EmblemHealth

**SailPoint IdentityNow®**

**Integration with ACPNY Domain**

Design Document



Version 1.0

Effective Date: 25/7/2018

Prepared By: Cognizant Technology Solutions

*All information contained herein is proprietary and shall be kept confidential.*

Approvals

Approval denotes acceptance of the business requirements contained herein and serves as authorization to move forward with related documents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Role** | **Date** |
| Arjun Sengupta | Cognizant | Reviewer |  |
| Saleem AT | Cognizant | Reviewer |  |
| Sudhir Kumar Panda | Cognizant | Reviewer |  |
| Manisha Roy | Cognizant | Approver |  |
| Randall Dulin | Cognizant | Approver |  |
| Jim Altinay | Emblem Health | Approver |  |
| Tom McDermott | Emblem Health | Approver |  |
| Drew Morrison | ACPNY | Approver |  |
| Heriberto Rodriguez | ACPNY | Reviewer |  |

Revision History

| **Version** | **Version Date** | **Author** | **Reviewed by** | **Comments** |
| --- | --- | --- | --- | --- |
| 1.0 | 7/25/2018 | Infosec |  | First draft |
| 2.0 | 8/1/2018 | Infosec |  | Added sections for secret question and password policy as well added the IIQ users source as well. |
| 3.0 | 8/7/2018 | Infosec |  | Updated after the review comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Design Document 2](#_Toc521515483)

[Revision History 4](#_Toc521515484)

[1.0 Introduction 7](#_Toc521515485)

[1.1 Document Purpose 7](#_Toc521515486)

[1.2 Scope 7](#_Toc521515487)

[1.2.1 In-Scope 7](#_Toc521515488)

[1.2.2 Out-of-Scope 7](#_Toc521515489)

[1.3 Definition & Acronyms 7](#_Toc521515490)

[1.4 Design Constraints 7](#_Toc521515492)

[2.0 Architecture 8](#_Toc521515493)

[2.1 EmblemHealth and ACPNY SSO integration with IdentityNow 8](#_Toc521515494)

[2.1.1 IDP initiated SSO 9](#_Toc521515495)

[2.1.2 SP Initiated SSO 9](#_Toc521515496)

[2.2 Environment and URL Details 10](#_Toc521515497)

[3.0 Schema 10](#_Toc521515498)

[3.1 Overview 10](#_Toc521515499)

[3.2 ACPNY AD structure and Attributes 10](#_Toc521515500)

[3.3 PeopleSoft feed for ACPNY 11](#_Toc521515501)

[3.4 Data Aggregation into SailPoint IIQ 12](#_Toc521515502)

[4.0 Configuration 12](#_Toc521515503)

[4.1 Setting up Virtual Appliance 12](#_Toc521515504)

[4.2 IQService Integration 12](#_Toc521515505)

[4.3 Creating Source 13](#_Toc521515506)

[4.3.1 ACPNY AD 14](#_Toc521515507)

[4.3.2 IIQ ALL Users 16](#_Toc521515508)

[4.4 Setting up of Identity Profile 17](#_Toc521515509)

[4.5 User Load from On-premise IdentityIQ into IdentityNow 18](#_Toc521515510)

[4.6 Pass-through Authentication 20](#_Toc521515511)

[4.7 Network Boundary Definition 21](#_Toc521515512)

[4.7.1 Web Browser Configuration 22](#_Toc521515513)

[4.8 Password Authentication for Intranet Access 23](#_Toc521515514)

[4.9 Two Factor Authentication for Internet Access 23](#_Toc521515515)

[4.10 Set Preference 25](#_Toc521515516)

[5.0 Appendix 27](#_Toc521515517)

[5.1 Duplicate Users 27](#_Toc521515518)

[5.2 Documents 27](#_Toc521515519)

[5.3 Set of Secret Questions in Identity Now 27](#_Toc521515520)

[5.4 Password Policy 28](#_Toc521515521)

[6.0 Reference 29](#_Toc521515522)

# Introduction

## Document Purpose

This document explains the design approach details to integrate ACPNY domain with Identity Now so that the ACPNY users are able to access Oracle Cloud applications on the Emblem Health domain

## Scope

### In-Scope

The in-scope design activities are listed below:

* Setup connectivity between ACPNY Active Directory and IdentityNow
* Setup Virtual appliance for QA and Production regions
* Establish policies to differentiate ACPNY users from EmblemHealth Users
* Setup Profiles and Access policies
* Importing ACPNY user data in Identity Now thorough PeopleSoft Feed
* Enforcing 2 Factor authentication for ACPNY users login from internet

### Out-of-Scope

The out-of-scope activities are listed below:

* Network Infrastructure and scalability
* Any other federation protocol apart from SAML 2.0

## Definition & Acronyms

| **Term** | **Definition** |
| --- | --- |
| ACS | Assertion Consumer Service |
| SAML | Security Assertion Markup Language |
| SSO | Single Sign-on |
| MFA | Multi-factor Authentication |

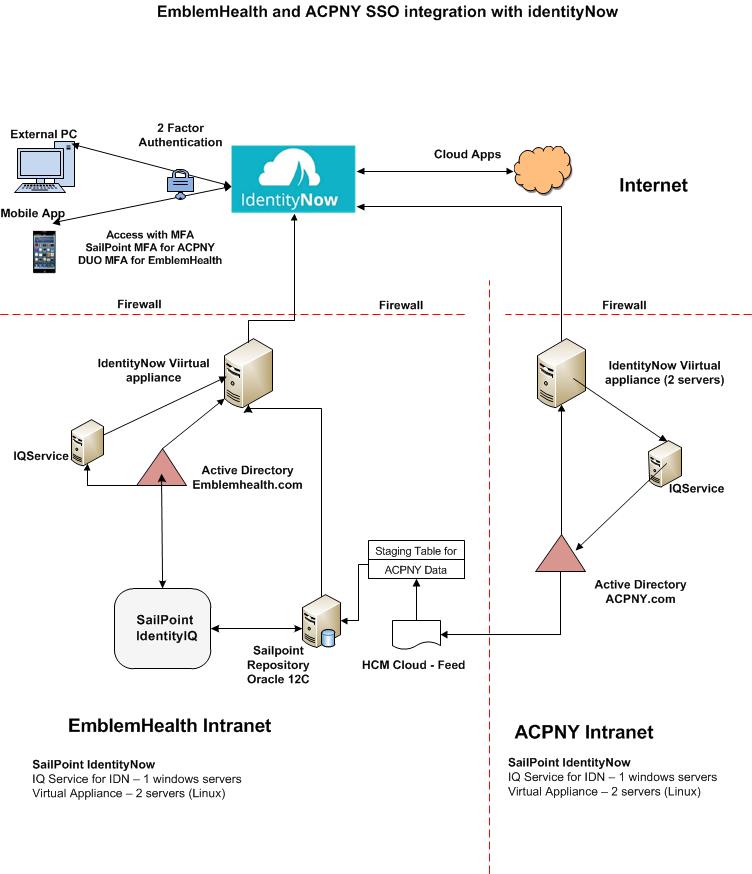


## Design Constraints

* Emblem Health Users and ACPNY Users cannot have the same Networkid’s in their respective Active Directories
* ACPNY does not have a certificate authority and the certificates are locally signed. This limits the ability to connect to multiple servers with the certificate or ability of IdentityNow to pull an AD certificate. If the AD server integrated with goes down or is in maintenance, we will not be able to switch to other servers.
* The Data loading in SailPoint is dependent on the PeopleSoft feed for ACPNY. The frequency of the feed needs to be discussed

# Architecture

## EmblemHealth and ACPNY SSO integration with IdentityNow



Above depicts the high level interactions between different components of EmblemHealth IdentityNow infrastructure within Emblem Health and ACPNY domains as well as internet while accessing an application.

