



File Access Manager Identity Collector

Version: 8.4

Revised: March 27, 2023

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices

Copyright © 2023 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

- Identity Collection** **1**
 - Cloud Identity Collectors 1
- Identity Collector Main Page** **1**
 - Filters 1
 - Editing an Identity Collector 2
 - Deleting an Identity Collector 2
 - Running the Synchronization Task 2
 - Setting an Authentication Store 2
- Active Directory Overview** **5**
 - General Details – Active Directory 5
 - Connection Details By DEC– Active Directory 6
 - Connection Details By Properties – Active Directory 7
 - Trusted Domains 8
 - Users Collection – Active Directory 9
 - Join Data Sources – Users 10
 - Dynamic Field Mapping (Users) 11
 - Group Collection – Active Directory 12
 - Join Data Sources – Groups 13
 - Dynamic Field Mapping (Groups) 14
 - Final Configurations 15
- Azure Active Directory Overview** **19**
 - General Details – Azure Active Directory 19
 - Connection Details – Azure 20
 - Users Collection – Azure 21
 - Join Data Sources – Users 22
 - Dynamic Field Mapping (Users) 23
 - Group Collection – Azure 24
 - Join Data Sources – Groups 25

Dynamic Field Mapping (Groups)	26
Final Configurations	27
NIS Overview	31
General Details – NIS	31
Connection Details – NIS	32
Users Collection – NIS	32
Join Data Sources – Users	33
Dynamic Field Mapping (Users)	34
Group Collection – NIS	35
Join Data Sources – Groups	36
Dynamic Field Mapping (Groups)	37
Final Configurations	38
Data Source Overview	42
General Details – Data Source	42
Connection Details (Users) – Data Source	43
Dynamic Field Mapping (Users)	44
Connection Details (Groups) – Data Source	45
Dynamic Field Mapping (Groups)	46
Connection Details (User Membership in Groups) – Data Source	47
Connection Details (Group Hierarchy) – Data Source	48
Final Configurations	49

Identity Collection

The Identity Collector is a software component responsible for synchronizing identity data (for example, accounts and attributes) from identity stores.

Examples of Identity Collectors include Active Directory (the most common Identity Store), NIS Identity Collector (used in Linux/Unix environments), Microsoft Azure Active Directory (used for cloud applications), and a Data Source Identity Collector.

You define Identity Collectors by creating a new Identity Collector, which represents the main Active Directory Domain, (or Authentication Store).

The section below describes how to create/edit an Active Directory identity collector. The process for creating/editing an NIS, Azure, and Data Source Identity Collectors is like that for creating/editing an Active Directory identity collector, with the main difference being actual configuration.

You can also configure and edit Cloud Identity Collectors (i.e. Box, DropBox, Google Drive, etc.).

The section, [Configuring the Permissions Collector](#), within the Administrator guide describes how to configure users, groups, and user-groups for homegrown Permissions Collection, which is like configuring a Data Source Identity Collector.

Cloud Identity Collectors

Cloud application Identity Collectors are created in the application setup process. They will be displayed and can be edited through the Identity Collector screen.

Cloud application Identity Collectors are created through the adding application setup process.

You can see the connected fields, join other data sources, and complete dynamic field mapping.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.

You cannot set Cloud application as authentication store.

Identity Collector Main Page

The Identity Collector page displays all previously created Identity Collectors. This screen also allows the user to add, edit, remove, sync and manage Identity Collectors. You can also set the Authentication Store.

Note: Cloud application Identity Collectors are created in the application setup process. They will be displayed on this screen and can also be edited here.

Access the Identity Collector page by navigating to **Admin > Identity Collectors**.

To create a new Identity Collector, click **Create New**.

Name

This is the name of an Identity Collector

Type

This is the type (Active Directory, Azure, NIS, Data Source) of Identity Collector

Actions

This column provides the user three possible options:

- Edit
- Delete
- More
 - a. Run Synchronization
 - b. Set Authentication Store

Note: If an Identity Collector is set an Authentication Store, that Identity Collector will display on the first row.

Filters

To filter the results on the grid, click the filter icon on the heading bar. Select the requested criteria.

A user can filter various Identity Collectors by providing a full or partial name or by selecting the known type.

Click **Apply** to apply the filter or click **Clear All** to clear the filters and repopulate the grid.

Editing an Identity Collector

1. Select the edit icon on the row of the Identity Collector you wish to edit.

Note: The Type field will be disabled.

With the exception of the Type field, every step in the wizard will be editable.

Deleting an Identity Collector

Note: If an Identity Collector is set as an Authentication Store, that Identity Collector cannot be deleted. If an Identity Collector is used within another part File Access Manager, it cannot be deleted.

Note: Only one Identity Collector can be deleted at a time.

1. Select the delete icon on the row of the Identity Collector you wish to delete.
2. A dialog will display confirming the deletion of the selected Identity Collector.

Running the Synchronization Task

A user is able to sync to an Identity Collector so that it has the most updated identities. If anything about the Identity Collector is changed, run the synchronization task to update the changes.

To run a synchronization, navigate to the Actions column on the Identity Collector row and click **More Options > Run Synchronization**.

Note: It is recommended that the Synchronization task is ran before selecting an Authentication Store.

Note: Cloud applications cannot run the Synchronization task.

Setting an Authentication Store

Authentication Stores are used by File Access Manager to authenticate users across its various interfaces.

Changing the Authentication Store from one Identity Collectors to another will affect the following:

- The users associated with File Access Manager and their access to it.
- It will stop the review processes of all running Access Certification Campaigns and Access Requests.
- It might affect predefined review processes.

Before you change your Authentication Store, we recommend running synchronization on the Identity Collector. This is to ensure you receive the most updated results and avoid losing the user's permissions.

1. Select the More Options button on the row of the Identity Collector you wish to set as the Authentication Store.
2. Select **Set Authentication Store**.

Note: The newly set Identity Collector will move to the top of the grid.

Caution: Cloud application Identity Collectors cannot be set as Authentication Stores.

Caution: You can connect the Authentication Store Identity Collector to other Identity Collectors by setting the Same User Field between two or more Identity Collectors in order to extend the Access Request's Usage list.

3. When creating a new Identity Collector, a toggle will display on the General Details steps to set the Identity Collector as the Authentication Store.

