Integrating EMC Unity CIFS with File Access Manager

Version: 8.2 Revised: August 09, 2021

Contents

Capabilities

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

Connector Overview

> For more information on the EMC architecture and CEE, refer to the EMC CEE using the Common Event Enabler for Windows, see docu48055_using-the-common-event-enabler-on-windows-platforms.pdf

CEE

CEE is a software package that allows File Access Manager to receive event notifications from Unity. It consists of two agents: Common Antivirus Agent (CAVA) and Common Event Publishing Agent (CEPA).

All NAS servers send notifications on events to the CEPA agent and CEPA sends the events to File Access Manager.

CEPA and NAS servers

- For CEPA to work, you need to have a SMB server configured on the NAS Server.
- A CEPA service can communicate with multiple NAS servers, and a NAS server can communicate with multiple CEPA services.
- CEPA servers work in pools, Dell Recommends a minimum of two CEPA servers per pool.
- Each NAS server needs to enable publishing events and configure at least one CEPA pool.

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

IdentityIQ File Access Manager Connector for EMC uses EMC CEPA over the Common Event Enabler Framework (or CEE, formerly known as CAVA) infrastructure for getting audit events from the Unity for CIFS access.

The Activity Monitor supports different architectures and can work with either a single or multiple, remote, or local CEE services.

Permissions Collector

IdentityIQ File Access Manager connects using EMC administrative shares and analyzes folder permissions.

Local groups and users are collected from the CIFS server during the Permission Collector process.

Supported Versions

EMC Dell EMC Unity OE version 4.1

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 .

Configure the CEE Service

Make sure that CEE is installed on a Windows machine in the domain, and that the log on user for the CEE services is an administrative user in the domain.

Supported Versions

Use the latest version of CEE.

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, make the following changes in the registry:

   ```
   [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.

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 NAS server CEE server, otherwise the communication between the NAS server and the CEE service will fail.

2. Make the following changes in the registry:

   ```
   [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 “Permissions” section.
4. Restart EMC CEE service.

Configuring Event Publishing in Unity

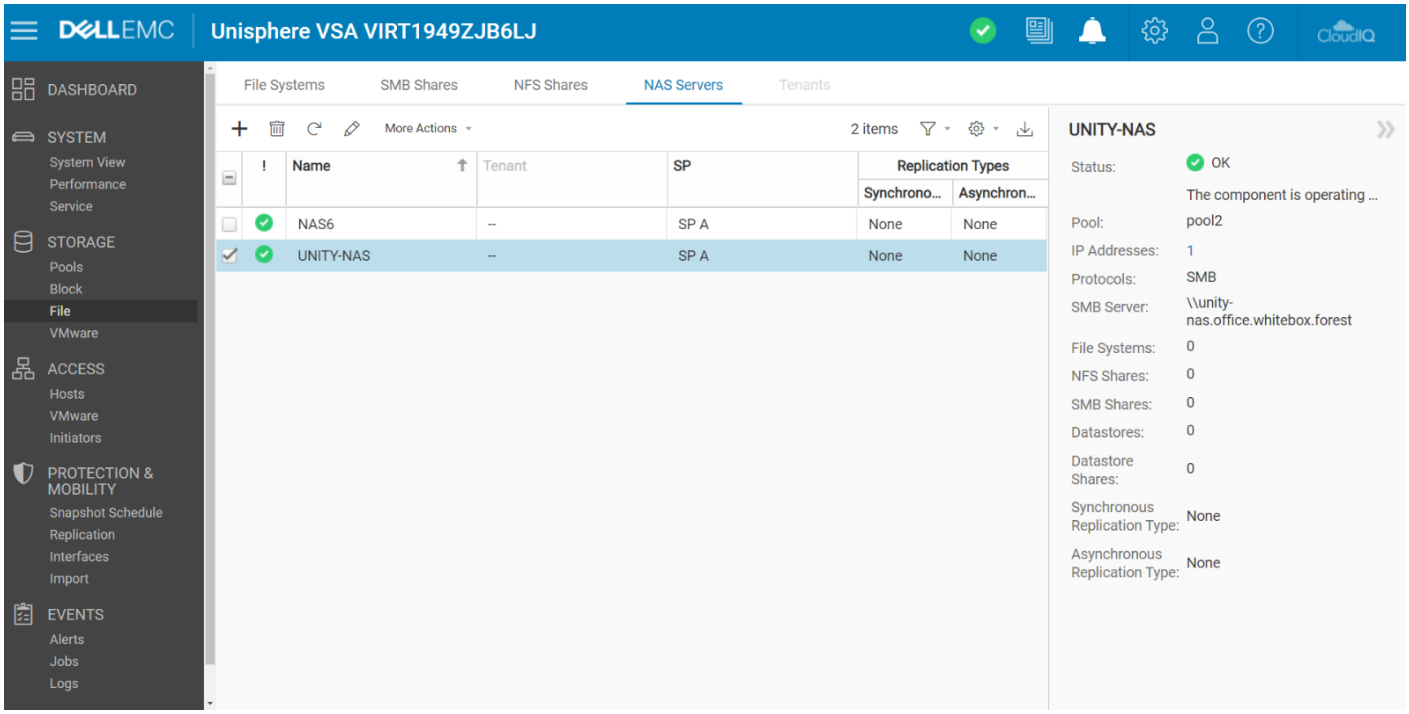
To enable event publishing on a share, Events publishing must be enabled on its NAS server and its File System as described in the following sections.

For more information on how to configure the CEPA and CEE refer to the EMC CEE version 7.0 using the Common Event Enabler for Windows

