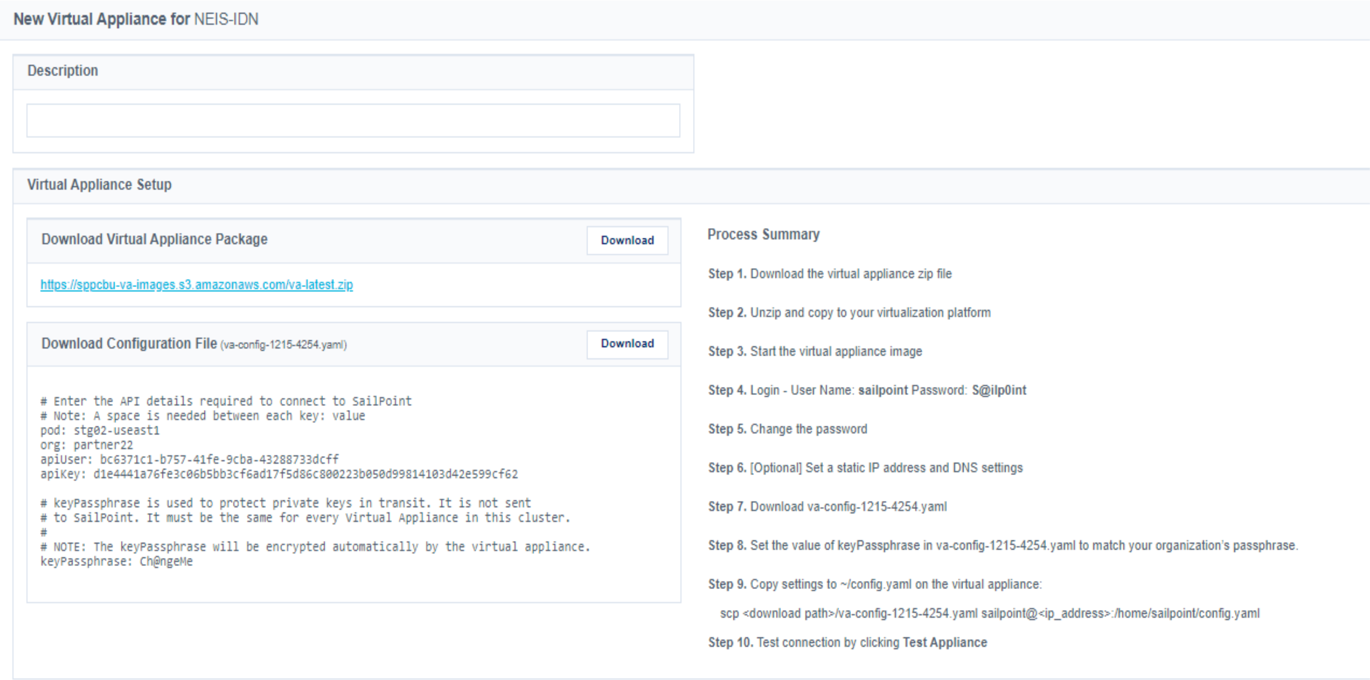
NEIS – IDN LDAP Integration

This document describes the integration of Non-Employee Identity Suite (NEIS) with Identity Now (IDN) using LDAP source type

Pre-requisite – NEIS is installed on server with trusted certificate, refer NEIS user guide for more information.

A. Configuration of Virtual Appliance: Following are the steps for setting up VA for IDN

   i. Login to partner url - https://partner22.identitynow.com/ui/admin#admin:dashboard:overview
   ii. Navigate to Connections –> Virtual Appliances
   iii. Click on New
   iv. Provide name and description
   v. Go to the next tab "Virtual Appliances"
   vi. Click on New button
   vii. Follow steps as per below screen-shot



New Virtual Appliance for NEIS-IDN

Description

Virtual Appliance Setup

Download Virtual Appliance Package

https://sppcbu-va-images.s3.amazonaws.com/va-latest.zip

Download Configuration File (va-config-1215-4254.yaml)

```
# Enter the API details required to connect to SailPoint
# Note: A space is needed between each key: value
pod: stg02-useast1
org: partner22
apiUser: bc6371c1-b757-41fe-9cba-43288733dcff
apiKey: d1e4441a76fe3c06b5bb3cf6ad17f5d86c800223b050d99814103d42e599cf62

# keyPassphrase is used to protect private keys in transit. It is not sent
# to SailPoint. It must be the same for every Virtual Appliance in this cluster.
#
# NOTE: The keyPassphrase will be encrypted automatically by the virtual appliance.
keyPassphrase: Ch@ngeMe
```

Process Summary

Step 1. Download the virtual appliance zip file

Step 2. Unzip and copy to your virtualization platform

Step 3. Start the virtual appliance image

Step 4. Login - User Name: **sailpoint** Password: **S@ilp0int**

Step 5. Change the password

Step 6. [Optional] Set a static IP address and DNS settings

Step 7. Download va-config-1215-4254.yaml

Step 8. Set the value of keyPassphrase in va-config-1215-4254.yaml to match your organization's passphrase.

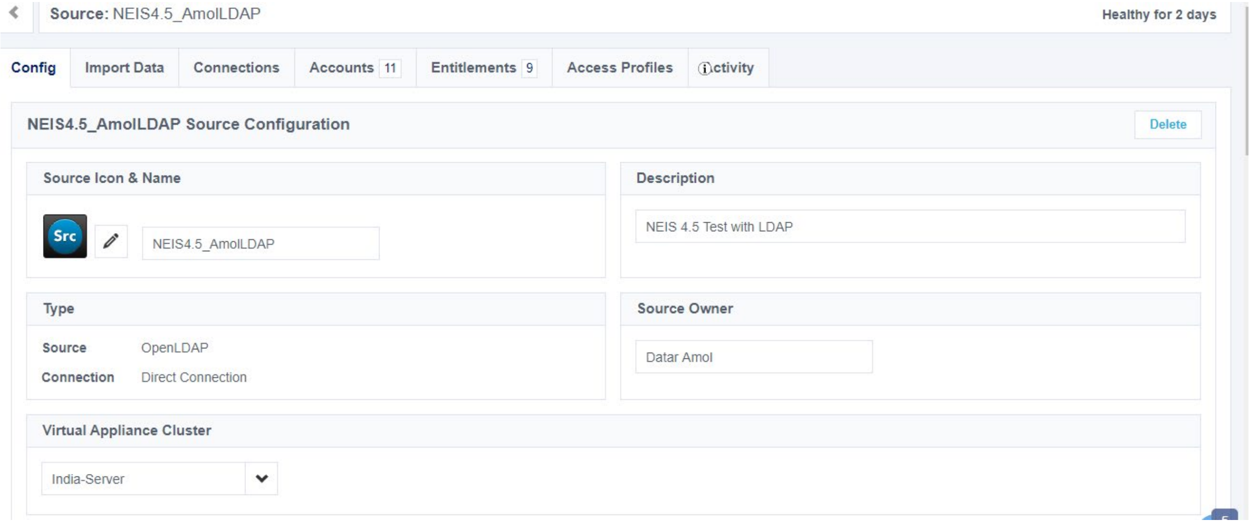
Step 9. Copy settings to ~/config.yaml on the virtual appliance:

```
scp <download path>/va-config-1215-4254.yaml sailpoint@<ip_address>:/home/sailpoint/config.yaml
```

Step 10. Test connection by clicking **Test Appliance**

B. Configure OPEN LDAP Connector – Following are the steps for setting up OPEN LDAP Connector in IDN

i. Click on Admin
ii. Go to Connections - Virtual Appliances, click on India-Server and click on Virtual Appliances and check the status
iii. Click on Connections - Source to configure connector
iv. Click new and setup Open LDAP
v. Click on Save
vi. Select Virtual Appliance Cluster - India-server
vii. Connection Settings - cn=Directory Manager,dc=system,dc=backend, testpass, host - 10.0.85.91, port – 6389
(This information is available on server were NEIS is installed at location \config\conf\IdPortal.json in “LdapServerConfig”)
viii. Group Membership Attribute - uniqueMember
ix. Account Settings: Search Scope - Subtree, Search DN = dc=system,dc=backend
x. Group Settings: Search Scope - Subtree, Search DN = dc=system,dc=backend
xi. Save and click on Test Connection



