SailPoint IdentityIQ

Version: 8.0

File Access Manager Windows File Server Connector Installation Guide

Table of Contents

List of Figures

List of Tables

Table of Revisions

Ver. #	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	1 Nov 2018
8.0	• Naming conventions to support rebranding to IdentityIQ File Access Manager • Clarifying the description of the list of servers on the installation screen • Updated and certified for Windows Server 2019	Josh Lewin	11 Aug 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 services.

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.

Installation Locations

The Activity Monitor of the Windows File Server connector - Must be installed locally on the monitored Windows file system.

Chapter 2: General

Path of Business Resource

The full path of the business resources is the UNC shared path, rather than the physical path of the folder. The physical paths display since they are represented by the administrative shares (c$, d$...) and are treated in the same way as any other share on the server.

- Crawler – The crawler crawls through all the shares and creates business resources with the share's full path (\\server_name\share\folder).
- Permissions Collector – The permissions collector analyzes share permissions, as well as NTFS permissions.
- Activity Monitor – The full path of activities is the share used to access the file/folder. Section 2.2 provides a more detailed explanation.

Backup Operator Privileges

The user configured in the permissions perquisites section must be a member of the local Backup Operator group of the file server. It eliminates the need to grant explicit permissions to the IdentityIQ File Access Manager user to all the folders on the file server. By using the Backup Operator privilege, IdentityIQ File Access Manager can crawl, collect permissions, and classify data even if the user does not have explicit permissions to the folder.

Windows Failover Cluster Share Scoping

IdentityIQ File Access Manager supports Windows Failover Cluster Share Scoping.

The Server Names and their corresponding shares are discovered as part of the crawl task, and the business resource tree is built with the Server Names at the first level.

Activity Monitor Operation Principles

IdentityIQ File Access Manager Windows FS Activity Monitor uses a Microsoft certified mini-filter driver (https://msdn.microsoft.com/en-us/library/windows/hardware/dn265170(v=vs.85).aspx).

The driver intercepts all I/O calls to determine which users have access to which files/folders, so there is no need for Windows auditing. Thus, no performance overhead is introduced on the monitored server.

Changes to local users and groups are also audited, but only on Windows 2008 and above.

The activity monitor detects which share was used to perform each operation (starting from Windows 2008). Local access and overlapping shares are special cases, which are detailed below:

Local Access

The system reports local access to a file/folder (for example, by using Remote Desktop) on the administrative share (c$), and a special field on the activity ("Is Local Access") is set to "True".

Overlapping Shares

Multiple shares can overlap on the same physical folders, as in the example below:

\\server\share1 -> c:\Files

\\server\share2 -> c:\Files

When a user accesses files on one share, that user also gains access to files on the overlapping share, and this activity will be duplicated for all overlapping shares. A special field called "Original Access Path" will be populated with the original share, used to access the file for all overlapping shares. Using the above example, if a user

creates a new file, called 1.txt, on the \\server\share1 share, the system will generate two activities – one for the \\server\share1\1.txt file, and another for the \\server\share2\1.txt file with the "Original Access Path" set to "\\server\share1".

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 Add File	A permission was added to a file.
Permission Add Folder	A permission was added to a folder.
Permission Remove File	A permission was removed from a file.
Permission Remove Folder	A permission was removed from a folder.
Read File	A file (its content or security properties) was read.
Rename File	A file was renamed.
Rename Folder	A folder was renamed.
Write File	A file was modified.
Add Member*	A local user/domain group was added to a local group.
Remove Member*	A local user/domain group was removed from a local group.
Create User*	A local user was created.
Delete User*	A local user was deleted.
Rename Object*	A local user/group name as changed.
Create Group*	A local group was created.
Delete Group*	A local group was deleted.
Remove Audit Account Management*	The Account Management Auditing was disabled in windows.

*** Supported on Windows 2008 and above.**

Permissions Collector Operation Principle

IdentityIQ File Access Manager connects to the Windows file server through CIFS, collects the local users and groups, and analyzes the share and NTFS permissions on all the folders.

Supported Versions

- 2003 SP1 and above, 2008, 2008R2, 2012, 2012R2, 2016, 2019
- 32 and 64-bit support

Chapter 3: Windows Server Failover Cluster

Windows Server Failover Cluster is an Active Passive Cluster based on Windows Server.

