



Integrating EMC Isilon 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**
 - Configuring Clusters with Multiple Access Zones 5
- Connector Overview** **6**
 - CEE 6
 - CEE & Activity Monitor 6
 - Activity Monitor 6
 - Permissions Collection Operation Principle 7
 - Monitored Activities 7
 - Sample Architecture 8
 - Multiple Access-Zone and Tenant Isolation Support 9
- Prerequisites** **11**
 - Software Requirements 11
 - How to Configure the CEE Service 11
 - Enable CEE Using Isilon OneFS WebUI 12
 - Enable and Configure Auditing Using CLI 12
 - Audit Event Configuration Using CLI 13
 - Required Permissions 13
 - Communications Requirements 15
- EMC Isilon Installation Flow Overview** **17**
- Collecting Data Stored in an External Application** **18**
- Adding an EMC-Isilon Application** **20**
 - Select Wizard Type 20
 - General Details 20
 - Connection Details 21
 - Configuring and Scheduling the Permissions Collection 24
 - Selecting and Scheduling the Data Classification Settings 33
 - Data Privacy 33
 - Configuring Activity Monitoring 34

| | |
|--------------------------------------------------------------------|-----------|
| Monitored Actions | 37 |
| Enabling Access Fulfillment for an Application | 37 |
| Installing Services: Activity Monitor and Collectors | 40 |
| Verifying the EMC Isilon Connector Installation | 43 |
| Verifying Application Configuration | 43 |
| Installed Services | 43 |
| Log Files | 44 |
| Verifying Monitored Activities | 44 |
| Permissions Collection | 44 |
| Troubleshooting | 45 |
| What if activities are not collected by the Activity Monitor | 45 |

Capabilities

File Access Manager can connect to EMC Isilon for:

- Storage structure analysis.
- Checking user permissions.
- Data classification.
- Performing access fulfillment.

This connector does not support Isilon NFS.

File Access Manager provides full support for multiple-access zones, and full tenant isolation, across all its Isilon connector components.

Configuring Clusters with Multiple Access Zones

There are several methods of configuring File Access Manager to support Isilon clusters containing multiple access zones:

Separate application per access zone

This is the recommended configuration. Set up each access zone as a new application in File Access Manager, adding the access zone in the Connection Details page.

Single application for the entire cluster

Configure one application for the Isilon cluster, regardless of access zones.

Leave the **access zone** field in the application configuration empty.

The File Access Manager configuration should mimic the way your organization uses the Isilon cluster and access zones. If you treat the access zones as different file servers - they should be configured as different applications in File Access Manager as well.

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>

CEE

- The CEE service is the EMC gateway for auditing. The Isilon OneFS communicates with the CEE service to receive event notifications.

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

- File Access Manager Connector for EMC Isilon uses EMC CEPA over the Common Event Enabler Framework (CEE, formerly known as CAVA) infrastructure to retrieve audit events from Isilon to access both CIFS files.
- Similarly, The connector uses the same CEE/CEPA architecture as the File Access Manager Connector for EMC Celera/VNX.
- The Activity Monitor for EMC Isilon can be installed on the same server as other EMC Celera/VNX CIFS/NFS Activity Monitors, and communicate with the same CEE service.
- The first Activity Monitor which is installed on a physical server creates the Activity Monitor service.
- Unlike other File Access Manager Activity Monitors, all subsequent Activity Monitors 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 Activity Monitor installed must be the LAST Activity Monitor uninstalled. If you uninstall the first Activity Monitor before uninstalling the other Activity Monitors, those Activity Monitors will not work, and it will not be possible to uninstall them.

This connector does not support Isilon NFS.

All activity monitors for access zones of the same cluster must be installed on the same File Access Manager server. See [Installing Activity Monitors for Access Zones of the Same Cluster](#) for more details.

Permissions Collection Operation Principle

- File Access Manager connects to the EMC Isilon OneFS shares and analyzes folders permissions.
- File Access Manager utilizes the Isilon OneFS Platform API to gather local users, groups and share permissions.