Source: NEIS4.5_AmolLDAP

NEIS4.5_AmolLDAP Source Configuration

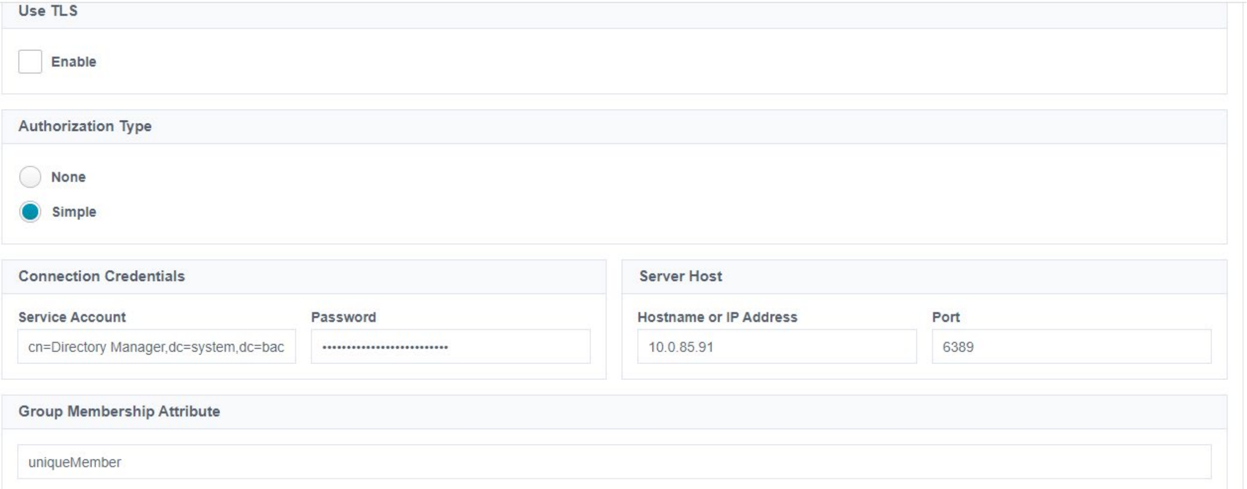
Source Icon & Name: NEIS4.5_AmolLDAP

Description: NEIS 4.5 Test with LDAP

Type
Source: OpenLDAP
Connection: Direct Connection

Source Owner: Datar Amol

Virtual Appliance Cluster: India-Server



Use TLS

□ Enable

Authorization Type

○ None

● Simple

Connection Credentials

Service Account: cn=Directory Manager,dc=system,dc=bac

Password: ••••••••••••••••••••••••••

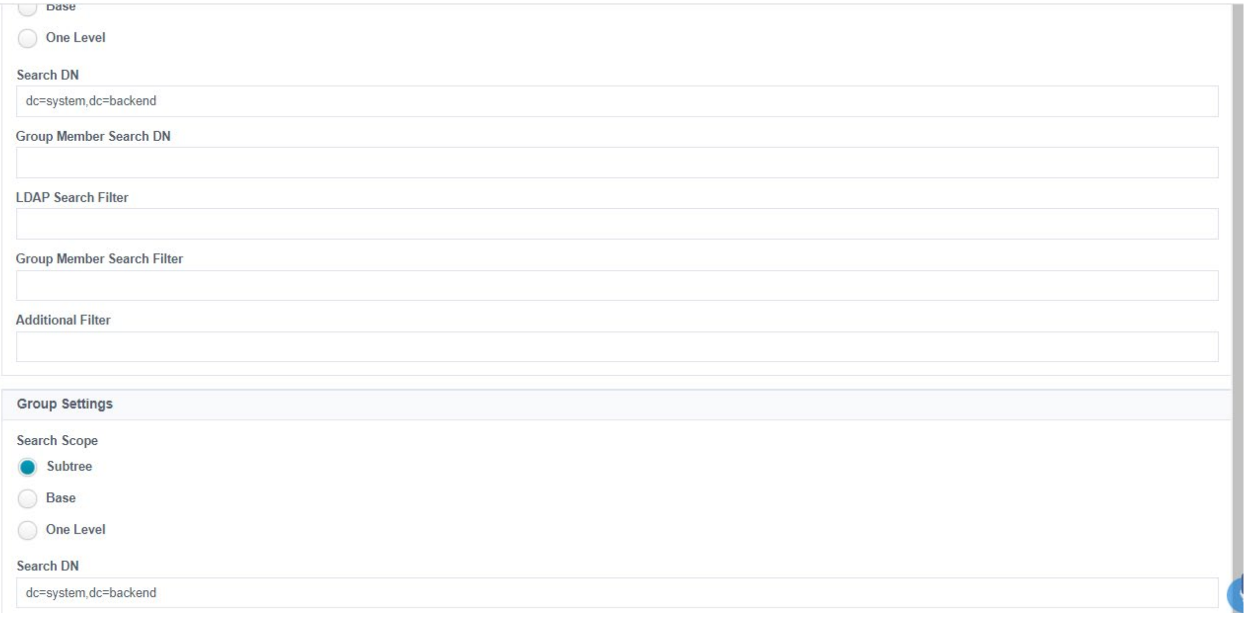
Server Host

Hostname or IP Address: 10.0.85.91

Port: 6389

Group Membership Attribute

uniqueMember



○ Base

○ One Level

Search DN: dc=system,dc=backend

Group Member Search DN:

LDAP Search Filter:

Group Member Search Filter:

Additional Filter:

Group Settings

Search Scope

● Subtree

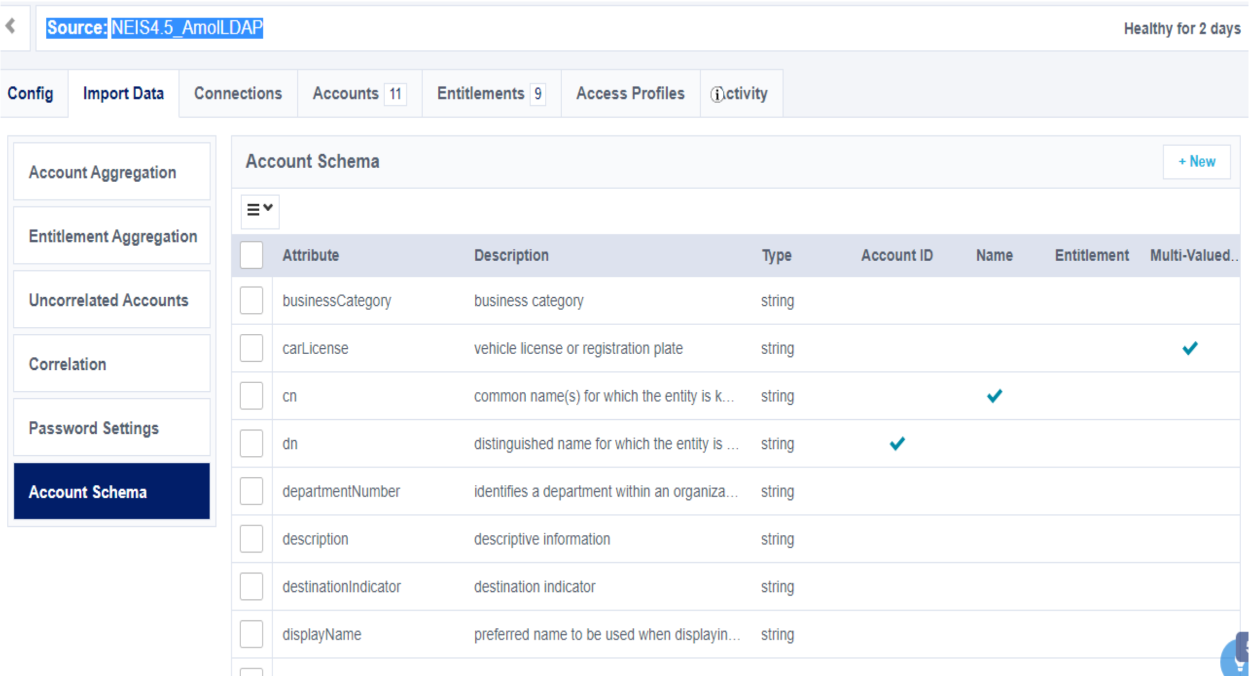
○ Base

○ One Level

Search DN: dc=system,dc=backend

C. Discover schema

i. Go to Connections-Source - Check for newly create Source: for e.g. NEIS4.5_AmolLDAP
ii. Click on Import Data - Account Schema
iii. Add new attributes as per the LDAP name
iv. Click on Save
v. Add highlighted Attributes manually using new option on the top right-hand corner.