docu48055_using-the-common-event-enabler-on-windows-platforms.pdf

Enabling Event Publishing in the NAS Server

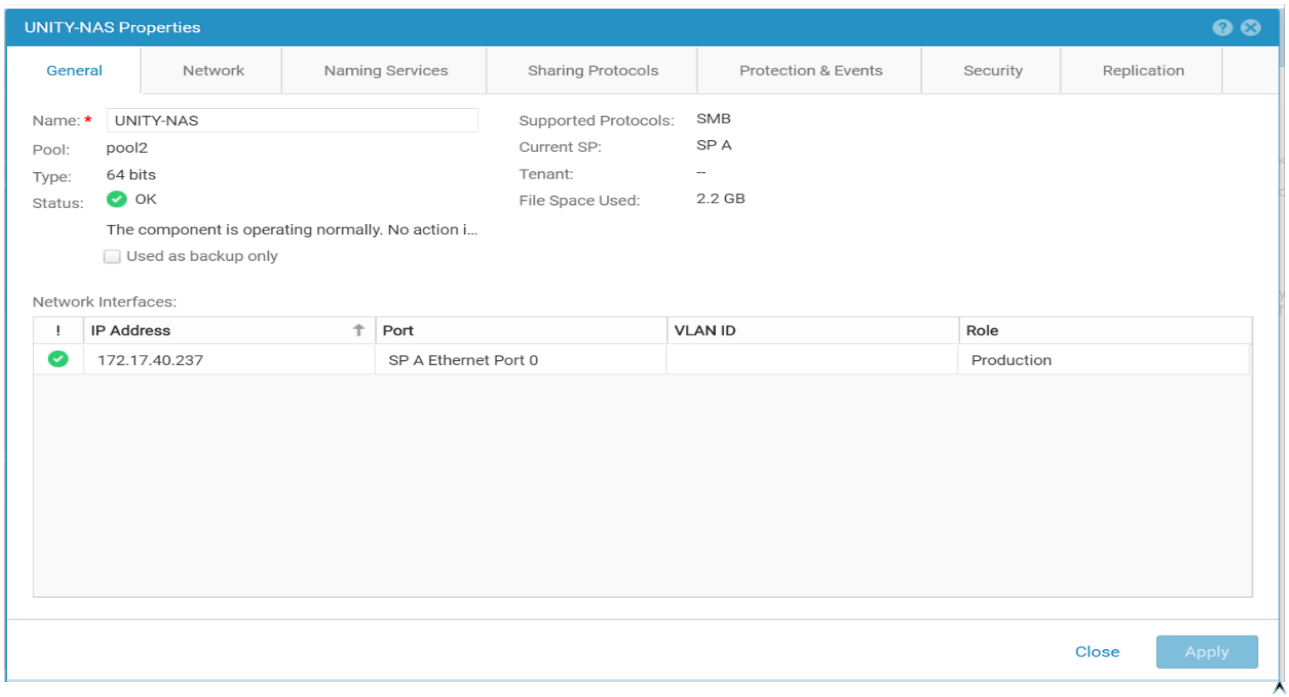
Open Unisphere and Navigate the File tab in the right pane under Storage.



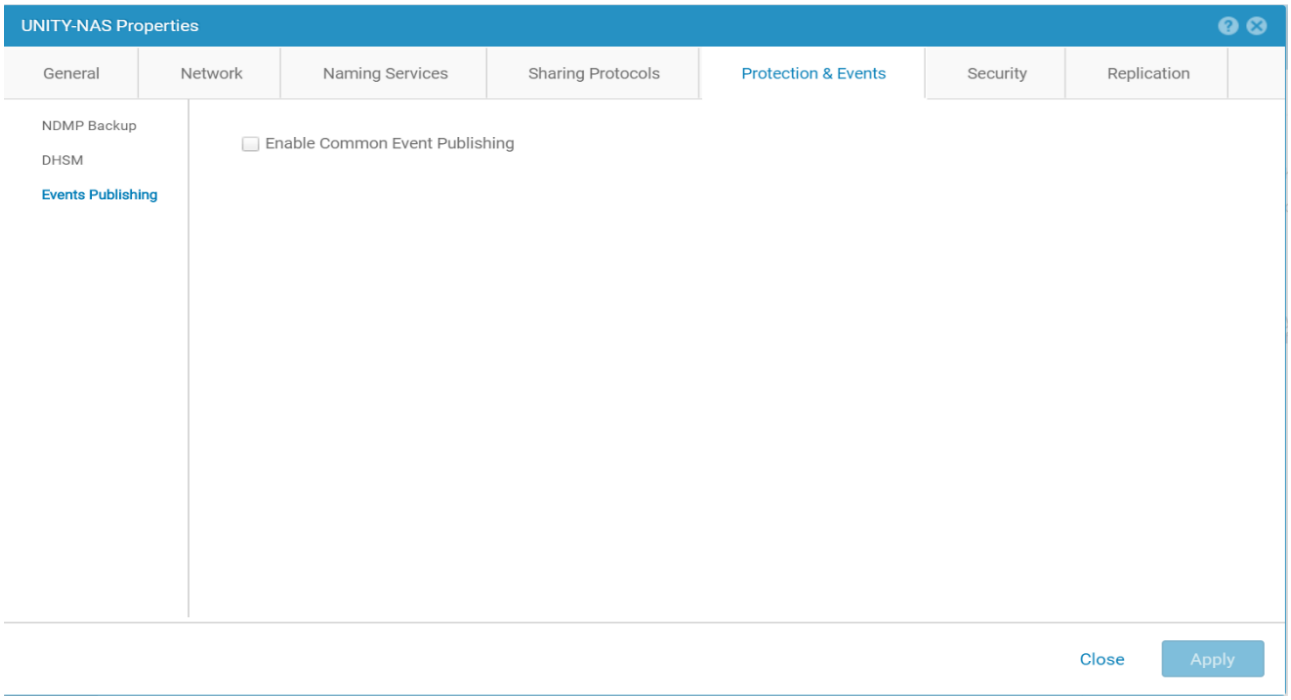
Click the "**NAS Servers**" tab.

For each NAS Server that you wish to enable activities, run the following:

1. Double click the NAS Server.



The Server's properties appear.