Monitored Activities

The following activities are monitored by the EMC Isilon 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.

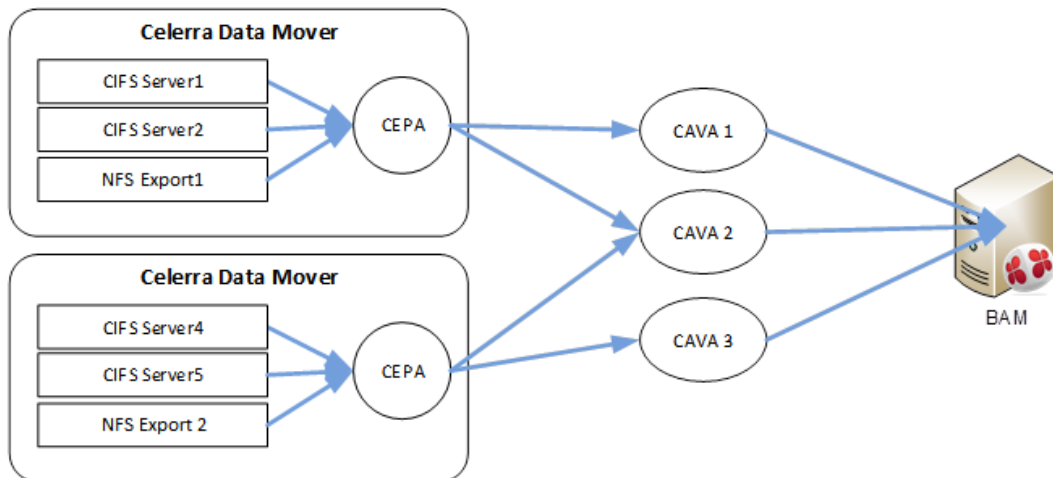
The second physical Data Mover is configured to send events to CEE 2 & 3. CEE 2 & 3 are configured to send event notifications to the Activity Monitor.

- 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



Multiple Access-Zone and Tenant Isolation Support

File Access Manager offers tenant isolation and full capabilities for multiple access-zones on Isilon Clusters. With the addition of the activity monitoring and permissions collection capabilities for multiple access-zones within an Isilon cluster and removing the dependency on the administrative (system)-zone-based OneFS API, each access zone within the cluster functions as an independent Isilon application within File Access Manager, with the complete set of File Access Manager capabilities.

This mode of access requires knowledge, connectivity and access rights of and to the managed access zone. This allows for a complete delegation of the configuration, administration and monitoring of an Isilon access zone to the tenant owner, and does not require centralized management. Tenant Isolation and management is critically valuable in multi-tenant hosted environments, where such isolation enhances data privacy and autonomous management.

The access zone and management API (optional) settings can be configured through the application configuration wizards.

With full tenant isolation, and full capability support for multiple access zones on the Isilon cluster, each access zone is treated as a separate entity.

Installing Activity Monitors for Access Zones of the Same Cluster

Due to limitations of the CEPA architecture, **all activity monitor services, monitoring access zones of the same cluster, must be installed on the same File Access Manager Server.**

The File Access Manager Isilon Activity Monitor is a multi-instance service, i.e. a single service serves multiple instances of the activity monitor, e.g., for the different access zones. As a result, only a single service will be created (and appear in the Windows Services list), however, this single service will create activity monitors instances for all the Isilon access zones it is configured to monitor.

There is no limitation to the number of clusters that can be monitor by a single File Access Manager service. Although all monitors for access zones of the same cluster must reside on the same File Access Manager server, activity monitors for other clusters and their access zones can also be installed on the same File Access Manager server, provided that sufficient resources are allocated for that machine.

We recommend that instances be added gradually, and resources be allocated appropriately to accommodate for the increase in activity volume, as the scope of the monitored environment grows, and more activity monitors are added to the server.

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](#) .

