SailPoint

Integrating Exchange with File Access Manager

Version: 8.3 Revised: March 30, 2022

Contents

Contents

Capabilities

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

Supported Versions

- Exchange 2013

- Exchange 2016 (including Exchange 2016 having a CAS installed on Windows server 2016)

Connector Overview

Monitoring Microsoft Exchange On-Premises is based on standard Microsoft Exchange monitoring capabilities. Access to Exchange On-Premises is based on Remote Power Shell capabilities.

Audit types include:

Mailbox Access Audit

> Administrators who access other users' mailboxes
>
> Users who access other users' mailboxes as delegates
>
> Owners who access their own mailbox

Administrator Audit PowerShell Cmdlets

> Every Set-* PowerShell is audited

> It is not recommended to enable Owner auditing on all mailboxes, due to Exchange overload and DB size.

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

Action	Description	Admin	Delegate	Owner
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
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

Exclusion of Specific Mailboxes from Auditing

Specific mailboxes can be excluded from Auditing by setting a configurable key in the Application Monitor app.config file.

To exclude mailboxes, set the `mailboxAuditExcludeByFilter` under the AppSetting tag with a regular expression that matches only the names of the mailboxes to be excluded.

Use this setting to exclude a relatively small number of mailboxes from Auditing, when in Full Learning mode. The No Learning mode configuration is preferable if many mailboxes are excluded from auditing.

> For example, Journal mailboxes monitor and register every Exchange Server event, which doubles the number of generated events. Use this feature to exclude them.

After all mailboxes have been fetched from the Exchange server, the system applies a filter on the returned result set to filter out excluded mailboxes. All other mailboxes will be audited, subject to the setting defined.

> The defined setting only affects the mailbox Audit and does not affect Admin Audit events.

By default, the system removes all Audit settings from all monitored mailboxes (including those excluded by the Exclude Audit by Filter operation) when the Application monitor service stops running. This prevents unnecessary Audit settings from remaining after other changes have been made to the Application Monitor configuration over time.

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 .

- PowerShell

Supported Versions

- Exchange 2013
- Exchange 2016 (including Exchange 2016 having a CAS installed on Windows server 2016)

Enable Remote PowerShell

- Run the following command on one of the Exchange CAS to enable remote PowerShell:

```
shell winrm q
```

> The Exchange environment on a 2019 server with an Activity Monitor must be configured to communicate with a 2019 CAS server.

> Previous versions of File Access Manager required the installation of an additional PowerShell endpoint on an Exchange CAS server that allowed unrestricted script execution. This requirement was removed beginning with SecurityIQ v5p1 to simplify the deployment of the connector.
> If your environment was upgraded from older versions, *it is recommended* that you delete the obsolete "WBXPowerShell" endpoint from the Exchange CAS server.

Permissions

- Create a designated domain user (for example, *siq_xch*).
- Assign the following user Exchange groups:
    - Recipients Management
    - Records Management
    - Public Folders Management
- From PowerShell on the CAS run the following:

```
Set-User [username] -RemotePowerShellEnabled $True
```

Fine-Grained Permissions

Exchange allows for creating custom admin roles, and this can be used to grant File Access Manager service account the minimum privileges they need.

Each of these admin roles will grant privileges to a specific set of cmdlets.

Listed below are the cmdlets we use sorted by service type:

BAM

- Get-ExchangeServer
- Set-AdminAuditLogConfig
- Search-MailboxAuditLog
- Set-Mailbox
- Get-Mailbox
- Get-User

Crawler

- Get-Mailbox
- Get-MailboxStatistics
- Get-MailboxFolderStatistics
- Get-PublicFolder

PC

- Get-ExchangeServer
- Get-Group
- Get-User
- Get-Mailbox
- Get-MailboxPermission
- Get-MailboxFolderPermission
- Get-MailboxFolderStatistics
- Get-ADPermission
- Get-PublicFolder
- Get-PublicFolderClientPermission

Using those as reference and following PowerShell commands, create and assign the needed roles:

BAM

New-ManagementRole -Name "FIleAccessManager Activities View-Only Recipients" -Parent "View-Only Recipients" -EnabledCmdlets Get-User,Get-Mailbox

