SecurityIQ One Drive for Business (Office 365) Connector Installation Guide

SecurityIQ Version: 6.0

Table of Contents

List of Figures

List of Tables

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 of the prerequisites.
2. Add a new application to the SecurityIQ Administrative Client.
3. Install the Activity Monitor or Data Classification Collector.
4. Do no install Permissions Collectors. OneDrive currently does not support the Cloud-Ready architecture for Permissions Collection. A Permissions Collection task will always run on the Central Permissions Collector service associated with the Application regardless of the number of Collectors associated with the Central Permissions Collector service.

Note: Permission Collector and Data Classification Collector 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. Activity Monitor Operation Principles

- SecurityIQ Activity Monitor for OneDrive uses the Microsoft Office365 Management Activity API.
- The Activity Monitor queries the API for OneDrive events.
- The Microsoft Office365 Management Activity API uses the OAuth 2.0 authorization protocol to authenticate and authorize API requests.
- Use of the API, SecurityIQ for OneDrive Connector requires a short authorization process during the definition of the OneDrive for Business application.
- After the initial authorization process, SecurityIQ will handle OAuth token management automatically and refresh the token if needed.

Note: It might take up to two hours for events to be received by the SecurityIQ for OneDrive Activity Monitor (a current Microsoft limitation).

2.2. Monitored Activities

Monitored events and activities are as defined in the Office365 Management Activity API specification: https://msdn.microsoft.com/en-us/library/office/mt607130.aspx#SharePointAuditOperations

2.3. Permissions Collector Operation Principles

- SecurityIQ OneDrive for Business permissions collection uses the Microsoft OneDrive REST API.
- The permissions collector queries OneDrive for Business for the existing Role Assignments to determine object permissions.
- An Azure Identity Collector must be configured to map the permissions to users and groups from the Azure Active Directory.

Note: Chapter 8 of the Administrative Client User Guide provides more information on how to define an Azure Identity Collector.

