



SailPoint Integration with RadiantOne: Deployment Guide

Contents
Chapter 1: Overview
Global Profile – Source Image for Provisioning4
Chapter 2: RadiantOne Configuration6
Defining Virtual View for Identities6
Define Source Objects7
Define Attribute Mapping8
Define Join to Extend Entries
Defining Virtual View for Groups and Membership10
Define Group Names11
Define Group Members12
Define Computation for MemberOf14
Chapter 3: SailPoint Configuration
Configure RadiantOne FID as an Application16
Configure Attribute Mapping between RadiantOne FID and IdentityIQ Identity Warehouse
Configure SailPoint Tasks
Aggregate Users
Aggregate Groups
Identity Refresh27
Sequence Task
Verify Import of RadiantOne FID Entries into the IdentityIQ Identity Warehouse
Schedule the Sequence task for Automatic Refresh of Entries in IdentityIQ Identity Warehouse30



SAILPOINT INTEGRATION GUIDE



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:

SAILPOINT INTEGRATION GUIDE

- 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 O drop-down menu, select Start.
- 4. On the Wizards tab, click on the Virtual Identity Wizard.
- Click ►
- Click new and enter a project name (e.g. spusers) and click x x
- 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*.
- 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".





VDS Virtual Identity		Logged in as cn=directory manager (Logou Exit wizard
Projects Identities Mapping	Authentication > Extension > Attribute Precedence > Deployment >	
Project name: spusers Instance : W-RLI10-LISAPC:2389 (vds_server)	Select Identity Objects Select a schema, and select the objects containing identities. These objects will be used to build a global profile.	0
Identities	Schema: adselab (Ldap) + Selected Identity Objects:	
Select Identity Objects Select Virtual Identity Object Class	user adselab.user	
Identity Overlap	nagy roz, meckigret son	
	φ.	ж
And	Starting point: CN=Users,DC=setree1,DC=com	
Identities	A BACK	NEXT ►

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 **■**EXT ►.

Define Attribute Mapping

- 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 ►
- Click ►
- 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 ►.
- 6. Select an attribute that contains a unique value for all users as the identification attribute.
- 7. Click ► .

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.

 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*.

SAILPOINT INTEGRATION 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.

	Logged i	in as cn=directory manager (Lo Exit wi
Authentication Extension Attribute Precedence	e > Deployment >	
Select Join Objects Select a schema, and select the join objects. These objects will be used to extend your profile.		0
Schema (softwidelaberser (Detaboser) + Sample dbo Employees	Selected Join Objects: sqlirdatabase.Sample.dbo.Employees	×
	Authentication Extension Attribute Precedence Select Join Objects Select a schema, and select the join objects. These objects will be used to send your profile. Schema entertaintense (Database) (Sample.dbo Employees	Authentication Extension Attribute Precedence Deployment Select Join Objects Select a schema, and select the join objects. These objects will be used to extend your profile. Schema celtradatoses (Doubleose) + Sample doo Employees + Selected Join Objects:

Figure 2. 4 : Defining Join Object

- 3. Click NEXT ►.
- 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 NEXT .

Define Join Conditions	
Define the join condition for each join object.	
EDIT	
Join Object	Join Condition
sqlhrdatabase.Sample.dbo.Employees	employeeNumber=EmployeeID

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 I attribute.





Define Join Attribute Mappings					0		Define Join Attribute Mappings					
fap the object attributes to the virtual identity	attribut	es for each join object.			-		Map the object attributes to the virtual ide	ntity attrib	utes for each join object.			
oin Object:							Join Object:		Attribute mappings from 'soll	rdatabase Sample dbo Em	plo()	
sqlhrdatabase.Sample.dbo.Employe	to	ttribute mappings from 'sqir 'user'	irdatabase.Sample.dbo.Er	mpio()			sqlhrdatabase.Sample.dbo.Employe		to 'user'			
Account		Source attribute	map to	Virtual identity attribute			Account		Source attribute	map to	Virtual identity attribute	
Address		source attribute	concorrectation	virtual identity attribute			Address			NUCLEUR NEW		
BirthDate			countryCode				BirthDate			isPrivilegeHolder		
City	-		createTimeStamp				City	-		jpegPhoto		
ClearanceLevel		dBCSPwd		3Pwd			ClearanceLevel		Region	1		
Country	23		dSASignature			3	Country	1		labeledURI		6
Department			dSCorePropagation	Data			Department			lastKnownParent		а.
EmployeeID	=		defaultClassStore				EmployeeID	=		lastLogoff		
Extension			department				Extension			lastLogon		
FirstName			departmentNumber				FirstName			lastLogonTimestamp		
HireDate		ClearanceLevel	description				HireDate			ImPwdHistory		
HomePhone			desktopProfile				HomePhone			localeID		
LastName			destinationIndicator				LastName			lockoutTime		
Notes			directReports				Notes			logonCount		
Photo			displayName				Photo			logonHours		

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

- 6. Click ►
- Choose to mount the virtual view of identities under a naming context (e.g. ou=people,o=sailpoint) and click
- 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.