Basic Terminology

The following definitions apply to the Windows Server Failover Cluster:

- Node – A physical server that is part of a Cluster
  All the nodes in a cluster must be configured when the "Is Cluster"' field in the application configuration wizard is checked.
- Server Name – a logical layer on top of the Node layer
  Shares in a Cluster belong to a Server Name, which is the name used when shares in the cluster are accessed. A Server Name (discovered automatically, as part of the crawling task) is active on only one Node at a time.
- File Share Scoping – In Windows Server 2008 Failover Clusters and forward, shares located on a cluster node can only be through the Server Name – not through the cluster node name in which they are currently active.

The example below is used in Section ***Resource Tree Structure***:

There is a cluster application in IdentityIQ File Access Manager, called ClusterApp.

ClusterApp consists of node1 and node2.

ServerName1 is currently active in node1, while ServerName2 is currently active in node2.

ServerName1 has one share: Share1 (\\ServerName1\Share1).

"Share1" is mapped to physical path "E:\folder1"

ServerName2 consists of Share2 and Share3 (\\ServerName2\Share2 and \\ServerName2\Share3).

"Share2" is mapped to physical path "E:\folder2"

"Share3" is mapped to physical path "E:\folder2\folder3"

Resource Tree Structure

IdentityIQ File Access Manager manages Business Resources that belong to a share only a Server Name in a Windows Server Failover Cluster. Physical paths that do not belong to a share on a Server Name are not displayed in IdentityIQ File Access Manager.

The Business Resources tree is represented as follows:

[Cluster Application]
    [Admin Audit]
    [Server Name]
        [Share]
        …
        [Share]
    [Server Name]
        [Share]

…

[Share]

The business resource tree for the above example is:

ClusterApp

Admin Audit

ServerName1

Share1

ServerName2

Share2

Share3

Activity Monitor

Activities on a share are replicated to shares with the same physical path, as is the case with a non-cluster connector

Events on files or folders that do not belong to shares mapped to the cluster Server Names are ignored.

In the example above, if a user reads a file locally in the physical path E:\folder2\folder3,

An event (marked “Local Access”) is created in Share3 in the path \\Share3, and in Share2 with the path \\Share2\folder3, since they both have the same physical path.

If a user reads a file remotely in the path \\Share2\folder3 or \\Share3, the result will be the same as when the user reads a file locally, but the activity is marked as not “Local Access”

If an event occurs in the physical path: C:\, the event is discarded and is not displayed in the Activities tab, since this path is not mapped to a share under a Server Name.

Chapter 4: Prerequisites

Software Requirements

Activity Monitor

- Windows 2003 – Microsoft .NET Framework 3.5 SP1 (May require reboot)
- Windows 2008 and above - Microsoft .Net Framework 4.5
- The Activity Monitor uses the "Account Management" Audit Policy to monitor changes in local users and groups. Unless changed, this audit policy is enabled by default on windows 2008R2 and above but needs to be enabled on windows 2008. Perform the following steps if the "Account Management" audit policy is not set:
  - Open cmd.exe with an administrator
  - run the following command:

```
auditpol /set /category:"Account Management" /Success:enable
```

  - To validate the Audit Policy was successfully set, run the following command:
    Be sure the "Security Group Management" and "User Account Management" subcategories are set to "Success".

```
auditpol /get /category:"Account Management"
```

- On Windows 2008R2 only, the following registry key needs to be set to identify the share which was used to perform the operation. Otherwise, all activities will be considered as Local Access:
  - Open the registry by running regedit.exe
  - Navigate to:
    HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\
  - Create a DWORD key called 'enableecp' and set its value to 1
  - Restart the server
  - This registry key has known issues, set it with cautions and after making sure it fits your environment. For more information, see:
    https://support.microsoft.com/en-us/kb/2817216

Note: Windows 2008 32bit might require a restart following the Activity Monitor installation.

Permissions Collector

- Microsoft .Net Framework 4.5

Data Classification

- Microsoft .Net Framework 4.5

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

The following detailed explanation describes required permissions by each IdentityIQ 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

Table 2. 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
Permissions Collector & Data Classification Analysis	Permissions Collector/Data Classification Server	Monitored server	CIFS/SMB (139, 445)

Chapter 5: Add New Application Wizard

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

   The New Application Wizard window of the New Application Wizard displays under the Welcome tab.
3. Select Standard Application.
4. Select Windows File Server (Connector) from the Application Type dropdown menu.
5. Click Next.

   The General Details window of the New Application Wizard displays under the General tab.
6. Type the logical name of the Windows File Server application in the *Name* field.
7. Type a description of the application in the *Description* field.
8. Select a logical container for the application from the **Container** dropdown menu.
9. Select an Active Directory Identity Collector from the **Identity Collector** dropdown menu.
10. Click **Next**.

