



Integrating DropBox with File Access Manager

Version: 8.2 Revised: July 05, 2021

Copyright and Trademark Notices.

Copyright © 2021 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,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive 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.

Contents

Contents	ii
Capabilities	4
Connector Overview	5
Permissions Collector Operation Principles	5
Monitored Activities	5
Connector Installation Flow Overview	6
Collecting Data Stored in an External Application	7
Adding a DropBox Application	8
Select Wizard Type	8
General Details	8
Connection Details	8
Configuring and Scheduling the Permissions Collection	10
Scheduling a Task	10
Configuring and Scheduling the Crawler	11
Setting the Crawl Scope	12
Including and Excluding Paths by List	12
Excluding Paths by Regex	13
Crawler Regex Exclusion Examples	13
Exclude all shares which start with one or more shares names:	13
Include ONLY shares which start with one or more shares names:	13
Narrow down the selection:	14
Excluding Top Level Resources	14
Special Consideration for Long File Paths in Crawl	15
Selecting and Scheduling the Data Classification Settings	16
Configuring Activity Monitoring	17
Configuring Data Enrichment Connectors	17
Verifying the DropBox Connector Installation	18
Installed Services	18

Contents

Log Files	18
Monitored Activities	18
Permissions Collection	18

Capabilities

This connector enables you to use IdentityIQ File Access Manager to access and analyze data stored in DropBox and do the following:

- Analyze the structure of your stored data.
- Monitor user activity in the resources.
- Classify the data being stored.
- Verify user permissions on the resources, and compare them against requirements.

See the IdentityIQ File Access Manager documentation for a full description.

Connector Overview

- IdentityIQ File Access Manager Connector for Dropbox for Business uses the Dropbox Business API for event monitoring, identity, and permissions collection.
- The Dropbox Business and Core APIs uses the OAuth 2.0 authorization protocol to authenticate and authorize API requests.
- SecurityIQ for Dropbox Connector is a registered Dropbox App, which requires a short authorization process to use the Dropbox Business API during the definition of the Dropbox application.
- After the initial authorization process, IdentityIQ File Access Manager handles the OAuth token management automatically and refreshes the token if needed.

Permissions Collector Operation Principles

Dropbox Permissions Collector uses Dropbox Content API to retrieve collaboration and to share information.

IdentityIQ File Access Manager creates a Dropbox Identity Collector automatically at the end of the “Add New Application” wizard, which collects the Users and Groups from Dropbox.

Monitored Activities

Monitored events are as defined in the Dropbox Business API specification:

<https://www.dropbox.com/developers-v1/business/docs#log-get-events>

This published event list is not comprehensive. Due to Dropbox API being under migration to v2 – the documentation currently available on the website is incomplete. IdentityIQ File Access Manager supports all event types. Some events are excluded by default. To modify which event types are excluded, edit the *excludedEventTypes* value in the *WBX.DropboxBAMHost.dll.config* file.

Connector Installation Flow Overview

To install the DropBox connector:

1. Configure all the prerequisites.
2. Add a new DropBox application in the Business Website.
3. Install the relevant services:
 - Activity Monitor
 - Permissions Collector
 - Data Classification Collector

Installing the permissions collector and data classification services is optional and should only be installed by someone with a full understanding of IdentityIQ File Access Manager deployment architecture. The IdentityIQ File Access Manager Administrator Guide has additional information on the architecture.

Collecting Data Stored in an External Application

Connector / Collector terminology:

Connector

The collection of features, components and capabilities that comprise IdentityIQ File Access Manager support for an endpoint.

Collector

The “Agent” component or service in a Data Classification and or Permission Collection architecture.

Engine

The core service counterpart of this architecture.

Identity Collector

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your IdentityIQ File Access Manager installation. See the server Installation guide for further details.

Install a Data Classification central engine

One or more central engines, installed using the server installer

Install a Permission Collection central engine

One or more central engines, installed using the server installer

Create an Application in File Access Manager

From the Business Website. The application is linked to central engines listed above.

Add an Activity Monitor

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

Adding a DropBox Application

In order to integrate with DropBox, we must first create an application entry in IdentityIQ File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin > Applications*
2. Click **Add New** to open the wizard.

Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

General Details

Application Type

DropBox

Application Name

Logical name of the application

Description

Description of the application

Tags

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

Event Manager Server

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu

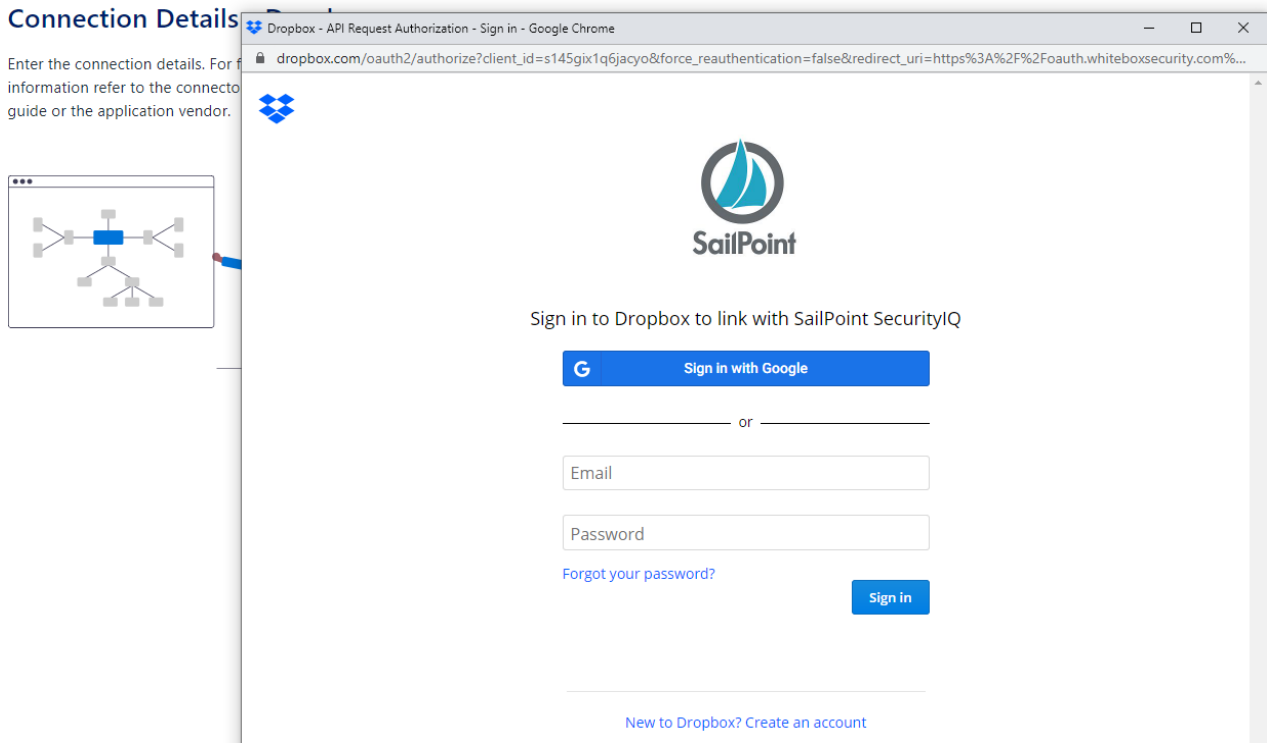
Click **Next**.

Connection Details

Complete the Connection Details fields:

Authorization Page

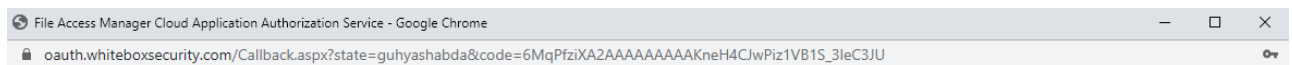
Press this link to open the DropBox Consent window shown below.



On the DropBox consent window, log in with a Team Admin user name.

You are redirected to the File Access Manager Cloud Application Authorization page with the authorization code.

This code has a timeout of about a minute, so copy the authorization code into the proper field in the application configuration page.



File Access Manager Cloud Application Authorization Service

Just one more step and you're all set

Please copy the following Authorization Code then paste it into the corresponding field in the Application Monitor Wizard within File Access Manager

6Gi5zf8mzoiA2iAzAdAAAagAihAlApAlolietne4CwQRPiGzB1S3IC3JUX|

Press Control+C to copy the code

Authorization Code

The result of the authorization process.

