SailPoint IdentityIQ

Version: 8.0

File Access Manager SQL Server Connector Installation Guide

Table of Contents

List of Figures

List of Tables

Table of Revisions

Ver. #	Description	Author	Date
8.0	Initial release	Josh Lewin	29 Jul 2019

Chapter 1: Connector Installation & Configuration

Overview

General

The SQL connector enables connection to an MS SQL resource. The connector supports crawling, permissions collection and activity monitoring.

Note: Permission Collector service 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 File Access Manager architecture.

Supported versions

System	Supported Versions	
MS SQL Server	2017 (14.0) 2016 (13.0) 2014 (12.0) 2012 (11.0)	

Notes:

- **MS SQL Server 2008 is no longer supported**
- **Just to clarify: IdentityIQ File Access Manager supports MS SQL Server versions 2008R2, 2012, 2014, 2016, 2017 for running the application database. This document, on the other hand, describes connecting to an MS SQL Server as an application containing business resources.**

Limitations of the SQL Server Connector

The following features are not supported by the SQL Server Connector

- Nested Roles – Roles within other roles (Database roles and Server roles)
- SQL Server Permission Covering

  See: https://docs.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-2017#chart-of-sql-server-permissions
- Contained Users - SQL Server Database Contained Users
  See: https://docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable
- MS SQL Server for Azure
- The following SQL Server Resources
  XML Schema Collections, Message Types, Contracts, Services, Remote Service Bindings, Routes, Full-text catalog and stoplists, Symmetric Key, Asymmetric Key, Certificate, Endpoints, Availability Groups, Database scoped credential

IdentityIQ features not supported by the SQL connector

- **What If** for local groups

- Access fulfillment
- Data Classification
- Effective Permissions are not calculated. The flag is always set to FALSE

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Admin Client.
3. Optionally, install the Activity Monitor.

Chapter 2: General

Activity Monitor Operation Principles

The activity monitor collects events from the SQL server using a query that is defined in the application configuration. Each row returned by the query is an activity, and stored in the IdentityIQ File Access Manager database.

To configure activity monitoring in IdentityIQ File Access Manager

1. Identify or create a database activity table that contains the activities
2. Create a query defining user activities as you wish to monitor them, that points to this activity table
3. Add the query to the configuration panel described below, under Activities Query
4. Map the fields in the Activities Query to the IdentityIQ File Access Manager activity fields, on the same configuration panel

Permissions Collector Operation Principles

General

IdentityIQ File Access Manager connects to the SQL Server through Microsoft ODBC driver, gathers local SQL Server principals and analyzes its objects and permissions on all the server's database instances.

Local principals gathering

Identity types

Before collecting all the permission-principal relations, 3 types of identities are collected:

- Server Logins – principals that might relate to a Windows user / active directory user or an SQL Server authentication user
- Server Roles – principals that act as SQL Server groups on the entire server scope
- Database Roles – principals that act as SQL Server groups on a database scope

Principals Naming

SQL Server Login names stored by the Permission Collection have certain naming patterns, whereas "domain" fields might act as - domain name, special groups such as NT SERVICE, Computer name or the server instance name (i.e. domain1\user2, NT SERVICE\MSSQLSERVER, machine45\user56)

SQL Server Database Role names stored as "database name\role name" (i.e. db1\public, db2\db_owner)

Business Resource Full Path conventions

Tree node types

Resource tree nodes are divided into 2 categories:

- A Real SQL Server object node
  such as a server instance, table, assembly, etc.
- A Virtual SQL Server node
  such as Tables, Databases, Security, etc.

