SailPoint IdentityIQ

Version: 8.0

File Access Manager Exchange 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
6.0	First Draft	Jonathan Rappeport	10 May 2018
6.1	Formatting changes only	Josh Lewin	11 Dec 2018
8.0	• Formatting • SIQETN-2349 - Exchange 2016 having a CAS installed on Windows server 2016 is not supported. • Rebranding SecurityIQ to IdentityIQ File Access Manager	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 Admin Client.
3. Install the Activity Monitor/Permissions Collector services.

Note: Permissions 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 IdentityIQ File Access Manager architecture.

Chapter 2: General

Connector Operation Principles

Monitoring Microsoft Exchange On-Premises is based on standard Microsoft Exchange monitoring capabilities. Access to Exchange On-Premises is based on Remote Power Shell capabilities.

Audit types include:

Mailbox Access Audit

- Administrators who access other users' mailboxes
- Users who access other users' mailboxes as delegates
- Owners who access their own mailbox

- Administrator Audit PowerShell Cmdlets (every Set-* PowerShell is audited)

Note: It is not recommended to enable Owner auditing on all mailboxes, due to Exchange overload and DB size.

Permissions Collector Operation Principle

The IdentityIQ File Access Manager Connector connects using the PowerShell interface and analyzes mailboxes, folders, public folders, and their permissions.

Mailbox Audit

4. Mailbox audit events are assigned to the relevant mailbox business resource.

5. The list of monitored mailbox types can be found in the BAMFramework.exe.config file under the *recipientTypeDetailsToMonitor* setting.

   - By default, the following types are defined and monitored:
     - UserMailbox
     - SharedMailbox

Note: Additional mailbox types can be added to this list, for reference follow this link.

Monitored Activities

Table 1. Monitored Activities

Action	Description	Admin	Delegate	Owner
Copy	An item is copied to another folder.	Yes	Yes	No
Create	An item is created in the mailbox. (For example, a message is sent or received.) Note that folder creation isn't audited.	Yes	Yes	Yes
FolderBind	A mailbox folder is accessed.	Yes	Yes	No

Action	Description	Admin	Delegate	Owner
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes	Yes	Yes
MessageBind	An item is accessed in the reading pane or opened.	Yes	No	No
Move	An item is moved to another folder.	Yes	Yes	Yes
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes	Yes	N/A
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes	Yes	N/A
SoftDelete	An item is deleted from the Deleted Items folder.	Yes	Yes	Yes
Update	An item's properties are updated.	Yes	Yes	Yes

Admin Audit Events (Administrator Audit Logging)

IdentityIQ File Access Manager features the following Admin audit events:

1. General Admin audit events are assigned to a special resource (**Audit Admin**).
2. Admin audit events that relate to a specific mailbox are assigned to the mailbox business resource.
   - The list of commands can be found in the BAMFramework.exe.config file in the *mailboxAuditLogCmdLets* setting.
   - By default, the following are defined as mailbox commands:
     - Remove-Mailbox
     - New-Mailbox
     - Set-Mailbox
     - Add-MailboxPermission
     - Remove-MailboxPermission
     - Set-MailboxAutoReplyConfiguration
3. Admin audit events related to a specific mailbox folder are assigned to the mailbox folder business resource.
   - The list of commands can be found in the BAMFramework.exe.config file in the *mailboxFolderAuditLogCmdLets* setting.
   - By default, the following are defined as mailbox folder commands:
     - Add-MailboxFolderPermission
     - Remove-MailboxFolderPermission
     - Set-MailboxFolderPermission
4. Admin audit events related to a specific public folder are assigned to the public folder business resource.

- The list of commands can be found in the BAMFramework.exe.config file in the *publicFolderAuditLogCmdLets* setting.
- By default, the following commands are defined as public folder commands:
  - Add-PublicFolderClientPermission
  - Remove-PublicFolderClientPermission
  - New-PublicFolder
  - Remove-PublicFolder
  - Add-PublicFolderAdministrativePermission
  - Remove-PublicFolderAdministrativePermission

Exclusion of Specific Mailboxes from Auditing

Specific mailboxes can be excluded from Auditing by setting a configurable key in the Application Monitor app.config file.

To exclude mailboxes, set the mailboxAuditExcludeByFilter under the AppSetting tag with a regular expression that matches only the names of the mailboxes to be excluded.

