



RSA Ready Implementation Guide for Administrative Interoperability

Last Modified: May 13, 2015

Partner Information


Product Information	
Partner Name	SailPoint
Web Site	www.sailpoint.com
Product Name	IdentityIQ
Version & Platform	6.4
Product Description	IdentityIQ, the industry's most innovative and complete on-premises IAM system, offers compliance, provisioning and access management in a unified solution, leveraging a common governance platform. IdentityIQ allows organizations to tailor complex IAM solutions to align with their unique business processes, while enabling end-users to participate in a wide variety of these processes.




Solution Summary

IdentityIQ is SailPoint's identity and access management (IAM) solution for enterprise customers who prefer an on-premise deployment. IdentityIQ resource connectors provide pre-packaged integrations with enterprise databases, directories, platforms and business applications running in their on-premise datacenters or in the cloud. The connectors allow businesses to provision and aggregate external user, account, entitlement and authentication credentials from a centralized location.

The SailPoint IdentityIQ RSA Authentication Manager resource connector enables RSA SecurID customers to manage RSA Authentication Manager users and groups, administrative roles and SecurID tokens from the IdentityIQ console.

 **Note:** RSA Authentication Manager groups are represented as IdentityIQ account-groups, administrative roles are represented as IdentityIQ entitlements and RSA SecurID tokens are represented by IdentityIQ permissions.

SailPoint IdentityIQ Integration Features	
Add, modify and delete RSA Authentication Manager users	Yes
Add, modify and delete RSA Authentication Manager groups	Yes
Assign/unassign RSA SecurID tokens	Yes ¹
Enable/disable RSA SecurID tokens	Yes
Clear RSA SecurID token PINs	No
Reset RSA SecurID token PINs	Yes
Enable Risk-Based Authentication (RBA).	No
Change user's authentication method (PASSCODE, Fixed-Tokencode, On-Demand Token or RBA)	No
Perform initial import of RSA Authentication Manager resources	Yes
Reconcile RSA Authentication Manager identity source with the IAM data store.	Yes
Reconcile RSA SecurID tokens with the IAM data store.	Yes


 **Important:** This guide contains instructions in that are necessary to deploy the RSA Authentication Manager connector. There are many configuration options that are out of the document's scope. See the SailPoint IdentityIQ administration documentation and the *SailPoint IdentityIQ RSA Authentication Manager Connector* guide for a complete list of the connector's features and comprehensive instructions for configuring them.

¹ The integration doesn't support token assignment for existing users. You can only assign a token when you create a new user.

Configuration

Before You Begin


This section provides instructions for enabling SailPoint IdentityIQ to provision RSA Authentication Manager resources. You should have working knowledge IdentityIQ, RSA Authentication Manager and RSA SecurID, as well as access to the appropriate end-user and administrative documentation. Ensure that both products are running properly prior to configuring the integration.

 **Note:** This document is not intended to suggest optimal installations or configurations.

Configure RSA Authentication Manager

Prerequisites

You must complete the following prerequisites on your IdentityIQ host to configure RSA Authentication Manager API security settings. Consult your *RSA Authentication Manager Developer's Guide* for version-specific instructions.

 **Important:** Consult the *Getting Started* and *Advanced Usage* sections in the *RSA Authentication Manager 8.1 Developer's Guide* for instructions to perform the configuration procedures listed below.

1. Set the required Java system properties.
2. Set the required system environment settings.
3. Export the root certificate from the RSA Authentication Manager server.
4. Import the server root certificate (Java) the local cacerts keystore.

Set the Command Client User Name and Password

When you install RSA Authentication Manager, the system creates a user name and password for securing API connections to a command server. Follow the procedure below to obtain the command client user name and password from RSA Authentication Manager:

1. Open a command prompt on your RSA Authentication Manager host, change directories to `RSA_AM_HOME/utls` and enter the following command:

```
rsautil manage-secrets --action list
```

2. When prompted, type your Operations Console username and password. (You created the Operations Console username and password when you configured RSA Authentication Manager.) The system will display the list of your internal system passwords.
3. Locate the values for your command client user name and password. For example:

```
Command Client User Name .....: cmdClient_ys0x7d41  
Command Client User Password .....: e9SHbk0w4i
```

[You will need these values](#) when you configure IdentityIQ.