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

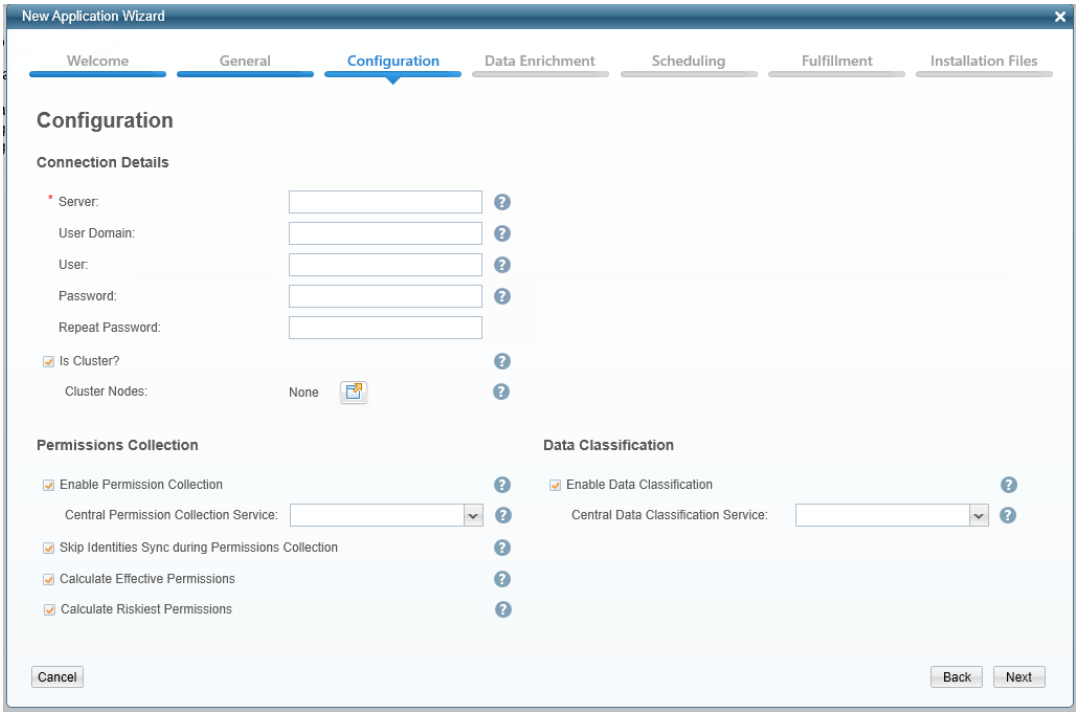

Figure 1. First Configuration Window

11. Complete the Connection Details fields:

Server

the short name of the file server to which users connect

User Domain

The user defined in the prerequisites

User

The user defined in the prerequisites

Password

The user defined in the prerequisites

Is Cluster

Configure as a cluster, or standalone.

Cluster Nodes

This option is available for cluster mode only. Press the button to add physical cluster node names. This will create multiple XML configuration files, one for each physical node in the cluster.

12. 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.)
    - *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)