3. PREREQUISITES

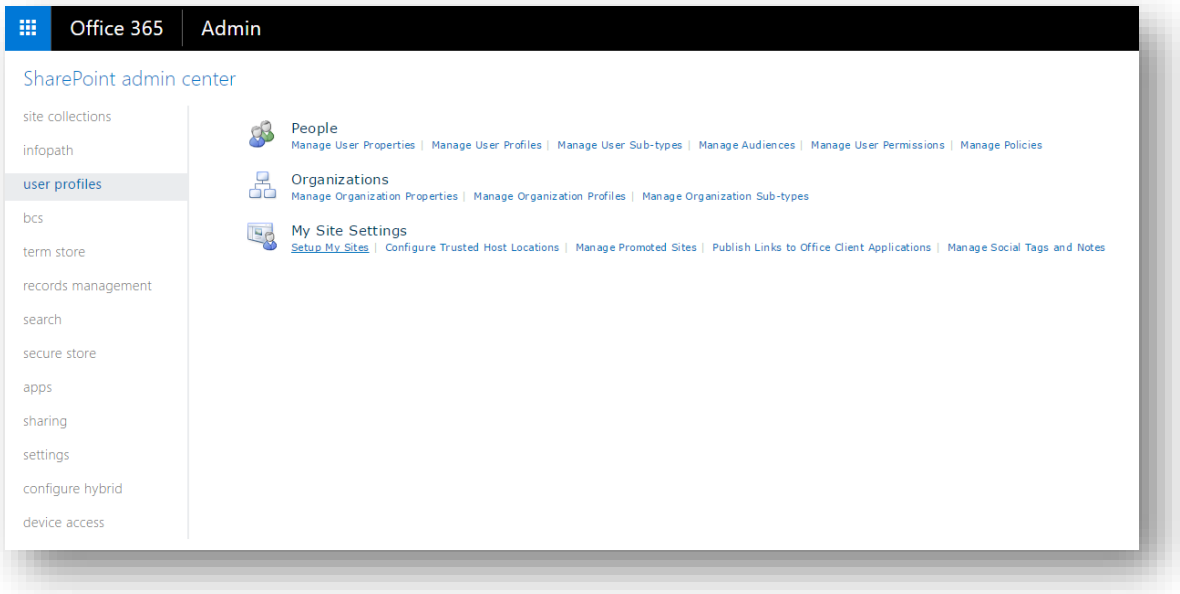
3.1. Software Requirements

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

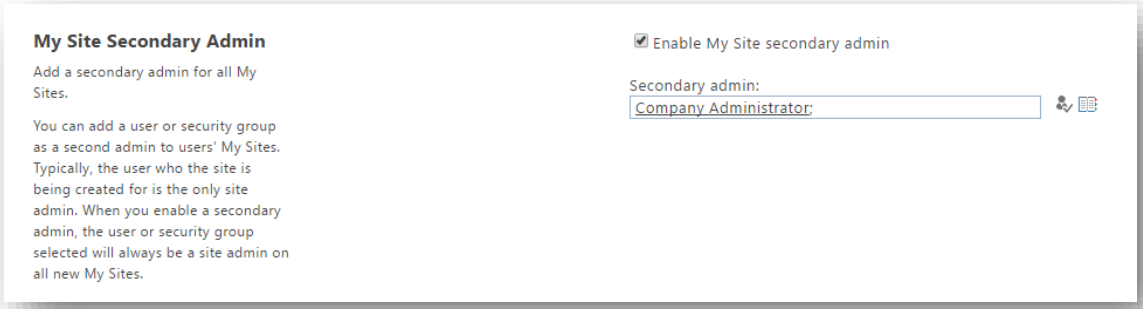
3.2. Permissions

- Granting access to Office365
  - Create a proprietary SecurityIQ service account in Azure / Office365 administration portal (e.g. **siq-srv@my-company.com**).
  - Assign the "SharePoint administrator" role to the new service account.
  - During the creation of the Application in the SecurityIQ administrative client – login with the newly created service account and grant Consent to the SecurityIQ Azure App.
  - This will allow the service account to enumerate the existing OneDrive accounts and query for audit information.
- Granting access to all existing OneDrive accounts
  - Owner access for the proprietary SecurityIQ user is required to Crawl, gather Permissions and perform Classification of documents stored on OneDrive accounts.
  - The built-in “Company Administrator” group automatically contains any user that was assigned the "SharePoint administrator" role in Azure.
  - To grant the required access, “Company Administrator” must be defined as a Secondary Owner of each OneDrive account.
  - In the installation package, you can find a script called *SIQUpdateOneDriveSecondaryOwners.ps1*. This script can be used to automatically update the Secondary Owners list of all existing OneDrive accounts so they to include “Company Administrator”. To run the script:
    - Open the Connectors\Util folder in the installation package.
    - Open the SharePoint Online Management Shell (install from here).
    - Run the script, you will be prompted to provide:
      - Credentials for Office365 Global Administrator
  - The tenant name of your Office365 subscription
  - SecurityIQ will not be able to crawl, collect permissions or classify content on OneDrive accounts who are not assigned with the ‘Site Collection Administrator’ permissions for the SecurityIQ user.
- Granting access to future OneDrive accounts
  - SharePoint Online administration portal allows configuration of default members of the Secondary Owners list for newly created OneDrive accounts.

- Browse to the admin portal (e.g. https://my-company-admin.sharepoint.com).
- Go to the “User Profiles” section, then click “Setup My Sites” under “My Site Settings”.



- Scroll down to “My Site Secondary Admin”



- Enable the “Enable My Site secondary admin” checkbox
- Write “Company Administrator” in the text box, and click the resolve button (once successfully resolved, the text should be underlined).
- Scroll to the bottom of the page and click “OK”.

3.3. Communications Requirements

Table 1. Communications Requirements

Requirement	Source	Destination	Port
SecurityIQ Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
SecurityIQ Access	Activity Monitor	SecurityIQ Servers	8000-8008

Requirement	Source	Destination	Port
Permissions Collection/Data Classification	Permissions Collector/Data Classification services	OneDrive REST API	https
Activity Audit	Activity Monitor	Office365 Activity 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.

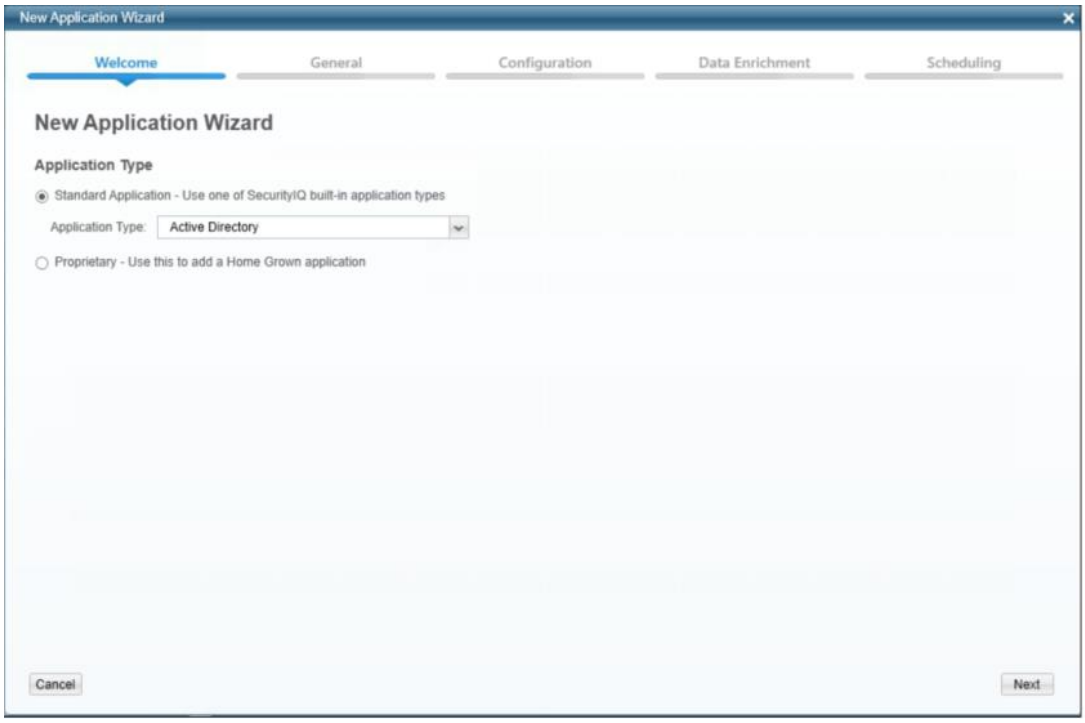


Figure 1. New Application Wizard Window

3. Select **Standard Application**.
4. Select **OneDrive for Business** from the **Application Type** dropdown menu.
5. Click **Next**.

