SailPoint IdentityIQ

Version: 8.0

File Access Manager EMC Isilon Connector Installation Guide

Table of Contents

List of Figures

List of Tables

Table of Revisions

Version #	Description	Author	Date
5.0	Final Version	Jonathan Rappeport	10 Jan 2017
5.1	First Draft	Jonathan Rappeport	08 Feb 2017
5.1	Second Draft	Jonathan Rappeport	13 Jun 2017
5.1	Third Draft	Jonathan Rappeport	26 Sep 2017
6.0	First Draft	Jonathan Rappeport	10 May 2018
6.1	Formatting changes only	Josh Lewin	11 Dec 2018
8.0	• Formatting. • Rebranding to fit IdentityIQ File Access Manger terms and screens	Josh Lewin	30 Jul 2019
	Port update for OneFS API platform	Josh Lewin	18 Sep 2019

Chapter 1: Connector Installation & Configuration

Overview

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Admin Client.
3. Install the Activity Monitor/Permissions Collector/Data Classification Collector services.
4. Special note: If working on a non-system access zone, refer to ***Configuring the collectors to work with a non-system Access Zone*** on page 17

Note: Permission Collector and Data Classification services installation 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 IdentityIQ File Access Manager architecture.

Chapter 2: General

Activity Monitor Operation Principles

- IdentityIQ 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.
- Similar, The IdentityIQ File Access Manager Connector for EMC Isilon uses the same CEE/CEPA architecture as the IdentityIQ 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 are installed, and communicate with the same CEE service.

Permissions Collector Operation Principle

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

Monitored Activities

Table 1. Monitored Activities

Action	Meaning
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.

Supported Versions

- EMC Isilon OneFS 7.1 and above.
- EMC Common Event Enabler CEE 6.5 and above.

Chapter 3: Overview

CEE

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

CEE & IdentityIQ File Access Manager 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 Service

The Connector for EMC Isilon can be installed on the same server as other EMC Celera/VNX CIFS/NFS Activity Monitors are installed and communicate with the same CEE service.

The first Activity Monitor which is installed on a physical server creates the Activity Monitor service. Different than other IdentityIQ File Access Manager Activity Monitors, from that moment 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.

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

Chapter 4: Prerequisites

Configure the CEE Service

If the CEE is not installed, the EMC CEE documentation provides installation instructions.

Refer to the IdentityIQ File Access Manager EMC Celera and VNX Connector Installation Guide for information on how to configure the 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) that need to be audited.
4. In the Event Forwarding section, 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
   The default port is 12228
5. Storage Cluster Name – Enter the same Host Name as in the IdentityIQ File Access Manager Application configuration wizard.