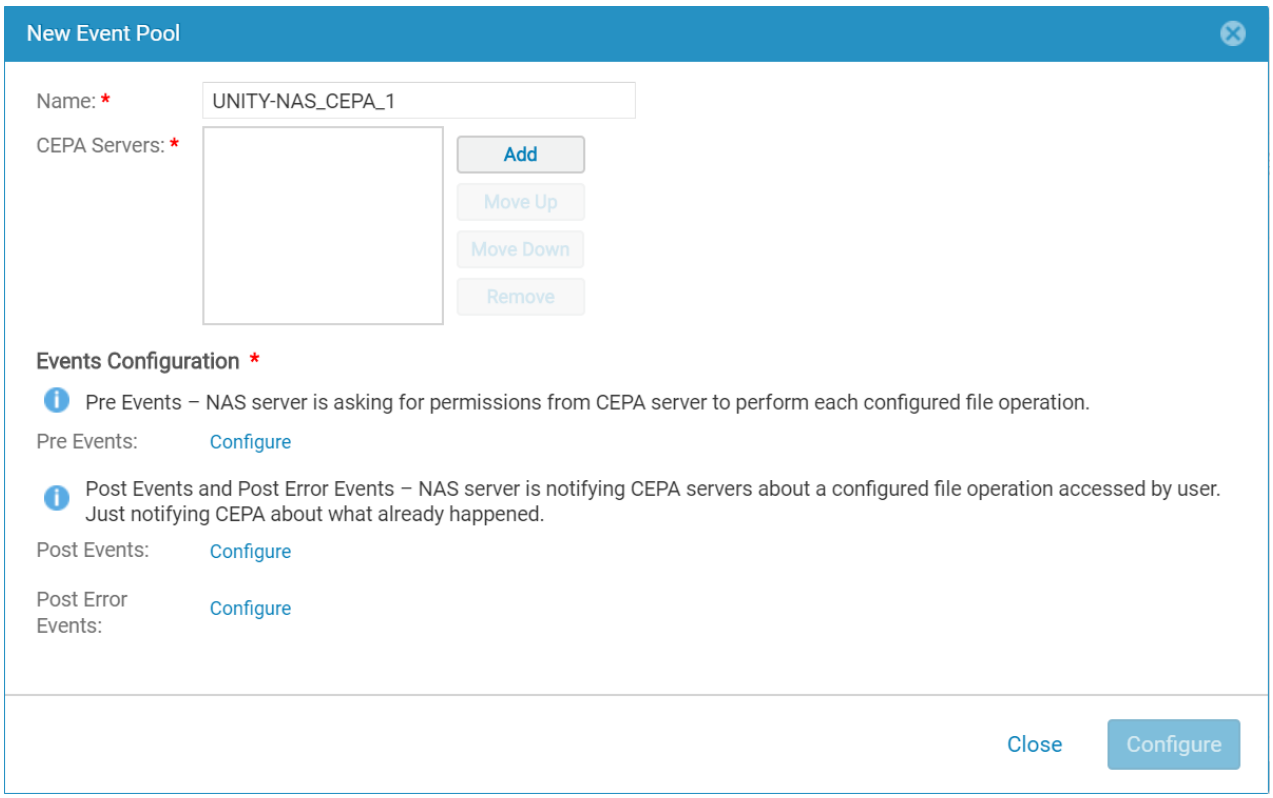


2. Open the "**Protection & Events**" Tab, and choose "**Events Publishing**" in the right pane

The Events Publishing details appears.

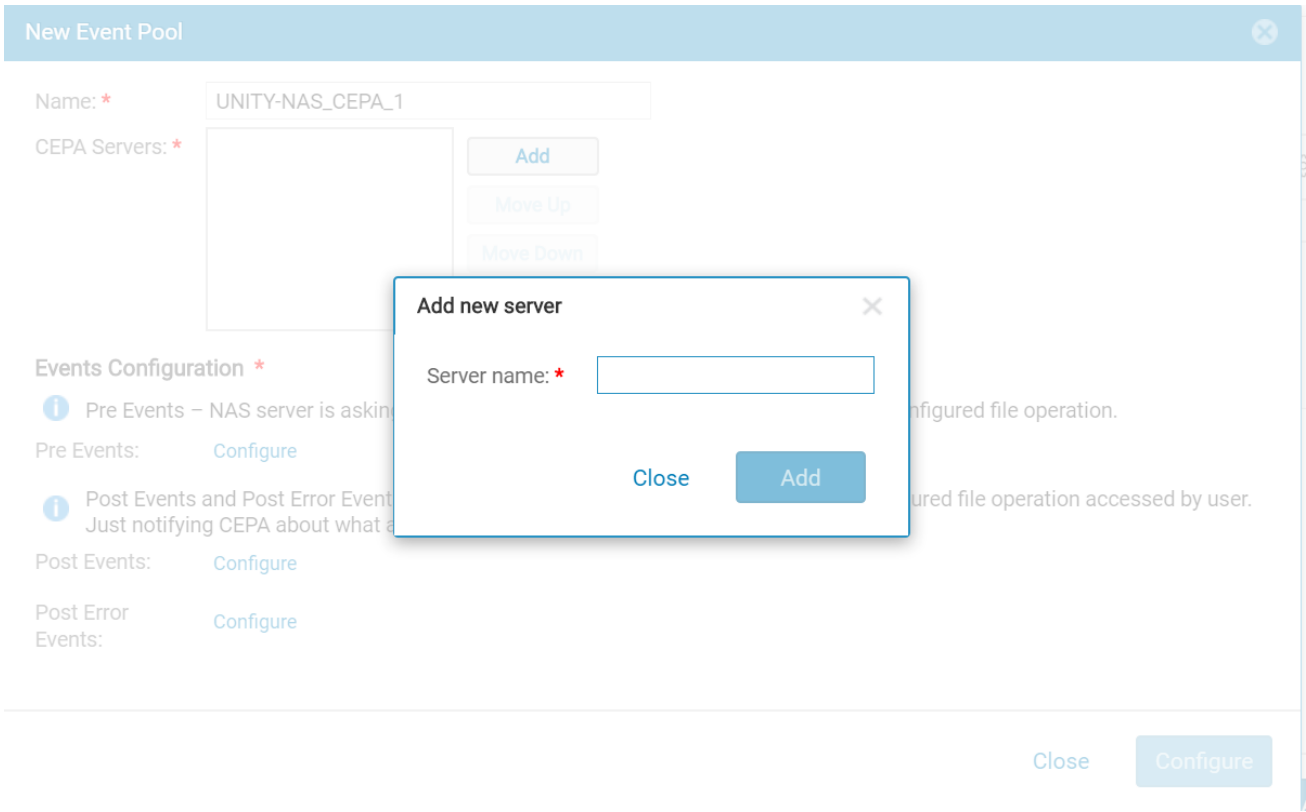
3. Check “Enable Common Event Publishing:

   The “New Event Pool” window will appear to create the first Event Pool

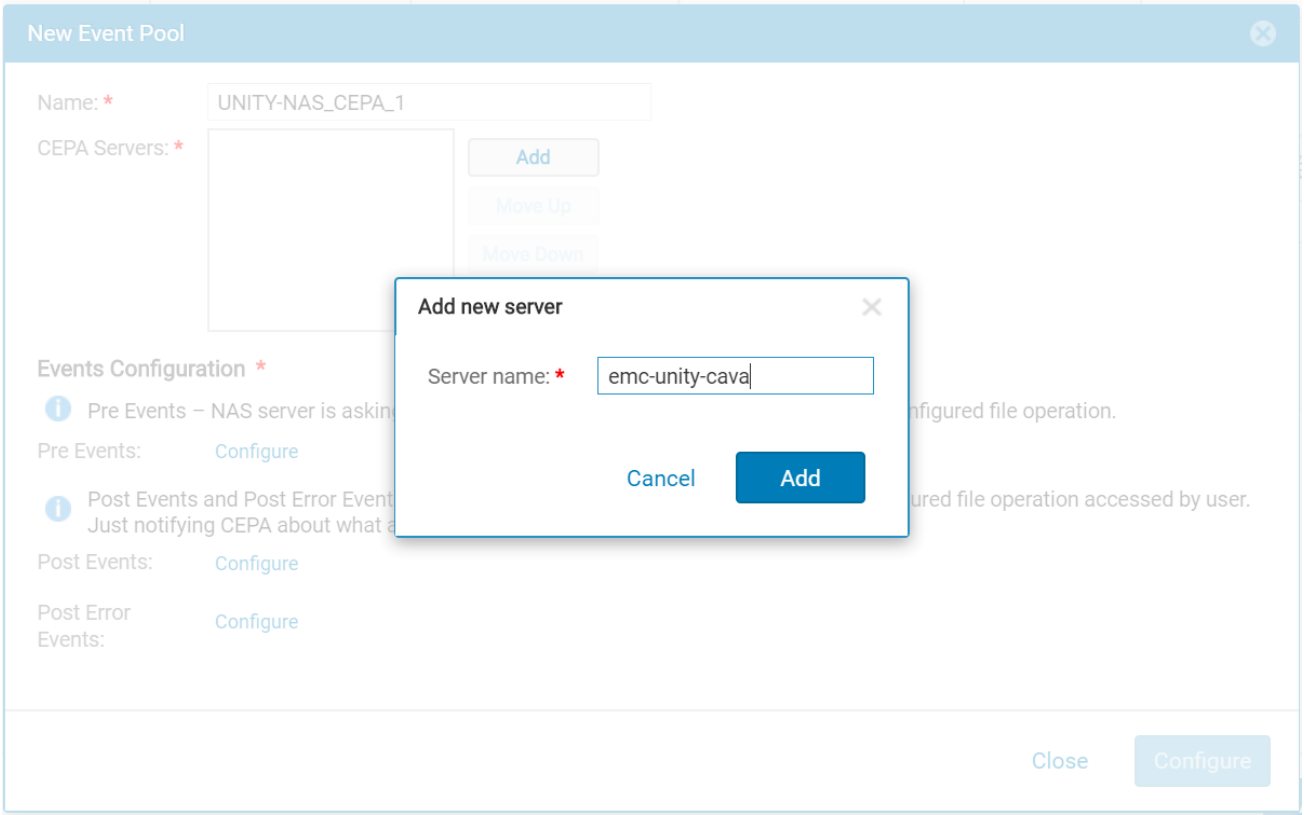


4. Click **Add**

   The “Add new server” window appears.