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

14. Click **Next**.

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

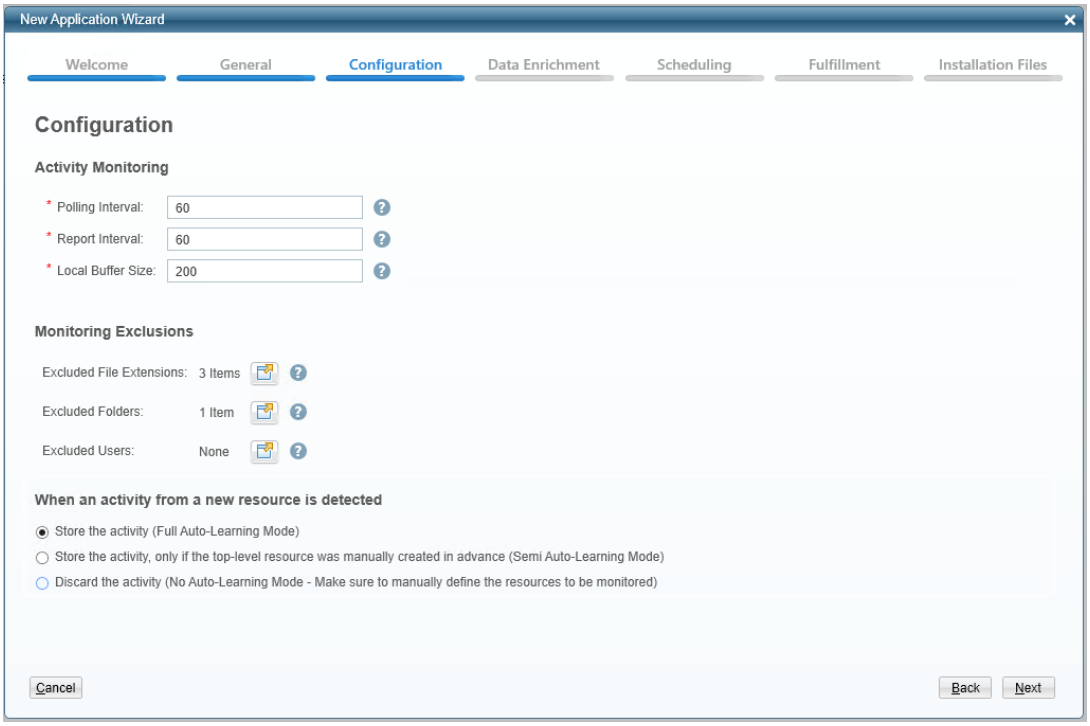

Figure 2. Second Configuration Window

15. Complete the Activity Monitoring fields:

    - *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.

16. Select the relevant Monitoring Exclusions items:

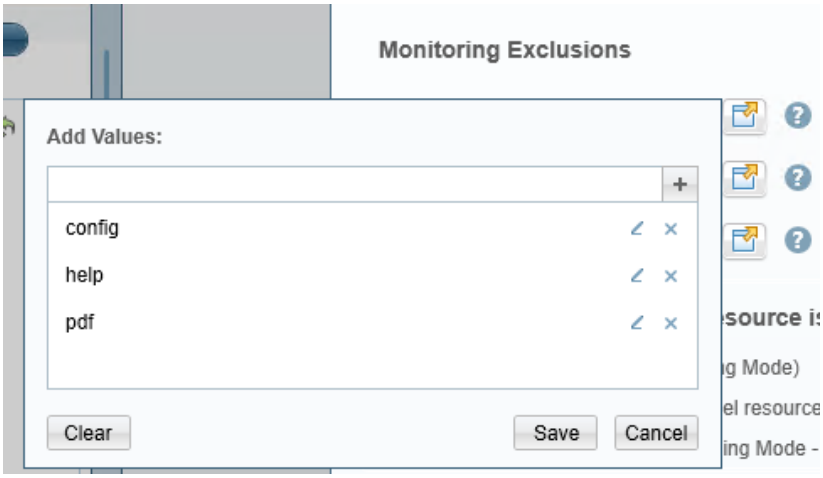

Figure 3. Inserting file extensions to exclude

- *Excluded File Extensions* - A list file extensions that are not monitored. Press "+" on the extension field to add the extension to the list. Press **Save** or **Cancel** to exit this entry panel.
- It is recommended to exclude the following extensions:
  - tmp
  - lnk
  - url
  - ico
- *Exclude Folders* (List folders that will not be monitored.) The excluded folders must be in the **physical path format** (for example, C:\Windows), and not in the share path of the folder. The exclusion of a folder will result in an event not being sent to any of the shares mapped to the physical folder.
  - It is recommended that drives not in use or lacking data be excluded (for example, C:).
- *Exclude Users* (List users whose activities will be monitored). The excluded user must include the domain name in this format:
  'Domain\User' or 'User' for local users
- It is strongly recommended that the following users in Windows be excluded:
  - Local System
  - NT Authority

17. Select the relevant Monitor Configuration fields:

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

18. Click **Next**.

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

19. 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: The chapter *Activities* 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.

20. 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 scheduling window of the New Application Wizard displays under the Scheduling tab.

