Setting the AD groups managers (managedBy) as data owners

Content

1. Add attributes DistinguishedName and managedBy to the identity collector

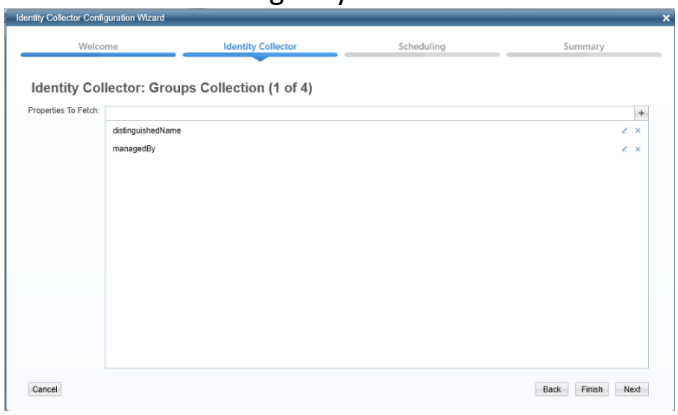
From the Admin Console, Go to Applications-Configuration-Permissions Collection-Identity Collectors.

Edit the primary domain Identity Collector.

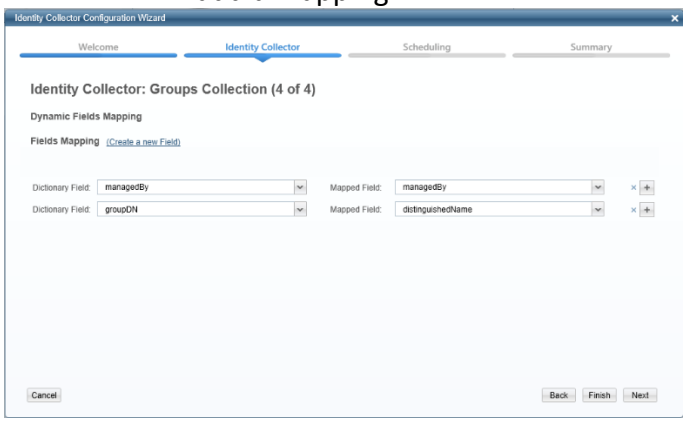
Go to Groups Collection page of the wizard.

And add the following attributes to the Properties to Fetch:

- DistinguishedName
- managedBy



add a mapping:



From the Website, run the Identity Collector Task.

2. Create a Data Source and name it “Managers for ADgroups”

Check the columns where the above info is stored in the DB

Connect to File Access Manager SQL DB and run the following query:

```
SELECT * FROM whiteops.ra_role
```

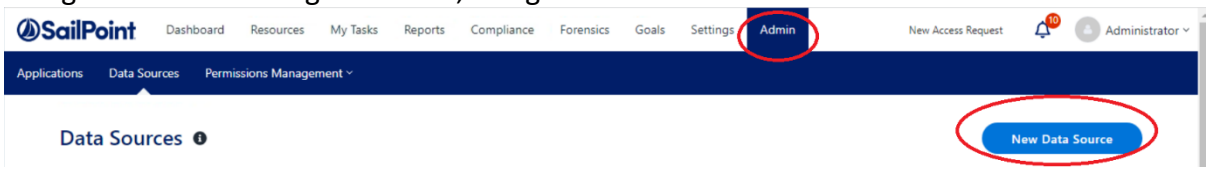
Check the titles of the columns that stores the distinguishedName and the managedBy fields. In the attached example

