SecurityIQ Dropbox for Business Connector Installation Guide

SecurityIQ Version: 6.0

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.

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. Government's Specially Designated Nationals (SDN) List; 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.

Copyright and Trademark Notices.

“SailPoint Technologies & Design,” “IdentityIQ,” “IdentityNow,” “AccessIQ,” “Identity Cube,” and “Managing the Business of Identity” are registered trademarks of SailPoint Technologies, Inc. “SecurityIQ,” “SailPoint” and the SailPoint logo are 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.

Table of Contents

1. Connector Installation & Configuration 1
   - 1.1. Overview 1
2. General 2
   - 2.1. Connector Operation Principles 2
   - 2.2. Monitored Activities 2
   - 2.3. Permissions Collector Operation Principles 2
3. Prerequisites 3
   - 3.1. Software Requirements 3
   - 3.2. Permissions 3
   - 3.3. Communications Requirements 3
4. Add New Application Wizard 4
5. Installation of Services 13
   - 5.1. Collector Installation 13
6. Verification 16
   - 6.1. Services 16
   - 6.2. Connectors Services 16
   - 6.3. Logs 16
   - 6.4. Monitored Activities 16
   - 6.5. Permissions Collection 16

List of Figures

Figure 1. Welcome Window 4
Figure 2. General Details Window 5
Figure 3. Configuration Window 6
Figure 4. OAuth Dropbox Consent Window 7
Figure 5. OAuth Cloud Application Authorization Service Window 7
Figure 6. Configuration Wizard 8
Figure 7. Data Enrichment Connectors Window 9
Figure 8. Permissions Collection Window 10
Figure 9. Crawler Window 11
Figure 10. Data Classification Window 12
Figure 11. SecurityIQ Collector Installation Manager 13
Figure 12. Service Configuration 14
Figure 13. Installation Folder 15

List of Tables

Table 1. Communications Requirements 3

Table of Revisions

Ver. #	Description	Author	Date
5.0	Final Version	Jonathan Rappeport	10 January 2017
5.1	First Draft	Jonathan Rappeport	08 February 2017
5.1	Second Draft	Jonathan Rappeport	13 June 2017
5.1	Third Draft	Jonathan Rappeport	26 September 2017
6.0	First Draft	Jonathan Rappeport	10 May 2018

1. CONNECTOR INSTALLATION & CONFIGURATION

1.1. Overview

1.1.1. Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the SecurityIQ Administrative 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 SecurityIQ deployment architecture. The SecurityIQ Administrator Guide has additional information on SecurityIQ architecture.

2. GENERAL

2.1. Connector Operation Principles

- SecurityIQ 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, SecurityIQ handles the OAuth token management automatically and refreshes the token if needed.

2.2. Monitored Activities

Monitored events are as defined in the Dropbox Business API specification: https://www.dropbox.com/developers-v1/business/docs#log-get-events

Note: 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. SecurityIQ supports much more event types than officially listed, including generic support for new (unrecognized) event types.

2.3. Permissions Collector Operation Principles

- SecurityIQ Dropbox Permissions Collector uses Dropbox Content API to retrieve collaboration and to share information.
- SecurityIQ creates a Dropbox Identity Collector automatically at the end of the “Add New Application” wizard, which collects the Users and Groups from Dropbox.

3. PREREQUISITES

3.1. Software Requirements

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

3.2. Permissions

- During the OAuth authorization process, a Dropbox for Business Team Admin user must grant the SailPoint SecurityIQ Dropbox Application access to the data on Dropbox.