Characters encoding

As each **real** object might contain special characters such as a period (.) or back-slash (\), the node name is wrapped in brackets '[' and ']'

Examples: [TABLE1], [VIEW1], [sp_help]

> **Note: Virtual node names are not wrapped in brackets, since the name of virtual nodes are fixed and defined by IdentityIQ File Access Manager**

Root node

Each resource full path starts with instance name [SERVER\INSTANCE NAME]

Components

- Virtual components starts with a colon (':')
  - [SERVER]:Databases
  - [SERVER]:Security:Users
- Real SQL Server objects start with a period, to separate it from other components
  - [Server].[DB1].[Schema2].[Table3]
  - [Server]:Security:Logins.[sa]

Chapter 3: Prerequisites

Software Requirements

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

Permissions

File Access Manager requires the following permissions on an SQL Server's login:

- GRANT CONNECT ANY DATABASE ON SERVER LEVEL
- GRANT VIEW ANY DEFINITION ON SERVER LEVEL (Which covers the permission: VIEW ANY DATABASE ON SERVER LEVEL)
- GRANT VIEW SERVER STATE ON SERVER LEVEL

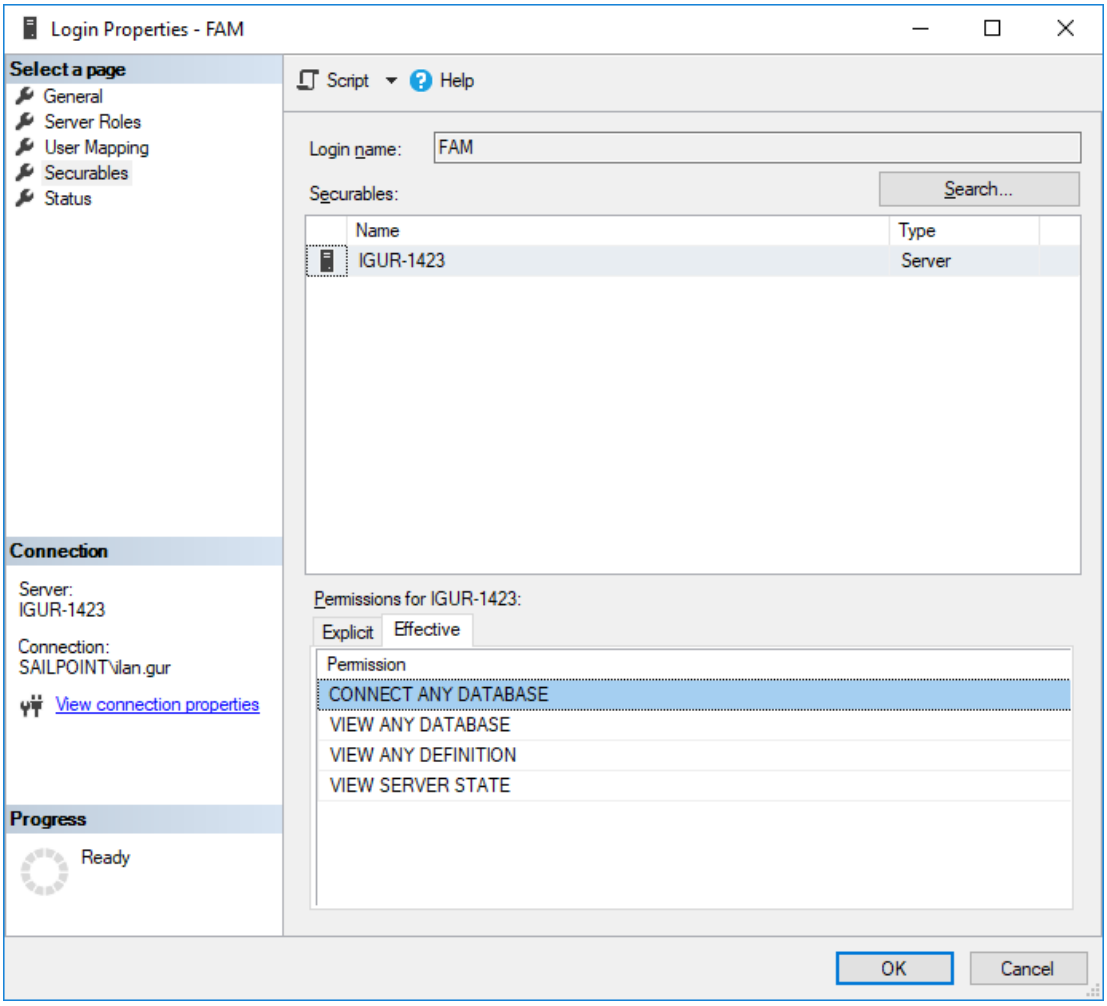

Figure 1. SQL Server permissions

Communications Requirements

Table 1. Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ File Access Manager Servers	8000-8008
Permissions Collection/ Activity Audit	Permissions Collector services/Activity Monitor	SQL Server Instance	As Configured in SQL Server Configuration Manager (usually TCP port 1433, Or port 0 to connect to SQL Server Browser)