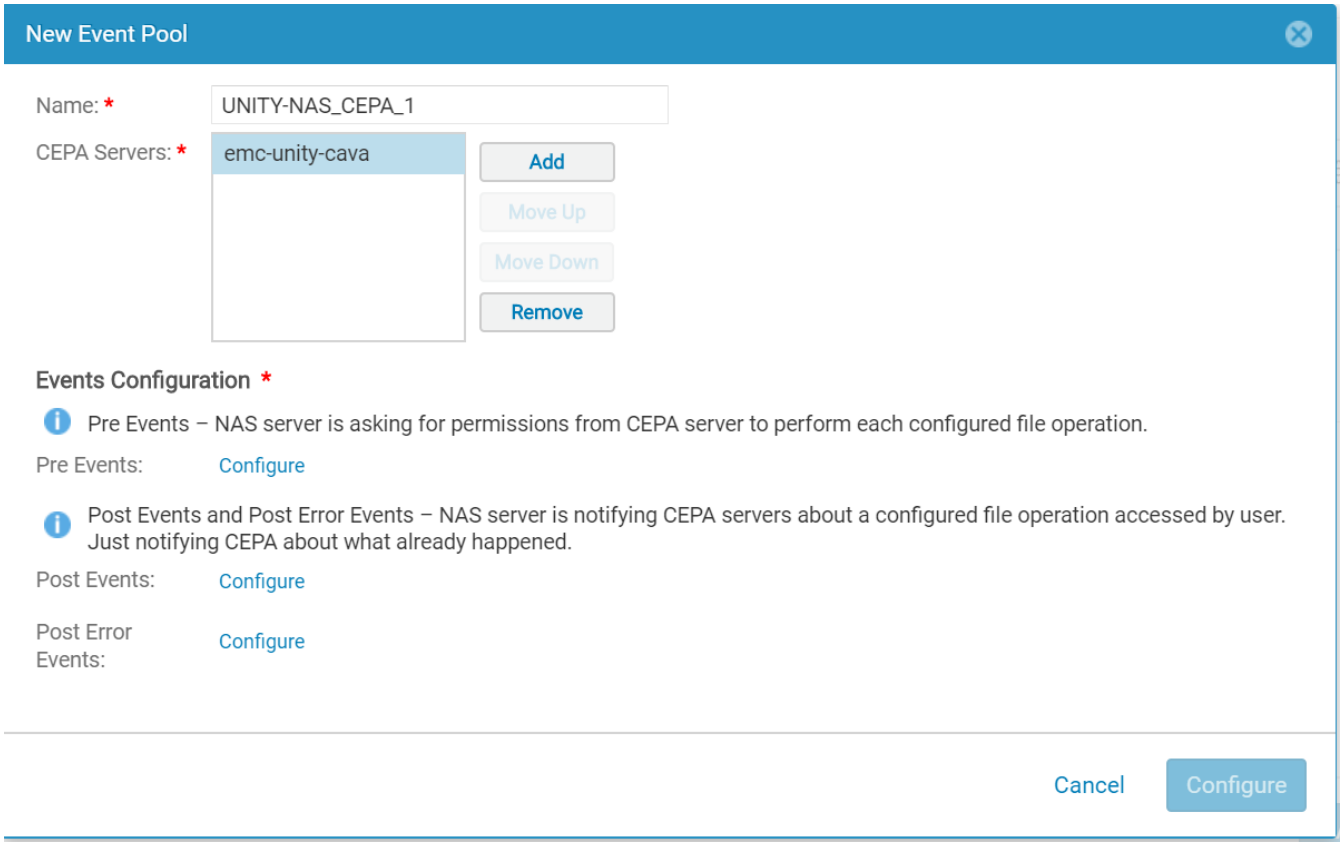


5. Fill the Server name of the CEE service and click **Add**



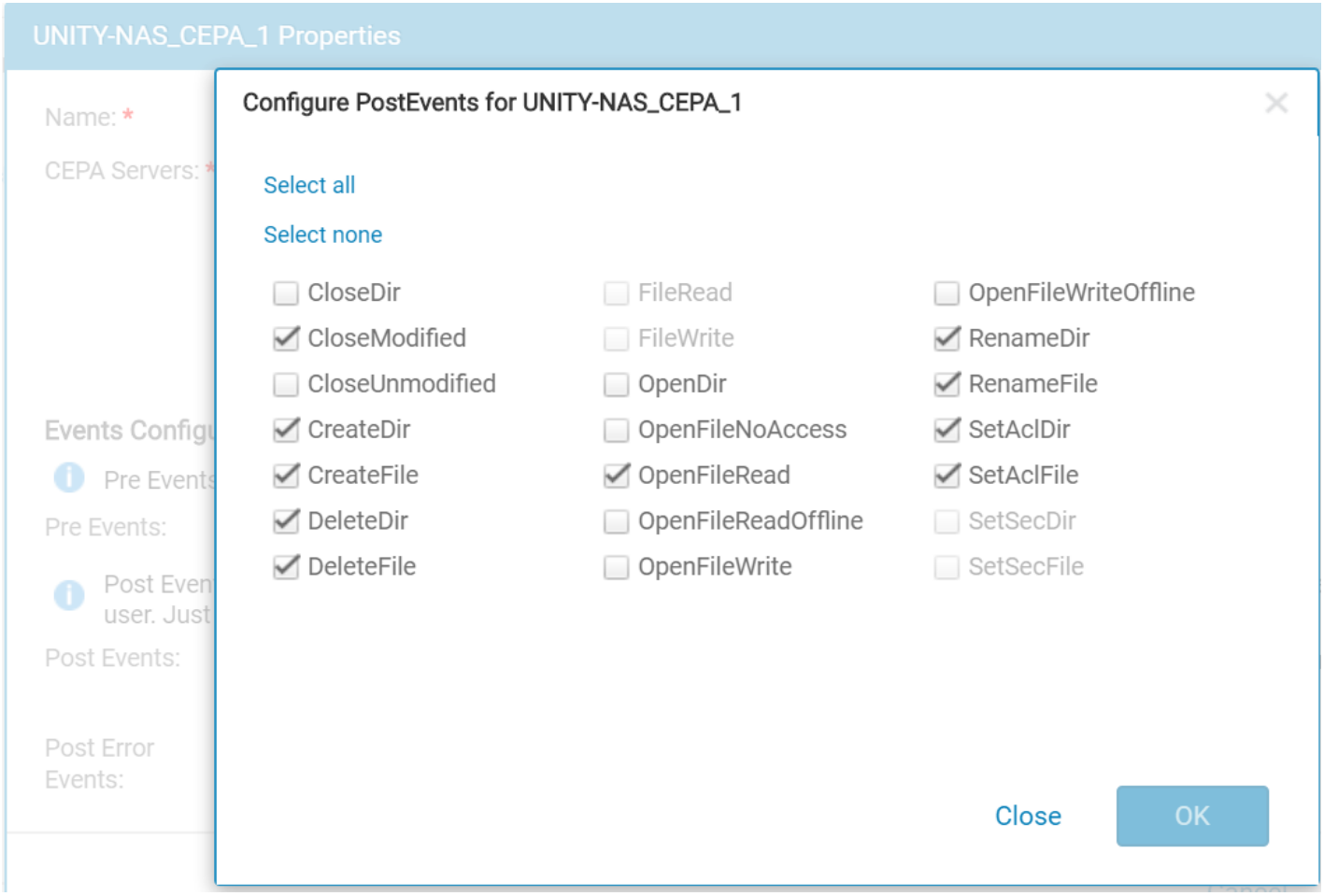
The “New Event Pool” window will reappear, with the list of servers listed.

Press Add to add additional servers with CEE service.



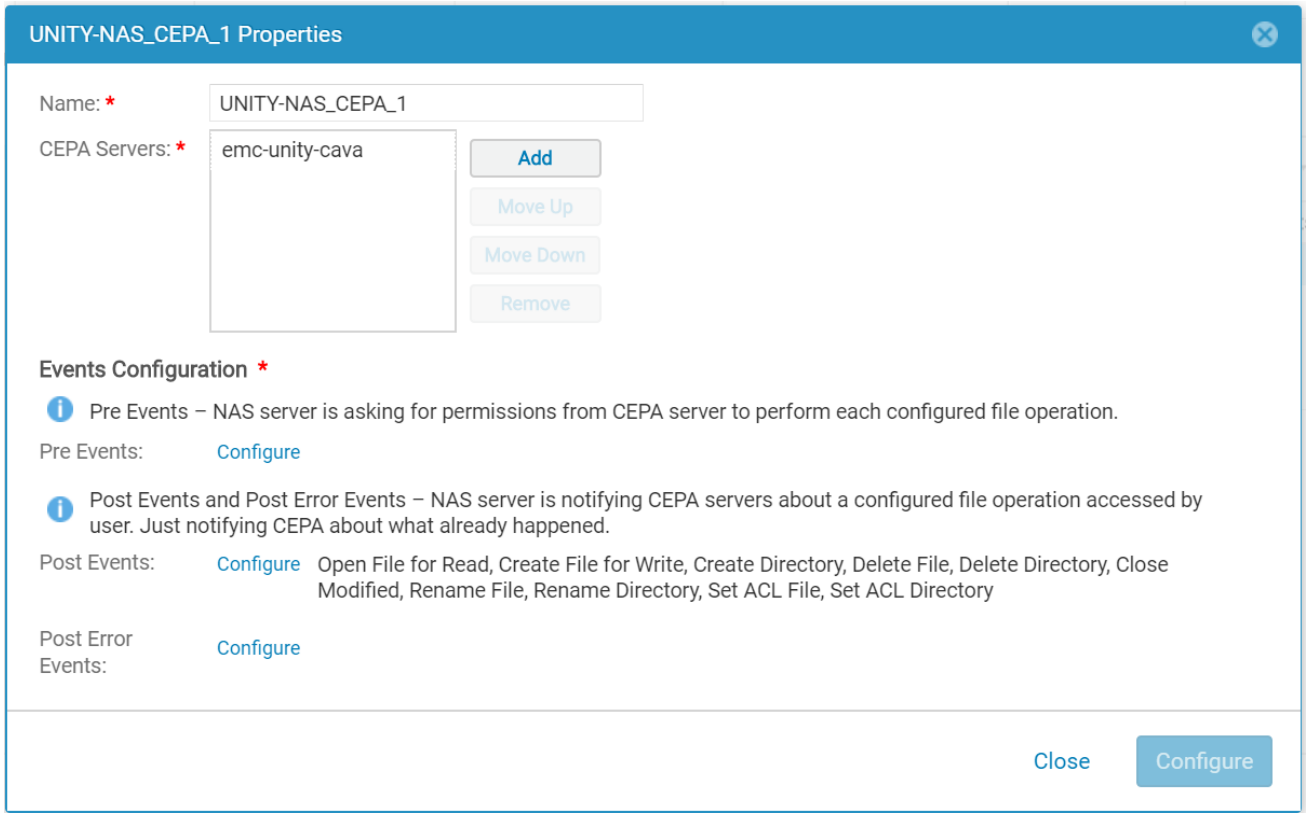
6. To configure the post events - Click **Configure**Next to **Post Events:**.

