SailPoint Integration with RadiantOne: Deployment Guide

Contents

Chapter 1: Overview

SailPoint IdentityIQ Lifecycle Manager improves end user productivity through fast, automated provisioning of access changes. This also reduces administrative burden on IT and help desk personnel and prevents inappropriate access to sensitive corporate data. Identities are imported from a variety of sources into the IdentityIQ Identity warehouse. From here, they are analyzed for compliance and provisioned out to target applications. A high-level SailPoint Infrastructure diagram is shown below.

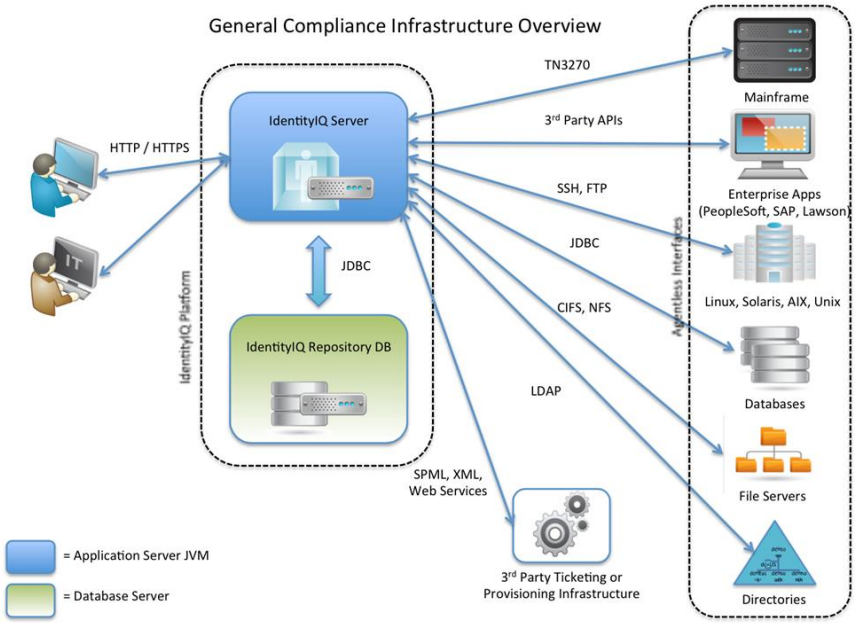

Figure 1. 1 : SailPoint Infrastructure Overview

RadiantOne FID manages identities and groups across a heterogeneous mix of sources, and can supply SailPoint with a reference image to provision target applications. This can reduce customization and integration costs, and accelerate the deployment of SailPoint.

Note - The purpose of this integration guide is to describe how to configure RadiantOne FID as an application for SailPoint allowing it to import the global reference list from FID into the IdentityIQ Identity Warehouse. Once the accounts are imported, provisioning policies can be defined. Steps to configure provisioning policies are out of the scope of this document.

SailPoint accesses the RadiantOne FID as a single LDAP application, and the LDAP queries are translated into the correct protocol for the appropriate backend sources. A high-level integration diagram is shown below.

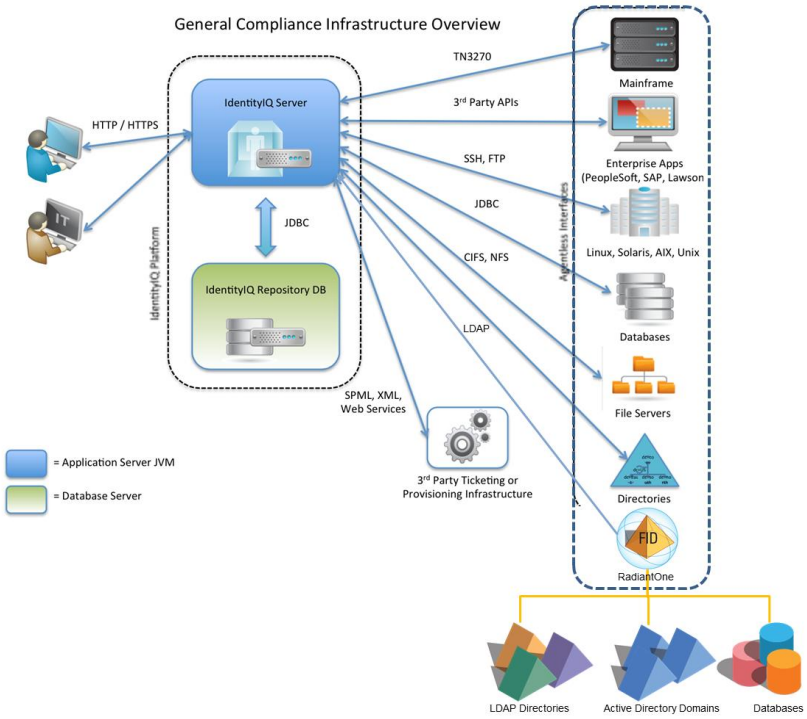

Figure 1. 2 : SailPoint with RadiantOne Integration Overview

Some of the many benefits of deploying RadiantOne include:

- RadiantOne is a supported application for SailPoint so integration works out-of-the-box.
- By acting as an abstraction layer between user directories and database, RadiantOne reduces the number of applications needed in SailPoint, simplifying the configuration and maintenance of the SailPoint deployment.
- RadiantOne provides a consolidated list of identities. Unique identities are merged into one virtual entry containing the global profile.
- RadiantOne solves identity and group integration problems and SailPoint is shielded from the complexities of evolving data source (e.g. mergers and acquisitions, divestitures…etc.). As new data sources are mounted in the RadiantOne namespace, the users and groups are automatically detected and imported by SailPoint.
- RadiantOne FID access is not limited to SailPoint, allowing other applications to benefit from the identity integration initiative and maximizing your return on investment.

Global Profile – Source Image for Provisioning

RadiantOne can join objects across multiple data sources, adding significant value. Joins allow you to create a complete user profile. RadiantOne can categorize users based on any attributes of their global profiles and automatically assign people to groups making them appear as static groups as well.

See the diagram below for an example:

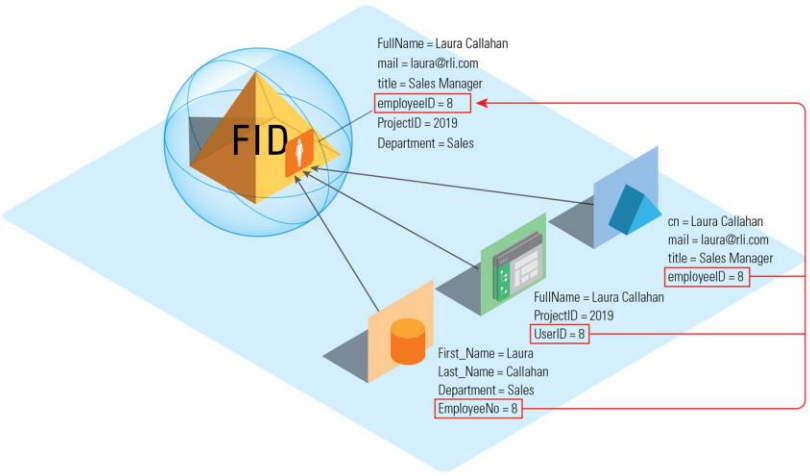

Figure 1. 3 : Example of Join in RadiantOne

Chapter 2: RadiantOne Configuration

Configuring RadiantOne for use with SailPoint can be accomplished in the following steps:

1. Use Virtual Identity Wizard to create virtual view of identities

2. Use Groups Builder Wizard to create virtual view of groups

Defining Virtual View for Identities

With RadiantOne FID as a virtual abstraction layer, identities that are scattered across the infrastructure (from AD, LDAP, RDBMS, Web Services) are integrated and presented in a common namespace.

In order for SailPoint to identify a user in the virtual namespace and be able to locate entries from many different types of underlying sources, the schemas must be mapped to a common naming context. For RadiantOne FID configured as an LDAP application, the mapping should be based on the criteria that SailPoint uses to search for users. For example, if user entries are searched based on a filter of *objectclass=user,* all required objects must match this class definition. Object class and attribute mapping are addressed by RadiantOne FID. The diagram below depicts an example.

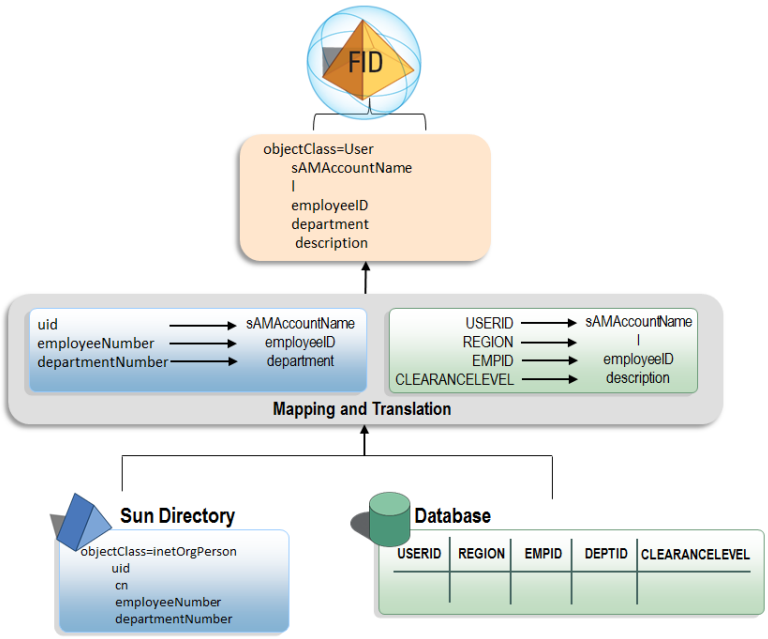

Figure 2. 1 : Example of Mapping Performed by RadiantOne

Basic RadiantOne FID configuration steps are described below. This assumes there are three sources of identities and there is overlap of users. Overlapping users can be identified/joined based on their employee number. The sources will be an HR database (containing all users),

an LDAP directory (containing only contractor accounts) and Active Directory (containing only employee accounts). The configuration used throughout this integration guide involves building a unique global list of users across Active Directory and an LDAP directory, and then extending these entries with additional attributes from a database. This use case is depicted in the diagram below.