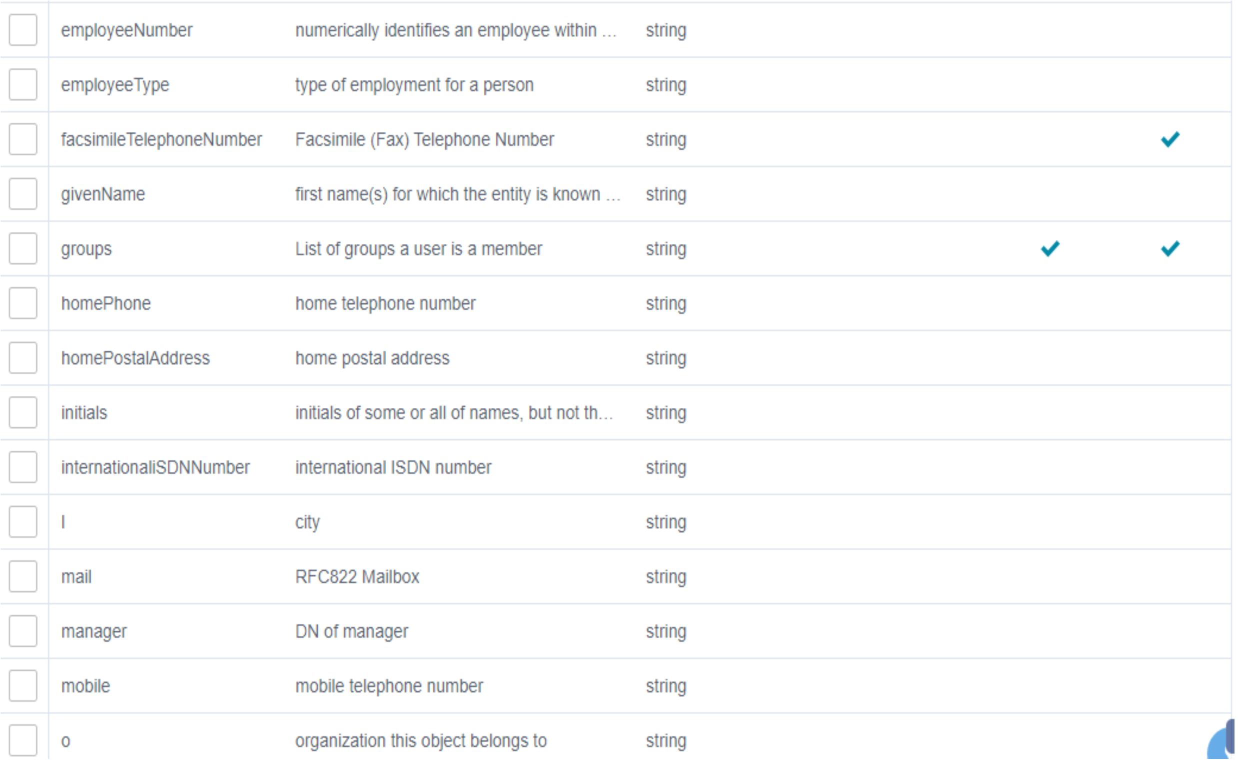


Source: NEIS4.5_AmolLDAP

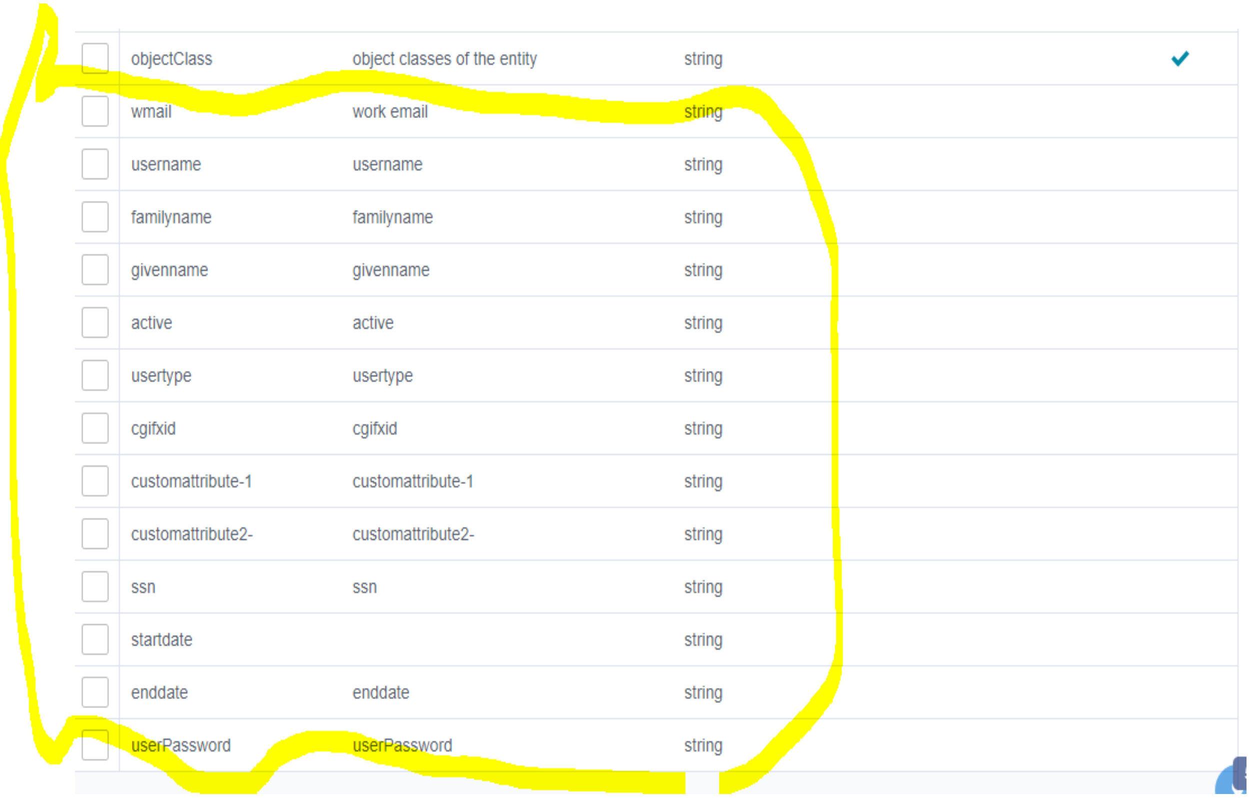
Healthy for 2 days

Account Schema

□	Attribute	Description	Type	Account ID	Name	Entitlement	Multi-Valued...
□	businessCategory	business category	string				
□	carLicense	vehicle license or registration plate	string				✓
□	cn	common name(s) for which the entity is k...	string		✓		
□	dn	distinguished name for which the entity is ...	string	✓			
□	departmentNumber	identifies a department within an organiza...	string				
□	description	descriptive information	string				
□	destinationIndicator	destination indicator	string				
□	displayName	preferred name to be used when displayin...	string				



□	employeeNumber	numerically identifies an employee within ...	string				
□	employeeType	type of employment for a person	string				
□	facsimileTelephoneNumber	Facsimile (Fax) Telephone Number	string				✓
□	givenName	first name(s) for which the entity is known ...	string				
□	groups	List of groups a user is a member	string			✓	✓
□	homePhone	home telephone number	string				
□	homePostalAddress	home postal address	string				
□	initials	initials of some or all of names, but not th...	string				
□	internationaliSDNNumber	international ISDN number	string				
□	l	city	string				
□	mail	RFC822 Mailbox	string				
□	manager	DN of manager	string				
□	mobile	mobile telephone number	string				
□	o	organization this object belongs to	string				

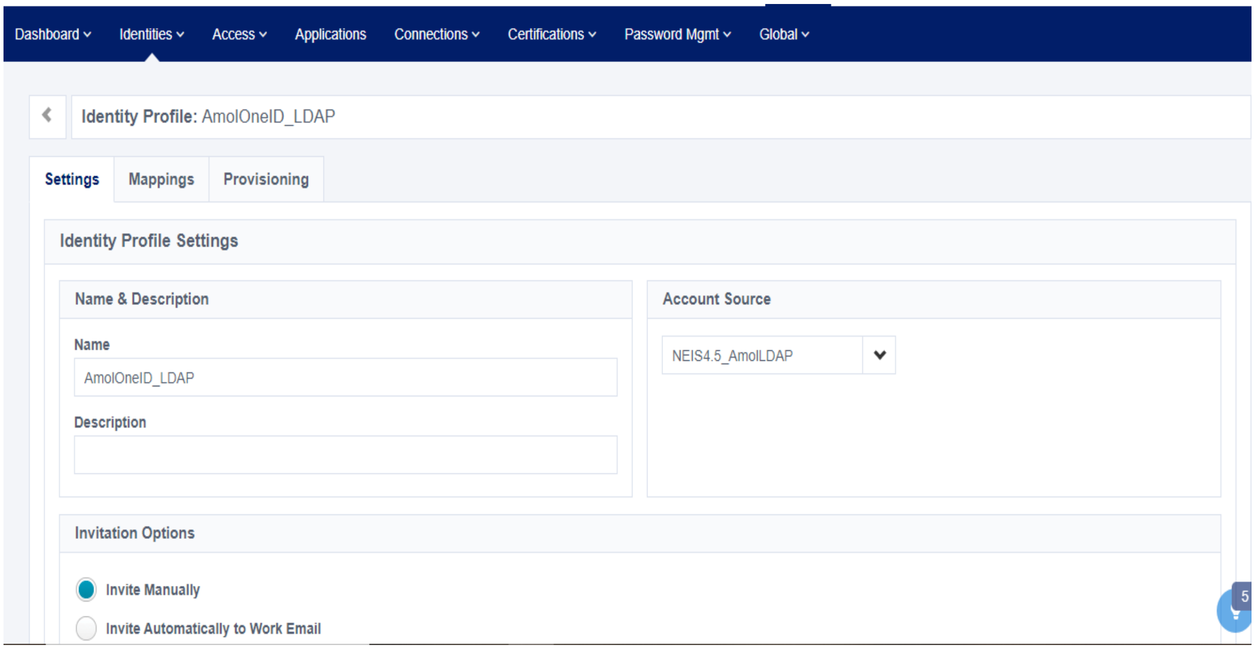


□	objectClass	object classes of the entity	string	✓
□	wmail	work email	string	
□	username	username	string	
□	familyname	familyname	string	
□	givenname	givenname	string	
□	active	active	string	
□	usertype	usertype	string	
□	cgifxid	cgifxid	string	
□	customattribute-1	customattribute-1	string	
□	customattribute2-	customattribute2-	string	
□	ssn	ssn	string	
□	startdate		string	
□	enddate	enddate	string	
□	userPassword	userPassword	string	

D. Create Identity Profile for NEIS

i. Click on Identities - Identity Profile
ii. Create new Identity, make sure you select same Source - NEIS4.5_AmolLDAP which was created earlier
iii. Setup mappings as per the requirement like - uid:username, email:wmail, lastname:familyname, firstname:givenname, License Status: Active, Lifecycle State:Active
iv. Save changes
v. Provisioning - Add 2 new attribute- true, false with provisioning setting as "Enabled"
vi. Click on Save changes

------------------This will complete actual NEIS - IDN Using LDAP setup ----------------------



Identity Profile: AmolOneID_LDAP

Identity Profile Settings

Name & Description

Name: AmolOneID_LDAP

Description:

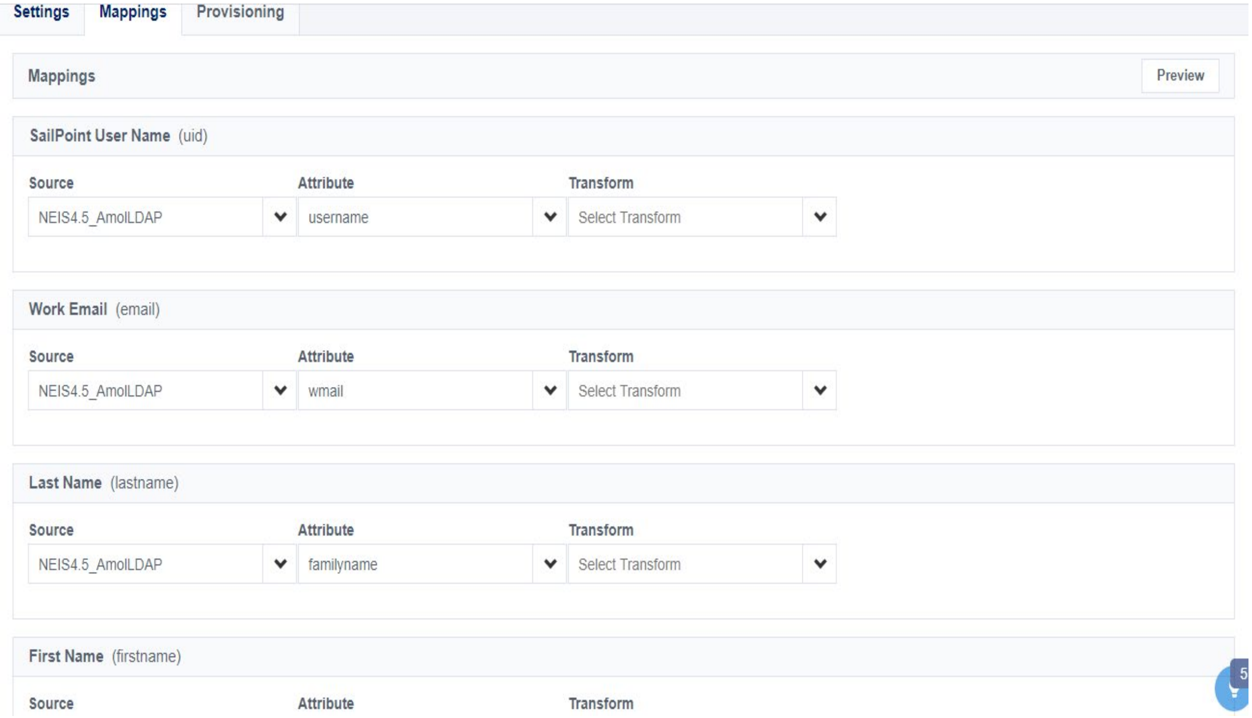
Account Source: NEIS4.5_AmolLDAP

Invitation Options

● Invite Manually

○ Invite Automatically to Work Email

Mapping



Mappings

SailPoint User Name (uid)

Source: NEIS4.5_AmolLDAP | Attribute: username | Transform: Select Transform

Work Email (email)