### IDP initiated SSO

***Intranet***

1. Users hits the EH IdentityNow url and enters network user ID and password
2. User credential is validated against ACPNY AD.
3. Upon successful credential validation user successfully logs intoIdentity Now Home.
4. User clicks on any SAML enabled application available on IdentityNow home page. IdentityNow generates SAML token and pass it to the application. Upon successful token validation, user will be navigated to application home page.

***Internet***

1. User accesses IdentityNow through web browser or mobile application. IdentityNow presents login page to user and user submits with EH network credential.
2. IdentityNow connects to ACPNY AD to validate user’s network credential. AD send success/failure response
3. Upon successful password authentication, user is asked to choose one of the strong authentication options either a code on phone or email, security questions etc.
4. Upon successful Strong authentication, user accesses SAML enabled application available on IdentityNow home page.
5. IdentityNow sends SAML token to the application and user logs into the application automatically without being prompted for authentication again.

### SP Initiated SSO

***Intranet***

1. Users hits the application url and is redirected to the identity now login page.
2. User enters network user ID and password
3. User credential is validated against ACPNY AD.
4. Upon successful credential validation the saml token gets generated.
5. Upon successfull token validation user logs into application home page.

***Internet***

1. User accesses Application URL through web browser or mobile application. IdentityNow presents login page to user and user submits with ACPNY network credential.
2. IdentityNow connects to ACPNY AD to validate user’s network credential. AD send success/failure response
3. Upon successful password authentication, user is asked to choose one of the strong authentication options either a code on phone or email, security questions etc.
4. Upon successful Strong authentication, user accesses the application. IdentityNow sends SAML token to the application and user logs into the application automatically without being prompted for authentication again.

## Environment and URL Details

| **Product** | **Environment name** | **URL** |
| --- | --- | --- |
| IdentityNow (Web Application) | Dev | <https://emblemhealth-dev.identitynow.com/> (Not integrated with ACPNY currently due to limited hardware) |
| Sandbox | <https://emblemhealth-sb.identitynow.com/> |
| Production | <https://emblemhealth.identitynow.com/> |

# Schema

## Overview

The users belonging to ACPNY domain will be imported into Identity Now from ACPNY active directory. The Same set of users will be loaded into SailPoint IIQ with the help of the data feed received from PeopleSoft HR and will be correlated with the users from ACPNY AD on the basis of their Network ID.

## ACPNY AD structure and Attributes

The below OU’s contain users in ACPNY AD.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl** | **OU name** | **Description** | **In Scope** |
| 1 | OU=Users,OU=ACPNY,DC=acpny,DC=com | All Employees in this ou under one level search scope | Yes |
| 2 | OU=InactiveAccounts,OU,Users,OU=ACPNY,DC=acpny,DC=com | Terminated/LOA users | No |
| 3 | The Below Ou under OU=Users,OU=ACPNY,DC=acpny,DC=com  OU=Vendors  OU=Emblem Health  OU=CareTech  OU=Staff  OU=Contractors  OU=McKesson  The below OU  OU=Vendors,OU=ACPNY,DC=acpny,DC=com | Vendor Accounts | No |

The Attributes for which the value will be populated in Identity Now from ACPNY AD

* User Principal Name
* Alternate Phone Number
* Display Name
* Employee Number
* First Name
* Last Name
* SamAccountName
* Work Email
* Work Phone Number
* memberOf

## PeopleSoft feed for ACPNY

A feed file from PeopleSoft HR containing the details of all the ACPNY users will be shared by the ACPNY team to load the users in SailPoint IIQ. The feed file will contains the details of all the users belonging to ACPNY Organizational unit that includes Vendors, Inactive users, Terminated users and employees. Only users belonging to USERS OU will be imported into SailPoint IIQ

The feed file from PeopleSoft HR contains the below fields:

* employeeNumber
* SAM Account Name
* First Name
* Last Name
* Email Address
* Domain Name
* Display Name
* Manager
* Telephone Number
* Mobile
* Distinguished Name
* Title
* Office
* Street Address
* State/Province
* Zip Code
* City

## Data Aggregation into SailPoint IIQ

The below process will be followed to aggregate ACPNY data into SailPoint IIQ.

ACPNY team will place a csv file containing the users that needs to be imported in IIQ through an MFT process.

An aggregation task will be executed in SailPoint IIQ to import only the user data belonging to “USERS OU” in ACPNY AD.

The table that stores ACPNY Users data in IIQ is a custom table and it contain the below columns:

* EMPLOYEEID
* FIRST\_NAME
* LAST\_NAME
* DISPLAY\_NAME
* EMAILID
* NETWORKID
* MANAGER
* USER\_TYPE
* TELEPHONE
* STATUS
* USER\_TERMINATION\_DATE

Where EMPLOYEEID is the primary key defined in the table.

# Configuration

## Setting up Virtual Appliance

Virtual Appliance (VA) is a Linux based virtual server situated within EH network. The appliance is used by IdentityNow to connect to any EH internal systems (e.g. On-premise Active Directory, IdentityIQ) which cannot be exposed to Internet.

All communication between IdentityNow and EH internal systems (E.g. AD) happens through Virtual appliance

The Virtual Appliance Servers are as follows:

|  |  |
| --- | --- |
| Environment | Server Details |
| SandBox | 10.1.166.133 |
| Production | TBD |

## IQService Integration

IQService is a component which acts as mediator between IdentityNow and on-premise Active Directory for all provisioning and password management operations. Since on-premise AD is an internal secure system, so, IdentityNow connect to it through IQService without exposing AD to internet.

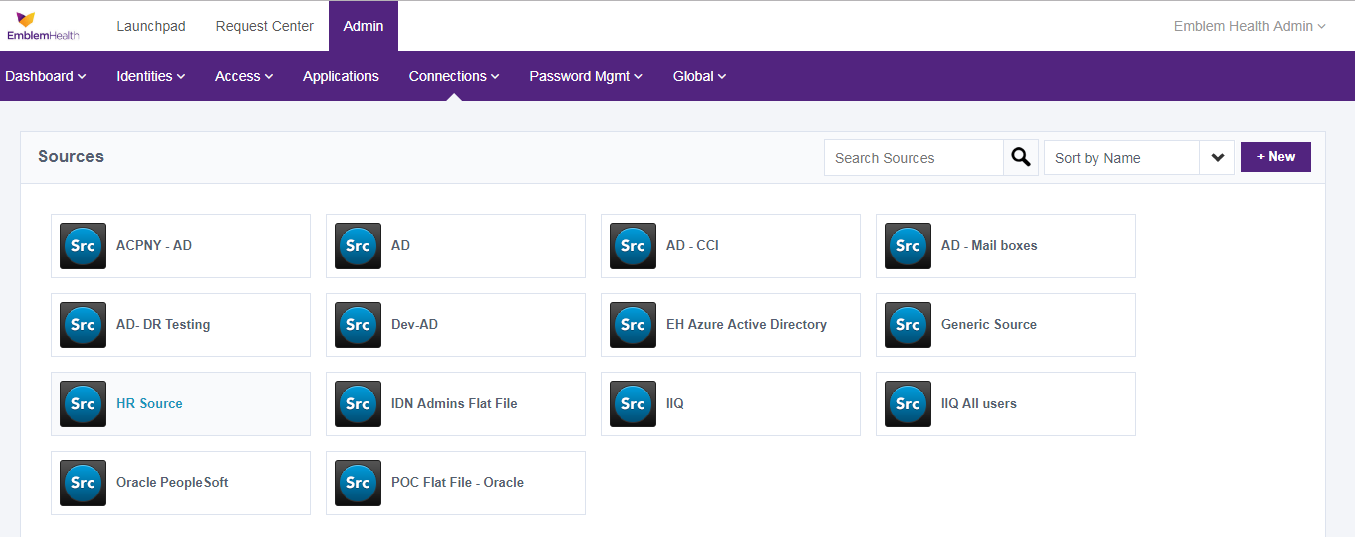
IQService runs on Windows server as a native service