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

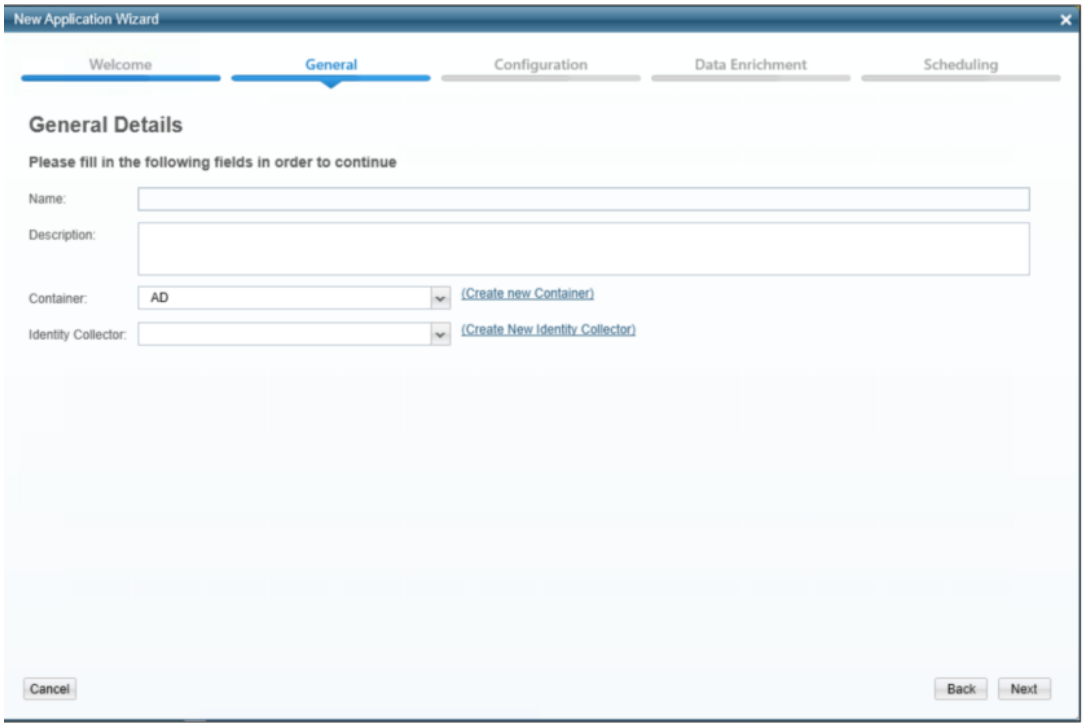


Figure 2. General Details Window

6. Type the logical name of the OneDrive for Business 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 Azure 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.

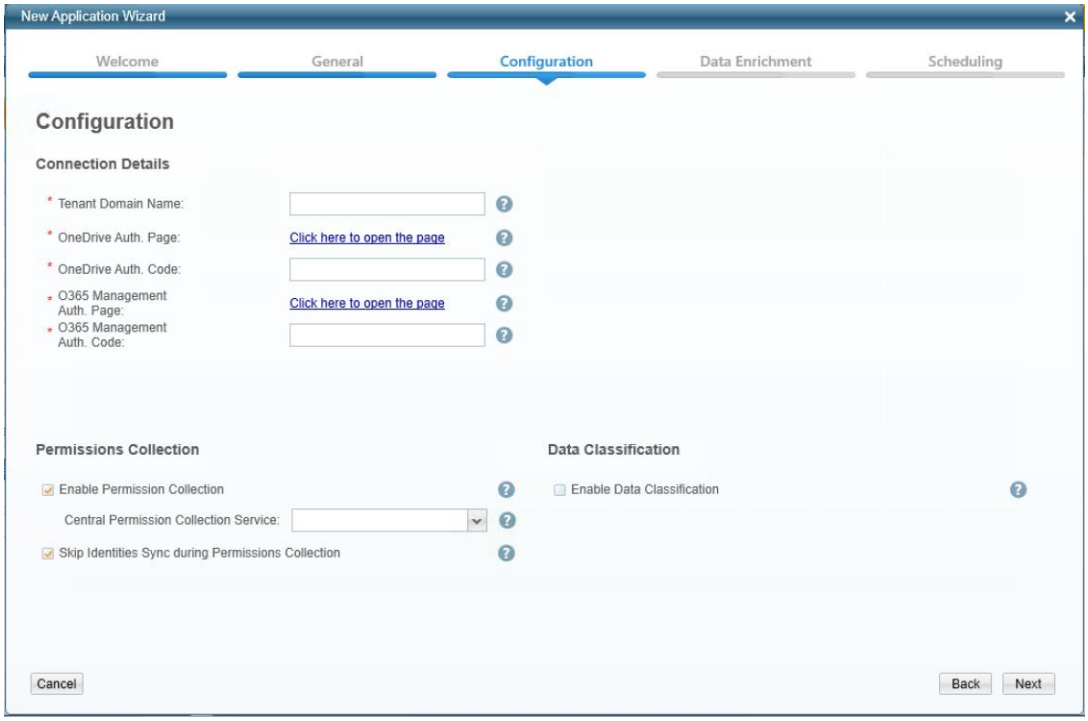


Figure 3. Configuration Window

11. Complete the Connection Details fields:
    - *Tenant Domain Name* (The name of the Azure domain are typically part of the OneDrive URL address.)
    - *OneDrive Authorization Page* (Click to open the authorization page.)
    - *Office365 Management Authorization Page* (Click to open the authorization page.)

