



Integrating Windows Server with File Access Manager

Version: 8.4

Revised: March 27, 2023

Copyright and Trademark Notices

Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

- Capabilities 5**
 - Supported Versions 5
- Connector Overview 6**
 - Monitored Activities 6
 - Permissions Collection Operation Principle 8
 - Path of Business Resource 8
 - Windows Server Failover Cluster 9
 - Resource Tree Structure 10
- Prerequisites 12**
 - Software Requirements 12
 - Backup Operator Privileges 12
 - Permissions 12
 - Communications Requirements 13
- Windows Server Installation Flow Overview 14**
- Collecting Data Stored in an External Application 15**
- Adding a Microsoft Windows Server Application 17**
 - Select Wizard Type 17
 - General Details 17
 - Connection Details 18
 - Configuring and Scheduling the Permissions Collection 19
 - Selecting and Scheduling the Data Classification Settings 27
 - Data Privacy 28
 - Configuring Activity Monitoring 28
 - Monitored Actions 31
 - Activity Monitoring Setup Notes for Windows File Server 32
 - Enabling Access Fulfillment for an Application 32
- Adding New Windows Server Bulk Application 35**
 - Scheduling Tasks 36

Completing the Installation	37
Installing Services: Activity Monitor and Collectors	39
Verifying the Windows Server Connector Installation	42
Installed Services	42
Log Files	42
Monitored Activities	42
Permissions Collection	43
Troubleshooting	44
Unable to See Events	44
The Application is not in the List of the Collector Installation Manager	44

Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in Windows Server 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.
- Manage access fulfillment - automated granting and revoking of access - according to rules set in File Access Manager.

See the File Access Manager documentation for a full description.

Supported Versions

The File Access Manager Microsoft Windows Server Connector supports the following versions of MS Windows Server:

2012 R2, 2016, 2019

32 and 64-bit support for all versions

Just to clarify - This document, describes connecting to an MS Windows server as an application containing business resources. This should not be confused with the list of supported MS Windows server versions on which we can install the File Access Manager.

Connector Overview

File Access Manager Windows FS Activity Monitor uses a Microsoft certified mini-filter driver

[https://msdn.microsoft.com/en-us/library/windows/hardware/dn265170\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/dn265170(v=vs.85).aspx)

The driver intercepts all I/O calls to determine which users have access to which files/folders, and also audits **Changes to local users and groups**. There is therefore no need for Windows auditing, and no performance overhead is introduced on the monitored server.

The activity monitor detects which share was used to perform each operation . Local access is a special cases, as detailed below:

Local Access

The system reports local access to a file/folder (for example, by using Remote Desktop) on the administrative share (C\$), and a special field on the activity ("Is Local Access") is set to "True".

Monitored Activities

Create File

A new file was created.

Create Folder

A new folder was created.

Create from Move

A "Create Folder" event generates this event on the newly created folder.

Create from Rename

A "Rename Folder" event generates this event on the newly created folder.

Delete File

A file was deleted.

Delete Folder

A folder was deleted.

Move File

A file was moved.

Move Folder

A folder was moved.

Permission Add File

A permission was added to a file.

Permission Add Folder

A permission was added to a folder.

Permission Remove File

A permission was removed from a file.

Permission Remove Folder

A permission was removed from a folder.

Read File

A file (its content or security properties) was read.

Rename File

A file was renamed.

Rename Folder

A folder was renamed.

Write File

A file was modified.

Add Member

A local user/domain group was added to a local group.

Remove Member

A local user/domain group was removed from a local group.

Create User

A local user was created.

Delete User

A local user was deleted.

Rename Object

A local user/group name as changed.

Create Group

A local group was created.

Delete Group

A local group was deleted.

Remove Audit Account Management

The Account Management Auditing was disabled in windows.

Permissions Collection Operation Principle

File Access Manager connects to the Windows file server through CIFS, collects the local users and groups, and analyzes the share and NTFS permissions on all the folders.

Path of Business Resource

The full path of the business resources is the UNC shared path, rather than the physical path of the folder. The physical paths display since they are represented by the administrative shares (c\$, d\$...) and are treated in the same way as any other share on the server.

