



Integrating EMC-Celerra with File Access Manager

Version: 8.3 Revised: March 30, 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

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

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

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

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

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

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

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

Contents

Contents	iii
Capabilities	5
Connector Overview	6
Physical & Virtual Data Mover	6
CIFS Server	6
CIFS Servers Aliases	6
NFS Exports	6
CEE	7
CEPA and Virtual Data Movers	7
CEE & Activity Monitor	7
Activity Monitor	7
Permissions Collection Operation Principle	7
CIFS Shares	7
NFS Exports	7
Monitored Activities	8
Sample Architecture	9
Prerequisites	10
Software Requirements	10
How to Configure the CEE Service	10
Enable CEPA on the Data Mover	11
Permissions	12
CIFS Access	12
NFS Access	12
Communications Requirements	13
EMC Celerra Installation Flow Overview	14
Collecting Data Stored in an External Application	15
Adding an EMC-Celerra Application	17
Select Wizard Type	17

General Details	17
Connection Details	18
Configuring and Scheduling the Permissions Collection	19
Permission Collection Setup Notes for EMC Celerra	20
Selecting and Scheduling the Data Classification Settings	25
Data Privacy	26
Configuring Activity Monitoring	26
Monitored Actions	28
Configuring Data Enrichment Connectors	28
Enabling Access Fulfillment for an Application	29
Installing Services: Activity Monitor and Collectors	31
Verifying the EMC Celerra Connector Installation	34
Installed Services	34
Log Files	34
Verifying Monitored Activities	34
Permissions Collection	34
Troubleshooting	35
Activities not Collected by the Activity Monitor	35
State and Status ONLINE, but no Events are Shown	36
Counters Increase but no Events are Collected	37

Capabilities

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

Connector Overview

For more information and a deep technical understanding of the EMC architecture and CEE, refer to the EMC CEE version 7.0 using the Common Event Enabler for Windows

<https://www.emc.com/collateral/TechnicalDocument/docu48055.pdf>

Physical & Virtual Data Mover

- Celerra/VNX architecture is based on physical components named data movers.
- A physical data mover can host multiple virtual data movers (VDMs).

Audit facility (CEPA) is single for each physical data mover, and must be configured separately for each physical data mover.

CIFS Server

- A CIFS server is an EMC component that corresponds to a file server (\\cifs_server_name).
- You can configure a CIFS server on a physical Data Mover or on a VDM. Typically, the CIFS servers are configured on a VDM.
- Every CIFS server requires an Application definition in File Access Manager.

CIFS Servers Aliases

- An alias is a synonym name of the CIFS server. It is defined in the CIFS server itself and is visible in the EMC Unisphere.
- Every CIFS server can have one or more aliases.
- All the activities are always saved in File Access Manager with the real name of the filer.
- The filer name configured in the application must be the real name only.
- A DNS alias is not an EMC alias.

You must configure the aliases in the application configuration as well. Failure to do so results in losing the events of users accessing the aliases.

NFS Exports

- An NFS export is an EMC component that can be associated with any existing network interface to expose a UNIX-style NFS file server.
- Every NFS network interface that exposes NFS exports requires an Application definition in File Access Manager.

CEE

- A CEE service is the EMC gateway for communicating and receiving events notifications from the data movers.
- All data movers send notifications on CIFS/NFS events to the CEE service. The service in the data mover responsible for sending the events to the CEE is called CEPA (Celerra Event Publishing Connector).
- There is an n:n relation between the CEPA service running on the data mover and the CEE service:
- Every CEE can communicate with multiple data movers.
- Every CEPA service on a data mover can communicate with multiple CEE servers (for high availability and load sharing).

CEPA and Virtual Data Movers

- For CEE to work, you need to have a CIFS server configured on the physical Data Mover. This is the global CIFS server or the default CIFS server on the physical Data Mover.

CEE & Activity Monitor

- Every Activity Monitor can communicate with one or more CEE servers.
- Every CEE service can be configured to work with a multiple Activity Monitor services.

Activity Monitor

- Each Activity Monitor in File Access Manager corresponds to a single CIFS server. The first Activity Monitor installed on a physical server creates the Activity Monitor service. Subsequent Activity Monitors installed will not create additional Activity Monitor services.
- Every Activity Monitor that is installed adds a **bamconfig.xml** file under the Activity Monitor to add itself to the same service.