 **Important:** Do not change the command client user name or password.

Create an RSA Authentication Manager Account for Connector Operations

The connector requires an RSA Authentication Manager administrative user account with special permissions in order to perform provisioning operations. Follow the steps below to create an administrative role and assign it to an RSA Authentication Manager administrative user:

1. Log in to the RSA Security Console, select **Administration**→**Administrative Roles**→**Add New** and enter a name for the role in the **Administrative Role Name** field.
2. Select the **Permission Delegation** checkbox and optionally enter a description for the role in the **Notes** field.
3. Select the appropriate security domain(s) and identity source from the **Administrative Scope** section and click the **Next** button.

Administrative Role Basics

Administrative Role Name: *

Permission Delegation: This role's permissions may be delegated to other administrators

Notes:

Administrative Scope

Security Domain Scope: * All: [Expand All](#) | [Collapse All](#) | [Check All](#) | [Uncheck All](#)

- SystemDomain
 - emc
 - pinal
 - rsa
 - waranowski

Identity Source Scope: Internal Database

4. Select the **View** checkbox for each policy in **Manage Policies** section.
5. Select the **May configure trusted realms** checkbox in the **Manage Trusted Realms** section.

Manage Policies	
? Password Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Lockout Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Risk-Based Authentication Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Self-Service Troubleshooting Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? SecurID Token Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Offline Authentication Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Workflow Policies:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Risk-Based Authentication (RBA) Message Policy:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Manage Security Questions	
? Security Question Configuration:	<input type="checkbox"/> May configure security questions enrollment and authentication options
? View Security Questions List:	<input type="checkbox"/> May view security questions list
Manage Trusted Realms	
? Trusted Realms:	<input checked="" type="checkbox"/> May configure trusted realms

6. Select the **All** checkbox in the **Manage Security Domains** section.
7. Select the **View** checkbox in the **Manage Delegated Administration** section.

Manage Security Domains	
? Security Domains:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Manage Delegated Administration	
? Administrative Roles:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Assign Administrative Roles:	<input type="checkbox"/> May assign administrative roles to users

8. Select the **All** checkbox in the **Users** row and the **Identity Attribute Definitions** row in the **Manage Users** section.

Manage Users	
? Users:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Reset Passwords:	<input checked="" type="checkbox"/> May reset passwords
? Enable/Disable/Unlock Accounts:	<input checked="" type="checkbox"/> May enable, disable, and unlock accounts
? Enable Users for RBA:	<input type="checkbox"/> May enable and disable users for RBA
? Delete Risk-Based Authentication (RBA) Device History:	<input type="checkbox"/> May delete the device history of users enabled for RBA
? Terminate Active Sessions:	<input checked="" type="checkbox"/> May terminate active user sessions
? Identity Attribute Definitions:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? User Attribute Restriction:	<input type="checkbox"/> May manage attribute categories <input type="checkbox"/> May only access specific attributes:
? User Scope Restriction:	<input type="checkbox"/> May only manage users that match a condition:
? Security Domain Mappings:	<input type="checkbox"/> May map external identity sources to security domains
? Console Display:	<input type="checkbox"/> May configure console display options

9. Select the **All** checkbox for the **User Groups** row in the **Manage User Groups** section.
10. Select the **May assign user group membership** checkbox in the **Manage User Groups** section.
11. Select the **View** checkbox for the **Reports** row in the **Manage Reports** section.
12. Click the **Next** button.

Manage User Groups	
? User Groups:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Assign User Group Membership:	<input checked="" type="checkbox"/> May assign user group membership

Manage Reports	
? Reports:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Run Reports:	<input type="checkbox"/> May run and schedule report jobs
? Report Job Manager:	<input type="checkbox"/> May manage all administrators' private report jobs.
? Audit Report Manager:	<input type="checkbox"/> May run and manage any of the activity reports

13. Go to the **Manage RSA SecurID Tokens** section and:

- Select the **All** checkbox for the **SecurID tokens** row.
- Select the **May assign tokens to users** checkbox.
- Select the **May distribute assigned software tokens to users** checkbox.
- Select the **May import and manage smart card details including PIN unlocking key** checkbox.

Manage RSA SecurID Tokens	
SecurID Tokens:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Reset PINs:	<input checked="" type="checkbox"/> May clear and require users to change SecurID PINs
Enable/Disable Tokens:	<input checked="" type="checkbox"/> May enable and disable SecurID tokens
Manage Offline Token Emergency Access:	<input checked="" type="checkbox"/> May manage offline token emergency access
Manage Online Token Emergency Access:	<input checked="" type="checkbox"/> May manage online token emergency access
Resynchronize Tokens:	<input checked="" type="checkbox"/> May resynchronize SecurID Tokens
Replace Tokens:	<input type="checkbox"/> May replace assigned tokens
Assign Tokens:	<input checked="" type="checkbox"/> May assign tokens to users
Distribute Software Tokens:	<input checked="" type="checkbox"/> May distribute assigned software tokens to users
Token Attribute Definitions:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
SecurID 800 Smart Card Details:	<input checked="" type="checkbox"/> May import and manage smart card details including PIN unlocking key

14. Select the **View** checkbox in the **Manage User Groups** section.

15. Go to the **Manage User Authentication Attributes** section and:

- Select the **Edit** and **View** checkboxes in the **Fixed Passcode** row.
- Select the **May manually clear cached copy of the user's Windows credentials** checkbox.
- Select the **May manage incorrect passcode count** checkbox.
- Select the **Edit** and **View** checkboxes in the **Default Shell** row.