The OneDrive authorization page displays.

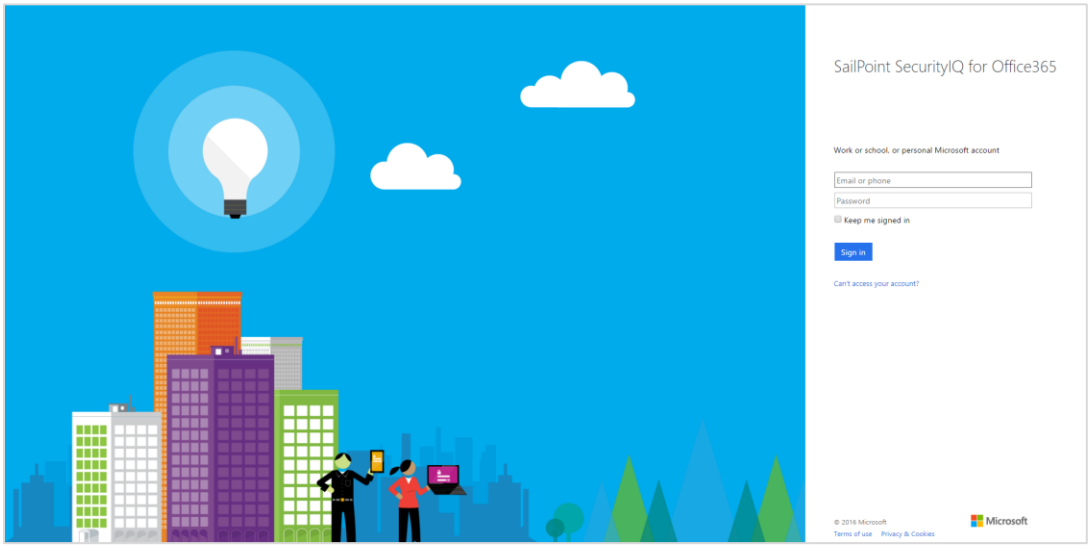


Figure 4. OAuth Microsoft Azure Consent Form

12. Login with an administrative user.

    You are redirected to the SecurityIQ Cloud authorization website.

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

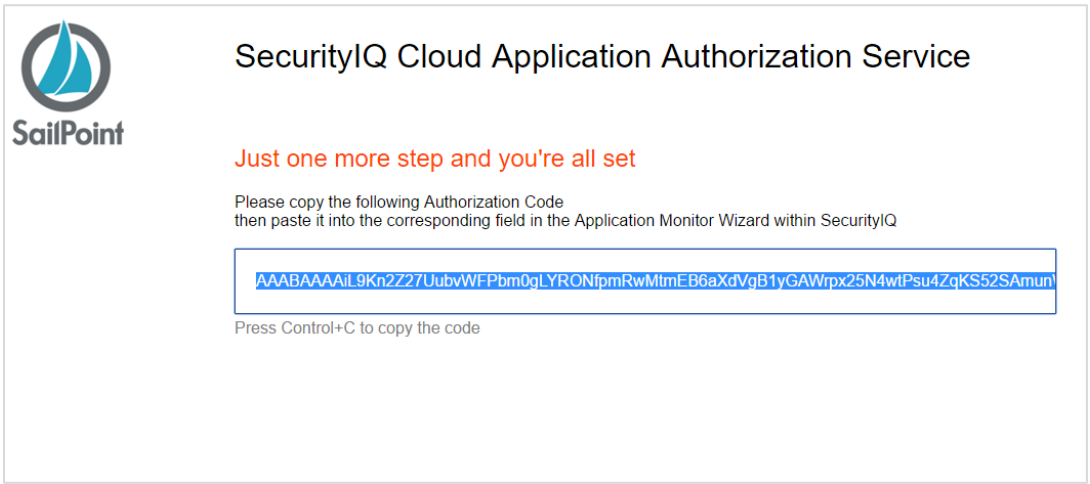


Figure 5. SecurityIQ Cloud Authorization Service Window

13. Copy the resulting authorization codes for OneDrive and Office365 to the *Authorization Code Configuration* field.
14. Revert to the Configuration window.
15. Click to enable Permission Collection, select a central permissions collector 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.)

16. Click to enable Data Classification and select a central data classification service from the list.
17. Click **Next**.