Note: When setting the Authentication Store through creating a new Identity Collector, the

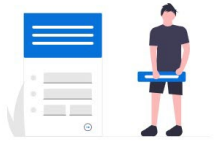
toggle will only display if there are no Authentication Stores currently enabled.

General Details

When creating a new Identity Collector, select an Identity Collector type based on your system's configured Identity Stores and provide a name.

Wizard supported Identity Collector types do not include Cloud application Identity Collectors. Those are created through the adding application setup process in the Wizard (under the Admin tab).

If editing an existing Identity Collector, all fields except for the Type field are editable.



Type
Choose the type of Identity Collector

Name *
Enter the Identity Collector name

Advanced Options ⓘ

Do you want to set the Authentication Store?

IDENTITY COLLECTOR
Step 1 of 2

Cancel Next

Active Directory Overview

The Active Directory Identity Collector is used to collect the user's and group's existing data.

General Details – Active Directory

To create an Active Directory Identity Collector:

1. Open the Identity Collectors panel by navigating to **Admin > Identity Collectors**.
2. Click **Create New** to open the Identity Collector Configuration Wizard .

Identity Collector General Details:

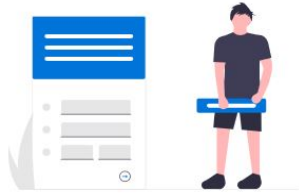
1. Select Active Directory for the type.
2. Provide a name for the Identity Corrector you are creating.
3. Within the Advanced Options section, choose if you would like to enable Access Fulfillment. If you enable access fulfillment, the system can add and/or remove users from groups in this identity collector.
4. Click **Next**.

General Details

When creating a new Identity Collector, select an Identity Collector type based on your system's configured Identity Stores and provide a name.

Wizard supported Identity Collector types do not include Cloud application Identity Collectors. Those are created through the adding application setup process in the Wizard (under the Admin tab).

If editing an existing Identity Collector, all fields except for the Type field are editable.



Type

Active Directory ▼ *

Name *

Enter the Identity Collector name

Advanced Options ⓘ

Do you want to enable Access Fulfillment?

IDENTITY COLLECTOR

Step 1 of 7

Cancel

Next

Connection Details By DEC– Active Directory

You can configure the Identity Collector by either an already existing DEC or by Properties.

1. Click **By DEC** to fill the Identity Collector with pre-configured data in DEC or click **By Properties** to enter a connection property manually from a list of defined properties.
 - a. If you selected **By DEC**, select the relevant Active Directory DEC's from the dropdown list.

Note: If you configured DEC to connect to Active Directory, you can reuse that configuration here.

- b. By default, File Access Manager retrieves several properties from Active Directory, such as Domain, and Display Name, etc. Add more properties by typing in the **Properties to Fetch** field and click the plus icon to add the property.

The properties you retrieve come from the Active Directory, and will be available later for mapping to the Data Dictionary fields.

Note: This can be done for both User Collection and Groups Collection. You need to complete the process either by joining Data Sources as the local key or by configuring to the Identity Collector in the Dynamic Field Mapping step.

2. Click **Next**.

Applications Data Sources Permissions Management Identity Collectors

Connection Details – (Active Directory) Identity Collector

The Active Directory Identity Collector is used to collect the user's and group's existing data.

Fill in the needed parameters to continue. Configure the Identity Collector by DEC settings or by properties.

You can retrieve extra properties from the Active Directory by adding them through Properties to Fetch.

By DEC **By Properties**

Note: You can create a new DEC in the Administrative Client. Navigate to Configuration > Activity Monitoring > Data Enrichment Connectors. Refresh

DEC
office.whitebox.forest

Users Collection
Properties to Fetch 0 Selected | Clear Selection
Type in an item and press + to add it to the list.

Groups Collection
Properties to Fetch 0 Selected | Clear Selection
Type in an item and press + to add it to the list.

IDENTITY COLLECTOR
Step 2 of 7

Cancel Previous **Next**

Connection Details By Properties – Active Directory

If you click **By Properties**, type the following data in the relevant fields:

Domain NetBios Name

Domain NetBios name

Domain DNS Name

System Domain Name

User

Provide the username that will be associated with this Identity Collector

Password

Provide the password for the Identity Collector

SSL

Select this if that connection to Active Directory is secure.

Base DN

This defines the distinguished name of a folder which the identities (users and groups) are collected. If nothing is set, the Base DN becomes a root and File Access Manager will collect user and groups from an existing Active Directory server.

By default, File Access Manager retrieves several properties from Active Directory, such as Domain, and Display Name, etc. Add more properties by typing in the **Properties to Fetch** field and click the plus icon to add the property.

Connection Details – (Active Directory) Identity Collector

The Active Directory Identity Collector is used to collect the user's and group's existing data.

Fill in the needed parameters to continue. Configure the Identity Collector by DEC settings or by properties.

You can retrieve extra properties from the Active Directory by adding them through Properties to Fetch.

By DEC **By Properties**

Domain NetBios Name *
Domain NetBios Name

Domain DNS Name *
Domain DNS Name

User *
Enter Username

Password *
Password

SSL

Base DN
Base DN

Users Collection ⓘ
Properties to Fetch 0 Selected | Clear Selection
Type in an item and press + to add it to the list. ▾

Groups Collection ⓘ
Properties to Fetch 0 Selected | Clear Selection
Type in an item and press + to add it to the list. ▾

IDENTITY COLLECTOR
Step 2 of 8

Cancel Previous **Next** Go to Set

Trusted Domains

When configuring an Active Directory Identity Collector By Properties, you need to complete the configuration by selecting the relevant Trusted Domains.

An internal list of Trusted Domains that were retrieved will display.

Trusted Domains Authentication

To complete the Active Directory's configuration process, select the relevant Trusted Domains from the internal list of Trusted Domains that were retrieved for the configured Active Directory.

You can also choose to synchronize external trusted domains. If you have a large number of domains, it might take a few minutes.

For each Trusted Domain, you can either use the predefined credentials, customize specific credentials, or choose not to sync the domain.

Trusted Domains Authentication

Synchronize External Trusts? (2 trusted domains were detected)

office.whitebox.forest [office]

User Default Credentials Specify Credentials Do not Sync

whitebox.forest [WHITEBOX] (In forest with office)

User Default Credentials Specify Credentials Do not Sync

IDENTITY COLLECTOR
Step 3 of 4

[Cancel](#) [Previous](#) [Next](#)

Users Collection – Active Directory

Verify that the system retrieved the requested data successfully.