   This will open the “Configure PostEvents…” window.



7. Check the following Event Types:
    - OpenFileRead
    - CreateFile
    - CreateDir
    - DeleteFile
    - DeleteDir
    - CloseModified
    - RenameFile
    - RenameDir
    - SetAclFile
    - SetAclDir

8. Click **OK** to return to the CEPA Properties window.



9. Optionally, rename the Event Pool in the **Name** field.
10. Click **Configure** to return to the NAS Properties window
11. Click **Close**

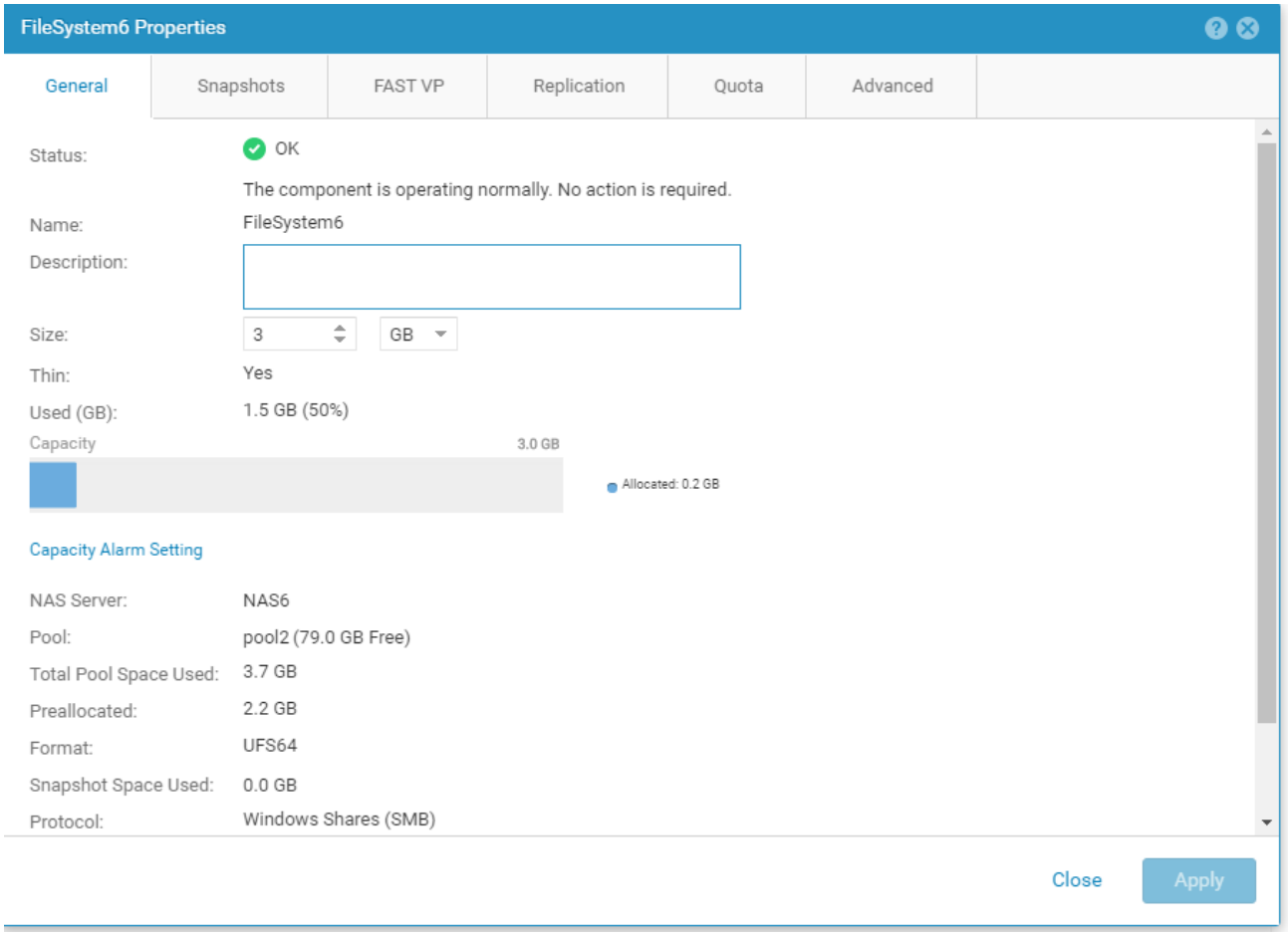
Enabling Event Publishing in the File System

Open Unisphere and Navigate the File tab in the right pane under Storage.

