RSA SECURID® ACCESS
Authentication Manager SDK Implementation Guide

CyberArk Privileged Account Security v9.7

RSA Partner Engineering
Last Modified: 8/24/2016

RSA READY

Solution Summary

Privileged accounts represent the largest security vulnerability an organization faces today. In the hands of an external attacker or malicious insider, privileged accounts allow attackers to take full control of an organization's IT infrastructure, steal confidential information, commit financial fraud and disrupt operations. Stolen or misused privileged account credentials are used in nearly all breaches. With this growing threat, organizations need to put controls in place to detect and respond to in-progress cyber attacks before they strike vital systems and compromise sensitive data.

CyberArk, the trusted expert in privileged account security, has developed a powerful, modular technology platform that provides the industry's most comprehensive privileged account security solution. The CyberArk Privileged Account Security (PAS) solution version 9.7 is based on the CyberArk Shared Technology Platform™, which combines an isolated vault server, a unified policy engine and a discovery engine to provide scalability, reliability and unmatched security for privileged accounts. A CyberArk administrator can manage applications, operating systems, databases, hypervisors, network devices and additional products independently or in combination. The CyberArk Central Policy Manager (CPM) plugin for RSA Authentication Manager supports remote password management for the following types of RSA privileged users:

- **RSA Security Console Administrators** – The RSA Security Console web application is RSA Authentication Manager's primary administrative interface. Any RSA Authentication Manager user who has an administrative role is a Security Console administrator. A Security Console Administrator with super admin privileges can use the RSA Authentication Manager server API to manage all other Security Console administrators' passwords.

Note: This guide uses the term *super admin* to refer to an RSA Authentication Manager Security Console administrator with super admin priviledges.

- **RSA Operations Console Users** – The RSA Operations Console web application allows a select group of users (Operation Console administrators) to manage replica servers, identity sources, certificates and backups, and to perform various other system operations. Operation Console users are also entitled to run the *rsautil* utility on the RSA Authentication Manager appliance command line.

Supported Features

Supported RSA Authentication Manager Password Management Features CyberArk Privileged Account Security Solution 9.7	
Manage passwords for RSA Security Console administrators	YES
Manage passwords for RSA Operation Console administrators	YES

Partner Product Configuration

Before You Begin

This section contains instructions for enabling the CyberArk PAS solution to manage RSA Authentication Manager user passwords. Before you begin, you should have working knowledge of CyberArk CPM and RSA Authentication Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that both products are running properly prior to configuring the integration.

Make the RSA Root Certificate Available for the Plugin

You must export your RSA Authentication Manage server's root certificate and import it into your CPM host's keystore before the plugin can use the server's API. Follow the steps below to make the certificate available for the plugin. Consult the *Building and Running .NET Applications* section on the *Getting Started and Advanced Usage* page of the *RSA Authentication Manager Developer's Guide* for step-by-step instructions to perform the procedures.

1. Use Internet Explorer to export the certificate from you RSA Authentication Manager server and save it on your local machine.
2. Copy the root certificate from the local machine to the CPM host.
3. Use the Certificate Import Wizard to import the certificate into the client keystore.

Obtain RSA Authentication Manager Credentials

You will need to obtain the various RSA Authentication Manager credentials listed in the following sections in order to configure the CyberArk plugin. Consult the *RSA Authentication Manager Administrator's Guide* and the *RSA Authentication Manager Developer's Guide* for more information.

- **Obtain the RSA Authentication Manager Operating System User's Credentials**
- **Obtain RSA Authentication Manager Super Admin Credentials**
- **Obtain RSA Authentication Manager Operations Console User Credentials**
- **Obtain the Command Client User Name and Password**

Obtain the RSA Authentication Manager Operating System User's Credentials

The plugin uses the *rsaadmin* operating system user to connect to the RSA Authentication Manager appliance over SSH and manage Operations Console users' passwords as well as its own.

> **Important:** The integration does not support password management for the operating syetem user.

Obtain RSA Authentication Manager Super Admin Credentials

The plugin requires multiple RSA super admin account credentials[1] to manage Security Console users' passwords via the RSA Authentication Manager API. You created a super admin account when you initially setup your RSA Authentication Manager instance. Use this account to create a second super admin account. Consult the *RSA Authentication Manager Administrator's Guide* for details. You will need the credentials for both accounts to **create CyberArk Security Console Accounts**.

[1] In order to mange a Security Console user's password, the plugin requires super admin credentials to establish an RSA Authentication Manager API connection. If the super admin's password in the CyberArk Vault ever needs to be resynchronized with RSA Authentication Manager, the plugin must use a second super admin account to perform the reconciliation process.

Obtain RSA Authentication Manager Operations Console User Credentials

You will need RSA Authentication Manager Operations Console account credentials to retrieve the command client username and password in the following section. You created an Operations Console User account when you initially setup your RSA Authentication Manager instance.

Obtain the Command Client User Name and Password

When you install RSA Authentication Manager, the system creates credentials for securing API connections to the API's a command server. These credentials are randomly generated and unique to the server. Follow the procedure below to obtain the command client user name and password from RSA Authentication Manager. You will need these values when you **create a Security Console super admin account** in the CyberArk CPM. Consult the *RSA Authentication Manager Developer's Guide* for more information.

> **Important:** Command Client credentials are shared secrets that identify API client requests to a specific RSA Authentication Manager command server instance. You will not manage the credentials in the COM. They aren't associated with an RSA user account, and they should never be modified.