This table displays the first fetched results from the connected Identity Collector and well as the fetched properties.

1. Select **Yes** or **No** to join this Identity Collector with any existing data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

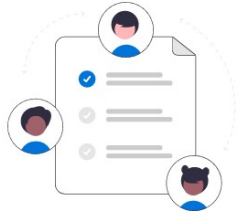
SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Request

Applications Data Sources Permissions Management Identity Collectors

Users Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.



Review the following data sample

sAMAccount...	distinguishe...	proxyAddres...	displayName	userPrincipal...	depa
Administrator	CN=administr...	Administrator...	Administrator...	Administrator...	test c
Guest	CN=Guest.CN...				
__VMware_C...	CN=__VMwa...		__VMware_C...		
krbtgt	CN=krbtgt.CN...				
WHITEBOX\$	CN=WHITEBO...				
wbx_ad_dec	CN=wbx_ad_d...		wbx_ad_dec	wbx_ad_dec@...	
wbx_ad_monit...	CN=wbx_ad_...		wbx_ad_monit...	wbx_ad_monit...	

Do you want to join this Identity Collector with another Data Source?

Yes

No

IDENTITY COLLECTOR
Step 3 of 7

[Cancel](#)
[Previous](#)
[Next](#)
Activate Wir
Go to Settings to

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional.

If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources.

Join Data Sources – Users

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Request


Applications Data Sources Permissions Management Identity Collectors

Users - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.



Data Source

You can create a new data source in Admin > Data Sources and click Refresh. Refresh

Data Source	Local Key	Remote Key	
Data Source ▼ *	Select Value ▼ *	Select Value ▼ *	

IDENTITY COLLECTOR
Step 4 of 8

Cancel Previous Next Activate \ Go to Settings

4. Click **Next**.

Dynamic Field Mapping (Users)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the User Dictionary Field dropdown.
2. From the Users Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Users - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Users Dictionary Field	Mapped Field
Select Field	Select Field

[+](#) [-](#)

Group Collection – Active Directory

Verify that the system retrieved the requested data successfully.

This table displays the first fetched results from the connected Identity Collector and well as the fetched properties.

1. Select **Yes** or **No** to join this Identity Collector with any existing data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

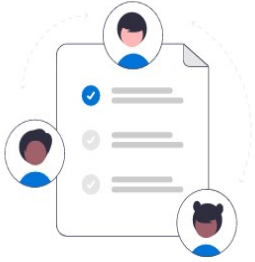
SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Req

Applications Data Sources Permissions Management Identity Collectors

Groups Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.



sAMAccount...	distinguishe...	memberOf	member	sIDHistory	obje
WinRMRemot...	CN=WinRMR...				AQU
Administrators	CN=Administr...		CN=DanTestG...		AQIA
Users	CN=Users.CN...		CN=DaveGro...		AQIA
Guests	CN=Guests.C...		CN=Domain ...		AQIA
Print Operators	CN=Print Ope...				AQIA
Backup Opera...	CN=Backup O...		CN=administr...		AQIA
Replicator	CN=Replicato...				AQIA

Review the following data sample

Do you want to join this Identity Collector with another Data Source?

Yes

No

IDENTITY COLLECTOR
Step 6 of 8

Cancel Previous Next

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional.

If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional group fields from other data sources by joining those data sources.

Join Data Sources – Groups

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Requ

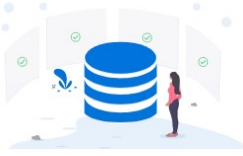
Applications Data Sources Permissions Management Identity Collectors

Groups - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc.). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh. **Refresh** ↻

Data Source	Local Key	Remote Key	
Data Source ▼ *	Select Value ▼ *	Select Value ▼ *	🗑️

Activat
Go to Set

Cancel Previous Next

IDENTITY COLLECTOR
Step 7 of 9

4. Click **Next**.

Dynamic Field Mapping (Groups)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the Group Dictionary Field dropdown.
2. From the Groups Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Groups - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Groups Dictionary Field	Mapped Field
Select Field	Select Field

Buttons: +, -

IDENTITY COLLECTOR

Step 5 of 8

[Cancel](#) [Previous](#) [Next](#)

Final Configurations

On the final screen in the Identity Collector wizard, a user can set a couple of final configurations and set the scheduler task.


SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Request

Applications Data Sources Permissions Management Identity Collectors

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.



Users Mapping Authentication

Map Accounts by Same User (Optional)
Select Field

Email Field Mapping (Optional)
proxyAddresses (If Microsoft Exchange Integration is valid)

Scheduler

Create a Schedule

Schedule Name *
office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

IDENTITY COLLECTOR
Step 9 of 9

Cancel Previous Save Save & Run

Users Collection

The following final configurations are optional:

- Email Field Mapping – select an email field to be used to send alerts. If your Active Directory is integrated with Microsoft Exchange, you can map the proxyAddresses field. Otherwise, select a Users Dynamic Field that is already mapped from the wizard.
- Unique User Accounts Mapping – used to connect the Authentication Store Identity Collector to other Identity Collectors by setting the Same User Field between two or more Identity Collectors, mainly clouds Identity collectors, which extends the Access Request's Usage list.

Scheduler

If you wish to create a scheduled task, check the **Create a Schedule** toggle and complete the following:

1. Provide a name for the schedule.
2. The Scheduler is Active by default. If you wish to turn the schedule task inactive, switch the toggle to Inactive.
3. If you are wanting to start the Identity Collector process immediately, select **Schedule**. If you want to schedule the Identity Collector after a specific task completes, select **Run After**.

Note: If Run After is selected, all Schedule options will disappear.

4. Select how frequent you want the Identity Collector task to run.
 - Once – one time run. Verify the date selected is in the future
 - Hourly – select the time and date for the run. Verify the date selected is in the future. Either select a specific end date or select **Never**
 - Daily – same as hourly
 - Weekly (Set as default) – select a day or multiple days for recurring runs. Either select a specific end date or select **Never**
 - Monthly – same as hourly
 - Quarterly – same as hourly
 - Half Yearly – same as hourly
 - Yearly – same as hourly
5. If you want the task to end on a specific future date, select **On** and then provide the ending date. If the task should run without an end date, select **Never**.
6. Click **Save** to store the Identity Collector without running synchronization.
OR
7. Click **Save & Run** to create and synchronize the Identity Collector.


SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings **Admin**

Applications Data Sources Permissions Management Identity Collectors

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.



Scheduler

Create a Schedule

Schedule Name *
office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

Frequency Type
Once

Once Recurrence
Time (UTC) *
09 : 26 AM

Start Date *
08/07/2022

Summary: Once starts on Aug 7, 2022 at 9:26 AM

IDENTITY COLLECTOR
Step 7 of 7

Cancel Previous Save Save & Run

Azure Active Directory Overview

Microsoft Azure Active Directory Identity Collector supports standard OAuth 2.0 Authorization for the Azure AD connector.

The authorization sequence directs the user through a standard Microsoft O365 consent flow. This grants the File Access Manager Azure AD Connector application the privilege to acquire and refresh access tokens for the relevant Tenant/ Domain. This is a similar configuration to other cloud connectors (like OneDrive).

General Details – Azure Active Directory

To create or edit an Azure Identity Collector:

1. Open the Identity Collectors panel by navigating to **Admin > Identity Collectors**.
2. Click **Create New** to open the Identity Collector Configuration Wizard .

Identity Collector General Details panel

1. Select Azure Files for the type.
2. Provide a name for the Identity Corrector you are creating.
3. Click **Next**.

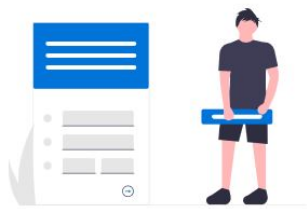
General Details

For a new Identity Collector, select an Identity Collector type and provide a name.

Wizard supported Identity Collector types do not include Cloud application Identity Collectors. Those are created through the adding application setup process in the Wizard (under the Admin tab).

If editing an existing Identity Collector, only the name can be edited.

Set up the Identity Collector type based on your system's configured identity stores. Data source Identity Collectors are based on the data sources set up in File Access Manager (under the Admin tab).



Type

Azure Active Directory ▼ *

Name *

Stacy's Test Azure

IDENTITY COLLECTOR

Step 1 of 3

Cancel

Next

Connection Details – Azure

1. Enter a valid Tenant Domain Name. Once entered, click the check mark to the right of the field.
2. Click the link under Authorization Page to enter the username and password. The user will then retrieve an authorization code.

Connection Details – (Azure) Identity Collector

Microsoft Azure Active Directory Identity Collector supports standard OAuth 2.0 Authorization for the Azure AD connector.

The authorization sequence directs the user through a standard Microsoft O365 consent flow. This grants the File Access Manager Azure AD Connector application the privilege to acquire and refresh access tokens for the relevant Tenant/ Domain. This is a similar configuration to other cloud connectors (like OneDrive).

IDENTITY COLLECTOR
Step 2 of 7

Cancel Previous Next

3. When the File Access Manager Cloud Application Authorization Service window displays, copy the code provided.

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

```
0.AVoAKouEnLpJOUyXSRGNBnF6hK0Zpts-YzFLnaK6JJX-nMVaAG0.AgABAAIAAAD--DLA3VO7QrddgJg7W
```

Press Control+C to copy the code

4. Paste the copied code into the Azure Authorization Code field.

Users Collection – Azure

Verify that the system retrieved the requested data successfully.

1. Select **Yes** or **No** to join this Identity Collector with any existing data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

Users Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.

sAMAccount...	distinguish...	proxyAddress...	displayName	userPrincipal...	depa
Administrator	CN=administr...	Administrator...	Administrator...	Administrator...	test c
Guest	CN=Guest.CN...				
__VMware_C...	CN=__VMwa...		__VMware_C...		
krbtgt	CN=krbtgt.CN...				
WHITEBOXS	CN=WHITEBO...				
wbx_ad_dec	CN=wbx_ad_d...		wbx_ad_dec	wbx_ad_dec@...	
wbx_ad_monit...	CN=wbx_ad_...		wbx_ad_monit...	wbx_ad_monit...	

Do you want to join this Identity Collector with another Data Source?

Yes

No

IDENTITY COLLECTOR
Step 3 of 7

Cancel Previous **Next**

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional.

If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources.

Join Data Sources – Users

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

4. Click **Next**.

Users - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc.). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.

Data Source

You can create a new data source in Admin > Data Sources and click Refresh. [Refresh](#)

Data Source **Local Key** **Remote Key**

Data Source ▼ * Select Value ▼ * Select Value ▼ * [+](#)

IDENTITY COLLECTOR
Step 4 of 8

[Cancel](#) [Previous](#) [Next](#) [Activate \ Go to Setting](#)

Dynamic Field Mapping (Users)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the User Dictionary Field dropdown.
2. From the Users Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Users - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Users Dictionary Field	Mapped Field
Select Field	Select Field

[+](#) [-](#)

Group Collection – Azure

Verify that the system retrieved the requested data successfully.

Note: For the Azure group data sample, File Access Manager displays each record of the sample data twice.

1. Select **Yes** or **No** to join this Identity Collector with any existing data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

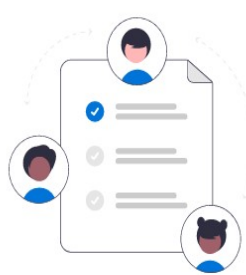
SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Req

Applications Data Sources Permissions Management Identity Collectors

Groups Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.



Review the following data sample

sAMAccount...	distinguishe...	memberOf	member	sIDHistory	obje
WinRMRemot...	CN=WinRMR...				AQU...
Administrators	CN=Administr...		CN=DanTestG...		AQIA
Users	CN=Users.CN...		CN=DaveGro...		AQIA
Guests	CN=Guests.C...		CN=Domain ...		AQIA
Print Operators	CN=Print Ope...				AQIA
Backup Opera...	CN=Backup O...		CN=administr...		AQIA
Replicator	CN=Replicato...				AQIA

Do you want to join this Identity Collector with another Data Source?

Yes

No

Cancel Previous Next

Active Directory Group Se

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional. If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional group fields from other data sources by joining those data sources.