- 4. On the Wizards tab, click on the Groups Builder Wizard.
- 5. Click **C** on the introduction page.
- 6. Click **■** and enter a project name (e.g. spgroups).
- 7. Click ► T►
- 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.
- 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*.

SAILPOINT INTEGRATION 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 Reverse and enter PAContractors for the group name and click Reverse.
- 12. Click erew group and enter PASales for the group name and click

Define Group Members

- 1. Select the PASales group and click on Define Dynamic Members.
- 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 I of "PA". See this example in the screen shot below.





Projects Configuration Membership Deployment		
Project name: spgroups Instance : W-RLH0-LISAPC:2389 (vds_server)	Define who belongs to the group 'PASales' Base DN:	0
Membership > Define your groups	curracole.orsalpoint C00005 Fite: [(6/c)pectossrpproor)(description*)/inPA/tde=VP Sales)]	×
Deptoyment Deptoyment Destroym	One Level Sub-Tree	PREVIEW
Membership	< BACK	NEXT 🕨

Figure 2.9 : Defining Dynamic Member Criteria

- 5. Click ►
- 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 I (location) of "PA". See this example in the screen shot below.

Projects Configuration Membership Deployment		
Project name: spgroups Instance : W-RL10-LISAPC.2389 (vds_server)	Define who belongs to the group 'PAContractors' Base DN:	0
Membership > Define your groups	CHOOSE CH	
	(8(cbjecolass=person)(tide=SF Contractor)(=PA(description=2))	
Deployment Under Charge there	One Level O Sub-Tree	FRENEW
Membership	4 BACK	NEXT ►

Figure 2. 10 : Defining Dynamic Group Member Criteria

- 10. Click **■**EXT ►.
- 11. Click 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).





Projects Configuration Membership Deployment		
Project name: spgroups Instance : W-RL110-LISAPC.2389 (vds_server)	Mount Point	0
Deployment	Mount under a new Naming Context	
> Mount groups Define a cache	Naming Context . umgroup.orsalipoint	
	O Mount under an existing Naming Context	
	Existing Naming Context: CH005E	
Membershin	Create node:	
VDS Configurations		
Deployment	■ BACK	NEXT 🕨

Figure 2. 11 : Defining Location to Mount Virtual View

- 13. Click ►
- 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 \rightarrow Interception \rightarrow 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.





Add Mapping	
Users Location	
o=sailpoint	Choose
Groups Location	
+ Add	× Delete
o=sailpoint	
isMemberOf Attribute Name	
memberOf	
Static Filter	
((uniquemember=@)(member=@))	

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

Home x I Main Control Panel x	Kone X II Main Control Facel X									
1 x x x x x x x x x x x x x x x x x x x										
§ScilPoint										
🗮 Home My Work - Identities - Applications - Intelligence - Setup -		🔷 + 🌲 The Administrator +								
Home Application Definition		✓ Edit								
Policy Violations > Application Risk Model O Activity Target Categories	Approvals > O Manage User Access >	Track My Requests								
Latest Approvals	Latest Violation Work Items Both 🗸	Latest Forms								
Currently no data	Currently no data	Currently no data								
Al >	AL 2	AL >								
Direct Reports Search lot	My Access Reviews	Certification Campaigns								
Currently no data	Currently no data	App Owner Certification Campage: 122 FY2015 A Owner By 449 Days								
Laurille ask-0000 (intensity in Intelling Complications Complications inf	AL 2	41.5								