1. Open a command prompt on your RSA Authentication Manager host, navigate to the */opt/rsa/am/|utils* directory and enter the following command:

   rsautil manage-secrets --action list

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

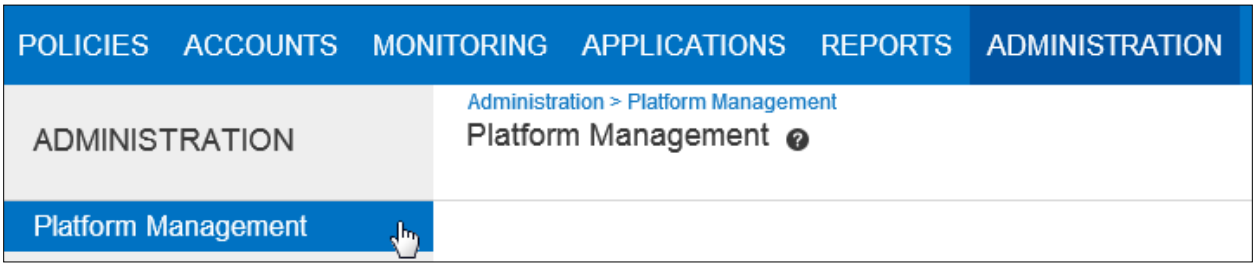
   Command Client User Name .....: **CmdClient_wnuoizd8**
   Command Client User Password .....: **ZNJVSP78smpzLZdPqmuN4OoZPZAByw**

Create CyberArk Accounts for RSA Authentication Manager Users

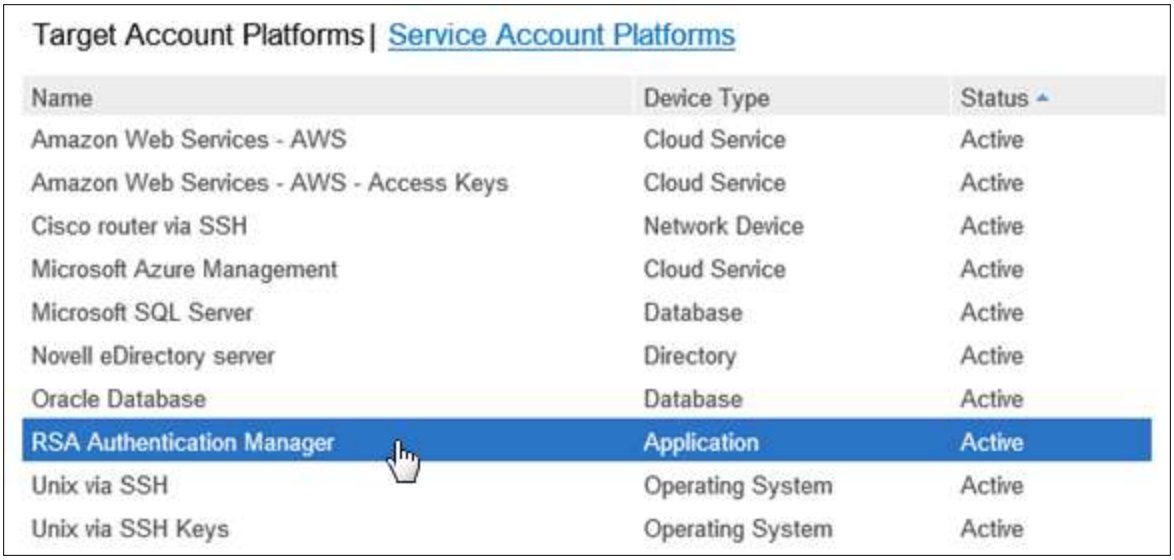
Follow the instructions below to create and link the accounts as illustrated.

Activate the RSA Authentication Manager Platform

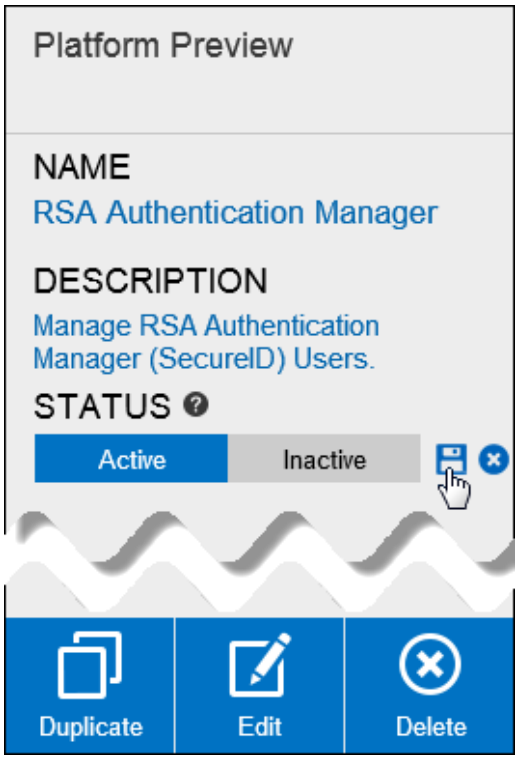
1. Log in to the Password Vault Web Access client (PVWA).
2. Select the **Administration** tab on the navigation bar and click the **Platform Management** button on the left hand side of the dashboard.



3. Click the **Target Account Platform** link at the top of the **Platform Management** view and select the **RSA Authentication Manager** platform. If the platform is active, **skip to the next section**. Otherwise continue to step 4.