Join Data Sources – Groups

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

4. Click **Next**.

Groups - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc.). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.

Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh. [Refresh](#)

Data Source **Local Key** **Remote Key**

Data Source Select Value Select Value

IDENTITY COLLECTOR
Step 7 of 9

[Cancel](#) [Previous](#) [Next](#)

Dynamic Field Mapping (Groups)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the Group Dictionary Field dropdown.
2. From the Groups Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Groups - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Groups Dictionary Field	Mapped Field
Select Field	Select Field

[+](#) [-](#)

IDENTITY COLLECTOR

Step 5 of 8

[Cancel](#) [Previous](#) [Next](#)

Final Configurations

On the final screen in the Identity Collector wizard, a user can set a couple of final configurations and set the scheduler task.

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.

Users Mapping Authentication

Map Accounts by Same User (Optional)

Select Field

Email Field Mapping (Optional)

proxyAddresses (If Microsoft Exchange Integration is valid)

Scheduler

Create a Schedule

Schedule Name

office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

IDENTITY COLLECTOR
Step 9 of 9

Cancel Previous Save Save & Run

Users Collection

The following final configurations are optional:

- Unique User Accounts Mapping – used to connect the Authentication Store Identity Collector to other Identity Collectors by setting the Same User Field between two or more Identity Collectors, mainly clouds Identity collectors, which extends the Access Request's Usage list.

Scheduler

If you wish to create a scheduled task, check the **Create a Schedule** toggle and complete the following:

1. Provide a name for the schedule.
2. The Scheduler is Active by default. If you wish to turn the schedule task inactive, switch the toggle to Inactive.
3. If you are wanting to start the Identity Collector process immediately, select **Schedule**. If you want to schedule the Identity Collector after a specific task completes, select **Run After**.

Note: If Run After is selected, all Schedule options will disappear.

4. Select how frequent you want the Identity Collector task to run.

- Once – one time run. Verify the date selected is in the future
 - Hourly – select the time and date for the run. Verify the date selected is in the future. Either select a specific end date or select **Never**
 - Daily – same as hourly
 - Weekly (Set as default) – select a day or multiple days for recurring runs. Either select a specific end date or select **Never**
 - Monthly – same as hourly
 - Quarterly – same as hourly
 - Half Yearly – same as hourly
 - Yearly – same as hourly
5. If you want the task to end on a specific future date, select **On** and then provide the ending date. If the task should run without an end date, select **Never**.
 6. Click **Save** to store the Identity Collector without running synchronization.

OR

7. Click **Save & Run** to create and synchronize the Identity Collector.

The screenshot displays the SailPoint Admin interface for configuring an Identity Collector. The top navigation bar includes 'Dashboard', 'Resources', 'My Tasks', 'Reports', 'Compliance', 'Forensics', 'Goals', 'Settings', and 'Admin'. The main navigation bar shows 'Applications', 'Data Sources', 'Permissions Management', and 'Identity Collectors'. The 'Final Configurations' section provides instructions and a diagram. The 'Scheduler' configuration panel is open, showing the following settings:

- Create a Schedule:**
- Schedule Name:** office.whitebox.forest Identity Collector - Identity collector Scheduler
- Active:**
- Frequency Type:** Once
- Once Recurrence:**
 - Time (UTC):** 09 : 26 AM
 - Start Date:** 08/07/2022
- Summary:** Once starts on Aug 7, 2022 at 9:26 AM

At the bottom of the configuration panel, there are buttons for 'Cancel', 'Previous', 'Save', and 'Save & Run'. The status bar at the bottom indicates 'IDENTITY COLLECTOR Step 7 of 7'.

NIS Overview

The NIS Identity Collector is used in Linux and Unix environments to collect user's and group's existing data.

General Details – NIS

To create or edit an NIS Identity Collector:

1. Open the Identity Collectors panel by navigating to **Admin > Identity Collectors**.
2. Click **Create New** to open the Identity Collector Configuration Wizard .

Identity Collector General Details panel

1. Select NIS for the Type.
2. Provide a name for the Identity Corrector you are creating.
3. Click **Next**.

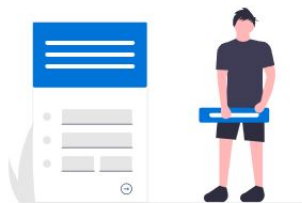
General Details

For a new Identity Collector, select an Identity Collector type and provide a name.

Wizard supported Identity Collector types do not include Cloud application Identity Collectors. Those are created through the adding application setup process in the Wizard (under the Admin tab).

If editing an existing Identity Collector, only the name can be edited.

Set up the Identity Collector type based on your system's configured identity stores. Data source Identity Collectors are based on the data sources set up in File Access Manager (under the Admin tab).



Type

 ▼ *

Name *

IDENTITY COLLECTOR

Step 1 of 3

Cancel

Next

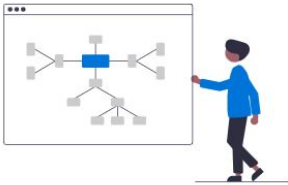
Connection Details – NIS

1. Provide the following information:

- NIS Server Address
- Username
- Password
- Port

Connection Details – (NIS) Identity Collector

NIS Identity Collector is used in Linux/Unix environments. Fill in the needed parameters in order to continue.



NIS Server Address *

Username *

Password *

SSH

Port *

IDENTITY COLLECTOR

Step 2 of 3

Cancel

Previous

Next

Users Collection – NIS

Verify that the system retrieved the requested data successfully.

Note: Only the first ten results will display.

1. Select **Yes** or **No** to join this data source to other data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

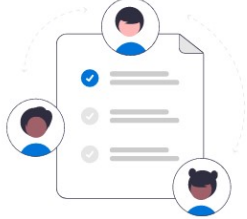
SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Request

Applications Data Sources Permissions Management Identity Collectors

Users Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.



Review the following data sample

sAMAccount...	distinguishe...	proxyAddres...	displayName	userPrincipal...	depa
Administrator	CN=administr...	Administrator...	Administrator...	Administrator...	test c
Guest	CN=Guest.CN...				
__VMware_C...	CN=__VMwa...		__VMware_C...		
krbtgt	CN=krbtgt.CN...				
WHITEBOX\$	CN=WHITEBO...				
wbx_ad_dec	CN=wbx_ad_d...		wbx_ad_dec	wbx_ad_dec@...	
wbx_ad_monit...	CN=wbx_ad_...		wbx_ad_monit...	wbx_ad_monit...	

