



Integrating HDS with File Access Manager

Version: 8.2 Revised: July 01, 2021

Copyright and Trademark Notices.

Copyright © 2021 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
Supported Versions	5
Connector Overview	6
Activity Monitor	6
Permissions Collector	6
Prerequisites	7
Software Requirements	7
Permissions	7
How to Configure the HNAS Audit Settings	8
How to Configure the Audit Log Consolidated Cache	8
How to Configuring Share Auditing	8
Communications Requirements	9
Connector Installation Flow Overview	10
Collecting Data Stored in an External Application	11
Adding an HDS Application	13
Select Wizard Type	13
General Details	13
Connection Details	14
Configuring and Scheduling the Permissions Collection	14
Scheduling a Task	15
Configuring and Scheduling the Crawler	16
Setting the Crawl Scope	17
Including and Excluding Paths by List	17
Excluding Paths by Regex	17
Crawler Regex Exclusion Examples	18
Exclude all shares which start with one or more shares names:	18
Include ONLY shares which start with one or more shares names:	18

Narrow down the selection:	18
Excluding Top Level Resources	19
Special Consideration for Long File Paths in Crawl	20
Selecting and Scheduling the Data Classification Settings	21
Configuring Activity Monitoring	22
Monitored Actions	23
Configuring Data Enrichment Connectors	23
Enabling Access Fulfillment for an Application	24
Installing Services: Collector Installation	26
Verifying the HDS Connector Installation	28
Installed Services	28
Log Files	28
Monitored Activities	28
Permissions Collection	28

Capabilities

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

See the IdentityIQ File Access Manager documentation for a full description.

Supported Versions

- HDS supports the File System Audit in HNAS version 11 and above.
- Permissions Collections and Data Classification supports all HNAS versions.

Connector Overview

Activity Monitor

IdentityIQ File Access Manager uses the HNAS File System Audit to monitor file system events. Once the audit is configured on the HNAS EVS, HNAS starts collecting events, and displays them in a Windows Event Log-like interface. The IdentityIQ File Access Manager HDS Activity Monitor remotely connects to the HNAS every 5 seconds to read and process new events, which it then sends to central servers every predefined interval.

The system generates events on HNAS only on shares or folders enabled for auditing. HNAS lets you define the event types and logged in users to monitor the Advanced Security Settings > Auditing tab of a share or folder.

Events received from HNAS contain the full physical path of the file, and not the share path. The Activity Monitor periodically correlates all shares and share mapping to physical paths, and translates the physical paths of events to their corresponding share paths. If the physical path is mapped to more than one share, the event is duplicated in all the matching share paths.

Permissions Collector

IdentityIQ File Access Manager must first run a crawl process to discover shares and folders on the HNAS.

The IdentityIQ File Access Manager Permissions Collector service connects remotely to these shares and folders, and analyzes their permissions.

Prerequisites

Make sure your system fits the descriptions below before starting the installation.

Software Requirements

IdentityIQ 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](#).

Permissions

IdentityIQ File Access Manager requires different permissions, based on the tasks to perform. The user configured in the Application configuration wizard must have the following permissions on the HNAS:

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

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

Activity Monitoring

The user must be a member of the local Administrator group on the HNAS

Crawling

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

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

Permission Collection

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

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

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

Access Fulfillment

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

Data Classification

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

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

How to Configure the HNAS Audit Settings

1. Log into the Hitachi NAS console using administrator credentials.
2. Navigate to Home > File Services > File System Audit Policies.
3. Select the EVS for which auditing will be enabled.
4. Click **add**.
5. The Add File System Audit Policy page opens to display a set of audit policy default settings.
6. Set the maximum log file to a value of at least 8MB (16MB is recommended) in the *Audit Log* section.
7. Select New or Wrap (Wrap is recommended) in the *Log roll over policy* section.
8. Click **OK**.
9. Repeat Steps 4 and 5 to enable auditing in additional EVS file systems.

How to Configure the Audit Log Consolidated Cache

1. Log into the Hitachi NAS Admin Services' EVS using SSH with administrator credentials.
2. Execute the following command to switch from admin EVS to file services EVS:

```
console-context --evs <EVS name>
```

3. Execute the following command to configure the audit log consolidated cache:

```
audit-log-consolidated-cache add -s <Size> <EVS name>
```

For example, in *audit-log-consolidated-cache add -s 50MB [file system name]*, the [file system name] is the name of the EVS file system on which the audit log consolidated cache file is stored. It is recommended that disk space of at least 50 MB be provisioned for an audit log consolidated cache to avoid losing events. It is also recommended that a new file system be created for the audit log consolidated cache.