Manage User Groups	
User Group Restricted Access:	<input type="checkbox"/> All <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View

Manage User Authentication Attributes	
Fixed Passcode:	<input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Manage Windows Password Integration:	<input checked="" type="checkbox"/> May manually clear cached copy of user's Windows credentials
Manage Incorrect Passcode Count:	<input checked="" type="checkbox"/> May manage incorrect passcode count
Default Shell:	<input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Logon Aliases:	<input type="checkbox"/> Edit <input type="checkbox"/> View
Manage Offline Emergency Access Passcode:	<input type="checkbox"/> May manage offline emergency access passcode

16. Select the **View** checkbox in the **Manage Authentication Agents** section.

Manage Authentication Agents	
? Authentication Agent:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Grant Access to Restricted Agents:	<input type="checkbox"/> May grant user groups access to restricted authentication agents
? Manage Node Secret:	<input type="checkbox"/> May manage the shared secret between the authentication agent and the authentication server.

17. Go to the **Trusted Realm Management** section and select the **View** checkbox in the **Trusted Users** row, the **Trusted User Groups** row and the **Trusted User Group Restricted Access** row.

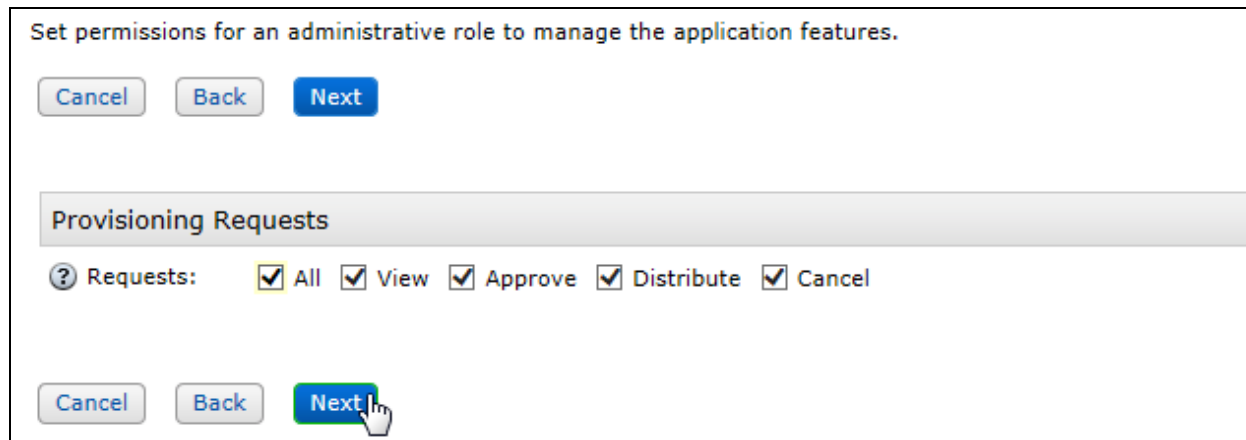
Trusted Realm Management	
? Trusted Users:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Trusted User Groups:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Trusted User Group Restricted Access:	<input type="checkbox"/> All <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
? Grant Trusted User Group Access to Trusted Users:	<input type="checkbox"/> May assign trusted used group memberships
? Grant Trusted User Group Access to Agents:	<input type="checkbox"/> May grant trusted used groups access to agents

Manage RADIUS	
? RADIUS Servers:	<input type="checkbox"/> Edit <input type="checkbox"/> View
? RADIUS Clients:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
? RADIUS Profiles:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
? Assign User RADIUS Profile:	<input type="checkbox"/> May assign a RADIUS profile to a user
? Assign Agent RADIUS Profile:	<input type="checkbox"/> May assign a RADIUS profile to an agent
? RADIUS User Attribute Definitions:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
? RADIUS User Attributes:	<input type="checkbox"/> Edit <input type="checkbox"/> View

18. Select the **May enable and disable users for on-demand authentication and provision associated PIN** checkbox in the **Manage On-Demand Authentication** section and click the **Next** button.