4. To enable the RSA Authentication Manager platform, click the **Edit** button on the **Platform Preview** pane, set the *Status* toggle switch value to the *Active* and click the disk icon.



Create a Command Client User Account

Use your **RSA Command Client credentials** to create a CyberArk Command Client Account. The plugin will use the account to communicate with RSA Authentication Manager's API server.

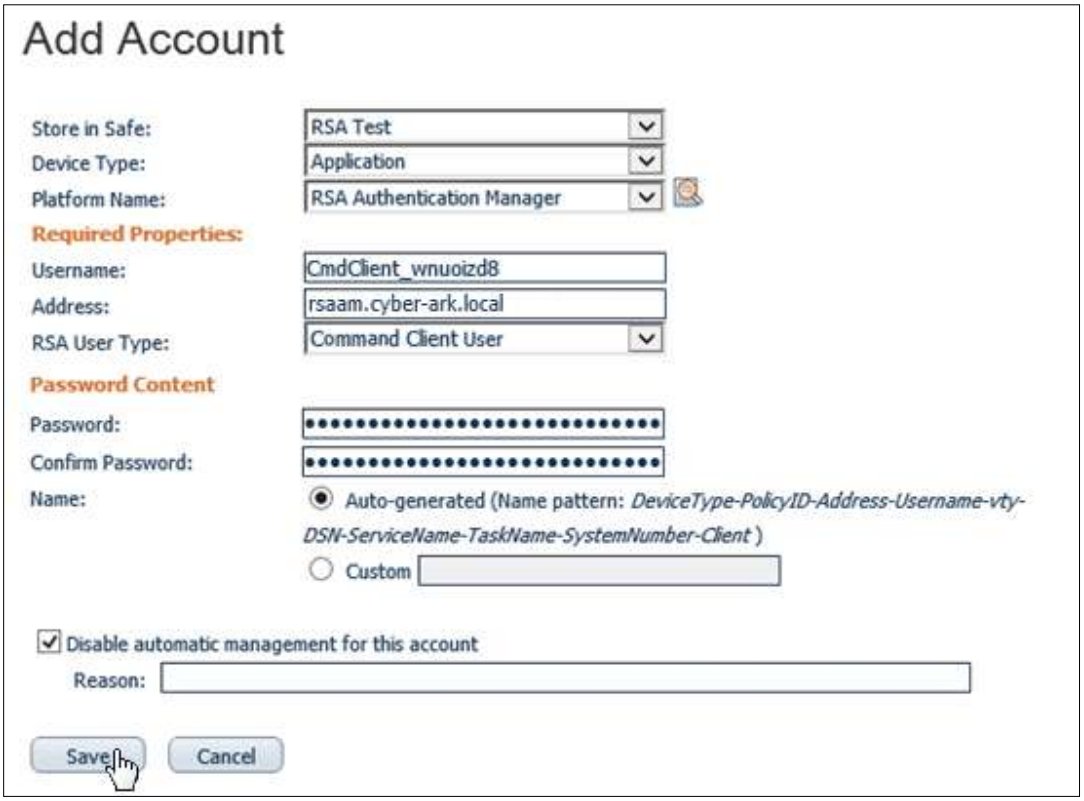
> **Important:** Never use CyeberArk to manage Command Client credentials. The credentials aren't associated with a user account. If you modify them, the plugin won't be able to communicate with RSA Authentiation Manger's API server.

1. Select the **Accounts** tab in the on the navigation bar at the top of the page.

2. Click the **Add Account** button underneath the navigation bar.

3. Select the appropriate safe from the **Store in Safe** dropdown list.
4. Select *Application* from the **Device Type** dropdown list.
5. Select *RSA Authentication Manager* from the **Platform Name** dropdown list.
6. Enter your **Command Client name** in the **Username** field.

7. Enter your RSA Authentication Manager primary server's IP address or fully qualified hostname in the **Address** field.
8. Select *Command Client User* from the **RSA User Type** dropdown list.
9. Enter your **Command Client password** in the **Password** and **Confirm Password** fields.
10. Select the **Disable automatic management for this account** checkbox.
11. Click the **Save** button.



Create and Configure Security User Accounts for RSA Super Admins

You must create a CyberArk Security User account for each of your **RSA Security Console super admins**. The plugin will use the accounts to manage passwords for other RSA Security Console administrators and RSA Operation Console users, and to reconcile one another's passwords if needed.