3.3. Communications Requirements

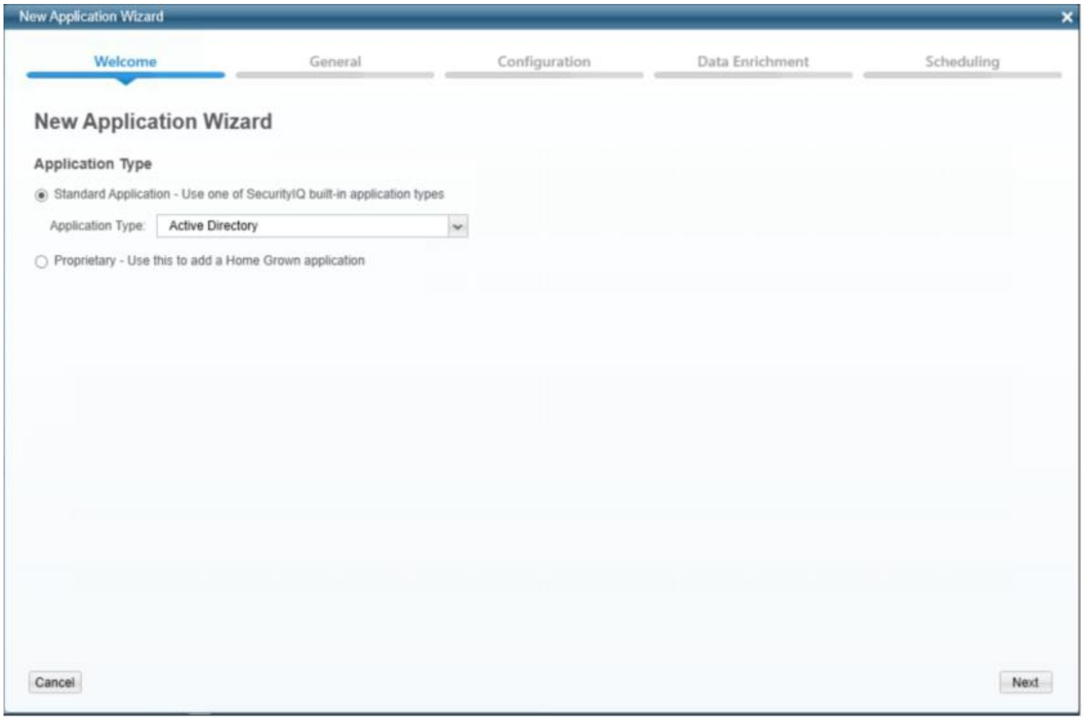
Table 1. Communications Requirements

Requirement	Source	Destination	Port
SecurityIQ Database Access	Permissions Collector/Data Classification	SecurityIQ DB	According to specific DB definitions
SecurityIQ Access	Activity Monitor	SecurityIQ Servers	8000-8008
Permissions Collection/Data Classification	Permissions Collector/Data Classification	Dropbox API	https
Activity Monitoring	Activity Monitor	Dropbox API	https

4. Add New Application Wizard

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

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



New Application Wizard

Application Type

● Standard Application - Use one of SecurityIQ built-in application types

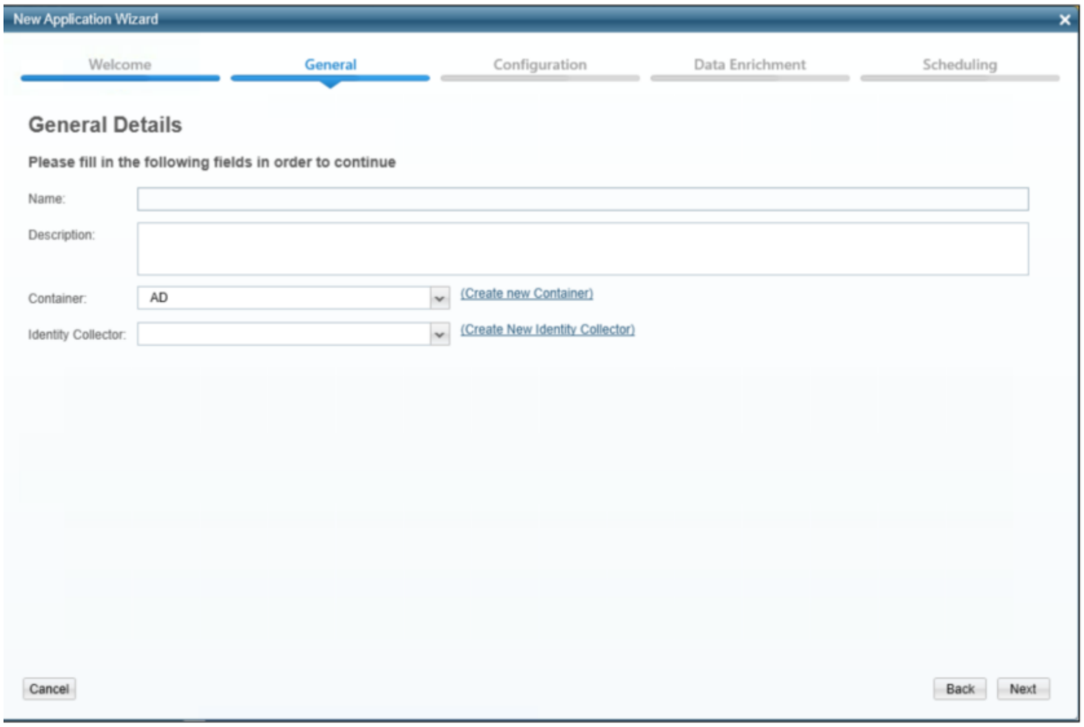
Application Type: Active Directory

○ Proprietary - Use this to add a Home Grown application

Figure 1. Welcome Window

3. Select Standard Application.
4. Select **Dropbox** from the **Application Type** dropdown menu.
5. Click **Next**.

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



New Application Wizard

General Details

Please fill in the following fields in order to continue

Name:

Description:

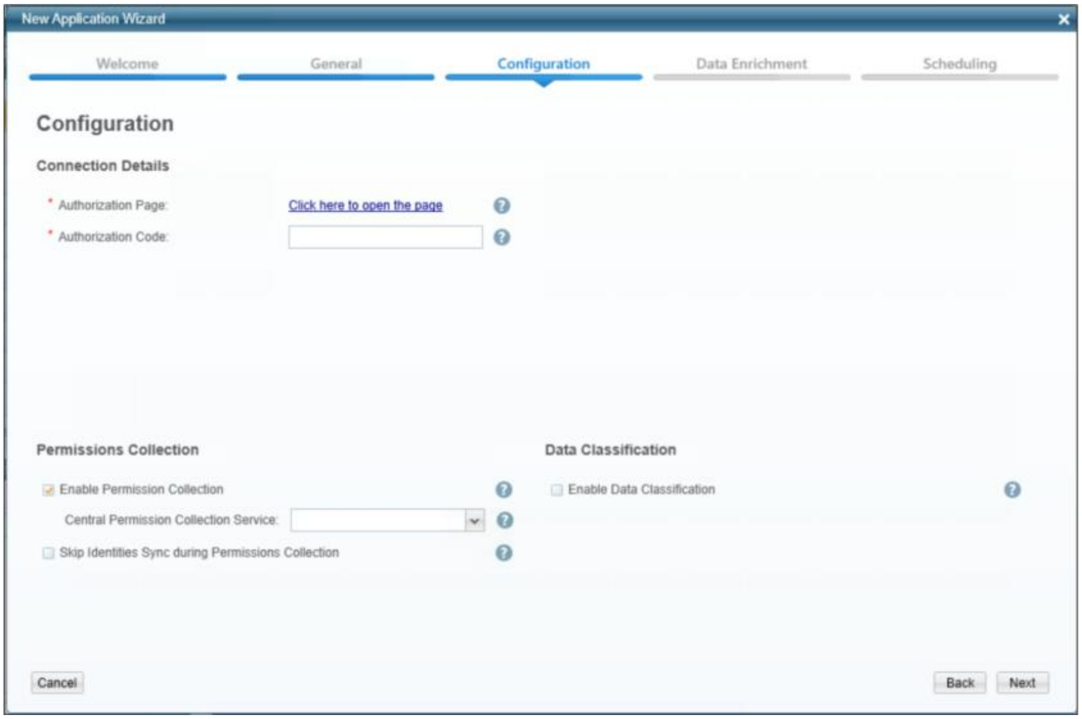
Container: AD

Identity Collector:

Figure 2. General Details Window

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 Monitor Configuration window of the New Application Wizard displays under the Configuration tab.



Configuration

Connection Details

* Authorization Page: Click here to open the page

* Authorization Code:

Permissions Collection

☑ Enable Permission Collection

Central Permission Collection Service:

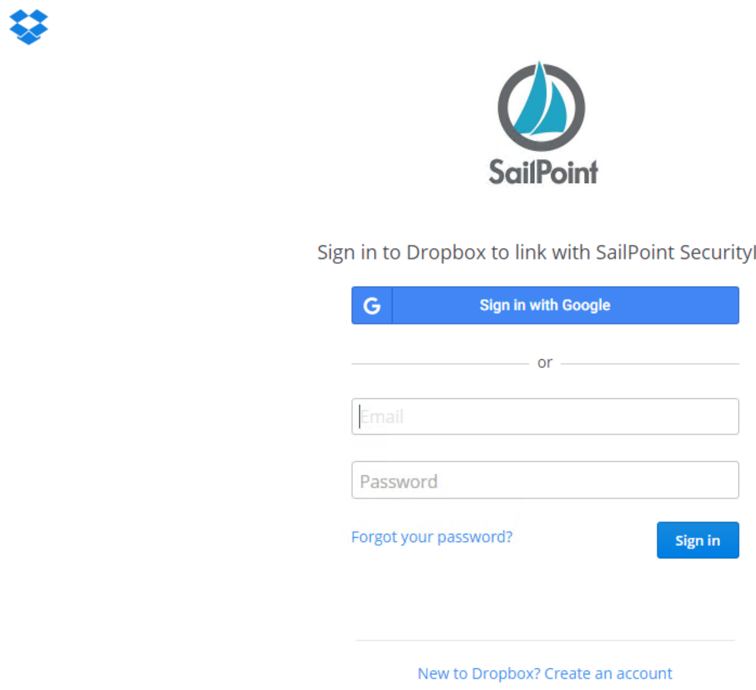
□ Skip Identities Sync during Permissions Collection

Data Classification

□ Enable Data Classification

Figure 3. Configuration Window

10. Complete the Connection Details fields:
    - *Authorization Page* (When selected, the Dropbox Consent window displays.)
    - *Authorization Code* (This is a result of the OAuth authorization process.)



SailPoint

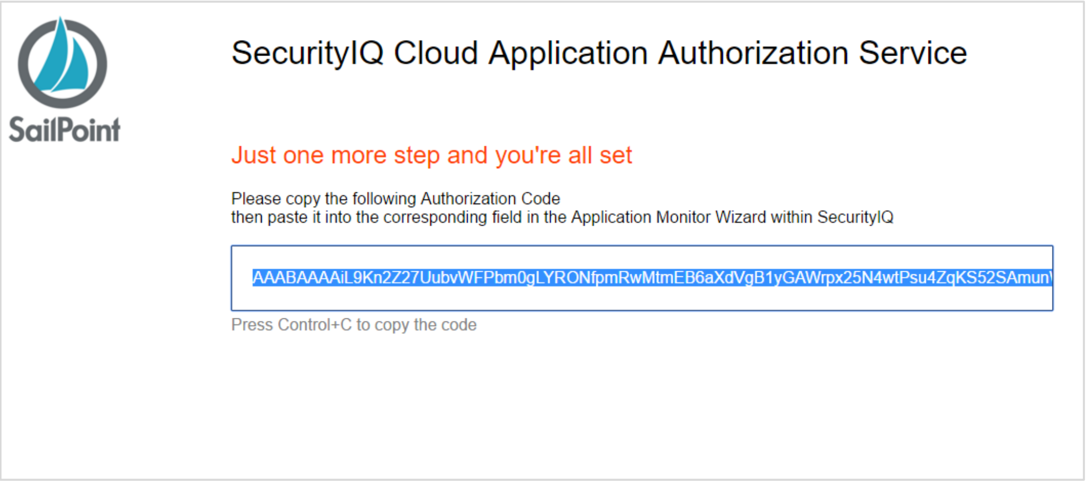
Sign in to Dropbox to link with SailPoint SecurityIQ

Figure 4. OAuth Dropbox Consent Window

11. Log in with a Team Admin user name.

    You are redirected to the SecurityIQ Cloud Authorization Website.