Manage On-Demand Authentication	
? Manage On-Demand Authentication:	<input checked="" type="checkbox"/> May enable and disable users for on-demand authentication and provision associated PIN

19. Select the **All** checkbox in the **Provisioning Requests** section and click the **Next** button.



The screenshot shows a configuration window titled "Set permissions for an administrative role to manage the application features." At the top, there are three buttons: "Cancel", "Back", and "Next". Below this is a section header "Provisioning Requests". Underneath the header, there is a label "? Requests:" followed by five checkboxes: "All", "View", "Approve", "Distribute", and "Cancel". All five checkboxes are checked. At the bottom of the window, there are three buttons: "Cancel", "Back", and "Next". A mouse cursor is pointing at the "Next" button.

20. Review the summary and click the **Save and Finish** button.

21. Create a new RSA Authentication Manager administrative user² and assign the administrative role to that user. You will need the user's credentials when you configure IdentityIQ.

! » Important: The new user's account must not have an expiration date. When you create the account, select the **Does not expire** radio button in the **Account Information** section.

² See the *RSA Authentication Manager Administration Guide* for information about creating users and assigning administrative roles

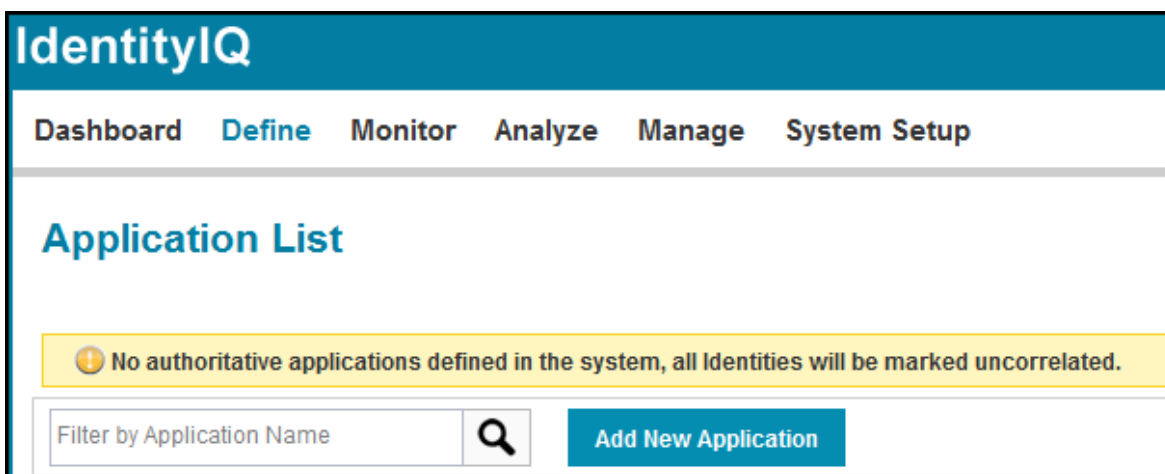
SailPoint IdentityIQ Configuration

You must define each application in your enterprise. Specify the connection properties, relevant attributes, targets and aggregation rules for each application. Use the **Application Configuration** page to define the applications in your enterprise. From this page you will specify the connection properties, relevant attributes, aggregation rules, and activity information for each application. Follow the steps below to create a new application:

1. Open a command prompt on the IdentityIQ host machine, navigate to the *identityiq* web application's *WEB-INF\bin* directory and type the following commands to launch the IdentityIQ console and import the *workflow_RSA_PIN_Reset.xml* configuration file

```
iis console
import workflow_RSA_PIN_Reset.xml
```

2. Login to IdentityIQ as a superadmin user.
3. Select the **Define** tab and click the **Add New Application** button.




4. Choose a unique name to identify the application and enter it into the **Name** field.
5. Enter the name of the application's owner in the **Owner** field.

*indicates a required field.