EMC Isilon

OneFS 7.1 and above.

EMC Common Event Enabler

CEE 6.5 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 CEE Using Isilon OneFS WebUI

1. Select "Cluster Management", then "Auditing"
2. Click "Enable Protocol Access Auditing"
3. Add Access Zone(s) you want to audit

Event Forwarding

Enter the uniform resource identifier (URI) where the CEE service is installed. The format of the entry is:

```
http://fully.qualified.domain.name:port/cee
```

Port

The default is 12228

Storage Cluster Name

Enter the same Host Name as in the File Access Manager Application configuration wizard.

Enable and Configure Auditing Using CLI

To enable auditing:

```
isi audit settings global modify --protocol-auditing-enabled on
```

To disable auditing:

```
isi audit settings global modify --protocol-auditing-enabled off
```

Add access zone to audit:

```
isi audit settings modify --audited-zones <ZONE>
```

View audit settings:

```
isi audit settings global view
```

Audit Event Configuration Using CLI

To enable specific audit events:

```
isi audit settings modify --audit-success create, rename, delete, read, write, get_security, set_security
```

To enable all audit events:

```
isi audit settings modify --audit-success all
```

To monitor all the activities listed under the Monitored Activates section

Enable all audit events.

Required 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 Access Zone:

- Share Read permissions to all shares
- Full Control permission for each normalized folder
- Member of the local Backup Operators group
- Member of the local Administrator group
- Permissions to access the OneFS Platform API

Add required permissions by creating a new role and associating the user with that role in one of the following ways:

Add Permissions via the Cluster Management Web Interface

1. Log in to the OneFS Cluster Management Web interface and performing the following actions:
2. Click on 'Access -> Membership and Roles'
3. Select the 'Role's tab
4. Click on the 'Create Role' button
5. Enter a name for the Role (ex. FileAccessManager)
6. Click on the 'Add a member to this role' button, and add the File Access Manager user which will be used in the Application configuration wizard
7. Scroll down and click on the 'Add a privilege to this role' button and add the following Privileges:
 - a. 'Platform API: Log in to the Platform API and WebUI' – read_only Access
 - b. Auth: Configure Identities and authentication sources – read_only Access
 - c. Audit: Configure audit capabilities – read_only Access
 - d. SMB: configure SMB server – read_only Access

Add Permissions via the Cluster Management Shell

Run the following commands from the cluster management shell:

```
isi auth roles create FileAccessManager
```

```
isi auth roles modify FileAccessManager --add-priv-ro=ISI_PRIV_LOGIN_PAPI
```

```
isi auth roles modify FileAccessManager --add-priv-ro=ISI_PRIV_SMB
```

```
isi auth roles modify FileAccessManager --add-priv-ro=ISI_PRIV_AUTH
```

```
isi auth roles modify FileAccessManager --add-priv-ro=ISI_PRIV_AUDIT
```

```
isi auth roles modify FileAccessManager --add-user='<domain>\<user>'
```

Add Permissions via built-in roles:

Associate the user with the SystemAdmin and SecurityAdmin built-in roles.

```
isi auth roles modify SystemAdmin --add-user='<domain>\<user>'
```

```
isi auth roles modify SecurityAdmin --add-user='<domain>\<user>'
```

Permissions Required for Each File Access Manager Task

The user must have the permissions listed below in order to perform these tasks:

Crawling

Share Read permissions to all the shares on the file server.

Be a member of the local Backup Operators group on the Access Zone.

Permission Collection

Share Read permissions to all the shares on the Access Zone.

Be member of the local Backup Operators group on the Access Zone.

Be a member of the local Administrators group to read the Share Permissions.

Permissions to the OneFS Platform API to read the local Users and Groups.

Access Fulfillment

Full Control permission on the normalized folders to be able to set the permissions.

Data Classification

Share Read permissions for all the shares on the Access Zone.

Be member of the local Backup Operators group on the Access Zone.