Chapter 4: Add New Application Wizard

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

   The New Application Wizard window of the New Application Wizard displays under the Welcome tab

2. Select Standard Application
3. Select **SQL Server** from the Application Type dropdown menu
4. Click **Next**

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

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

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

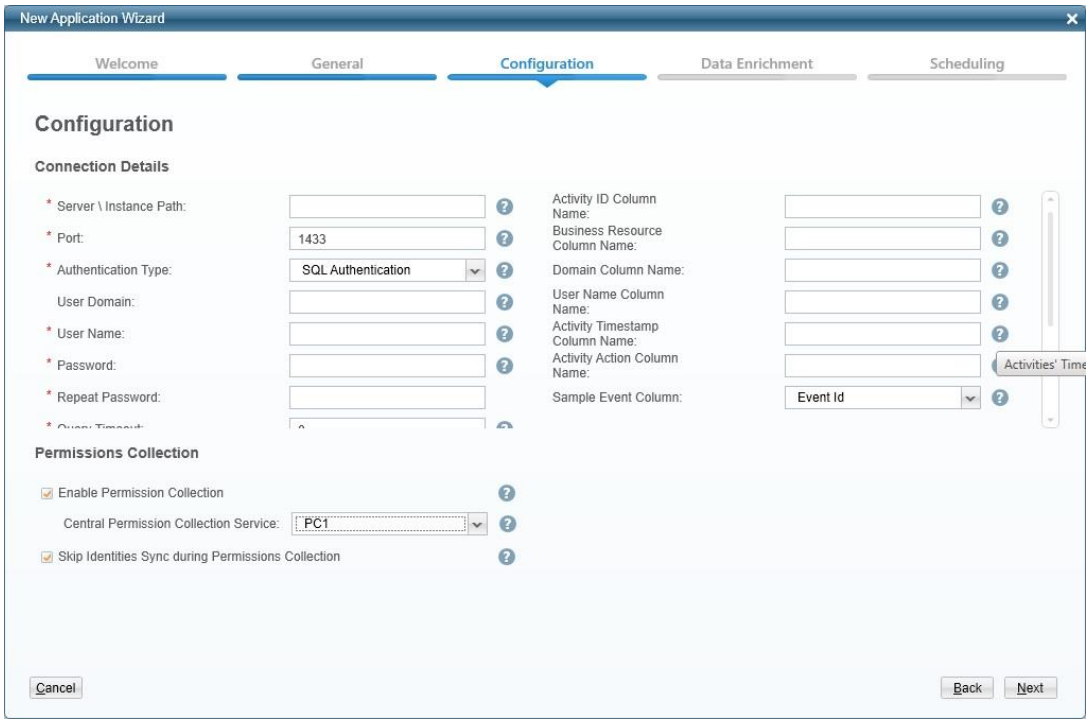

Figure 2. Configuration Window

10. Complete the Connection Details fields:

Server \ Instance Path

The name of the SQL Server Instance

Port

The port of the instance, or 0 - for SQL browser connectivity

Authentication Type

Choosing Windows authentication will use AD Credentials to re-authenticate for the given user/password. The default is not to use Windows authentication

User Domain

For Windows authentication only. For SQL Authentication this field should remain empty

User Name / password

Windows user name without domain, or SQL login for SQL authentication

Note: Do not use the format domain\username.

Activities Query

This query will periodically run to fetch new activities

Activity ID Column Name

The column name in the Activities Query which identifies the unique id of the activity. This column is used to query for new activities periodically

Business Resource Column Name

The column name in the Activities Query which will be displayed to the user as the Business Resource Full Path in the Activities Forensics

Domain Column Name

The column name in the Activities Query which will be displayed to the user as the Domain in the Activities Forensics – not mandatory

User Name Column Name

The column name in the Activities Query which will be displayed to the user as the User Name in the Activities Forensics

Activity Timestamp Column Name

The column name in the Activities Query which represents the time the activity occurred

Activity Action Column Name

The column name in the Activities Query which represents the action of the activity – not mandatory

Sample Event Column

Either by Event ID or by date

Note: The SQL Server connector will add a condition to fetch only new events for each query. This condition is created with the Sample Event Column.