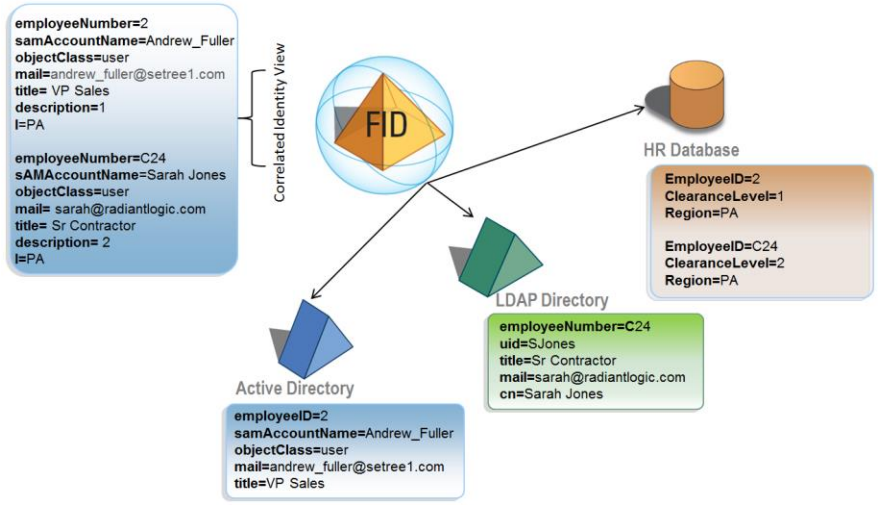

Figure 2. 2 : Example of a Virtual View in FID

Although there are many possible ways to configure virtual views for identities, this integration guide will leverage the Virtual Identity Wizard. For more details on this wizard, please see the *RadiantOne Identity Service Wizards Guide*.

Define Source Objects

1. Start the RadiantOne Main Control Panel.
2. Log in with *cn=directory manager* and the password you defined for this user during the RadiantOne install when prompted.
3. On the Main Dashboard tab, from the drop-down menu, select Start.
4. On the Wizards tab, click on the Virtual Identity Wizard.
5. Click NEXT.
6. Click new and enter a project name (e.g. spusers) and click NEXT.
7. If you do not already have the schemas extracted from the data sources (or even data sources defined), use the + button to do so. The schema objects selected must be the ones associated with the user entries in the backends (e.g. InetOrgPerson for the LDAP, and user for AD). For more information incuding exact steps on this process, please see the *RadiantOne Identity Service Wizards Guide*.
8. After connections to the backends are established and the schemas have been extracted, the drop-down list will be be populated with these objects. Select the object (e.g. objectclass) for each of the data sources and use the button to define it as a "Selected Identity Object".

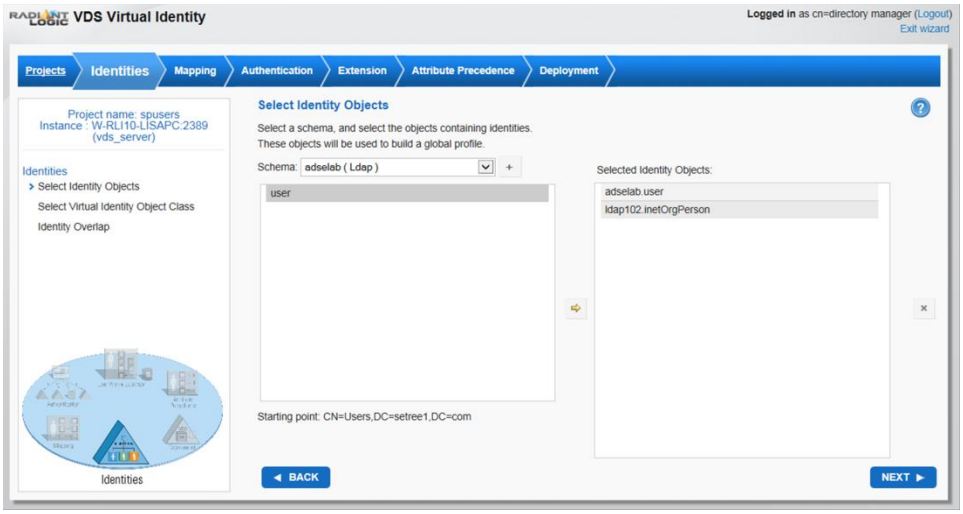

Figure 2. 3 : Defining Identity Source Objects

9. Click NEXT ►.
10. Select the objectclass to associate the virtual entries with. You should make sure that the objectclass you select here later matches the one used to configure the application in SailPoint (e.g. user).
11. Click NEXT ►.

Define Attribute Mapping

1. Choose the No option to indicate there is no user overlap across the Active Directory and LDAP directory. Active Directory contains only employee accounts and the LDAP directory only contains contractor accounts in this example.
2. Click NEXT ►.
3. Click NEXT ►.
4. For each identity object in the drop-down list, define the attributes you want to return from each source (and what attribute they should be mapped to in the virtual entries). In this example, the attributes mapped from AD are: employeeNumber, givenName, mail, postalCode, sAMAccountName, sn, title, userPrincipalName. The attributes mapped from LDAP are: employeeNumber, givenName, mail, sn, title, and uid.
5. Click NEXT ►.
6. Select an attribute that contains a unique value for all users as the identification attribute.
7. Click NEXT ►.

Define Join to Extend Entries

As mentioned in the beginning of this section, the unique list of users from AD and LDAP will be extended with attributes from an HR database (because all user accounts are in the HR database). In the next step of the wizard, this join will be defined.

1. If you do not already have the schemas extracted from the database (or even a data source defined), use the + button to do so. The schema object (table) selected must be

the one associated with the user entries in the backend and contain the attributes you want to use to extend the entries with. For more information incuding exact steps on this process, please see the *RadiantOne Identity Service Wizards Guide*.

2. Select the schema object from the source object list on the left and use the  button to move the object into the Selected Join Objects column on the right.

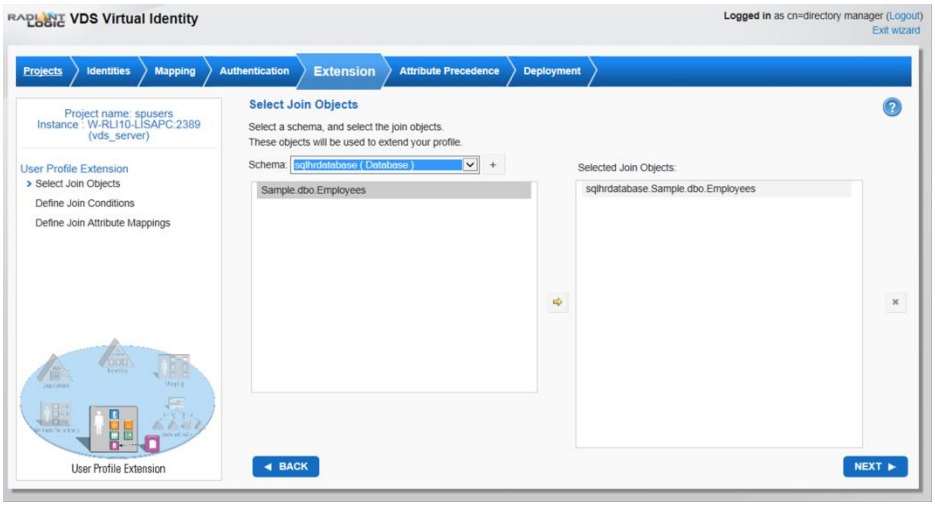

Figure 2. 4 : Defining Join Object

3. Click  .
4. Select the join object and click EDIT to define the join condition. This example will base the join on employeeNumber for the global, unique list matching EmployeeID in the database table. Click  .

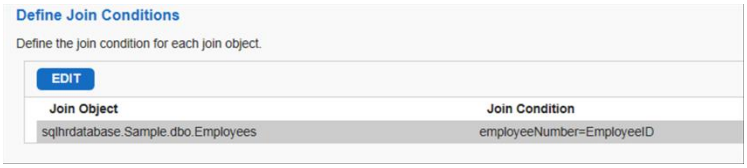

Figure 2. 5 : Defining Join Condition

5. In this example, the ClearanceLevel attribute in the database will be mapped into the description attribute of the global profile and the Region attribute will be mapped to the l attribute.

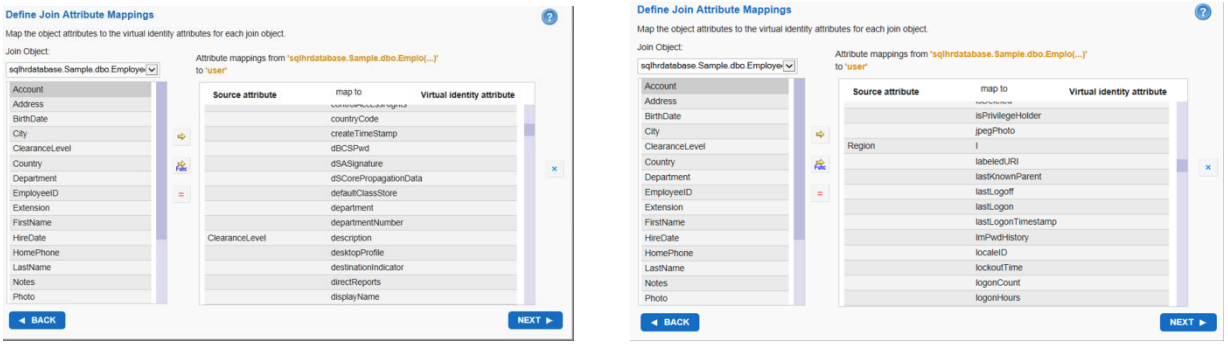

Figure 2. 6 : Defining Attribute Mapping from Join/Secondary Object

6. Click NEXT ►.
7. Choose to mount the virtual view of identities under a naming context (e.g. ou=people,o=sailpoint) and click NEXT ►.
8. Define a persistent cache with refresh and initialize the cache. For complete details your caching options and refresh strategies, please see the *RadiantOne Deployment and Tuning Guide*.
9. Click FINISH to complete the wizard.

Defining Virtual View for Groups and Membership

RadiantOne FID can act as a single data source for accessing group information. It can map and aggregate existing groups contained in multiple heterogeneous backend data sources and/or dynamically build groups on-the-fly based on any attributes of the user entries. Either way, this allows applications to search in one directory to find the group and evaluate the members. The diagram below depicts user-defined groups where members are dynamically determined based on attributes available in the user profiles. Also shown is how RadiantOne can compute membership and return a memberOf attribute in the user entries.