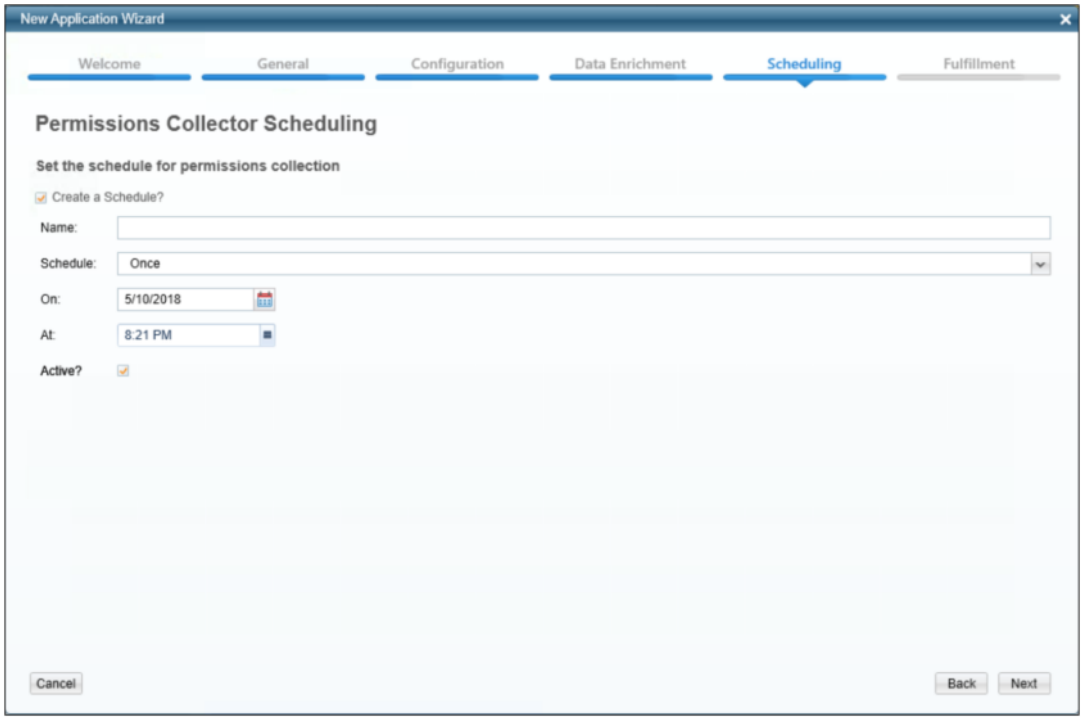

Figure 4. Permissions Collection Window

21. Check the **Create a Schedule** check box.
22. Type a name for the permissions collection scheduling task in the *Name* field.
23. Select a scheduling frequency from the **Schedule** dropdown menu.
24. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
25. Check the **Active** check box if relevant.
26. Click **Next**.

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

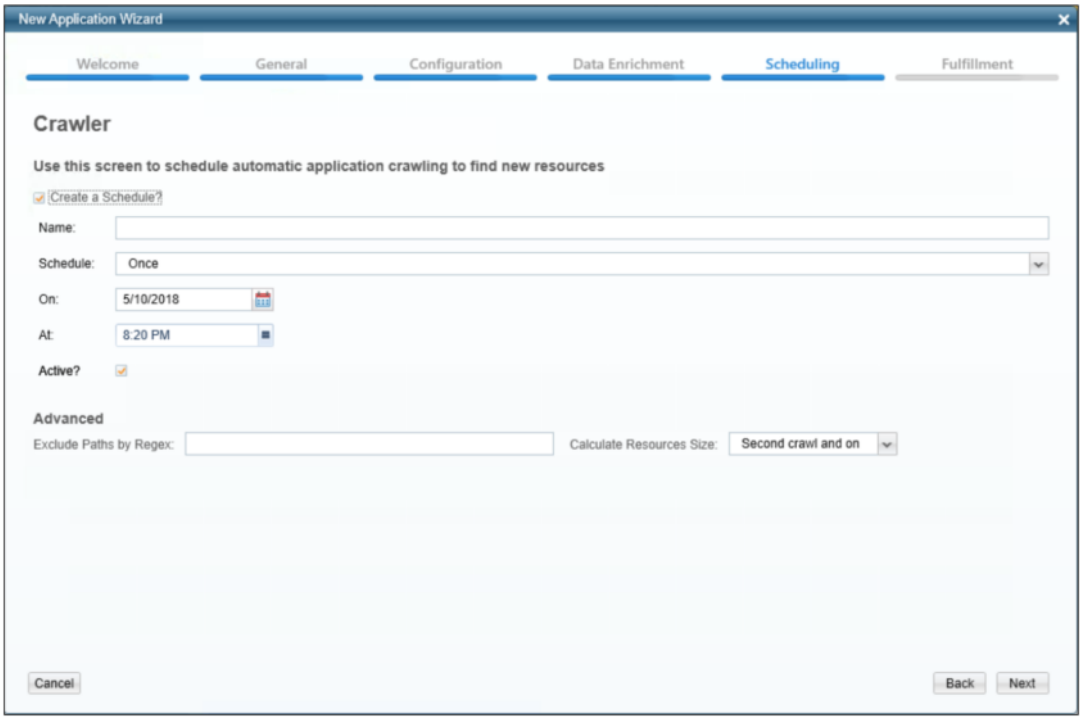

Figure 5. Crawler Window

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

    Note: See the chapter *Crawling* of the IdentityIQ File Access Manager Administrator Guide for more information.