Note: If the authentication process was successful, the system displays an authorization code.



SailPoint

SecurityIQ 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 SecurityIQ

AAABAAAAiL9Kn2Z27UubvWFPbm0gLYRONfpmRwMtmEB6aXdVgB1yGAWrpx25N4wtPsu4ZqKS52SAmun

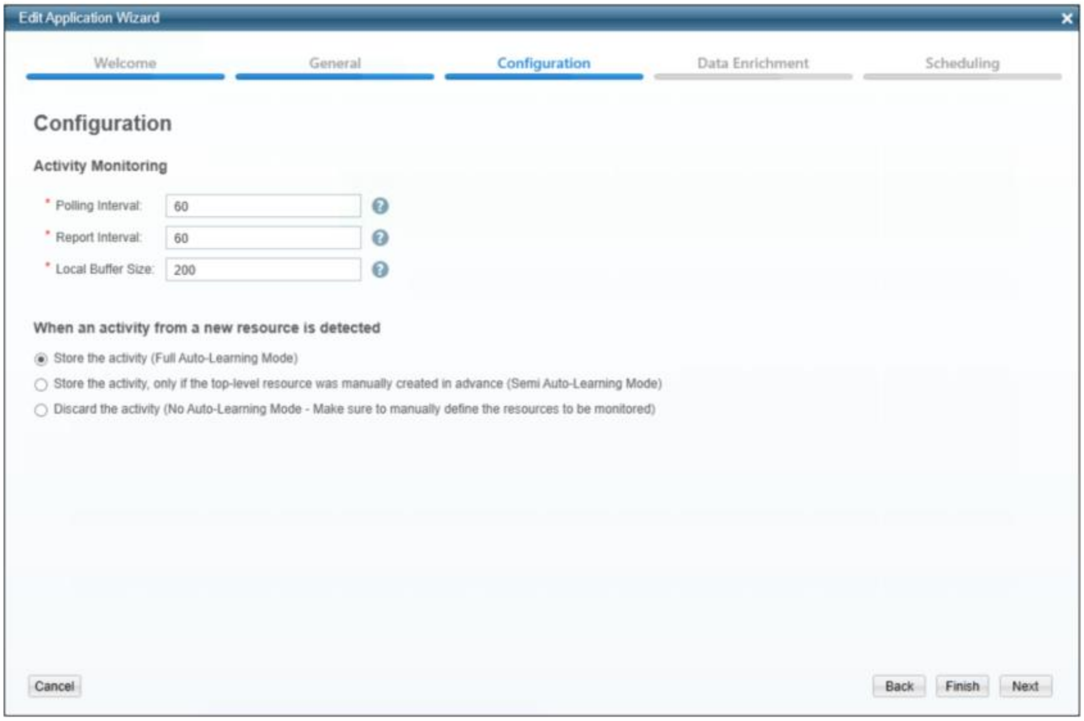
Press Control+C to copy the code

Figure 5. OAuth Cloud Application Authorization Service Window

12. Copy the resulting authorization code to the *Authorization Code Configuration* field.

13. Revert to the Configuration window.

14. Click to enable Permission Collection 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.)
15. Click to enable Data Classification and select a central data classification service from the list
16. Click **Next**.



Configuration

Activity Monitoring

* Polling Interval: 60

* Report Interval: 60

* Local Buffer Size: 200

When an activity from a new resource is detected

● Store the activity (Full Auto-Learning Mode)

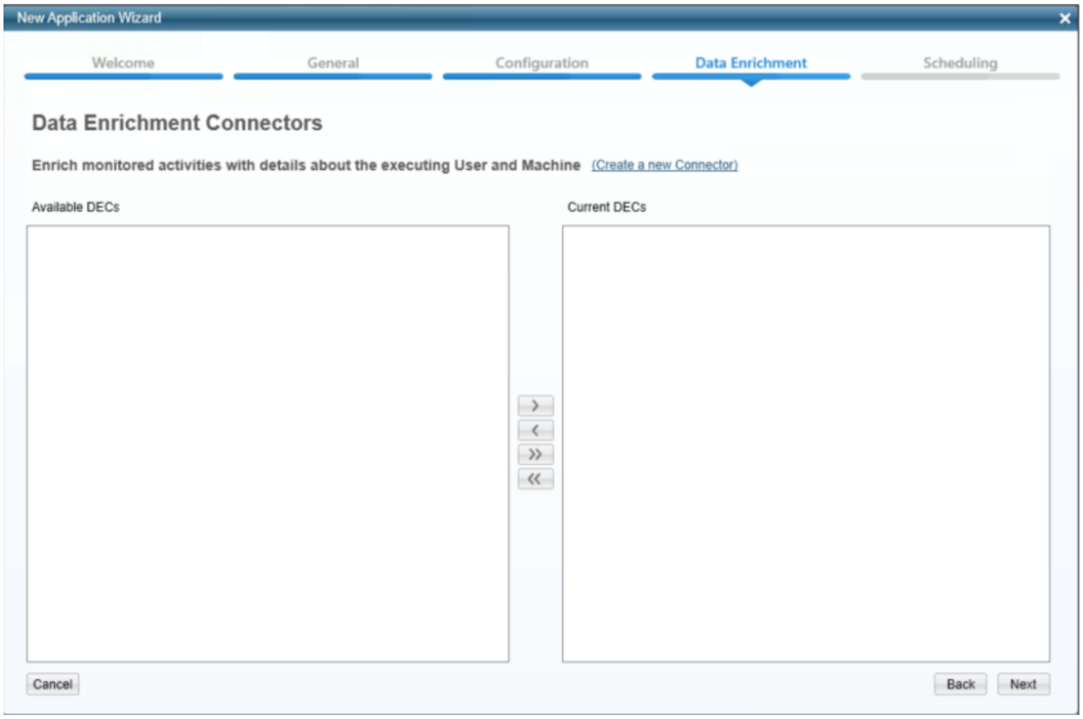
○ Store the activity, only if the top-level resource was manually created in advance (Semi Auto-Learning Mode)