Do you want to join this Identity Collector with another Data Source?

Yes

No

Activate Wir
Go to Settings t

IDENTITY COLLECTOR
Step 3 of 7

Cancel Previous **Next**

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional.

If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources.

Join Data Sources – Users

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

4. Click **Next**.

SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Request


Applications Data Sources Permissions Management Identity Collectors

Users - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc.). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.



Data Source

You can create a new data source in Admin > Data Sources and click Refresh. Refresh ↻

Data Source	Local Key	Remote Key	
Data Source ▼ *	Select Value ▼ *	Select Value ▼ *	🗑️

IDENTITY COLLECTOR
Step 4 of 8

Cancel Previous Next Activate \ Go to Setting

Dynamic Field Mapping (Users)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the User Dictionary Field dropdown.
2. From the Users Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Users - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Users Dictionary Field	Mapped Field
Select Field	Select Field

[+](#) [-](#)

Group Collection – NIS

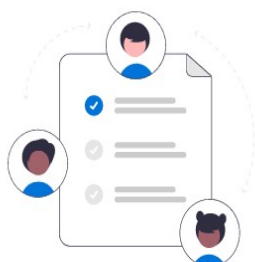
Verify that the system retrieved the requested data successfully.

1. Select **Yes** or **No** to join this data source to other data sources. A user may want to join data sources in order to gain additional attributes that can be configured to the Identity Collector.

Groups Collection

This table displays the first fetched results from the connected Identity Collectors or for Cloud connected applications, for either Users or Groups.

Active Directory Identity Collectors also display fetched properties. To complete the Identity Collector enrichment, map the fetched properties in the Dynamic Field Mapping step.



Review the following data sample

sAMAccount...	distinguishe...	memberOf	member	sIDHistory	obje
WinRMRemot...	CN=WinRMR...				AQU...
Administrators	CN=Administr...		CN=DanTestG...		AQIA
Users	CN=Users,CN...		CN=DaveGro...		AQIA
Guests	CN=Guests,C...		CN=Domain ...		AQIA
Print Operators	CN=Print Ope...				AQIA
Backup Opera...	CN=Backup O...		CN=administr...		AQIA
Replicator	CN=Replicato...				AQIA

Do you want to join this Identity Collector with another Data Source?

Yes

No

IDENTITY COLLECTOR
Step 6 of 8

Cancel Previous **Next** Activa
Go to Se

If you select **No** to joining data sources, click **Next** to be taken to the Dynamic Field Mapping screen, which is optional. If you select **Yes** to joining data sources, you can use one of the Identity Collector fields as the local key to gather additional group fields from other data sources by joining those data sources.

Join Data Sources – Groups

Complete the following:

1. Select the desired data source you want to join with from the first drop down.
2. Select a Local Key you want to join.
3. Select a Remote Key you want to join it to.

Note: Click the plus icon to join more data sources.

4. Click **Next**.

SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings Admin New Access Requ

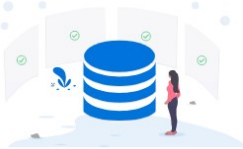
Applications Data Sources Permissions Management Identity Collectors

Groups - Join Data Sources

To join a Data Source for either users or groups, first select the appropriate Data Source from the predefined list (i.e. HR DB, IIQ, etc). Next, map between the Data Source values from the Remote Key to the Local Key, which includes the Identity Collector's default properties. For an Active Directory Identity Collector, this also includes fetched properties.

The joined Data Sources are the foundation for gathering additional fields that could be configured to the Identity Collector in the Dynamic Fields Mapping (next step).

Joining Data Sources is not mandatory. You can skip it by deleting all the Data Source rows.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh. Refresh ↻

Data Source	Local Key	Remote Key	
Data Source ▼ *	Select Value ▼ *	Select Value ▼ *	🗑️

IDENTITY COLLECTOR
Step 7 of 9

Cancel Previous Next Activat Go to Set

Dynamic Field Mapping (Groups)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the Group Dictionary Field dropdown.
2. From the Groups Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.**Groups - Dynamic Fields Mapping (optional)**

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Groups Dictionary Field

Select Field
▼

Mapped Field

Select Field
▼

+
-

IDENTITY COLLECTOR

Step 5 of 8

Cancel

Previous

Next

Final Configurations

On the final screen in the Identity Collector wizard, a user can set a couple of final configurations and set the scheduler task.

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.

Users Mapping Authentication

Map Accounts by Same User (Optional)
Select Field

Email Field Mapping (Optional)
proxyAddresses (If Microsoft Exchange Integration is valid)

Scheduler

Create a Schedule

Schedule Name
office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

IDENTITY COLLECTOR
Step 9 of 9

Cancel Previous Save Save & Run

Users Collection

The following final configurations are optional:

- Unique User Accounts Mapping – used to connect the Authentication Store Identity Collector to other Identity Collectors by setting the Same User Field between two or more Identity Collectors, mainly clouds Identity collectors, which extends the Access Request's Usage list.

Scheduler

If you wish to create a scheduled task, check the **Create a Schedule** toggle and complete the following:

1. Provide a name for the schedule.
2. The Scheduler is Active by default. If you wish to turn the schedule task inactive, switch the toggle to Inactive.
3. If you are wanting to start the Identity Collector process immediately, select **Schedule**. If you want to schedule the Identity Collector after a specific task completes, select **Run After**.

Note: If Run After is selected, all Schedule options will disappear.

4. Select how frequent you want the Identity Collector task to run.

- Once – one time run. Verify the date selected is in the future
 - Hourly – select the time and date for the run. Verify the date selected is in the future. Either select a specific end date or select **Never**
 - Daily – same as hourly
 - Weekly (Set as default) – select a day or multiple days for recurring runs. Either select a specific end date or select **Never**
 - Monthly – same as hourly
 - Quarterly – same as hourly
 - Half Yearly – same as hourly
 - Yearly – same as hourly
5. If you want the task to end on a specific future date, select **On** and then provide the ending date. If the task should run without an end date, select **Never**.
 6. Click **Save** to store the Identity Collector without running synchronization.