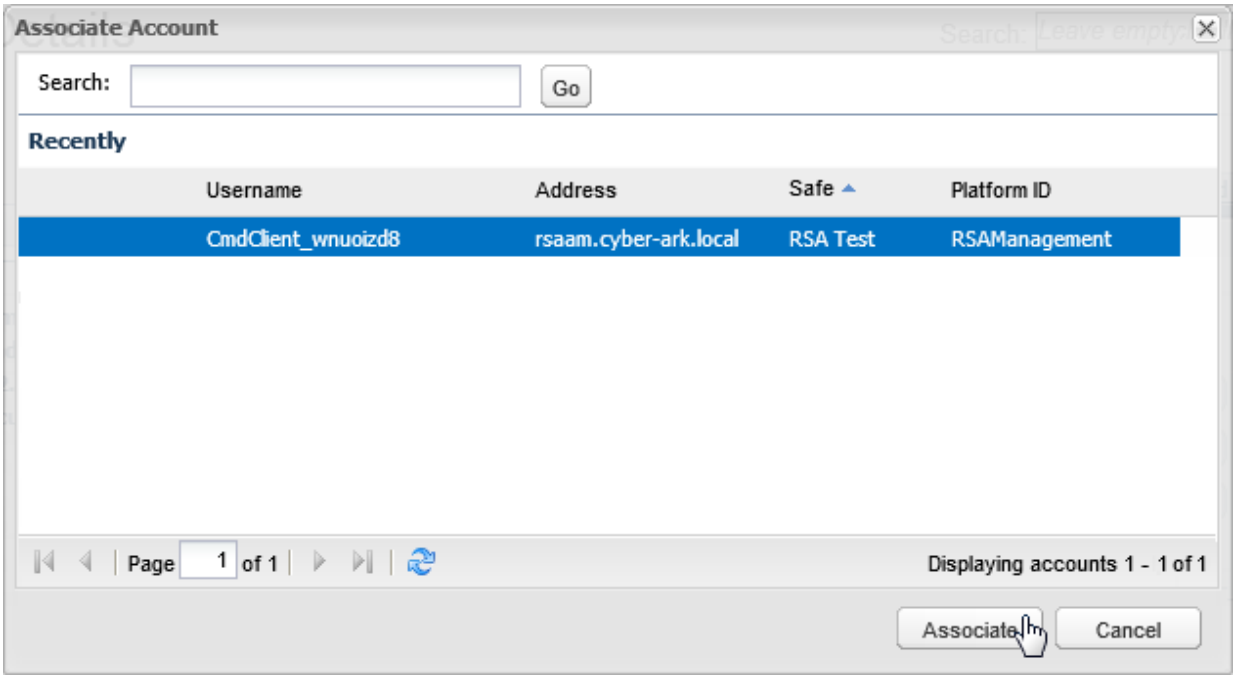
Add a Security User Account with Super Admin Credentials

Follow the instructions below for each of your RSA Authentication Manager super admin users.

1. Select the **Accounts** tab on the navigation bar and click the **Add Account** button.
2. Select the appropriate safe from the **Store in Safe** dropdown list.
3. Select *Application* from the **Device Type** dropdown list and *RSA Authentication Manager* from the **Platform Name** dropdown list.
4. Enter the **super admin's name** in the **Username** field.
5. Enter your RSA Authentication Manager primary server's IP address or fully qualified hostname in the **Address** field.
6. Select *Security User* from the **RSA User Type** dropdown list.
7. Enter the **super admin's password** in the **Password** and **Confirm Password** fields.
8. Select the **Disable automatic management for this account** checkbox.
9. Click the **Save** button.

10. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Logon Account** label.

11. Locate and select your Command Client account on the **Associate Account** form and click the **Associate** button.



Link the RSA Super Admin CyberArk Security User Accounts

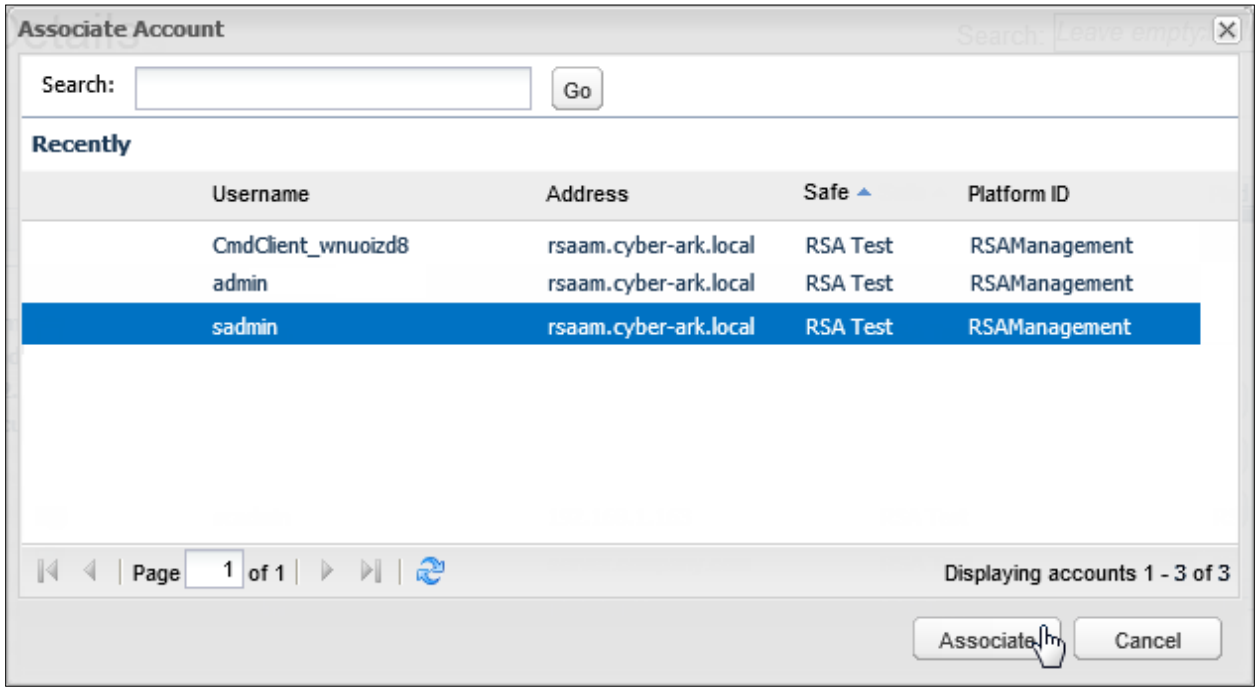
Follow the instructions below for each Security User account you created in the previous section. You will modify each account to use the other one as its reconciliation account. Consult CyberArk's PAS administrative documentation for more information about linked accounts.