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 Isilon cluster | CEE Service | HTTP in the port defined under the prerequisites section |

Prerequisites

| Requirement | Source | Destination | Port |
|----------------------------------------------|---------------------------------------------------------------------|--------------------------------------|----------------------|
| OneFS Platform API | Activity Monitor and Permissions Collector | EMC Isilon | HTTP+HTTPS * 8080 |
| CEE Events Push | CEE Service | File Access Manager Activity Monitor | RPC (135 + Dynamic) |
| Permissions Collection & Data Classification | Permissions Collection service and / or Data Classification service | EMC Isilon | SMB |

For OneFS API state, the default port is 8080. The port is set by the administrator, and can be changed. Usually it will be 80, 8080 or 443. If this setting doesn't work, consult your Isilon administrator.

EMC Isilon Installation Flow Overview

To install the EMC Isilon connector:

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

In order to integrate with EMC Isilon, 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

EMC-Isilon

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

Host Name

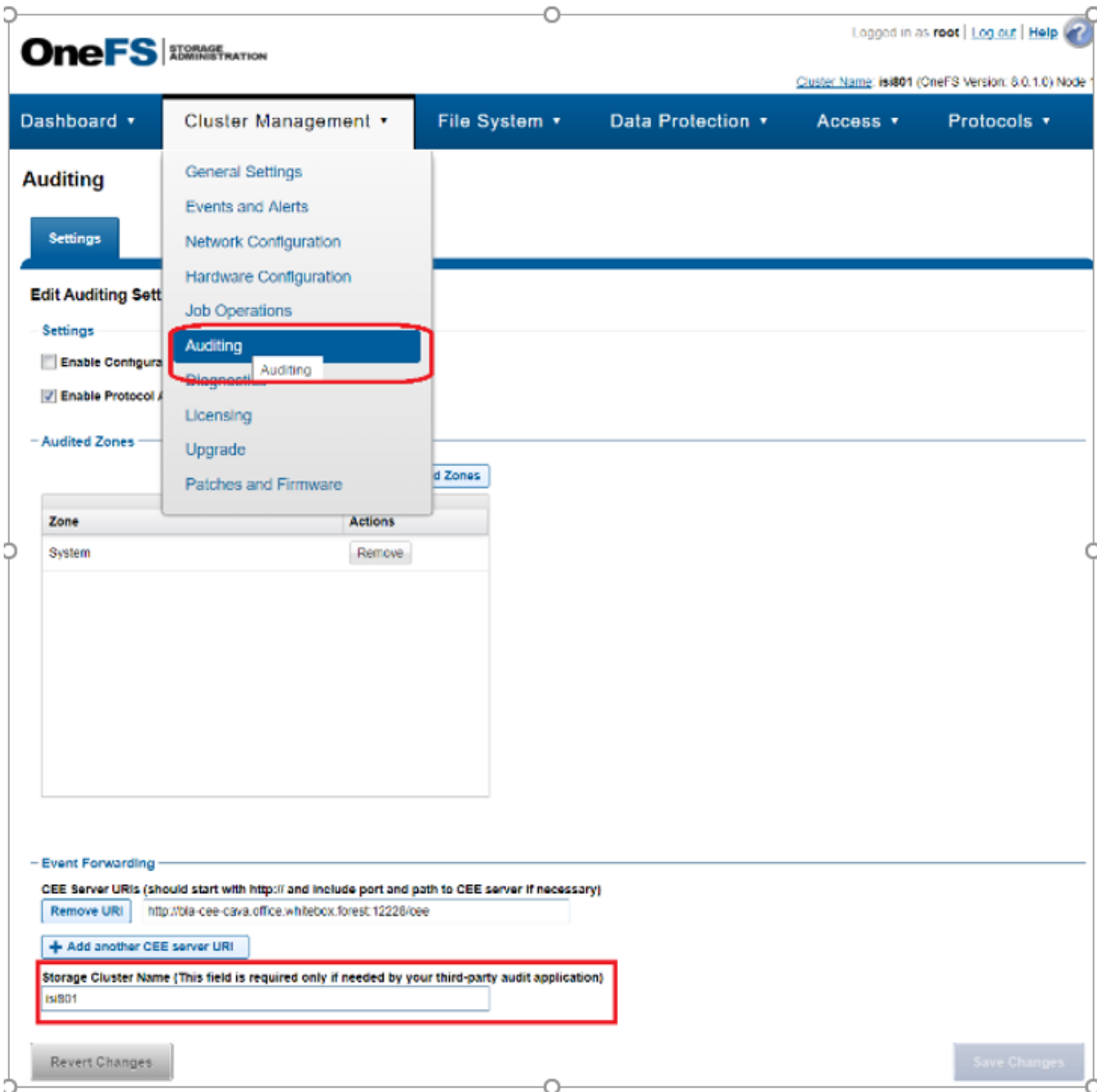
The real name used when connecting to the CIFS server. This will be used by the SMB (CIFS) protocol.