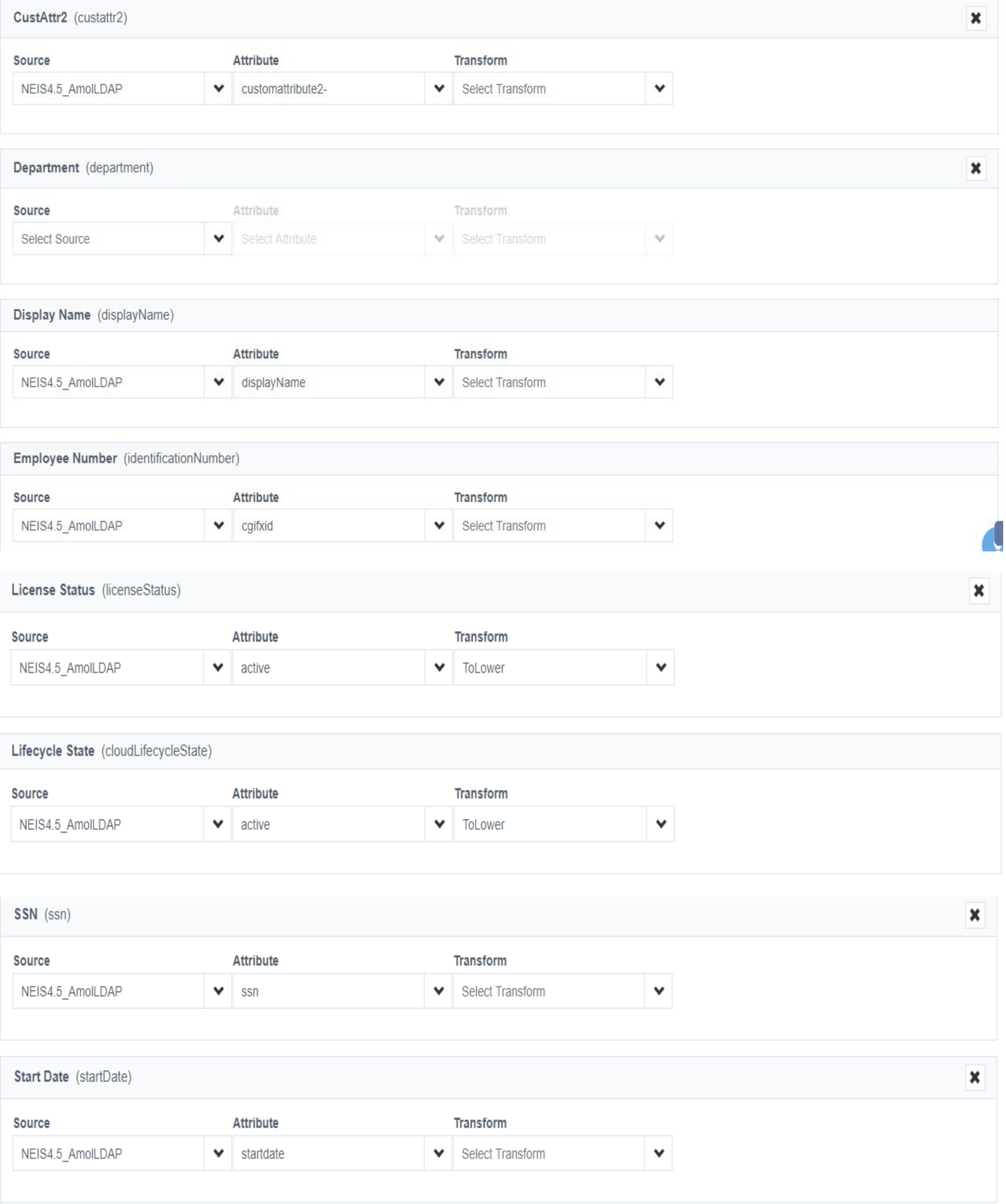
Source: NEIS4.5_AmolLDAP | Attribute: wmail | Transform: Select Transform

Last Name (lastname)

Source: NEIS4.5_AmolLDAP | Attribute: familyname | Transform: Select Transform

First Name (firstname)

Source | Attribute | Transform



CustAttr2 (custattr2)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	customattribute2-	Select Transform

Department (department)

Source	Attribute	Transform
Select Source	Select Attribute	Select Transform

Display Name (displayName)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	displayName	Select Transform

Employee Number (identificationNumber)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	cgifxid	Select Transform

License Status (licenseStatus)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	active	ToLower

Lifecycle State (cloudLifecycleState)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	active	ToLower

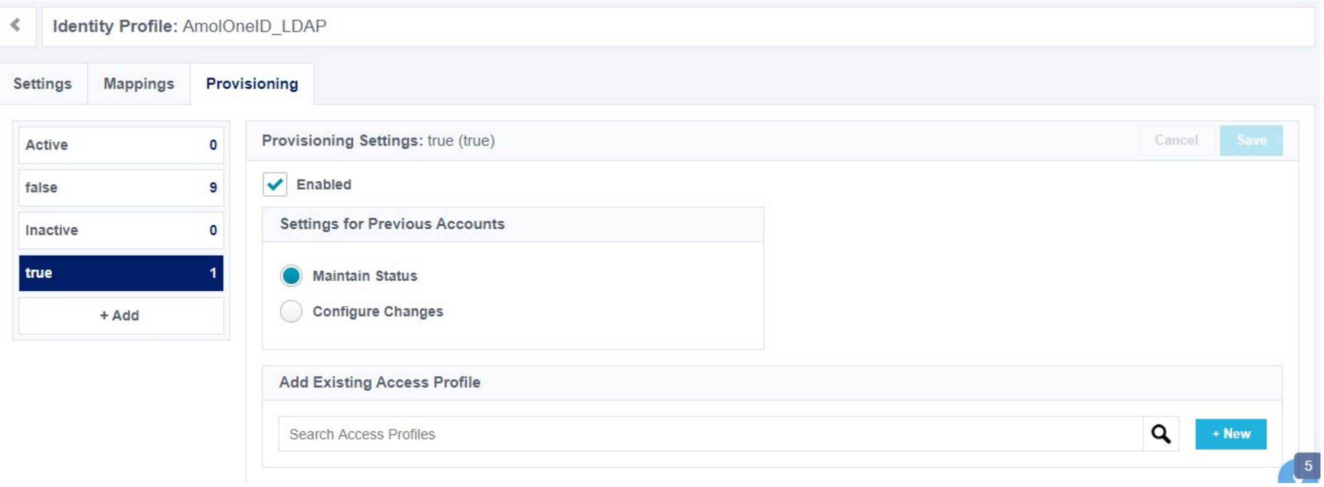
SSN (ssn)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	ssn	Select Transform

Start Date (startDate)

Source	Attribute	Transform
NEIS4.5_AmolLDAP	startdate	Select Transform

Provisioning



Identity Profile: AmolOneID_LDAP

Active	0
false	9
Inactive	0
true	1

Provisioning Settings: true (true)

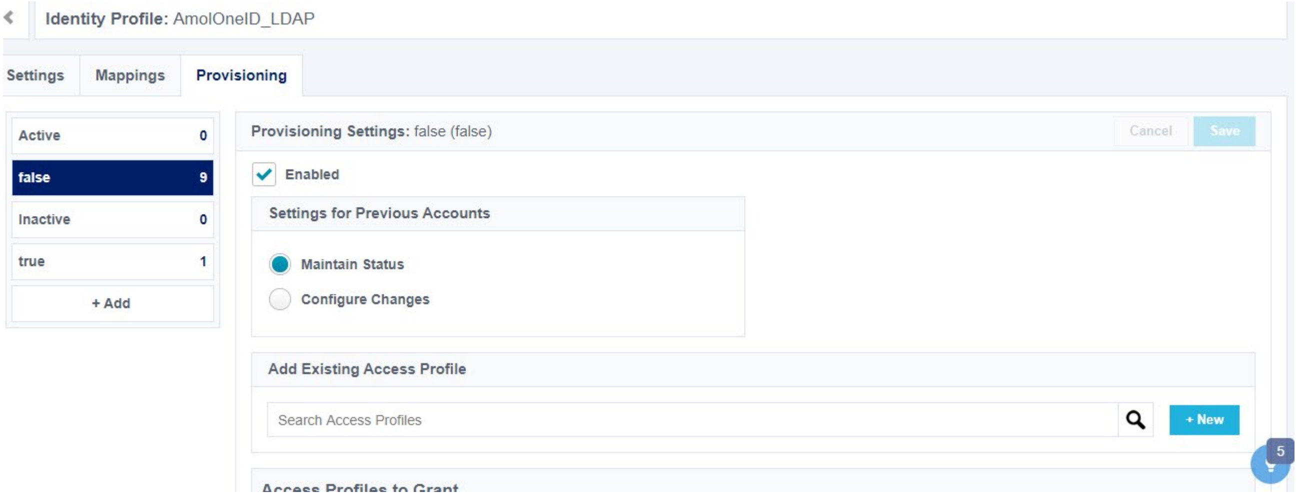
☑ Enabled

Settings for Previous Accounts

● Maintain Status

○ Configure Changes

Add Existing Access Profile



Identity Profile: AmolOneID_LDAP

Active	0
false	9
Inactive	0
true	1

Provisioning Settings: false (false)