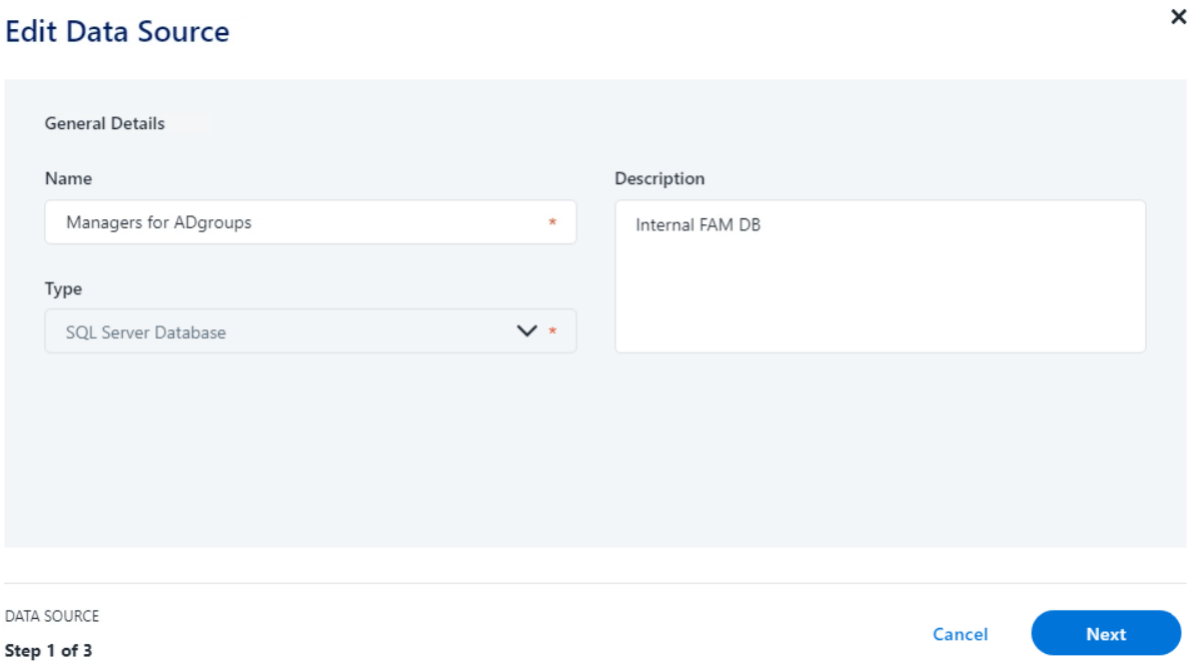
- distinguishedName appears in column role_field2
- managedBy appears in column role_field1

role_field1	role_field2
CN=Mary Johnson,OU=Austin,OU=Ame...	CN=Development,OU=Groups,OU=Demo,DC=seri,DC...
CN=Dennis Barnes,OU=Munich,OU=Eu...	CN=Employment,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Jane Grant,OU=Singapore,OU=Asi...	CN=ENG_Internal,OU=Groups,OU=Demo,DC=seri,DC...
CN=Jane Grant,OU=Singapore,OU=Asi...	CN=ENG_Mgmt,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Jane Grant,OU=Singapore,OU=Asi...	CN=ENG_Prod,OU=Groups,OU=Demo,DC=seri,DC=s...
CN=Jane Grant,OU=Singapore,OU=Asi...	CN=ENG_Stage,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Lori Ferguson,OU=Taipei,OU=Asia-...	CN=FinanceUsers,OU=Groups,OU=Demo,DC=seri,DC...
CN=Mary Johnson,OU=Austin,OU=Ame...	CN=GlobalComm,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Jane Grant,OU=Singapore,OU=Asi...	CN=globalExport,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Debra Wood,OU=Brussels,OU=Eur...	CN=HelpDesk,OU=Groups,OU=Demo,DC=seri,DC=sa...
CN=Debra Wood,OU=Brussels,OU=Eur...	CN=HostingVPN,OU=Groups,OU=Demo,DC=seri,DC=...
CN=Mary Johnson,OU=Austin,OU=Ame...	CN=InternalAudit,OU=Groups,OU=Demo,DC=seri,DC=...

Create a Data Source “SQL Server Database” type.