Domain Name, Username, Password

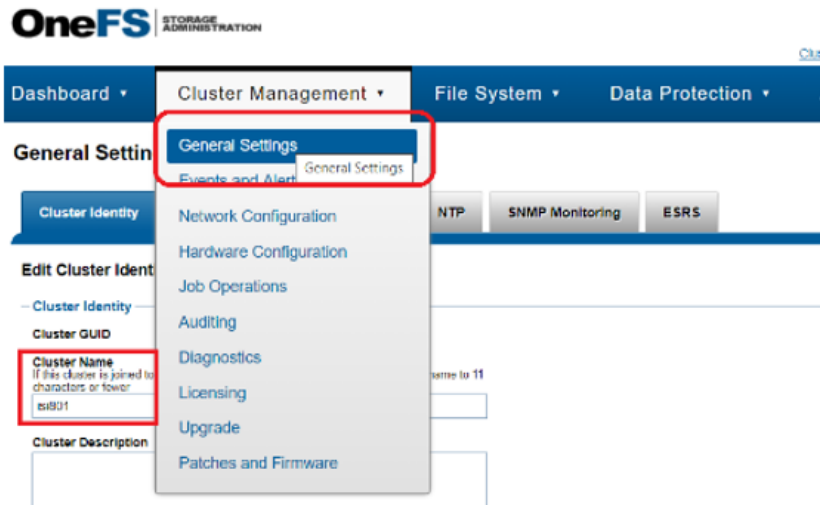
Credentials for the user defined in the prerequisites.

Storage Cluster Name

The name configured in the Auditing section of the Isilon OneFS Admin Console under the *Cluster Management >> Auditing settings tab.*



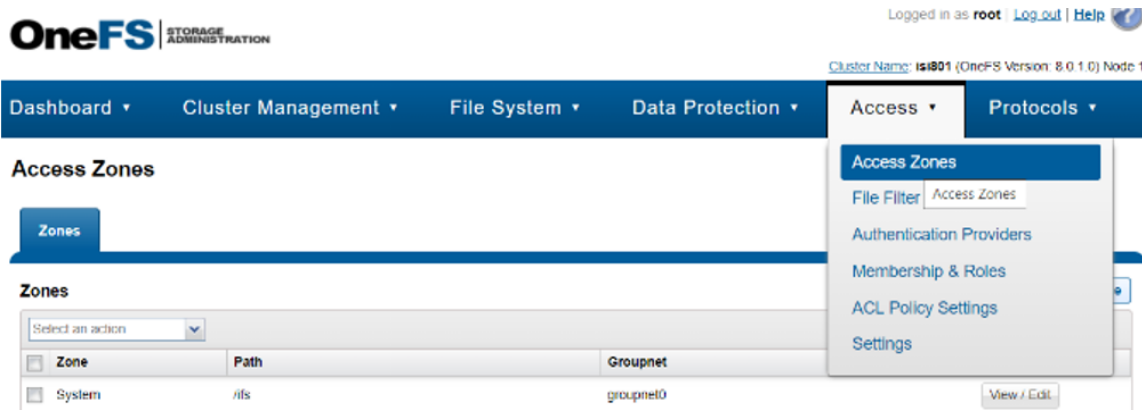
If this is not configured, the name of the Isilon cluster itself, under *Cluster Management* >> *General Settings*.