○ Discard the activity (No Auto-Learning Mode - Make sure to manually define the resources to be monitored)

Figure 6. Configuration Wizard

17. Fill in the Connection Details with an Authorization Code.
18. Under Permission Collection, check the “Enable Permission Collection” checkbox if appropriate.
19. Under Data Classification, check the “Enable Data Classification” checkbox if appropriate.
20. Click **Next**.

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



Data Enrichment Connectors

Enrich monitored activities with details about the executing User and Machine (Create a new Connector)

Figure 7. Data Enrichment Connectors Window

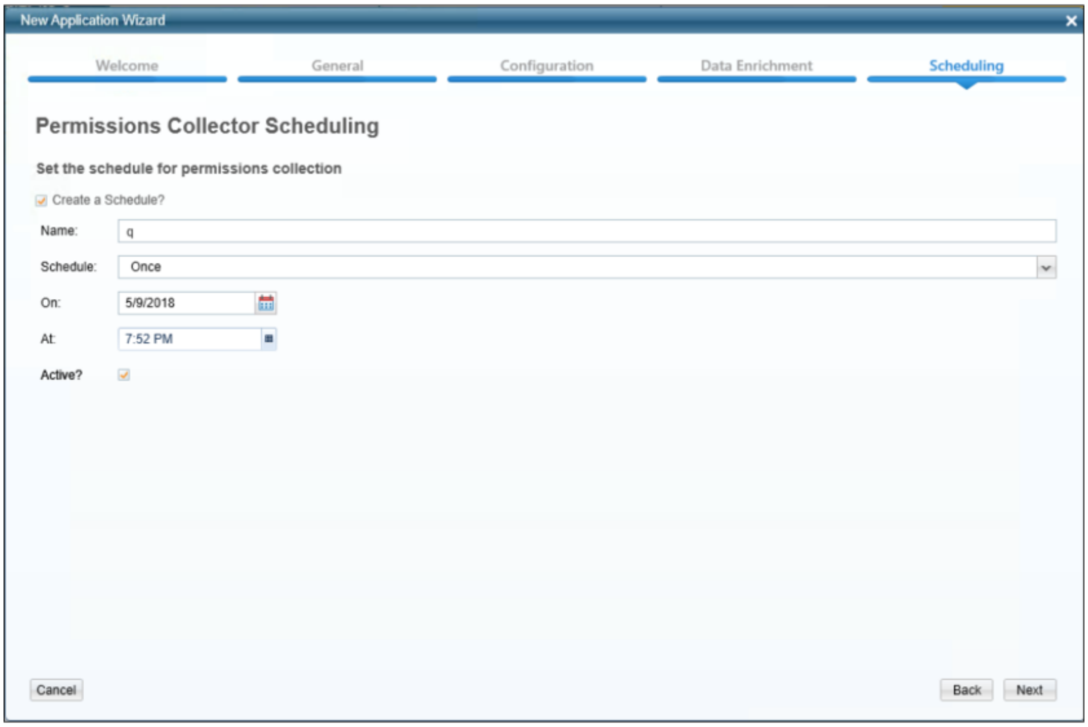
21. Select the data enrichment connectors (DECs) to enrich monitored activities from the Available DECs text box, and use the > or >> arrows to move them to the Current DECs text box.

Note: Chapter 6 of the SecurityIQ Administrative Client User Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

22. 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.



Permissions Collector Scheduling

Set the schedule for permissions collection

☑ Create a Schedule?