Use this setting to exclude a relatively small number of mailboxes from Auditing, when in Full Learning mode. The No Learning mode configuration is preferable if many mailboxes are excluded from auditing.

Note: For example, Journal mailboxes monitor and register every Exchange Server event, which doubles the number of generated events. Use this feature to exclude them.

After all mailboxes have been fetched from the Exchange server, the system applies a filter on the returned result set to filter out excluded mailboxes. All other mailboxes will be audited, subject to the setting defined.

Note: The defined setting only affects the mailbox Audit and does not affect Admin Audit events.

By default, the system removes all Audit settings from all monitored mailboxes (including those excluded by the Exclude Audit by Filter operation) when the Application monitor service stops running. This prevents unnecessary Audit settings from remaining after other changes have been made to the Application Monitor configuration over time.

Supported Versions

- Exchange 2010 (SP1 and above)
- Exchange 2013
- Exchange 2016 (In case of Exchange 2016 having a CAS installed on Windows server 2016, see comments in the next chapter)

Chapter 3: Prerequisites

Software Requirements

- Activity Monitor/Permissions Collection
  - Microsoft .Net Framework 4.5
- PowerShell

Requirements

- Run the following command on one of the Exchange CAS to enable remote PowerShell:

```
shell winrm qc
```

Notes:

- **The Exchange environment on a 2010 server with an Activity Monitor must be configured to communicate with a 2010 CAS server, while an environment on a 2013 server with an Activity Monitor must be configured to communicate with a 2013 CAS server.**
- **Previous versions of IdentityIQ File Access Manager required the installation of an additional PowerShell endpoint on an Exchange CAS server that allowed unrestricted script execution. This requirement was removed beginning with SecurityIQ v5p1 to simplify the deployment of the connector.**
  If your environment was upgraded from older versions, it is recommended that you delete the obsolete "WBXPowerShell" endpoint from the Exchange CAS server.
- **Important: Due to a known Microsoft bug when running Microsoft Exchange 2016 installed on a Windows 2016 server, customers must install an additional Client Access Service (CAS) on a non-2016 Windows Server, and then configure the IdentityIQ File Access Manager Exchange Application Monitor to access that CAS server. We will update this guidance when Microsoft provides an update to Microsoft Exchange 2016.**

Permissions

- Create a designated domain user (for example, *siq_xch*).
- Assign the following user Exchange groups:
  - Recipients Management
  - Records Management
  - Public Folders Management
- From PowerShell on the CAS run the following:

```
Set-User [username] -RemotePowerShellEnabled $True
```

Audit Bypass

The IdentityIQ File Access Manager Connector for Exchange sets the mailbox audit for the selected mailboxes according to the configuration in the Application. However, there are application service accounts (for example,

BlackBerry or IXOS) which create many mailbox audit log entries that overload the Exchange and creates a lot of noise in IdentityIQ File Access Manager.

You can configure a user or computer account to bypass mailbox audit logging, so that actions taken by that user or account for any mailbox are not logged.

By bypassing a trusted user or computer accounts that require frequent access to mailboxes, you can reduce the noise in mailbox audit logs.

For more information, see:

https://technet.microsoft.com/en-us/library/ff461934%28v=exchg.150%29.aspx

Note: It is recommended to set an alert on bypass commands to verify that users are not bypassed unexpectedly.

Audit Age Log Limit

By default, audit logging is configured to store audit log entries for 90 days.

After 90 days, the audit log entry is cycled. You can change the audit log age limit using the Set-Mailbox cmdlet with the *AuditLogAgeLimit* parameter.

You can specify the number of days, hours, minutes, and seconds to retain audit log entries.

Logs need not be retained for a long time (more than a few days), since IdentityIQ File Access Manager offloads the data from the exchange.

Note: It is not recommended to retain an audit for a long time, since doing so expands the Exchange DB.

The following site provides more information:

https://technet.microsoft.com/en-us/library/bb123981%28v=exchg.150%29.aspx

Communications Requirements

Table 2. Communications Requirements

Requirement	Source	Destination	Port
IdentityIQ File Access Manager Message Broker	Permissions Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor/Permissions Collector	IdentityIQ File Access Manager Servers	8000-8008
Remote PowerShell	Activity Monitor/Permissions Collector	CAS server	80 or 443

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 Exchange from the **Application Type** dropdown menu.