Access Zone

(Optional) Use this field if configuring a separate application per access zone. See [Configuring Clusters with Multiple Access Zones](#) for further details.

The name of the access zone as it is configured in the Isilon cluster configuration, in the Access section of the Isilon OneFS Admin Console, under *Access >> Access Zones*.



Use OneFS API

Click this checkbox to enable / disable access to the OneFS API, and reversely, disable / enable tenant Isolation.

OneFS API is located only on the System zone and is used by the permission collection and activity monitor components of the Isilon connector to fetch Share Information as well as local users and roles for each individual access zone.

Unchecking this will disable the activity monitor access to the API and the information will be collected solely using the SMB protocol, and access only the managed Access Zone. Access to the Management API is no

longer required for activity monitoring, and is skipped by default, using native SMB Access to the managed Access Zone instead.

However, you can choose to keep the old configuration and keep access the Management API on the System zone, to retrieve Share and Local Identities information.

Management IP

Valid only If access to the OneFS API is enabled, by checking the Use OneFS API checkbox above.

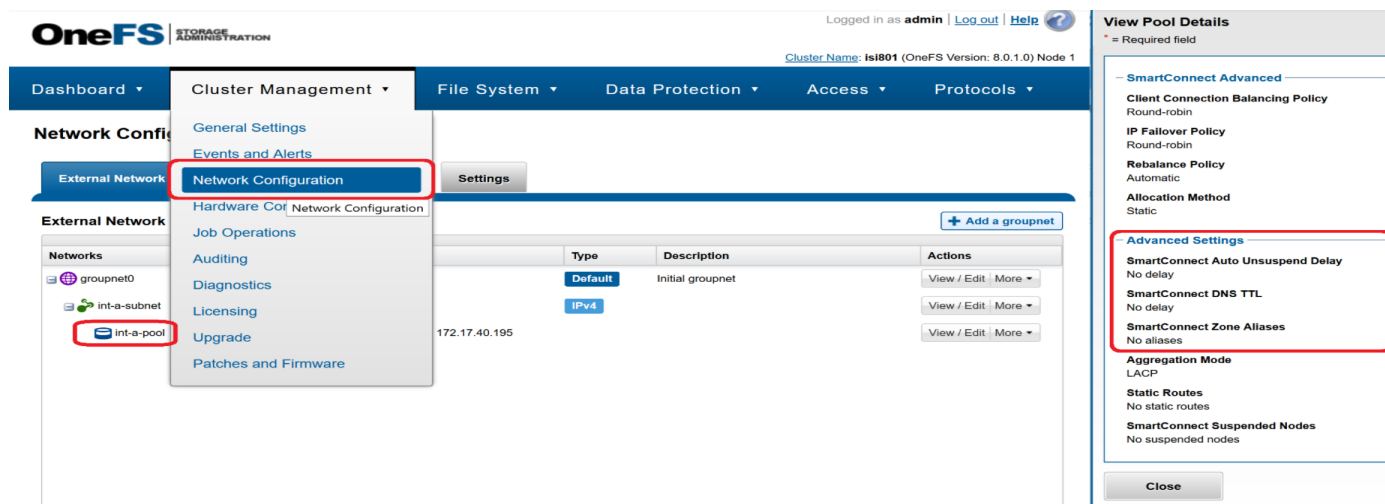
This field specifies the location of the Management API (System access zone).

This field accepts IP addresses and / or any resolvable DNS name (FQDN or otherwise).