Figure 3.1: SailPoint Application Menu

3. Click on Add New Application.

Characterization Definition of Characterization of Characterization				4 - 8 X							
$(\rightarrow \mathbb{C} \)$ C D calculations (in the function of a productions of the function of the func											
C -> C () () (connection) (setting-disense) abbreations by											
@SailPoint											
🗮 Home My Work - Identifies - Applications - Intellig	ance • Setup •		I 0- 4	The Administrator +							
Application Definition											
Filter by Application Name Q Add New Application											
Name	Host	Туре	Modified								
Active Directory	seri.sailpointdemo.com	Active Directory - Direct	8/04/16 06:13:58 pm								
Enterprise Directory	seri.sailpointdemo.com	SunOne - Direct	9/30/16 08:23:17 pm								
ERP Portal	seri.sailpointdemo.com	SOAPConnector	9/30/16 08:23:17 pm								
HR	localhost3306	JDBC	10/05/16 07:28:44 pm								
Mainframe	localhost	RACF	6/15/15 12:17:38 am								
Oracle EBS	localhost	Delimited File Parsing Connector	6/15/15 12:17:27 am								
PRISM	seri.sailpointdemo.com	JDBC	9/30/16 08:23:17 pm								

Figure 3. 2 : Adding a SailPoint Application





SAILPOINT INTEGRATION GUIDE

۵9	GailPoi	nt								
≡	Home	My Work	- Identiti	es - Ap	plications 👻	Intelligence	→ Se	stup -		
E	Edit A	pplicatio	on Radia	ntOneFl	D					
C	Details	Configurat	on Correla	tion Risk	Activity Da	ata Sources	Rules	Password Policy		
	*indicate *Name	s a required fie	eld.					Revoker 🗵		
	Radian	OneFID							*	
	*Owner	2			-			Proxy Application 2		
	The Applic	Administrator		`	~			Profile Class ?	*	
	LDAP	adon type 👔		•						
	Descrip	tion 🕐								
	в	ΙŪ	E E		Englis	h (United State	s) •	Authoritative Application 🤉		
								Case Insensitive		
								Native Change Detection 2		
	7 -6 102	t abarastare Cou	hofee markup)							
	1 01 102	- crimec(C13 (8)	covery markup)							

Figure 3. 3 : Application Details

Save Cancel

- 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).





Ø۵	ailPoin	t					
≡	Home	My Work	• Identities •	Applications +	Intelligence 🗸		Setup -
E	dit Ap	plicatio	n RadiantO	neFID			
D	etails	Configuratio	on Correlation	Accounts Ris	k Activity Data	a So	ources Rules Password Policy
s	Settings	Schema	Provisioning Po	licies			
	LDAP Configuration						
					Use \$\$L	2	0
				A	Ithorization Type	?	Simple V
					o sei		cn=directory manager
					Password	2	
					Host *	?	s-selab-cfs.westus.cloudapp.azure.com
					Port *	?	2389
					Page Size	?	100
				Authentication S	earch Attributes	•	on sAMAccountName mail
	Accou	nt Group					
			Sear	ch Scope 🔹 😒	ubtree 🔻		
			Se	arch DN * 🔹 o=	sailpoint		
			Iterate Sea	rch Filter 🔹 (o	bjectclass=user)		
			Group Member Se	earch DN 🔹 o=	sailpoint		
			Group Member Sea	rcn Filter			
	Test Co	nnection	Fit	ter String 🕴			

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).





09	GailPoir	nt						
=	Home	My Work	 Identities - 	Applications +	Intelligence +	Set	tup •	
1	Edit A	pplicatio	on RadiantOr	eFID				
	Details	Configuration	on Correlation	Accounts Ris	k Activity Data	Sourc	ces Rules Password Policy	
	Settings	Schema	Provisioning Pol	cies				
	LDAP Configuration Use SSL 1 Luse SSL 1							
	Grou	onnection	Searc Se Iterate Sear Fitte Test Successful	h Scope (?) Su nrch DN (?) 0= ch Filter (?) (00 rr String (?)	ibtree • ailipoint jectclass=group)			

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.