The first installed Activity Monitor must be the last Activity Monitor uninstalled. If you uninstall the first Activity Monitor before uninstalling the other installed Activity Monitors, those Activity Monitors will not work, and it will not be possible to uninstall them.

Permissions Collection Operation Principle

CIFS Shares

- File Access Manager connects using EMC administrative shares and analyzes folder permissions.
- Local groups and users are collected from the CIFS server during the permissions collection process.

NFS Exports

- File Access Manager connects using standard NFSv3 access to analyze UNIX-style folder permissions.
- A NIS Identity Collector is used to resolve UIDs/GIDs permissions discovered during the permissions collection process.

Monitored Activities

The following activities are monitored by the EMC Celerra connector

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 Change File

A file’s permissions were changed.

Permission Change Folder

A folder’s permissions were changed.

Read File

A file was read.

Rename File

A file was renamed.

Rename Folder

A folder was renamed.

Write File

A file was modified.

Sample Architecture

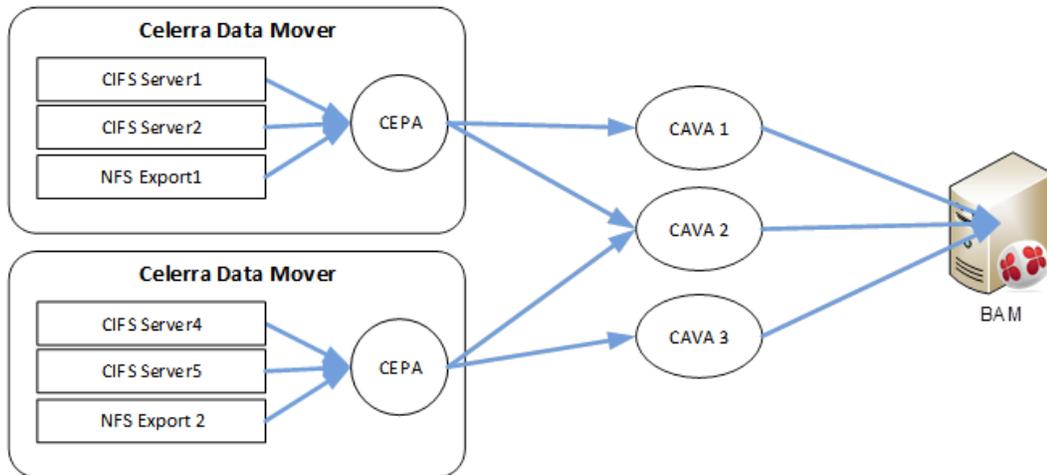
In the schema below, the first physical Data Mover is configured to send events to CEE 1 & 2. CEE 1 & 2 are configured to send event notifications to the Activity Monitor.

The second physical Data Mover is configured to send events to CEE 2 & 3. CEE 2 & 3 are configured to send event notifications to the Activity Monitor.

- CIFS Server 1
- CIFS Server 2
- NFS Export 1

The Activity Monitor monitors using CEE 2 & 3:

- CIFS Server 4
- CIFS Server 5
- NFS Export 2



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](#).

EMC CAVA/CEE

Version 4.9.3 and above

How to Configure the CEE Service

Connecting to a Remote CEE

For enterprises with an existing central CEE infrastructure, where the Activity Monitor will be installed on a different server than the CEE service:

1. On every CEE server, open the registry and perform the following changes:

```
[HKLM\Software\EMC\CEE\CEPP\Audit\Configuration]
```

```
Endpoint=whitebox@<File Access Manager Activity Monitor server ip address>
```

```
Enabled=1
```

If multiple monitor servers exist, the list should look like: whitebox@ip, whitebox@ip, ...

2. Restart the EMC CEE service.

Connecting to a Local CEE (No Central Infrastructure)

When installing the CEE service and the Activity Monitor service on the same server:

1. Install CEE Pack on the monitor server.
The CEE service must be installed on a server in the same domain as the physical data mover CEE server, otherwise the communication between the data mover and the CEE service will fail.

2. Open the registry and perform the following changes:

```
[HKLM\Software\EMC\CEE\CEPP\Audit\Configuration]
```

```
Endpoint=whitebox
```

```
Enabled=1
```

3. Set the logon user for the services to a user according to the "**required permissions**" section.
4. Restart EMC CEE service.

