

Setting the AD groups managers (managedBy) as data owners

Content

1. Add attributes DistinguishedName and managedBy to the identity collector	2
2. Create a Data Source and name it "Managers for ADgroups"	3
Check the columns where the above info is stored in the DB.....	3
Create a Data Source "SQL Server Database" type.	3
3. Set a Scope to the groups' owners	6
4. Grant Owner Capabilities for the imported owners	6
Document Revision History.....	8

1. Add attributes DistinguishedName and managedBy to the identity collector

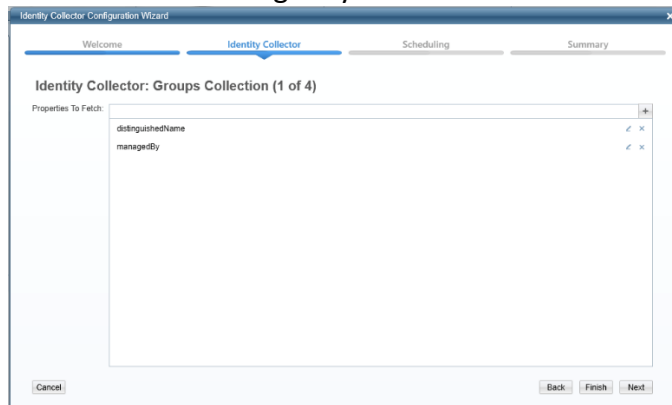
From the Admin Console, Go to Applications-Configuration-Permissions Collection-Identity Collectors.

Edit the primary domain Identity Collector.

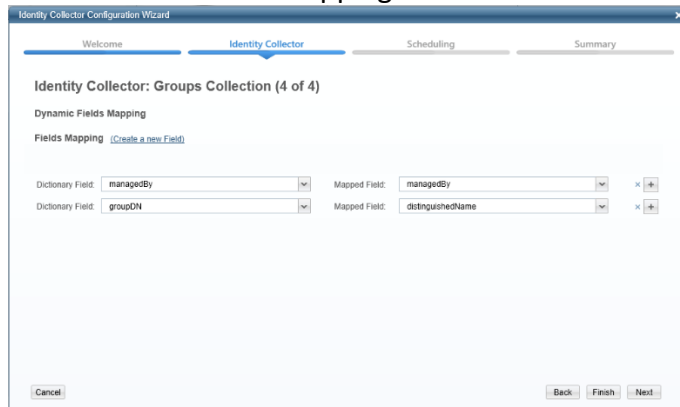
Go to Groups Collection page of the wizard.

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 SecurityIQ 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 Bames,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.

Data Source Wizard

Data sources are tables of information.
Data sources information can be imported from external sources or be based on File Access Manager reports.

General Details:

Name:

Description:

Type:

Create the query that based on SecurityIQ-Internal 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'
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
```

Data Source Wizard

Please fill in the needed parameters in order to continue

By DEC

WPC:

By Properties (SQL Server Authentication)

Server Name: Port:

Database: User:

Password: Timeout:

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'
FROM whiteops.ra_role rr
LEFT JOIN whiteops.ra_user ru ON rr.role_field1=ru.user_full_name
LEFT JOIN whiteops.business_service bs ON bs.full_path=rr.role_field2
WHERE rr.role_field1 IS NOT NULL
```

Test it and verify you can see results:

Data Source Wizard

Data Source Wizard

Please check that the requested information has been successfully fetched

Group (Resource Full Path)	Application Name	Allow Full Sco
CN=AccountingGeneral,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=AccountsPayable,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=AccountsReceivable,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=AuditMgmt,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=BenefitCommittee,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=Benefits,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=Buyer,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=campusAccess,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=CompCommittee,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False
CN=Compensation,OU=Groups,OU=Demo,DC=seri,DC=sailpointdemo,DC=com	SERI Active Directory	False

