365 admin center > Settings > Domains**.

It can be identified by its .onmicrosoft.com suffix and that it cannot be deleted.

Application ID

Enter the Application ID for the Azure application used by the File Access Manager SharePoint Online Connector.

Certificate File

The certificate assigned to the Azure application used by the File Access Manager SharePoint Online Connector.

Either navigate to the certificate by clicking on Choose a File or drag the certificate onto the Certificate File Path field.

Supported file formats: pfx, p12.

Certificate Password

Enter the password for the certificate

> When editing this application, if a new certificate is uploaded, then the former password cannot be used. The user has to provide a new password.

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.

> If using a proxy in your File Access Manager environment, see How to Use Proxy in a File Access Manager Environment in the Azure File Guide.

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 drives which start with one or more user names:

Starting with John.Doe:

Regex: ^Personal\/John\.Doe@.*

Starting with John.Doe or Jane.Doe

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

Include ONLY drives which start with one or more user names:

Starting with John.Doe
Regex: ^(?!Personal\/John\.Doe@.*).*
Starting with John.Doe or Jane.Doe
^(?!Personal\/(John|Jane)\.Doe@.*).*

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**.

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 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.

Activity Data Retention Period

> By default, this feature is disabled.

When selecting the Clear Activity Data option, a user is able to provide a time frame (1 to 100) in either months or years for all activity to be retained. Once that time period is met, all data will be removed.

A user can also select to backup the data before it is deleted by selecting the Backup Events Before Clearing option.

> The Backup Before Clearing Option will only be enabled if the backup option is set during the system installation. If a user has not selected the backup option during the installation nor provided a backup path, this option will not be enabled.

Activity Data Retention Period

Activity data will be retained for the specified period. Following that time period, activities will be cleared.

✅ Clear Activity Data

How long do you want to keep activity data? *

| 12 | ⬍ | | Month(s) | ⌄ |

Check this option to backup activity data before it is cleared.

✅ Backup Events Before Clearing

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(Applic-
ations>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 Enrich-
ment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

Installing Services: Activity Monitor and Collectors

The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

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.
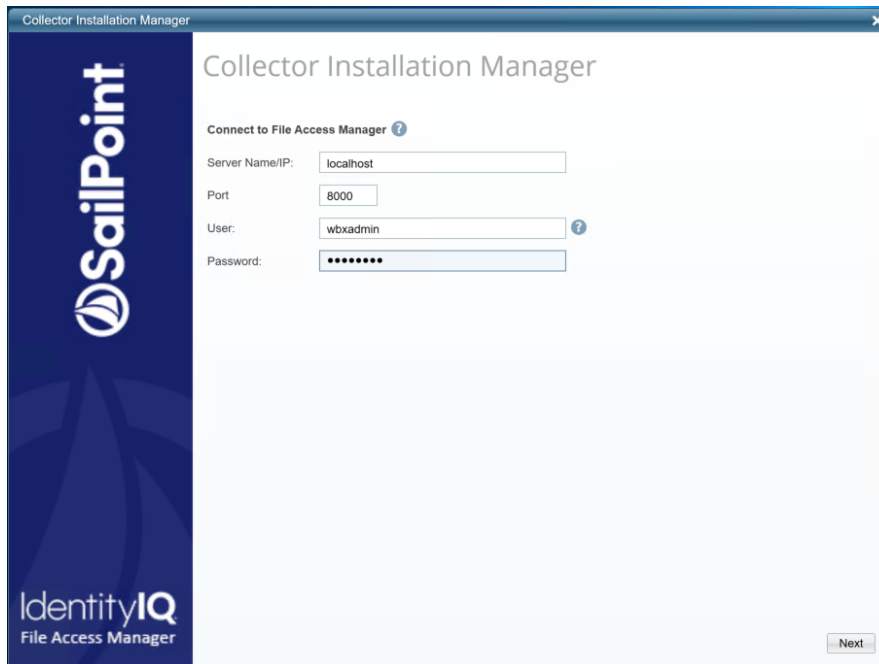
2. Enter the credentials to connect to File Access Manager.

   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**.

   The Service Configuration window displays.

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

5. When installing a SharePoint Activity Monitor, you will be prompted for service account credentials. This service account will be used by the Activity Monitor service to run the service and authenticate against the SharePoint IIS servers to fetch the logs ("Log on as"). Make sure the service account provided has local administrator privileges on the local server (hosting the Activity Monitor service) and can access the activity logs on the IIS servers.

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

7. If you are installing the Data Classification, select the Central Classification Collector to which to connect this service, and click **Add**.

8. Click **Next**.

   The Installation Folder window displays.

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

9. Browse and select the location of the target folder for installation.

10. Browse and select the location of the folder for system logs.

11. Click **Next**.

12. The system begins installing the selected components.

13. 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

Verifying Application Configuration

After the configuration of one of the following applications is complete, verify it was properly configured by running the Test Connection task.

The Test Connection will run and validate a series of validations to see if the application was configured correctly.

Common OneDrive Validations

The following is a list of common validations that run when the test connection is run with a OneDrive application.

- Server responsiveness

- Verifying the connectivity to the OneDrive API

- Verifying the permissions to read file data through the API

- Verifying the event auditing is active through Office 365 API

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.