Enable CEPA on the Data Mover

1. The CEPA configuration is separate and must be done for each physical data mover.
2. If you have multiple virtual data movers with CIFS servers, the CEPA configuration must be on the physical data mover (usually server_2 data mover when there is a single physical data mover).
3. If the configuration file (cepp.conf) does not exist, create a new one.
4. Log in to the system with your administrative username (nasadmin) and password.
5. Use a text editor to create a new, blank file called **cepp.conf** file in the home folder with the following content:

```
ft level=[0/1] location=<location> size=<size>

pool name=sepapool \

servers=<cee1 FQDN>|<cee2 FQDN>|<cee3 FQDN> \

preevents= \ postevent-
s=OpenFileRead|CreateFile|FileWrite|FileRead|CreateDir|D-
eleteFile|De-
leteDir|CloseModi-
fied|RenameFile|RenameDir|SetAclFile|SetAclDir|SetSecFile|SetSecDir\

posterrevents= \

option=ignore \

reqtimeout=500 \

retrytimeout=50
```

The `ft level` parameter sets the fault tolerance level assigned. Valid values are 0-3, where:

- 0 = continue and tolerate lost events (default)
- 1 = continue and use a persistence file as a circular event buffer for lost events
- 2 = continue and use a persistence file as a circular event buffer for lost events until the buffer is filled and then stop CIFS
- 3 = upon heartbeat loss of connectivity, stop CIFS

It is recommended that this value be set to 1. If you kept the recommended value, fill in the `<location>` and `<size>` parameters, where:

location

Directory where the persistence buffer file resides relative to the root of a file system. If a location is not specified, the default location is the root of the file system.

size

Maximum size of the persistence buffer file, in MB. The default is 1 MB and the range is 1 MB to 100 MB. It is recommended to set it at 100MB

It is important to verify that all CEE FQDN server names are resolved and reachable from the data mover. You can also fill in the IP address of the server instead of FQDN.

6. Copy the newly created file to the data mover:

```
server_file <movername> -put cepp.conf cepp.conf
```

If cepp.conf exists, verify that the postevents parameter has the required values.

7. For NFS run the following command:

```
server_mount <data_mover> -o ceppcifs,ceppnfs <file system name> /<file system path>
```

Synchronize with Domain Watch and Start the Service

```
server_date server_# -timesvc start ntp <domain controller ip>
```

Start the CEPA Service on the Data Mover

```
server_cepp <movername> -service -start
```

Permissions

File Access Manager requires different permissions, based on the tasks and data collected. The user configured in the Application configuration wizard must have the following permissions:

CIFS Access

Activity Monitoring

Requires a domain user with administrative privileges on the local machine (on which the CEE service is installed)

Crawling

Requires a user who is a member of the local Backup Operators group on the virtual CIFS server

Requires a user with Share Read access to all the shares on the virtual CIFS server

Permission Collection

Requires a user with Shared Read access to all CIFS shares on the virtual CIFS server

Requires a user who is a member of the local Backup Operators group on the virtual CIFS server

Requires a user who is a member of the local Administrators group on the virtual CIFS server to be able to read share permissions and local users and groups

Data Classification

Requires a user with Share Read access to all CIFS shares on the virtual CIFS server

Requires a user who is a member of the local Backup Operators group on the virtual CIFS server

NFS Access

Activity Monitoring

Prerequisites

Requires a domain user with administrative privileges on the local machine (on which the CEE service is installed)

Crawling

Requires a user with permission to mount all NFS exports on the virtual NFS server

Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server

Permission Collection

Requires a user with permission to mount all NFS exports on the virtual NFS server

Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server

Data Classification

Requires a user with permission to mount all NFS exports on the virtual NFS server

Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Internal Access	Application	File Access Manager servers	8000-8008
File Access Manager Message Broker	Permissions Collector / Data Classification Collector	RabbitMQ	5671
EMC CEE	EMC Data Mover	CEE Service	RPC (135 + Dynamic)
CEPA Events Push	CEE Service	File Access Manager Application	RPC (135 + Dynamic)
CIFS - Permissions Analysis & Data Classification	Permissions Collection service and / or Data Classification service	CIFS file server	SMB
NFS - Permissions Analysis & Data Classification	Permissions Collection service	NFS file server	NFSv3

EMC Celerra Installation Flow Overview

To install the EMC Celerra connector:

1. Configure all the prerequisites.
2. Add a new EMC Celerra 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 an EMC-Celerra Application

In order to integrate with EMC Celerra, 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

Select NetApp Type

- EMC Celerra – CIFS
- EMC Celerra – NFS

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.