Enable and Configure Auditing Using CLI

1. To enable auditing:

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

2. To disable auditing:

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

3. Add access zone to audit:

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

4. View audit settings:

```
isi audit settings global view
```

Audit Event Configuration Using CLI

1. To enable specific audit events:

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

2. To enable all audit events:

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

3. To monitor all the activities listed under the Monitored Activates section, enable all audit events.

Required Permissions

IdentityIQ 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_write Access
    c. Privilege: Create new roles and assign privileges – read_write Access
    d. SMB: configure SMB server – read_write 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=ISI_PRIV_LOGIN_PAPI
isi auth roles modify FileAccessManager --add-priv=ISI_PRIV_SMB
isi auth roles modify FileAccessManager --add-priv=ISI_PRIV_AUTH
isi auth roles modify FileAccessManager --add-priv=ISI_PRIV_ROLE
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>'
```

The following describes, in detail, the permissions required by each IdentityIQ File Access Manager task:

Crawling

- The user must have Share Read permissions to all the shares on the file server.
- The user must be a member of the local Backup Operators group on the Access Zone.

Permission Collection

- The user must have Share Read permissions to all the shares on the Access Zone.
- The user must be member of the local Backup Operators group on the Access Zone.
- The user must be a member of the local Administrators group to read the Share Permissions.
- The user must have permissions to the OneFS Platform API to read the local Users and Groups.

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 Access Zone.