> **Important:** Follow the instructions in this section for each of your RSA Super Admin CyberArk Security User accounts. In the example, the RSA Super Admins are named *admin* and *sadmin*. The *admin* user's account is edited below to use the *sadmin* user's account for reconciliation. The *sadmin* user's account should also be edited to use the *admin* user's account for reconciliation (not shown).

1. Select the **Accounts** tab on the navigation bar.
2. Select the row of the super admin Security User Account you want to modify in the table and check the checkbox in the row's first column.
3. Click the **Manage** menu above the table and click the **Edit** icon.

4. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Reconcile Account** label.

5. Select the other super admin Security User Account (*sadmin* in the example) from the list of accounts and click the **Associate** button.



Create an Operating System User Account

Use your RSA Authentication Manager **operating system user's (*rsaadmin*) credentials** to create a CyberArk Operating System User Account. The plugin will use the account to connect to the RSA Authentication Manager appliance over SSH in order to manage Operations Console users' passwords.

> **Important:** The integration does not support password management for the operating syetem user. You should only use the account as decribed below.

1. Select the **Accounts** tab on the navigation bar and click the **Add Account** button.
2. Select the appropriate safe from the **Store in Safe** dropdown list.
3. Select *Application* from the **Device Type** dropdown list.
4. Select *RSA Authentication Manager* from the **Platform Name** dropdown list.
5. Enter *rsaadmin* in the **Username** field.
6. Enter your RSA Authentication Manager primary server's IP address or fully qualified hostname in the **Address** field.
7. Select *Operating System User* from the **RSA User Type** dropdown list.
8. Enter your RSA Authentication Manager **operating system user's password** in the **Password** and **Confirm Password** fields.
9. Select the **Disable automatic management for this account** checkbox.
10. Click the **Save** button.

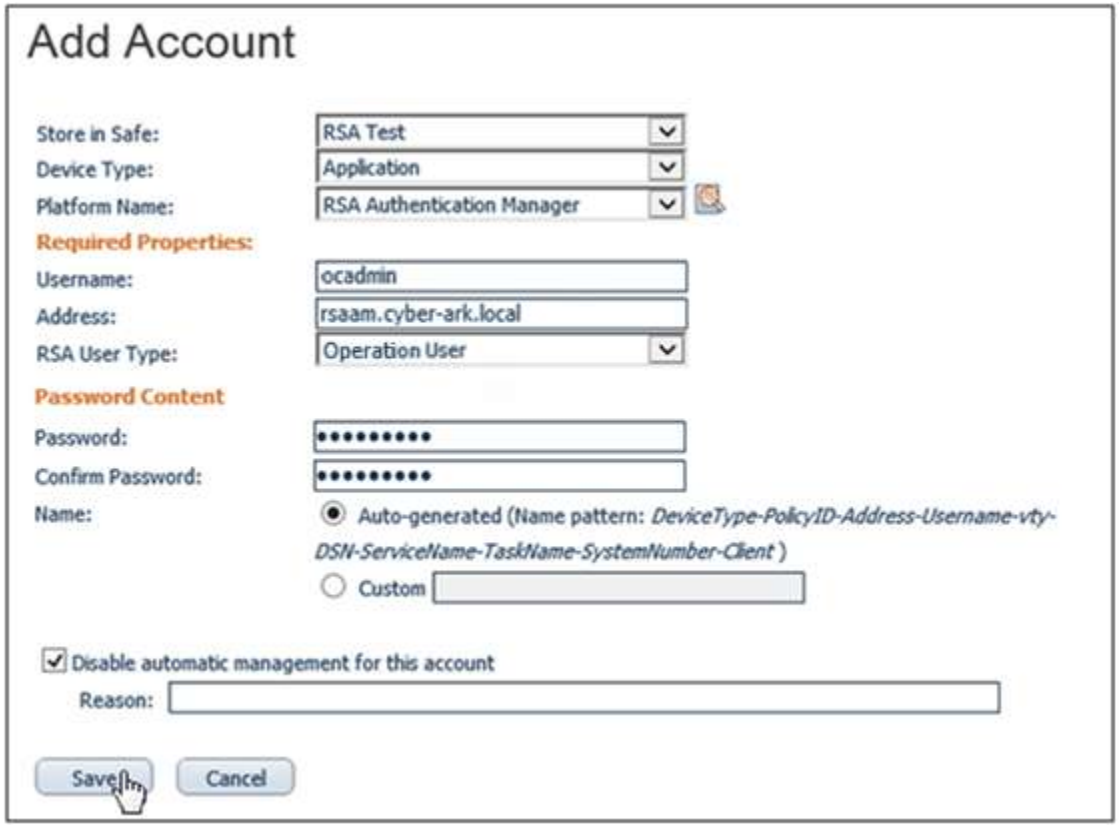
Create Additional Accounts for RSA Authentication Manager Users

Follow the instructions below to create accounts for RSA Operations Console users and additional RSA Security Console administrators.