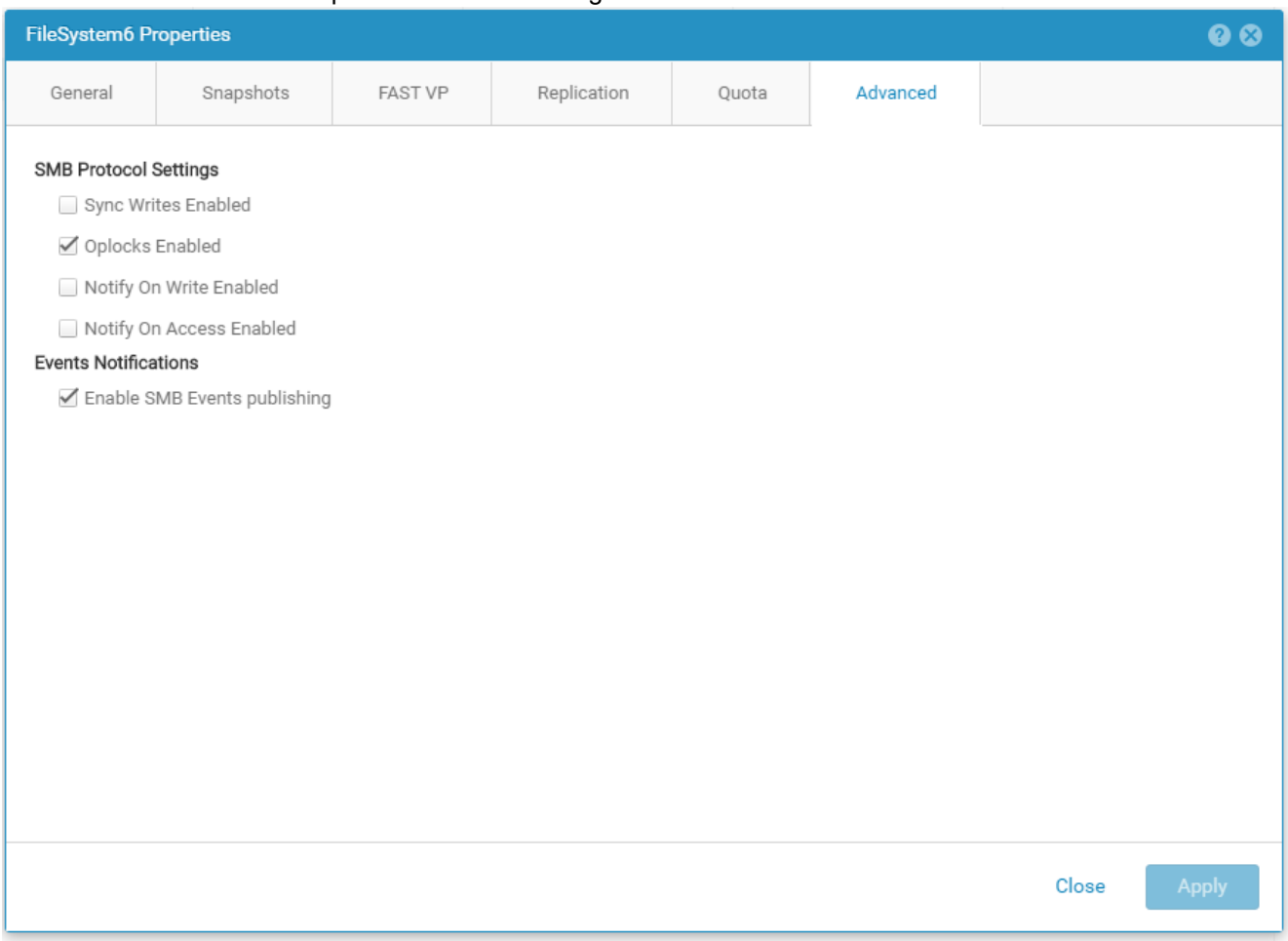
Click the **File Systems** tab.

To enable activities for a file system:

1. Double click the File System to open the File System Properties window.



2. Click the “Advanced” Tab to open the advanced configuration tab.



3. Check **Enable SMB Events publishing** and click **Apply**.

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 file server:

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

Why do we need this access?

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

Activity Monitoring

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

Crawling

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

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

Permission Collection

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

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

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

Access Fulfillment

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

Data Classification

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

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

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ File Access Manager Servers	8000-8008
EMC CEE	EMC NAS server	CEE Server	RPC (135 + Dynamic)
CEPA Events Push	CEE Server	File Access Manager Application	RPC (135 + Dynamic)
Permissions Collector & Data Classification Analysis	Permissions Collector/Data Classification Server	Monitored server	CIFS/SMB (139, 445)

Connector 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
    - 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 EMC Unity CIFS Application

In order to integrate with EMC Isilon, 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

EMC Celerra-CIFS

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 ManagerIdentityIQ 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

Complete the Connection Details fields:

Host Name

The host name of SMB Server name of the NAS server. not FQDN, and without trailing slashes

Domain Name

The user defined in the prerequisites

Username / Password

Credentials of the user defined in the prerequisites

Aliases

> The alias field should remain empty for the EMC Unity configuration

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 “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.

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.

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 yo u are on this screen, press this button to retrieve the updated structure.

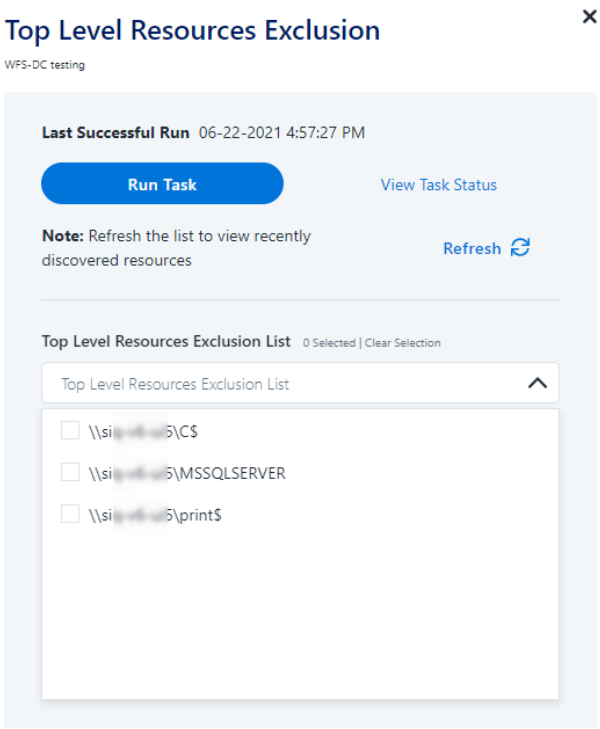
Once triggered, you can see the task status in

Settings > *Task Management* > *Tasks*

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

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

4. Click the top level resource list, and select top level resources to exclude.
5. Click *Save* to save the change.
6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.