Query Timeout

In minutes. The default timeout is 0, which means 'wait indefinitely'.

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

12. Click **Next** to open the Activity Monitoring configuration screen

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 and Crawler scheduling windows. You can navigate between these windows, using the Next and Back buttons.

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

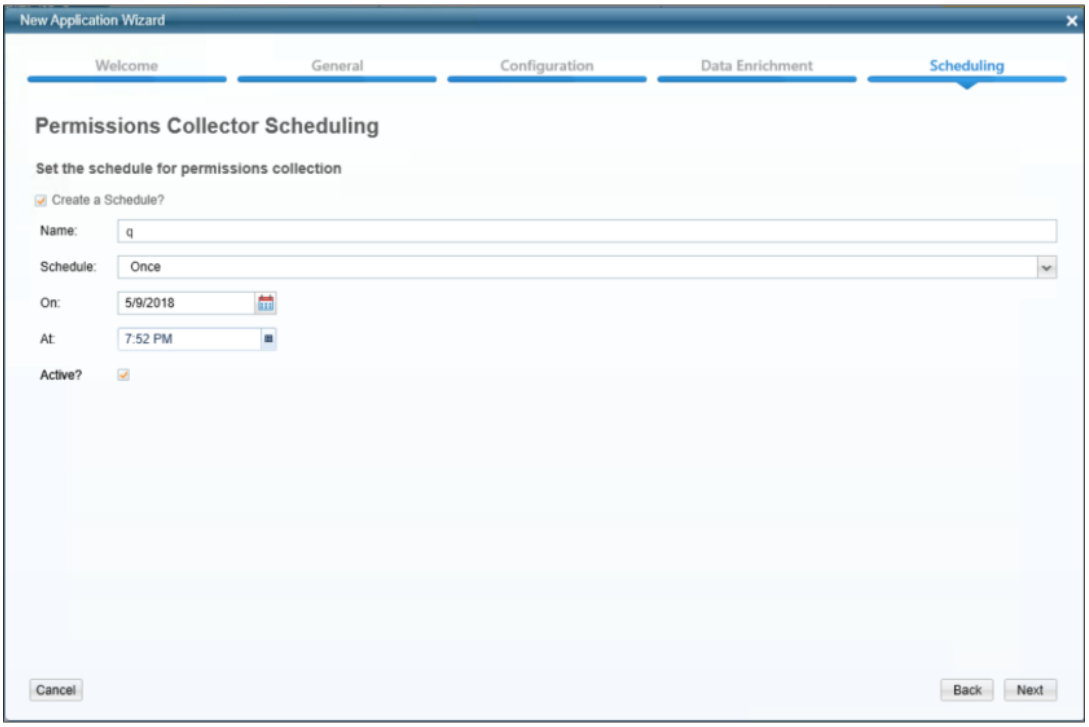

Figure 3. Permissions Collection Window

17. Check the **Create a Schedule** checkbox.
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.

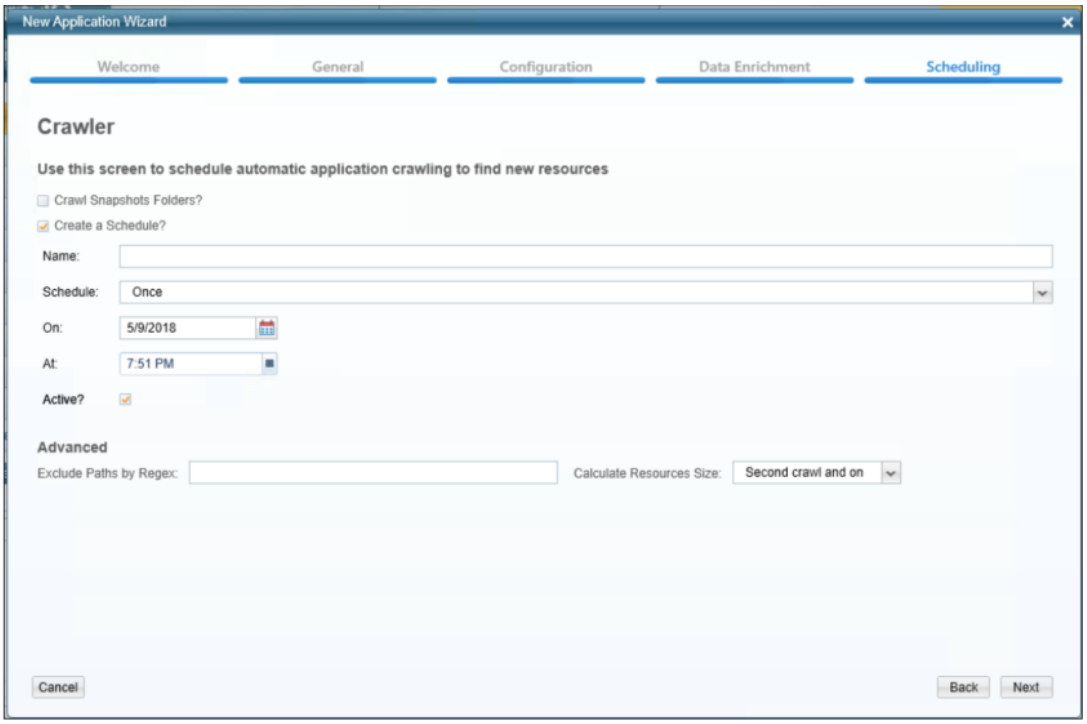

Figure 4. Crawler Window