3. Click **Next**.

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

4. Type the logical name of the Exchange application in the *Name* field.

5. Type a description of the application in the *Description* field.

6. Select a logical container for the application from the **Container** dropdown menu.

7. Select an Active Directory Identity Collector from the **Identity Collector** dropdown menu.

8. Click **Next**.

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

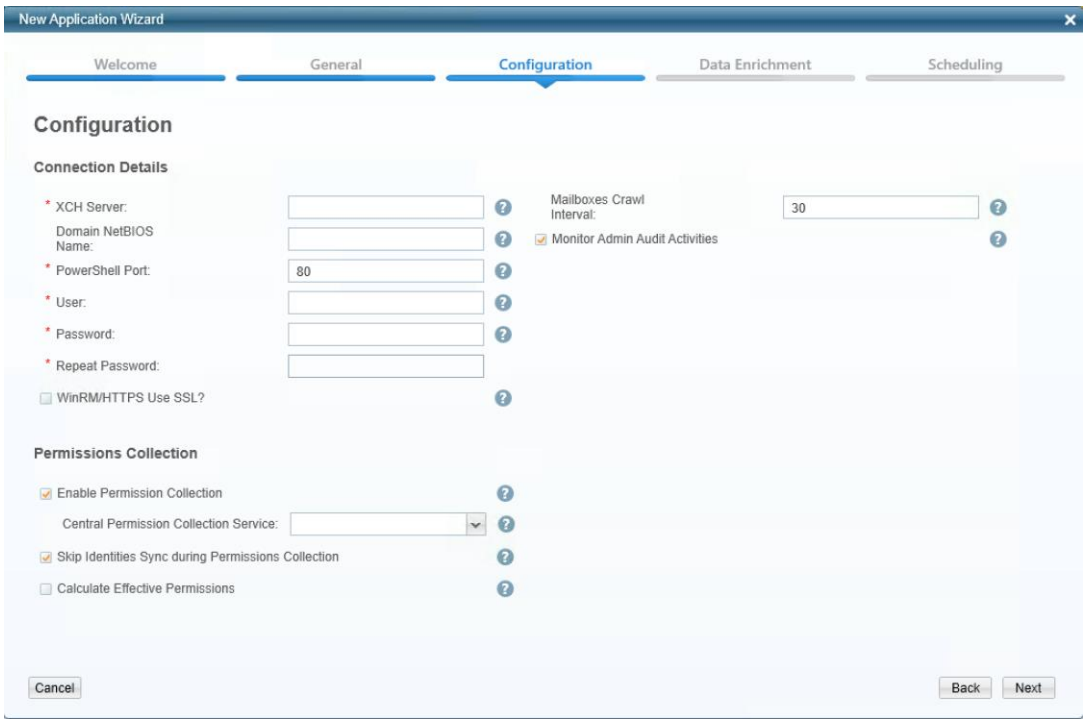

Figure 1. Configuration Window I

9. Complete the Connection Details fields:

   - *XCH Server* (This is the Exchange CAS server)
   - *Domain NetBios Name* (This is the short domain name.)
   - *PowerShell Port* (This is 80 if working with HTTP or 443 if working with HTTPS.)
   - *User and Password* (This is the user defined in the prerequisites.)

- *WinRM/HTTPS User SSL* (Use the SSL when connecting with WinRM/SSL.)
- *Mailboxes Crawl Interval* (This is the interval for checking for newly created mailboxes (minutes) if working in Auto Learning Mode.)
- *Monitor Admin Audit Activities* (This monitors Exchange Administrator Set-* commandlets.)

Note: User Domain, User, and Password are the user defined in the prerequisites.

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.)

The Configuration window displays under the Configuration tab.