☑ Enabled

Settings for Previous Accounts

● Maintain Status

○ Configure Changes

Add Existing Access Profile

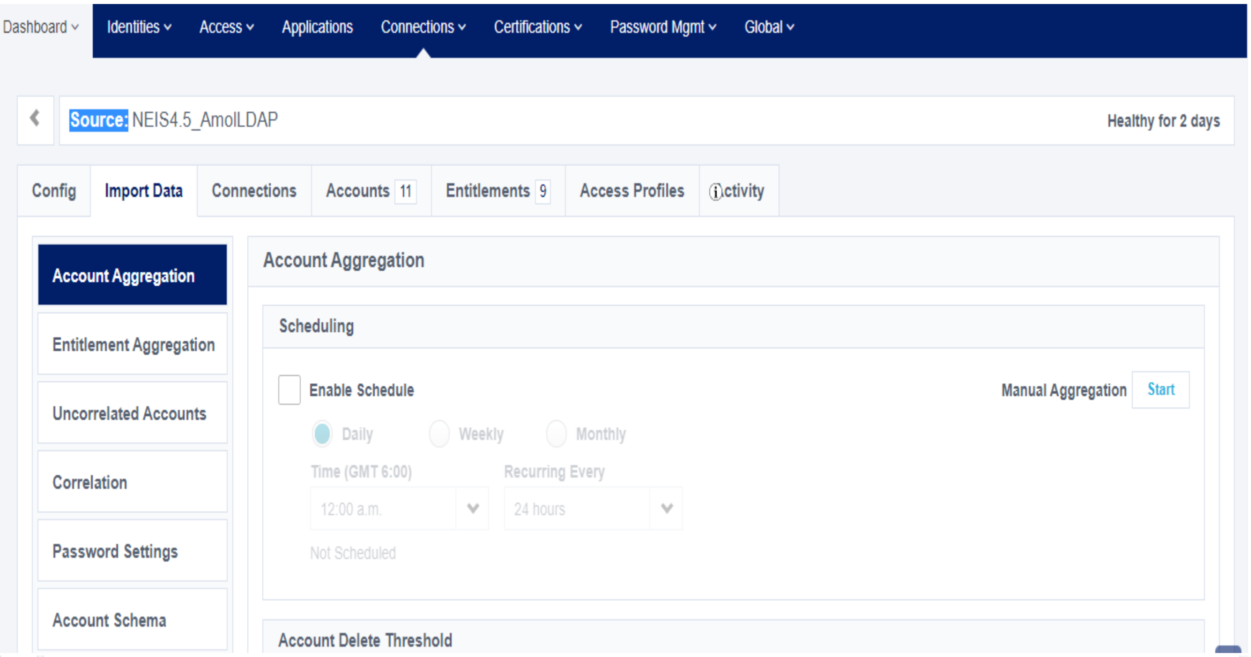
Access Profiles to Grant

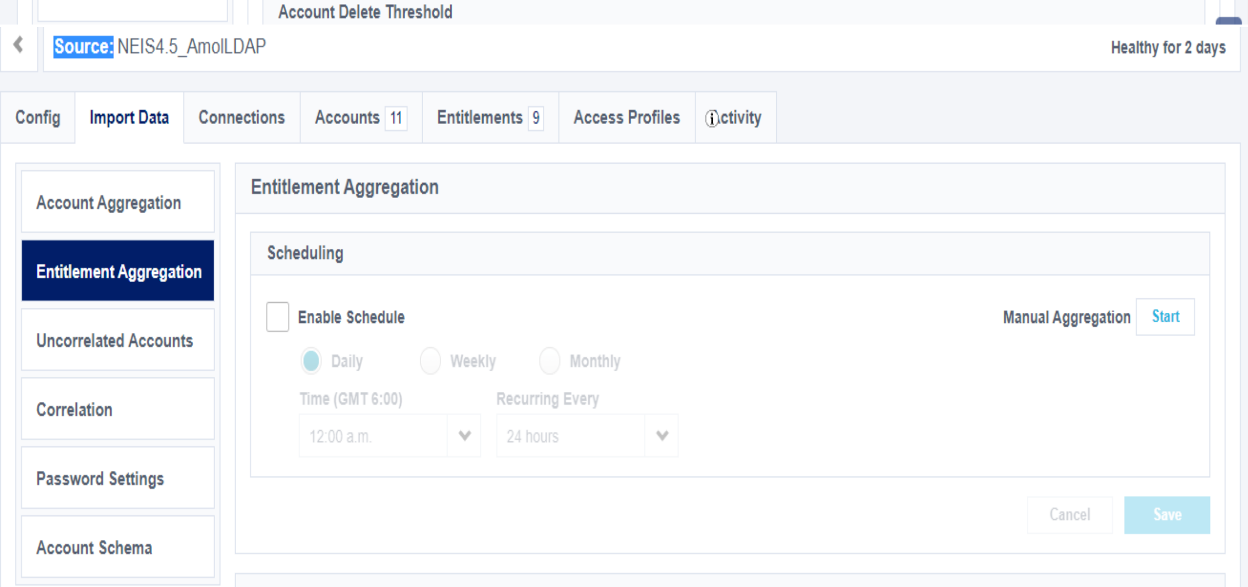
Integration Test – Aggregating Accounts from NEIS to IDN

Assuming NEIS has few Accounts, Groups already in place

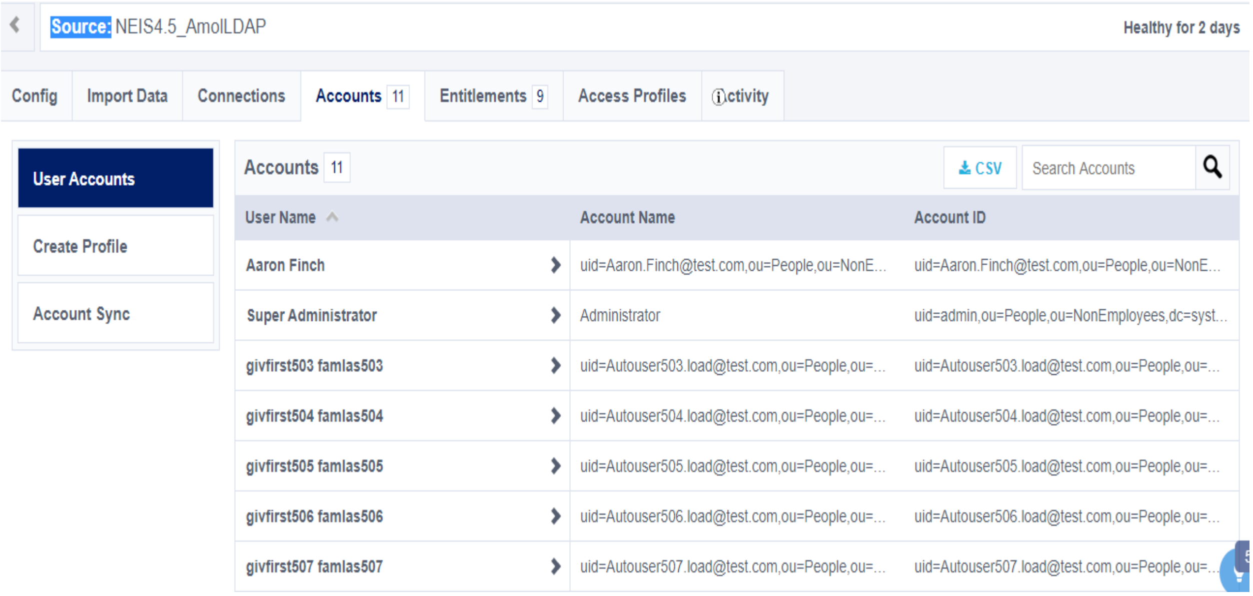
1. Account and Entitlement Aggregation
   i. Click on Connections - Source: NEIS4.5_AmolLDAP
   ii. Click on Import Data - Account Aggregation
   iii. Click on Start - This will start pulling records from NEIS to IDN, check the LDAP GW console to see data is being push
   iv. Click on Import Data - Entitlement Aggregation
   v. Click on Start - This will start pulling groups from NEIS to IDN, check the LDAP GW console to see data is being push
   vi. Once successfully job run, click on Accounts tab to see the record details
   vii. See the details of an account
   viii. In Account tab for associate Source

ix. Click on Entitlements





After Job completion click on Accounts tab



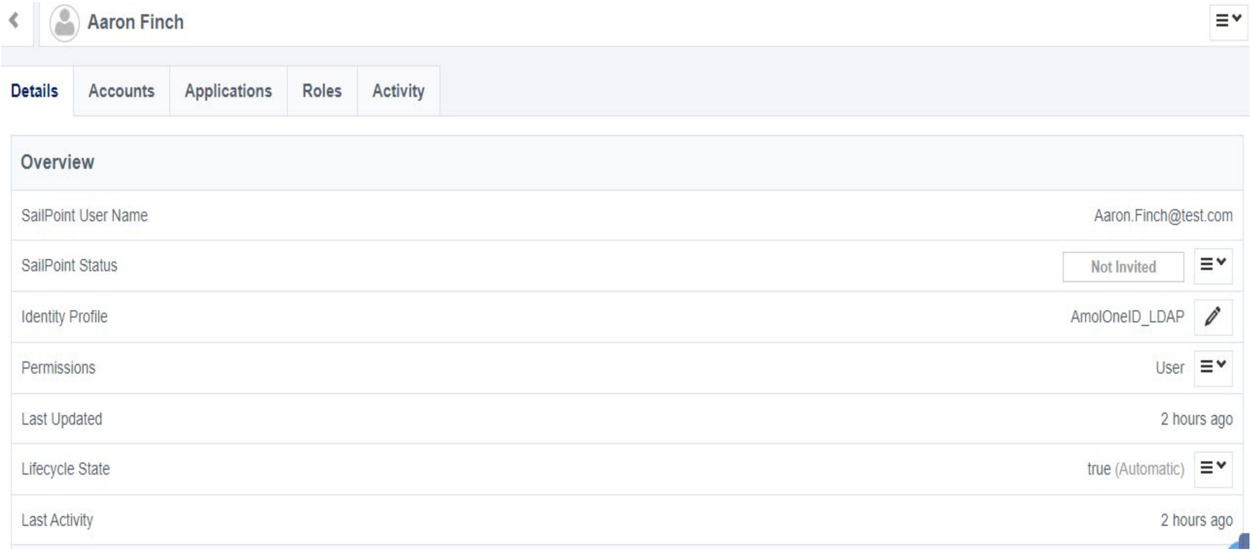
Source: NEIS4.5_AmolLDAP

Healthy for 2 days

Accounts 11

User Name	Account Name	Account ID
Aaron Finch	uid=Aaron.Finch@test.com,ou=People,ou=NonE...	uid=Aaron.Finch@test.com,ou=People,ou=NonE...
Super Administrator	Administrator	uid=admin,ou=People,ou=NonEmployees,dc=syst...
givfirst503 famlas503	uid=Autouser503.load@test.com,ou=People,ou=...	uid=Autouser503.load@test.com,ou=People,ou=...
givfirst504 famlas504	uid=Autouser504.load@test.com,ou=People,ou=...	uid=Autouser504.load@test.com,ou=People,ou=...
givfirst505 famlas505	uid=Autouser505.load@test.com,ou=People,ou=...	uid=Autouser505.load@test.com,ou=People,ou=...
givfirst506 famlas506	uid=Autouser506.load@test.com,ou=People,ou=...	uid=Autouser506.load@test.com,ou=People,ou=...
givfirst507 famlas507	uid=Autouser507.load@test.com,ou=People,ou=...	uid=Autouser507.load@test.com,ou=People,ou=...