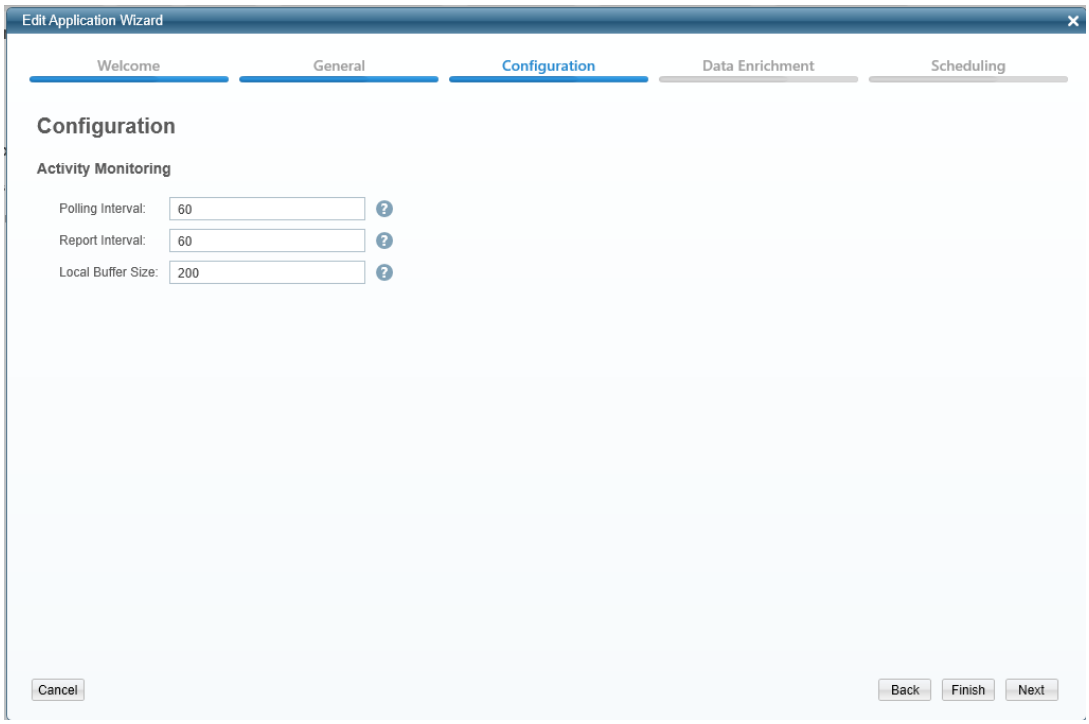


Figure 6. Activity Monitoring Configuration

18. 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.

19. Click **Next**.

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

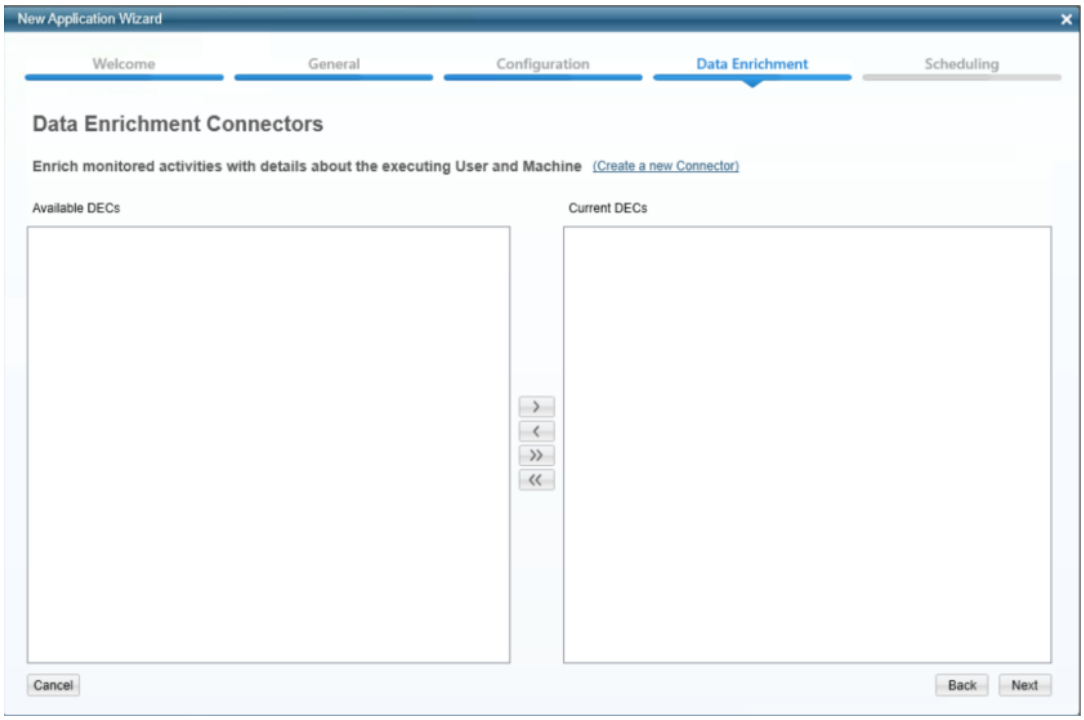


Figure 7. Data Enrichment Connectors Window

20. 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.

21. 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.