- The user must be member of the local Backup Operators group on the Access Zone.

Communications Requirements

Table 2. Communications Requirements

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

Note: 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.

Software Requirements

- **Activity Monitor**: .NET 4.5

- **Permissions Collector**: .NET 4.5.
- **Data Classification Collector**: .Net 4.5.

Chapter 5: Add New Application Wizard

1. Admin Client Navigate to **System → Applications → New → Application**

   The New Application Wizard window displays under the Welcome tab

2. Select Standard Application
3. Select EMC Isilon as the application type
4. Click Next

   The General Details window of the New Application Wizard displays under the General tab.

5. Type the logical name of the application in the Name field
6. Type a description of the application in the Description field
7. Select a logical container for the application from the Container dropdown menu
8. Select an identity collector from the Identity Collector dropdown menu
9. Click **Next.**

The Configuration window of the New Application Wizard displays under the Configuration tab.

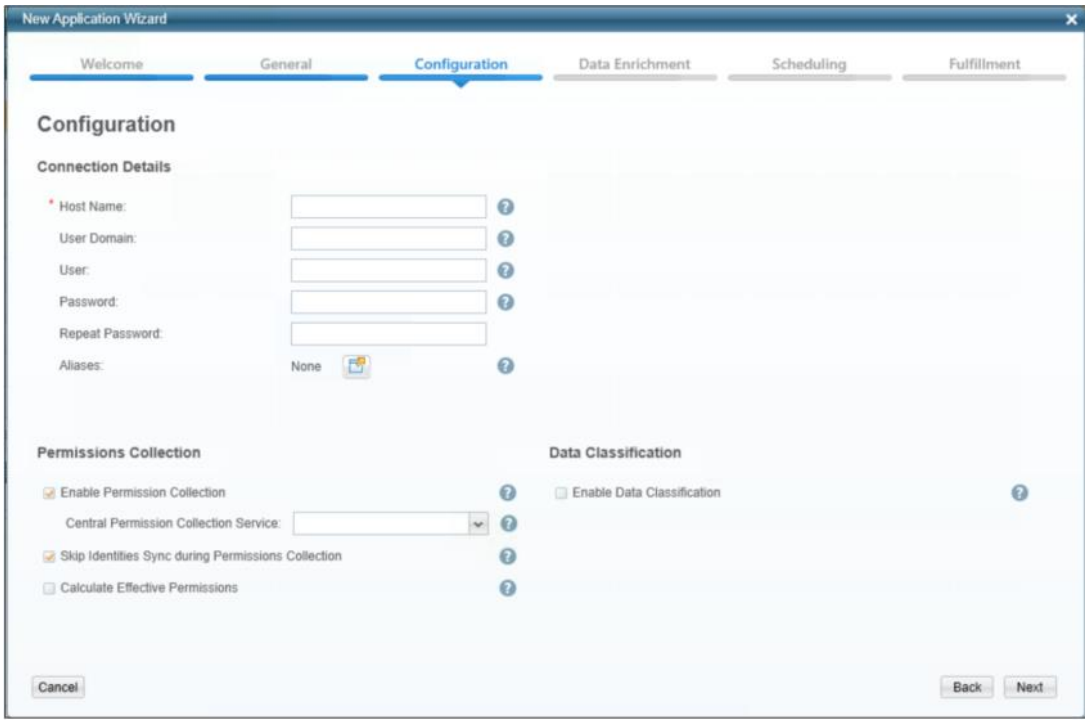

Figure 1. Configuration Window I

10. Complete the Connection Details fields:

    - *Host Name* (The real name of the CIFS server as users connect to it). **This must be identical to the host name configured above.**
    - *User Domain*, *User*, & *Password* (for the user defined in the prerequisites)
    - *Aliases* (aliases defined in the Isilon for the CIFS server)

11. Click to enable Permission Collection, select a central permissions collection service and complete the relevant Permissions Collection items:

    - *Skip Identities Sync* (Skip identity synchronization before running permission collection tasks when the identity collector is common to many different connectors.)
    - *Calculate Effective Permissions* (Calculate the effective permissions during the permissions collection run (not recommended unless required.)