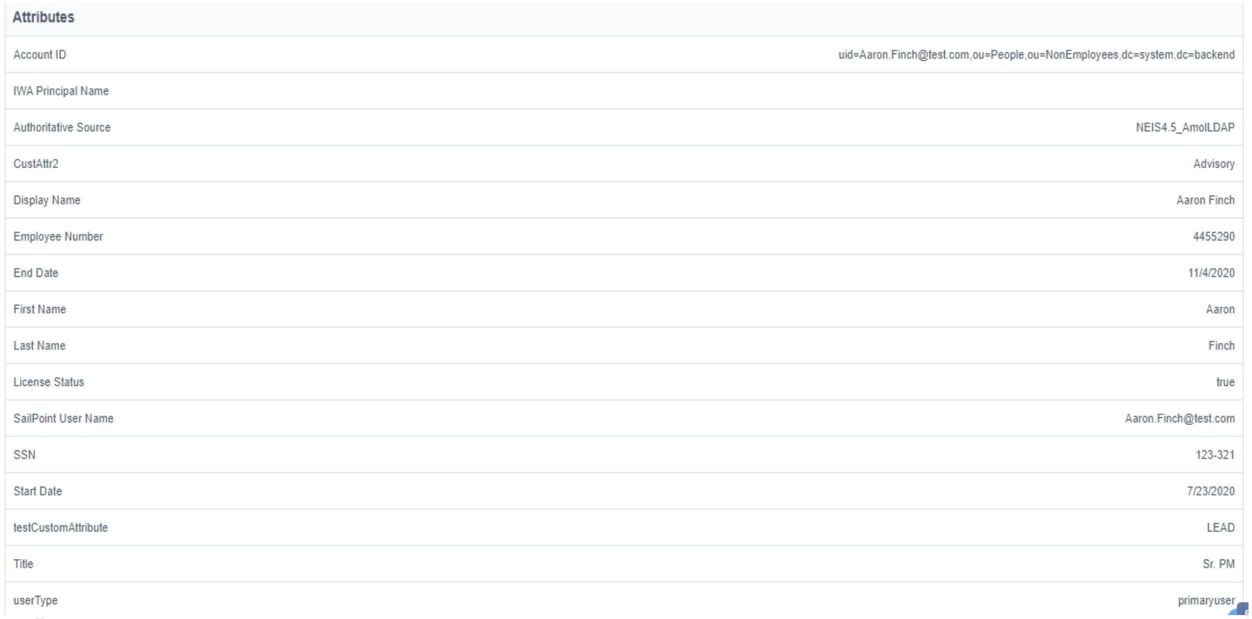
- **User details – For Active User**



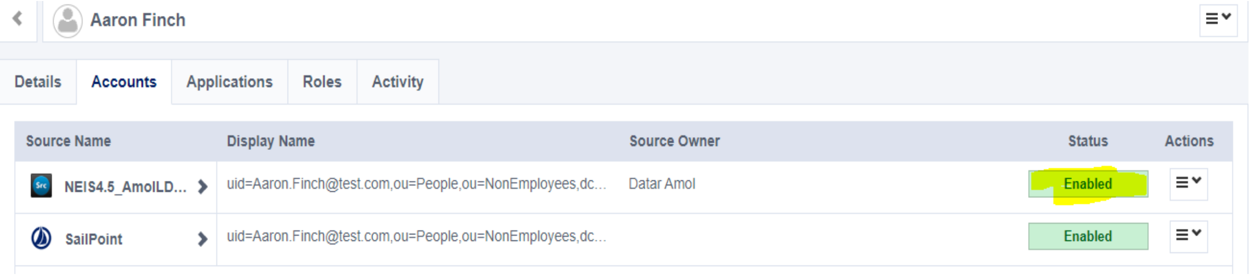
Aaron Finch

Overview

SailPoint User Name	Aaron.Finch@test.com
SailPoint Status	Not Invited
Identity Profile	AmolOneID_LDAP
Permissions	User
Last Updated	2 hours ago
Lifecycle State	true (Automatic)
Last Activity	2 hours ago



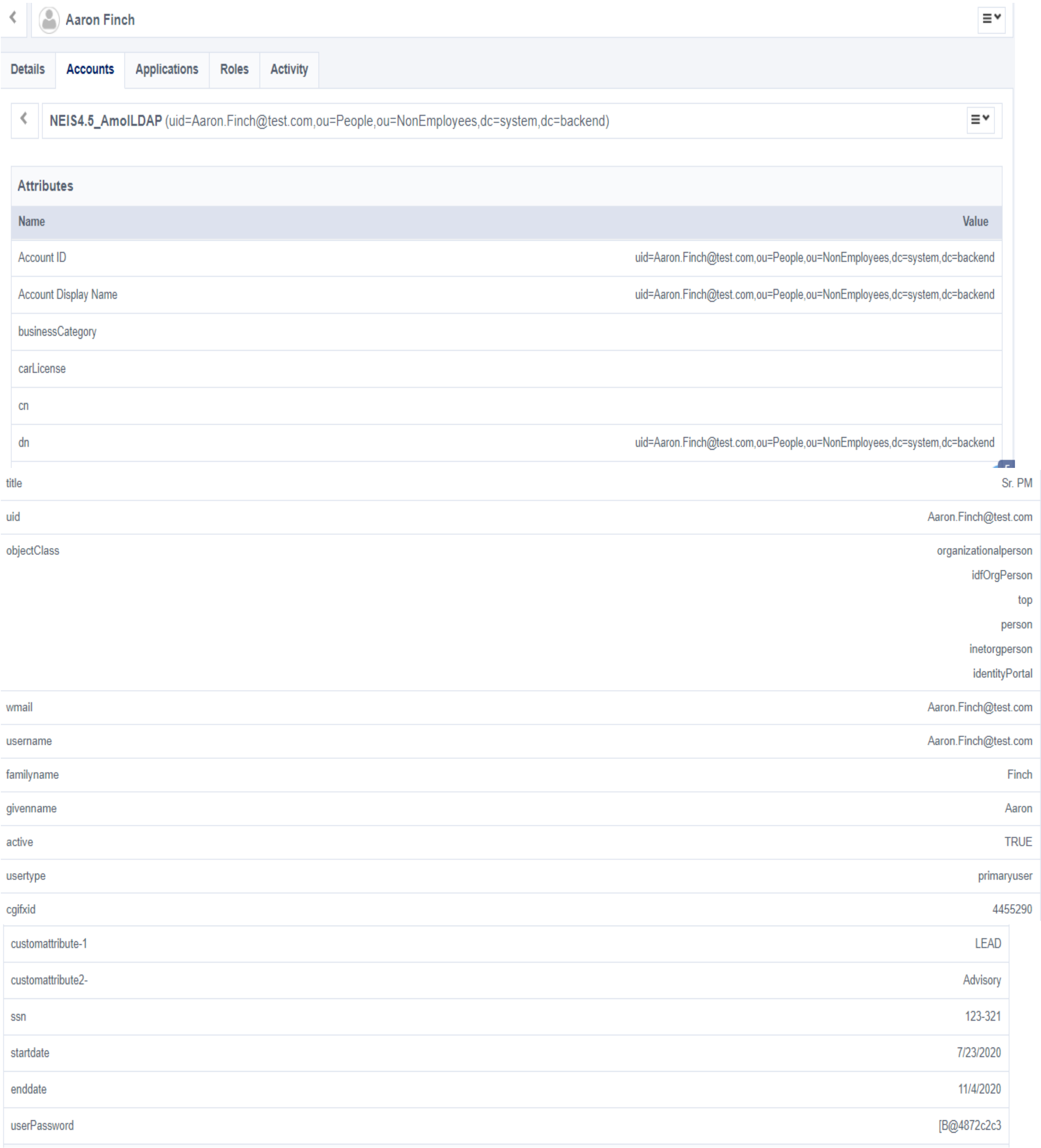
Attributes	
Account ID	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend
IWA Principal Name	
Authoritative Source	NEIS4.5_AmolLDAP
CustAttr2	Advisory
Display Name	Aaron Finch
Employee Number	4455290
End Date	11/4/2020
First Name	Aaron
Last Name	Finch
License Status	true
SailPoint User Name	Aaron.Finch@test.com
SSN	123-321
Start Date	7/23/2020
testCustomAttribute	LEAD
Title	Sr. PM
userType	primaryuser



Aaron Finch

Source Name	Display Name	Source Owner	Status	Actions
NEIS4.5_AmolLD...	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc...	Datar Amol	Enabled	☰
SailPoint	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc...		Enabled	☰