Create Operation User Accounts

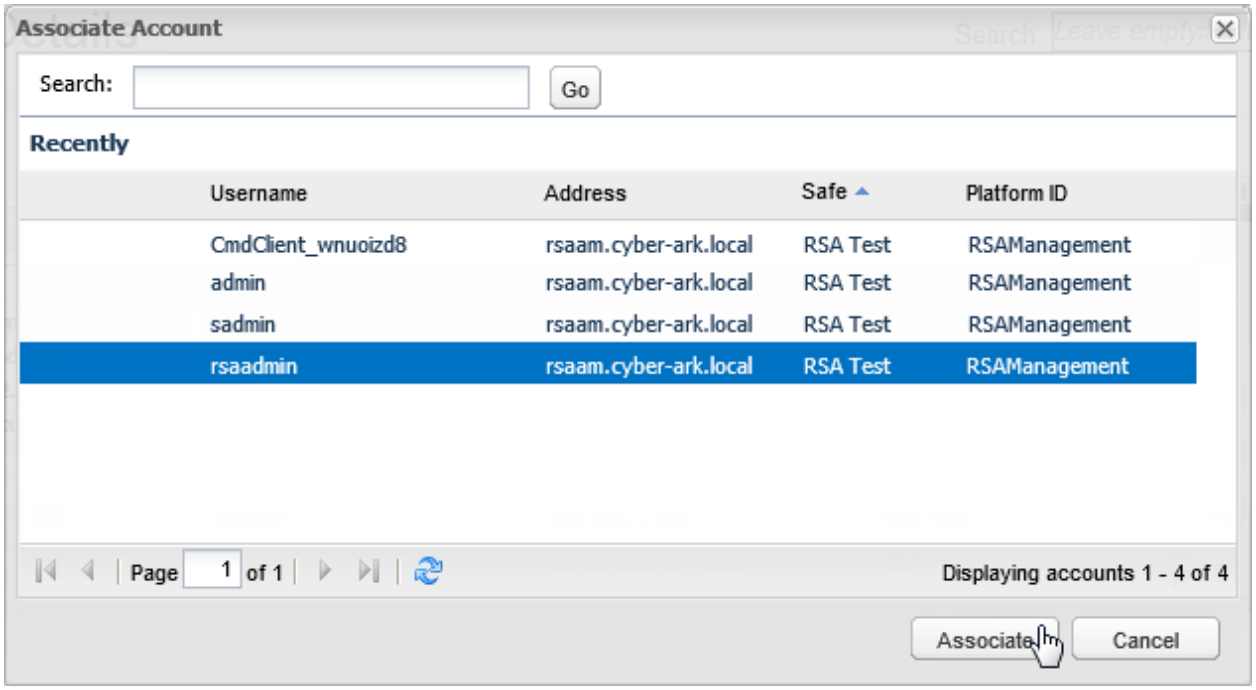
Follow the instructions below for each of your RSA Authentication Manager Operations Console users.

1. Select the **Accounts** tab on the navigation bar and click the **Add Account** button.
2. Select the appropriate safe from the **Store in Safe** dropdown list.
3. Select *Application* from the **Device Type** dropdown list and *RSA Authentication Manager* from the **Platform Name** dropdown list.
4. Enter the RSA Authentication Manager Operations Console user's username in the **Username** field.
5. Enter your RSA Authentication Manager primary server's IP address or fully qualified hostname in the **Address** field.
6. Select *Operation User* from the **RSA User Type** dropdown list.
7. Enter the Operations Console user's password in the **Password** and **Confirm Password** fields.
8. Select the **Disable automatic management for this account** checkbox.
9. Click the **Save** button.



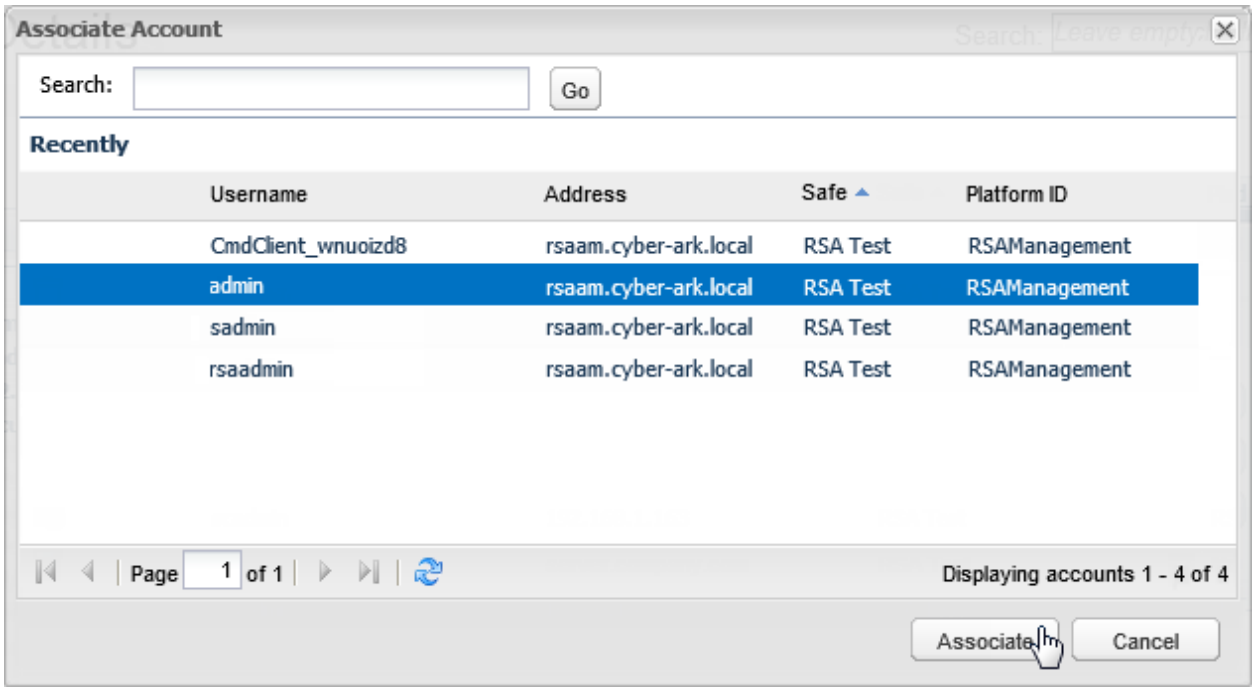
10. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Logon Account** label.