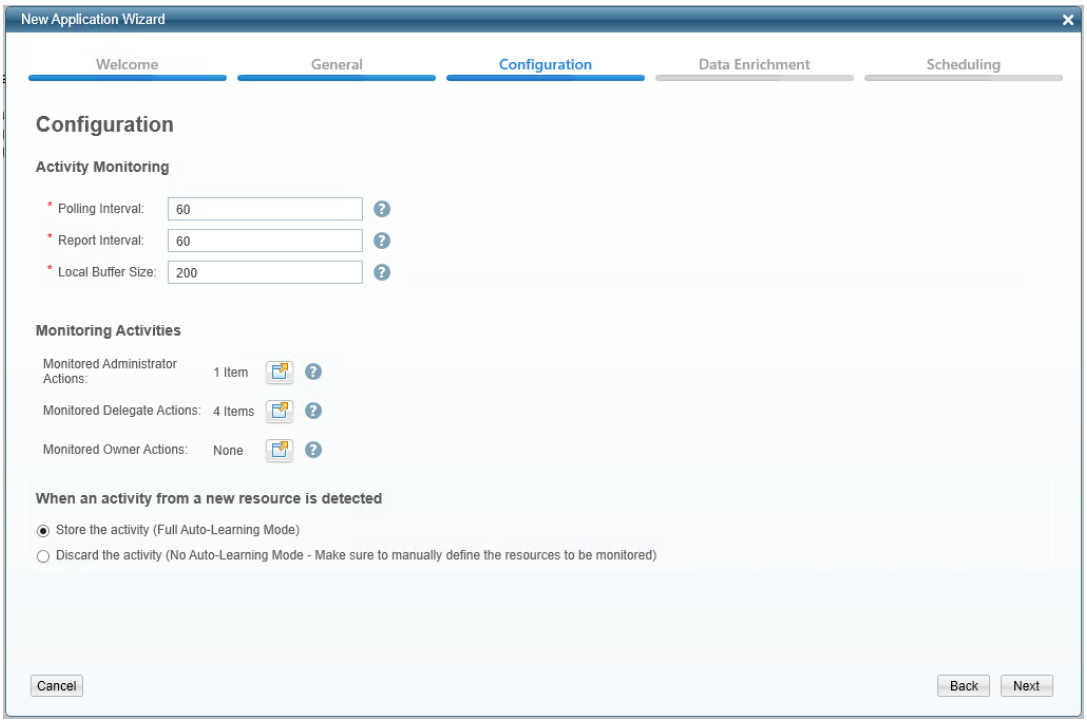

Figure 2. Configuration Window II

11. 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]

Monitoring Activities:

12. *To select the activities to monitor for each user group:*

a. Press the Select Activities button to open the select activities panel per user type.
b. Select the required activities to monitor
c. Click **Save** or **Cancel** to exit.

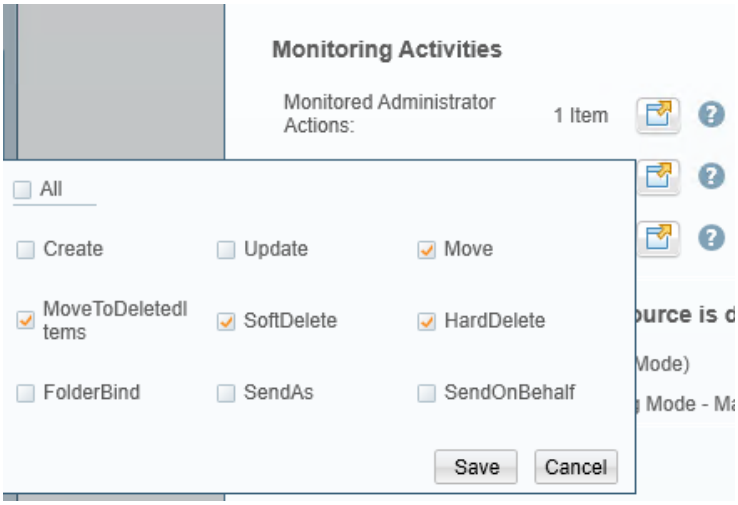

Figure 3. Monitoring Activities' options

Notes:

- **This cyclic buffer stores activities on the Activity Monitor machine in case network errors prevent activities from being sent.**
- **Monitoring Activities are relevant only in full auto-learning mode. When working in Discard mode, you must configure the monitored activities for each monitored business resource by editing the business resource itself.**

- *Monitored Administrator Actions* (Choose administrator actions to be monitored.)
- *Monitored Delegate Actions* (Choose delegate actions to be monitored.)
- *Monitored Owner Actions* (Choose owner actions to be.)

13. Select the relevant Monitor Configuration fields:

    - *Store the activity (Full Auto-Learning Mode)* (Monitor all activities from all mailboxes to create new mailboxes in the Business Resources Tree automatically. This will cause the Activity Monitor to search for new mailboxes every defined interval and set the mailbox audit according to the defined in ”Monitoring Activities” above.)
    - *Discard the activity (No Auto-Learning Mode*. Be sure to manually define only the mailboxes to be monitored by editing the mailbox business resource and selecting which activities to monitor.)