4. Increase the size of the Event Pool in the EventLogEventCache by running the following command:

```
fsm set auto-heap-pool-sizeEventLogEventCache::Event 200000
```

The pool limit can be increased to 200,000, which is enough for a 50 MB audit log consolidated cache.

How to Configuring Share Auditing

1. Open Computer Management (run *compmgmt.msc*).
2. Click *More Actions > Connect to another computer*.
3. Type the IP or DNS of the EVS.
4. Click **OK**.
5. Navigate to *System Tools > Shared Folders > Shares*.
6. The EVS shares display on the right.
7. Right click on a share, and select *Properties*.
8. Click the *Security* tab.

9. Click **Advanced**
10. The Advanced Security Settings window displays.
11. Select the *Auditing* tab.
12. Click **Add** or **Edit** to add/edit users/groups to be audited.
13. Select *Everyone* to make the EVS log events for all users.
14. Select *Success* in the *Type* field.
15. Select *Full Control* in the *Basic Permissions* field.
16. Repeat to audit additional shares.

To avoid unnecessary overhead, define only those users or groups to be monitored, as well as any actions required for monitoring. (For example, removing Read will result in much less overhead on the HNAS.)
HSD may provide more information on how to avoid unnecessary overhead.

17. Generate activity on the shares created in a required file system in order to verify if auditing is enabled on the EVS for that file system.
18. Execute the following command on the Hitachi NAS Console to see if the events are generated:

```
audit-log-show <Name of file system>
```

Communications Requirements

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector / Data Classification Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ File Access ManagerServers	8000-8008
Collecting Events	Activity Monitor	HDS	MSRPC (135)
Permissions Collection	Permissions Collector	HDS	SMB (139/445)
Data Classification	Data Classification	HDS	SMB (139/445)

Connector Installation Flow Overview

To install the HDS connector:

1. Configure all the prerequisites.
2. Add a new HDS application in the Business Website.
3. Install the relevant services:
 - Activity Monitor
 - 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 IdentityIQ File Access Manager deployment architecture. The IdentityIQ File Access Manager Administrator Guide has additional information on the architecture.

Collecting Data Stored in an External Application

Connector / Collector terminology:

Connector

The collection of features, components and capabilities that comprise IdentityIQ 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 IdentityIQ 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 IdentityIQ File Access Manager Administrator Guide

Adding an HDS Application

In order to integrate with HDS, we must first create an application entry in IdentityIQ 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

HDS

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/IdentityIQ 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**.

Connection Details

Server Name

The name of the HNAS filer to which users connect

Domain Name

The user defined in the prerequisites

Username

The user defined in the prerequisites

Password

The user defined in the prerequisites

Click **Next**

Configuring and Scheduling the Permissions Collection


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

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

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

If the "IdentityIQ FAM 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 IdentityIQ File Access Manager Administrator Guide for further details.

Calculate Effective Permissions

Calculate effective permissions during the permissions collection run

Calculate Riskiest Permissions

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

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

Skip Identities Sync during Permission Collection

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connectors.

This option is checked by default.

Permissions Source

NTFS, Share, Both

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

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 Resources' 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. See the example below in section [Business Resource Structure](#) to better understand the business resource full path structure.

Crawler Regex Exclusion Examples

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

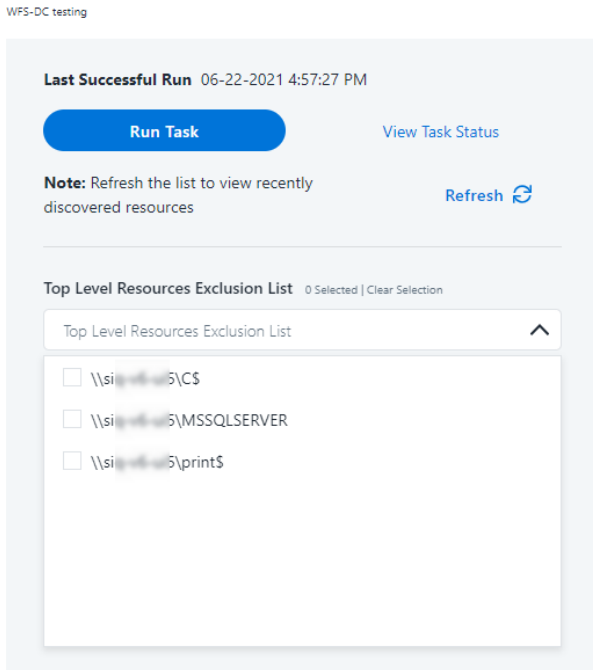
Settings > Task Management > Tasks

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



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 IdentityIQ File Access Manager Administrator Guide for more information

Click **Next** or **Finish**.