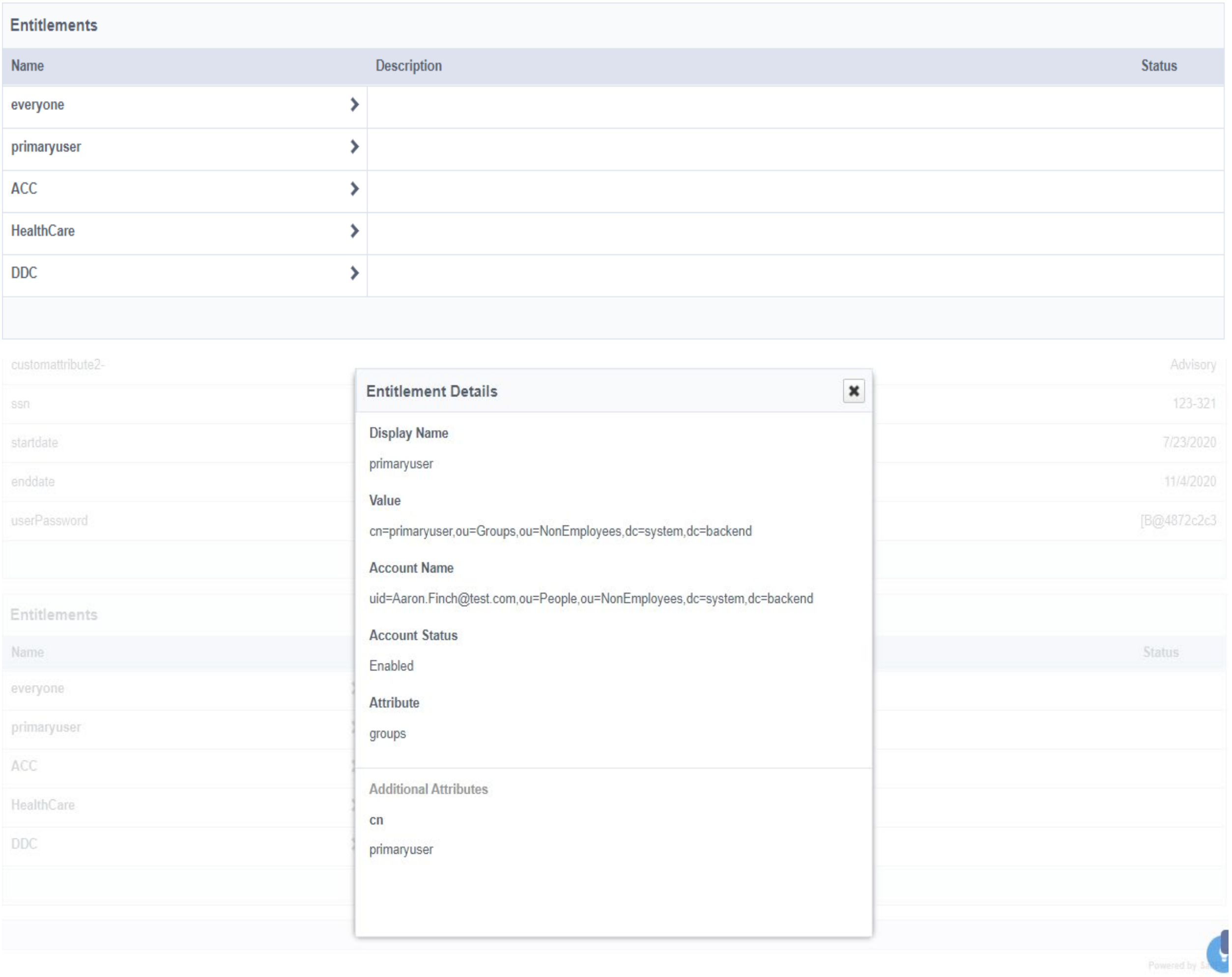
- **Click on Source Name**



NEIS4.5_AmolLDAP (uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend)

Attributes

Name	Value
Account ID	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend
Account Display Name	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend
businessCategory	
carLicense	
cn	
dn	uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend
title	Sr. PM
uid	Aaron.Finch@test.com
objectClass	organizationalperson idfOrgPerson top person inetorgperson identityPortal
wmail	Aaron.Finch@test.com
username	Aaron.Finch@test.com
familyname	Finch
givenname	Aaron
active	TRUE
usertype	primaryuser
cgifxid	4455290
customattribute-1	LEAD
customattribute2-	Advisory
ssn	123-321
startdate	7/23/2020
enddate	11/4/2020
userPassword	[B@4872c2c3



Entitlements

Name	Description	Status
everyone		
primaryuser		
ACC		
HealthCare		
DDC		

customattribute2-	Advisory
ssn	123-321
startdate	7/23/2020
enddate	11/4/2020
userPassword	[B@4872c2c3

Entitlements

Name	Status
everyone	
primaryuser	
ACC	
HealthCare	
DDC	

Entitlement Details

Display Name
primaryuser

Value
cn=primaryuser,ou=Groups,ou=NonEmployees,dc=system,dc=backend

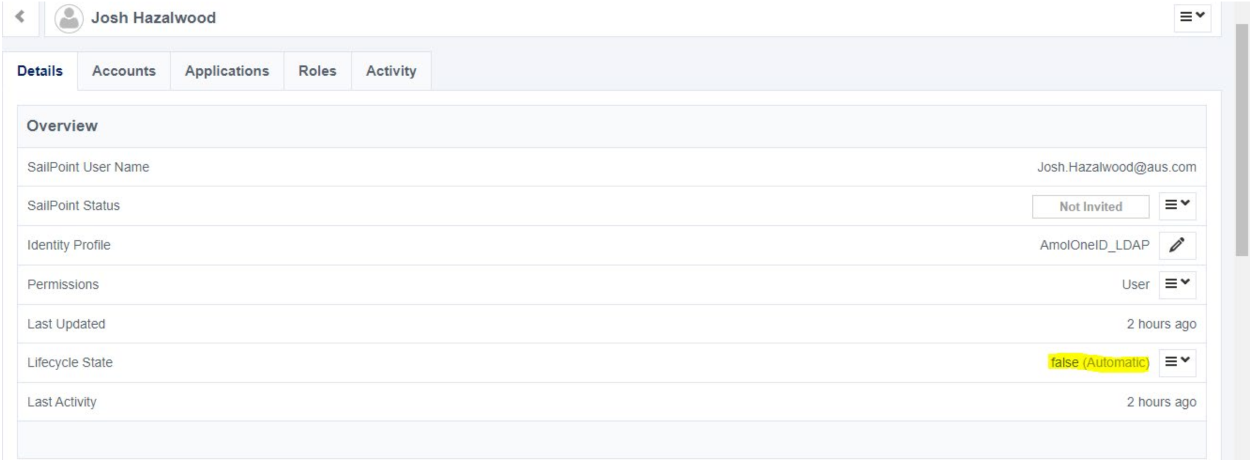
Account Name
uid=Aaron.Finch@test.com,ou=People,ou=NonEmployees,dc=system,dc=backend

Account Status
Enabled

Attribute
groups

Additional Attributes
cn
primaryuser

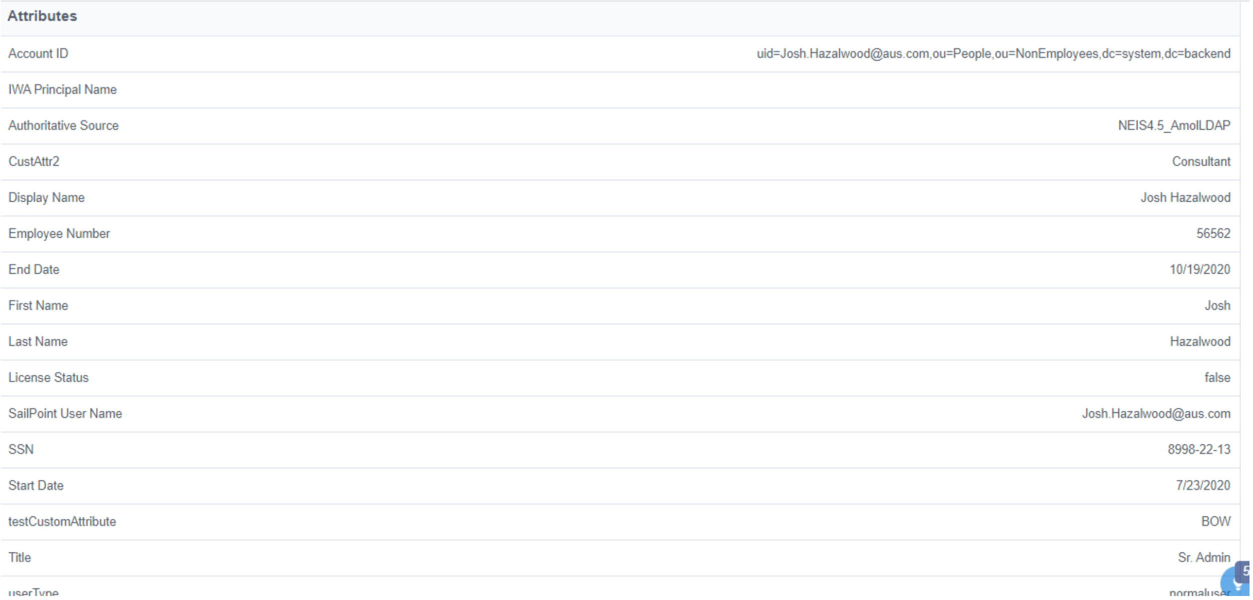
- **User details – For In-Active user**



Josh Hazalwood

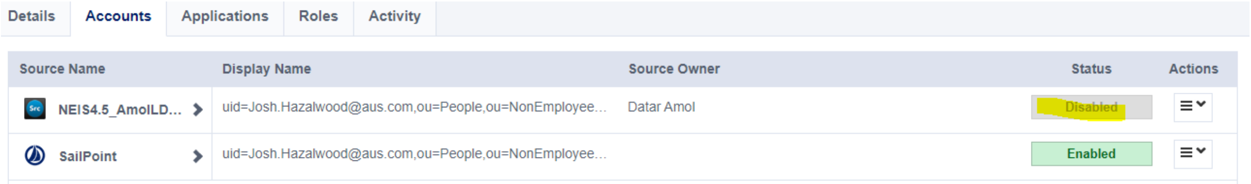
Overview

SailPoint User Name	Josh.Hazalwood@aus.com
SailPoint Status	Not Invited
Identity Profile	AmolOneID_LDAP
Permissions	User
Last Updated	2 hours ago
Lifecycle State	false (Automatic)
Last Activity	2 hours ago