    Note: 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).

12. Click to enable Data Classification and select a central data classification service from the list

13. Click **Next**

The second Configuration window of the New Application Wizard displays under the Configuration tab.

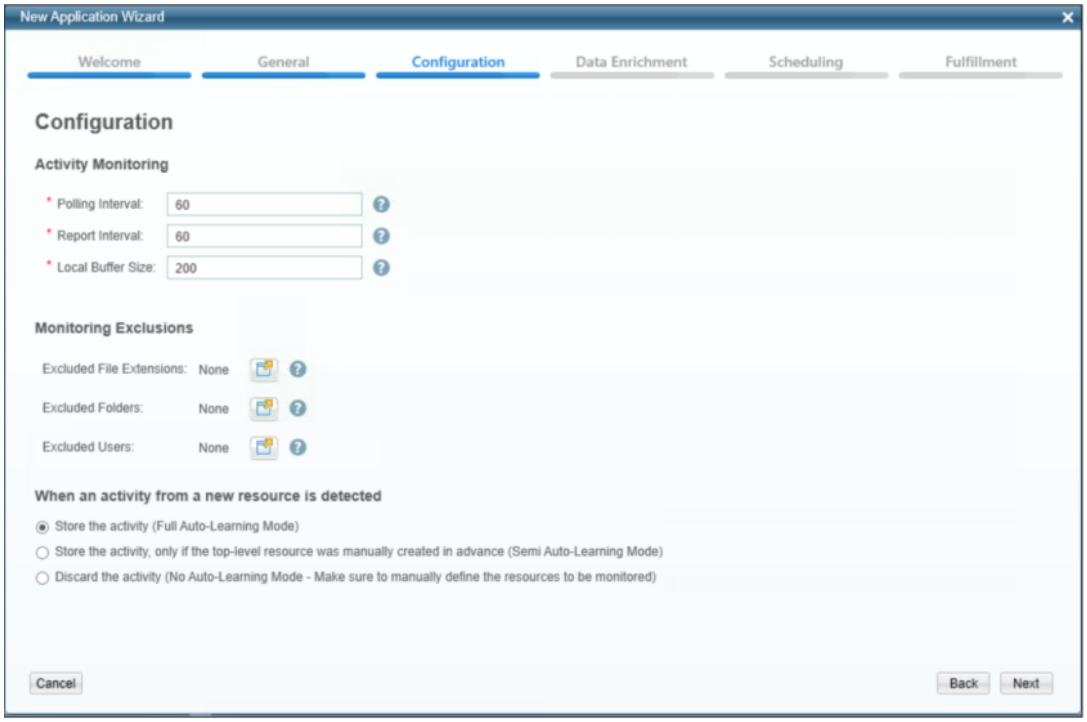

Figure 2. Configuration Window II

14. Select the relevant Monitoring Behavior items:

- *Polling Interval* (Activity fetching interval [in seconds])
- *Report Interval* (Activity Monitor Health reporting interval [in seconds])
- *Local Buffer Size (*Local buffer size for activities [in MB])

Note: This cyclic buffer stores activities on the Activity Monitor machine in case network errors prevent activities from being sent.

15. Select the Monitoring Configuration options.

- *Excluded File Extensions (*List of file extensions that are not monitored)
- *Exclude Folders* (List of folders that are not monitored)
- *Exclude Users* (List of users whose activities are monitored)

Note: Each excluded user must be in the form of Domain/User

When an activity from a new resource is detected:

- **Store the activity** (Full Auto-Learning Mode) - Monitors all activities from all site collections (automatically creates new folders in the Business Resources Tree).
- **Store the activity, only if the top-level resource was manually created in advance** (Semi Auto-Learning Mode - Monitors only manually defined resources and their sub-folders to be monitored.
- **Discard the activity** (No Auto-Learning Mode—Make sure to manually define the resources to be monitored)—Monitors only manually-defined resources to be monitored.

The Data Enrichment Connectors window of the New Application Wizard displays under the Data Enrichment tab.

16. Select the data enrichment connectors (DECs) to enrich monitored activities from the Available DECs text box and use the > or >> arrows to move them to the Current DECs text box.