Using File Access Manager website, navigate to Admin





Use Case 1:

File Access Manager reads ManagedBy AD groups' attribute and set the ManagedBy to be the Owner of the group (business resource) in File Access Manager:

Insert File Access Manager SQL DB details and add the following query:

```
SELECT bs.full_path 'Group (Resource Full Path)','SERI Active Directory' AS 'Application Name','False' AS 'Allow Full Scope',ru.user_domain AS 'Owner Domain',ru.[user_name] AS 'Owner Name', 'Data Owner' AS 'Action'
FROM whiteops.ra_role rr
INNER JOIN whiteops.ra_user ru ON rr.role_field1=ru.user_full_name
INNER JOIN whiteops.business_service bs ON bs.full_path=rr.role_field2
```

Use Case 2:

This use case assumes that every folder has an exactly one security group that grants access to it. This group grants access to this folder only. We want to set the managedBy user to be FAM Owner of the AD group and Owner on the folder the group grant access to.

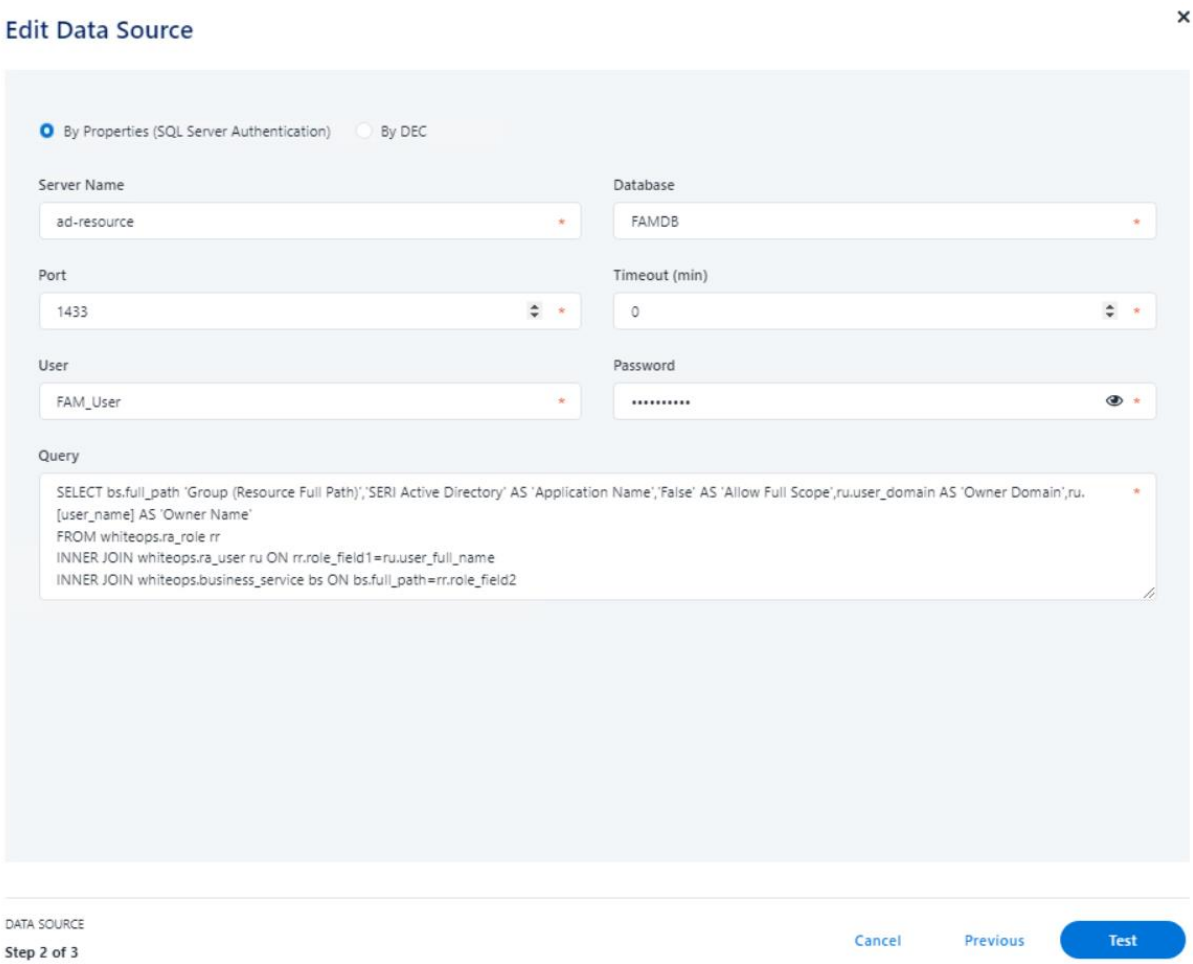
```
--Set Owners to AD group according the ManagedBy attribute
SELECT bs.full_path 'Group (Resource Full Path)','SERI Active Directory' AS 'Application Name','False' AS 'Allow Full Scope',ru.user_domain AS 'Owner Domain',ru.[user_name] AS 'Owner Name', 'Data Owner' AS 'Action'
FROM whiteops.ra_role rr
INNER JOIN whiteops.ra_user ru ON rr.role_field1=ru.user_full_name
INNER JOIN whiteops.business_service bs ON bs.full_path=rr.role_field2
UNION
--Set the AD group Owner to be the owner on the folder it grants access to
```

```
--Group starts with SecGroup-
SELECT rerv.full_path 'Resource Full Path',b.name AS 'Application Name','False' AS
'Allow Full Scope',
ru.user_domain AS 'Owner Domain',ru.[user_name] AS 'Owner Name', 'Data Owner'
AS 'Action'
  FROM [FAMDB].[whiteops].[ra_entitlements_roles_view] rerv
  LEFT JOIN whiteops.business_resource_owners_view brov ON
brov.business_service_id=rerv.bam_id
  LEFT JOIN whiteops.ra_user ru ON ru.user_full_name=rerv.role_field1
  LEFT JOIN whiteops.bam b ON b.id=rerv.bam_id
  WHERE ru.[user_name] IS NOT NULL
  AND role_name like 'SecGroup-%'   --add this line if the security groups that you'd
like to set the Owners for has a naming convention that starts with SecGroup- (or
change to the relevant naming convention)
```

