Integrating Exchange Online with File Access Manager

Version: 8.3 Revised: March 30, 2022

Contents

Contents ... **iii**

Capabilities ... **5**

Exchange Online Connector OAuth 2.0 Support ... 5

Connector Overview ... **6**

Permissions Collection Operation Principle ... 6

Mailbox Audit ... 6

Monitored Activities ... 6

Admin Audit Events (Administrator Audit Logging) ... 7

Prerequisites ... **9**

Software Requirements ... 9

Creating an Azure Application for Exchange Online ... 9

Creating and Configuring the Application Automatically ... 9

Creating and Configuring the Application Manually ... 10

Step 1: Register the Application in Azure AD ... 10

Step 2: Assign API Permissions to the Application ... 10

Step 3: Generate a self-signed certificate ... 11

Step 4: Attach the Certificate to the Azure AD Application ... 12

Step 5: Assign Azure AD role to the application ... 12

Permissions ... 13

Audit Bypass ... 13

Audit Age Log Limit ... 13

Communications Requirements ... 13

Exchange Online Connector Installation Flow Overview ... **15**

Collecting Data Stored in an External Application ... **16**

Exchange Online Connector Installation Flow Overview ... 16

Adding an Exchange Online Application ... **18**

Select Wizard Type ... 18

General Details ... 18

Connection Details 19
Configuring and Scheduling the Permissions Collection 19
Selecting and Scheduling the Data Classification Settings 26
Data Privacy 27
Configuring Activity Monitoring 27
Configuring Data Enrichment Connectors 27
Installing Services: Activity Monitor Collector 28
Verifying the Exchange Online Connector Installation 30
Installed Services 30
Log Files 30
Monitored Activities 30
Permissions Collection 30

Capabilities

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

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

See the File Access Manager documentation for a full description.

Exchange Online Connector OAuth 2.0 Support

- The connector uses fully Modern Authentication methods, and does not require Legacy Authentication methods be enabled, tenant-wide, or otherwise.

Connector Overview

Access to Exchange Online is based on Microsoft Exchange Online PowerShell API capabilities.

Audit types include:

- Mailbox Access Audit
  - Administrators who access other users' mailboxes
  - Users who access other users' mailboxes as delegates
- Administrator Audit PowerShell Cmdlets (every Set-* PowerShell is audited)

Permissions Collection Operation Principle

The File Access Manager Connector connects using the PowerShell interface and analyzes mailboxes, folders, public folders, and their permissions.

Mailbox Audit

1. Mailbox audit events are assigned to the relevant mailbox business resource.
2. The list of monitored mailbox types can be found in the `BAMFramework.exe.config` file under the *recipientTypeDetailsToMonitor* setting.

By default, the following types are defined and monitored:

UserMailbox

SharedMailbox

> Additional mailbox types can be added to this list, for reference follow this link.

Monitored Activities

Action	Description	Admin	Delegate	Owner
Copy	An item is copied to another folder.	Yes	Yes	No
Create	An item is created in the mailbox. (For example, a message is sent or received.) Note that folder creation isn't audited.	Yes	Yes	Yes
FolderBind	A mailbox folder is accessed.	Yes	Yes	No
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes	Yes	Yes
MessageBind	An item is accessed in the reading pane or opened.	Yes	No	No
Move	An item is moved to another folder.	Yes	Yes	Yes
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes	Yes	Yes

Action	Description	Admin	Delegate	Owner
SendAs	A message is sent using Send As permissions.	Yes	Yes	N/A
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes	Yes	N/A
SoftDelete	An item is deleted from the Deleted Items folder.	Yes	Yes	Yes
Update	An item's properties are updated.	Yes	Yes	Yes

Admin Audit Events (Administrator Audit Logging)

File Access Manager features the following Admin audit events:

1. General Admin audit events are assigned to a special resource (*Audit Admin*).
2. Admin audit events that relate to a specific mailbox are assigned to the mailbox business resource.
    - The list of commands can be found in the framework configuration file in the *mailboxAuditLogCmdLets* setting.