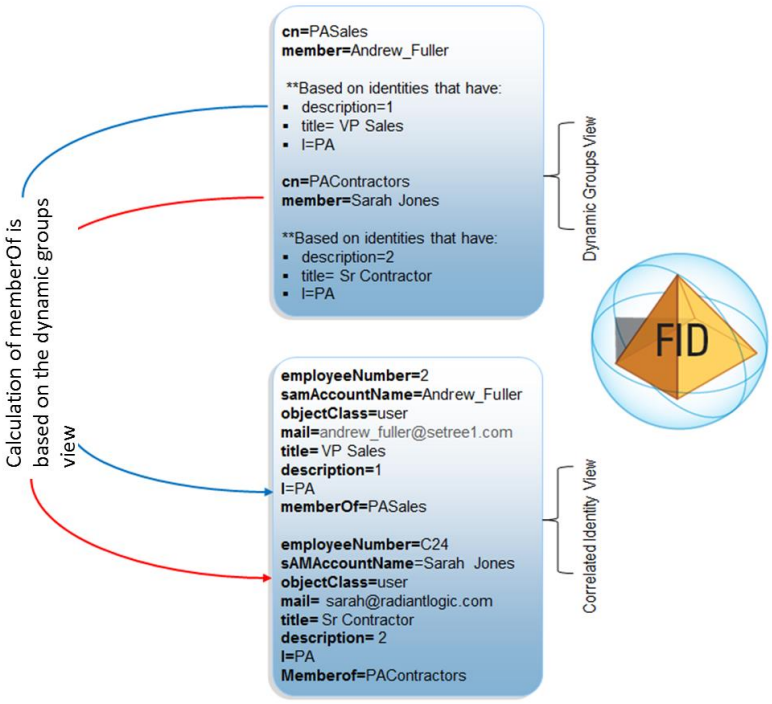

Figure 2. 7 : Example of User-Defined Groups with Dynamic Members

In order for applications to locate groups, the schemas must be mapped to a common naming structure. The naming should be based on the criteria that the application uses to search. For example, if SailPoint is configured to look for group entries based on a filter of objectclass=group, then all required groups objects must match this class definition. Both objectclass and attribute mappings are addressed with RadiantOne FID.

From SailPoint's perspective, RadiantOne FID returns a list of groups and members corresponding to the search request. The complexity of how the groups and members are actually built is hidden and happens behind-the-scenes. You gain the advantage of having attribute-driven groups as opposed to statically defining members solely based on the group name.

Basic configuration steps for building user-defined groups are described below. This assumes that all users (possible group members) have been aggregated in RadiantOne FID below a common naming context (e.g. ou=people,o=sailpoint) and groups will be dynamically built based on specific attribute criteria. For more details on the Groups Builder Wizard please see the *RadiantOne Identity Service Wizards Guide*.

Define Group Names

1. Start the RadiantOne Main Control Panel.
2. Log in with *cn=directory manager* and the password you defined for this user during the RadiantOne install when prompted.

3. On the Main Dashboard tab, from the drop-down menu, select Start.
4. On the Wizards tab, click on the Groups Builder Wizard.
5. Click NEXT ► on the introduction page.
6. Click NEW and enter a project name (e.g. spgroups).
7. Click NEXT ►.
8. Decide on which objectclass to associate the group entries with. To match the configuration in this deployment guide, the *group* objectclass will be used.
9. You have the option to configure user-defined groups or auto-generated groups. For purposes of the example used in this integration guide, user-defined groups are described. For more information on user-defined and auto-generated groups, please see the *RadiantOne Identity Service Wizards Guide*.

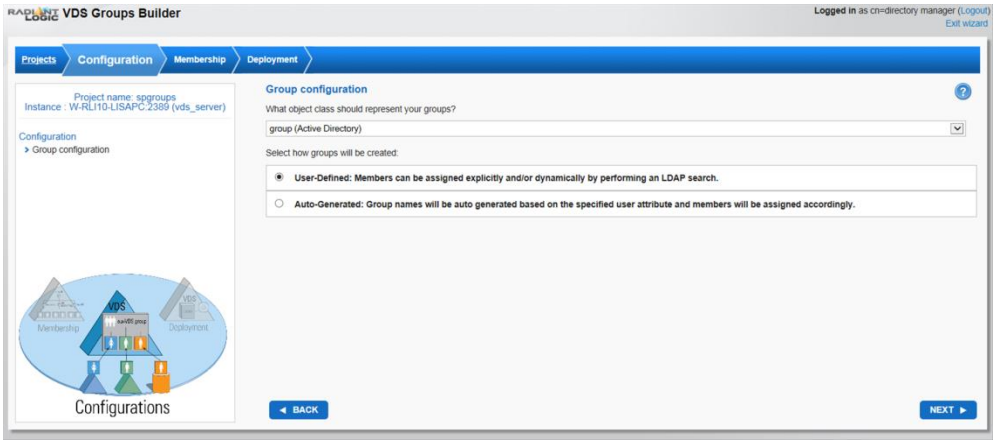

Figure 2. 8 : Defining a Virtual View for User-Defined Groups

10. Click NEXT ►.
11. To match the configuration in this deployment guide, a group named PAContractors and a group named PASales will be created. Click NEW GROUP and enter PAContractors for the group name and click NEXT ►.
12. Click NEW GROUP and enter PASales for the group name and click NEXT ►.

Define Group Members

1. Select the PASales group and click on Define Dynamic Members.
2. The search base dn should be ou=people,o=sailpoint (e.g. of the aggregated list of users).
3. The search scope can be *one* as all group member candidates will be one level below ou=people,o=sailpoint.
4. In the context of this integration guide, the filter to determine group members should be any user profile that contains a title of “VP Sales”, a description of “1” and a l of “PA”. See this example in the screen shot below.

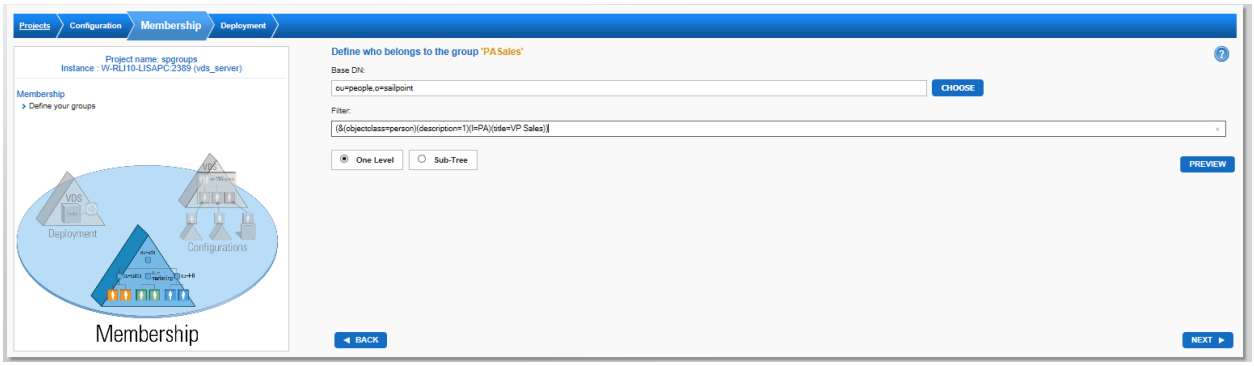

Figure 2. 9 : Defining Dynamic Member Criteria

5. Click NEXT ►.
6. Select the PAContractors group and click on Define Dynamic Members.
7. The search base dn should be ou=people,o=sailpoint (e.g. the aggregated list of users).
8. The search scope can be *one* as all group member candidates will be one level below ou=people,o=sailpoint.
9. The filter to determine group members should be any user profile that contains a title of “Sr Contractor”, a description of “2” and a l (location) of “PA”. See this example in the screen shot below.

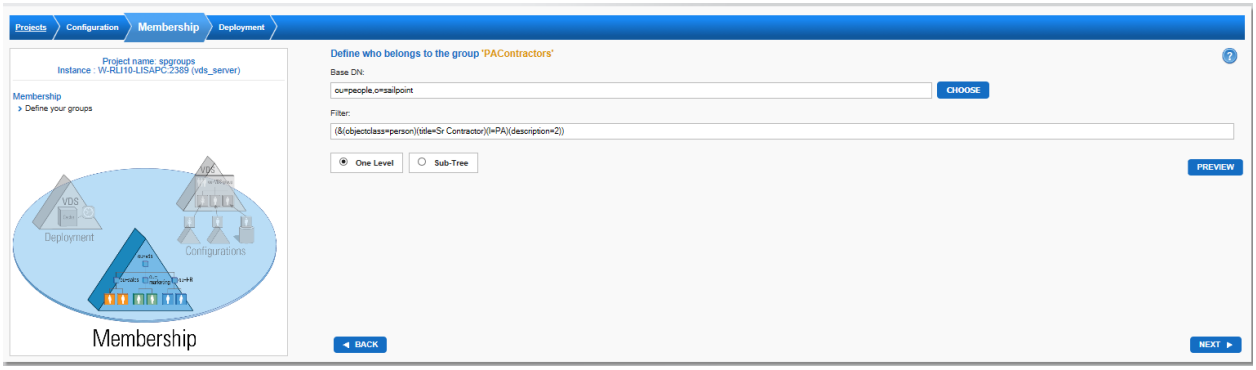

Figure 2. 10 : Defining Dynamic Group Member Criteria

10. Click NEXT ►.
11. Click NEXT ► again as this example will not add any more groups or members.
12. Choose the option to Mount Under an New Naming Context (e.g. ou=groups,o=sailpoint).

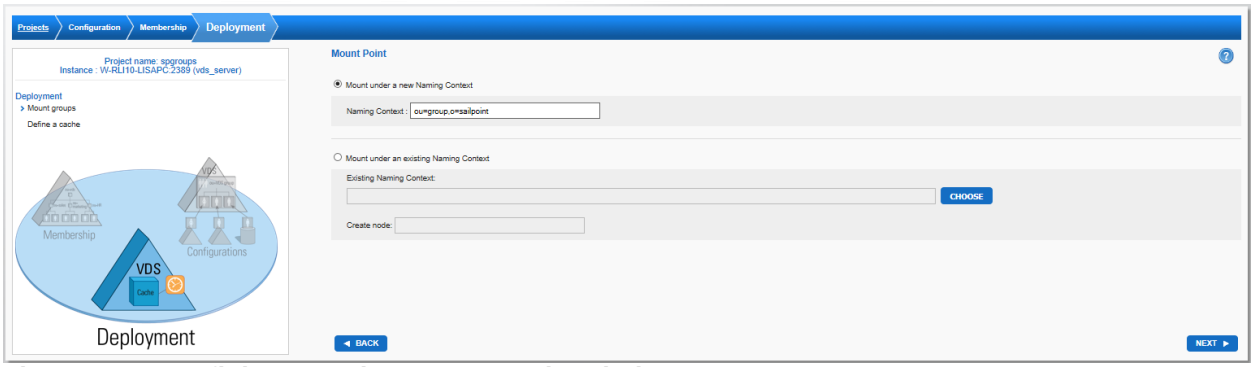

Figure 2. 11 : Defining Location to Mount Virtual View

13. Click NEXT ►.
14. Define a persistent cache with refresh (to avoid having to evaluate the membership rule every time this virtual view is searched) and initialize the cache. For complete details your caching options and refresh strategies, please see the *RadiantOne Deployment and Tuning Guide*.

Define Computation for MemberOf

Now that the virtual identities are assigned to proper virtual groups, a computation for memberOf can be defined on the identity view so the group membership can be reflected in the user entries. Even if you don't leverage the mapping for memberOf when importing accounts into SailPoint, other applications can access FID and retrieve group membership by using the memberOf attribute of the user account instead of searching the group entries directly.