Name * RSA-8.1

Owner * The Administrator

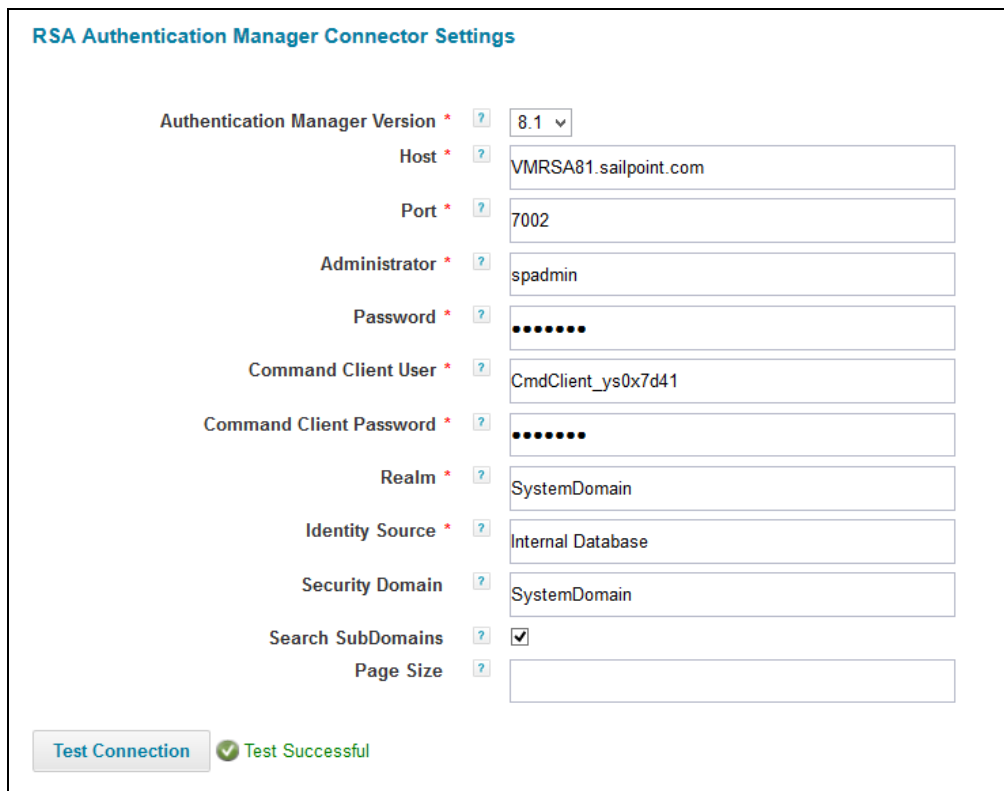
Revoker

 **Note:** Unless you include a revoker, the owner you specify will be responsible for the application's certification and account group certification. See the SailPoint IdentityIQ administration guide for details.

6. Select *RSA Authentication Manager – Direct* from the **Application Type** dropdown list.



7. Select the version of your RSA Authentication Manager server from the **Authentication Manager Version** dropdown list. The integration supports versions 8.0 and 8.1.
8. Enter the server's hostname and API connection port number in the **Host** and **Port** fields.
9. Enter your RSA Authentication Manager [administrator's username and password](#) in the **Administrator** and **Password** fields.
10. Enter the RSA [Command Client User's username and password](#) in the **Command Client Username** and **Command Client Password** fields.
11. Enter the name of the RSA Authentication Manager realm you will manage in the **Realm** field and the realm's identity source name in the **Identity Source** field.
12. Enter the name of the security domain you will manage in the **Security Domain** field. If you would like to manage its sub domains as well, check the **Search SubDomains** checkbox.
13. Click the **Save** button.

A screenshot of the 'RSA Authentication Manager Connector Settings' form. The form contains several fields with labels and help icons (question marks). The fields and their values are: 'Authentication Manager Version' (8.1), 'Host' (VMRSA81.sailpoint.com), 'Port' (7002), 'Administrator' (spadmin), 'Password' (masked with dots), 'Command Client User' (CmdClient_ys0x7d41), 'Command Client Password' (masked with dots), 'Realm' (SystemDomain), 'Identity Source' (Internal Database), 'Security Domain' (SystemDomain), 'Search SubDomains' (checked checkbox), and 'Page Size' (empty field). At the bottom left, there is a 'Test Connection' button and a green checkmark with the text 'Test Successful'.

Certification Checklist for RSA Authentication Manager

Date Tested: May 13, 2015

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.1.1	Appliance
RSA Authentication Manager API	8.1.1	Windows 2008
IdentityIQ	6.4	Windows 2008

Test	Result
Data Management	
Import RSA Authentication Manager data	✓
Reconcile RSA Authentication Manager data	✓
User Management	
Add a user	✓
Modify a user	✓
Delete a user	✓
Add a group	✓
Modify group	✓
Delete a group	✓
Add a user to a group	✓
Remove a user from a group	✓
Authentication Management	
Assign a token	✓
Un-assign a token	✓
Enable a token	✓
Disable a token	✓
Clear a PIN	✗
Reset a PIN	✓
Assign a password	✓
Unassign a password	✗
Change a user's authentication method	✗
Enable RBA	✗

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function