      For Exchange: The config file is WBX.Exchange2010BAMHost.dll.config

      For Exchange Online it is WBX.ExchangeOnlineBAMHost.dll.config
    - By default, the following are defined as mailbox commands:
        - Remove-Mailbox
        - New-Mailbox
        - Set-Mailbox
        - Add-MailboxPermission
        - Remove-MailboxPermission
        - Set-MailboxAutoReplyConfiguration
3. Admin audit events related to a specific mailbox folder are assigned to the mailbox folder business resource.
    - The list of commands can be found in the BAMFramework.exe.config file in the *mailboxFolderAuditLogCmdLets* setting.
    - By default, the following are defined as mailbox folder commands:
        - Add-MailboxFolderPermission
        - Remove-MailboxFolderPermission
        - Set-MailboxFolderPermission
4. Admin audit events related to a specific public folder are assigned to the public folder business resource.
    - The list of commands can be found in the BAMFramework.exe.config file in the *publicFolderAuditLogCmdLets* setting.
    - By default, the following commands are defined as public folder commands:

- Add-PublicFolderClientPermission
- Remove-PublicFolderClientPermission
- New-PublicFolder
- Remove-PublicFolder
- Add-PublicFolderAdministrativePermission
- Remove-PublicFolderAdministrativePermission

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 .

Creating an Azure Application for Exchange Online

A new Azure application must be created and configured to support the File Access Manager Exchange Online 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 **CreateExchangeOnlineApp.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 Exchange Online.

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:

```
.\CreateExchangeOnlineApp.ps1
```

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

```
.\CreateExchangeOnlineApp.ps1 -AppName "Exchange Online FAM App" -DirectoryRole
"Exchange Administrator" -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. This can be ignored.

> 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 (the last line of output from the script output that contains text “adminconsent”) into your browser.

> The following output should be gathered or noted when running the script. This information will be used to configure the Exchange Online 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 Exchange Online authentication through the Azure portal.

> These steps are adapted from the following online Microsoft documentation:
>
> https://docs.microsoft.com/en-us/powershell/exchange/app-only-auth-powershell-v2?view=exchange-ps#set-up-app-only-authentication

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**, click **View**.
3. On the **Overview** page that opens, under **Manage**, select **App registrations**.
4. On the **App registrations** page that opens, click **New registration**.
5. On the Register an application page that opens, configure the following settings:

   Name

   Enter something descriptive. For example, Exchange Online 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 (on or about line 44).
3. Modify the **resourceAppId**, **resourceAccess**, **id**, and **type** values as shown below:

```
"requiredResourceAccess": [
   {
      "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
      "resourceAccess": [
         {
            "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
            "type": "Role"
         }
      ]
   }
],
```

4. Click **Save**.
5. On the **Manifest** page, under **Manage**, select **API permissions**.
6. **Grant admin consent manually**

   On the **API permissions** page that opens, do the following:

   API / Permissions name

   Verify the value **Exchange.ManageAsApp** is shown.

   Status

   The initial value is Not granted for <Organization>.

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

   Click **Yes**.

   The Status value should now be **Granted for <Organization>**.
7. Close the current API permissions page (not the browser tab) to return to the App registrations page. You'll 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: Attach the Certificate to the Azure AD Application

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

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

   If you need to get back to Apps registration page

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

   b. Under **Manage Azure Active Directory**, click **View**.

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

2. On the application page that opens, under **Manage**, select **Certificates & secrets**.
3. Click **Upload Certificate**.
4. Browse to the self-signed certificate (.cer file) that you created in Step 3.
5. Click **Add**.

   The certificate is now shown in the Certificates section.

6. 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.

Step 5: Assign Azure AD role to the application

The following admin roles are available. Each of these roles has the necessary permissions for File Access Manager functionality. Choose a role and assign the new Azure Application to it to complete the configuration.

- Global administrator
- Compliance administrator
- Exchange administrator

1. Open the Azure AD portal at https://portal.azure.com/
2. Under **Manage Azure Active Directory**, click **View**.
3. On the **Overview** page that opens, under **Manage**, select **Roles and administrators**.
4. Find and select one of the supported roles by clicking on the name of the role (not the check box) in the results.
5. On the Assignments page that opens, click **Add assignments**.
6. In the **Add assignments** flyout that opens, find and select the app that you created in Step 1.
7. Click **Add**.
8. Back on the Assignments page, verify that the app has been assigned to the role.

Permissions

- The Office365 Exchange Online service uses a similar permission model as the equivalent Exchange On-Premises.

Audit Bypass

The File Access Manager Connector for Exchange Online sets the mailbox audit for the selected mailboxes according to the configuration in the Application. However, there are application service accounts (for example, BlackBerry or IXOS) which create many mailbox audit log entries that overload the Exchange and create a lot of noise in File Access Manager.

You can configure a user or computer account to bypass mailbox audit logging, so that actions taken by that user or account for any mailbox are not logged.

By bypassing a trusted user or computer accounts that require frequent access to mailboxes, you can reduce the noise in mailbox audit logs.

For more information, see:

https://technet.microsoft.com/en-us/library/ff461934%28v=exchg.150%29.aspx

> It is recommended to set an alert on bypass commands to verify that users are not bypassed unexpectedly.

Audit Age Log Limit

By default, audit logging is configured to store audit log entries for 90 days.

After 90 days, the audit log entry is cycled. You can change the audit log age limit using the *Set-Mailbox cmdlet with the AuditLogAgeLimit* parameter.

You can specify the number of days, hours, minutes, and seconds to retain audit log entries.

Logs need not be retained for a long time (more than a few days), since File Access Manager offloads the data from the exchange.

> It is not recommended to retain an audit for a long time, since doing so expands the Exchange DB.

The following site provides more information:

https://technet.microsoft.com/en-us/library/bb123981%28v=exchg.150%29.aspx

Communications Requirements

Communications Requirements

Requirement	Source	Destination	Port
File Access ManagerMessage Broker	Permissions Collector Server	RabbitMQ	5671