Although there are different methods within RadiantOne to define this computation, this document describes using the RadiantOne Main Control Panel. The high level steps are defined here. For more details on the RadiantOne Main Control Panel, please see the *RadiantOne System Admin Guide*. Remember, prior to following the configuration in this section, you should have configured a persistent cache for your groups virtual view (as described in the previous section).

1. Launch the RadiantOne Main Control Panel.
2. Log in with *cn=directory manager* and the password you defined for this user during the RadiantOne install.
3. Click Settings → Interception → Special Attributes Handling (requires Expert Mode).
4. In the isMemberOf section, click the + Add button. The Add Mapping window displays.
5. Click the Choose button. Select the root naming context where the identity view is mounted (e.g. o=sailpoint). Click OK.
6. Click the + Add button below Groups Location. Select the root naming context where the groups are mounted (e.g. o=sailpoint). Click OK.
7. Enter *memberOf* for the isMemberOf Attribute Name.

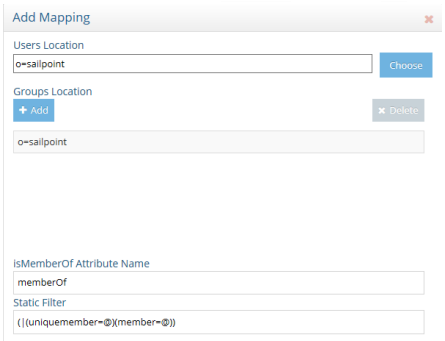

Figure 2. 12 : Computation for MemberOf Attribute

8. Click OK.
9. Click Save in the upper-right corner.

Chapter 3: SailPoint Configuration

Configure RadiantOne FID as an Application

In order to be the reference image used to provision targets, RadiantOne FID must be configured as an application in SailPoint.

1. Log into the SailPoint Admin Console.
2. Click on the Application menu and select Application Definition

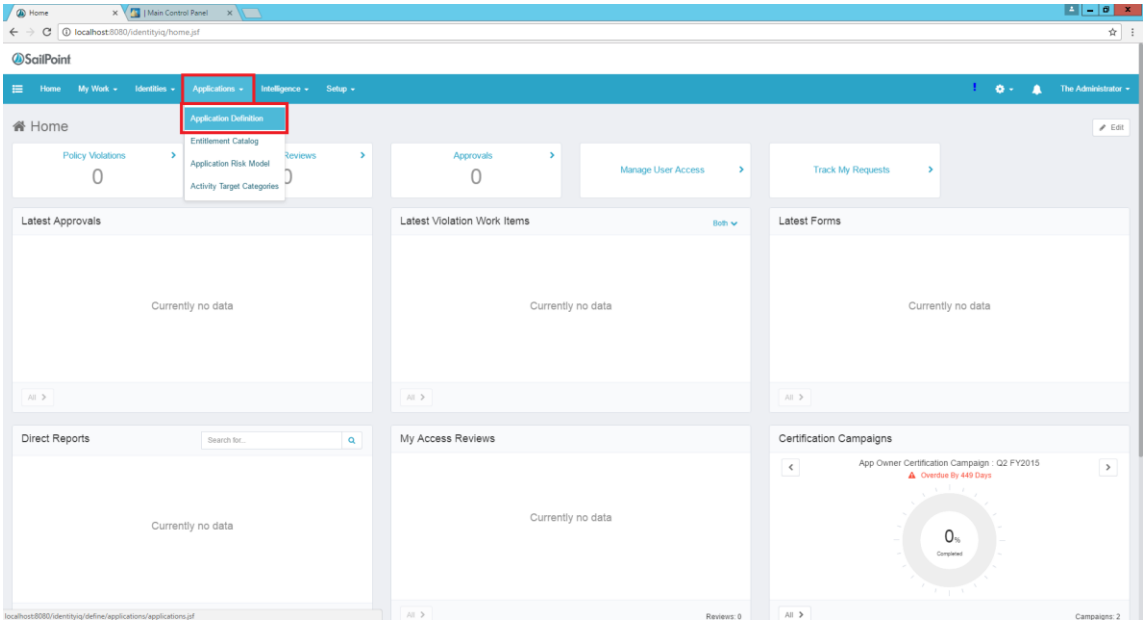

Figure 3. 1 : SailPoint Application Menu

3. Click on Add New Application.

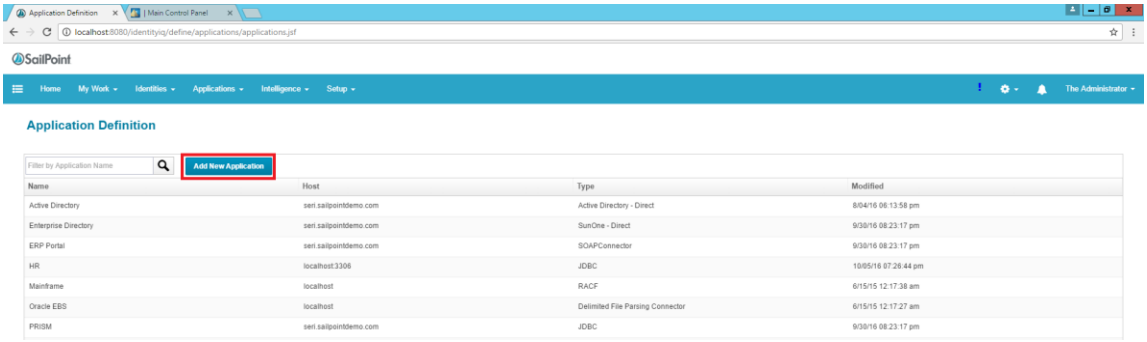

Figure 3. 2 : Adding a SailPoint Application

4. On the Details tab, enter a unique name to represent RadiantOne FID and select *LDAP* for the Application Type.

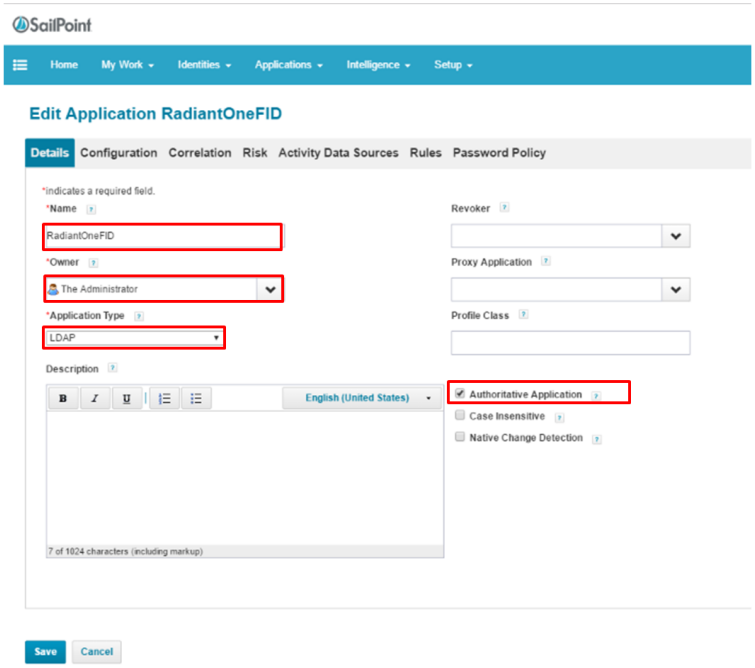

Figure 3. 3 : Application Details

5. On the Configuration Tab, enter the user credentials, host, and port to connect to RadiantOne FID. Enter the page size and authentication search attributes to condition the search to identify users.
6. On the Account tab, select the scope of search to issue to find users, the starting point in the virtual namespace (Search DN), the filter to identify users (Iterate Search Filter), the starting point in the virtual namespace where groups associated with the users are located (Group Member Search DN), the filter to identify groups (Group Member Search Filter).

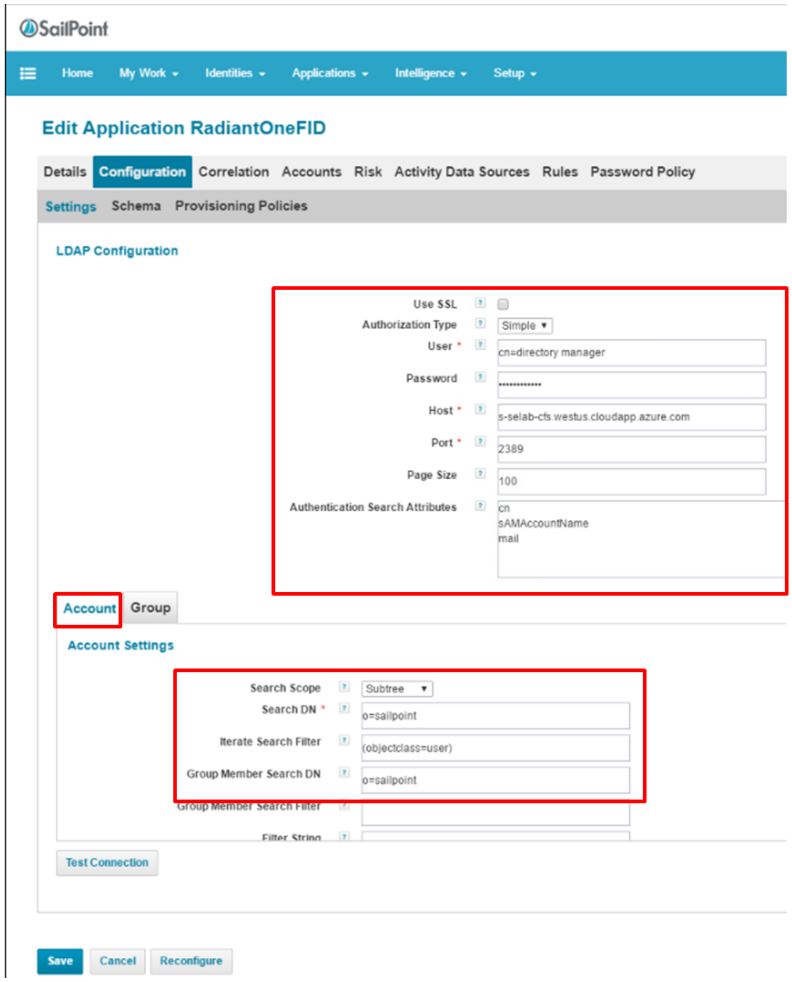

Figure 3. 4 : Application Configuration Settings

7. On the Group tab, select the scope of search to issue to find groups, the starting point in the virtual namespace (Search DN), and the filter to identify groups (Iterate Search Filter).

