



# **SailPoint IdentityIQ**

Version 8.1

## **File Access Manager**

### **Active Directory Connector Installation Guide**

This document and the information contained herein is SailPoint Confidential Information.

**Copyright and Trademark Notices.**

Copyright © 2020 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “AccessIQ,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “Managing the Business of Identity,” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

**Patents Notice.** <https://www.sailpoint.com/patents>

**Restricted Rights Legend.** All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

**Regulatory/Export Compliance.** The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

# Table of Contents

---

<b>Chapter 1 Connector Installation and Configuration</b> .....	<b>1</b>
Overview .....	1
Installation Flow .....	1
Installation Locations .....	1
<b>Chapter 2 General</b> .....	<b>2</b>
Connector Operation Principles .....	2
Monitored Activities .....	3
Permissions Collector Operation Principles .....	4
Supported Versions .....	4
<b>Chapter 3 Prerequisites</b> .....	<b>5</b>
Software Requirements .....	5
Enabling the Audit Policy .....	5
Permissions .....	5
Communications Requirements .....	6
<b>Chapter 4 Add New Application Wizard</b> .....	<b>7</b>
<b>Chapter 5 Installation of Services</b> .....	<b>12</b>
Collector Installation .....	12
<b>Chapter 6 Special Configurations</b> .....	<b>14</b>
Excluding Domain Controllers below Windows 2008 .....	14
Monitoring Logon Events .....	14
Excluding Objects from Monitoring .....	14
Crawling .....	15
<b>Chapter 7 Verification</b> .....	<b>16</b>
Services .....	16
Collectors' Installation Status .....	16
Logs .....	16
Monitored Activities .....	16
Permissions Collection .....	16
<b>Chapter 8 Troubleshooting</b> .....	<b>17</b>

# Chapter 1: Connector Installation and Configuration

---

## Overview

---

### Installation Flow

---

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Administrative Client.
3. Install the Activity Monitor/Permissions Collector services.

**Note:** Permission Collector service installation is optional and should only be installed by someone with a full understanding of File Access Manager deployment architecture. The *IdentityIQ File Access Manager Administrator Guide* has additional information on architecture.

### Installation Locations

---

**Activity Monitor** – installed remotely on a File Access Manager monitor application server, which can be a server joined to any domain, including a domain different from the monitored domain.

# Chapter 2: General

---

## Connector Operation Principles

---

- File Access Manager Activity Monitor (Activity Monitor) for Active Directory (AD) is based on the native changes auditing capability in AD. AD writes these changes to the various domain controller event logs and the monitor collects them centrally so there is no need to install connectors on domain controllers.
- The Activity Monitor service correlates the events and digests them, which makes events possible for people to read.
- GPO auditing uses a proprietary method with no local connectors on the DCs. The method accesses all GPOs on all DCs through the SYSVOL share, and correlates GPO audit change events with the content of the GPOs.
- To access the domain controllers, the Activity Monitor reads the list of all Domain Controllers from the domain every hour.
- Crawling and Permissions Collection work with standard LDAP queries to retrieve all the domain objects and their respective permissions.

**Note:** The Activity Monitor and Permissions Collector services can be installed on any server, including servers that are NOT members of the monitored domain. An application must be configured in File Access Manager for each monitored domain, with a separate set of Activity Monitor/Permissions Collection services, as described below.

## Monitored Activities

---

**Table 1—Monitored Activities**

Action	Meaning
Create	An object was created in the domain.
Undelete	An object was restored in the domain.
Move	An object's location was changed in the domain.
Delete	An object was deleted in the domain.
Audit Policy Change	The domain audit policy was changed.
FSMO Role Change	The owners of the domain FSMO roles were changed.
Domain Policy Change	The domain security policy was changed.
Account Lock	An account was locked, which includes the computer that originally caused the lock.
Reset Password	A user password was reset by another user.
Modify	An object attribute was changed on a domain object, including the Old and New values of the attribute. *1.
Account Logon	A user logged on in the domain*2.
Failed Login Attempt	A user login attempt to Active Directory was rejected
Added Permission	A permission was added to an object in the domain.
Removed Permission	A permission was removed from an object in the domain.
GPO Status Modify	The GPO enable/disable status was modified.
GPO Security Filtering Modify	Objects to which the GPO applies were changed.
GPO Property Modify	A property was changed in a GPO, including the old and new value of the property *1.
GPO Link Modify	A GPO Link was changed.
GPO Link Added	A GPO link was added.
GPO Link Removed	A GPO link was removed.