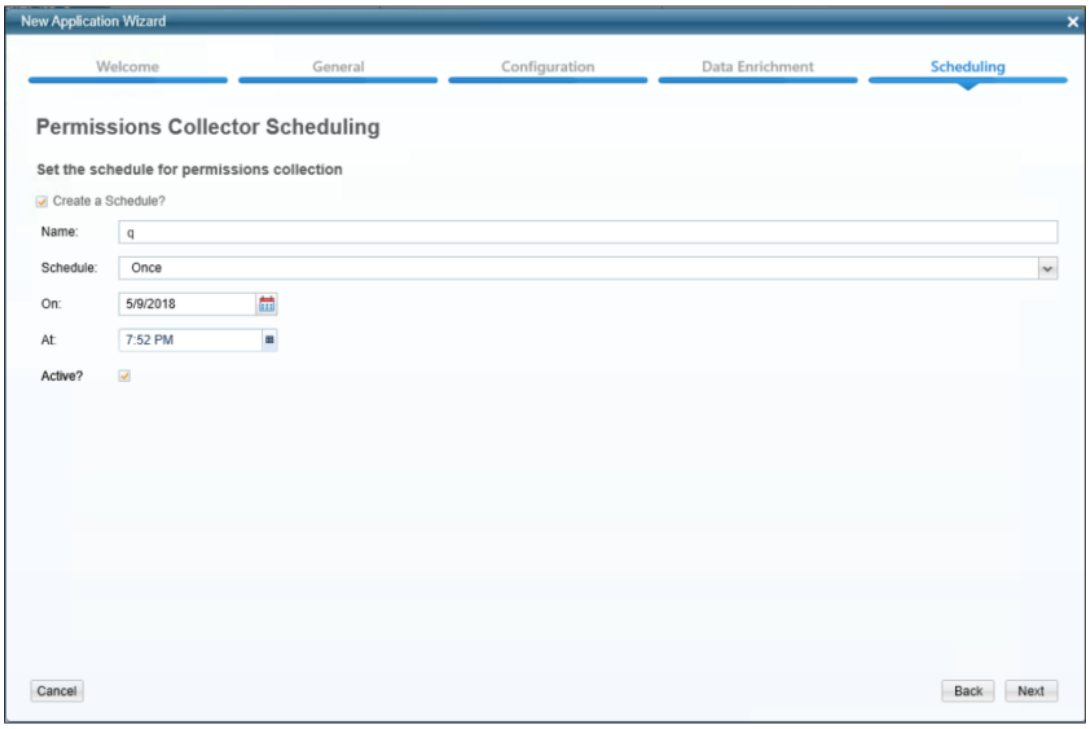


Figure 8. Permissions Collection Window

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

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

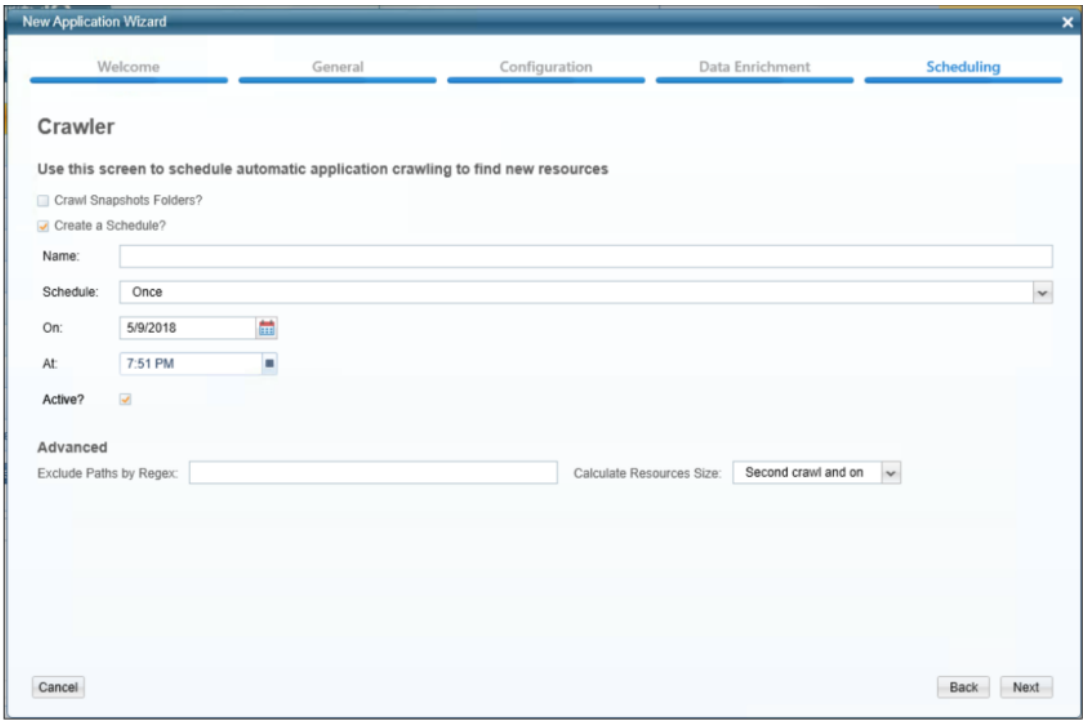


Figure 9. Crawler Window

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

34. Click **Next**.

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

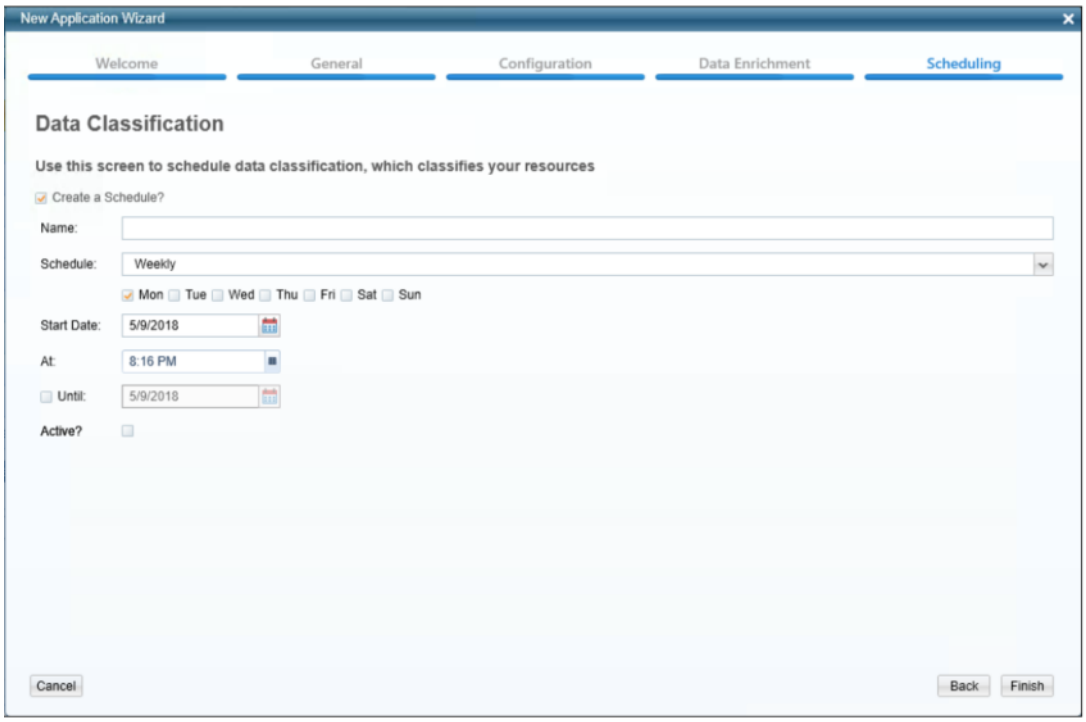


Figure 10. Data Classification Window

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

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

40. Click **Finish**.

5. INSTALLATION OF SERVICES

5.1. Collector Installation

1. Run the "SecurityIQ Collector 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.

Figure 11. SecurityIQ Collector Installation Manager

2. Enter the credentials to connect to SecurityIQ. 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.

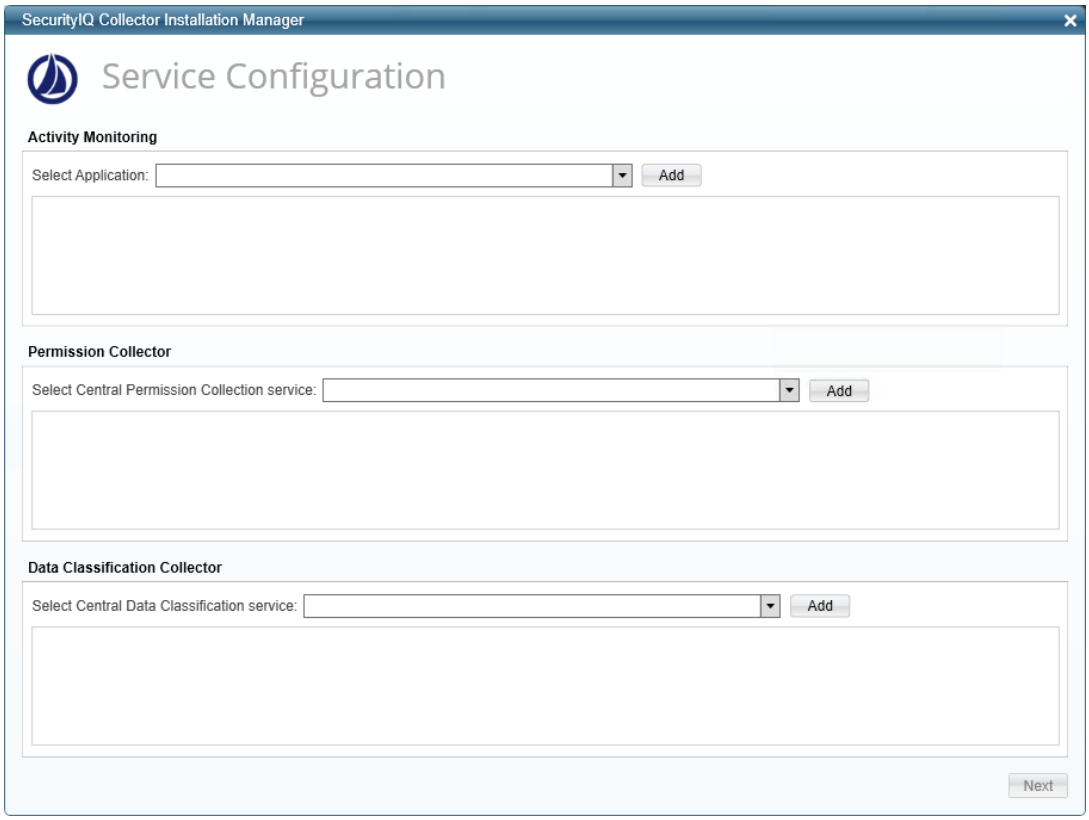


Figure 12. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application, and click **Add**.
5. If you are installing the Permission Collector or a Data Classification Collector, select the Central Permission Collector or Data 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.