Below are the steps to be performed to configure IQService for IdentityNow:

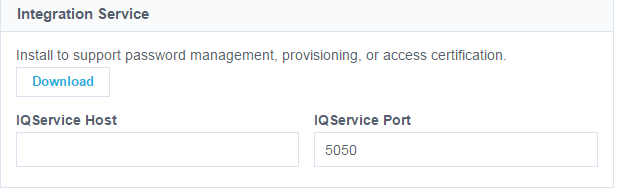
Login to IdentityNow as admin

Navigate to Admin tab

Go to Connection🡺Sources



Click on “ACPNY-AD”. Under “Integration Service”, click on the “Download” button.



This will download the IQService package to be installed and configured on a Windows server machine.

Now copy the package to a Windows machine and unzip it

Run below command to install IQService on the Windows box

IQService.exe –i

Please refer the below link for more information:

<https://community.sailpoint.com/docs/DOC-3871>

## Creating Source

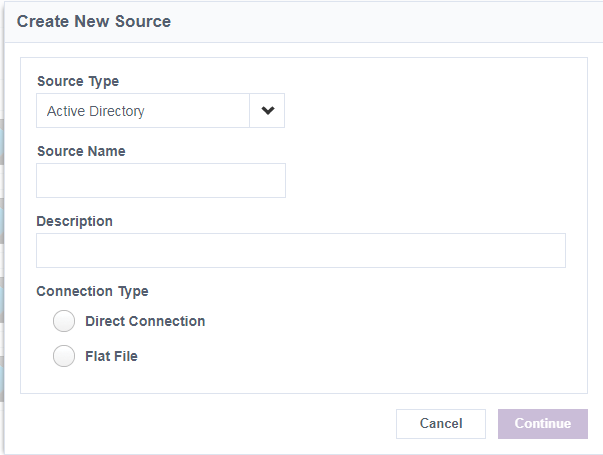
In IdentityNow, a source is a third party application, database, or directory management system that maintains its own set of user accounts or personnel records. IdentityNow collects data from these sources.

### ACPNY AD

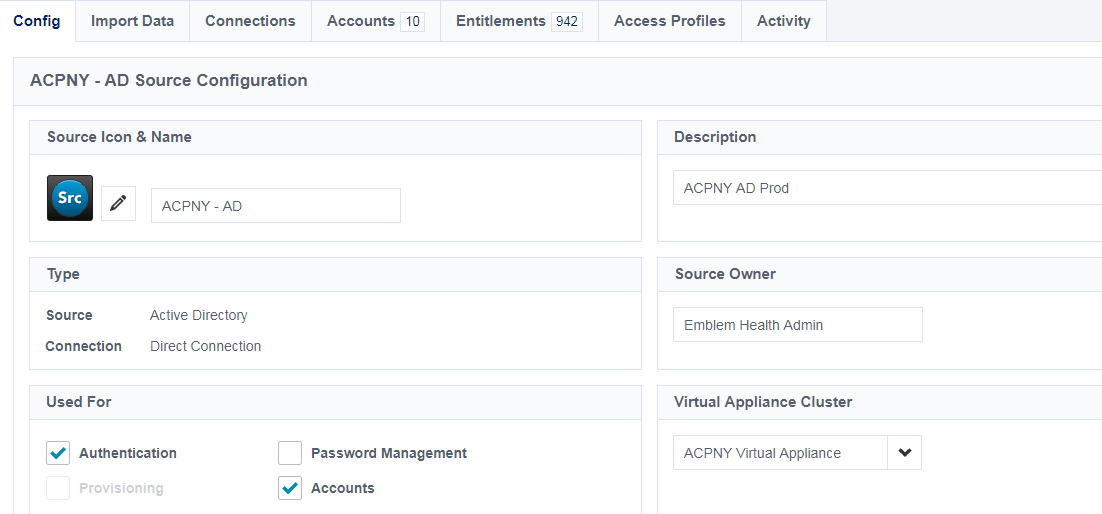
A source was created for ACPNY Active directory in IdentityNow to import ACPNY AD data.

Follow the below steps to create a Source in Identity Now

1. Sign in to IdentityNow and go to the Admin interface.
2. Go to **Connections > Sources**
3. **Click New**. The Create New Source dialog box is displayed.
4. **Select Source Type as Active Directory**
5. Enter a **Source Name** as ACPNY-AD and description as **ACPNY AD Prod**
6. **Under** Connection Type, select **Direct Connection**.
7. Click Continue



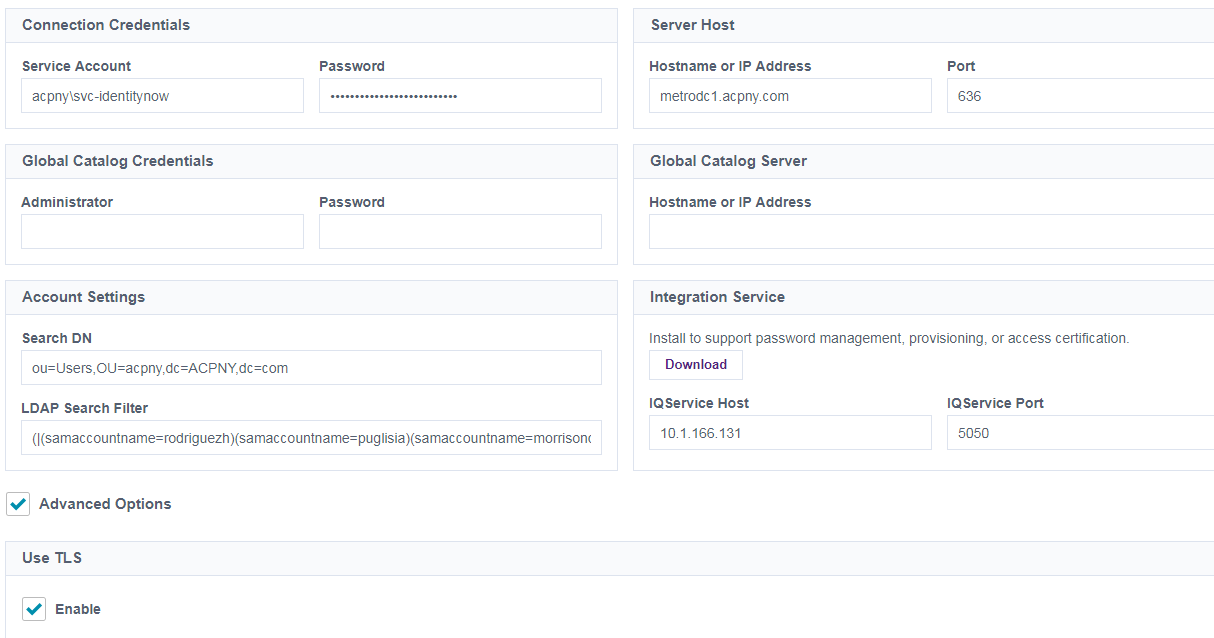
1. In the Active Directory Source Config panel, under **Used For**, select “Authentication” and “Account”.
2. Set the **Source Owner** as Emblem Health Admin.
3. In **Virtual Appliance Cluster**, select the virtual appliance cluster that will be used as the application connector for the source.