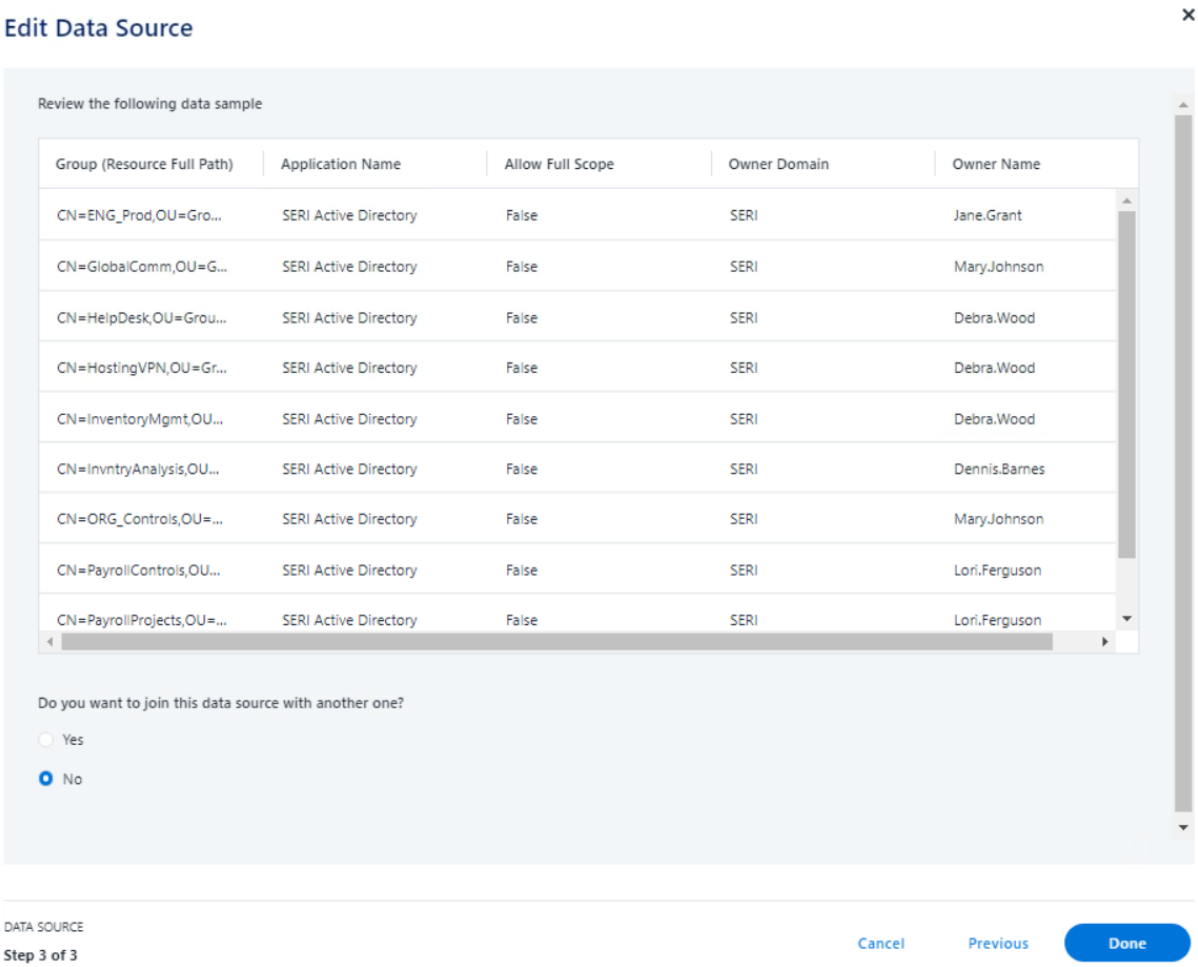
Use Case 3:

This use case assumes that every relevant folder has a security group with the same name as the folder that grants access to it. Verify there no other folders with the same name. We want to set the managedBy user to be FAM Owner of the AD group and Owner on the folder with the same name of the group.

```
--Set Owners to AD group according the ManagedBy attribute
SELECT bs.full_path 'Group (Resource Full Path)','SERI Active Directory' AS
'Application Name','False' AS 'Allow Full Scope',ru.user_domain AS 'Owner
Domain',ru.[user_name] AS 'Owner Name', 'Data Owner' AS 'Action'
FROM whiteops.ra_role rr
INNER JOIN whiteops.ra_user ru ON rr.role_field1=ru.user_full_name
INNER JOIN whiteops.business_service bs ON bs.full_path=rr.role_field2
UNION
--Set the AD group Owner to be the owner on the folder with the same name as the
group name
SELECT bs.full_path 'Resource Full Path',b.name AS 'Application Name','False' AS
'Allow Full Scope',
rr.role_domain AS 'Owner Domain',ru.[user_name] AS 'Owner Name', 'Data Owner'
AS 'Action'
  FROM whiteops.business_service bs
  LEFT JOIN whiteops.business_service bs2 ON  bs2.[name]=bs.[name]
  LEFT JOIN whiteops.ra_role rr ON bs2.name=rr.role_name
  LEFT JOIN whiteops.bam b ON bs.parent_bam_id=b.id
  LEFT JOIN whiteops.ra_user ru ON ru.user_full_name=rr.role_field1
        WHERE   bs.type_enum_id=0 --folder
        AND     bs2.type_enum_id=4 --group
        AND ru.user_name IS NOT NULL
```