Note: See the chapter *Activities* in the of the IdentityIQ File Access Manager Administrator Guide for more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

17. Click **Next.**

Note: The Scheduling tab contains the Permissions Collection, Crawler, and Data Classification (if supported) scheduling windows. You can navigate among those windows, using the Next and Back buttons.

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

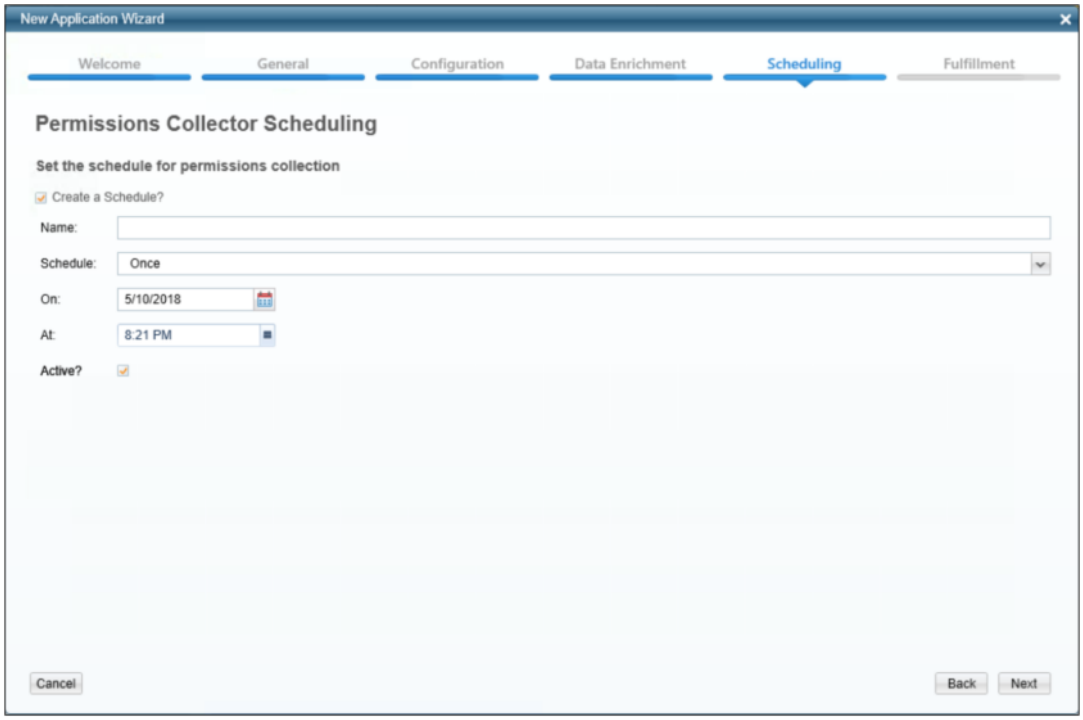

Figure 3. Permissions Collection Window

18. Select **Create a Schedule**.

19. Type a name for the permissions collection scheduling task in the *Name* field.

20. Select a scheduling frequency from the **Schedule** dropdown menu.

21. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).

22. Select **Active** if relevant.

23. Click **Next**.

The Crawler window of the New Application Wizard displays under the Scheduling tab.

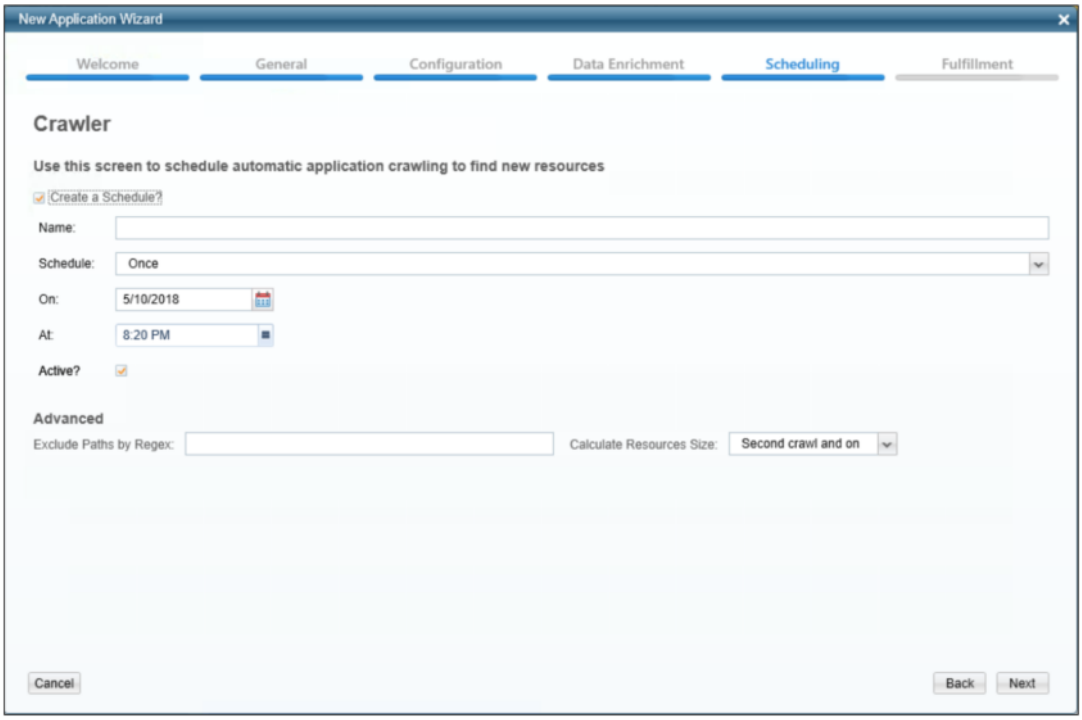

Figure 4. Crawler Window

24. Select **Create a Schedule**.
25. Type a name for the crawling scheduling task in the *Name* field.
26. Select a scheduling frequency from the **Schedule** dropdown menu.
27. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
28. Select **Active** if relevant.
29. Type in the names of folders to exclude from the crawling process in the *Exclude Paths by Regex* field.

    Note: See the chapter *Crawling* in the IdentityIQ File Access Manager Administrator Guide for more information.
30. Click **Next**.

The Data Classification window of the New Application Wizard displays under the Scheduling tab.

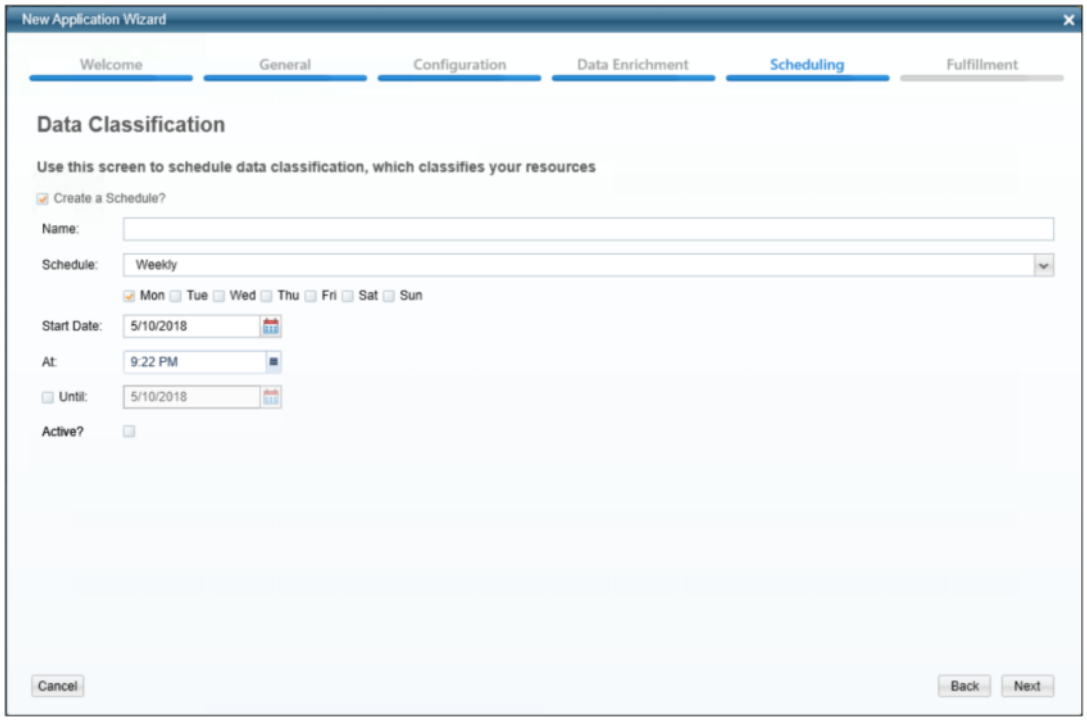

Figure 5. Data Classification Window

31. Select **Create a Schedule**.
32. Type a name for the data classification scheduling task in the *Name* field.
33. Select a scheduling frequency from the **Schedule** dropdown menu.
34. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
35. Select **Active** if relevant.