New-ManagementRole -Name "FileAccessManager Activities Audit Logs" -Parent "Audit Logs" -EnabledCmdlets Set-Mailbox,Search-MailboxAuditLog,Set-AdminAuditLogConfig

New-ManagementRole -Name "FileAccessManager Activities View-Only Config" -Parent "View-Only Configuration" -EnabledCmdlets Get-ExchangeServer

New-RoleGroup -Name "FileAccessManager Activities Role Group" -Roles "FIleAccessManager Activities View-Only Recipients","FileAccessManager Activities Audit Logs","FileAccessManager Activities View-Only Config"

Add-RoleGroupMember -Identity "FileAccessManager Activities Role Group" -Member <domain\activities_user>

Crawler and PC

New-ManagementRole -Name "FileAccessManager Crawl And Permissions View-Only Recipients" -Parent "View-Only Recipients" -EnabledCmdlets Get-Mailbox,Get-MailboxStatistics,Get-MailboxFolderStatistics,Get-PublicFolder-,Get-Group,Get-User,Get-MailboxPermission,Get-MailboxFolderPermission,Get-PublicFolderClientPermission

New-ManagementRole -Name "FileAccessManager Crawl And Permission View-Only Config" -Parent "View-Only Configuration" -EnabledCmdlets Get-ExchangeServer,Get-ADPermission

New-RoleGroup -Name "FileAccessManager Crawl And Permissions Role Group" -Roles "FIleAccessManager Crawl And Permissions View-Only Recipients","FileAccessManager Crawl And Permission View-Only Config"

Add-RoleGroupMember -Identity "FileAccessManager Crawl And Permissions Role Group" -Member <domain\crawl_user>

Another option to having all permissions assigned to a single user:

All

New-ManagementRole -Name "FIleAccessManager View-Only Recipients" -Parent "View-Only Recipients" -EnabledCmdlets Get-User,Get-Mailbox,Get-MailboxStatistics,Get-MailboxFolderStatistics,Get-PublicFolder,Get-Group,Get-MailboxPermission,Get-MailboxFolderPermission,Get-PublicFolderClientPermission

New-ManagementRole -Name "FileAccessManager Audit Logs" -Parent "Audit Logs" -EnabledCmdlets Set-Mailbox,Search-MailboxAuditLog,Set-AdminAuditLogConfig

New-ManagementRole -Name "FileAccessManager View-Only Config" -Parent "View-Only Configuration" -EnabledCmdlets Get-ExchangeServer,Get-ADPermission

New-RoleGroup -Name "FileAccessManager Group" -Roles FIleAccessManager View-Only Recipients","FileAccessManager Audit Logs","FileAccessManager View-Only Config"

Add-RoleGroupMember -Identity "FileAccessManager Group" -Member <domain\user>

Audit Bypass

The File Access Manager Connector for Exchange 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

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor / Permissions Collector	File Access Manager Servers	8000-8008
Remote PowerShell	Activity Monitor / Permissions Collector	CAS server	80 or 443

Exchange Installation Flow Overview

To install the Exchange connector:

1. Configure all the prerequisites.

2. Add a new Exchange application in the Business Website.

3. Install the relevant services:

   - Activity Monitor - This is the activity collection engine, used by all connectors that support activity monitoring.

   - Permissions Collector

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.

Install Permission Collectors (optional)

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

For further details, see section **Application > Central Service > Collector Relations** in the File Access Manager Administrator Guide

Adding an Exchange Application

In order to integrate with Exchange, 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

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:

XCH Server Name

> Server Name of either the Exchange Server (or one of the Exchange servers), or the Cluster Logical Name. Do not use IP Addresses

Domain NetBios Name

> Short domain name.

PowerShell Port

> 80 if working with HTTP
>
> 443 if working with HTTPS

Username and Password

> The user defined in the prerequisites.

WinRM/HTTPS User SSL

> Use SSL when connecting with WinRM/SSL.

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

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 which 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@.*).*

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 "|" .

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 4,000 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.

Configuring Activity Monitoring

Configure the activity monitoring processes 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 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 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.

Activity Monitor

> The activity monitor is installed per application, and collects SharePoint Audit entries and IIS activity logs.