ailPo	pint				
Horr	ne My Work - Identities - Aç	plications - Intelligence - Setup -			
dit	Application PadiantOneE	ID			
	Application RadiantOner	U			
etails	Configuration Correlation Acco	ounts Risk Activity Data Sources Rules Pa	assword Policy		
etting	s Schema Provisioning Policies				
Obje	ect Type: account				
Deta	ils			1	
Noti	Chiest Ture	Display Michaela			
user	r	cn			
Iden	tity Attribute	Instance Attribute			
dn					
	Include Permissions	Remediation Modifiable			
Attri	hiites	Readonly *		J	
	Name	Description	Туре	Properties	
	businessCategory	business category	string		•
	carLicense	vehicle license or registration plate	string	Multi-Valued	•
	cn	common name(s) for which the entity is known by	string		•
	dn	distinguished name for which the entity is known	by string •		•
	departmentNumber	Identifies a department within an organization	string		•
	description	descriptive information	string		•
	destinationIndicator	destination indicator	string		•
	displayName	preferred name to be used when displaying entri	es string •		•
	employeeNumber	numerically identifies an employee within an orga	anizat string •		•
	employeeType	type of employment for a person	string		•
	facsimileTelephoneNumber	Facsimile (Fax) Telephone Number	string	Multi-Valued	•
	givenName	first name(s) for which the entity is known by	string		•
	groups	List of groups a user is a member	group	Managed, Entitlement, Multi-Valued	•
	homePhone	home telephone number	string		\$
	homePostalAddress	home postal address	string		- 0

Figure 3. 6 : User Attributes

Obje	ect Type: group			
Deta	lls			
Native Object Type		Display Attribute]
grou	qu	cn		
Iden	tity Attribute	Instance Attribute		
dn				
	Include Permissions	Group Membership Attribute		
		member		
		Remediation Modifiable		
		Readonly v		
Attri	butes			
	Name	Description	Туре	Properties
	Name	Description common name(s) for which the entity is known to	Type Iy String T	Properties
	Name on dn	Description common name(s) for which the entity is known to Directory Path	Type string •	Properties 🎸 Edit
	Name on 0	Description common name(s) for which the entity is known t Directory Path organization this object belongs to	Type wy string • string • string •	Properties
	Name on o ou	Description common name(s) for which the entity is known to Directory Path organization this object belongs to organizational unit this object belongs to	Type istring • string • string • string • string •	Properties
	Name on o ou ou owner	Description common name(s) for which the entity is known to Directory Path organization this object belongs to organizational unit this object belongs to owner (of the object)	Type sting •	Properties
	Name cn dn o ou owner description	Description common name(s) for which the entity is known to pirectory Path organization this object belongs to organizational unit this object belongs to owner (of the object) descriptive information	Type string • string •	Properties
	Name cn dn o o o u o u o u description	Description common name(s) for which the entity is known to Directory Path organization this object belongs to organizational unit this object belongs to owner (of the object) descriptive information	Type y string • (string • (string • (string • (string • (string • (string •	Properties

Preview

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.

٨	@SailPoint					
=	Home My Work • Identities • Applications • Intelligenc	te • Setup •			1 0 -	0
	Application Definition				Global Settings	
	Filter by Application Name Q Add New Application				Compliance Manager	
	Name	Host	Туре	Modified	Plugins	
	Active Directory	seri sailpointdemo.com	Active Directory - Direct	8/04/16 05:13:58 pm		1
	Enterprise Directory	seri.salipointdemo.com	SunOne - Direct	9/30/16 08:23:17 pm		
	ERP Portal	seri sailpointdemo.com	SOAPConnector	9/30/16 08:23:17 pm		
	HR	localhost.3306	JDBC	10/05/16 07:26:44 pr	n	
	Mainframe	localhost	RACF	6/15/15 12:17:38 am		
	Oracle EBS	localhost	Delimited File Parsing Connector	6/15/15 12:17:27 am		
	PRISM	seri sailpointdemo.com	JDBC	9/30/16 08:23:17 pm		
	R1 Auth 2	localhost	LDAP	11/04/16 06:56:09 pr	n	
	R1 Authority	localhost	LDAP	11/03/16 10:47:43 pr	n	
	R1 Dependent 2	localhost	SunOne - Direct	10/27/16 12:18:46 ar	n	
	R1Deps	localhost	LDAP	11/04/16 06:51:39 pr	n)	
	RadiantOne VDS	localhost	LDAP	9/14/16 09:28:34 pm		
	RadiantOneFID	s-selab-cfs westus cloudapp azure com	LDAP	12/07/16 06:52:18 pr	n	