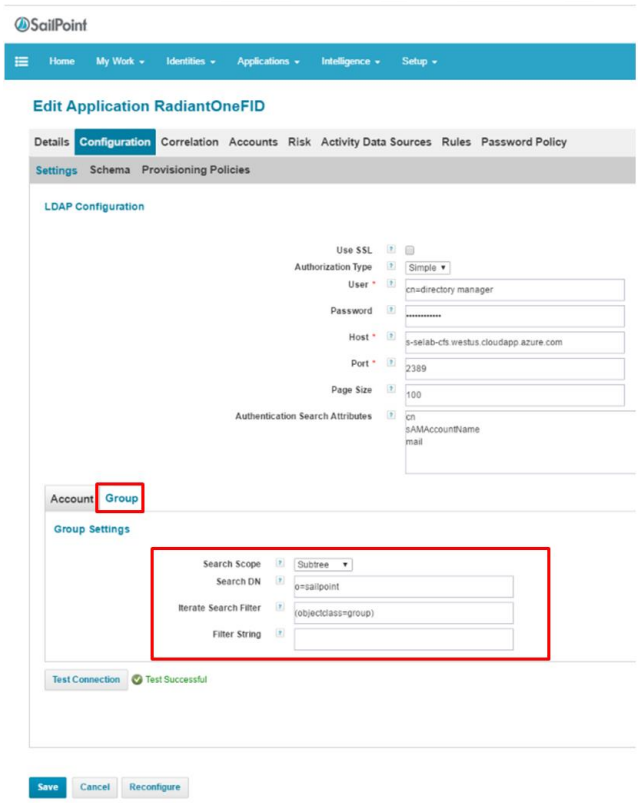

Figure 3. 5 : Application Configuration Settings

8. Click Test Connection to ensure a connection can be made to RadiantOne FID.
9. In the Schema section, information about the attributes associated with the users and groups can be managed. Make sure the Native Object Type listed matches the object class associated with your user and group accounts in RadiantOne FID.

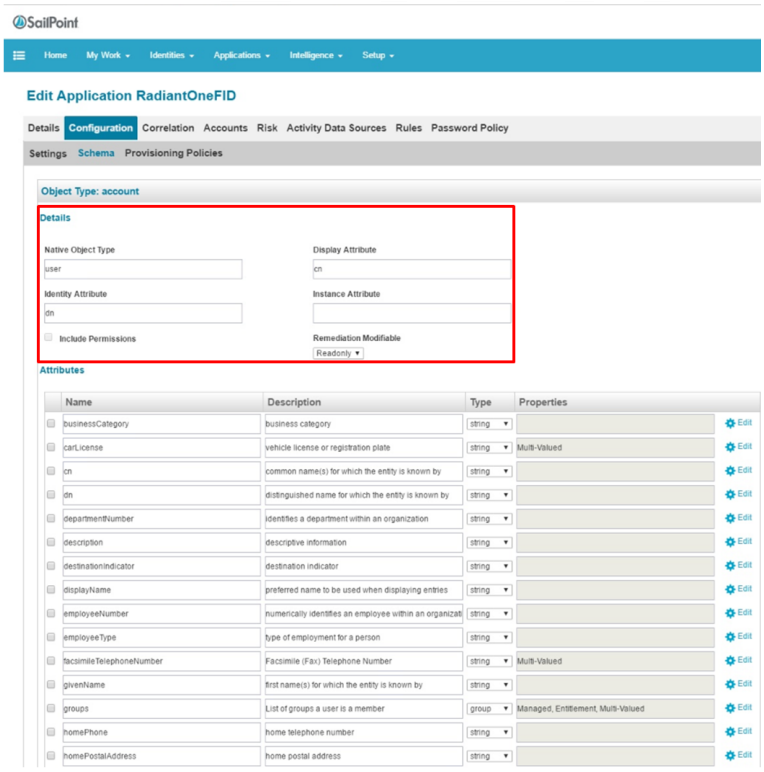

Figure 3. 6 : User Attributes

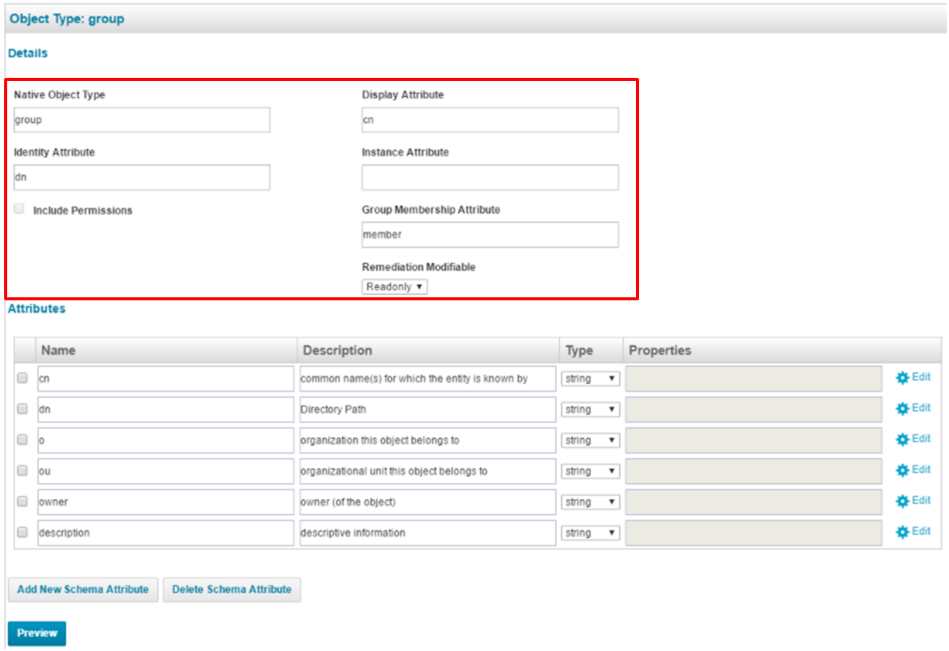

Figure 3. 7 : Group Attributes

10. Save the application.

Configure Attribute Mapping between RadiantOne FID and IdentityIQ Identity Warehouse

In order for identities to be imported from RadiantOne FID into the IdentityIQ Identity Warehouse, attribute mapping between the two systems must be configured.

1. In the SailPoint Admin Console, click on the settings icon (small gear at the right top) and select Global Settings.

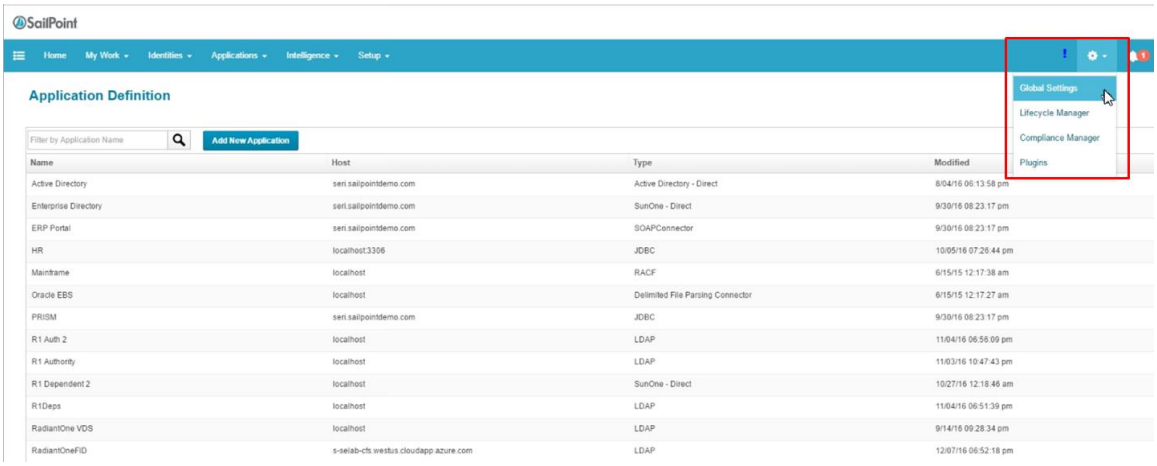

Figure 3. 8 : SailPoint Global Settings

2. Click on Identity Mappings.

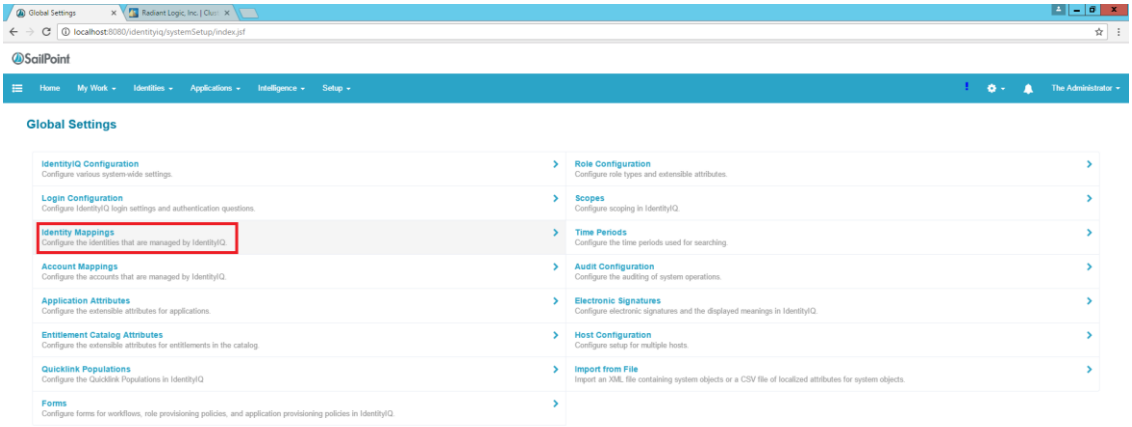

Figure 3. 9 : SailPoint Identity Mappings

3. Click on an IdentityIQ attribute that needs mapped to an attribute in FID. The example below describes a mapping for Display Name.

