SailPoint IdentityIQ

Version: 8.0

File Access Manager Google Drive 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
5.1	Fourth Draft	Jonathan Rappeport	31 Dec 2017
6.0	First Draft	Jonathan Rappeport	10 May 2018
6.1	Formatting changes only	Josh Lewin	11 Dec 2018
8.0	• Updated Copyright • Format • Rebranding to IdentityIQ File Access Manager 8.0 • Support for Google Drive Activity API V2 • Update scope in Google setting	Josh Lewin	30 Jul 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.
3. Install the Permissions Collector/Activity Monitor/Data Classification Collector 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.

Chapter 2: General

Connector Operation Principles

- IdentityIQ File Access Manager Connector for Google Drive uses the following Google APIs:
  - Google Drive Activities API and Google Reports API for event monitoring
  - Google Drive API for resource crawling and permissions collection
  - Google Admin SDK (Directory API) for domain identities (users, groups, and so on)
- Google APIs are accessed via a Service Account, defined within the scope of the customer's Google Apps Domain. The Service Account has Domain-wide delegation permission so that it can impersonate domain users and access their Google Drive activities and data.

Business Resources Tree

- Google Drive represents files and folders in a graph (a.k.a. map) data structure so that every node may have multiple parent and children nodes. In a tree structure, however, every node can have only one parent. For example, a folder shared by two users actually has two different parents – one in each of the user's personal drives.
- To maintain a recognizable structure for Google Drive resources, IdentityIQ File Access Manager displays business resources in a tree, exactly as they are arranged from the user's perspective.
- When users share folders, flattening the graph structure into a tree results in duplicate resources, which are maintained to keep the structure recognizable.
- If external users (external to the company's Google Apps domain) share folders with domain users, a separate "External" tree root represents those resources.
- The following is a sample schematic of the IdentityIQ File Access Manager Google Drive resource tree:
  - External
    - private@gmail.com
      - sharedFolder1
  - Users
    - u1@my-company.com
      - Folder1
      - Folder2
  - u2@my-company.com
  - u3@my-company.com

Monitored Activities

Monitored Administrator audit events (Google Domain events) include:

- User Events and group events (USER_SETTINGS and GROUP_SETTINGS, respectively)

Activity Association to Business Resource

Domain administration events (for example, user creation and association with groups) are associated with a special "Admin Audit" resource. This resource is created automatically at the root level of the IdentityIQ File Access Manager Google Drive application when the first administrative event arrives.

Events and activities are only associated with the resource nested under the resource owner's tree. For example, if *u1@my-company.com* shares a folder named "Sales" with *u2@my-company.com,* the activities performed in/on this folder are only associated with the owner of the folder. This association prevents event duplication and assures that the real data owner of the folder controls the folder's activities.

In the following Activity Association tree, owners are indicated **in bold**.

- Google Drive Activity Monitor
  - **Admin Audit** <= admin events here
  - Users
    - u1@my-company.com
      - **Sales** <= resource events here
      - Private Pictures 2017
    - u2@my-company.com
      - Shared from colleagues
        - ✓ Sales <= no events here
      - Ideas

Events in which the event actor is not the resource owner feature an additional field that contains the original access path. For example, if *u2@my-company.com* creates a file in the "*Sales*" folder, the event includes the following access path:
*u2@my-company.*com/Shared from colleagues/Sales.

Permissions Collector Operation Principles

The IdentityIQ File Access Manager Google Drive Permissions Collector uses Google Drive API to retrieve information on collaboration and sharing.

IdentityIQ File Access Manager automatically creates a Google Drive Identity Collector (when the "Add New Application" wizard finishes) which collects the users and groups from the Google Apps Domain.

Chapter 3: Prerequisites

Software Requirements

- Activity Monitor/Permissions Collector/Data Classification Collector service
  - Microsoft .Net Framework 4.5

Permissions

To enable IdentityIQ File Access Manager to interact with Google Apps:

1. Create a service account within your domain space and generate a private key that IdentityIQ File Access Manager can use for authentication.
2. Enable the Google SDKs used by IdentityIQ File Access Manager.
3. Delegate domain-wide authority to the service account.