Special Consideration for Long File Paths in Crawl

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

`excludeVeryLongResourcePaths`

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

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

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

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

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

Background

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

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

Identifying the Problem

When using an SQL Server database version 2014 and ealier

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 yo 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

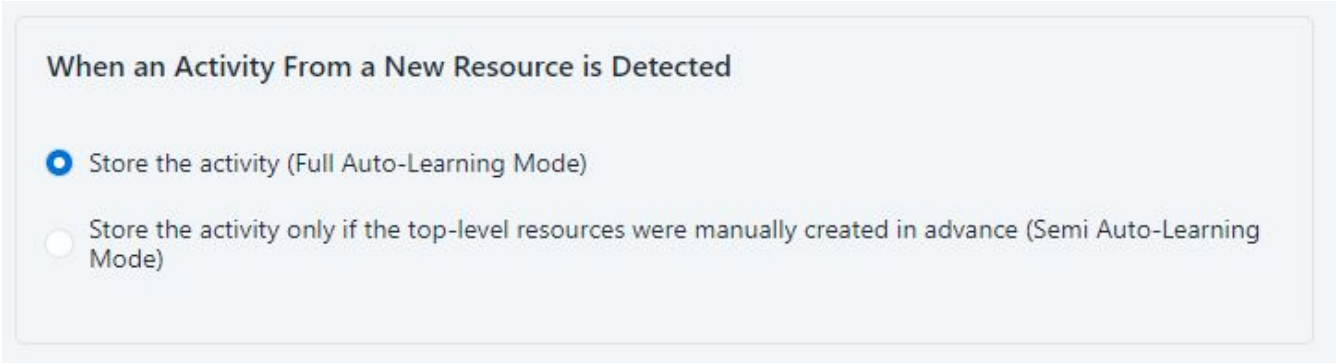
List of users whose activities are not monitored

> 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.



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 DECs text box.

Use the > or >> arrows to move the selected DECs to the Current DECs text box.

The user can select multiple DECs. 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 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:

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.

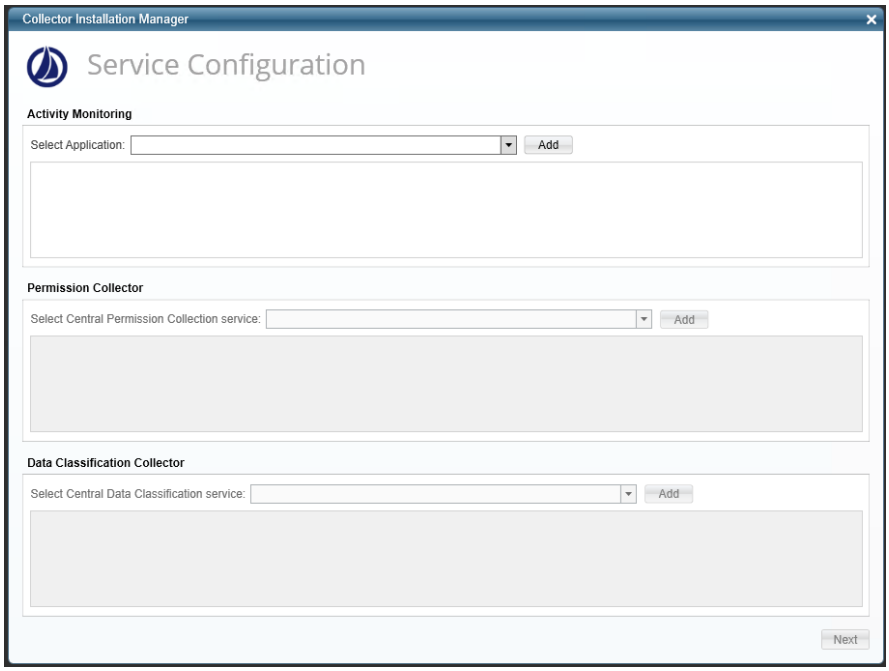
Installing Services: Collector Installation

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 EMC Unity CIFS 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 Activity Monitor- <Application_Name> service is running.
- File Access Manager Central Data Classification - <Application_Name> service is running.
- File Access Manager Central Permissions Collection - <Application_Name> service is running.

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

Monitored Activities

1. Simulate activities on the CIFS server.
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*)

Troubleshooting

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

What if Activities are not Collected by the Activity Monitor

If activities are not collected by the Activity Monitor, we need to track the status of the components, starting with the Data Mover, an checking to the Activity Monitor service.

1. Login to unisphere
2. In the right pane, click **File** under Storage, and choose the NAS Servers tab.

   Check for errors in the status of the NAS servers.
3. In right pane, click **Logs** under Events.

   Check for any relevant error.
4. Verify that all the prerequisites were set: (See Prerequisites)
   - The post events were configured correctly in the NAS server configuration.
   - The CEE service is running with a domain user who is an administrator on the CEE service server.
   - The CEE service and the NAS server CIFS server are joined to the same active directory domain.
   - The CEPA IP address listed in the output of the command above matches the address of the server running the CEE service
   - There is no firewall between the NAS server and the server running the CEE service
   - The windows firewall is off on the server running the CEE service
5. Stop the Activity Monitor service, wait for 60 seconds
6. **Stop the event publishing in each NAS server.**
   - Click **File** under Storage in the right pane
   - Choose the NAS Servers tab.
   - Double click each NAS server
   - Choose the **Protection & Events** tab.
   - Click **Events Publishing** in the right pane
   - Uncheck **Enable Common Event Publishing**
7. Stop the EMC CEE service on the CEE server
8. Stop the Activity Monitor service.
9. **Start the event publishing in each NAS server**
   - Click **File** under Storage in the right pane
   - Choose the NAS Servers tab.
   - Double click each NAS server

- Choose the **Protection & Events** tab.
- Click **Events Publishing** in the right pane
- Check **Enable Common Event Publishing**

10. Start the Activity Monitor service, and wait for 60 seconds
11. Start the EMC CEE service, wait for 60 seconds

What if the Counters Increase But No Events Are Collected

If the counters increase, but no events are collected:

1. Check the statistics log file of the Activity Monitor to see if events are received by the Activity Monitor.
2. If no events are received by the Activity Monitor validate the Application configuration:
   - Make sure the CIFS server name is properly configured in the Application filer name field.
     This value must be the actual name of the CIFS server name, and not the FQDN or one of the aliases and without trailing slashes.
   - If the CIFS server has aliases defined to it (validate that in the EMC management), make sure these aliases are defined under the aliases in the Application configuration.