**Note:** 1. The old value will be empty and will not display in the Administrative Client if it was empty before the change. This is also true for the New value, if the attribute's value was deleted.

**Note:** 2. The account logon is not monitored by default. (The Special Configuration section below describes how to configure the Activity Monitor to collect Account Logon events)

## Permissions Collector Operation Principles

---

- IdentityIQ File Access Manager connects to the domain using LDAP, to crawl and analyzes the permissions of its objects.

## Supported Versions

---

- Activity Monitor
- The system only supports change auditing on Domain Controllers installed on Windows Server 2008 and above.  
**Note: Only the operating system version of the domain controller (not the domain functionality level) is relevant.**
- Permissions Collection and Crawling are supported for all domain and forest versions, and operating systems.

# Chapter 3: Prerequisites

---

## Software Requirements

---

- Activity Monitor/Permissions Collector
  - Microsoft .Net Framework 4.5

## Enabling the Audit Policy

---

**Note:** IdentityIQ File Access Manager relies on the standard Active Directory advanced audit. The advanced audit overrides the simple audit, making the former obsolete. Be sure to migrate existing simple auditing to Advanced Auditing before proceeding.

**Note:** This guide does not deal with complex GPO scenarios. Be sure that changes do not affect GPO precedence or corrupt other GPOs. The bullets below list the settings in the Domain Controllers GPO.

Apply the following in a Domain Controller GPO.

1. Open “Default Domain Controller Policy”.
2. Navigate to **Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies**.
3. Set **Audit to success in the following settings**
  - Account Management → Audit User Account Management
  - DS Access → Audit Directory Services Changes
  - Logon/Logoff → Audit Account Lockout
  - Policy Change → Audit Policy Change
  - Policy Change → Audit Authentication Policy Change
  - Policy Change → Audit Authorization Policy Change

**To enable login audits:**

  - Set Audit Kerberos Authentication Service to Success in  
->Account Logon

## Permissions

---

The Active Directory user configured in the Application configuration below must be granted permissions to manage the audit settings of the domain objects, as well as to access the Domain Controller event logs.

1. Grant Manage Auditing and Security Log Privilege
  - a. Open Default Domain Controller Policy on a DC.

- b. Navigate to **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment** and set the following settings:

Open *Manage auditing and security log* by double clicking or pressing **Enter**.

Add the domain user to the Users/Groups list.

**Note:** The syntax of the user added to the list must be **Domain\User**.

- 2. Add the user to the “Event log readers” security group.

## Communications Requirements

---

**Table 2—Communications Requirements**

Requirement	Source	Destination	Port
IdentityIQ File Access Manager Message Broker	Permissions Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor/Permissions Collector	IdentityIQ File Access Manager Servers	8000-8008
Event log remote	Activity Monitor	All Domain Controllers	MS RPC (135)
SYSVOL access	Activity Monitor	All Domain Controllers	CIFS/SMB (139, 445)
Additional queries	Activity Monitor/Permissions Collector	All Domain Controllers	LDAP (389)

# Chapter 4: Add New Application Wizard

1. Navigate to

**Admin Client**

**Applications >> New >> Application**

2. The **New Application Wizard** window displays under the Welcome tab.

3. Select Standard Application.

4. Select **Active Directory** 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 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.

The screenshot shows the 'New Application Wizard' window with the 'Configuration' tab selected. The 'Connection Details' section includes fields for Domain Name, Port (389), SSL, Domain NetBIOS Name, Base DN, User, Password, Repeat Password, Specific Server Connection, Pool Size (50), and Timeout (15). The 'Permissions Collection' section includes checkboxes for 'Enable Permission Collection', 'Skip Identities Sync during Permissions Collection', and 'Calculate Effective Permissions', along with a dropdown for 'Central Permission Collection Service'. There are 'Cancel', 'Back', and 'Next' buttons at the bottom.