Aliases

SmartConnect Zone Aliases used as alternative DNS Names for the CIFS Server. All aliases must be provided to ensure that all activities performed on that server, through all access paths, are monitored by File Access Manager.

These are available under the IP Pool Settings, in the Network Configuration section of the Isilon OneFS Admin Console, under the *Cluster Management >> Network Configuration* tab.



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

Calculate effective permissions during the permissions collection run.

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 Comments on Isilon for the CIFS server

The permissions are managed on the NTFS level, or on the Share Level (as when the shares are configured with Full Control to everyone, and all the permissions are defined in the folders, in which case you should select NTFS, which is the 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 “|” .

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

Last Successful Run 06-22-2021 4:57:27 PM

[Run Task](#) [View Task Status](#)

Note: Refresh the list to view recently discovered resources [Refresh](#)

Top Level Resources Exclusion List 0 Selected | Clear Selection

Top Level Resources Exclusion List ^

- \\si-...-5\C\$
- \\si-...-5\MSSQLSERVER
- \\si-...-5\print\$

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 > Activity Monitoring > Data Enrichment Connectors).

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., \\servername\share1\folder1.

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, 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.

When an Activity From a New Resource is Detected

Store the activity (Full Auto-Learning Mode)

Store the activity only if the top-level resources were manually created in advance (Semi Auto-Learning Mode)

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.

Click **Next**.

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.

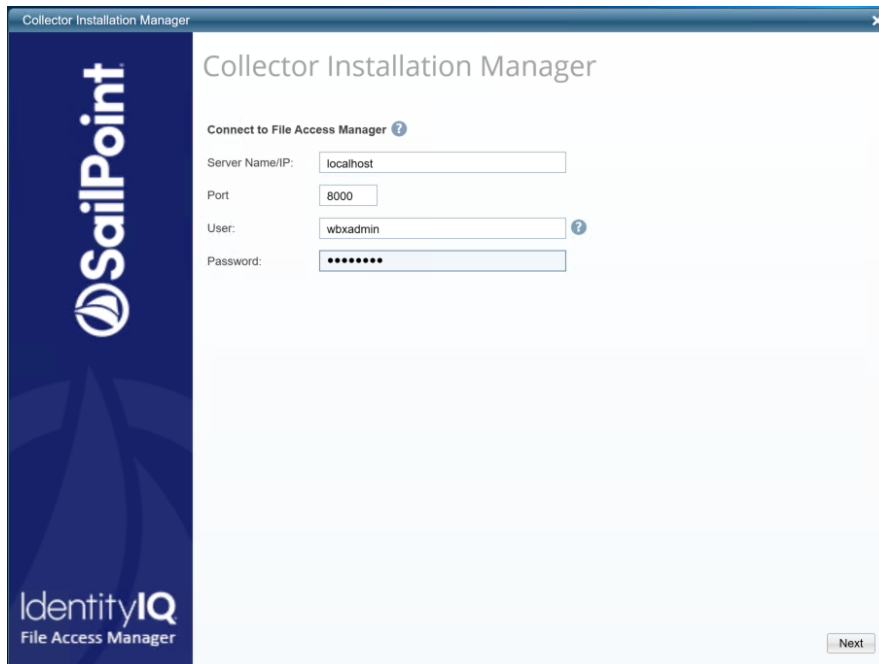
Installing Services: Activity Monitor and Collectors

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.