1. In the Connection Credentials enter the Service account created for Identity Now in ACPNY Active directory.

Add permission links

1. Set the host details and as well as the search DN for the Active directory we are trying to connect from Identity Now.
2. Enter the details of the server hosting the IQ service.
3. Check the Enable TLS option.



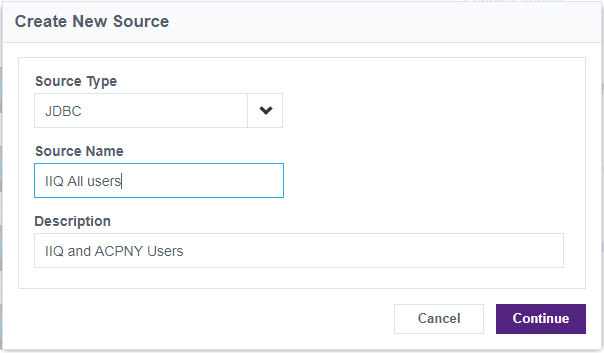
Note: The Query above will be (OU=Users,OU=ACPNY,DC=acpny,DC=com with one level search scope

1. Click on Save and Test Connection for testing.

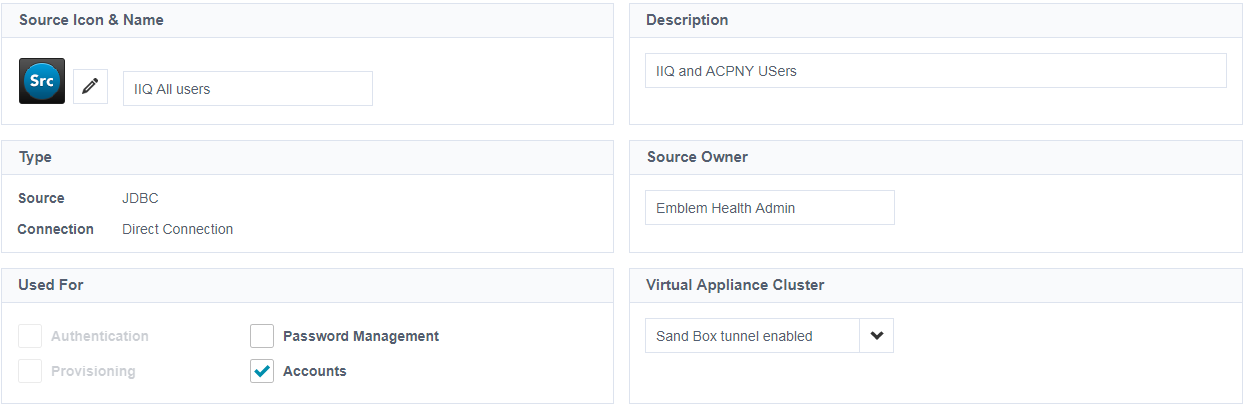
### IIQ ALL Users

A new source is created in IdentityNow was created that imported the consolidated data of ACPNY users and Emblem Health users in IdentityNow system*.*Follow the below steps to create a Source in Identity Now

1. Sign in to IdentityNow and go to the Admin interface.
2. Go to **Connections > Sources**
3. **Click New**. The Create New Source dialog box is displayed.
4. **Select Source Type as JDBC**
5. Enter a **Source Name** as **IIQ All users** and description as **IIQ and ACPNY Users**
6. Click Continue



1. Under **Used For**, select “Account”.
2. Set the **Source Owner** as Emblem Health Admin.
3. In **Virtual Appliance Cluster**, select the virtual appliance cluster that will be used as the application connector for the source.

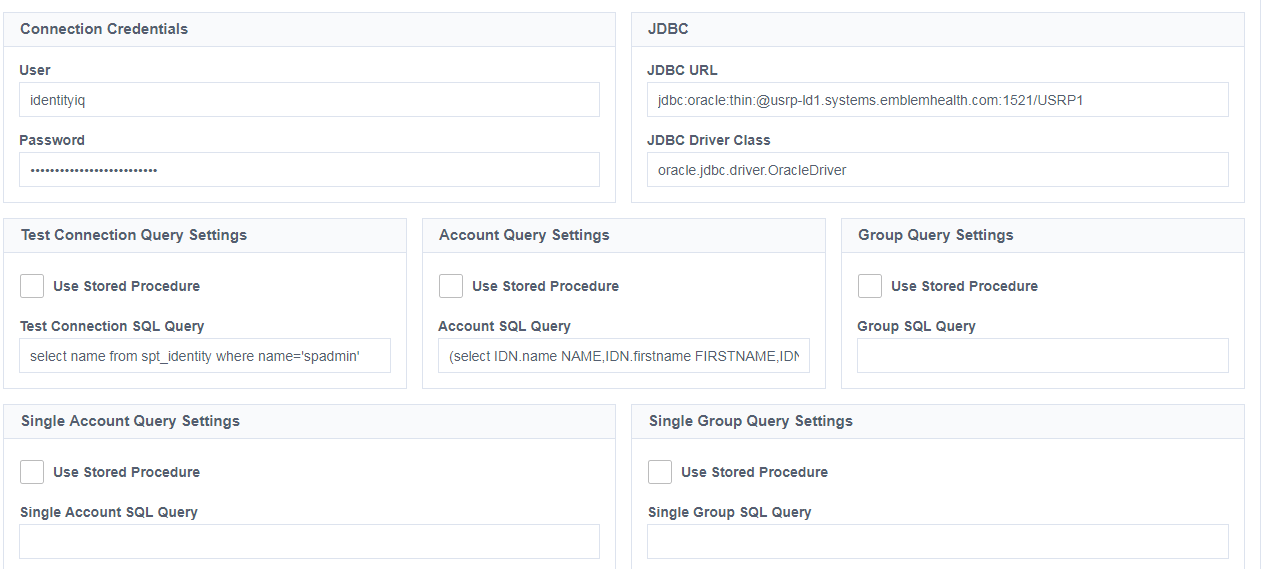


1. In the Connection Credentials enter the IIQ database schema username and password
2. Set the host details and as well as the driver for the database we are trying to connect from Identity Now.
3. In the “Test Connection Query Settings” update the below query

“select name from spt\_identity where name='spadmin'”

1. In the **“Account Query Settings”** update the below query:

(select IDN.name NAME,IDN.firstname FIRSTNAME,IDN.lastname LASTNAME,IDN.email EMAIL,IDN.display\_name DISPLAY\_NAME,MGR.DISPLAY\_NAME MANAGER,IDN.extended1 NETWORKID,IDN.extended2 ENDDATE,IDN.extended3 EMPLOYEETYPE from spt\_identity IDN, spt\_identity MGR where IDN.manager=MGR.id )UNION (select ACPNY.EMPLOYEEID NAME,ACPNY.FIRST\_NAME FIRSTNAME,ACPNY.LAST\_NAME LASTNAME,ACPNY.EMAILID EMAIL,ACPNY.DISPLAY\_NAME DISPLAY\_NAME,ACPNY.MANAGER MANAGER,ACPNY.NETWORKID NETWORKID,ACPNY.USER\_TERMINATION\_DATE ENDDATE,ACPNY.USER\_TYPE USERTYPE from EH\_SP\_Custom\_ACPNY\_Identity ACPNY)