Figure 3.8 : SailPoint Global Settings





2. Click on Identity Mappings.

🕼 Global Settings 🛛 🗴 🕼 Radiant Logic, Inc. Clus: 🗴 🚺	L _ 6 🛛
← → C O localhost:8080/identityig/systemSetup/index.jsf	\$
@SailPoint	
🗮 Home My Work - Identities - Applications - Intelligence - Setup -	l 💿 - 🌲 The Administrator -
Global Settings	
IdentityIQ Configuration Configure various system wide settings.	Role Configuration > Configure role types and extensible attributes.
Login Configuration Configure Identify(Q login settings and authentication questions.	Scopes > Configure scoping in IdentifyIQ.
Identify Mappings Configure the identities that are managed by Identify(Q.	Time Periods Sconfigure the time periods used for searching.
Account Mappings Configure the accounts that are managed by IdentityIQ.	Audit Configuration > Configure the auditing of system operations.
Application Attributes Configure the extension applications.	Electronic Signatures Sconfigure electronic signatures and the displayed meanings in Identity(Q.
Entitlement Catalog Attributes So Configure the extension of the catalog.	Host Configuration > Configure setup for multiple hosts.
Quicklink Populations Configure the Quicklink Populations in Identity(Q	Import from File Import an XML file costalning system objects or a CSV file of localized attributes for system objects.
Forms Configure forms for workflows, role provisioning policies, and application provisioning policies in IdentifyIQ.	

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.

i lénéh Atsibutes x 🕼 Radiant Logic Inc. Dui: X 📜				
\rightarrow C 🔘 localhost:8080/identityiq/sys	stemSetup/identities/identitySourceMappings.jsf?forceLoad=true	*		
0SoilPoint				
Home My Work - Identities -	Applications + Intelligence + Setup +	! 🔷 - 🌲 The Administrat		
Identity Attributes				
Attribute .	Primary Source Mapping	Advanced Options		
Department		Group Factory		
Display Name	cn from the RadiantOneVDS application			
Email	userPrincipalName from the RadiantOneVDS application			
Employee ID	sAMAccountName from the RadiantOneVDS application	Searchable		
First Name	givenName from the RadiantOneVDS application			
Inactive		Editable		
Job Title		Group Factory		
LastName	sn from the RadiantOneVDS application			
Location		Group Factory		
Manager		Group Factory		
Phone Number				
Previous Job Title				
Previous Manager				
Region		Group Factory		

Figure 3. 10 : Attribute Mapping



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

Lidt identity Attribute X Advant Logic, Inc. Clust X						
← → C O localhost:8080/identityiq/systemSetup/identities/identitySo	ourceMappings.jsf			¥ :		
@SailPoint	SailPoint					
📰 Home My Work - Identities - Applications - Intelligen				🕴 🧔 🔹 🌲 The Administrator 📼		
Edit Identity Attribute						
		g to onenge no position minin are not.				
Identity Attribute						
Attribute Name	displayName					
Display Name	att_display_name					
Advanced Options						
Attribute Type	String •					
Edit Mode	Read Only 🔻					
Multi-Valued						
Group Factory						
Value Change Rule	- Select Rule 🔻 💶					
Value Change Workflow	- Select Business Process	¥				
Source Mappings						
on from the Radiant/DeVDS application						
or normale havianticite vois approaction						
Add Source Delete Sources						
Target Mappings	Attribute	Transformation Rule	Provision All Accounts			
Add Target Delete Targets						
formal Connect						

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.

Application*	RadiantOneFID		~	
Attribute*	Select an Attribute Select an Attribute businessCategory carLicense	¥		
	departmentNumber Ly description destinationIndicator displayName dn employeeNumber employeeType facsimiteTelephoneNumber givenName groups homePhone homePostalAddress initials internationaliSDNNumber	d Canc	el	

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.

	SailPoint			
≡	Home My Work - Identities - Applications -	Intelligence +	Setup 🗸	
	Identity Attributes		Certifications	
	Attribute - Prin	mary Source Ma	Policies	
	Department			
	Display Name cn f	rom the RadiantOr	Tasks	
	Email mai	i from the Radiant	Groups	
	Employee ID emp	ployeeNumber from	Business Processes tion	
	First Name give	enName from the F		
	Inactive		Lifecycle Events	
	Job Title title	from the RadiantC	Batch Requests	
	Last Name sn f	rom the RadiantOn	eFID application	