Create a project:

a. Go to your Google Apps developer console: https://console.developers.google.com.
b. Make sure that you are using an administrator account for your Google Apps domain.
c. On the left-side pane, select Projects and click “Create Project”.
d. Name the project (e.g., “IdentityIQ File Access Manager”) and click “Create”.

Enable Google APIs:

a. On the left panel, switch to the "Overview" tab.
b. Using the Search box, find and enable the following APIs:
   i. Google Drive API
   ii. Apps Activity API
   iii. Admin SDK

Create a service account:

a. On the left-side pane, click the “Credentials” tab.
b. Click “Create credentials", Select “Service Account key”.
c. From the "Service account" dropdown list choose "New service account".
d. Input a name for the new service account in "Service account name" (e.g. "IdentityIQFAM").
e. Choose "P12" under "Key type".
f. Click "Create".
g. A certificate file (".p12") will be downloaded to your computer, this file will be needed in the Add New Application Wizard in Section 4.
h. A popup window will appear showing the password to the .p12 file. Save this password for later use used in Section 4.

> **Note:** Since this popup is displayed only once, you must copy the password. Otherwise you will have to define a new service account!

Delegation of domain-wide authority to the service account:

a. In the Google Developers Console, click the main menu button (in the top left corner) and switch to the "IAM and Admin" page.
b. On the left panel, switch to the "Service accounts" tab.
c. Find the newly created service account and click "Edit" (on the right end of its table row).
d. Check the "Enable Google Apps Domain-wide Delegation" checkbox.
e. Click the "View Client ID" link (under the "Options" column)
f. Copy the Client ID number.

Define permissions for your service account:

a. From a new browser window (keep the Developer Console open on a separate window), go to your Google Apps administrative console: https://admin.google.com.
b. Click “Security” (if it is not listed, click the “More controls” button at the bottom of the screen).
c. Click “Show more”.
d. Click “Advanced Settings”.
e. Click “Manage API client access”.
f. Under “Client Name”, paste the “Client ID” of the service account you created before.
g. Under “One or More API Scopes”, paste the following (in one line, comma delimited):
h. Click “Authorize”.

```
https://www.googleapis.com/auth/activity,https://www.googleapis.com/auth/drive.activity,https://www.googleapis.com/auth/admin.directory.group.member.readonly,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.reports.audit.readonly,https://www.googleapis.com/auth/drive.readonly
```

Limiting IdentityIQ File Access Manager Permissions

During the Application setup, you must provide a Domain Admin User for IdentityIQ File Access Manager to collect data on the Google Drive domain.
You can provide the Super Admin, or create a dedicated IdentityIQ File Access Manager Google account with fewer permissions.
The IdentityIQ File Access Manager Google account requires the following permissions:

On the desired OU (Organizational Unit) level

- Organizational Units -> Read
- Users -> Read

Domain-wide

- Groups -> Read
- Reports

Note the following regarding crawling, permissions collections, and activities:

Crawling

- The resource tree contains only OU users and folders for which a IdentityIQ File Access Manager user has permissions.

Permissions Collection

- IdentityIQ File Access Manager only analyzes resources for permissions under scoped OUs.

- Since groups are defined on a domain-wide basis, rather than by OU, IdentityIQ File Access Manager collects all domain groups.
- If users from OUs (for which a IdentityIQ File Access Manager user lacks permission) have permissions on resources under the analyzed OU, those users are considered IdentityIQ File Access Manager External Accounts, since IdentityIQ File Access Manager cannot collect information on those users.

Activities

- IdentityIQ File Access Manager only collects activities for users for which a IdentityIQ File Access Manager user has permissions.
- IdentityIQ File Access Manager collects administrator activities (such as changing users or passwords) on a domain-wide basis, rather than by user/OU.

Data Classification

- IdentityIQ File Access Manager only indexes and classifies resources collected during a crawl (only resources to which a IdentityIQ File Access Manager user has permissions).

To create, and grant permissions to, a IdentityIQ File Access Manager Google Administrator account perform the following steps:

1. Sign in to the Google Administrator console (admin.google.com) using the Super Admin account (or any account that can create and grant Administrator roles and create users).
2. Click Users

   Note: If you cannot see Users, click the More Controls bar at the bottom of the screen.
3. Choose an OU on which to create a IdentityIQ File Access Manager account by hovering over the plus (+) sign at the bottom right corner of the screen.
4. Click Add User.
5. Fill in a name and primary email address for the user (for example, identityiqfam_reader).
6. Click Create.
7. Click Admin Roles on the Google Admin console.