Click **Next**

Configuring and Scheduling the Permissions Collection


Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the “IdentityIQ FAM Central Permission Collector” wasn’t installed during the installation of the server, this configuration setting will be disabled.

To configure the Permission Collection

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

Central Permissions Collection Service

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section “Services Configuration” in the IdentityIQ File Access Manager Administrator Guide for further details.

Skip Identities Sync during Permission Collection

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connectors.

This option is unchecked by default.

Scheduling a Task

Create a Schedule

Click on this option to view the schedule setting parameters.

Schedule Task Name

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

Schedule

Select a scheduling frequency from the dropdown menu.

- **Schedule Types and Intervals**

Once

Single execution task runs.

Run After

Create dependency of tasks. The task starts running only upon successful completion of the first task.

Hourly

Set the start time.

Daily

Set the start date and time.

Weekly

Set the day(s) of the week on which to run.

Monthly

The start date defines the day of the month on which to run a task.

Quarterly

A monthly schedule with an interval of 3 months.

Half Yearly

A monthly schedule with an interval of 6 months.

Yearly

A monthly schedule with an interval of 12 months.

Date and time fields

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.


Active check box

Check this to activate the schedule.

Click **Next**.

Configuring and Scheduling the Crawler

To set or edit the Crawler configuration and scheduling

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

Calculate Resources' Size

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never
- Always
- Second crawl and on (This is the default)

Create a Schedule

Click to open the schedule panel. See [Scheduling a Task](#)


Setting the Crawl Scope

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

Including and Excluding Paths by List

To set the paths to include or exclude in the crawl process for an application

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type


1. Scroll down to the Crawl configuration settings.
2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
3. Click Include / Exclude Resources to open the input fields.

4. To add a resource to a list, type in the full path to include / exclude in the top field and click + to add it to the list.
5. To remove a resource from a list, find the resource from the list, and click the x icon on the resource row.

When creating exclusion lists, excludes take precedence over includes.

Excluding Paths by Regex

To set filters of paths to exclude in the crawl process for an application using regex

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions. See the example below in section [Business Resource Structure](#) to better understand the business resource full path structure.

Crawler Regex Exclusion Examples

The following are examples of crawler Regex exclusions:

Exclude all shares which start with one or more shares names:

Starting with `\\server_name\shareName`

Regex: `\\\\server_name\\shareName$`

Starting with `\\server_name\shareName` or `\\server_name\OtherShareName`

Regex: `\\\\server_name\\(shareName|OtherShareName)$`

Include ONLY shares which start with one or more shares names:

Starting with `\\server_name\shareName`

Regex: `^(?!\\\\server_name\\shareName($|\\.*)) .*`

Starting with `\\server_name\shareName` or `\\server_name\OtherShareName`

Regex: `^(?!\\\\server_name\\(shareName|OtherShareName)($|\\.*)) .*`

Narrow down the selection:

Include **ONLY** the C\$ drive shares: \\server_name\C\$

Regex: `^(?!\\\\\\\\server_name\\\\C\$(\$|\\\\.*)) .*`

Include **ONLY** one folder under a share: \\server\share\folderA

Regex: `^(?!\\\\\\\\server_name\\\\share\$(\$|\\\\folderA$|\\\\folderA\\\\.*)) .*`

Include **ONLY** all administrative shares

Regex: `^(?!\\\\\\\\server_name\\\\[a-zA-Z]\$(\$|)).*`

To write a backslash or a Dollar sign, add a backslash before it as an escape character.

To add a condition in a single command, use a pipe character “|”.

Excluding Top Level Resources

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

To exclude top level resources from the crawl process

1. Open the application screen

Admin > Applications

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. **Run Task**

The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

Before running the task for the first time, the message above this button is:

"Note: Run task to detect the top-level resources"

If the top level resource list has changed in the application while you are on this screen, press this button to retrieve the updated structure.