File Access ManagerAccess	Activity Monitor and Permissions Collector servers	File Access Manager Servers	8000-8008

Requirement	Source	Destination	Port
Remote PowerShell	Activity Monitor/Permissions Collector server	Office 365 Cloud	80 or 443

Exchange Online Connector Installation Flow Overview

To install the Exchange Online connector:

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

> Exchange 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 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 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.

Exchange Online Connector Installation Flow Overview

To install the Exchange Online connector:

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

> Exchange 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.

Adding an Exchange Online Application

In order to integrate with Exchange 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

Exchange 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 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:

Tenant Domain Name

Use your company name as registered in Azure. Otherwise, fill in the full DNS name of a custom domain name. e.g., company_name.com.

Application ID

Enter the Application ID for the Azure Application used by the File Access Manager Exchange Online Connector

Certificate File Path

Either navigate to the certificate by pressing Chose 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

Click **Next**.

Configuring and Scheduling the Permissions Collection

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

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

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

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

To configure the Permission Collection

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

  The actual entry fields vary according to the application type.

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

Central Permissions Collection Service

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

Calculate Effective Permissions

Calculate effective permissions during the permissions collection run

Calculate Riskiest Permissions

Calculates the riskiest permission on a resource – for example, Full Control is riskier than Read permissions if both are on a resource.

This option is available when selecting **Calculate Effective Permissions**

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.

Crawl Mailboxes, Crawl Public Folders

Select the types of folders to scan.

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 Public Folders\\shareName

Regex: Public Folders\\\\shareName$

Starting with Public Folders\\shareName or Public Folders\\OtherShareName

Regex: Public Folders\\\\(shareName|OtherShareName)$

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

Starting with Public Folders\\shareName

Regex: ^(?!Public Folders\\\\shareName($|\\.*)).*

Starting with Public Folders\\shareName or Public Folders\\OtherShareName

Regex: ^(?!Public Folders\\\\(shareName|OtherShareName)($|\\.*)).*

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

Regex: : ^(?!\\\\Public Folders\\shareName\$($|\\folderA$|\\folderA\\.*)).*

Exclude all mailboxes that start with one or more user names:

Starting with John.Doe

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

Starting with John.Doe or Jane.Doe

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

Include ONLY mailboxes that start with one or more user names:

Starting with John.Doe

Regex: ^(?!Mailboxes\/John\.Doe@.*).*

Starting with John.Doe or Jane.Doe

Regex: ^(?!Mailboxes\/(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*

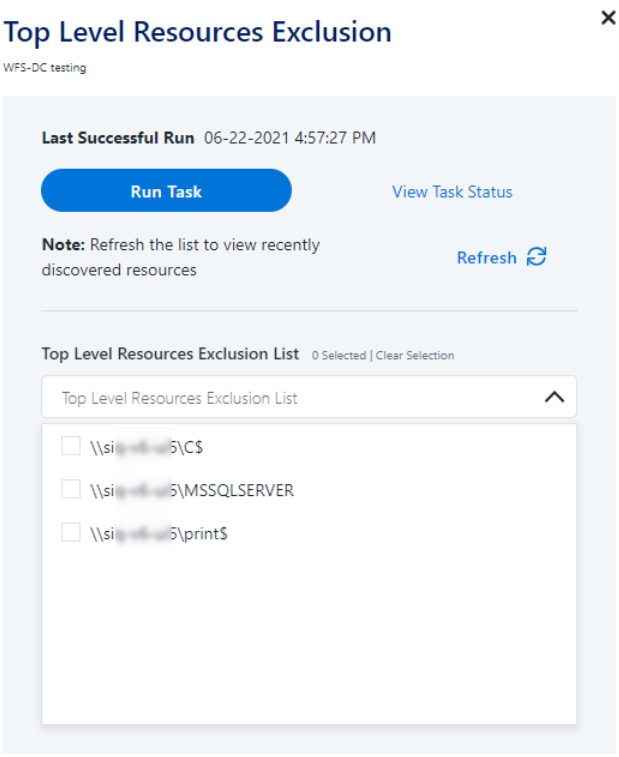
   > This will only work if the user has access to the task page

   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.

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

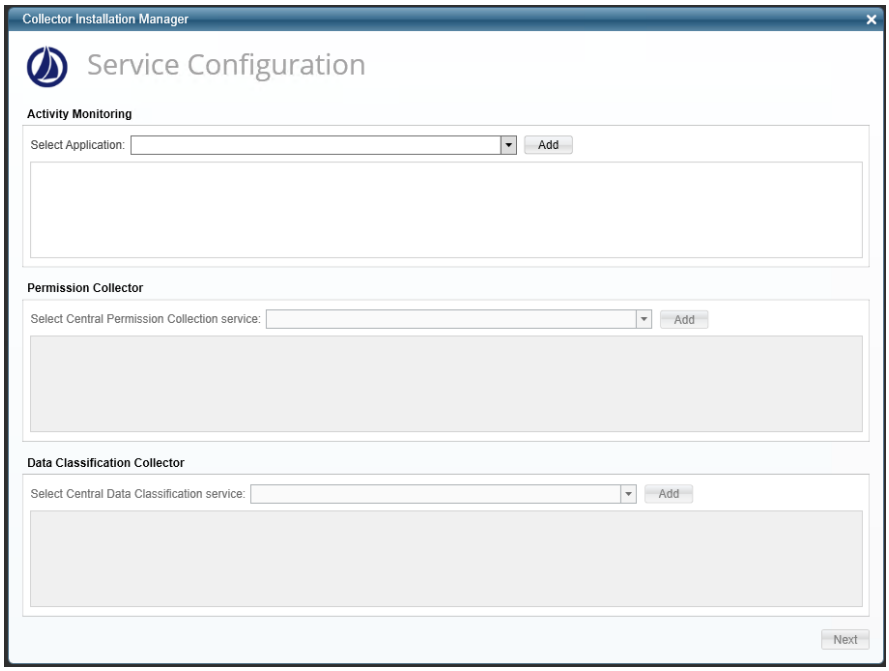
The activity monitor is installed per application, collecting activity logs.

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 Exchange 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 Permissions Collection - <Service Name> service is running.
- File Access Manager Central Activity Monitor - <Service Name> service is running.

Log Files

Check the log files listed below for errors

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

Monitored Activities

1. Simulate activities on Exchange 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*)