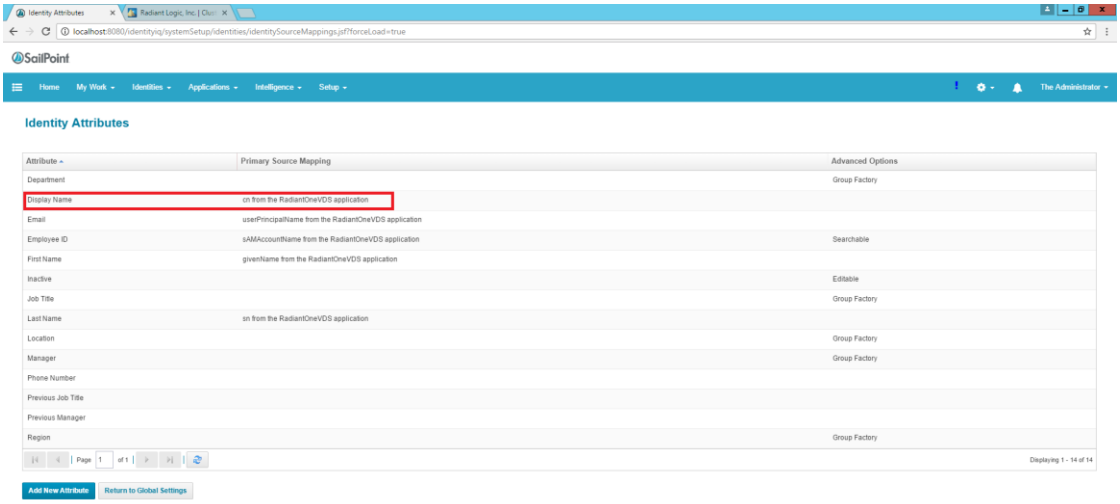

Figure 3. 10 : Attribute Mapping

4. In the Source Mappings section, click Add Source.

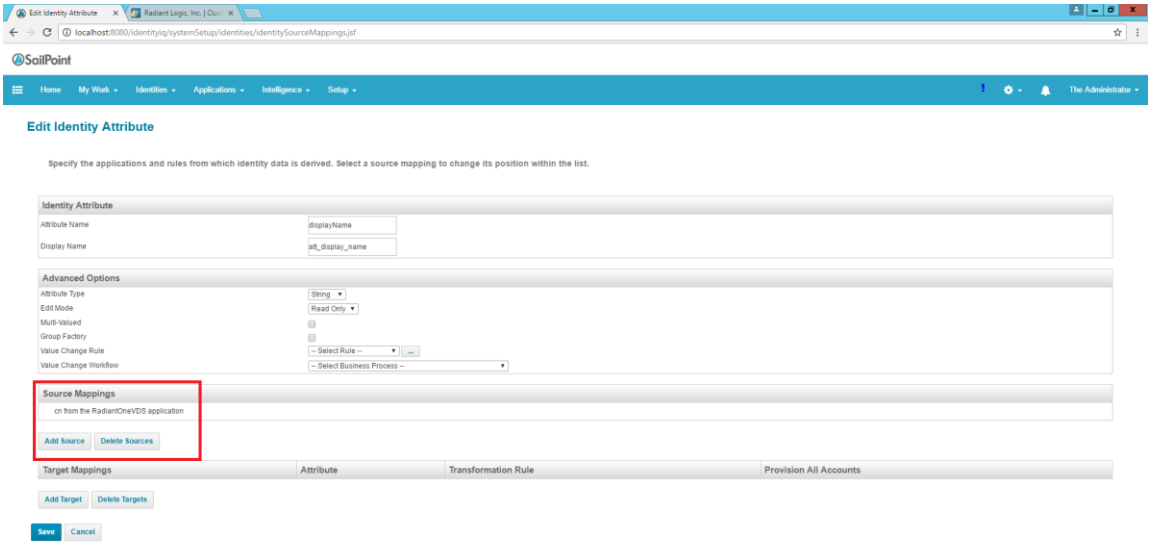

Figure 3. 11 : Identity Attribute Mapping

5. From the Application drop-down list, select the application configured for RadiantOne FID.
6. For the RadiantOne FID application, select the attribute from the drop-down list to map to the Display Name attribute in IdentityIQ.

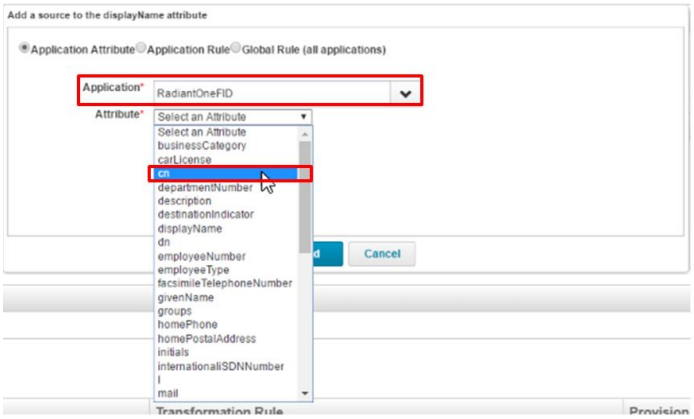

Figure 3. 12 : Attribute Mapping

7. Click Save to return to the Identity Mappings screen.
8. Repeat steps 3-7 for all attributes that you want to import from RadiantOne FID into the IdentityIQ Identity Warehouse.

Configure SailPoint Tasks

Tasks are used to import (aggregate) and refresh users and groups into SailPoint IdentityIQ

Identity Warehouse.

Aggregate Users

1. In the SailPoint Admin Console, click on the Setup menu and select Tasks.

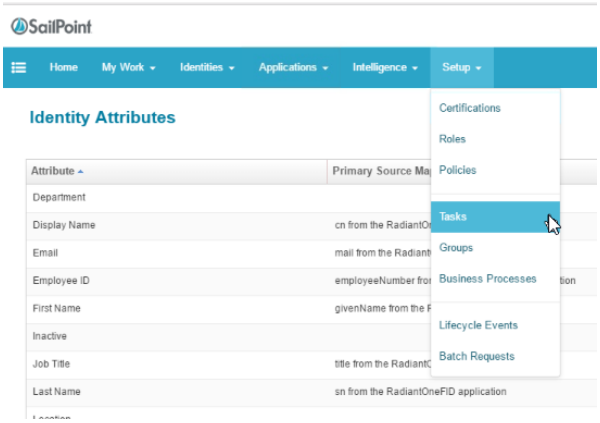

Figure 3. 13 : SailPoint Setup Menu

2. Click in the New Task drop-down menu and select Account Aggregation.

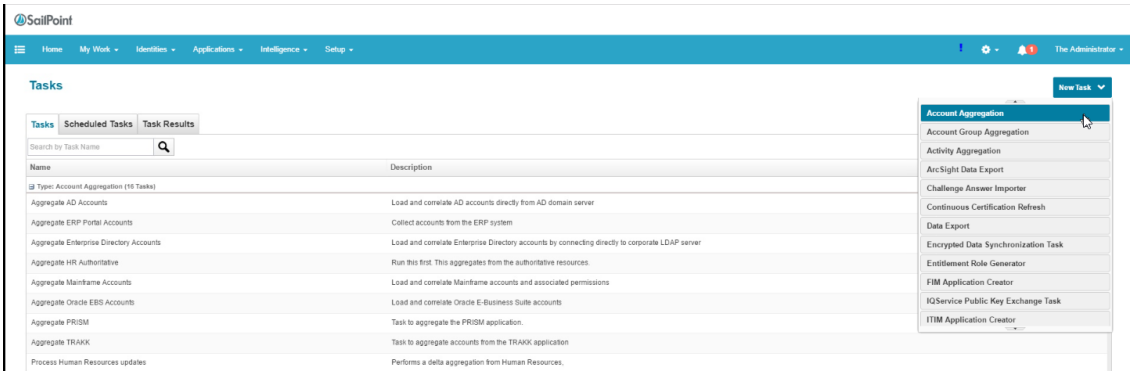

Figure 3. 14 : SailPoint Task Menu

3. Enter a unique name for the task.
4. Select the RadiantOne FID application to scan.

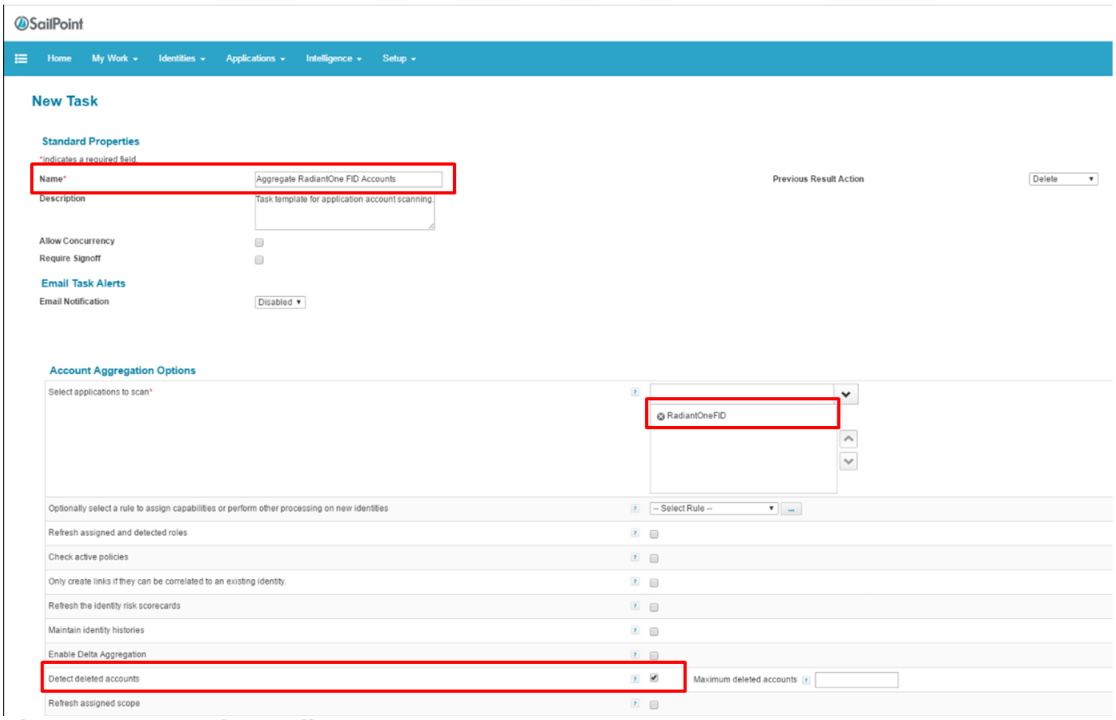

Figure 3. 15 : Task Details

5. Save the Task.

Aggregate Groups

1. In the SailPoint Admin Console, click in the New Task drop-down menu and select Account Group Aggregation.

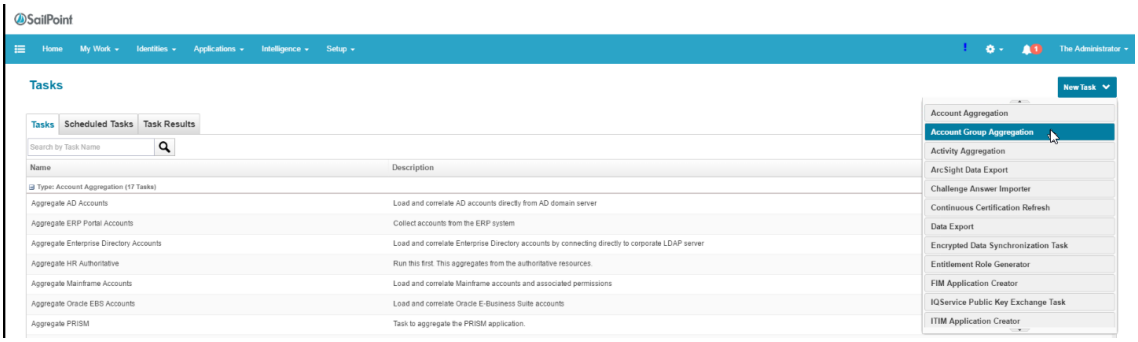

Figure 3. 16 : SailPoint Tasks

2. Enter a unique name for the task.
3. Select the RadiantOne FID application to scan.
4. Check the option to Detect Deleted Account Groups.
5. Choose *en_US* from the drop-down list for Automatically Promote Descriptions to this Locale.
6. Enter *description* as the Description Attribute (this should be the default).