6. Click **Next**.

The Installation Folder window displays.

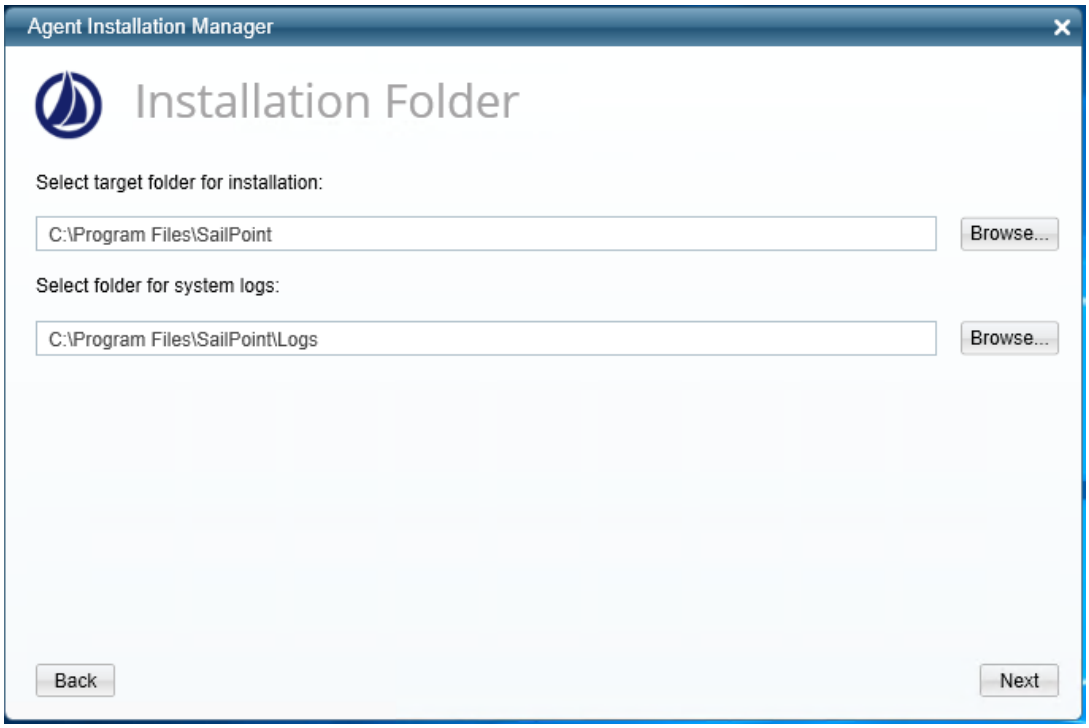


Figure 13. Installation Folder

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.

7. Browse and select the location of the target folder for installation.
8. Browse and select the location of the folder for system logs.
9. Click **Next**.

   The system begins installing the selected components.
10. Click **Finish** (which displays after all 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 Application**—<Application_Name> service is running.
- **SecurityIQ Data Classification**—<Application_Name> service is running.

6.3. Logs

- "%SIQ_HOME_LOGS%\ONEDRIVE_FOR_BUSINESS - <Application_Name>.log" does not contain errors.
- "%SIQ_HOME_LOGS%\DataClassification-<Application_Name>.log" does not contain errors.

6.4. Monitored Activities

1. Simulate activities on OneDrive.
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 Permission Forensics window.

7. TROUBLESHOOTING

3. There are 3 common scenarios where OneDrive accounts will not appear in the resources tree, or will partially appear there:
   a. Uninitialized OneDrive accounts (accounts which were never accessed and activated). These accounts can't be crawled, and will not appear in the resources tree since they exist. In the Crawl task details, you will see the following summary message (X stands for the number of uninitialized accounts):
   Not initialized accounts: X (see logs for details)
   b. Inaccessible OneDrive accounts. These are accounts which were not granted the prerequisites Site Collection Administrator permissions, and cannot be accessed. In the Crawl task details, you will see the following summary message (X stands for the number of uninitialized accounts):
   Not accessible accounts: X (see logs for details)
4. Partial folder structure for a OneDrive account. These are the hardest problem to troubleshoot. It can happen when there is at least 1 publicly shared object (folder or file) under the OneDrive account, which makes it possible for external users to Crawl it, but only for the publicly shared objects will be returned. No error message is logged for these accounts, and you should verify that the required Site Collector Administrator permissions were granted.