**Figure 1. Configuration Window I**

11. Complete the Connection Details fields:

- **Domain Name**

FQDN of the domain.

- **Port**

The communication port configuration. The port value must be 389 or 636 if SSL is checked.

- **SSL**

Must be checked to connect with LDAPS, and the Port field must be set to 636, if set.

- **Domain NetBIOS Name**

The short name of the domain.

- **Base DN**

Distinguished Name (DN) – The level in the AD tree from which to perform a search. This field should remain empty unless needed.

- **User**

The samAccountName of the user defined in the prerequisites, or the UPN if the user is from a different trusted domain.

- **Password**

The user's password

**Note:** If the user is from a different trusted domain, type the UPN in the User field (username@fqdn), and type the short name of the domain in the Domain NetBIOS Name.

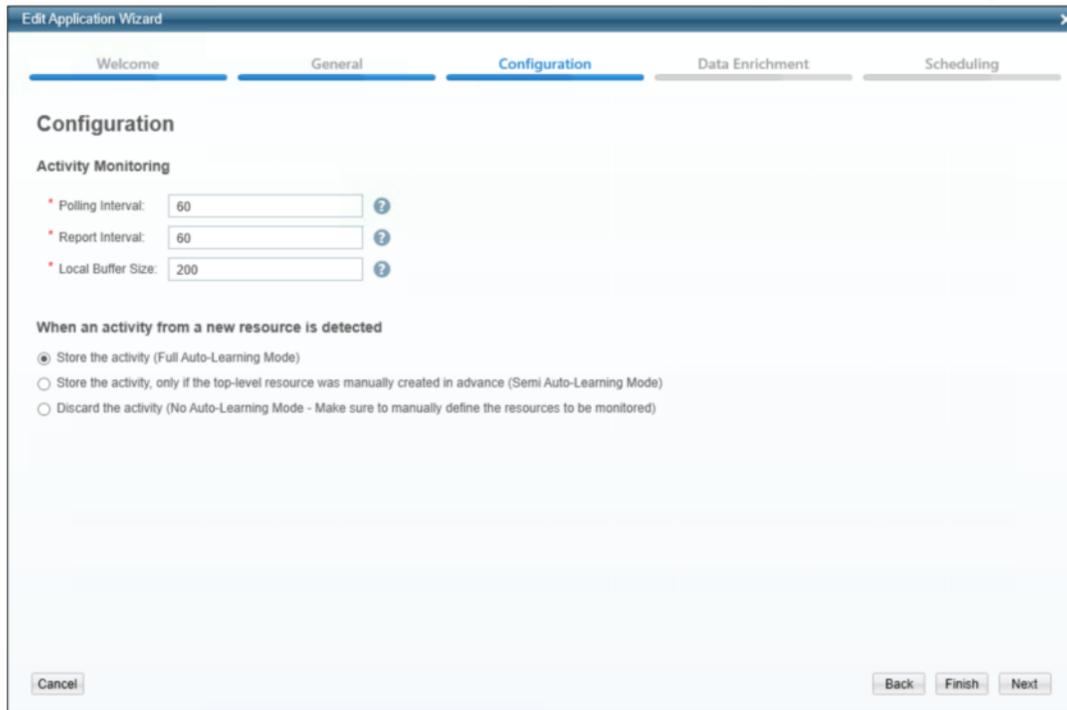
- *Specific Server Connection* (Connection through a specific server instead of selecting a DC dynamically)
- *Pool Size* (Number of parallel LDAP connections to DCs)
- *Timeout* (Timeout for each LDAP query in seconds)

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 permissions collection tasks when the identity collector is common to many different connectors.)
- *Calculate Effective Permissions* (Calculate effective permissions during the permissions collection run.)

13. Click **Next**.

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



**Figure 2. Configuration Window II**

14. Complete the Activity Monitoring requirements:

- *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 relevant Monitor Configuration fields:

- *Store the activity (Full Auto-Learning Mode)* (Monitor all activities from all site collections to create new folders in the Business Resources Tree automatically.)
- *Discard the activity (No Auto-Learning Mode)* (Be sure to manually define only the resources to be monitored.)