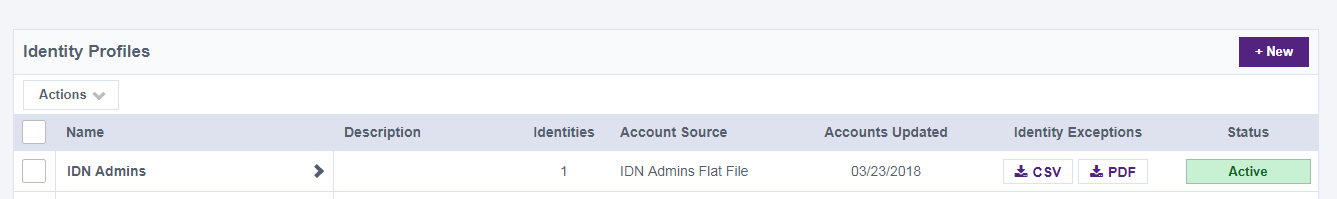
1. Upload the ojdbc7.jar file

## Setting up of Identity Profile

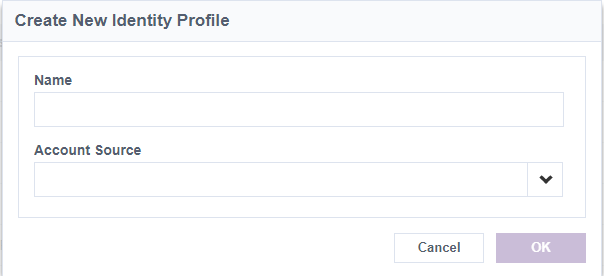
An identity profile represents the identity information loaded from a specific, authoritative source, the authentication method assigned to users from that source, and a variety of other information specific to that group of users. It also loads the users from the specified source into the system as identities.

Follow the below steps to create an Identity Profile in Identity Now

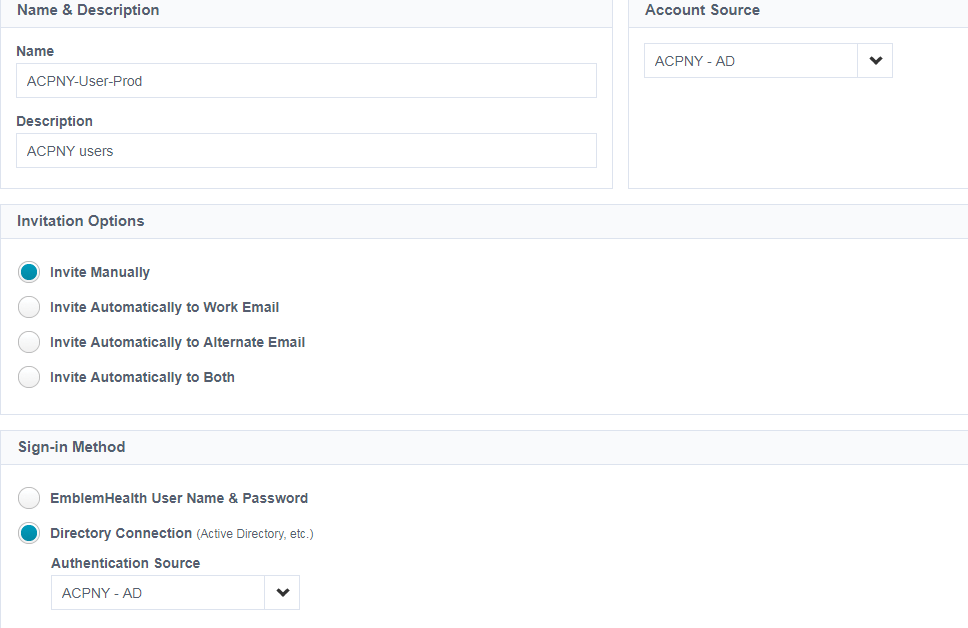
1. In the Admin interface, go to Identities > Identity Profiles.
2. Click New.



1. In Create New Identity Profile, provide a name for the new profile.



1. In **Account Source**, select the source you want to use as a basis for creating the identities. In this case
2. Click OK.
3. Provide a description of the identity profile.
4. Under **Sign-in Method**, select **Directory Connection and set the Authentication Source as ACPNY-AD.**



1. For setting Strong Authentication go to section [4.8](#_Two_Factor_Authentication) .
2. Click on Save.

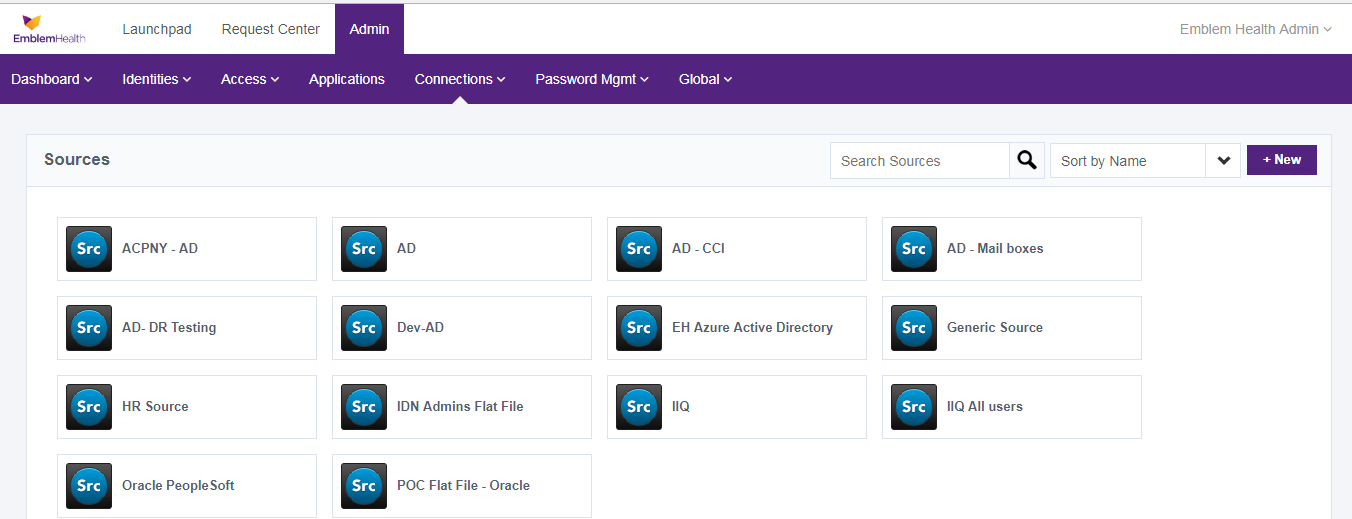
## User Load from On-premise IdentityIQ into IdentityNow

This activity is needed to load all EH and ACPNY user profiles from on-premise IdentityIQ into IdentityNow. In order to load all EH and ACPNY users from IdentityIQ, “IIQ” source would need to be configured in IdentityNow.