11. Locate and select your Operating System User account on the **Associate Account** form and click the **Associate** button.



12. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Reconcile Account** label.

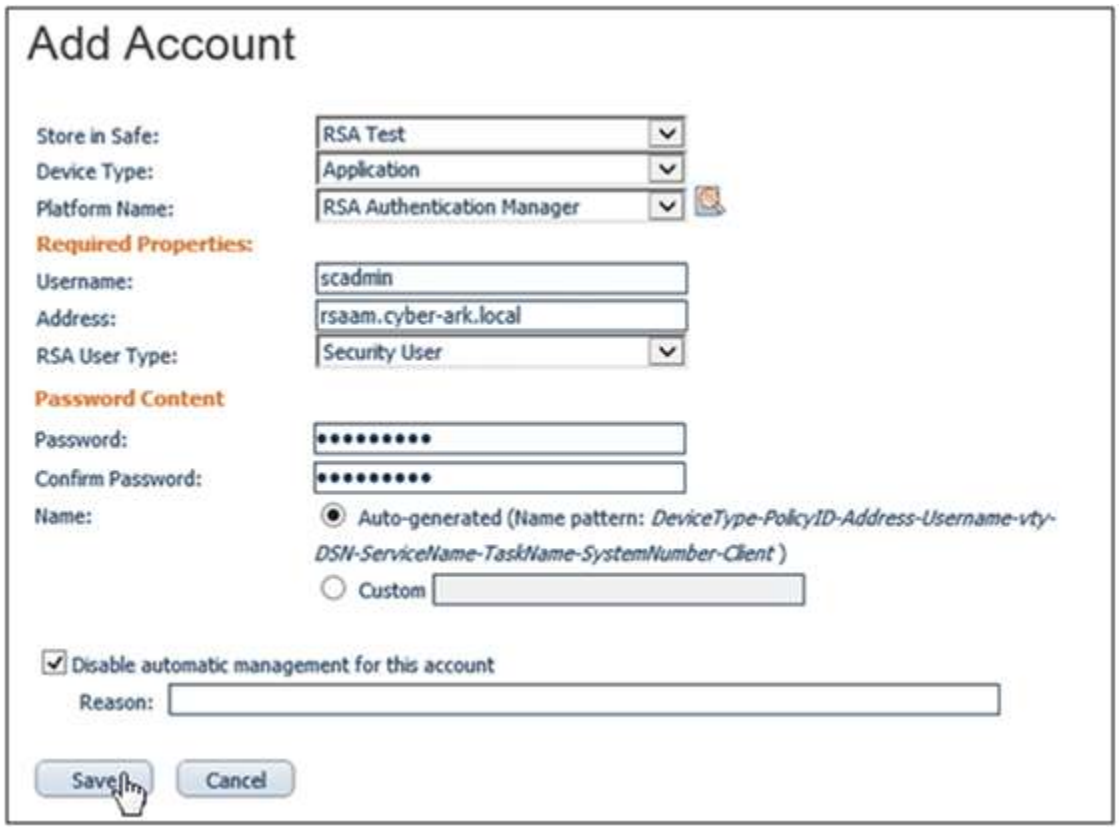
13. Select one of your super admin Security User Accounts from the list of accounts and click the **Associate** button.



Create Additional Security User Accounts

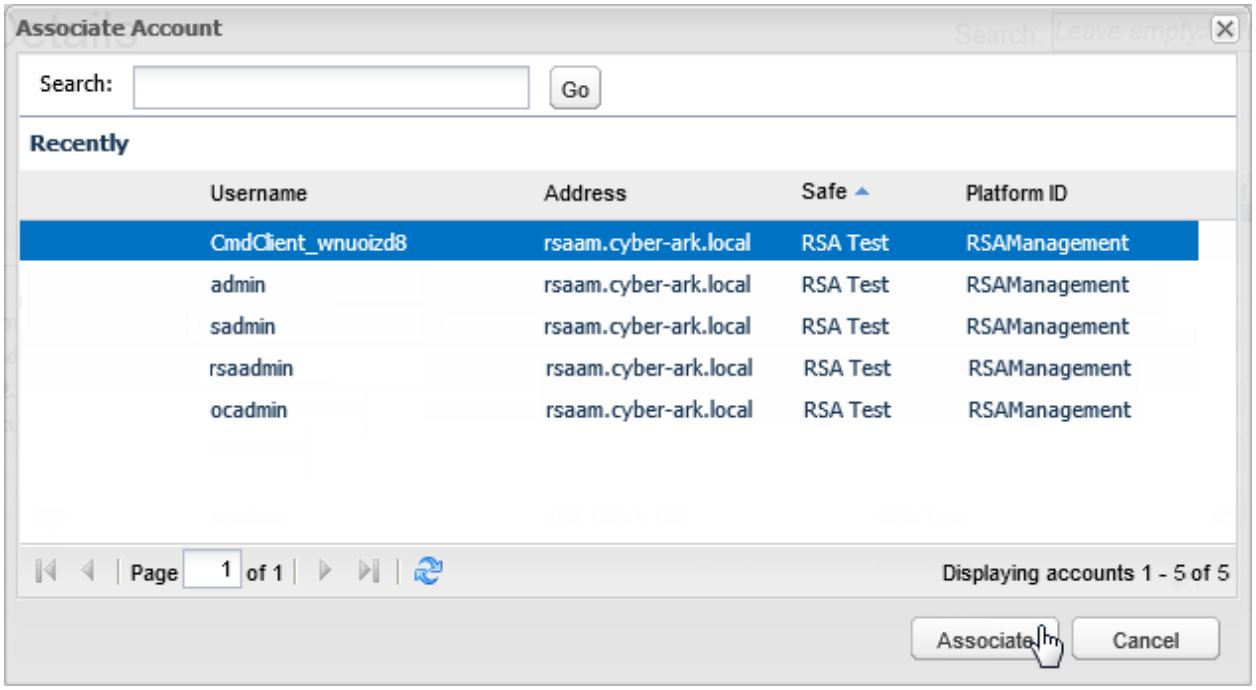
Follow the instructions below for each of your RSA Authentication Manager Security Console administrators who do not have super admin privileges.