Name: q

Schedule: Once

On: 5/9/2018

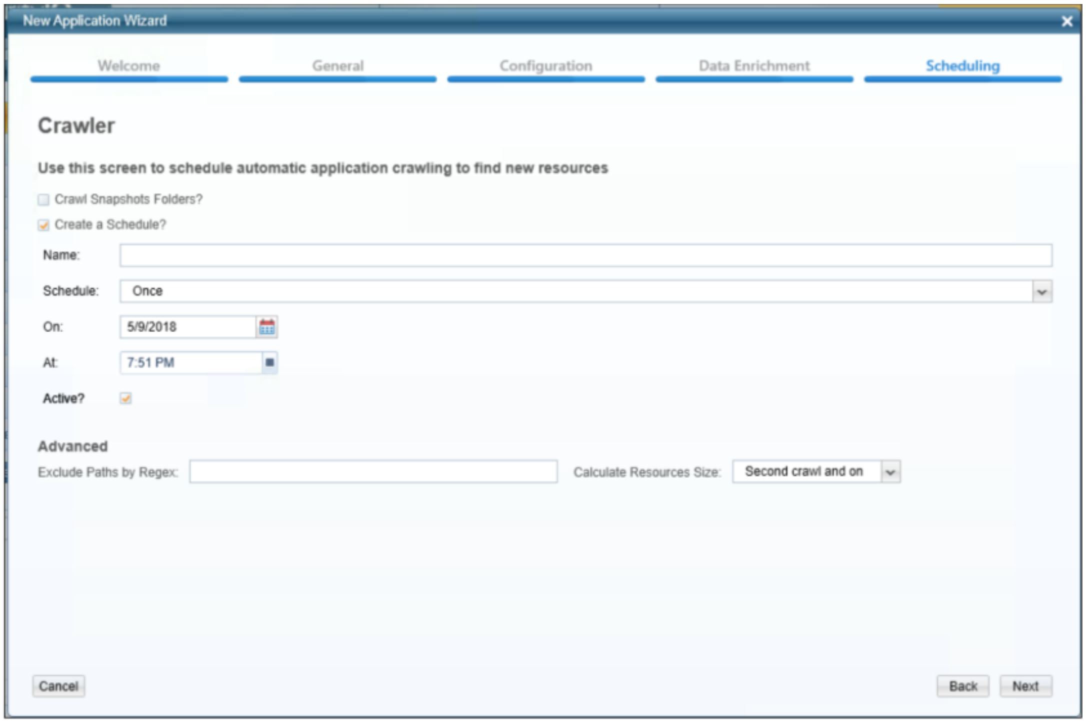
At: 7:52 PM

Active? ☑

Figure 8. Permissions Collection Window

23. Check the **Create a Schedule** check box.
24. Type a name for the permissions collection 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. Click **Next**.

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



Crawler

Use this screen to schedule automatic application crawling to find new resources

☐ Crawl Snapshots Folders?

☑ Create a Schedule?

Name:

Schedule: Once

On: 5/9/2018

At: 7:51 PM

Active? ☑

Advanced

Exclude Paths by Regex:

Calculate Resources Size: Second crawl and on

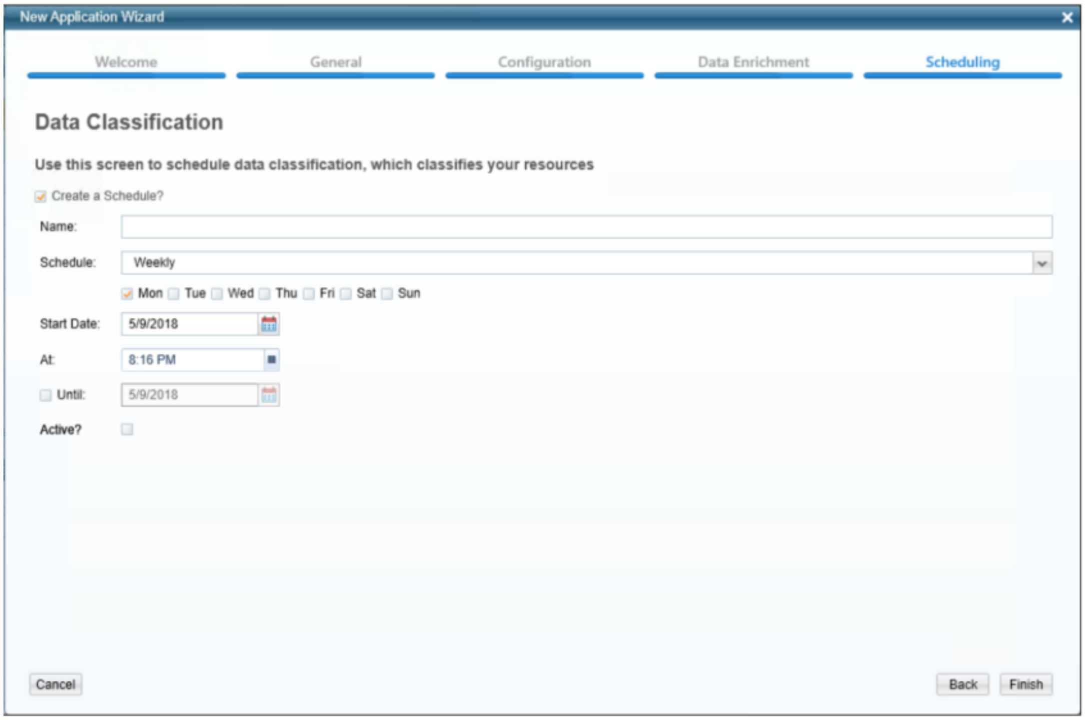
Figure 9. Crawler Window

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

Note: Chapter 7 of the SecurityIQ Administrative Client User Guide provides more information on the Crawling Process.

35. Click **Next**.

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



Data Classification

Use this screen to schedule data classification, which classifies your resources

☑ Create a Schedule?