Below steps are followed to configure IIQ with IdentityNow:

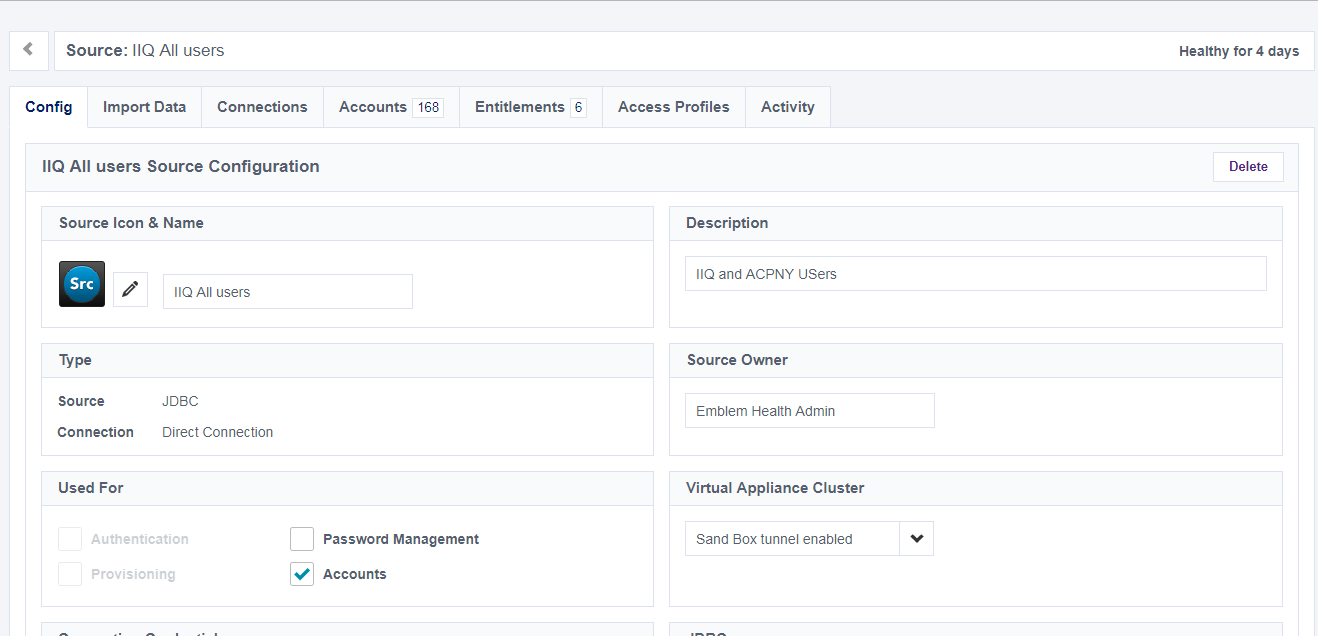
Login to IdentityNow as admin

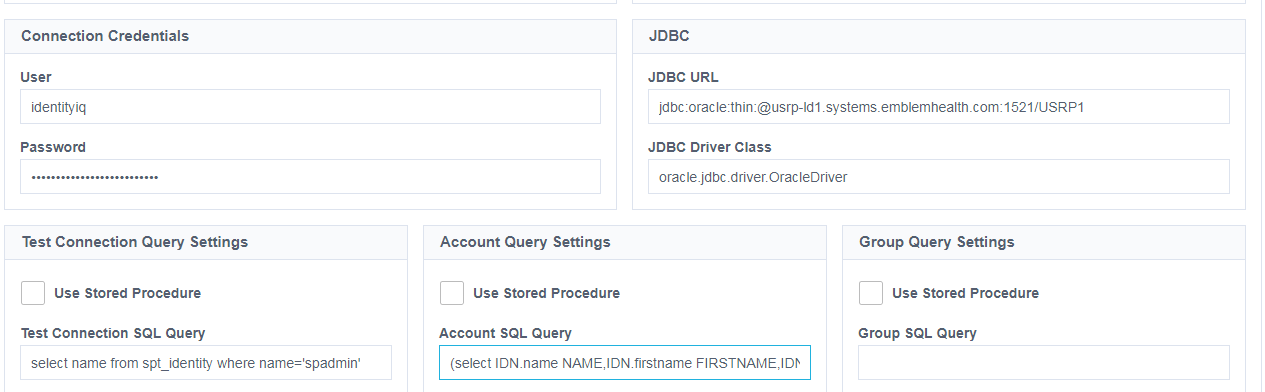
Navigate to Connections🡺Source



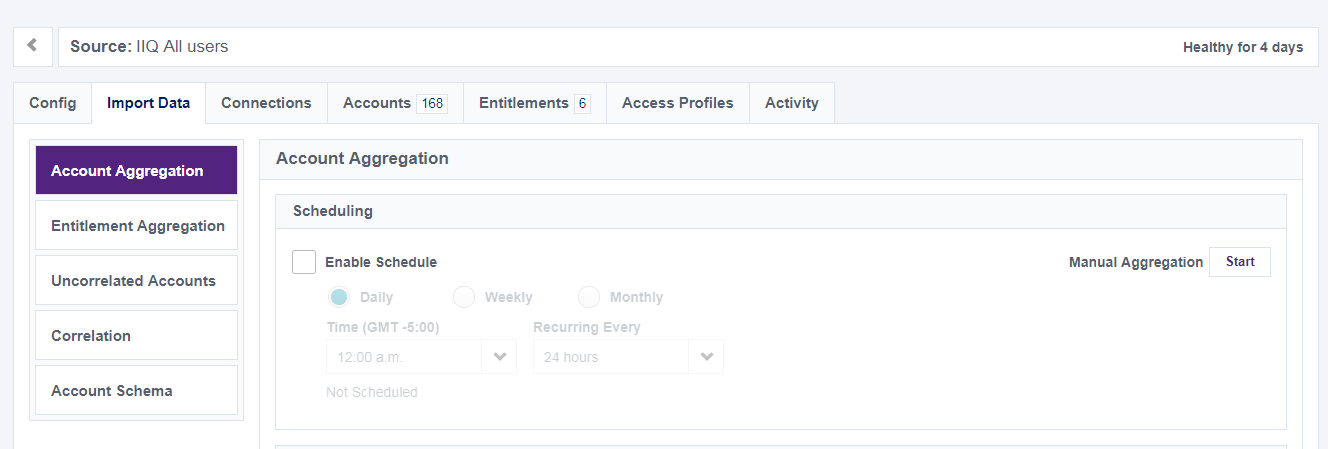
Click on IIQ All Users

Configure “IIQ All Users” with required connection and table (spt\_identity, EH\_SP\_Custom\_ACPNY\_Identity) details so that IdentityNow can connect to IIQ backend database to pull identities and load it in IdentityNow.





Go to Import Data tab and Click on Start in the Account Aggregation tab to load all the Emblem and ACPNY users.



This source will be used in the SSO applications.

## Pass-through Authentication

Pass-through authentication will allow ACPNY users to login into IdentityNow using their network credential without remembering another set of credential.

Pre-requisite:

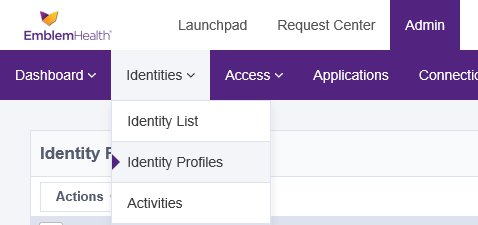
* One AD application should be configured as source
* The AD source should have “Authentication” option checked under “Used For” section in IdentityNow
* IQService needs to be installed and configured on a Windows box

Below are the steps to be followed to configure pass-through authentication in IdentityNow

Login to IdentityNow as admin

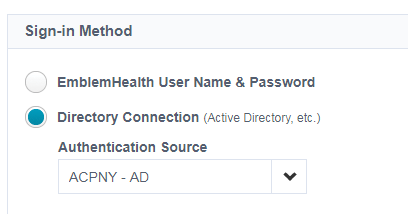
Navigate to Admin tab

Go to Identities🡺Identity Profiles



Select an identity to set authentication method

Select “Direct Connections” option radio button and select “ACPNY-AD” application from dropdown.