   Note: If you cannot see Admin Roles, click the More Controls bar at the bottom of the screen.
8. Click Create a New Role. (This will be the OU targeted role.)
9. Type a role name and description (for example, IdentityIQFAM OU Reader).
10. Click Create.
11. Check the following checkboxes under the Privileges tab → Admin Console Privileges:
    a. Organizational Units → Read
    b. Users → Read
12. Click Save.
13. Select the newly created role, and click Assign Admins under the Admins tab.
14. Select the desired OU from the drop-down list and type the name of the IdentityIQ File Access Manager account.
15. Click Confirm Assignment.

Note: The role applies to the OU and all its descendants. You can assign the role to the same user on another OU later.

16. Click Create a New Role. (This will be a domain-wide role.)
17. Type a role name and description (for example, IdentityIQFAM Domain Reader).
18. Click Create.
19. Check the Reports checkbox under the Privileges tab → Admin Console Privileges.
20. Check the Groups → Read checkbox under the Privileges tab → Admin API Privileges.
21. Click Save.
22. Select the newly created role, and click Assign Admins under the Admins tab.
23. Type the IdentityIQ File Access Manager account.
24. Click Confirm Assignment.

Communications Requirements

Table 1. Communications Requirements

Requirement	Source	Destination	Port
IdentityIQ FAM RabbitMQ	Permission Collector/Data Classification Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ File Access Manager Servers	8000-8008
Permissions Collector /Data Classification Collector	Permissions Collector/Data Classification	Google APIs	https
Activity Monitoring	Activity Monitor	Google APIs	https

Chapter 4: Add New Application Wizard

1. Admin Client Navigate to **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 **Google Drive** 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. Click **Next**.

   The Configuration window of the New Application Wizard displays under the Configuration tab.
10. 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.)
11. Click to enable Data Classification and select a central data classification service from the list.
12. Click **Next**
13. Complete the Monitor Behavior 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.
14. Click **Next**.

    The Data Enrichment Connectors window of the New Application Wizard displays under the Data Enrichment tab.
15. 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.