Name:

Schedule: Weekly

☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Start Date: 5/9/2018

At: 8:16 PM

□ Until: 5/9/2018

Active? □

Figure 10. Data Classification Window

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

Note: Chapter 9 of the SecurityIQ Administrative Client User Guide provides more information on Data Classification.

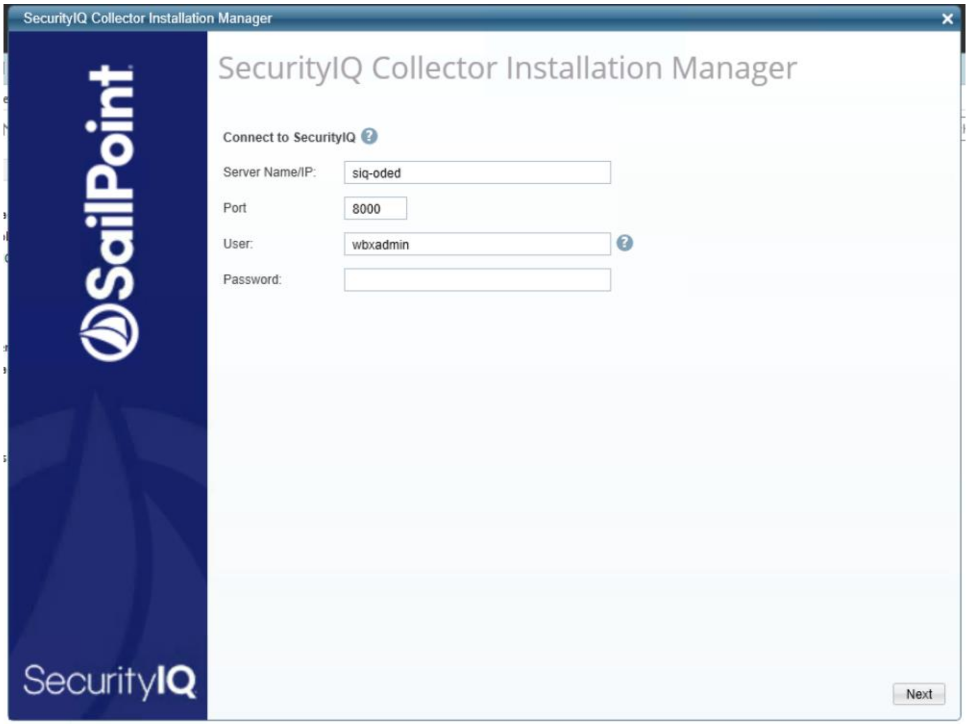
41. Click **Finish**.

5. Installation of Services

5.1. Collector Installation

1. Run the "SecurityIQ Agent Manager" as an Administrator.
   The installation files are located in the installation package under 'Connectors\ SecurityIQ Collector Manager.exe'.

   The SecurityIQ Collector Installation Manager window displays.



SecurityIQ Collector Installation Manager

Connect to SecurityIQ

Server Name/IP: siq-oded

Port 8000

User: wbxadmin

Password:

Figure 11. SecurityIQ Collector Installation Manager

2. Enter the credentials to connect to the SecurityIQ database. The User should be the same as the one used to log in to the Administrative Client.
3. Click **Next**.

The Service Configuration window displays.