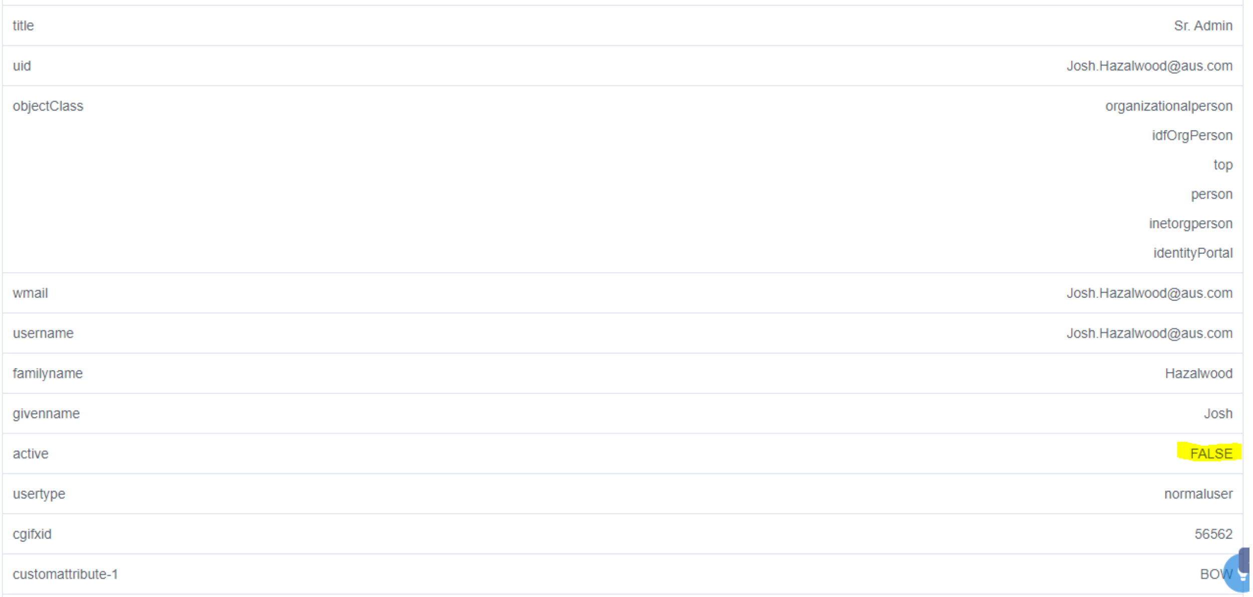


Attributes

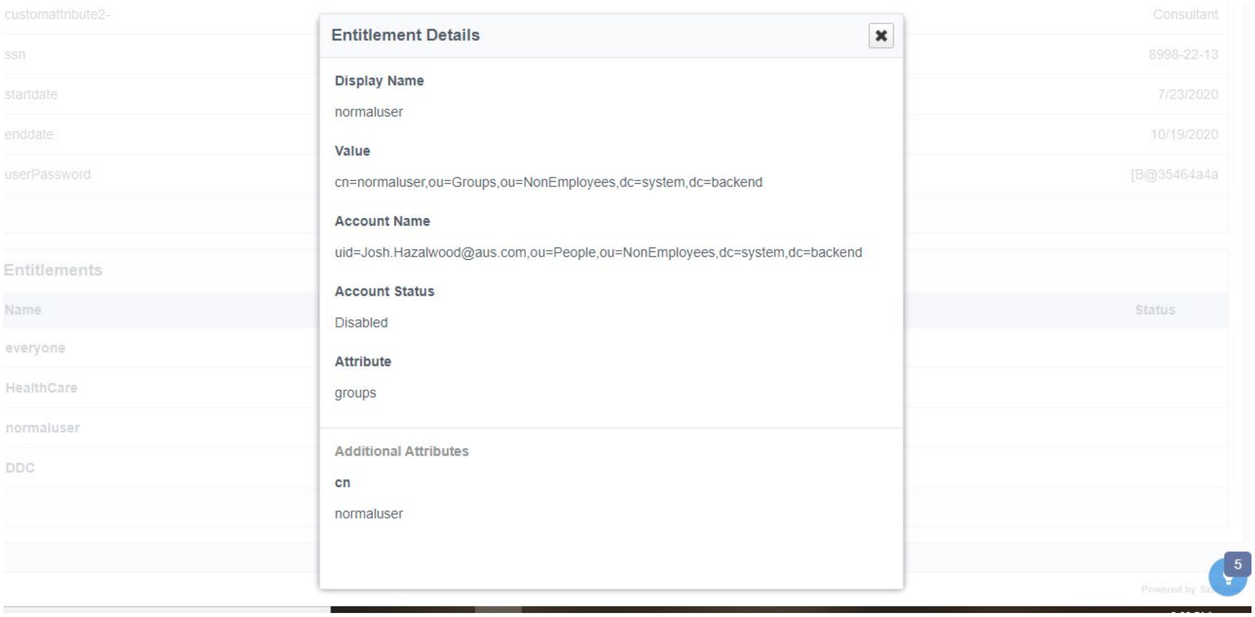
Account ID	uid=Josh.Hazalwood@aus.com,ou=People,ou=NonEmployees,dc=system,dc=backend
IWA Principal Name	
Authoritative Source	NEIS4.5_AmolLDAP
CustAttr2	Consultant
Display Name	Josh Hazalwood
Employee Number	56562
End Date	10/19/2020
First Name	Josh
Last Name	Hazalwood
License Status	false
SailPoint User Name	Josh.Hazalwood@aus.com
SSN	8998-22-13
Start Date	7/23/2020
testCustomAttribute	BOW
Title	Sr. Admin
userType	normaluser



Source Name	Display Name	Source Owner	Status	Actions
NEIS4.5_AmolLD...	uid=Josh.Hazalwood@aus.com,ou=People,ou=NonEmployee...	Datar Amol	Disabled	≡ ▾
SailPoint	uid=Josh.Hazalwood@aus.com,ou=People,ou=NonEmployee...		Enabled	≡ ▾



title	Sr. Admin
uid	Josh.Hazalwood@aus.com
objectClass	organizationalperson idfOrgPerson top person inetorgperson identityPortal
wmail	Josh.Hazalwood@aus.com
username	Josh.Hazalwood@aus.com
familyname	Hazalwood
givenname	Josh
active	FALSE
usertype	normaluser
cgifxid	56562
customattribute-1	BOW



customattribute2-	Consultant
ssn	8998-22-13
startdate	7/23/2020
enddate	10/19/2020
userPassword	[B@35464a4a

Entitlements

Name	Status
everyone	
HealthCare	
normaluser	
DDC	

Entitlement Details

Display Name

normaluser

Value

cn=normaluser,ou=Groups,ou=NonEmployees,dc=system,dc=backend

Account Name

uid=Josh.Hazalwood@aus.com,ou=People,ou=NonEmployees,dc=system,dc=backend

Account Status

Disabled

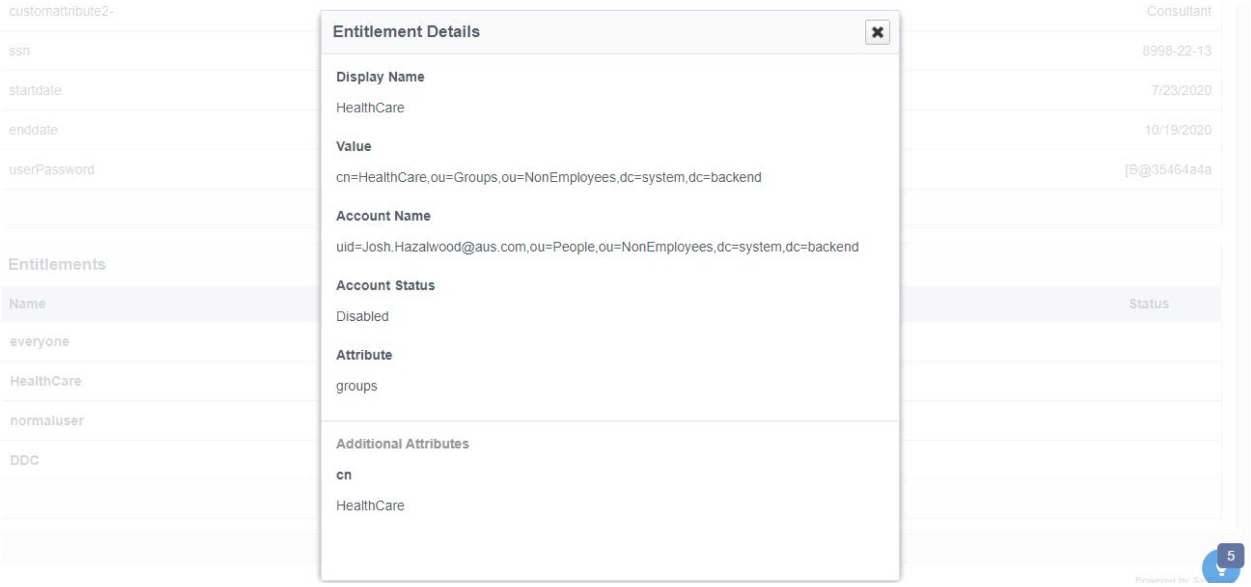
Attribute

groups

Additional Attributes

cn

normaluser



customattribute2-	Consultant
ssn	8998-22-13
startdate	7/23/2020
enddate	10/19/2020
userPassword	[B@35464a4a

Entitlements

Name	Status
everyone	
HealthCare	
normaluser	
DDC	

Entitlement Details

Display Name

HealthCare

Value

cn=HealthCare,ou=Groups,ou=NonEmployees,dc=system,dc=backend

Account Name

uid=Josh.Hazalwood@aus.com,ou=People,ou=NonEmployees,dc=system,dc=backend

Account Status

Disabled

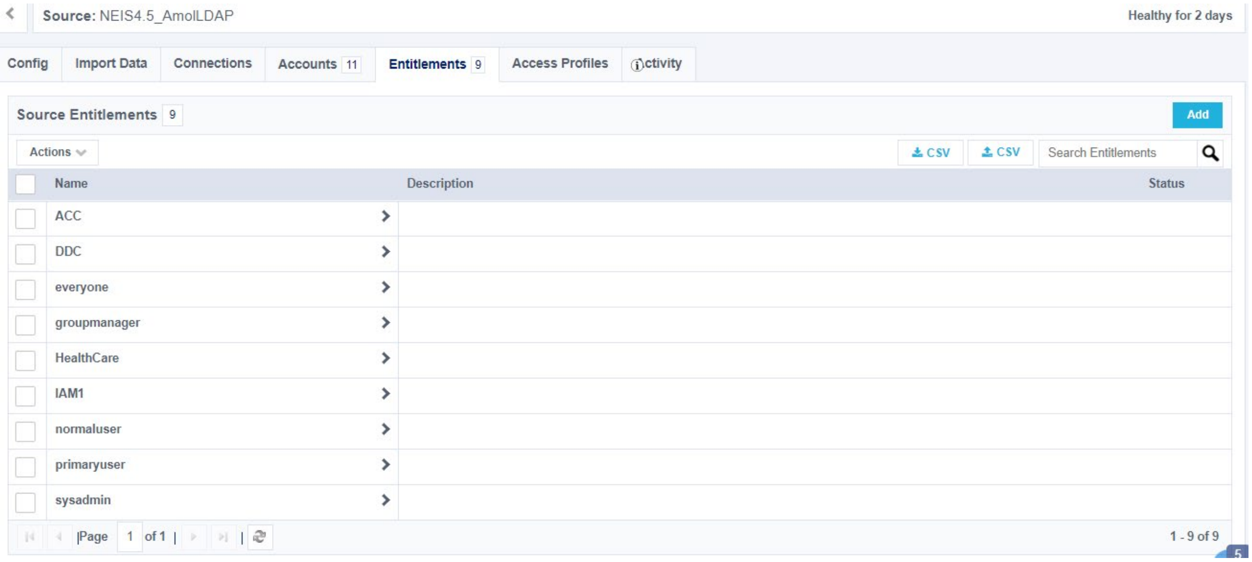
Attribute

groups

Additional Attributes

cn

HealthCare



Source: NEIS4.5_AmolLDAP

Healthy for 2 days

Source Entitlements 9

Name	Description	Status
ACC		
DDC		
everyone		
groupmanager		
HealthCare		
IAM1		
normaluser		
primaryuser		
sysadmin		

2. To see the updated records in IDN

   i. Update user in NEIS

   ii. Perform same operations - Account & Entitlement Aggregation on IDN again to see the updated data