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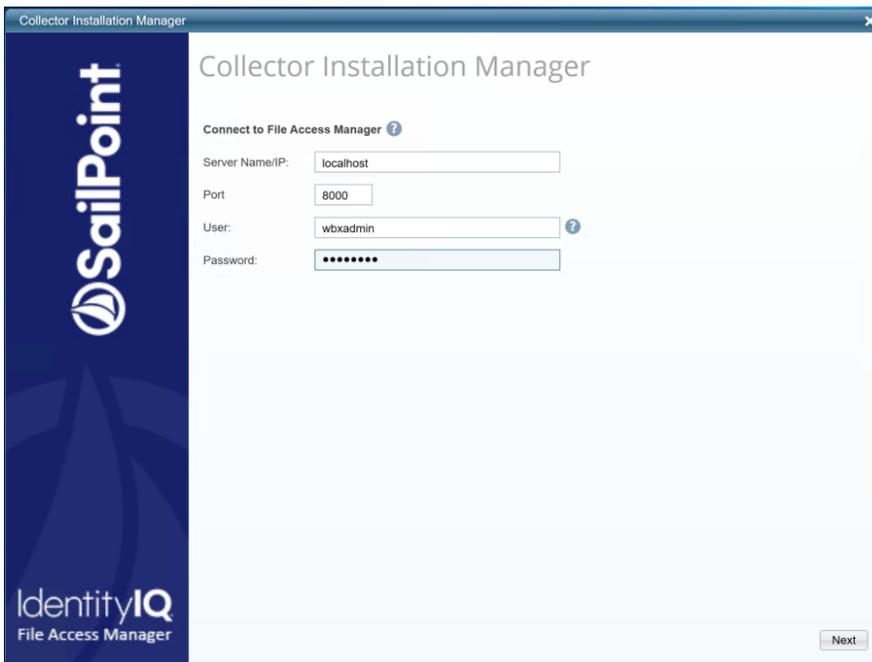
2. Enter the credentials to connect to File Access Manager.

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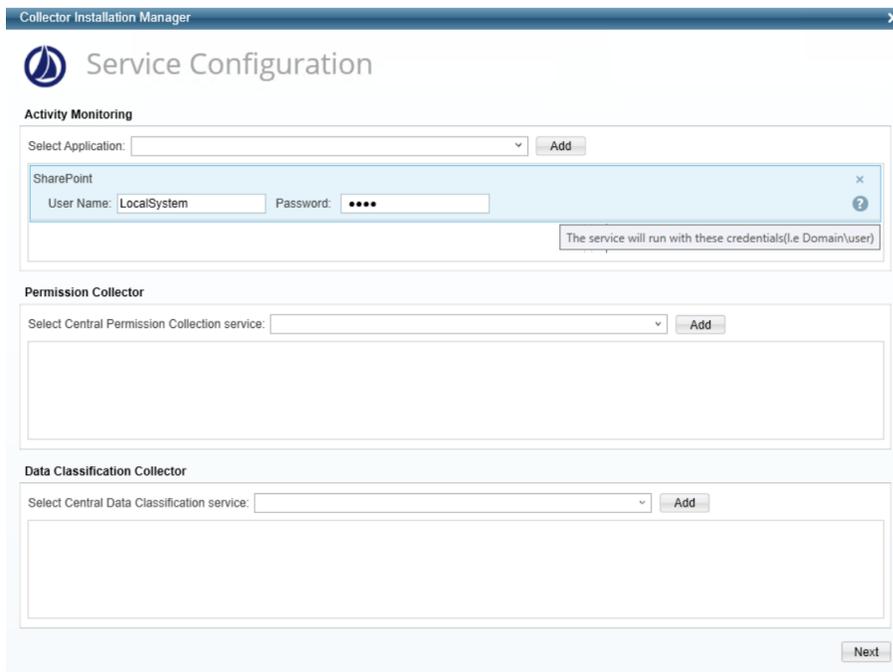
4. If you are installing the Activity Monitor, select the application, and click **Add.**

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. 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.

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

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

10. Click **Next**.

11. The system begins installing the selected components.

12. 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 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%\Exchange2010BAM-<Application_Name>.log"

Monitored Activities

1. Simulate activities on Exchange.

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*)