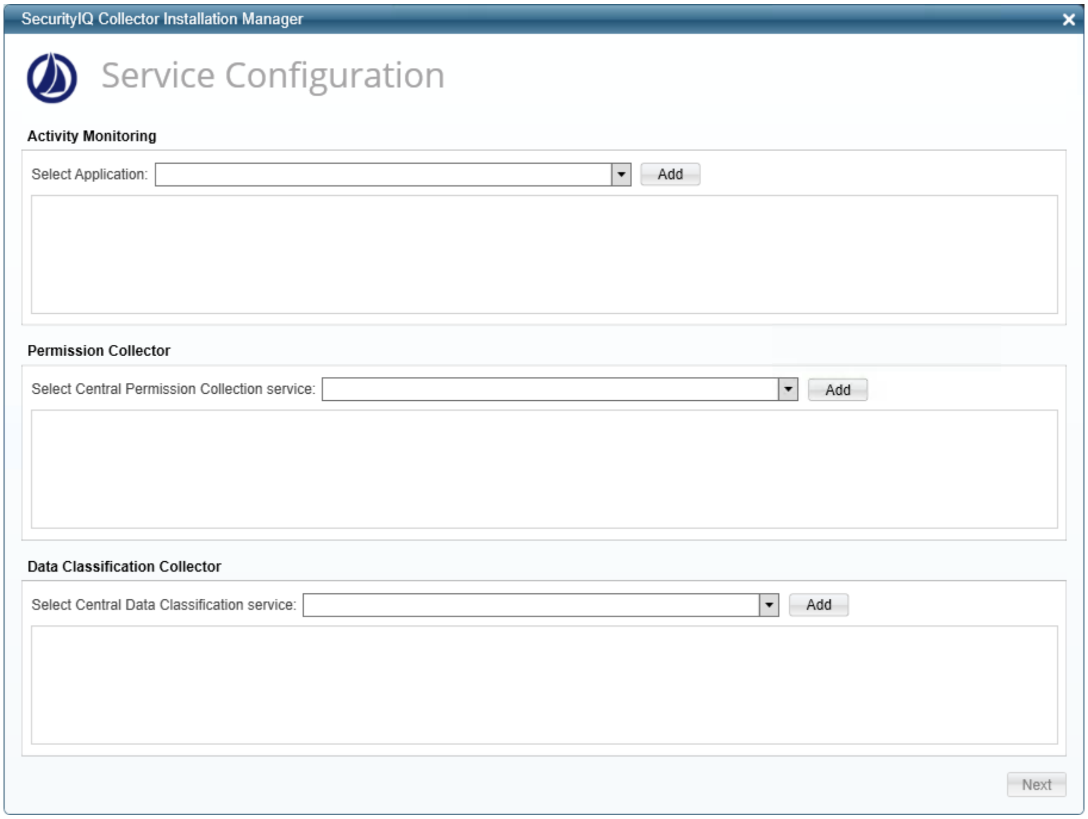

SecurityIQ Collector Installation Manager
Service Configuration
Activity Monitoring
Select Application:
Add
Permission Collector
Select Central Permission Collection service:
Add
Data Classification Collector
Select Central Data Classification service:
Add
Next

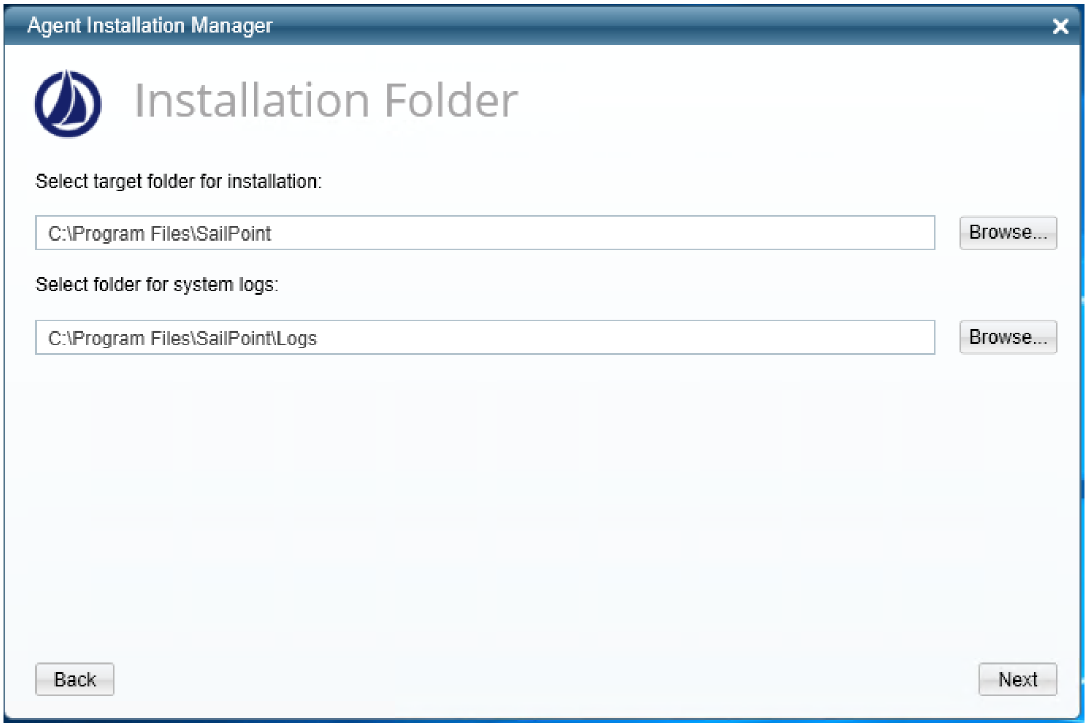
Figure 12. Service Configuration

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**.

Note: The SecurityIQ Administrator Guide has additional information on SecurityIQ architecture, which is important to review before installing the Permission Collector.

7. Click **Next**.

The Installation Folder window displays.


Agent Installation Manager

Installation Folder

Select target folder for installation:

C:\Program Files\SailPoint

Select folder for system logs:

C:\Program Files\SailPoint\Logs

Figure 13. Installation Folder

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**.

    The system begins installing the selected components.
11. Click **Finish** (which displays after all of the selected components have been installed).

Note: The SecurityIQ Administrative Client User Guide provides more information on Permissions Collection.

6. VERIFICATION

6.1. Services

6.2. Connectors Services

- **SecurityIQ Activity Monitor—**<Application_Name> service is running.
- **SecurityIQ Permissions Collection—**<Application_Name> service is running.
- **SecurityIQ Data Classification**—<Application_Name> service is running.
- **SecurityIQ Watchdog**—<Application_Name> service is running.

6.3. Logs

- “%SIQ_HOME_LOGS%\DROPBOX - <Application_Name>.log" does not contain errors.
- “%SIQ_HOME_LOGS%\RoleAnalytics-<Application_Name>.log" does not contain errors.
- “%SIQ_HOME_LOGS%\DataClassification-<Application_Name>.log" does not contain errors.
- “%SIQ_HOME_LOGS%\Watchdog-<Application_Name>.log" does not contain errors.

6.4. Monitored Activities

1. Simulate activities on the Dropbox for Business.
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.

6.5. Permissions Collection

1. Run the Crawler and Permissions Collector tasks in the SecurityIQ Administrative Client.
2. Verify that:
   - The tasks completed successfully.
   - Business resources were created on the BRs tree.
   - Permissions display in the Permissions Forensics window.