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: See the chapter *Activities* in the IdentityIQ File Access Manager Administrator Guide for 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 among those windows, using the Next and Back buttons.

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

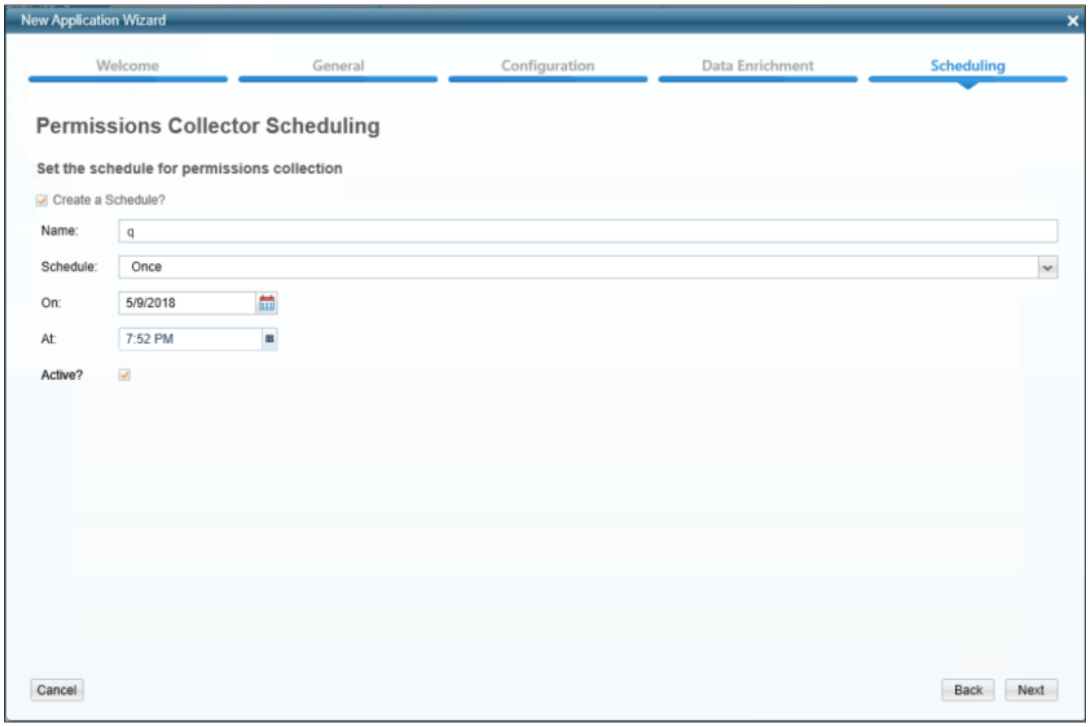

Figure 4. Permissions Collection Window

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.