Figure 3. 13 : SailPoint Setup Menu

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

@SailPoint		
Home My Work + Identities + Applications + Intelligence + Sets	p *	🚺 💠 🛛 🚺 The Administrator •
Tasks		New Task 🗸
Tasks Scheduled Tasks Task Results		Account Aggregation
Search by Task Name		Activity Aggregation
Name	Description	ArcSight Data Export
Type: Account Aggregation (16 Tasks)		Challenge Answer Importer
Aggregate AD Accounts	Load and correlate AD accounts directly from AD domain server	Continuous Certification Refresh
Aggregate ERP Portal Accounts	Collect accounts from the ERP system	Data Export
Aggregate Enterprise Directory Accounts	Load and correlate Enterprise Directory accounts by connecting directly to corporate LDAP server	Encrypted Data Synchronization Task
Aggregate HR Authoritative	Run this first. This aggregates from the authoritative resources.	Entitlement Role Generator
Aggregate Mainframe Accounts	Load and correlate Mainframe accounts and associated permissions	FIM Application Creator
Aggregate Oracle EBS Accounts	Load and correlate Oracle E-Business Suite accounts	IQService Public Key Exchange Task
Aggregate PRISM	Task to aggregate the PRISM application.	ITIM Application Creator
Aggregate TRAKK	Task to aggregate accounts from the TRAKK application	
Process Human Resources undates	Performs a delta appreciation from Human Resources	

Figure 3. 14 : SailPoint Task Menu

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





SailPoint		
Home My Work - Identitie	s • Applications • Intelligence • Setup •	
New Task		
Standard Properties *indicates a required field.		
Name*	Aggregate RadiantOne FID Accounts	Previous Result Action Delete
Description	Task template for application account scanning.	
Allow Concurrency	8	
Require Signoff		
Email Task Alerts		
Email Notification	Disabled *	
Account Aggregation Option Select applications to scan*	•	RadiantOneFD
Optionally select a rule to assign capa	bilities or perform other processing on new identities	P Select Rule *
Refresh assigned and detected roles		2
Check active policies		
Only create links if they can be correla	ted to an existing identity.	
Refresh the identity risk scorecards		
Maintain identity histories		
Enable Delta Aggregation		
Detect deleted accounts		Maximum deleted accounts
Refresh assigned scope		

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.

ØSailPoin	f						
📰 Home	My Work 👻	Identities +	Applications +	Intelligence +	Setup 👻		🔹 🔹 🍂 The Administrator 🗸
Tasks							New Task 🗸
Tasks 5	cheduled Task	Task Resu	ilts				Account Aggregation
Search by 1	ask Name	٩					Account Group Aggregation
Name						Description	ArcSight Data Export
Type: Acc	ount Aggregation (17 Tasks)					Challenge Answer Importer
Aggregate	AD Accounts					Load and correlate AD accounts directly from AD domain server	Continuous Certification Refresh
Aggregate	ERP Portal Account	its				Collect accounts from the ERP system	Data Export
Aggregate	Enterprise Director	y Accounts				Load and correlate Enterprise Directory accounts by connecting directly to corporate LDAP server	Encrypted Data Synchronization Task
Aggregate	HR Authoritative					Run this first. This aggregates from the authoritative resources.	Entitlement Role Generator
Aggregate	Mainframe Account	ts				Load and correlate Mainframe accounts and associated permissions	FIM Application Creator
Appregate	Dracle EBS Accourt	nts				Load and correlate Oracle E-Business Suite accounts	IQService Public Key Exchange Task
Aggregate	PRISM					Task to aggregate the PRISM application.	ITIM Application Creator

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).

ailPoint			
Home My Work - Identities	Applications Intelligence Setup		
lew Task			
Standard Properties			
Name*	Aggregate RadiantOne FID Group Accounts	Previous Result Action	Delete
Description	task lemplate for application group scanning.		
Allow Concurrency			
Require Signoff			
Email Task Alerts			
Email Notification	Disabled •		
Email Notification Account Group Aggregation O Select applications to scan*	Disable •		
Email Notification Account Group Aggregation O Select applications to scan*	Disable •	RadianDreFID	
Email Notification Account Group Aggregation O Select applications to scan*	Disable •	RadiantOneFID	
Email Notification Account Group Aggregation O Select applications to scen*	Disables •	RadianDreFID	
Email Notification Account Group Aggregation O Select applications to scan* Fifter object hypes to scan	Disable •	RadiantOneFD	
Account Group Aggregation O Select applications to scan* Fifter object types to scan Enable Delta Aggregation	Disable •	RadiantOneFD	
Account Group Aggregation O Select applications to scan* Fifter object types to scan Enable Delta Aggregation Defect derieked account groups	ptions	Redambre/FD	
Account Group Aggregation O Select applications to scan* Fifter object types to scan Enable Delta Aggregation Detect deleted account groups Automatically promote descriptions to to	ptions	PadambeeFD	
Email Notification Account Group Aggregation O Select applications to scan* Filler object types to scan Enable Delta Aggregation Description attitude (default "description Description attitude (default "description	ptions ts locate T	Image: Constrained on the second on the s	

- Save Save and Execute Cancel Refresh 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.