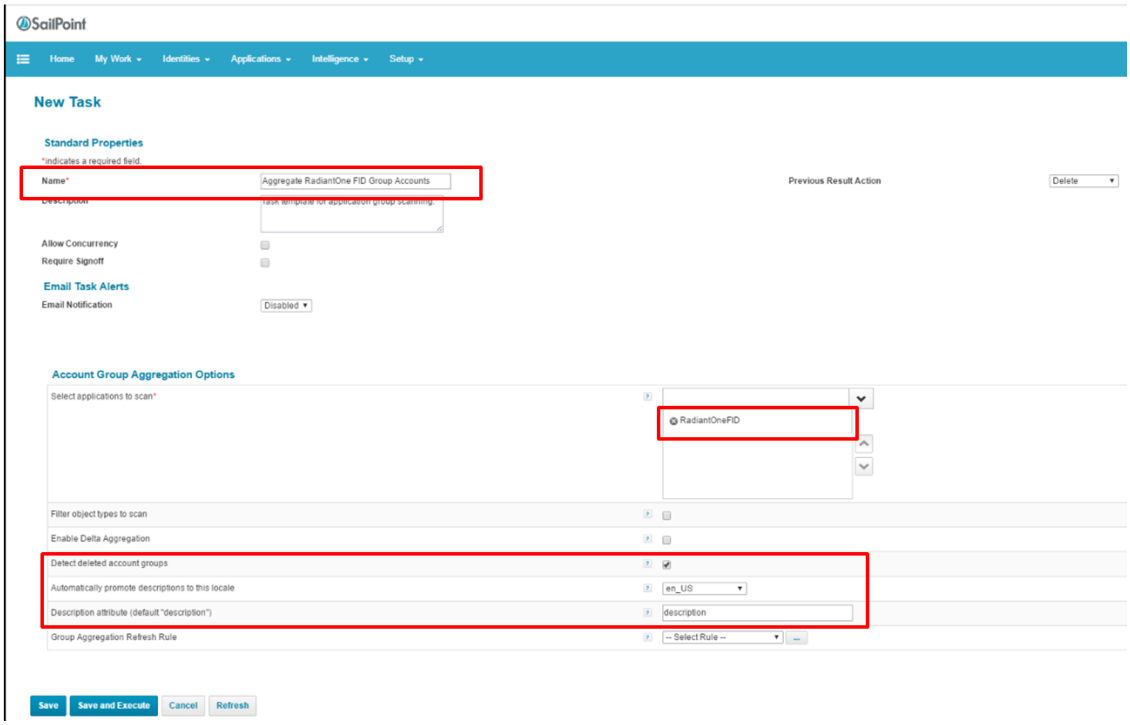

Figure 3. 17 : Task Details

7. Save the Task.

Identity Refresh

1. In the SailPoint Admin Console, click in the New Task drop-down menu and select Identity Refresh.

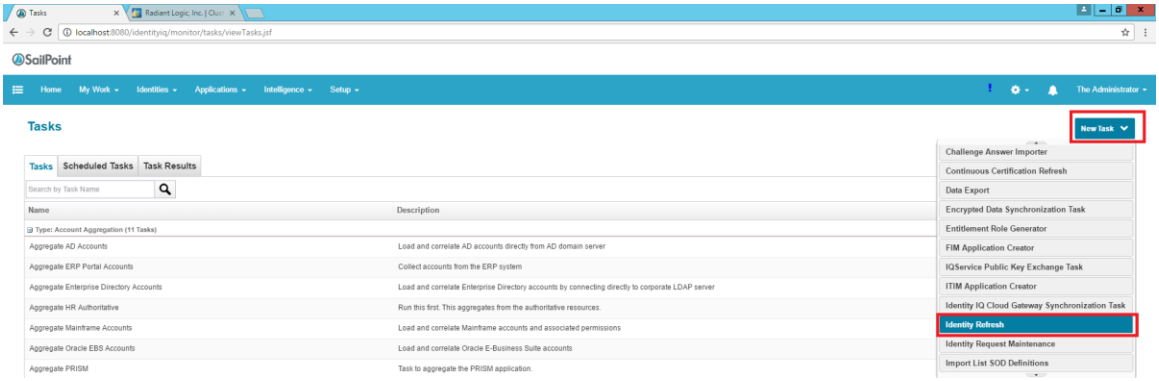

Figure 3. 18 : SailPoint Tasks

2. Enter a unique name for the task.
3. Check the option to Refresh Identity Attributes.
4. Check the option to Refresh Identity Entitlements for all links.

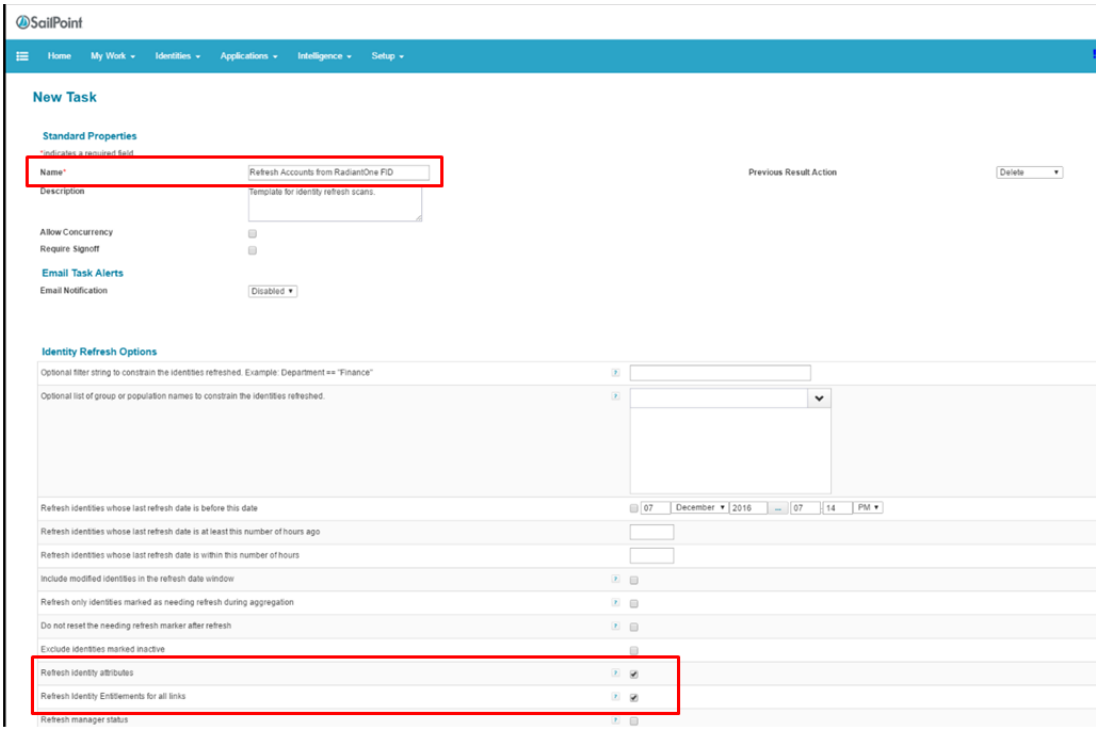

Figure 3. 19 : Task Details

5. Check the option to Promote Managed Attributes.

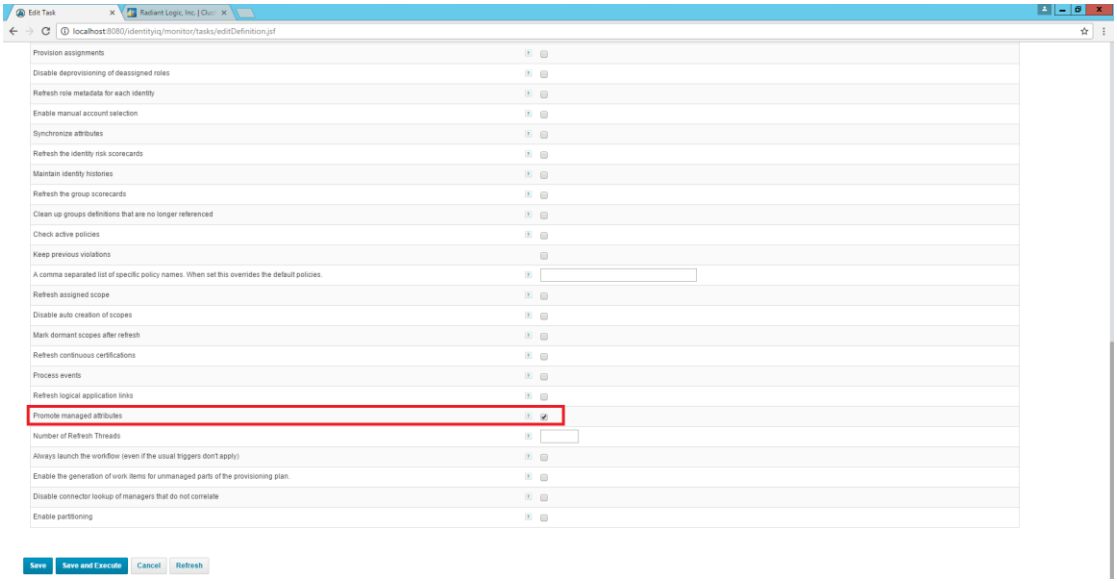

Figure 3. 20 : Task Details

6. Save the Task.

Sequence Task

A Sequence Task is used to run specified tasks in a specific order.