Crawler

The crawler crawls through all the shares and creates business resources with the share's full path (\\server_name\share\folder).

Permissions Collector

The permissions collector analyzes share permissions, as well as NTFS permissions.

Activity Monitor

The full path of activities is the share used to access the file/folder. Section 2.2 provides a more detailed explanation.

Windows Server Failover Cluster

Windows Server Failover Cluster is an Active Passive Cluster based on Windows Server.

Basic Terminology

The following definitions apply to the Windows Server Failover Cluster:

Node

A physical server that is part of a Cluster

All the nodes in a cluster must be configured when the “Is Cluster” field in the application configuration wizard is checked.

Server Name

a logical layer on top of the Node layer

Shares in a Cluster belong to a Server Name, which is the name used when shares in the cluster are accessed.

A Server Name (discovered automatically, as part of the crawling task) is active on only one Node at a time.

File Share Scoping

shares located on a cluster node can only be through the Server Name – not through the cluster node name in which they are currently active.

The example below is used in Section [Resource Tree Structure](#):

There is a cluster application in File Access Manager, called ClusterApp.

ClusterApp consists of node1 and node2.

ServerName1 is currently active in node1, while ServerName2 is currently active in node2.

ServerName1 has one share: Share1 (\\ServerName1\Share1).

“Share1” is mapped to physical path “E:\folder1”

ServerName2 consists of Share2 and Share3 (\\ServerName2\Share2 and \\ServerName2\Share3).

“Share2” is mapped to physical path “E:\folder2”

“Share3” is mapped to physical path “E:\folder2\folder3”

Windows Failover Cluster Share Scoping

File Access Manager supports Windows Failover Cluster Share Scoping.

The Server Names and their corresponding shares are discovered as part of the crawl task, and the business resource tree is built with the Server Names at the first level.

Resource Tree Structure

File Access Manager manages Business Resources that belong to a share only a Server Name in a Windows Server Failover Cluster. Physical paths that do not belong to a share on a Server Name are not displayed in File Access Manager.

The Business Resources tree is represented as follows:

- [Cluster Application]
 - [Admin Audit]
 - [Server Name]
 - [Share]
 - [Share]
 - [Server Name]
 - [Share]
 - [Share]

The business resource tree for the above example is:

- ClusterApp
- Admin Audit
 - [Server1]
 - [Share1]
 - [Share2]
 - [Server2]

- [Share3]
- [Share4]

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](#) .

Backup Operator Privileges

The user configured in the permissions prerequisites section must be a member of the local Backup Operator group of the file server. It eliminates the need to grant explicit permissions to the File Access Manager user to all the folders on the file server. By using the Backup Operator privilege, File Access Manager can crawl, collect permissions, and classify data even if the user does not have explicit permissions to the folder.

Permissions

File Access Manager requires different permissions, based on the tasks that require those permissions. The user configured in the Application configuration wizard must have the following permissions on the file server:

- Share Read permissions to all shares on the file server
- Full Control permission for each normalized folder
- Member of the local Backup Operators group on the file server
- Member of the local Administrators group on the file server

Why do we need this access?

The following detailed explanation describes required permissions by each File Access Manager task:

Activity Monitoring

No special permission is required, since the Activity Monitor service runs locally on the monitored service with Local System privileges.

Crawling

The user must have Share Read permissions to all the shares on the file server.

The user must be a member of the local Backup Operators group on the file server.

Permission Collection

The user must have Share Read permissions to all the shares on the server.

The user must be member of the local Backup Operators group on the server.

The user must be a member of the local Administrators group to read the Share Permissions, and the local Users and Groups of the server.

Access Fulfillment

The user must have Full Control permission on the normalized folders to be able to set the permissions.

Data Classification

The user must have Share Read permissions for all the shares on the server.

The user must be member of the local Backup Operators group on the server.

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor	File Access Manager Servers	8000-8008
Permissions Collector & Data Classification Analysis	Permissions Collector/Data Classification Server	Monitored server	CIFS/SMB (139, 445)

Windows Server Installation Flow Overview

To install the Windows Server connector:

1. Configure all the prerequisites.
2. Add a new Windows Server 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
 - Data Classification Collector

Installing the permissions collector and data classification services is optional and should only be installed by someone with a full understanding of File Access Manager deployment architecture. The File Access Manager Administrator Guide has additional information on the architecture.