1. Select the **Accounts** tab on the navigation bar and click the **Add Account** button.
2. Select the appropriate safe from the **Store in Safe** dropdown list.
3. Select *Application* from the **Device Type** dropdown list and *RSA Authentication Manager* from the **Platform Name** dropdown list.
4. Enter the RSA Security Console administrator's username in the **Username** field.
5. Enter your RSA Authentication Manager primary server's IP address or fully qualified hostname in the **Address** field.
6. Select *Security User* from the **RSA User Type** dropdown list.
7. Enter the RSA Security Console administrator's password in the **Password** and **Confirm Password** fields.
8. Select the **Disable automatic management for this account** checkbox.
9. Click the **Save** button.



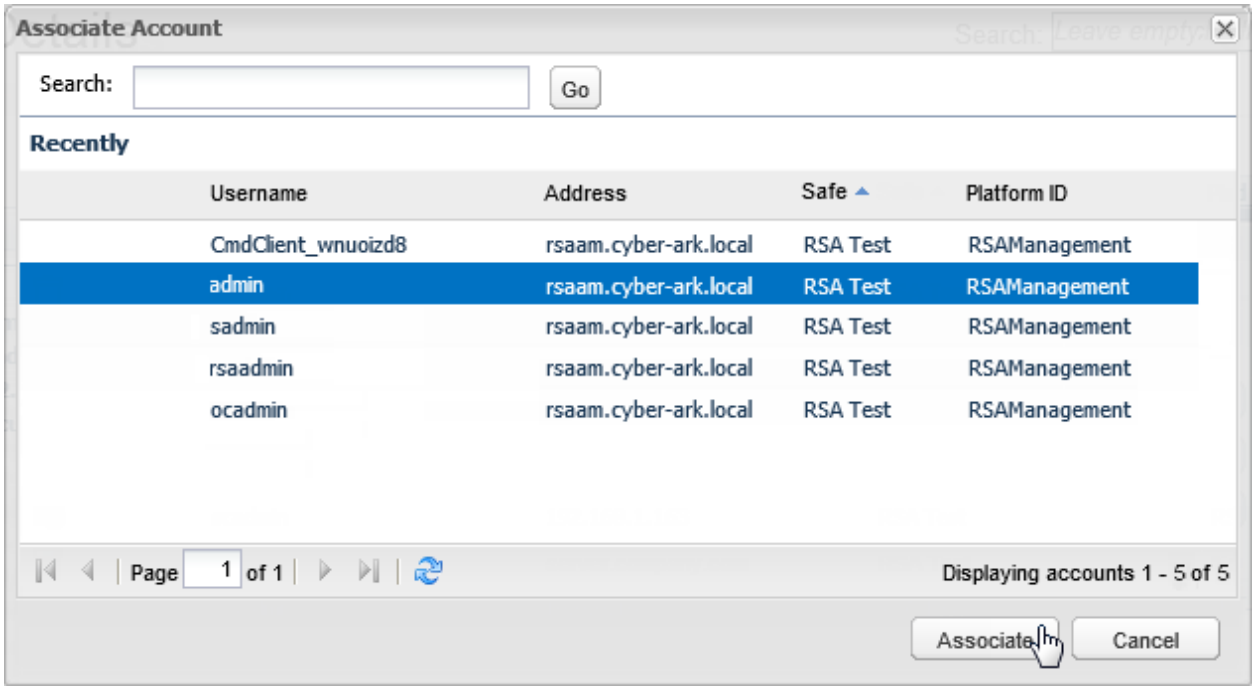
10. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Logon Account** label.

11. Locate and select your Command Client account on the **Associate Account** form and click the **Associate** button.



12. Select the **CPM** tab on the **Accounts Details** page and click the **Associate** button to the right of the **Reconcile Account** label.

13. Select one of your RSA super admin CyberArk Security User Accounts from the list of accounts and click the **Associate** button.



Certification Checklist for RSA Authentication Manager

Dates Tested 08/09/2016 and 08/19/2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1.1	Virtual Appliance
Privileged Account Security	9.7	Virtual Appliance

Credential Management

Functionality	
Password Management	
Manage Security Console Admin passwords	✓
Manage Operations Console Admin passwords	✓
Login Management	
Automated Login Support for Security Console Administrators	✗
Automated Login Support for Operations Console Administrators	✗

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