    Note: See the chapter *Data Classification* in the IdentityIQ File Access Manager Administrator Guide for more information

36. Click **Next**

The Access Fulfillment window of the New Application Wizard displays under the Fulfillment tab.

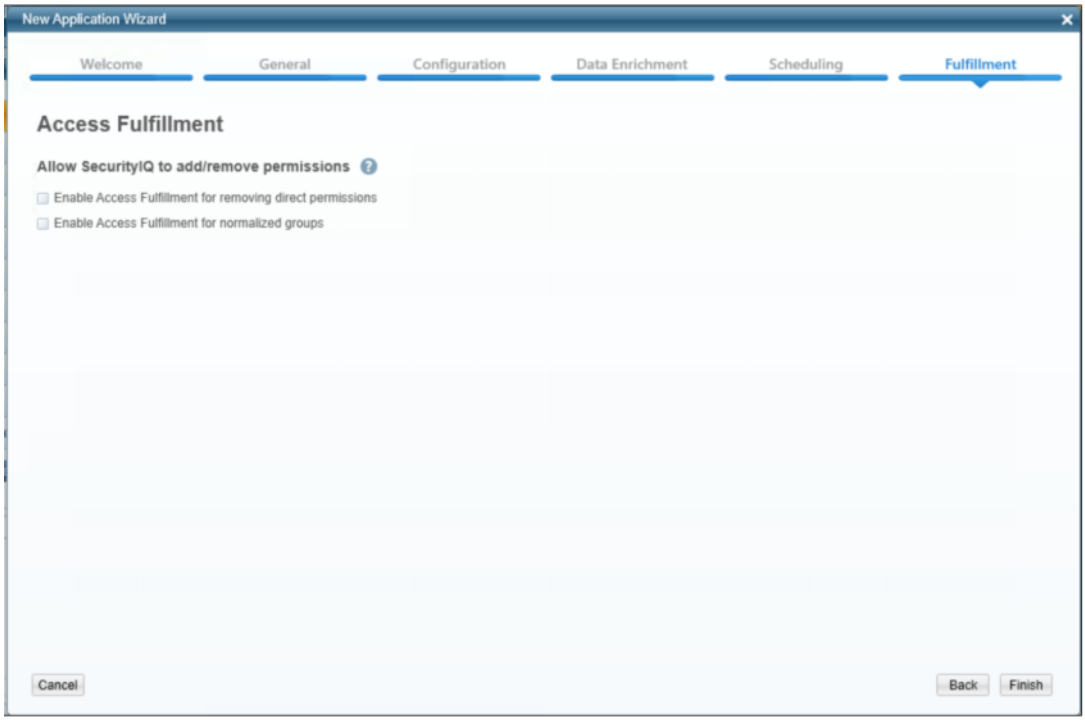

Figure 6. Access Fulfillment Window

37. Select "**Enable Access Fulfillment for removing direct permissions**" to enable access direct permission remediation.

38. Select "**Enable Access Fulfilment for normalized groups**" to allow IdentityIQ File Access Manager to add and remove permissions to IdentityIQ File Access Manager specific groups.

    Note: See the section *Access Fulfillment* under the *Permissions* of the IdentityIQ File Access Manager Administrator Guide for further information.

39. Click **Finish**.

Chapter 6: Installation of Services

Collector Installation

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

   The Collector Installation Manager window displays.

Figure 7. Collector Installation Manager

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, user the format domain\username.

3. Click **Next**.

Note: If you are running the installation manager for the first time, you will receive a security certificate notification to confirm that the Collector Installation service is using SSL.

The Service Configuration window displays.

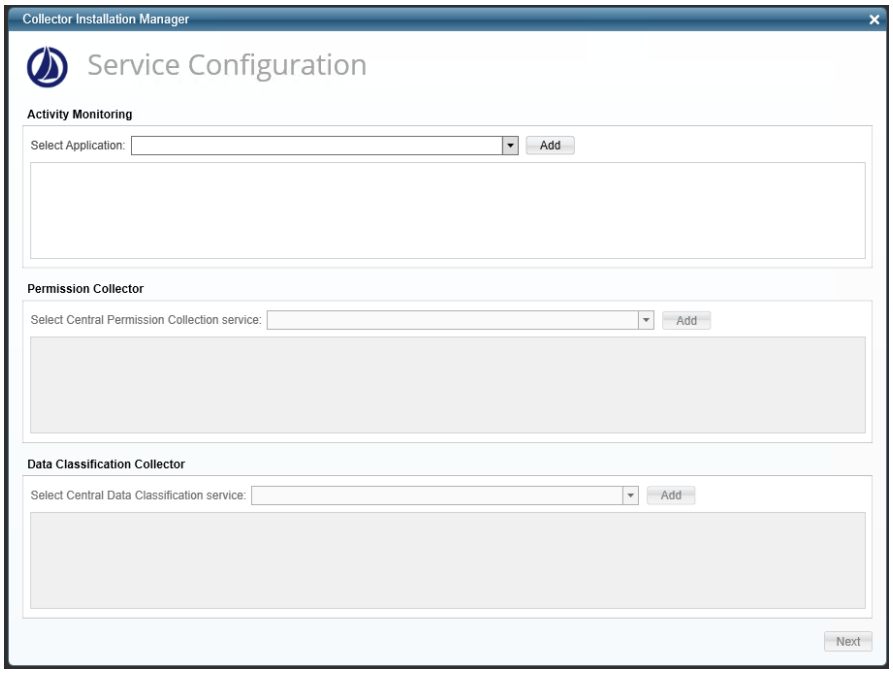

Figure 8. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application, and click **Add.**
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 Collector, select the Central Data Classification to which to connect this service, and click **Add**.
7. Click **Next**

   The Installation Folder window displays.

   Note: 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** (which displays after all the selected components have been installed).

Configuring the collectors to work with a non-system Access Zone

If your configuration consists of a non-system access zone, the collectors must be configured accordingly.