Identity Collector

EMC Celerra CIFS – Choose an active Directory identity collector

EMC Celerra NFS – Choose a Network Information Service (NIS) identity collector

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

Connection Details

CIFS Connection Details

Host Name

The real name used when connecting to the CIFS server

Domain Name, Username, & Password

Credentials for the user defined in the prerequisites

Aliases

Aliases defined in the EMC for the CIFS server

Type in an alias, and click **+** to add it to the list.

Click the delete icon on any item to remove it from the list.

NFS Connection Details

Host Name

The network address, typically the IP address, of the interface on which the NFS exports are exposed

Username

An NIS username, or root, to use when connecting to the NFS file server

Group Name

An NIS group name, or root, to use when connecting to the NFS file server

Aliases (optional)

Network aliases for the NFS server

Type in an alias, and click **+** to add it to the list.

Click the delete icon on any item to remove it from the list.

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

Valid for EMC Celerra-CIFS only

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**

Valid for EMC Celerra-CIFS only

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.

Permissions Source

NTFS, Share, Both

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

Valid for EMC Celerra-CIFS only

Permission Collection Setup Notes for EMC Celerra

Calculate Effective Permissions is for EMC Celerra CIFS only.

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 “|”.

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

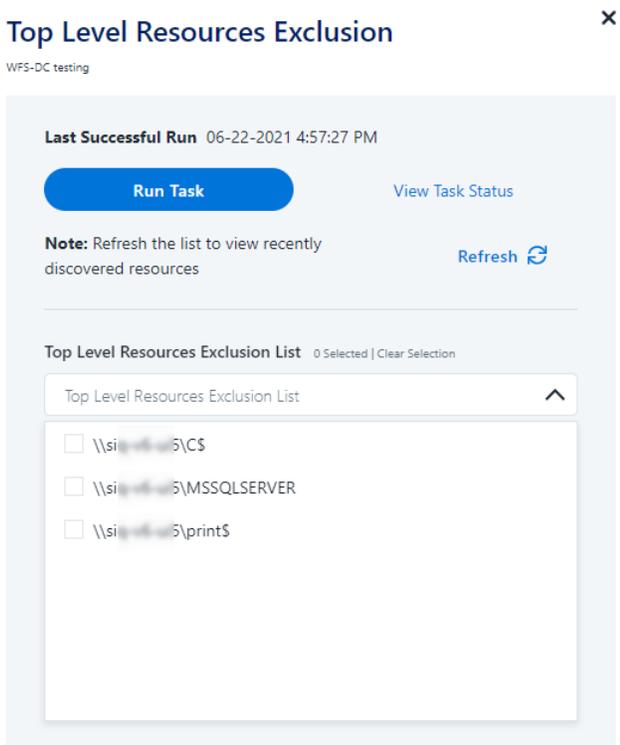
Settings > Task Management > Tasks



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.



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.

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

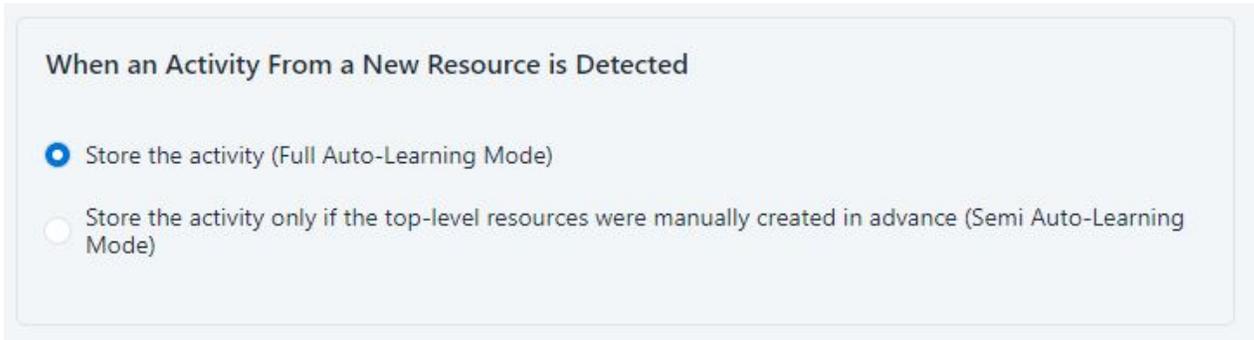
List of users whose activities are not monitored

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

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.