16. Click **Next**.

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

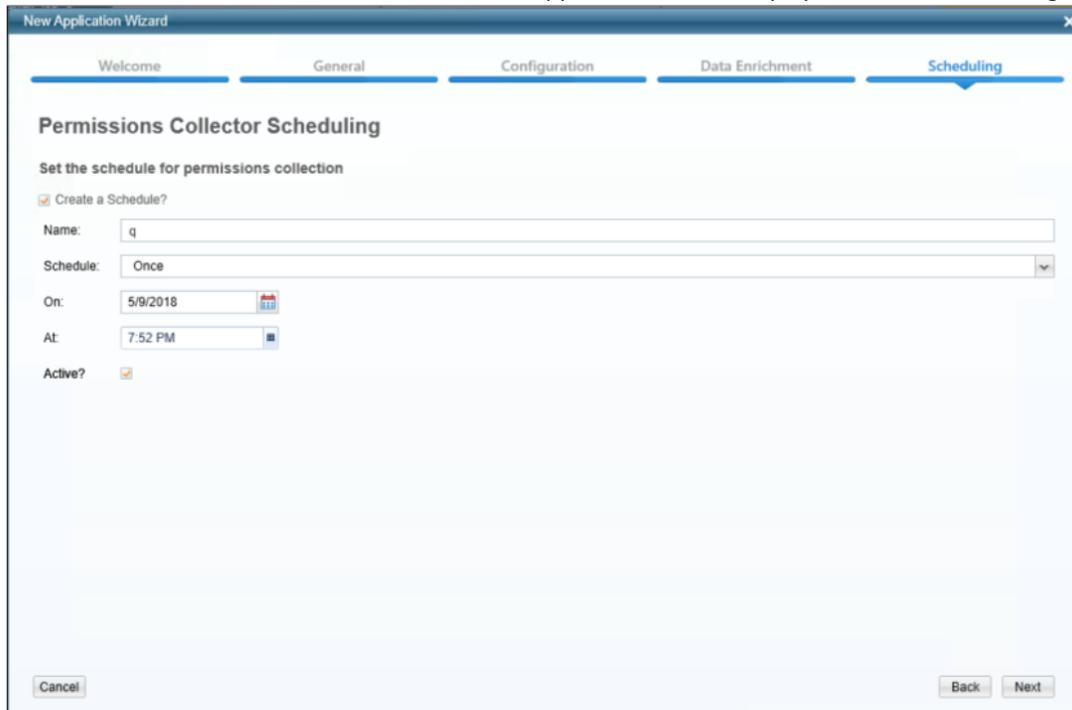
17. Select the data enrichment connectors (DECs) to enrich monitored activities from the Available DECs text box and use the > or >> arrows to move them to the Current DECs text box.

**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.

18. 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.



The screenshot shows a window titled "New Application Wizard" with a navigation bar containing tabs for "Welcome", "General", "Configuration", "Data Enrichment", and "Scheduling". The "Scheduling" tab is selected. The main content area is titled "Permissions Collector Scheduling" and contains the following fields and controls:

- Section: "Set the schedule for permissions collection"
- Check box: "Create a Schedule?" (checked)
- Text field: "Name:" with the value "q"
- Dropdown menu: "Schedule:" with the value "Once"
- Date field: "On:" with the value "5/9/2018" and a calendar icon
- Time field: "At:" with the value "7:52 PM" and a clock icon
- Check box: "Active?" (checked)
- Buttons: "Cancel", "Back", and "Next" at the bottom.

**Figure 3. Permissions Collection Window**

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

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

The screenshot shows the 'Crawler' window within the 'Edit Application Wizard'. The window has a title bar 'Edit Application Wizard' and a navigation bar with tabs: 'Welcome', 'General', 'Configuration', 'Data Enrichment', and 'Scheduling'. The 'Scheduling' tab is active. The main content area is titled 'Crawler' and contains the following elements: a sub-header 'Use this screen to schedule automatic application crawling to find new resources'; a checked checkbox 'Create a Schedule?'; a 'Name:' text input field; a 'Schedule:' dropdown menu set to 'Once'; an 'On:' date picker set to '5/10/2018'; an 'At:' time picker set to '7:50 PM'; an 'Active?' checked checkbox; and an 'Advanced' section with an 'Exclude Paths by Regex:' text input field. At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**Figure 4. Crawler Window**

25. Check the **Create a Schedule** check box.
26. Type a name for the crawling scheduling task in the *Name* field.
27. Select a scheduling frequency from the **Schedule** dropdown menu.
28. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
29. Check the **Active** check box if relevant.
30. Type in the distinguished names 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.