Collecting Data Stored in an External Application

Terminology:

Connector

The collection of features, components and capabilities that comprise File Access Manager support for an endpoint.

Collector

The “Agent” component or service in a Data Classification and or Permission Collection architecture.

Engine

The core service counterpart of this architecture.

Identity Collector

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your File Access Manager installation. See the server Installation guide for further details.

Install a Data Classification central engine

One or more central engines, installed using the server installer

Install a Permission Collection central engine

One or more central engines, installed using the server installer

Create an Application in File Access Manager

From the Business Website. The application is linked to central engines listed above.

Add an Activity Monitor

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

Install Permission Collectors and / or Data Classification Collector (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 a Microsoft Windows Server Application

In order to integrate with Windows Server, 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

Windows File Server (Agent)

Application Name

Logical name of the application

Description

Description of the application

Tags

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

Event Manager Server

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu.

Identity Collector

Select from the Identity Collector dropdown menu.

- You can create identity collectors in the administrative client. **Applications > Configuration > Permissions Management > Identity Collectors.**

See section "OOTB Identity Collection" in the Collector Installation Manager File Access Manager Administrator Guide for further details.

- If adding a new identity collector, press the **Refresh** button to update the Identity Collector dropdown list.

Click **Next.** to open the Connection Details page.

Connection Details

Server Name

Name of the server which is monitored

Domain Name

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Username

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Password

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Is Cluster Mode

Click this checkbox to configure the Windows servers as a cluster.

Cluster Nodes

This option is available for cluster mode only. Click the button to type in physical cluster nodes to the dropdown list. This will create multiple XML configuration files, one for each physical node in the cluster.

Type in a cluster node, and click the **+** icon to add this item to the list

To delete an item from the list, click the delete icon on the line.

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.

Calculate Resource Size

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never
- Always
- Second crawl and on (This is the default)

Create a Schedule

Click to open the schedule panel. See [Scheduling a Task](#)


Setting the Crawl Scope

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

Including and Excluding Paths by List

To set the paths to include or exclude in the crawl process for an application

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

The actual entry fields vary according to the application type.


1. Scroll down to the Crawl configuration settings.
2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
3. Click Include / Exclude Resources to open the input fields.

4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.
5. To remove a resource from a list, find the resource from the list, and click the **x** icon on the resource row.

When creating exclusion lists, excludes take precedence over includes.

Excluding Paths by Regex

To set filters of paths to exclude in the crawl process for an application using regex.

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

The actual entry fields vary according to the application type.

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions.

Crawler Regex Exclusion Example

The following are examples of crawler Regex exclusions:

Exclude all shares which start with one or more shares names:

Starting with `\\server_name\shareName`

Regex: `\\\\server_name\\shareName$`

Starting with `\\server_name\shareName` or `\\server_name\OtherShareName`

Regex: `\\\\server_name\\(shareName|OtherShareName)$`

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

Starting with `\\server_name\shareName`

Regex: `^(?!\\\\\\server_name\\shareName($|\\.*)) .*`

Starting with `\\server_name\shareName` or `\\server_name\OtherShareName`

Regex: `^(?!\\\\\\server_name\\(shareName|OtherShareName)($|\\.*)) .*`

Narrow down the selection:

Include ONLY the C\$ drive shares: `\\server_name\C$`

Regex: `^(?!\\\\\\server_name\\C\\$($|\\.*)) .*`

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

Regex: `^(?!\\\\\\server_name\\share\\$($|\\folderA$|\\folderA\\.*)) .*`

Include ONLY all administrative shares

Regex: `^(?!\\\\\\server_name\\[a-zA-Z]\\$($|\\.*)) .*`

To write a backslash or a Dollar sign, add a backslash before it as an escape character.

To add a condition in a single command, use a pipe character “|” .

in Windows file server, the share `\\<server name>\Admin$` is excluded by default.

Excluding Top Level Resources

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

To exclude top level resources from the crawl process

1. Open the application screen

Admin > Applications

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. *Run Task*

The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

Before running the task for the first time, the message above this button is:

"Note: Run task to detect the top-level resources"

If the top level resource list has changed in the application while you are on this screen, press this button to retrieve the updated structure.