1. Run the **Collector Installation Manager** as an Administrator.

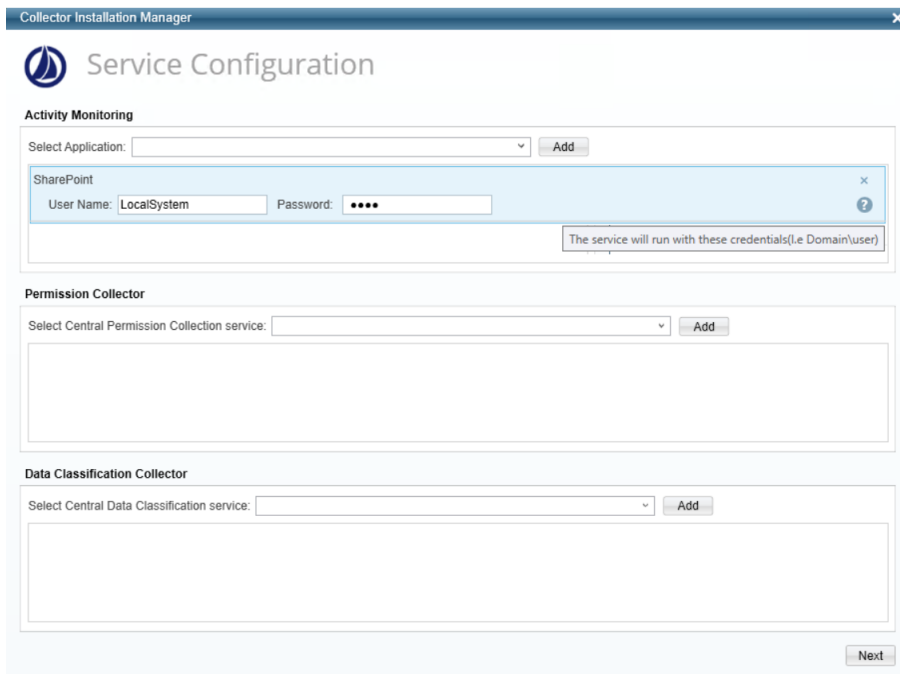
The installation files are in the installation package under the folder Collectors.

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 Isilon Connector Installation

Verifying Application Configuration

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

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

Common Isilon Validations

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

- Server responsiveness
- Verifying the ability to list shares
- Verifying the ability to read share permissions
- Verifying the membership to the Backup Operators group
- Verifying access to the OneFS API
- Verifying the audit setting are correct on the Isilon server
- Verifying the Activity Monitoring event listener is running

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 storage system.
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.

What if activities are not collected by the Activity Monitor

1. If activities are not collected by the Activity Monitor, the status of the components should be tracked, from the Isilon OneFS to the Activity Monitor service.
2. Log in to the OneFS as an administrative user.
3. Type the following command to display the audit events stored on the Isilon:

```
isi_audit_viewer -t protocol
```

Isilon is properly configured for auditing if the command results in a display of events. Check all the CEE and Activity Monitor configurations described above.

4. Run the following command:

```
isi audit settings view
```

5. Verify that the CEE URL is correct, and that the host name configured matches the host name configured in the Application configuration.
6. Verify that the CEE server is accessible in the configured port from the Isilon by pinging it, and running telnet to the configured port.
7. Run the following command:

```
isi zone zones view [Zone Name]
```

8. Make sure the Zone is configured for all event types to be monitored.

Advanced troubleshooting:

1. The file `/var/log/isi_audit_cee.log` on the Isilon contains the internal `audit_cee` process log. Use the “`cat`” command to view its contents.
2. If no content is displayed, raise the debugging level of the process by running the following command:

```
isi_ilog --level debug+ --application isi_audit_cee
```

3. To make the process change log levels, make a change to the audit configuration in order to see the log line.

The following lines indicate a problem with the CEE connection:

- a. 2014-02-20 12:49:17 vwjaws2-1 isi_audit_cee[65098][0x800d020b0]: DEBUG: deliver_event: No CEE servers available.
 - b. 2014-02-20 12:49:17 vwjaws2-1 isi_audit_cee[65098][0x800d05da0]: DEBUG: heart-beater: available servers: []
4. When finished, lower the log level to info.
 5. If none of the above helps, we can use a tool called **DebugView** (Part of Windows Sysinternals) to help us see debug messages from the CEE:
 - a. Download DebugView (<https://technet.microsoft.com/en-us/sysinternals/debugview.aspx>).
 - b. Extract to an accessible folder on the CEE server.
 - c. Run `Dbgview.exe`.