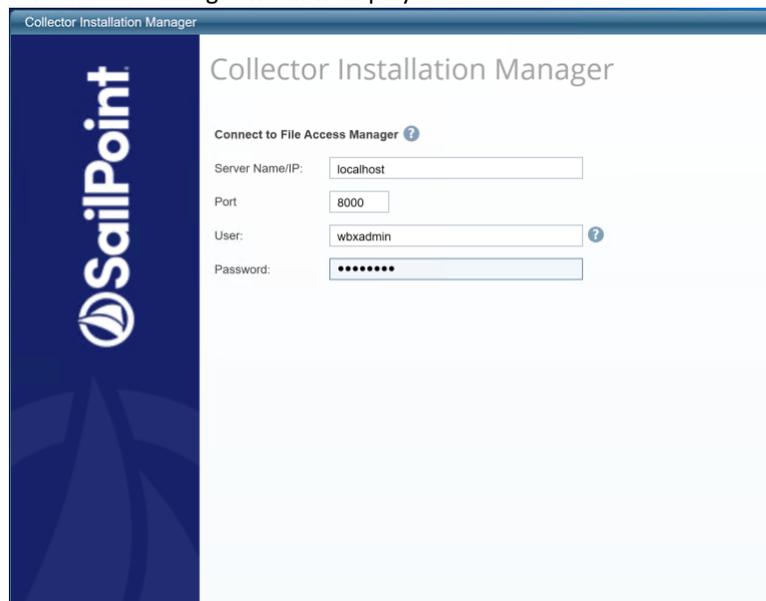
**Note:** By default, File Access Manager crawls specific object types, which can be overridden, as described in the Configurations section below.

Click **Finish**.

# Chapter 5: Installation of Services

## Collector Installation

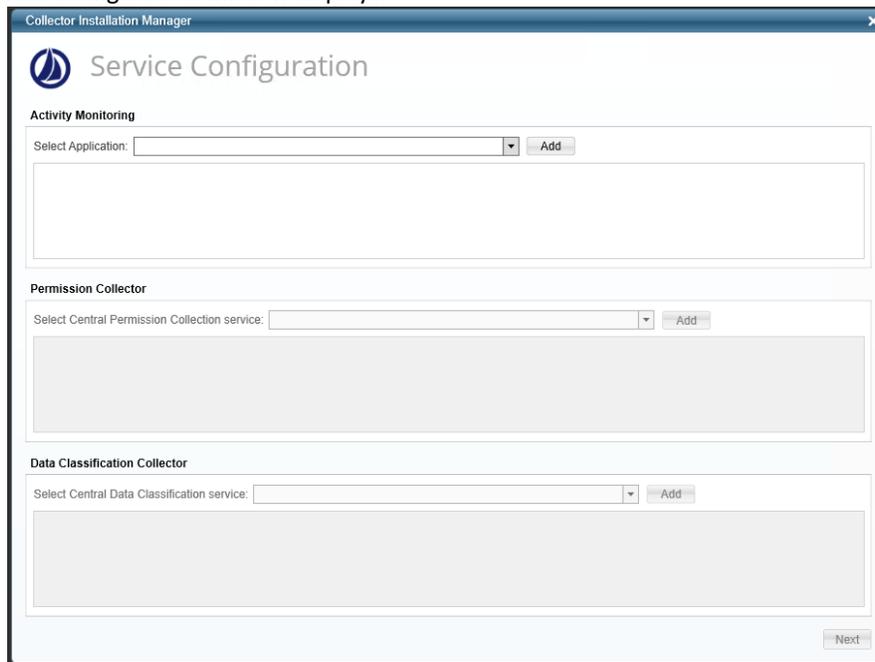
1. Run the “Collector Installation Manager” as an Administrator.  
The installation files are located in the installation package under the folder **Collectors**.  
The Collector Installation Manager window displays.