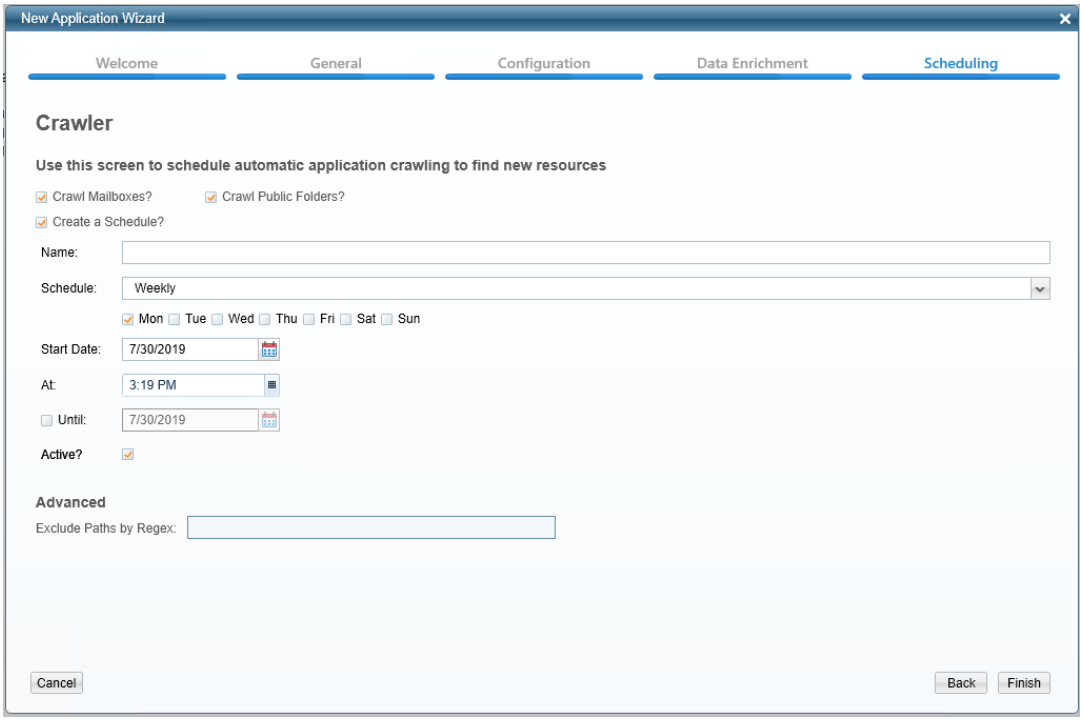

Figure 5. Crawler Window

23. Select whether to crawl mailboxes, and/or public folders.

24. If you want to create a schedule, select **Create a Schedule**.

    a. Type a name for the crawling scheduling task in the *Name* field.

    b. Select a scheduling frequency from the **Schedule** dropdown menu.

    c. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).

    d. Check the **Active** check box if relevant.

    e. Type in the names of folders to exclude from the crawling process in the *Exclude Paths by Regex* field.

Note: For more information, see the chapter *Crawling* in the IdentityIQ File Access Manager Administrator Guide .

25. 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 6. 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.

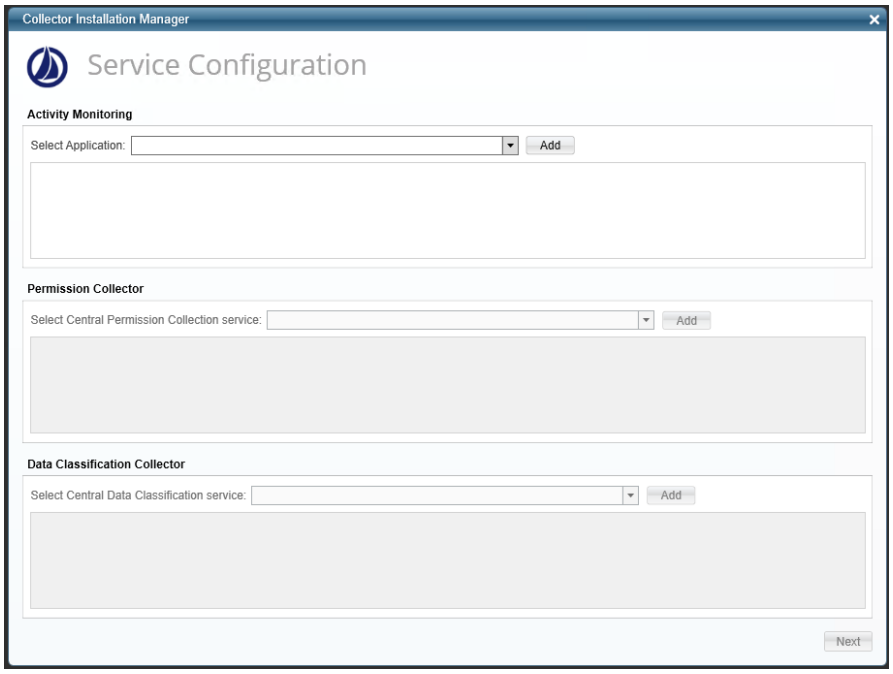

Figure 7. Service Configuration

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**.

   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.

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

    Note: For more information, see the chapter *Permissions* in the IdentityIQ File Access Manager Administrator Guide .

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 Central Permissions Collection** - <Service Name> service is running.
- **File Access Manager Central Data Classification** - <Service Name> service is running.
- **File Access Manager Central Activity Monitor** - <Service Name> service is running.

Logs

- "%SAILPOINT_HOME_LOGS%\EXCHANGE_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\Permissions Collection_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\Watchdog_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on Exchange.
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 Permission Forensics window.