OR

7. Click **Save & Run** to create and synchronize the Identity Collector.

SailPoint Dashboard Resources My Tasks Reports Compliance Forensics Goals Settings **Admin**

Applications Data Sources Permissions Management Identity Collectors

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.

Scheduler

Create a Schedule

Schedule Name *
office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

Frequency Type
Once

Once Recurrence
Time (UTC) *
09 : 26 AM

Start Date *
08/07/2022

Summary: Once starts on Aug 7, 2022 at 9:26 AM

IDENTITY COLLECTOR
Step 7 of 7

Cancel Previous Save Save & Run

Data Source Overview

The Data Source Identity Collector is based on already configured Data Sources.

Depending on what is needed, the Data Source fields are configured by mapping them to the mandatory and optional fields.

You can map Data Source Identity Collector relationships between users, groups, user memberships within a group, and by group hierarchies.

General Details – Data Source

To create or edit a Data Source Identity Collector:

1. Open the Identity Collectors panel by navigating to **Admin > Identity Collectors**.
2. Click **Create New** to open the Identity Collector Configuration Wizard .

Identity Collector General Details panel

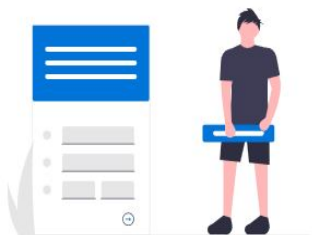
1. Select Data Source as the Type.
2. Provide a name for the Identity Corrector you are creating.
3. Within the Advanced Options section, the option to set up Groups is automatically selected. Select if you want to set the Groups Hierarchy.
4. Click **Next**.

General Details

When creating a new Identity Collector, select an Identity Collector type based on your system's configured Identity Stores and provide a name.

Wizard supported Identity Collector types do not include Cloud application Identity Collectors. Those are created through the adding application setup process in the Wizard (under the Admin tab).

If editing an existing Identity Collector, all fields except for the Type field are editable.



Type

Data Source ▼ *

Name *

Enter the Identity Collector name

Advanced Options ⓘ

Do you want to set Groups?

Do you want to set Groups Hierarchy?

IDENTITY COLLECTOR

Step 1 of 7

Cancel

Next

Connection Details (Users) – Data Source

This is the first of four connection screens for data source.

1. From the drop down, select an already existing data source you wish to connect to.

Note: If a data source is recently created, click the **Refresh** button to view the newly created data source from the drop down.

2. From the Username dropdown, select the appropriate username.
3. If needed, you can map additional data in the Optional Field to the system default properties. This mapped data from the data source will be saved in the database.

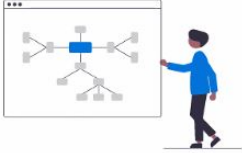
Applications Data Sources Permissions Management Identity Collectors

Connection Details - (Data Source) Identity Collector

The Data Source Identity Collector is based on already configured Data Sources.

Depending on what is needed, the Data Source fields are configured by mapping them to the mandatory and optional fields.

You can map Data Source Identity Collector relationships between users, groups, user memberships within a group, and by group hierarchies.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click **Refresh**.

Data Source

Users - Field Mapping

Map mandatory and optional fields to the relevant Data Source values.

Username

Optional Field **Value**

IDENTITY COLLECTOR
Step 2 of 3

Dynamic Field Mapping (Users)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the User Dictionary Field dropdown.
2. From the Users Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.

Users - Dynamic Fields Mapping (optional)

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Users Dictionary Field	Mapped Field
Select Field	Select Field

[+](#) [-](#)

Connection Details (Groups) – Data Source

This screen only displays if the Groups toggle was selected in the General Details screen.

This is the second of four connection screens for data source.

1. From the drop down, select an already existing data source you wish to connect to.

Note: If a data source is created, click the **Refresh** button to view the newly created data source from the drop down.

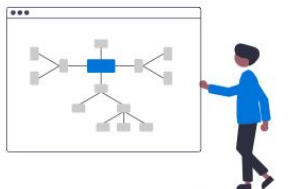
2. From the Group Name dropdown, select a mandatory value to be mapped to the data source.
3. If needed, you can map additional data in the Optional Field to the system default properties. This mapped data from the data source will be saved in the database.

Connection Details - (Data Source) Identity Collector

The Data Source Identity Collector is based on already configured Data Sources.

Depending on what is needed, the Data Source fields are configured by mapping them to the mandatory and optional fields.

You can map Data Source Identity Collector relationships between users, groups, user memberships within a group, and by group hierarchies.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh.

 ▼ * Refresh

Groups - Field Mapping

Map mandatory and optional fields to the relevant Data Source values.

Group Name

 ▼ *

Optional Field	Value
<input type="text" value="Select Field"/> ▼	<input type="text" value="Select Value"/> ▼

+ 🗑️

IDENTITY COLLECTOR
Step 4 of 8

Cancel Previous Next

Dynamic Field Mapping (Groups)

This feature allows the user to rename the previously fetched properties by mapping them to a dictionary field, and therefore changing their name.

Note: Dynamic Field Mapping is not mandatory.

1. To create a new data dictionary field, use the link provided. Once created, click **Refresh** to have the new data dictionary field display in the Group Dictionary Field dropdown.
2. From the Groups Dictionary Field dropdown, select a mapped property.
3. From the Mapped Field dropdown, select a value that is to be mapped to the new data dictionary field.

Note: To add more dictionaries, click the plus icon.

4. Click **Next**.**Groups - Dynamic Fields Mapping (optional)**

Each type of Identity Collector fetches a different default set of properties for both users and groups.

The Dynamic Fields Mapping allows renaming the fetched properties by mapping them to a Dictionary field.

It can also be used to enrich the Identity Collector (not including Data Source type) by mapping additional fields based on either Joined Data Sources, which were predefined in the previous wizard screen, or by mapping predefined Properties to Fetch (for Active Directory only).

Dynamic Field Mapping is not mandatory. You can skip it by leaving the fields empty or deleting them.



Data Dictionary Fields

You can create a new User or Group Type Dictionary in [Admin > Permission Management > New Data Dictionary Field](#) and click Refresh.

[Refresh](#)

Groups Dictionary Field	Mapped Field
Select Field ▼	Select Field ▼

+
🗑️

IDENTITY COLLECTOR

Step 5 of 8

Cancel

Previous

Next

Connection Details (User Membership in Groups) – Data Source

This screen only displays if the Groups toggle was selected in the General Details screen.