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** checkbox 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 **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, user the format domain\username.

3. Click **Next**.

The Service Configuration window displays.

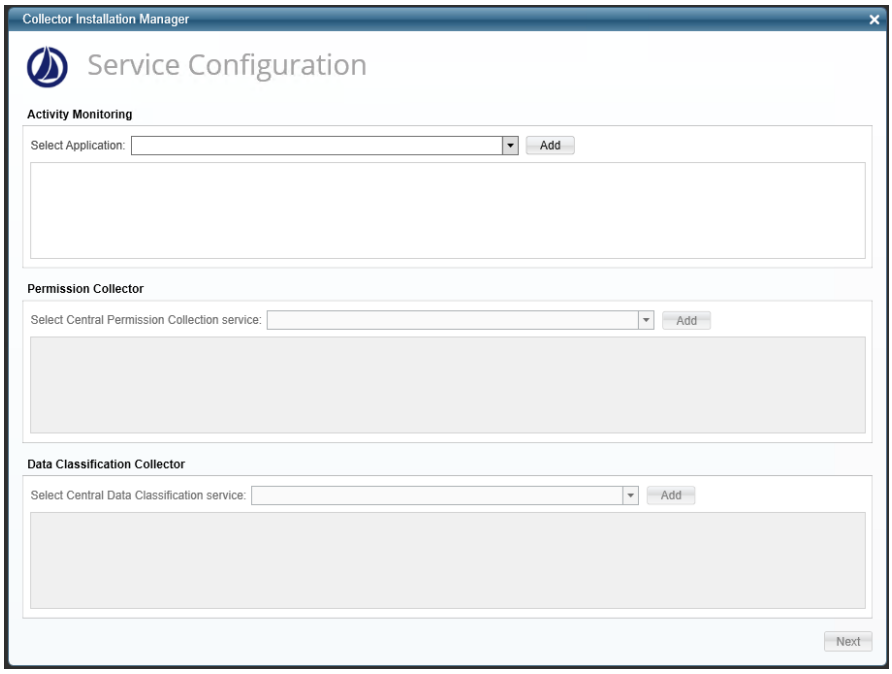

Figure 6. Service Configuration

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

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 Permission Collection - <Application Name> service is running.

Logs

- "%SAILPOINT_HOME_LOGS%\ PermissionsCollection_ <Central Permission Collection Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on SQL Server.
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 Web Client under

   Web Client **Forensics** > **Activities**

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.