Save the changes

## Network Boundary Definition

It is important to define ACPNY network boundary in IdentityNow to achieve below purposes:

1. Users accessing IdentityNow from within ACPNY network do not need to authenticate again will not be prompted for strong authentication
2. Strong Authentication will be enforced only for accessing IdentityNow from Internet

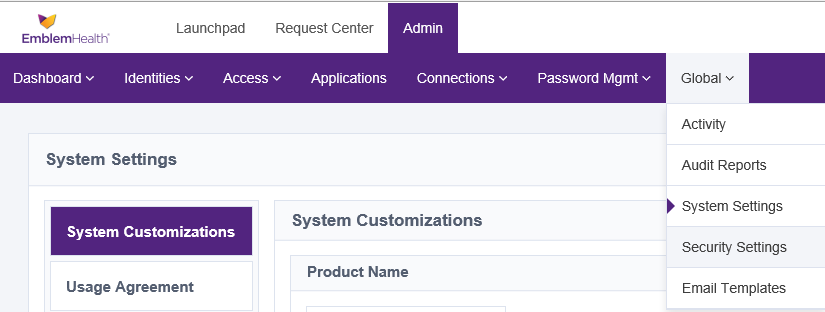
**Note**: Before proceeding with below configuration changes in IdentityNow, interfacing public IP address blocks need to be received from networking team. These IP addresses will be the ones when users connect to Internet from within ACPNY Network.

EmblemHealth Production Public IP Blocks are given below:

* 162.254.244.2/28
* The DR Ip address

To define network boundary in IdentityNow, follow below steps:

1. Login to IdentityNow using admin privilege and navigate to **Global🡪System Settings**



1. Under “Network Definition” panel, add the network IP address blocks



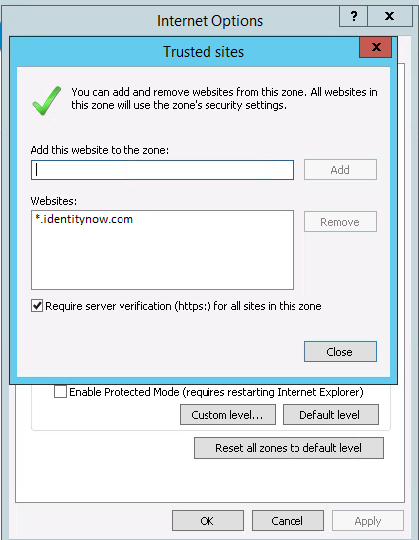
1. Click on “Save” button.

### Web Browser Configuration

Follow the steps to configure Internet Explorer web browser to support Kerberos:

1. Open web browser and navigate to **Tools🡪Internet Options🡪Security🡪Trusted Sites**. Add below URL as trusted sites. Once done, click “Close”.

* **\*. identitynow.com**



1. Click on “Custom level…” button under same “Trusted Sites” option. Make sure “Logon” option is set to “***Automatic Logon with current username and password***” under “User Authentication” tab

[Note: In test environment, above steps need to be performed manually. In production, these are ideally pushed through AD GPO. Reference: <https://docs.pingidentity.com/bundle/p1_adconnectInstall_cas/page/adAgent_addTrustedIeGroupPolicy.html> ]

## Password Authentication for Intranet Access

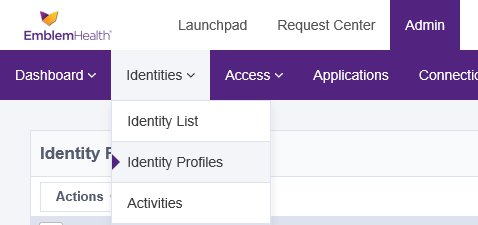
Any request coming from ACPNY network (determined by matching the IP address of the incoming request packet with the ones configured in IdentityNow under “network Definition” panel.) results default password authentication. User needs to key in ACPNY network ID and password for sign-in if the user tries to access Identity Now from within ACPNY network.

## Two Factor Authentication for Internet Access

For requests that are outside of ACPNY network (determined by matching the IP address of the incoming request packet with the ones configured in IdentityNow under “network Definition” panel.) will have to undergo strong authentication wherein after hitting the Identity Now url and putting the Network Id and password the user is prompted for a second factor authentication screen.

Follow below steps to configure Two factor authentication for IdentityNow internet access

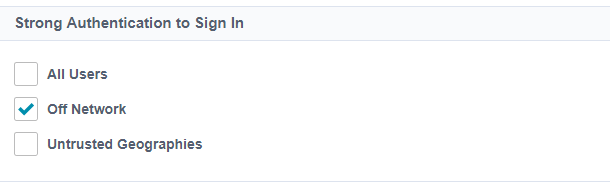
1. Login to IdentityNow using admin privilege and navigate to **Identities🡪Identity Profiles**



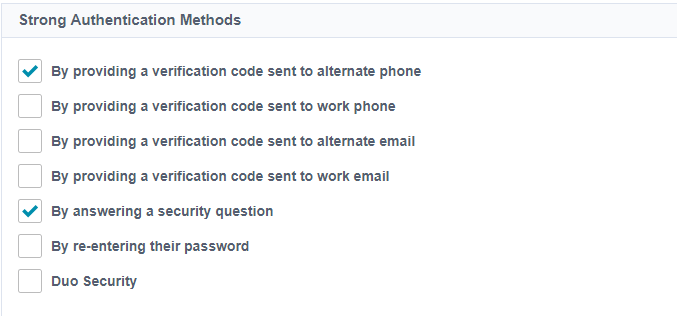
1. Click on the correct identity profile.



1. Under “**Settings**” tab, go to “Strong Authentication” panel and select the checkbox “All Users”



1. The selections mentioned in the below screen needs to be done for Strong Authentication Method”.



1. Click “Save” button.

**Note:** The below user attributes are configuredfor use in Strong authentication.

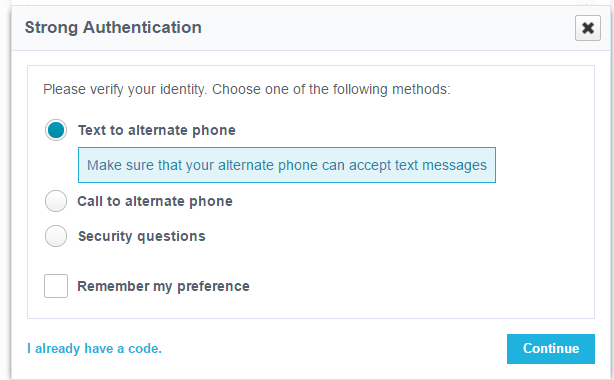
|  |  |
| --- | --- |
| **Attribute** | **Value** |
| Alternate phone | User mobile phone number |
| Security Questions | The security questions set during first time login to identity now. |

## Set Preference

User can set a few parameters in its preference of IdentityNow which will help them to establish authenticity of the identity during forgot password or unlock account etc. IdentityNow preference will allow users to update secret question/answers, phone number, email addresses to be used to communicate one time token codes or password reset emails respectively.