Test it and verify you can see results:


Edit Data Source
Review the following data sample
Group (Resource Full Path)
Application Name
Allow Full Scope
Owner Domain
Owner Name
CN=ENG_Prod,OU=Gro...
SERI Active Directory
False
SERI
Jane.Grant
CN=GlobalComm,OU=G...
SERI Active Directory
False
SERI
Mary.Johnson
CN=HelpDesk,OU=Grou...
SERI Active Directory
False
SERI
Debra.Wood
CN=HostingVPN,OU=Gr...
SERI Active Directory
False
SERI
Debra.Wood
CN=InventoryMgmt,OU...
SERI Active Directory
False
SERI
Debra.Wood
CN=InvntryAnalysis,OU...
SERI Active Directory
False
SERI
Dennis.Barnes
CN=ORG_Controls,OU=...
SERI Active Directory
False
SERI
Mary.Johnson
CN=PayrollControls,OU...
SERI Active Directory
False
SERI
Lori.Ferguson
CN=PayrollProjects,OU=...
SERI Active Directory
False
SERI
Lori.Ferguson
Do you want to join this data source with another one?
Yes
No
DATA SOURCE
Step 3 of 3
Cancel
Previous
Done

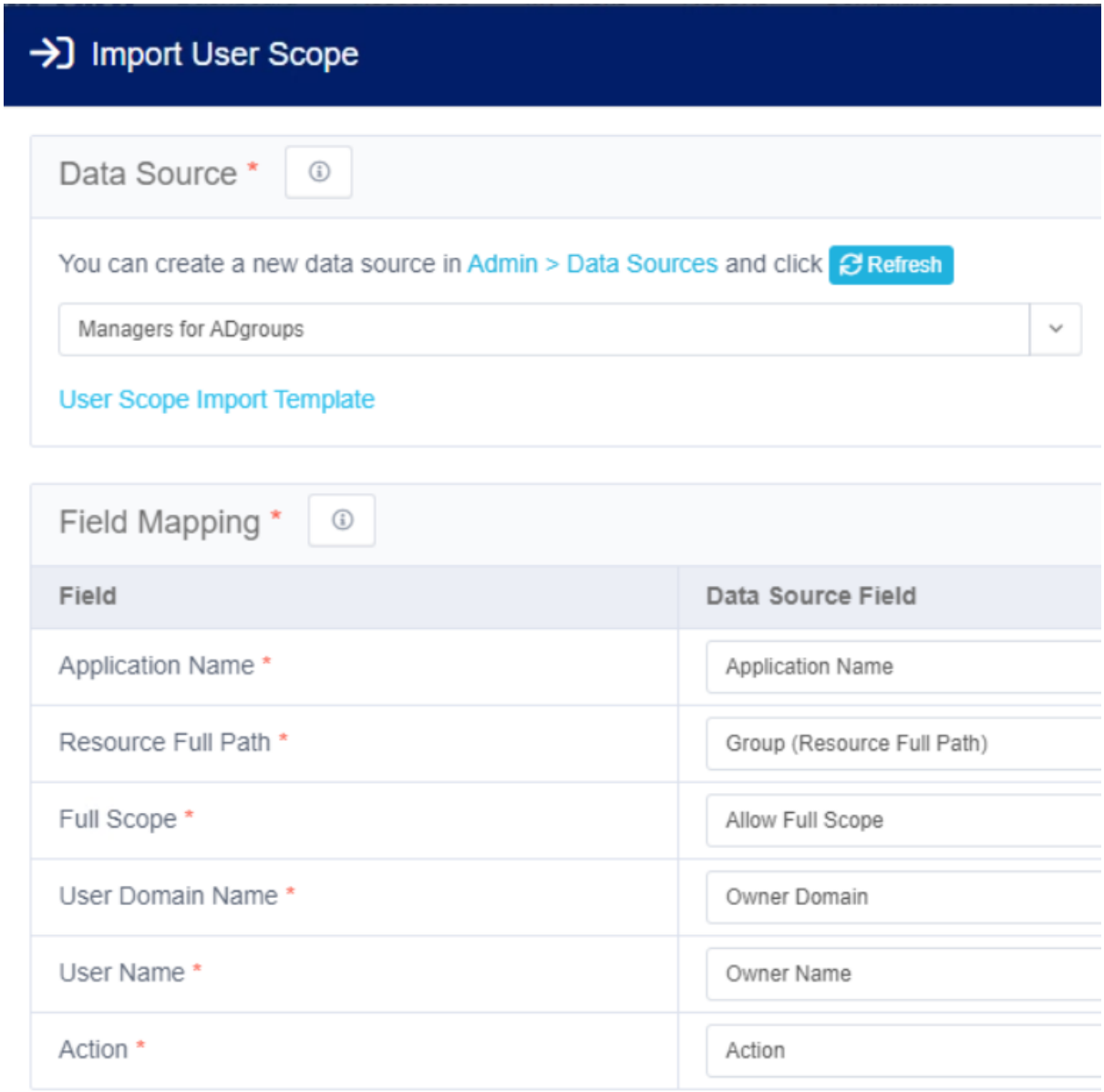
Click Done.