This is the third of four connection screens for data source.

1. From the drop down, select an already existing data source you wish to connect to.

Note: If a data source is created, click the **Refresh** button to view the newly created data source from the drop down.

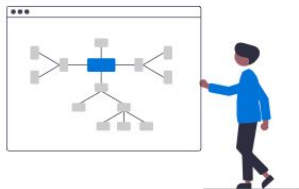
2. From the Group Name and Username dropdown, select the appropriate value.
3. From the Group Name dropdown, select a mandatory value to be mapped to the data source.
4. If needed, you can map additional data in the Optional Field to the system default properties. This mapped data from the data source will be saved in the database.

Connection Details - (Data Source) Identity Collector

The Data Source Identity Collector is based on already configured Data Sources.

Depending on what is needed, the Data Source fields are configured by mapping them to the mandatory and optional fields.

You can map Data Source Identity Collector relationships between users, groups, user memberships within a group, and by group hierarchies.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh.

Data Source

User membership in groups - Field Mapping

Map mandatory and optional fields to the relevant Data Source values.

Group Name	<input type="text" value="Select Value"/>	Username	<input type="text" value="Select Value"/>
Optional Field	<input type="text" value="Select Field"/>	Value	<input type="text" value="Select Value"/>

IDENTITY COLLECTOR
Step 6 of 8

Connection Details (Group Hierarchy) – Data Source

This screen only displays if the Groups toggle and the Group Hierarchy toggle were selected in the General Details screen.

This is the final screen when connecting data sources.

1. From the drop down, select an already existing data source you wish to connect to.

Note: If a data source is created, click the **Refresh** button to view the newly created data source from the drop down.

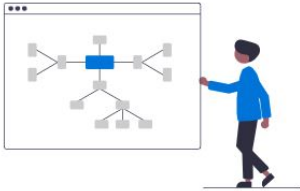
2. From the Child Group Name and Parent Group Name dropdown, select the appropriate value.
3. If needed, you can map additional data in the Optional Field to the system default properties. This mapped data from the data source will be saved in the database.

Connection Details - (Data Source) Identity Collector

The Data Source Identity Collector is based on already configured Data Sources.

Depending on what is needed, the Data Source fields are configured by mapping them to the mandatory and optional fields.

You can map Data Source Identity Collector relationships between users, groups, user memberships within a group, and by group hierarchies.



Data Source

You can create a new data source in [Admin > Data Sources](#) and click Refresh.

 ▼ * Refresh

Groups Hierarchy - Field Mapping

Map mandatory and optional fields to the relevant Data Source values.

Child Group Name	Parent Group Name
<input type="text" value="Select Value"/> ▼ *	<input type="text" value="Select Value"/> ▼ *
Optional Field	Value
<input type="text" value="Select Field"/> ▼	<input type="text" value="Select Value"/> ▼

+
🗑️

IDENTITY COLLECTOR

Step 7 of 8

Cancel

Previous

Next

Final Configurations

On the final screen in the Identity Collector wizard, a user can set a couple of final configurations and set the scheduler task.

Final Configurations

We recommend creating a Schedule to keep an updated Identity Collector.

For Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard.

Users Mapping Authentication

Map Accounts by Same User (Optional)
Select Field

Email Field Mapping (Optional)
proxyAddresses (If Microsoft Exchange Integration is valid)

Scheduler

Create a Schedule

Schedule Name
office.whitebox.forest Identity Collector - Identity collector Scheduler

Active

Schedule Run After

IDENTITY COLLECTOR
Step 9 of 9

Cancel Previous Save Save & Run

Users Collection

The following final configurations are optional:

- Unique User Accounts Mapping – used to connect the Authentication Store Identity Collector to other Identity Collectors by setting the Same User Field between two or more Identity Collectors, mainly clouds Identity collectors, which extends the Access Request's Usage list.

Scheduler

If you wish to create a scheduled task, check the **Create a Schedule** toggle and complete the following:

1. Provide a name for the schedule.
2. The Scheduler is Active by default. If you wish to turn the schedule task inactive, switch the toggle to Inactive.
3. If you are wanting to start the Identity Collector process immediately, select **Schedule**. If you want to schedule the Identity Collector after a specific task completes, select **Run After**.

Note: If Run After is selected, all Schedule options will disappear.

4. Select how frequent you want the Identity Collector task to run.

- Once – one time run. Verify the date selected is in the future
 - Hourly – select the time and date for the run. Verify the date selected is in the future. Either select a specific end date or select **Never**
 - Daily – same as hourly
 - Weekly (Set as default) – select a day or multiple days for recurring runs. Either select a specific end date or select **Never**
 - Monthly – same as hourly
 - Quarterly – same as hourly
 - Half Yearly – same as hourly
 - Yearly – same as hourly
5. If you want the task to end on a specific future date, select **On** and then provide the ending date. If the task should run without an end date, select **Never**.
 6. Click **Save** to store the Identity Collector without running synchronization.

OR

7. Click **Save & Run** to create and synchronize the Identity Collector.

The screenshot displays the SailPoint Admin interface for configuring an Identity Collector. The top navigation bar includes 'SailPoint', 'Dashboard', 'Resources', 'My Tasks', 'Reports', 'Compliance', 'Forensics', 'Goals', 'Settings', and 'Admin'. The main navigation menu shows 'Applications', 'Data Sources', 'Permissions Management', and 'Identity Collectors'. The 'Final Configurations' section provides instructions on creating a schedule and notes that for Cloud Identity Collectors, the Permissions Collector Scheduler can be set from the Application's wizard. A diagram illustrates the data flow between components. The 'Scheduler' configuration panel is open, showing the following settings:

- Create a Schedule:**
- Schedule Name:** office.whitebox.forest Identity Collector - Identity collector Scheduler
- Active:**
- Frequency Type:** Once
- Once Recurrence:** Time (UTC) 09 : 26 AM
- Start Date:** 08/07/2022
- Summary:** Once starts on Aug 7, 2022 at 9:26 AM

At the bottom of the configuration panel, there are buttons for 'Cancel', 'Previous', 'Save', and 'Save & Run'. The status bar at the bottom indicates 'IDENTITY COLLECTOR Step 7 of 7'.