33. Click **Next**.

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

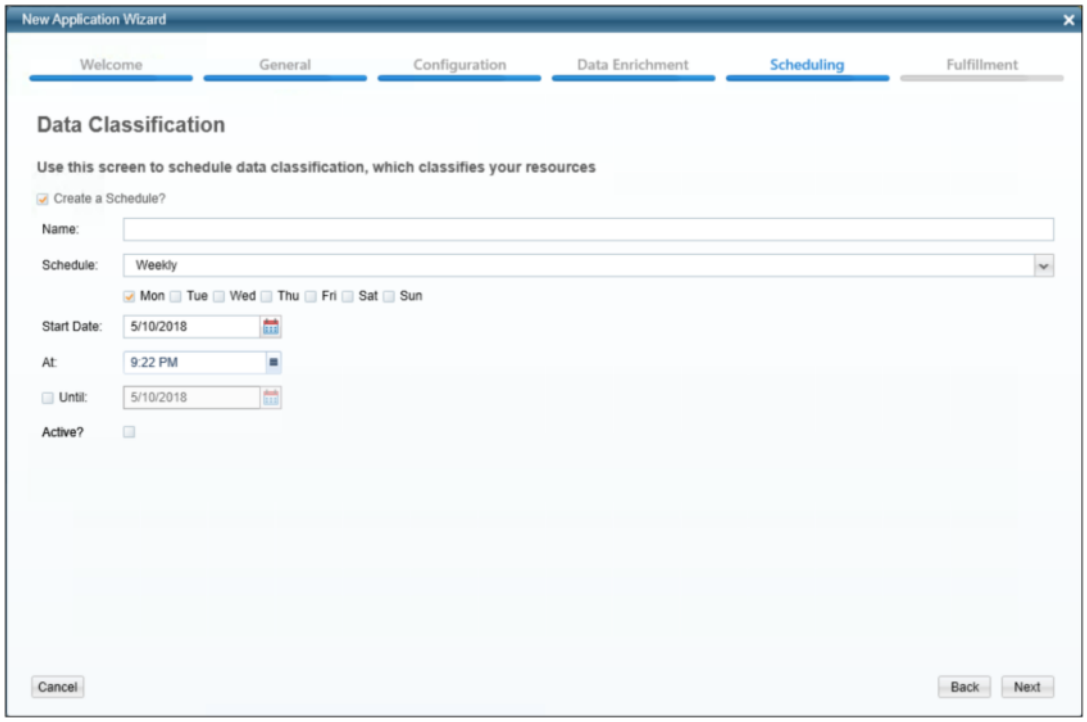

Figure 6. Data Classification Window

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

Note: See the chapter *Data Classification* of the IdentityIQ File Access Manager Administrator Guide for further information.

39. Click **Next**. This will open the Access Fulfillment window of the New Activity Monitor Wizard.
40. Check the relevant fulfillment option.
41. Check the "Enable Access Fulfillment for removing direct permissions" checkbox to enable access direct permission remediation.
42. Check the "Enable Access Fulfillment for normalized groups" checkbox to allow IdentityIQ File Access Manager to add to, and remove permissions from, specific IdentityIQ File Access Manager groups

Note: See *Access Fulfillment* in the IdentityIQ File Access Manager Administrator Guide For additional information.

43. Click **Next**.

44. Browse and select the destination file (used for installing the Activity Monitor/Permissions Collector/Data Classification services) in the *Destination* field.

45. Click **Finish**.

Chapter 6: Add New Bulk Application Wizard

Perform the following steps to add a new bulk application wizard:

1. Admin Client Navigate to **System → Applications → New → Bulk Application**
2. The New Bulk Applications Wizard window of the New Bulk Applications Wizard displays under the Welcome tab
3. Select **Windows File Server**
4. Click **Download Template** and download the bulk installation Excel template

   Note: Each application type has a different template
5. Fill in a new row in the template for each application to be installed
6. In the wizard, click on **Browse** and select the template you filled
7. Click **Upload** to upload the template
8. Once the template is uploaded, the **Upload Status** table contains a row for each application in the template
9. Each row indicates whether the parameters for that application are valid