16. Click **Next**.

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

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

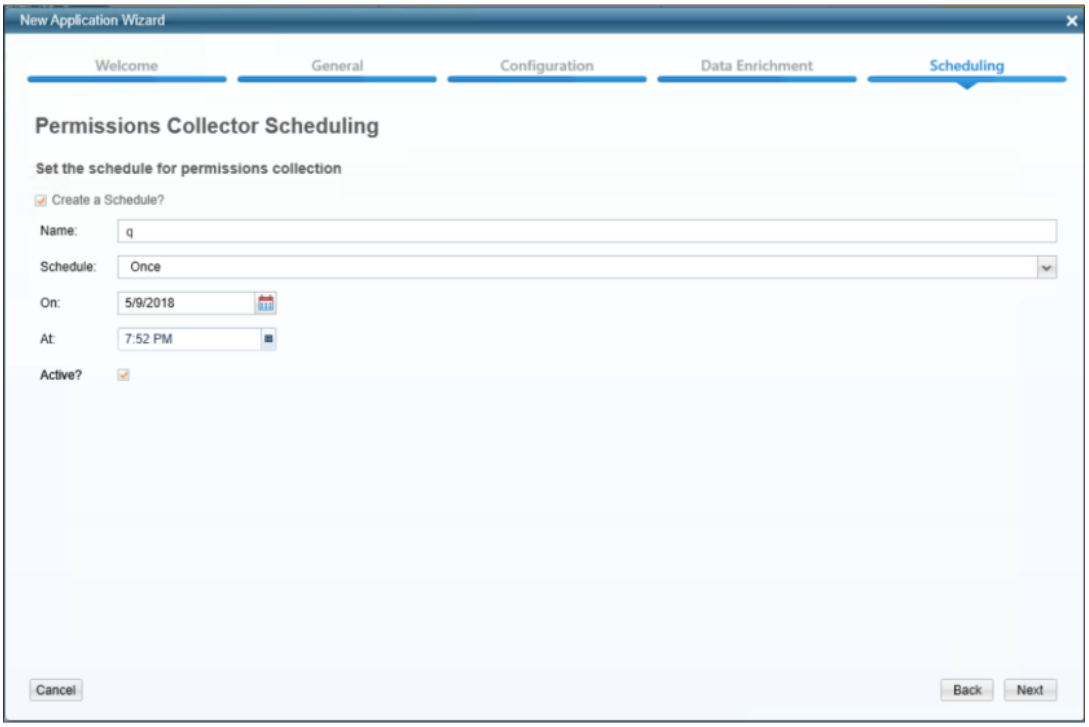

Figure 1. Permissions Collection Window

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

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

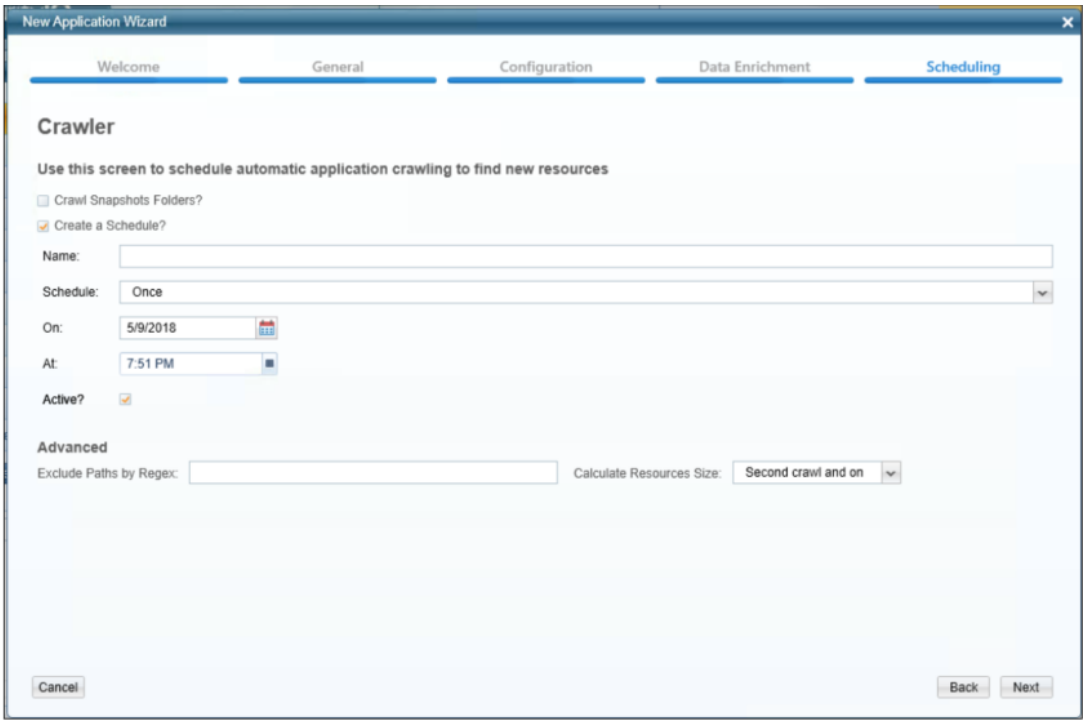

Figure 2. Crawler Window

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

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

29. Click **Next**.

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

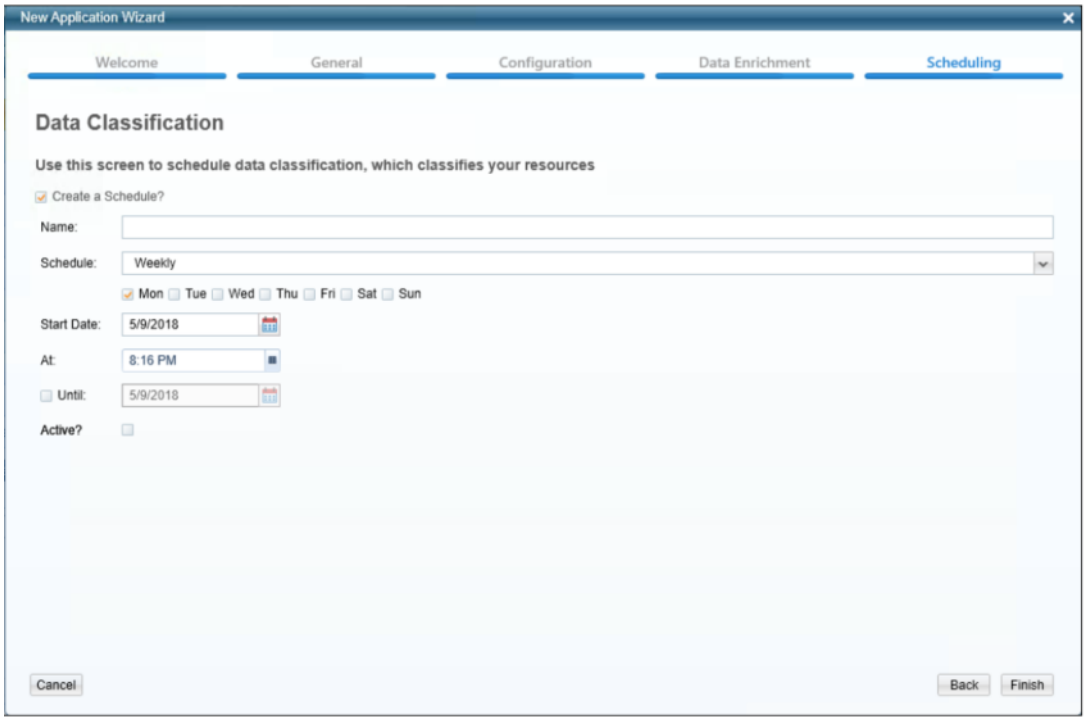

Figure 3. Data Classification Window

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

    Note: See the chapter *Data Classification*- of the IdentityIQ File Access Manager Administrator Guide for more information.
35. 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 4. 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.

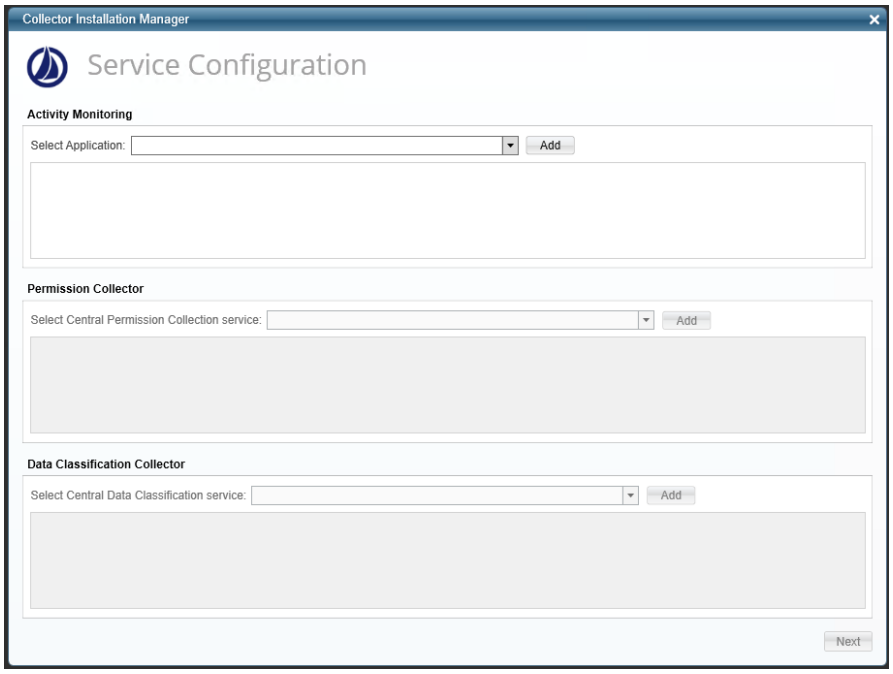

Figure 5. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application, and click Add.
5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click Add.
6. If you are installing the Data Classification Collector, select the Central 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 the chapter *Permissions* of IdentityIQ File Access Manager Administrator Guide for further information on permission collection.

Chapter 6: 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 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%\GDrive_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\RoleAnalytics_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\Watchdog_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on Google.
2. Wait a minute (approximately).
3. Query for activities in the IdentityIQ File Access Manager Admin Client by <Application _Name>.
4. Verify that the activities display in the IdentityIQ File Access Manager Admin 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 Permissions Forensics window.