* Only the first ten results are displayed

Cancel Back Finish Next

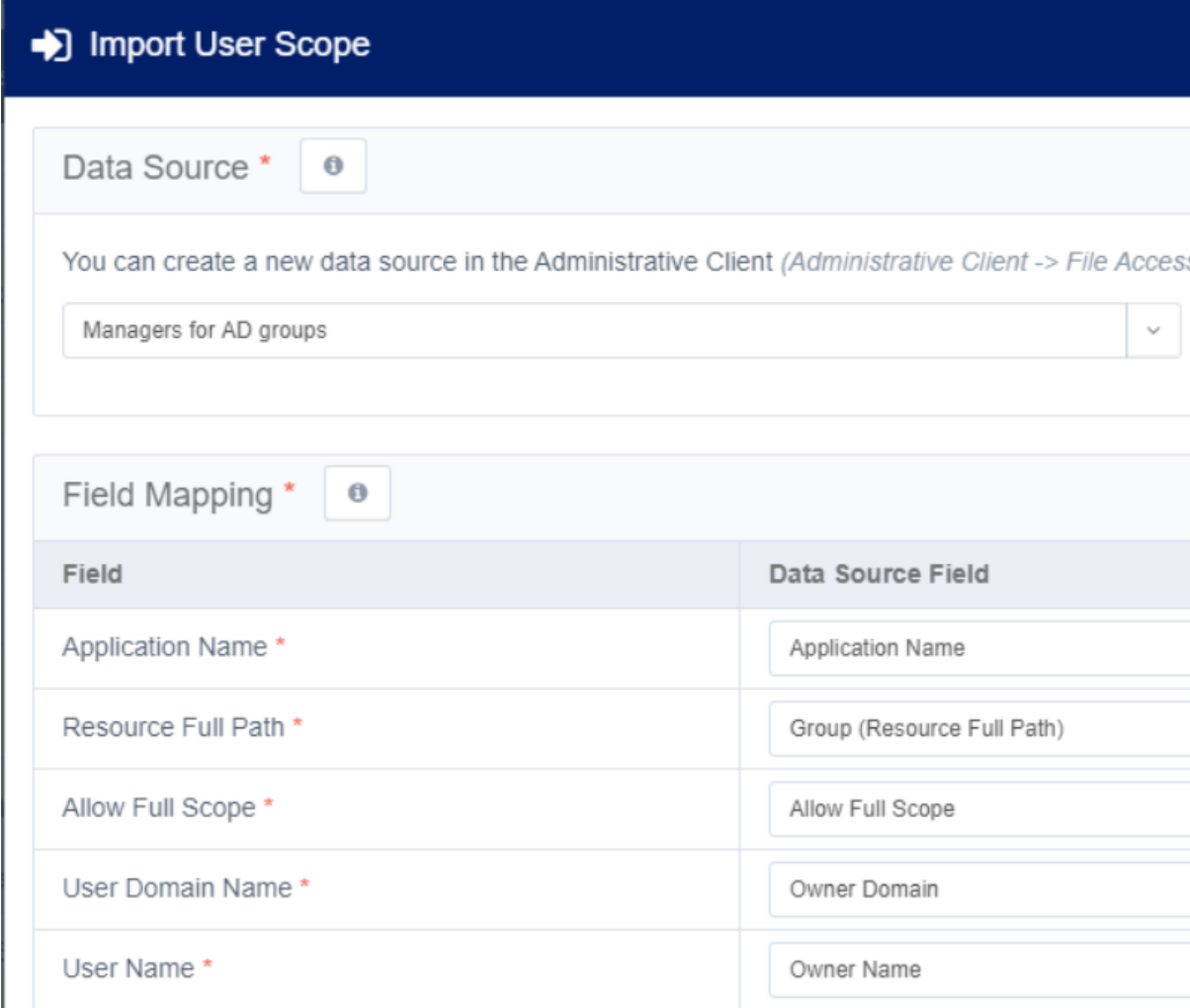
Click Finish.

3. Set a Scope to the groups' owners

Go to SecurityIQ Web interface

 Import User Scope

Settings->Capabilities -> and set the values as appear in the screenshot



Field	Data Source Field
Application Name *	Application Name
Resource Full Path *	Group (Resource Full Path)
Allow Full Scope *	Allow Full Scope
User Domain Name *	Owner Domain
User Name *	Owner Name

4. Grant Owner Capabilities for the imported owners

Login to FAM SQL DB and run the following script"

```
INSERT INTO [whiteops].[web_role_ra_user](ra_user_id,web_role_id)
SELECT DISTINCT(ru.id), 3 -- the number 3 means Data Owner capability
FROM whiteops.ra_role rr
INNER JOIN whiteops.ra_user ru On rr.role_field1=ru.user_full_name
```

Verify you see these users as Owners:

Data Owner ⓘ

	User/Group Account	Department	Actions
	Dennis Barnes (SERI\Dennis.Barnes)	Regional Operations	
	Jane Grant (SERI\Jane.Grant)	Regional Operations	
	Jerry Bennett (SERI\Jerry.Bennett)	Executive Management	
	John Williams (SERI\John.Williams)	Regional Operations	
	Lori Ferguson (SERI\Lori.Ferguson)	Regional Operations	
	Michelle Perez (SERI\Michelle.Perez)	Human Resources	
	Patricia Jones (SERI\Patricia.Jones)	Regional Operations	
	Randy Knight (SERI\Randy.Knight)	Regional Operations	
	Sarah Campbell (SERI\Sarah.Campbell)	Human Resources	