Once triggered, you can see the task status in

Settings > Task Management > Tasks

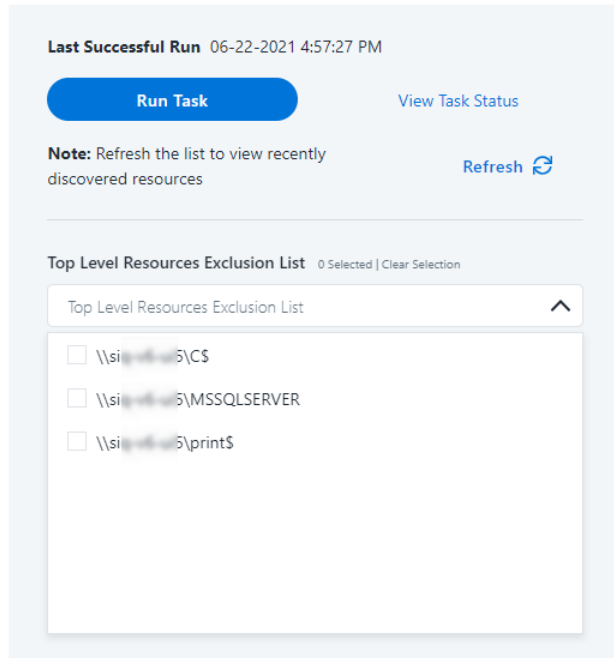
This will only work if the user has access to the task page

When the task has completed, press **Refresh** to update the page with the list of top level resources.

4. Click the top level resource list, and select top level resources to exclude.
5. Click *Save* to save the change.
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.

Top Level Resources Exclusion

WFS-DC testing



Special Consideration for Long File Paths in Crawl

If you need to support long file paths above 4,000 characters for the crawl, set the flag

`excludeVeryLongResourcePaths`

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

You should not enable exclusion of long paths, unless you experience an issue.

Background

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

Identifying the Problem

When using an SQL Server database version 2014 and earlier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

Setting the Long Resource Path Key


The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

`%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\`

Search for the key **`excludeVeryLongResourcePaths`** and correct it as described above.

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

To configure the activity monitoring polling parameters

- 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 **Activity Configurations & Decs** settings page.

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.

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 DEC's text box.

Use the > or >> arrows to move the selected DEC's to the Current DEC's text box.

The user can select multiple DEC's. Simply select each desired DEC.

You can create a new DEC in the Administrative Client (Applications>Configuration>ActivityMonitoring>DataEnrichmentConnectors).

After creating a new DEC, click **Refresh** to refresh the dropdown list.

The chapter Connectors of the File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

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, e.g., C:\folder1\subfolder2.

Enter one value at a time as described above.

Exclude Users

List of users whose activities are not monitored, e.g., user1, domain\user2, user3@domain.com.

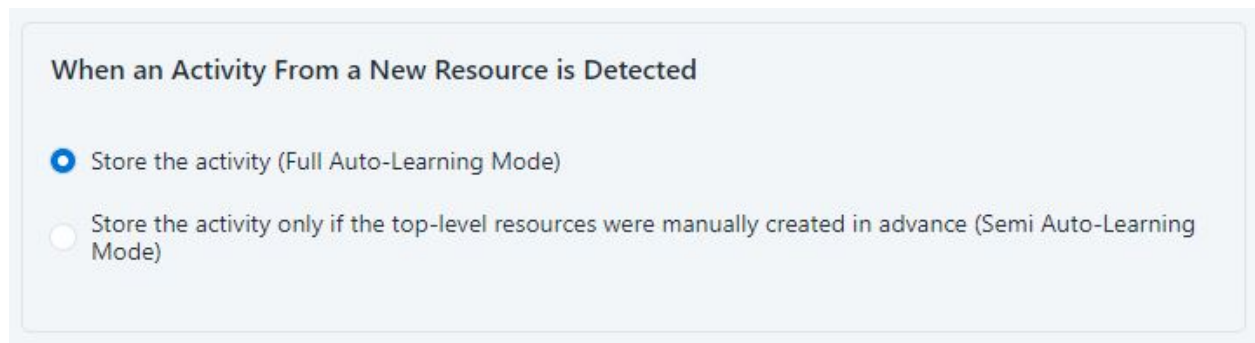
Enter one value at a time as described above.