⊕ Tests x Testsert Logic (hc; Curi x) ←		4 ■ 0 ×
🗮 Home My Work - Identities - Applications - Intelligence - Setup -		🔷 🔹 🌲 The Administrator 📼
Tasks		New Task 🗸
		Challenge Answer Importer
Tasks Scheduled Tasks Task Results		Continuous Certification Refresh
Search by Task Name		Data Export
Name	Description	Encrypted Data Synchronization Task
Type: Account Aggregation (11 Tasks)		Entitlement Role Generator
Aggregate AD Accounts	Load and correlate AD accounts directly from AD domain server	FIM Application Creator
Aggregate ERP Portal Accounts	Collect accounts from the ERP system	IQService Public Key Exchange Task
Aggregate Enterprise Directory Accounts	Load and correlate Enterprise Directory accounts by connecting directly to corporate LDAP server	ITIM Application Creator
Aggregate HR Authoritative	Run this first. This aggregates from the authoritative resources.	Identity IQ Cloud Gateway Synchronization Task
Aggregate Mainframe Accounts	Load and correlate Maintrame accounts and associated permissions	Identity Refresh
Aggregate Oracle EBS Accounts	Load and correlate Oracle E-Business Suite accounts	Identity Request Maintenance
Aggregate PRISM	Task to aggregate the PRISM application.	Import List SOD Definitions

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.

@SailPoint		
🗮 Home My Work + Identities +	Applications - Intelligence - Setup -	
New Task		
Standard Properties		
Name*	Refresh Accounts from RadiantOne FID	Previous Result Action
Description	Template for identity refresh scans.	
Allow Concurrency		
Require Signoff		
Email Task Alerts		
Citra Romonout	Disabled •	
Identity Refresh Options		
Optional filter string to constrain the identities re	freshed. Example: Department == "Finance"	×
Optional list of group or population names to co	nstrain the identities refreshed.	
Refresh identities whose last refresh date is be	lore this date	07 December • 2016 - 07 14 PM •
Refresh identities whose last refresh date is at	east this number of hours ago	
Refresh identities whose last refresh date is wit	hin this number of hours	
Include modified identifies in the refresh date w	indow	
Refresh only identities marked as needing refre	sh during aggregation	×
Do not reset the needing refresh marker after re	fresh	2 D
Exclude identities marked inactive		
Refresh identity attributes		 8
Refresh Identity Entitlements for all links		2 B
Refresh manager status		

Figure 3. 19 : Task Details

5. Check the option to Promote Managed Attributes.





Edit Task × 🖪 Radiant Logic, Inc. Clust × 🔲		A _ 6
C 🕼 localhost:8080/identityiq/monitor/tasks/editDefinition.jsf		
Provision assignments	8.0	
Disable deprovisioning of deassigned roles	E D	
Refresh role metadata for each identity	E	
Enable manual account selection		
Synchronize affributes	8.0	
Refresh the identity risk scorecards	E D	
Maintain identity histories	E	
Refresh the group scorecards	E	
Clean up groups definitions that are no longer referenced	E 🙃	
Check active policies		
Keep previous violations	0	
A comma separated list of specific policy names. When set this overrides the default policies.		
Refresh assigned scope	E ()	
Disable auto creation of scopes	× 0	
Mark dormant scopes after refresh		
Refresh continuous certifications	×	
Process events	×	
Refresh logical application links	×	
Promote managed attributes		
Number of Refresh Threads		
Always launch the workflow (even if the usual triggers don't apply)	8 g	
Enable the generation of work items for unmanaged parts of the provisioning plan.	8 g	
Disable connector lookup of managers that do not correlate	8 D	
Enable partitioning		

cute Cancel Refresh Figure 3. 20 : Task Details

6. Save the Task.

Save Save a

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.