Configuring Activity Monitoring

Configure the activity monitoring process frequency.

Polling Interval (sec)

Activity fetching interval [in seconds]. Default is set to 60 seconds,

Report Interval (sec)

Activity Monitor Health reporting interval [in seconds]. Default is set 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.

more quWhen 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)

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 > Activity Monitoring > Data Enrichment Connectors*). After creating a new DEC, Click **Refresh** to refresh the dropdown list.

The chapter **Connectors** of the IdentityIQ 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

- 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: Collector Installation

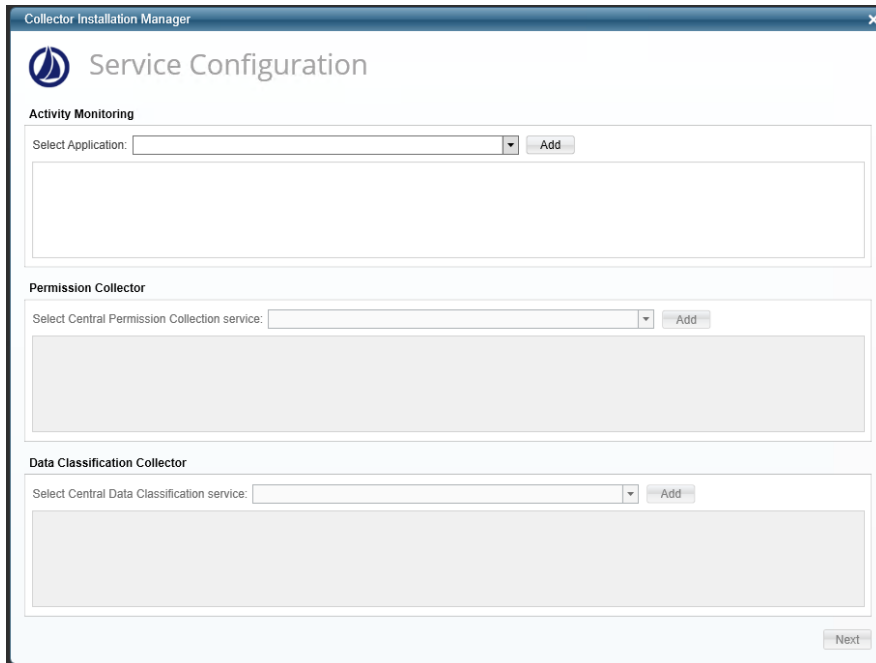
1. Run the **Collector Installation Manager** as an Administrator.
The installation files are in the installation package under the folder **Collectors**.

The Collector Installation Manager window displays.



2. Enter the credentials to connect to IdentityIQ File Access Manager.
 - a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
 - b. An IdentityIQ 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 Monitoring collector, select the application, and click **Add**.

In some applications, additional credentials may be required to allow granting elevated permission for activity monitoring collection.

5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**
6. If you are installing the Data Classification, select the Central Classification Collector to which to connect this service, and click **Add**
7. Click **Next**.

The Installation Folder window displays.

If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

8. Browse and select the location of the target folder for installation.
9. Browse and select the location of the folder for system logs.
10. Click **Next**.
11. The system begins installing the selected components.
12. Click **Finish**

The Finish button is displayed after all the selected components have been installed.

The *IdentityIQ File Access Manager Administrator Guide* provides more information on the collector services.

Verifying the HDS 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 IdentityIQ File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Permissions Collection - <Service Name>
- File Access Manager Central Activity Monitor - <Service Name>
- File Access Manager Central Data Classification - <Service 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%\HDS-<Application_Name>.log"
- .

Monitored Activities

1. Simulate activities on the HNAS.
2. Wait a minute (approximately).
3. Verify that the activities display in the IdentityIQ 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*)