Click **Next**.

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.

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.

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.

Installing Services: Activity Monitor and Collectors

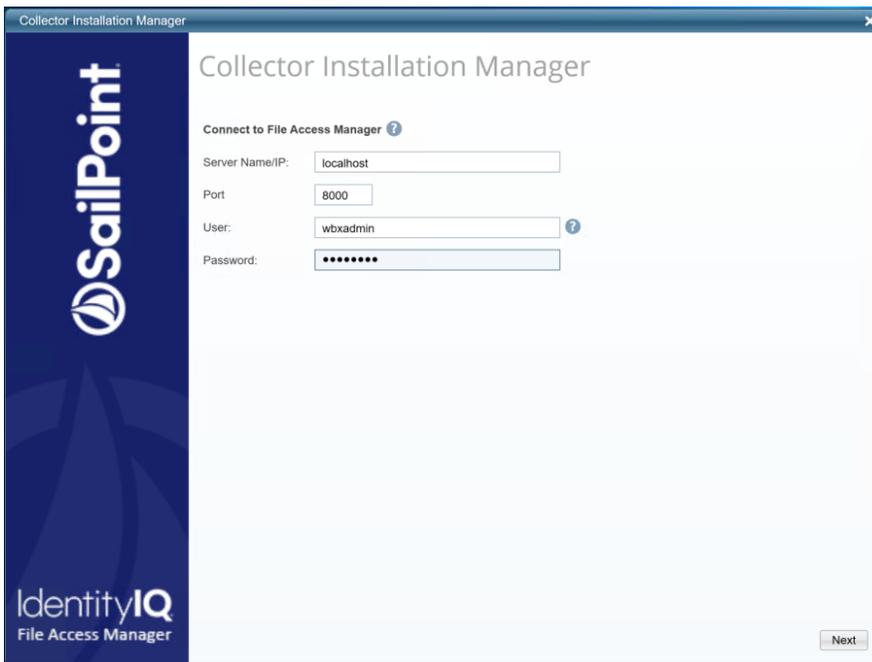
The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

Activity Monitor

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

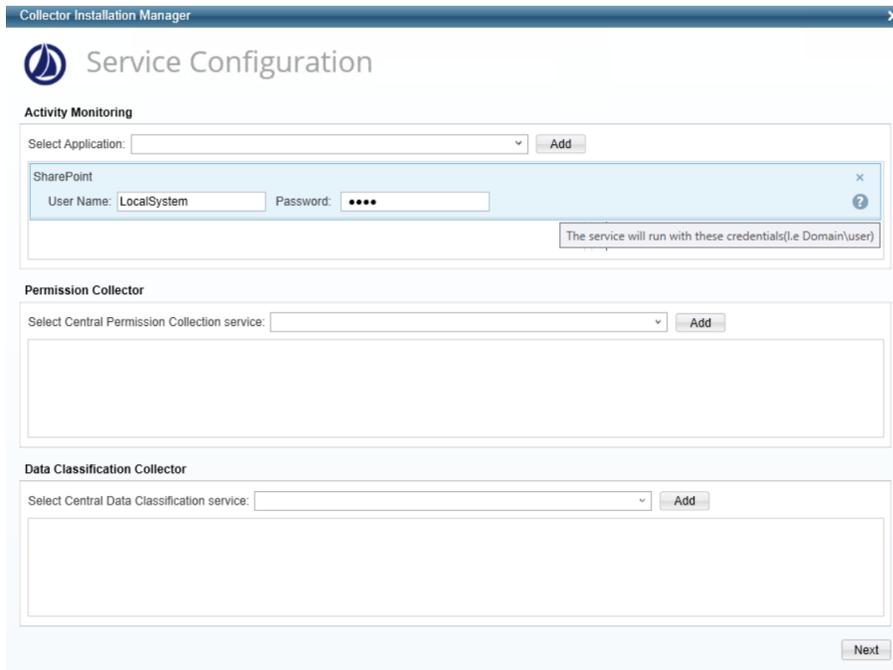
1. Run the **Collector Installation Manager** as an Administrator.
The installation files are in the installation package under the folder **Collectors**.