If the access zone is non-system, update the parameter to state the zone.

If the API is on a non-system access zone, or the API is on the system access zone, but the access zone isn't a non-system zone, (so they are on separate zones) we must configure the IP of the API.

The configuration is performed in the relevant configuration file (*.exe.config) in the service folders.

The parameters to set are in the section <!-- Isilon parameters -->

`isilonAccessZone` - the Access Zone we want to connect to. The default is System

`isilonManagementIp` – This parameter is used in cases where the management API is located on another zone, hence another IP from the “Data” Access Zone we connected to.

Chapter 7: Verification

Services

Connectors Services

Verify in windows Service manager or other tool, that the IdentityIQ File Access Manager services are running.

for example,

- **File Access Manager Central Permissions Collection** - <Service Name> service is running.
- **File Access Manager Central Data Classification** - <Service Name> service is running.

Logs

Check the log files for errors

- "%SAILPOINT_HOME_LOGS%\EMCCelerra_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\RoleAnalytics_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on the storage system.
2. Wait a minute (approximately).
3. Query for activities in the Administrative Client by <Application_Name>.
4. Verify that the activities display in the Administrative Client.

Permissions Collection

1. Run the Crawler and Permissions Collector tasks in the IdentityIQ File Access Manager Admin Client.
2. Verify that:
   - The tasks completed successfully
   - Business resources were created on the BRs tree
   - Permissions display in the Permission Forensics window

Chapter 8: Troubleshooting

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.

3. Log in to the OneFS as an administrative user.

4. Type the following command to display the audit events stored on the Isilon:

```
isi_audit_viewer -t protocol
```

5. 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.

6. Run the following command:

```
isi audit settings view
```

7. Assure that the CEE URL is correct, and that the host name configured in Section 4.2.5 matches the host name configured in the Application configuration.

8. Assure that the CEE server is accessible in the configured port from the Isilon by pinging it, and running telnet to the configured port.

9. Run the following command:

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

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

11. Advanced troubleshooting:

    a. 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.

    b. 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
```

    c. 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:

```
2014-02-20 12:49:17 vwjaws2-1 isi_audit_cee[65098][0x800d020b0]: DEBUG:
deliver_event: No CEE servers available.
2014-02-20 12:49:17 vwjaws2-1 isi_audit_cee[65098][0x800d05da0]: DEBUG:
heartbeater: available servers: []
```

    d. When finished, lower the log level to info.

    If none of the above helps, we can use a tool called DebugView (a part of Windows Sysinternals) to help us see debug messages from the CEE:

12. Download DebugView (https://technet.microsoft.com/en-us/sysinternals/debugview.aspx).

13. Extract to an accessible folder on the CEE server.

14. Run Dbgview.exe.

15. Under Capture, assure that the following items are checked:

    - Capture Win32
    - Capture Global Win32
    - Pass-Through

- Capture Events

16. Open the Registry Editor (Run -> regedit)
17. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration
18. Modify both Debug and Verbose to 3f (Hexadecimal).

You should now be able to see debug messages from the CEE.

For example, you can check storage to CEE communications by looking for messages such as the following message:

```
[EMC CEE]: CBaseSourceUtility::HandleEvent: <CheckFileRequest>
<Args action="9"
name="XABcAGUAbQBjAC0AYwBpAGYAcwAtAG4AZQB3AC4AbwBmAGYAaQBjAGUALgB3AGgAaQB0AGUAYgBvA
HgALgBmAG8AcgBlAHMAdABcAEMASABFAEMASwAkAA==" id="1497870527"
celerraIP="172.16.60.75" type="0" protocol="0"/>
.
.
</CheckFileRequest>
```

Event of action=”9” is a connection event coming from the storage. If this is displayed regularly, that indicates that the connection to the storage is stable.

The following message displays a working connection between the CEE and the File Access Manager Activity Monitor:

```
[EMC CEE]: CEPPAPIWrapper[AUDIT][whitebox][siq-test]::CCEPPAPIWrapper::HeartBeat():
Response: HB Status: 0 - CEPP_SERVICE_ONLINE
```

If the status of the message is anything other than `CEPP_SERVICE_ONLINE`, that indicates that the CEE cannot connect to the File Access Manager Activity Monitor.