/@	Tasks X 🖾 Radiant Logic, Inc. Clust X		± _ 5 ×
\leftarrow	C O localhost8080/identityiq/monitor/tasks/viewTasks.jsf		x :
۵	SailPoint		
=	Home My Work - Identifies - Applications - Intelligence - Setup -		🔹 🔹 🌲 The Administrator 🗝
	Tasks		New Task 🗸
			Missing Managed Entitlements Scan
	Tasks Scheduled Tasks Task Results		Novell Application Creator
	Search by Task Name Q		OIM Application Creator
	Name D	Description	Policy Scan
	Aggregate Enterprise Directory Accounts	Load and correlate Enterprise Directory accounts by connecting directly to corporate LDAP server	Propagate Role Changes
	Aggregate HR Authoritative R	Run this first. This aggregates from the authoritative resources.	Refresh Logical Accounts
	Aggregate Maintrame Accounts L	Load and correlate Mainframe accounts and associated permissions	Role Importer
	Aggregate Oracle EBS Accounts L	Load and correlate Oracle E-Business Suite accounts	Role Index Refresh
	Aggregate PRISM Ti	Task to aggregate the PRISM application.	Run Rule
	Anmanate TRAKK	Task in annianata arrounts from the TRAKK anniiration	Sequential Task Launcher
	Process Limna Decauras undatas	Dorforme a della assessation from Liuman Desaurose	System Maintenance
		remente e vene egyregenen nom menen rosovulvee,	Target Aggregation
	STI Template Account Aggregation	task temptate for application account scanning.	

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.





Standard Properties			
"indicates a required seid. Name*	RadiantOne FID Tasks	Previous Result Action	Delete
Description	Template for creating a task that runs multiple other tasks.		
Allow Concurrency			
Require Signoff			
Email Task Alerts			
Email Notification	Disabled *		
Enter the list of tasks you would like to run.	Tasks will be run in the order that they are entered.	Aggregate RadiantOne FID Accounts Aggregate RadiantOne FID Group Accou. Aggregate RadiantOne FID Refersh Accounts from RadiantOne FID	
Task execution timeout			
Task execution timeout Print log statements to indicate which tasks	s have been completed.		

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.

(a) Edit Task x	🕼 Radiant Logic, Inc. J Cluri 🗴 🔽	± = 8 ×
$\epsilon \rightarrow c$ 🛈 localhost 8080	30/identityiq/monitor/tasks/editDefinition.jsf	☆ :
	Identifies + Applications + Intelligence + Setup +	🔷 🔹 🌲 The Administrator 👻
Edit Task	Identity Warehouse	
	Identity Correlation	
Standard Properties	Identity Risk Model	

Figure 3. 23 : SailPoint Identities Menu

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

	@SailPoint
	🗮 Home My Work - Identities - Applications - Intelligence - Setup -
	View Identity Andrew Fuller
②SailPoint	
☷ Home My Work - Identities -	Attributes Entitlements Application Accounts Policy History Risk Activity User Rights Events
Identity Warehouse	User Name Andrew Fuller First Name Andrew
identity warehouse	Last Name Fuller
Andrew Fuller	Email andrew_fuller@settee1.com
Figure 3, 24 : Sample User Sear	Manager

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.

	Entitlements	Application Accounts	Policy Hist	ory Risk	Activity	User Rights	Events		
olicatio	on Accounts								
Ap	plication			Account	Name			Status	Last R
Radi	iantOneFID 🔺			Andrew Full	er			Active	Dec 7, 20
Details f	for Application A	ccount Andrew Fuller							
	cn Andrew	Fuller							
d	escription 1								
	dn cn=And	rew Fuller,ou=People,o=sailpo	int.						
employe	eeNumber 2								
gi	ivenName Andrew								
	groups PASales	8							
	I PA								
	mail andrew	_fuller@setree1.com							
ob	ojectClass organiz	ationalPerson							
	person								
	top								

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.

	SailPo	pint			
≡	Hom	e My Work -	k	dentities 👻	Applications -
	Task	s			
	Tasks	Scheduled Task	s	Task Resul	ts
	Search b	y Task Name		Q,	
	Name				
	Import D	emo User Response:			
	Process	HR Joiners			
	Radiant	One FID Tasks	_		
	Reaggre	egate Monitored User		Edit Schodulo	
	Refresh	Monitored Users	-	Execute In	Background
	Refresh	Role Indexes	0	Delete	Duonground

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.





Name*	Refresh Accounts from RadiantOne FID	1
Description		
First Execution	07 December V 2016 07 32 PM V	Run Now
Execution Frequen	Hourly Once Hourly Daily Weekly Monthly Cuarterly Annually	

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.

SailPoint		
Home My Work - Identities - Applications - Intelligence -	Setup +	
Tasks		
Taska Cabadulad Taska Task Dasults		
Search by Schedule Name	Q Resul	
Name	Task Next Execution A Last Execution	
Name Refresh Accounts from RadiantOne FID	Task Next Execution A Last Execution RadiantOne FID Tasks 127/116 7-32 FM	

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.