The user format to be used depends on how the activity is logged by the endpoint. If you are not sure which of the user formats above to use, either specify all of them, or leave the list empty for now and navigate to the **Forensics > Activities** screen in the File Access Manager Website after some activities flow in to see how the user is depicted in them and use that depiction in the exclusion list.

When an activity from a new resource is detected:(Modes of Storing Activities)

Full Auto-Learning Mode – Will audit everything (every action) on every resource.

Semi Auto-Learning Mode – Will monitor activities on resources nested under the top-level resources that are marked for Monitoring. This operation mode will also allow the user to select what type of activities are being monitored.



Monitored Actions

The user has the ability set monitored actions within Manage Resources.

1. Navigate to **Admin > Applications**.
2. Under the Actions column, click the ellipsis on the desired application.
3. Click **Manage Resources**.

The Manage Resources will display with all resources listed.

4. Click **Manage Monitored Actions**.
5. Toggle the **Enable Activity Monitoring for this Resource Hierarchy**.

The user can now select the type of actions they want monitored.

All actions are automatically selected initially.

Activity Monitoring Setup Notes for Windows File Server

For Windows File Server: The excluded folders must be in the physical path format (for example, C:\Windows), and not in the share path of the folder. The exclusion of a folder will result in an event not being sent to any of the shares mapped to the physical folder.


It is strongly recommended that the following users in Windows be excluded:

- Local System
- NT Authority

Enabling Access Fulfillment for an Application

Access fulfillment is enabled per application in the application setting screen, for applications that support fulfillment (See the compatibility table in Compass for the full list)

To enable Access Fulfillment for an application:

1. Open the configuration 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.
2. Press **Next** till you reach the **Access Fulfillment** settings page.

The setting pages and entry fields vary according to the application type.

3. For non-normalized resources, you can click **Enable Access Fulfillment for Revoking Explicit Permissions** . See [Access Fulfillment for Removal of Explicit Permissions](#).
4. Click **Enable Access Fulfillment for Normalized Groups**.

Identity Collector

Fulfillment requires an identity collector in order to run. If you did not select an identity collector in the General Details configuration page, you can select one from the drop down list now.

If there is no identity collector defined for this application, or if you want to use a different identity collector than the ones in the dropdown list, you can create a new identity collector in the Administrative Client (**Applications > Configuration > Permissions Management > Identity Collectors**).

See [Create/Edit an Active Directory Identity Collector](#) for more details on creating an identity collector.

Managed Group OU (DN)

The organizational unit in which the managed permission groups will be created. Make sure that the chosen identity collector's user has permissions to create groups under this location (e.g. OU=FileAccessManagerManaged, DC=SailPoint, DC=COM)

OU refers to an Organizational Unit, and DN refers to a Distinguished Name.

How to Handle 'List Folder Contents' Permissions

Not relevant for SharePoint

- Create and manage a dedicated permissions group for it - this is the default value
- Revoke these permissions

How to Handle Inexact Permissions Matches

During the normalization process, the application has to decide what to do with permissions that do not match the normalized permissions.

- Fail the normalization process
 - Elevate to the nearest permission match
 - Revoke the permission
5. Open the Advanced Settings panel for additional settings:

Group Cache Sync Interval(sec)

This setting will add a pause to the process of setting normalize permissions on the resource. This will allow the endpoint's local AD groups cache to sync the newly created managed groups.

The default is 0 - signifying the process will not pause by default.

Use Template Permission Group

Template groups are created per application and added as a template to every managed resource. These groups are not managed by File Access Manager, and are usually used to ensure that users who need application-wide access such as backup or archiving users have access.

Select for each permission group whether File Access Manager should create a group or whether to use an existing group, for the following groups:

- List Folder Contents
- Read & Execute
- Modify
- Full Control

If you select **Use an Existing Group**, select the required group to use from the dropdown list.

Once an application is enabled for access fulfillment, you can set specific resources to be normalized using the [Manage Normalized Resources](#) page.