1. In the SailPoint Admin Console, click in the New Task drop-down menu and select Sequential Task Launcher.

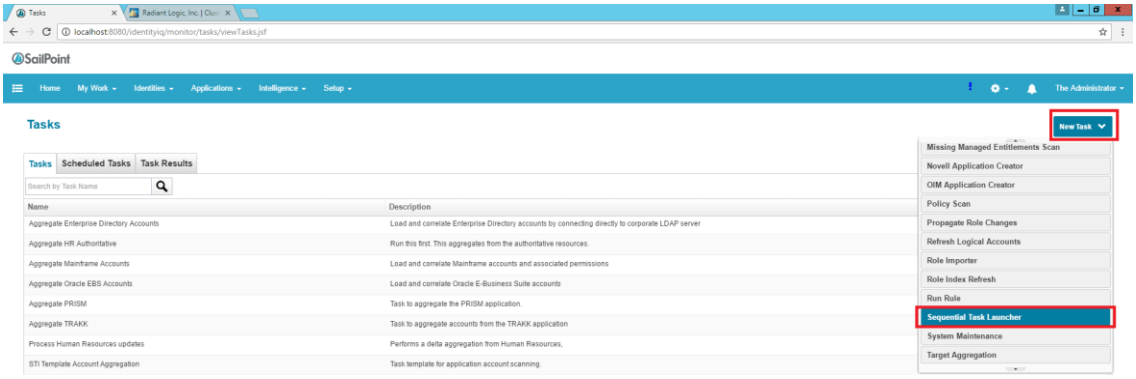

Figure 3. 21 : SailPoint Task Menu

2. Enter a unique task name.
3. Enter the list of tasks to execute in the order you want them run.

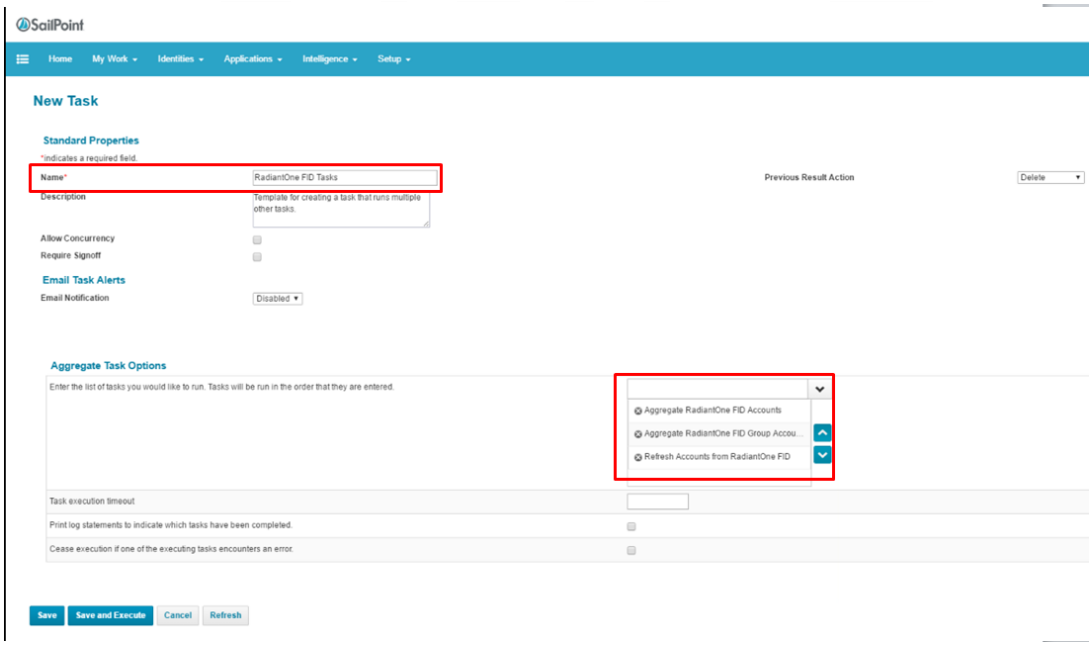

Figure 3. 22 : Task Sequence

4. Save and Execute the task.

Verify Import of RadiantOne FID Entries into the IdentityIQ Identity Warehouse

1. In the SailPoint Admin Console, click on the Identities menu and select Identity Warehouse.

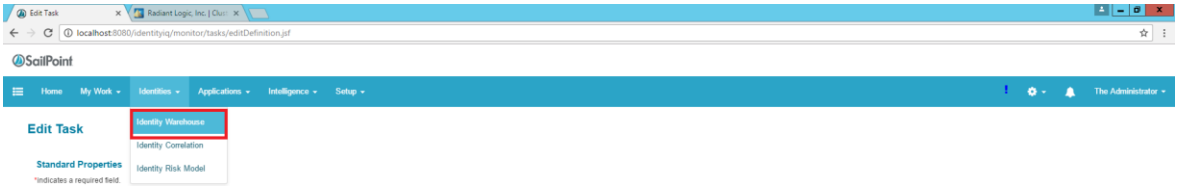

Figure 3. 23 : SailPoint Identities Menu

2. Search for an identity of a user you know was imported from RadiantOne FID.

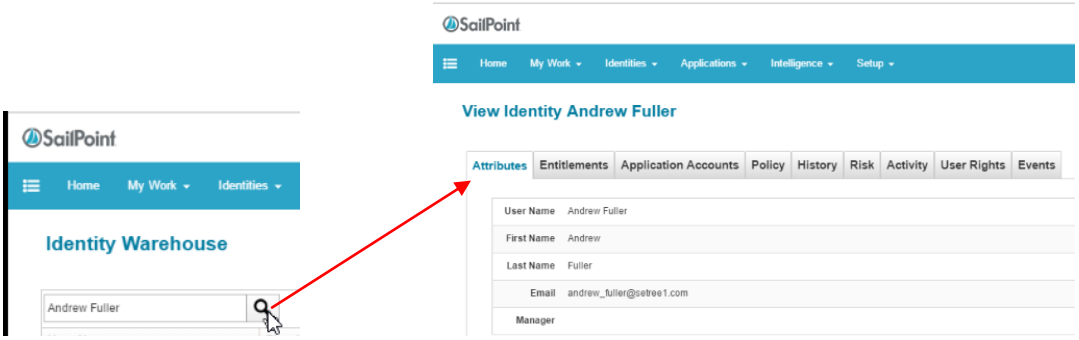

Figure 3. 24 : Sample User Search

3. Click on the identity.

4. Select the Application Accounts tab. It should indicate that that user is associated with the RadiantOne FID application and show the attributes pulled from this application.

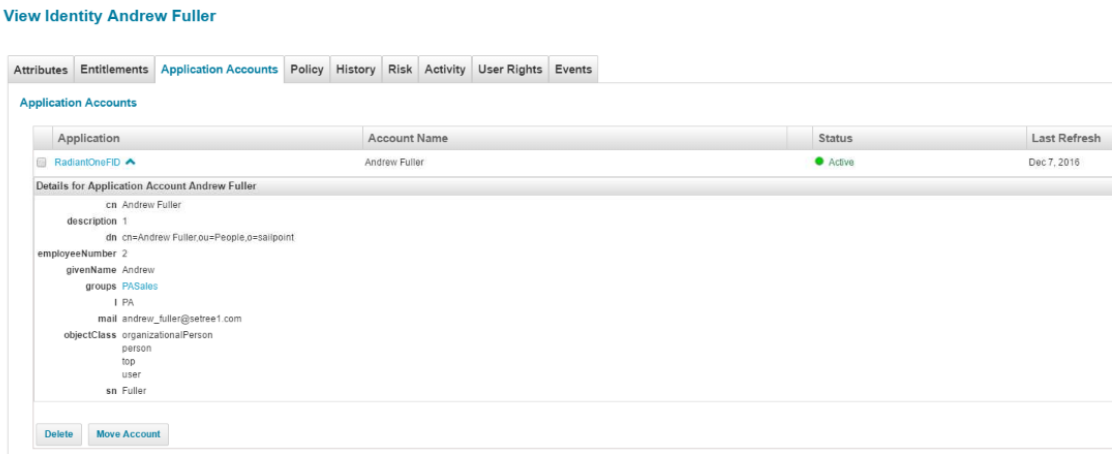

Figure 3. 25 : Sample Account Details

Schedule the Sequence task for Automatic Refresh of Entries in IdentityIQ Identity Warehouse

1. In the SailPoint Admin Console, click on the Setup menu and select Tasks.
2. Right-click on the Sequence Task and select Schedule.

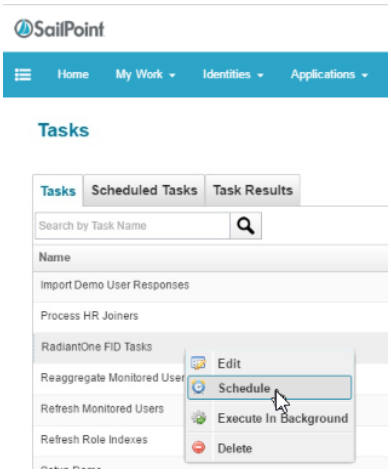

Figure 3. 26 : Scheduling a Task Sequence

3. Enter a unique name, select the first execution date/time and frequency it should be run.
4. Click Schedule.

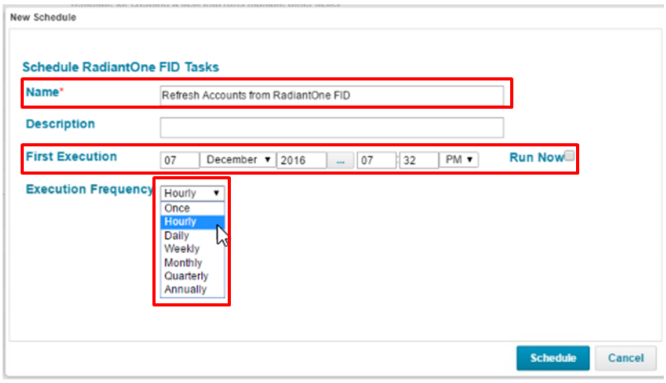

Figure 3. 27 : Schedule Details

5. Click on the Scheduled Tasks menu to verify the task. When the task runs, identities from RadiantOne FID are updated in the IdentityIQ Identity Warehouse.

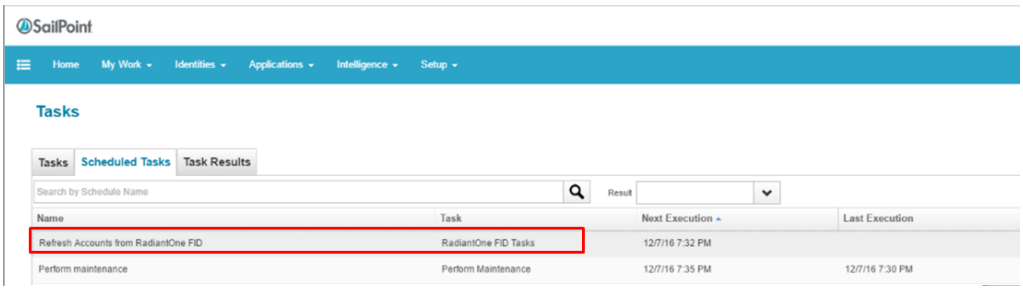

Figure 3. 28 : Menu of Scheduled Tasks

Provisioning to Targets

Now that identities and groups have been imported from RadiantOne FID into the SailPoint IdentityIQ Identity Warehouse, provisioning policies can be configured. Please refer to the SailPoint documentation for details on how to provision accounts from the Identity Warehouse to your desired targets.