   Note: At this stage, the applications have only been validated, and have not yet been created.
10. Change the template and upload it if there are errors to be corrected
    If you do not correct errors, applications with errors will be ignored, and only valid applications will be created
11. Click **Next.**

    Note: You can navigate among the Permissions Collection and Crawler scheduling windows (under the Scheduling tab) with the Next and Back buttons
12. The Permissions Collection window of the New Bulk Applications Wizard displays under the Scheduling tab

    Note: A schedule is created for each application with the name: [Application Name] – RoleAnalytics Task, with the same details
13. If you wish to schedule a Permission Collection task, check the **Create a Schedule** checkbox
14. Select a scheduling frequency from the **Schedule** dropdown menu
15. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected)
16. Check the **Active** check box if relevant
17. Click **Next**
18. The Crawler window of the New Bulk Applications Wizard displays under the Scheduling tab.

    Note: A schedule is created for each application with the name: [Application Name] – Crawler Task, with the same details.
19. Check the **Create a Schedule** checkbox.

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. Check the **Active** checkbox if relevant
23. Click **Create**

    Note: The applications are created at this stage

    The Application Creation Status window of the New Bulk Applications Wizard displays under the Status tab

24. A table lists the creation status of each application
25. Click **Next**
26. The Installation File window of New Bulk Applications Wizard displays
27. Browse to select the destination for the .zip file, which contains the files required to install the Activity Monitor/Permissions Collector/Data Classification services for each application.
    A text file with the command line for remote installation of the Activity Monitor connector is also created. (This file can be used for unattended installations of the Activity Monitor.) See "***Activity Monitor Bulk/Unattended Installation***" on page 21 for further information.
28. Click **Finish**

Chapter 7: 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**.

The Service Configuration window displays.

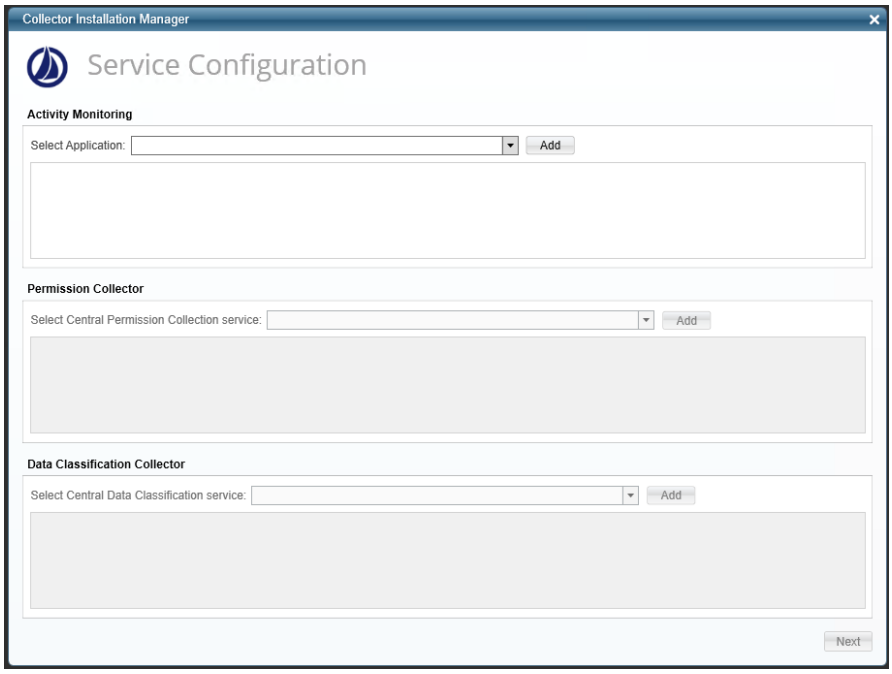

Figure 8. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application and click **Add.**

   Note: The application in the activity monitor dropdown list will not show all the windows file server applications defined. You will see only the windows file server application with the same host name as the one configured above in Chapter 5:Add New Application Wizard, in the Configuration screen.

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 Classification Collector to which to connect this service, and click **Add**.

7. Click **Next** to open the **Installation Folder** window.

   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).

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

Activity Monitor Installation

Standalone Installation in Cluster Architecture

In a cluster architecture, install an activity monitor collector for each physical node in the cluster.

Note: See the chapter *Activities* of the IdentityIQ File Access Manager Administrator Guide for more information.