Adding New Windows Server Bulk Application

To add Windows Server applications in bulk, use the New Application Wizard in the File Access Manager Administrative Client.

1. Navigate to **Applications > New > Bulk Application**.

The New Bulk Application Wizard window displays under the Welcome tab.

2. Select **Windows File Server**.

3. Click **Download Template** and download the bulk installation Excel template.

Each application type has a different template.

4. Fill in a new row in the template for each application to be installed.

In the multiple selection fields, such as **Central DC Service**, and **Central PC Service**, you can select valid options from the drop down list in the Excel file.

Save the template file.

5. In the wizard, click **Browse** and select the template you filled.

6. Click **Upload** to upload the template.

7. Once the template is uploaded, the *Upload Status* table contains a row for each application in the template.

8. If there are errors displayed in the *Upload Status* table, correct the parameters and upload the template again.

- This stage is for validation only
- Applications with errors will be ignored, and won't be created

9. Click **Next**.

You can navigate among the Permissions Collection and Crawler scheduling windows (under the Scheduling tab) with the Next and Back buttons.

The Permissions Collection window of the New Bulk Applications Wizard displays under the Scheduling tab.

A schedule is created for each application with the name: PermissionCollection_<Service_Name> Task, with the same details.

Scheduling Tasks

In the next configuration screens you can schedule tasks to collect and analyze the BRs in the connected servers.

The scheduling includes:

- Permissions Collector
- Crawler - Automatic application crawling to find new resources
- Data Classification - to classify your results

Fill in the scheduling fields for each scheduling screen:

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.

See the chapter “Crawling” in the File Access Manager Administrator Guide for more information on the crawling mechanism.

Press **Next** and **Back** to navigate between the screens.

Completing the Installation

After the Data Classification screen, click **Next**.

The applications are created at this stage.

The Application Creation Status window of the New Bulk Applications Wizard displays under the Status tab.

A table lists the creation status of each application.

Click **Next**.

The **Installation File** window of **New Bulk Applications Wizard** displays.

1. Browse to select the destination for the .zip file, which contains the files required to install the Activity Monitor / Permissions Collector / Data Classification services for each application.
2. A text file with the command line for remote installation of the Activity Monitor connector is also created. This file can be used for unattended installations of the Activity Monitor. See [Activity Monitor Bulk/Unattended Installation](#) for further information.
3. Click **Finish**.

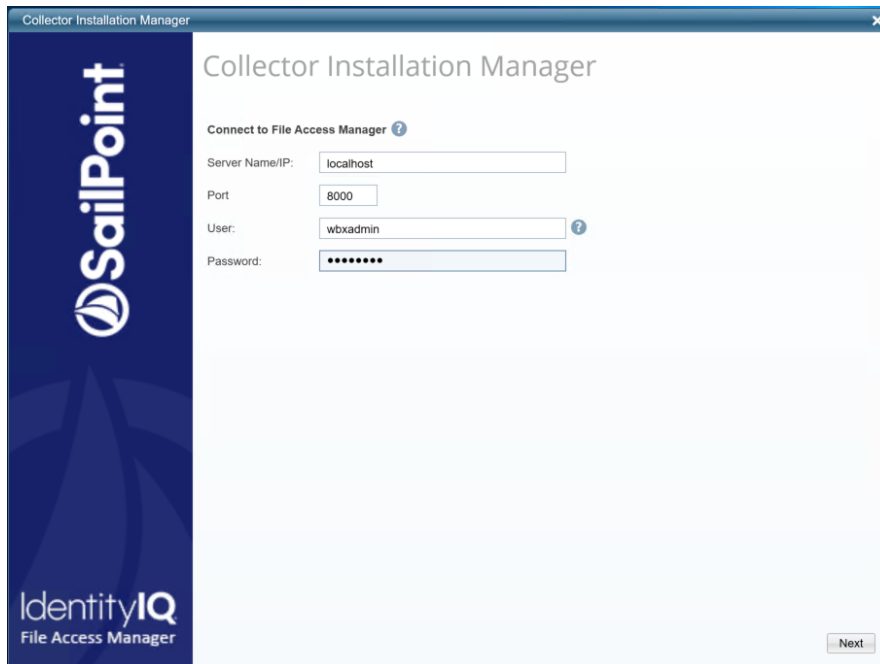
Installing Services: Activity Monitor and Collectors

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.