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. 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 EMC Celerra Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Activity Monitor - <Application_Name>.
- File Access Manager Permissions Collection - <Application_Name>.
- File Access Manager Data Classification - <Application_Name> .

Log Files

Check the log files listed below for errors

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

Verifying Monitored Activities

1. Simulate activities on the CIFS/NFS 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 in the business website.
2. Verify that:
 - The tasks completed successfully
 - Business resources were created on the BRs tree
 - Permissions display in the Permission Forensics window

Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

Activities not Collected by the Activity Monitor

If activities are not collected by the Activity Monitor, we need to track the status of the components, starting from the data mover to the Activity Monitor service.

Log in to the data mover with your administrative user, and follow the suggestions below:

- **Verify the CEPA facility status on the data mover**

Use the command:

```
server_cepp <data mover> -service -status
```

Output:

```
server_2 : CEPP Started
```

- **If the CEPA isn't listed as "Started"**

Start it with the following command:

```
server_cepp <data mover> -service -start
```

- **Display information about the CEPA service**

Use the following command:

```
server_2 : CEPP Started
```

```
server_cepp <data mover> -pool -info
```

Output:

```
server_2 :
```

```
pool_name = sepapool
```

```
server_required = yes
```

```
access_checks_ignored = 0
```

```
req_timeout = 5000 ms
```

```
retry_timeout = 25000 ms
```

```
pre_events =
```

```
post_events =
```

```
OpenFileRead,CreateFile,FileWrite,FileRead,CreateDir,De-
```

```
leteFile,De-
```

```
leteDir,CloseModi-
```

```
fied,RenameFile,enameDir,SetAclFile,SetAclDir,SetSecFile,SetSecDir
```

```
post_err_events =
```

```
CEPP Servers:
```

```
ip = [ip address of the CEE server], state = ONLINE, status = ONLINE
```

- Make sure the post events correspond to the definitions described in the prerequisites section
- **If the state and status are not both ONLINE**

There might be a problem with the connection to the CEE service, or with the connection between the CEE service and the Activity Monitor service.

The CEPA facility is delicate to communication errors and in some cases the CEE does not recover from a

communication failure.

- Make sure all the prerequisites were set.
- Make sure the CEE service is running with a domain user who is an administrator on the CEE service server.
- Make sure the CEE service and the physical data mover CIFS server are joined to the same active directory domain.
- Make sure the CEPA ip address listed in the output of the command above matches the IP address of the server running the CEE service
- Make sure there is no firewall between the data mover and the server running the CEE service
- Make sure the windows firewall is off on the server running the CEE service
- **Try restarting the services**
 - Stop the CEPA facility with the following command:

```
Server_cepp <data mover> -service -stop
```
 - Stop the EMC CEE service on the CEE server and the Activity Monitor service.
 - Start the CEPA facility
 - Start the EMC CEE service, wait for 60 seconds
 - Start the Activity Monitor service
 - Wait for 60 seconds, and issue the comand `server_cepp <data mover> -pool -info` again

State and Status ONLINE, but no Events are Shown

If the state and status are both ONLINE, but no events are shown, check the event counters, in the data mover, using the following command:

```
server_cepp <data mover> -pool -stats
Output:
server_2 :
pool_name = pool1
Event Name Requests Min(us) Max(us) Average(us)
OpenFileWrite 2 659 758 709
CloseModified 2 604 635 620
Total Requests = 4
Min(us) = 604
Max(us) = 758
Average(us) = 664
```

Look at the count of the different events.

Issue the command a few more times and verify that the counters increase.

Those counters represent the total number of requests for all the CIFS server in all the virtual data movers. If the counters do not increase, it might be that no users are working on the CIFS server at the moment.

Counters Increase but no Events are Collected

If the counters increase, but no events are collected:

1. Check the statistics log file of the Activity Monitor to see if events are received by the Activity Monitor.
2. If no events are received by the Activity Monitor, validate the Application configuration:
 - a. Make sure the CIFS server name is properly configured in the Application filer name field. This value must be the actual name of the CIFS server name, and not the FQDN or one of the aliases.
 - b. If the CIFS server has aliases defined to it (validate that in the EMC management), make sure these aliases are defined under the aliases in the Application configuration.