3. Set the Import User Scope task

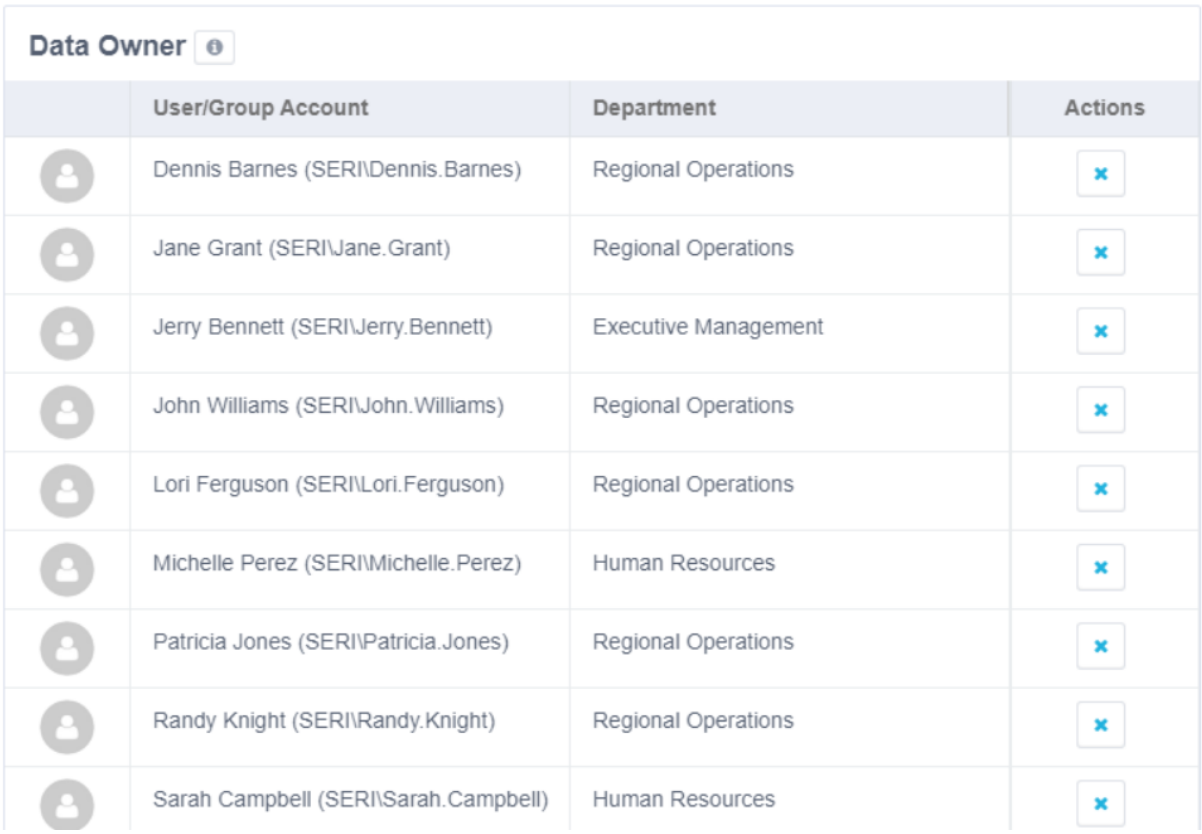
Using File Access Manager Web interface

Settings->Capabilities -> 

and set the values as appear in the screenshot

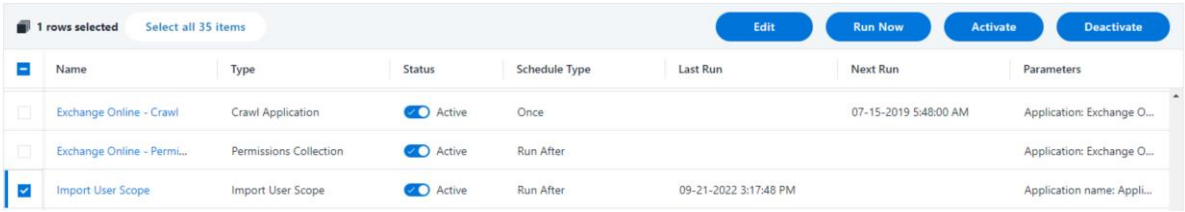


Go back to capabilities and verify you see these users as Owners:

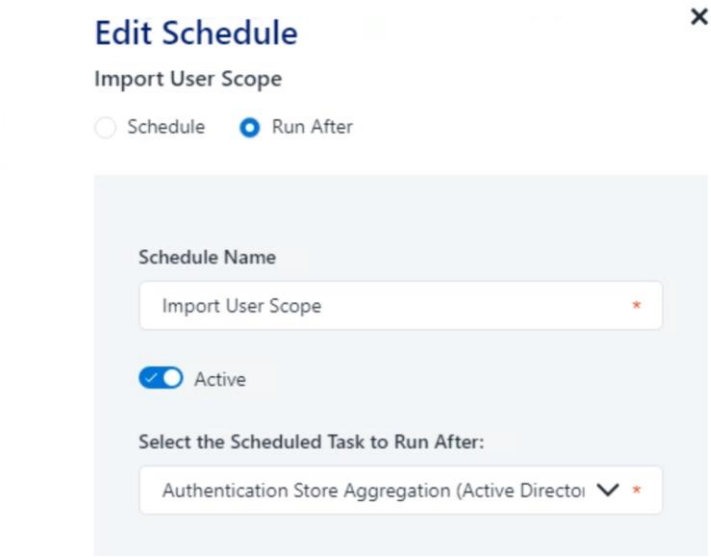


Schedule the Import User Scope task to run after the Identity collector

Go to Settings -> Task Management -> Scheduled Tasks page,
Find the Import User Scope task, check it and click Edit



Schedule it to run automatically after the Identity Collector:



Schedule the Identity Collector to run automatically on a regular basis according to your needs (Once a day / every hour / etc)

Once the Import user scope completes its run, the Owner is set the resource. However, it may take around 10 minutes to see it in the UI.

Document Revision History

Revision Date	Written/Edited By	Comments
June25nd 2017	Tom Blinder	Original document
Feb 24th 2021	Tom Blinder	Updating to 8.1 structure
Sept 19th 2022	Tom Blinder	Updating to 8.2 structure
Sept 22nd 2022	Tom Blinder	Add use cases 2 and 3 to section 2