Once triggered, you can see the task status in

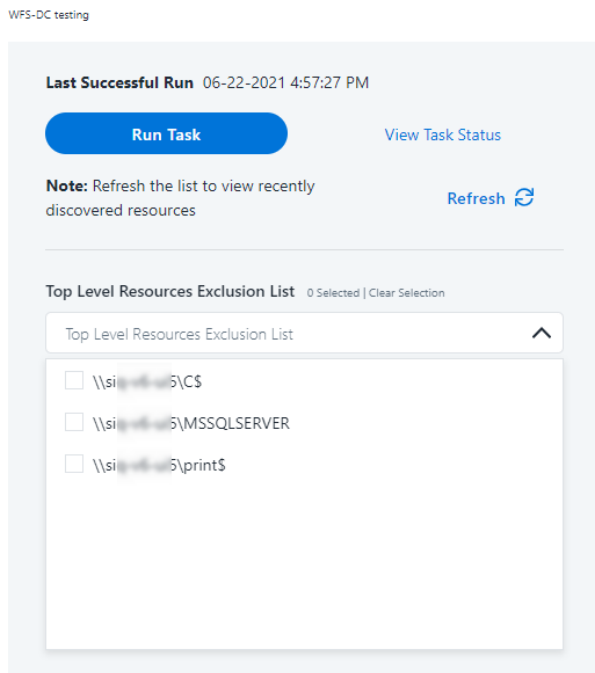
Settings > Task Management > Tasks

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

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

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

Top Level Resources Exclusion



Special Consideration for Long File Paths in Crawl

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

`excludeVeryLongResourcePaths`

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

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

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

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

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

Background

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

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

Identifying the Problem

When using an SQL Server database version 2014 and earlier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

Setting the Long Resource Path Key


The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

`%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\`

Search for the key **excludeVeryLongResourcePaths** and correct it as described above.

Selecting and Scheduling the Data Classification Settings

To associate an application with a data classification service, and set the schedule

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Data Classification** settings page.

The actual entry fields vary according to the application type

Central Data Classification Service

Associate the application with a Central Data Classification Service. This service is responsible for running the Data Classification tasks.

If the “Central Data Classification” wasn’t installed during the installation of the server, this field is disabled.

Disabling Data Classification

To disable data classification, delete the entry from the central data classification field.

Disabling data classification can also be achieved by setting the scheduler to be inactive (which is the default setting for data classification).

Create a Schedule

This option is enabled only if a central data classification service is selected.

See [Scheduling a Task](#)

See the chapter “Data Classification” in the IdentityIQ File Access Manager Administrator Guide for more information

Click **Next** or **Finish**.

Configuring Activity Monitoring

Configure the activity monitoring process frequency.

Polling Interval (sec)

Activity fetching interval [in seconds]. Default is set to 60 seconds,

Report Interval (sec)

Activity Monitor Health reporting interval [in seconds]. Default is set to 60 seconds.

Local Buffer Size (MB)

Local buffer size for activities [in MB]). Default is set to 200MB.

This cyclic buffer is used to store activities on the Application Monitor’s machine in case of network errors that prevent the activities from being sent.

Configuring Data Enrichment Connectors

The Data Enrichment Connectors (DEC) configuration enables us to select data enrichment sources. These can be used to add information from other sources about identities.

An enrichment source could be a local HR database that is used to combine users' job descriptions or departments to the information stored in the identity store.

Select the data enrichment connectors to enrich monitored activities from the Available DEC’s text box.

Use the > or >> arrows to move the selected DEC’s to the Current DEC’s text box.

The user can select multiple DEC’s. Simply select each desired DEC.

You can create a new DEC in the Administrative Client (*Applications > Configuration > Activity Monitoring > Data Enrichment Connectors*). After creating a new DEC, Click **Refresh** to refresh the dropdown list.

The chapter **Connectors** of the IdentityIQ File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

Verifying the DropBox Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the IdentityIQ File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Activity Monitor - <Application_Name>
- File Access Manager Central Permissions Collection - <Application_Name>
- File Access Manager Central Data Classification - <Application_Name>
- File Access Manager Watchdog- -<Application_Name>

Log Files

Check the log files listed below for errors

- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\DROPBOX-<Application_Name>.log"

Monitored Activities

1. Simulate activities on DropBox.
2. Wait a minute (approximately).
3. Verify that the activities display in the IdentityIQ File Access Manager website under
Forensics > Activities

Permissions Collection

1. Run the Crawler and Permissions Collector tasks (*Settings > Task Management > Scheduled Tasks*)
2. Verify that:
 - The tasks completed successfully
 - Business resources were created in the resource explorer (*Admin > Applications > [application column] > Manage Resources*)
 - Permissions display in the Permission Forensics page (*Forensics > Permissions*)