Below are the steps to be performed to set preferences:

* + - 1. Login to IdentityNow using their network ID and password
      2. If the user logs in to IdentityNow for the first time, IdentityNow will ask to set secret questions/answers, alternate/work email addresses
      3. If user is not a first time login, then already set preferences can be changed by clicking on “Preference” link to change any or all of the following:
         1. Alternate Email Address
         2. Work Email Address
         3. Alternate Phone Number
         4. Work Phone Number
         5. Answers of Secret Questions
      4. Click on “Edit” button to change preference
      5. Upon clicking on “Edit” button, strong authentication prompt will appear to re-check authenticity of the logged user again



* + - 1. Choose any of them and continue to authenticate to IdentityNow

Once done, edit preferences followed by clicking on “Save” button

# Appendix

## Duplicate Users

The excel sheet shared by the ACPNY team contains 2 duplicate users that are both present in Emblem health AD and ACPNY AD and are active.

The users are

|  |  |
| --- | --- |
| **ACPNY User DN** | **Emblem User DN** |
| CN=Steve Welsh,OU=Atos,OU=Vendors,OU=ACPNY,DC=acpny,DC=com | CN=Welsh\, Sean,OU=Employees,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM |
| CN=Lauriellen James,OU=Atos,OU=Vendors,OU=ACPNY,DC=acpny,DC=com | CN=James\, Latetra,OU=Employees,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM |

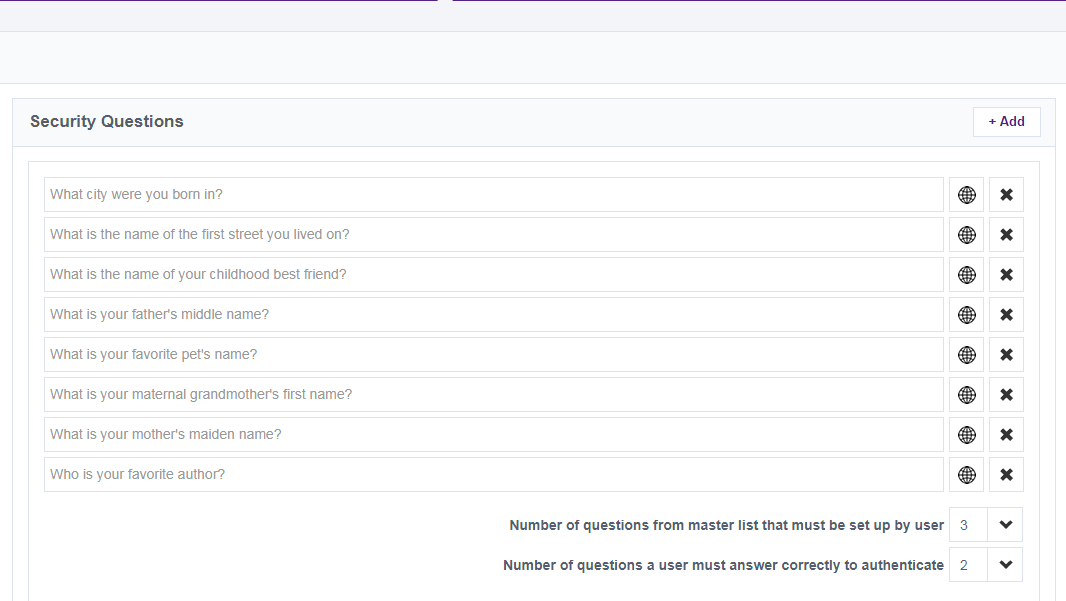
## Documents

|  |  |
| --- | --- |
| **Document** | **Location** |
| VA Configuration | Z:\3 PROJECTS and ACTIVITIES\2018\IAM Transformation\Sailpoint\_IdentityNow\ACPNY\VA Configuration Guide.docx |
| Setting up AD Access Permissions | Z:\3 PROJECTS and ACTIVITIES\2018\IAM Transformation\Sailpoint\_IdentityNow\ACPNY\AD Service Account Permissions.docx |
| ACPNY AD OU’s Diagram | Z:\3 PROJECTS and ACTIVITIES\2018\IAM Transformation\Sailpoint\_IdentityNow\ACPNY\AD OUs.vsd |

## Set of Secret Questions in Identity Now

Identity Now has a set of security questions that the user needs to select from on first time login to IdentityNow Portal.

User must select 3 security questions from the dropdown and User need to answer 2 security questions for Strong Authentication. Below Screenshot contains the security questions set in Identity Now.



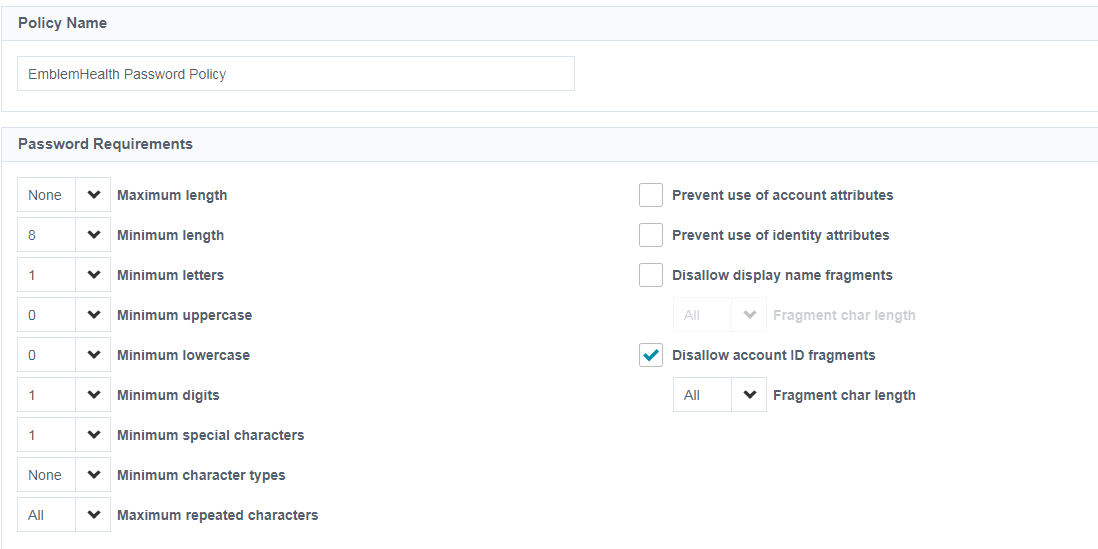
## Password Policy

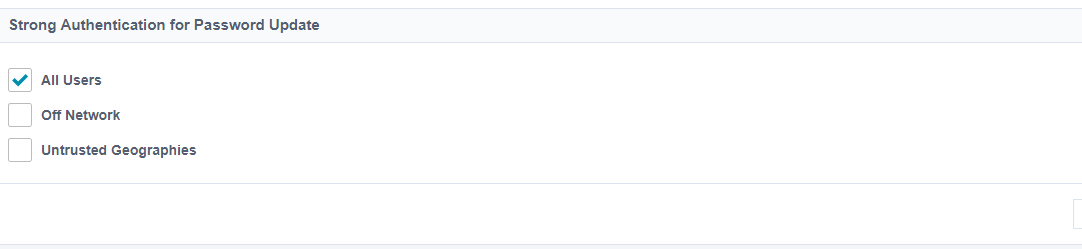
The Below Password Policy is set in Identity Now.

a) Minimum of eight (8) characters long.

b) Consist of a combination of following items:

* Minimum 1 letter
* Minimum 1 Numbers
* Minimum 1 Special characters





# Reference

* Setting up Virtual Appliance: <https://community.sailpoint.com/docs/DOC-9372>
* IdentityNow SAML URL: <https://community.sailpoint.com/docs/DOC-2192#jive_content_id_URLs_for_IDPInitiated_SAML_Requests>
* Setting up AD Access Permissions: <https://community.sailpoint.com/docs/DOC-2431>