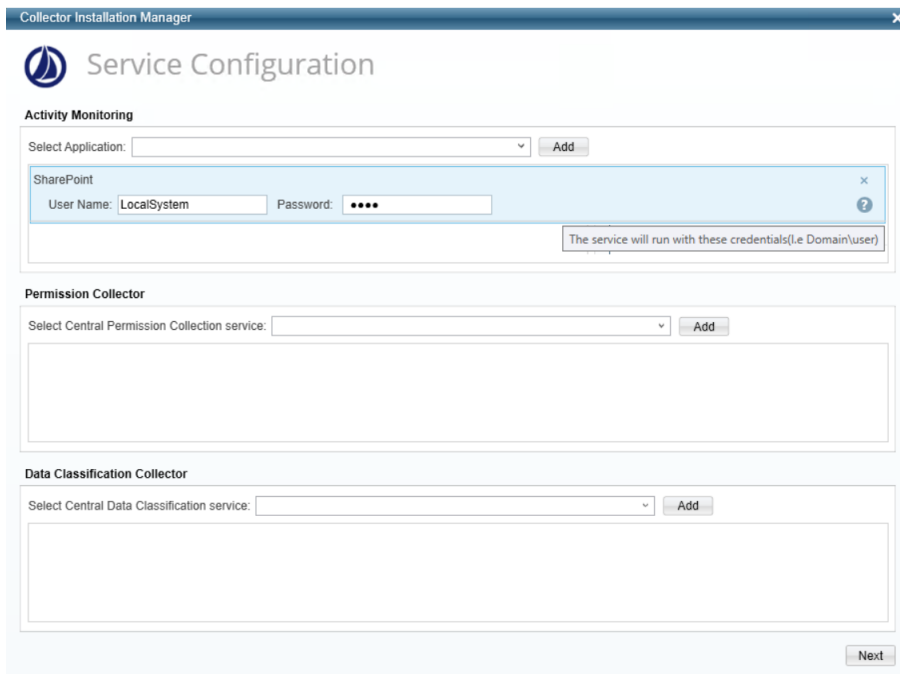
The installation files are in the installation package under the folder Collectors.

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 Windows Server 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 ManagerActivity Monitor - <Application_Name>
- File Access ManagerCentral Permissions Collection - <Application_Name>
- File Access ManagerCentral Data Classification - <Application_Name>

Log Files

Check the log files listed below for errors

- "%SAILPOINT_HOME_LOGS%\FilesMiniFilter_<Application_Name>.log"
- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\FilesMiniFilter-<Application_Name>.log"

Monitored Activities

1. Simulate activities on Windows Server.
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.

Unable to See Events

Symptom

The following error displays in a log file while you attempt to install the monitoring connector:

```
ERROR, WBX.whiteOPS.Agents.FilesMiniFilterActivity Monitor.FileMiniFilterActivity MonitorManager,connect, An unexpected error occurred while you attempt to start the mini-filter:
```

```
System.DllNotFoundException:  
Unable to load DLL 'wbapi.dll': The specified module could not be found. (Exception from HRESULT: 0x8007007E)—at WBX.whiteOPS.Agents.FilesMiniFilterActivity Monitor.SafeNativeMethods64.start(UInt32 bufferSizeInBytes, UInt32 trustedProcessId)—at WBX.whiteOPS.Agents.FilesMiniFilterActivity Monitor.FileMiniFilterActivity MonitorManager.connect()
```

Reason

Visual C++ 2010 redistributable package was not installed as part of the Activity Monitor service installation.

Solution Steps

See step 3 of [Windows Server Core](#).

The Application is not in the List of the Collector Installation Manager

Symptom

The application does not appear in dropdown list of the Collector Installation Managers in the Activity Monitoring

Reason

Either the application was not defined or the Host Name as defined in the (as defined when adding the application) does not match the server's short name on which the Collector Installation Manager was opened on.

Solution Steps

Verify that the Windows Server application was in fact created.

In case it exists, make sure the *Host Name* is correct.