Activity Monitor Bulk/Unattended Installation

1. Prerequisites:

   a. Verify that the correct .net version is installed. (see Chapter 1: Connector Installation & Configuration on page 1)

   b. For the Windows file server Activity Monitor to work properly the Visual C++ 2010 redistributable package should be installed.

   c. The Visual C++ 2010 redistributable package installer can be found in the installation files under Collectors\vcredist_x64.exe

2. To install the Activity Monitor service:

   a. Copy the distribution file WBXCollectorInstaller.exe to an installation folder on each server.

   b. Run the **Application wizard** for the Windows File Server, after the application was created as part of the bulk creation of new applications. For more information, see Chapter 6: "***Add New Bulk Application Wizard***" on page 17.

   c. This will create a script for installing the Activity Monitor. You can download the script from the wizard screen at this stage.

   d. To access the script, you can alternately click the **Installation Files** button in the **System → Applications** screen, from any application.

   

   Check the "Command line to remotely install the Activity Monitoring connector on Windows" checkbox.

   The command will have the following format, and must be run from the directory in which we put the WBXCollectorInstaller.exe.

```
WBXCollectorInstaller.exe -i --log "[SAILPOINT _HOME_LOGS_FOLDER]" --agent-conf-url
"[AGENT_CONFIGURATION_MANAGER_ADDRESS]" -h "[SAILPOINT_HOME_FOLDER]" --system-guid
"[SYSTEM_GUID]" --valid-cert-hashes "[VALID_CERTIFICATE_HASHES]"
```

Parameters:

AGENT_CONFIGURATION_MANAGER_ADDRESS: Network address of the server which hosts the SecurityIQ Agent Configuration Manager Service (will be filled by the installation wizard).

SAILPOINT_HOME_FOLDER: A home folder for the SailPoint installation (typically: C:\Program Files\SailPoint).

SAILPOINT _HOME_LOGS_FOLDER: A home folder for SailPoint Application logs (typically: C:\Program Files\SailPoint\Logs).

SYSTEM_GUID: The Unique system guide of this Installation.

(will be filled by the installation wizard).

VALID_CERTIFICATE_HASHES: The server certificate hashes that are used to authenticate the Agent Configuration Manager Service

(will be filled by the installation wizard).

Example:

```
WBXCollectorInstaller.exe -i --log "C:\Program Files\SailPoint\Logs" --agent-conf-
url "siq-mtz-jim:8000" -h "C:\Program Files\SailPoint" --system-guid "D108BD1A-
E85F-4264-ACB7-12F0C50016EA" --valid-cert-hashes
"AEA6047CB9D4614BC9E38E8BBB3AD060C8C7CFBF"
```

Windows Server Core

Perform the following steps:

1. Verify that .net3.5 is installed.

```
dir "%SYSTEMROOT%\Microsoft.NET\Framework64" /b /ad
```

2. Copy connector installation binaries to the server.
3. Install Visual C++ 2010 redistributable package by running vcredist_x64.exe from the installation folder
4. Follow the steps in Section *"Activity Monitor Bulk/Unattended Installation"* on page 21.

Chapter 8: Verification

Services

Verify in Windows Service Manager or other tool, that the IdentityIQ File Access Manager services are running. for example,

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

Logs

- "%SAILPOINT_HOME_LOGS%\FilesMiniFilter_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on Windows File Server.
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 9: Troubleshooting

Unable to see events

Symptom

The following error displays in a log file while you attempt to install the monitoring connector:

```
ERROR, WBX.whiteOPS.Agents.FilesMiniFilterActivity Monitor.FileMiniFilterActivity
MonitorManager,connect, An unexpected error occurred while you attempt to start the
mini-filter:
System.DllNotFoundException:
Unable to load DLL 'wbapi.dll': The specified module could not be found. (Exception
from HRESULT: 0x8007007E)—at WBX.whiteOPS.Agents.FilesMiniFilterActivity
Monitor.SafeNativeMethods64.start(UInt32 bufferSizeInBytes, UInt32
trustedProcessId)—at WBX.whiteOPS.Agents.FilesMiniFilterActivity
Monitor.FileMiniFilterActivity MonitorManager.connect()
```

Reason

Visual C++ 2010 redistributable package was not installed as part of the Activity Monitor service installation.

Solution Steps

Perform Step 3 of Activity Monitor Installation, Windows Server Core.

The application is not in the list of Collector Installation Managers

Symptom

The application does not appear in dropdown list of the Collector Installation Managers in the Activity Monitoring

Reason

Either the application was not defined or the *Host Name* (defined in section 5.11) does not match the server's short name on which the Collector Installation Manager was opened on.

Solution Steps

Create the application in case it does not exist.

In case it exists, make sure the *Host Name* is correct.