**Figure 5. 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, use the format domain\username.
3. Click **Next**.

The Service Configuration window displays.



**Figure 6. 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. Click **Next**.
7. 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).

**Note:** The *IdentityIQ File Access Manager Administrator Guide* provides more information on Permissions Collection.

# Chapter 6: Special Configurations

---

## Excluding Domain Controllers below Windows 2008

---

If there are domain controllers installed on an operating system older than Windows 2008, the system displays an error message in the Activity Monitor log, indicating that the Activity Monitor cannot connect to the Domain Controllers.

To exclude these Domain Controllers, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called "ExcludedDCs":  
`<add key="ExcludedDCs" value="" />`
4. Add the FQDN of the domain controllers to be excluded, separated by the | character:
5. `<add key="ExcludedDCs" value="old-dc1.deprecated.com|old-dc2.10.years.old.os.com" />`
6. Restart the Activity Monitor service.

## Monitoring Logon Events

---

To add monitoring of Logon events, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called "readLogonEvents", and set it to true:  
`<add key="readLogonEvents" value="true" />`
4. Restart the Activity Monitor service.

## Excluding Objects from Monitoring

---

By default, the Activity Monitor excludes the dnsNode and msExchActiveSyncDevice object classes from monitoring.

To exclude additional object classes from monitoring, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called "excludedObjectClasses", and set its value to the object classes to exclude:

```
<add key="excludedObjectClasses"
value="dnsNode|msExchActiveSyncDevice"/>
```

**Note:** The value must contain a list of object classes separated by the '|' character.

## Crawling

---

By default, IdentityIQ File Access Manager crawls and creates business resources for the following object types in the domain:

- User
- Group
- Organizational Unit (OU)
- Domain
- Computer
- Container

Overriding the default object types is not recommended, since they are the most common, and serve to exclude irrelevant object types (such as DNS records or Exchange Active Sync objects).

To override the default behavior, perform the following steps:

1. Open the Permissions Collector configured for the Active Directory Application installation folder.
2. Edit the RoleAnalyticsServiceHost.exe.config file
3. Under the <appSettings> section, add the following key:

```
<add key="relevantTypes" value="objectClass|objectClass|...|objectClass" />
```

**Note:** The value must contain a list of object classes separated by the | character and the domain object class must be one of the object classes in the defined list.

Restart the Permissions Collector service.

# Chapter 7: Verification

---

## Services

---

### Collectors' Installation Status

---

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

for example,

- **File Access Manager Central Activity Monitor** - <Application\_Name> service is running.
- **File Access Manager Central Permissions Collection** - <Application\_Name> service is running.

## Logs

---

- "%SAILPOINT\_HOME\_LOGS%\ACTIVE\_DIRECTORY\_<Application\_Name>.log" does not contain errors.
- "%SAILPOINT\_HOME\_LOGS%\Permissions Collection\_<Application\_Name>.log" does not contain errors.

## Monitored Activities

---

1. Simulate activities on Active Directory.
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 Administrative Client.
2. Verify that:
  - The tasks completed successfully.
  - Business resources were created on the BRs tree.
  - Permissions display in the Permissions Forensics window.

# Chapter 8: Troubleshooting

---

If activities are not shown in the Administrative Client:

- Verify that all prerequisites were set.
- Check the Activity Monitor logs for errors.
- If there are errors on accessing the domain controllers (such as RPC server or server not available) verify that this domain controller is running on Windows 2008 or above.
- Open the event viewer of the domain controller on which the change was made, with the user configured in the Application configuration.  
(If the viewer fails to open, verify that the user has the permissions described in the prerequisites section.)
- Search for events with IDs 5136-5141.  
(Verify the connection to the domain controller in which the change was made, and verify that the change audit policy was enabled as written in the prerequisites section.)
- If no events were found, run the following command on the domain controller:

`Auditpol /get /subcategory: "directory service changes"`

Verify that the settings described in the "Enabling the Audit Policy" are "Success".

- If these settings are not defined, trigger a GPO update by running the following command:  
`gpupdate /force`

If the settings are still not defined, verify that the GPO is properly configured in, and applied to, the domain controller.