Courion Corporation
PasswordCourier 8.3

RSA Secured Implementation Guide
Administrative Interoperability

Last Modified: December 31, 2014

Partner Information

Product Information	
Partner Name	Courion Corporation
Web Site	www.courion.com
Product Name	PasswordCourier
Version & Platform	8.3
Product Description	PasswordCourier, Courion's password management solution, enables organizations to deploy self-service password reset and synchronization across a wide variety of enterprise systems. PasswordCourier is the industry standard for secure, self-service password management, featuring multiple access options, robust service desk integration, and the ability to enforce consistent password policies on any system, application, or Web portal.

Solution Summary

Courion PasswordCourier offers end-users self-service capabilities to manage their credentials, and it enables them to use a single password to access multiple systems. Courion has integrated PasswordCourier with hundreds of applications and platforms to ensure that password policies are enforced consistently across the enterprise.

The PasswordCourier Password Management Module (PPM) for RSA Authentication Manager allows RSA SecurID users to resynchronize their tokens, set/reset their token PINs and reset their RSA static passwords without calling the help desk for assistance.

Overview of the Courion PasswordCourier Integration's Supported Features	
Import Standard Card, Key Fob, PINPAD, and SoftID seed records	No
Add, modify and delete an RSA Authentication Manager user	No
Assign/unassign an RSA SecurID token	No
Enable/disable an RSA SecurID token	No
Resynchronize an RSA SecurID token	Yes
Clear/reset an RSA SecurID token's PIN	Yes
Change an RSA Authentication Manager static password	Yes
Reconcile RSA Authentication Manager users with data store	No

Important: Most of the features listed above aren't applicable to this integration because Courion PasswordCourier is an end-user self-service tool. However, Courion also offers an RSA Authentication Manager integration with their AccountCourier product. The Courion AccountCourier integration allows Courion administrators to provision and manage RSA Authentication Manager users and tokens.

See RSA Partner Engineering's *Courion AccountCourier 8.3 - RSA Authentication Manager 8.1* implementation guide for details.

Before You Begin

This guide provides instructions for enabling Courion PasswordCourier end-users to manage their RSA Authentication Manager credentials. You should have working knowledge of the Courion Suite, PasswordCourier and RSA Authentication Manager, as well as access to end-user and administrative documentation. Ensure that all products are running properly prior to configuring the integration.

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

Before you configure the Password Management Module for RSA Authentication Manager, you must also map your RSA Authentication Manager users to Courion PasswordCourier users. Consult the Courion PasswordCourier administrator's guide for more information.

Important: This document lists a subset of the integration's functionality. A full list of the integration's use cases and workflows are well outside of this document's scope. Please see the appropriate PasswordCourier documentation for a complete list and description of the PPM's features and comprehensive instructions for configuring, using and troubleshooting the integration.

Configuration

This section describes the procedures you must perform on RSA Authentication Manager and Courion PasswordCourier to enable the integration. It is divided in to the following subsections:

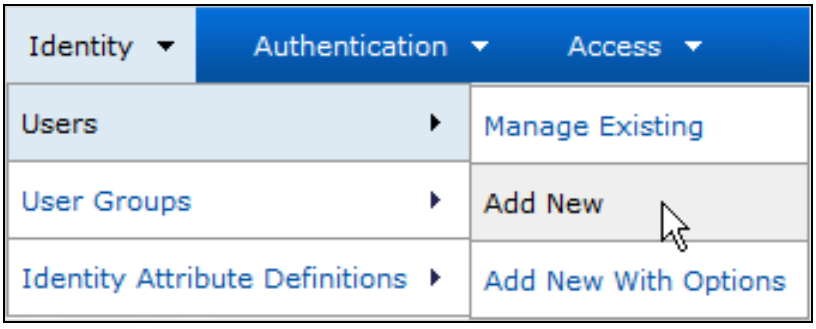
RSA Authentication Manager Configuration

Before you configure the PasswordCourier Password Management Module, you must create an RSA Authentication Manager administrative user account and give it the permissions the module needs perform various provisioning and reconciliation operations.

Create an RSA Administrative User for PasswordCourier

An RSA Authentication Manager Administrative Role is a collection of administrative privileges that are limited to a specific security domain scope. Follow the instructions below to create an RSA Authentication Manager user account and assign it an administrative role that contains the permissions required for the integration.

1. Log in to the RSA Security console as a super administrator.
2. Click the **Identity** menu, click the **Users** submenu and select the **Add New** menu item.



3. Based on your requirements, decide on the RSA Authentication Manager domain you wish to manage and select it from the **Security Domain** dropdown list.

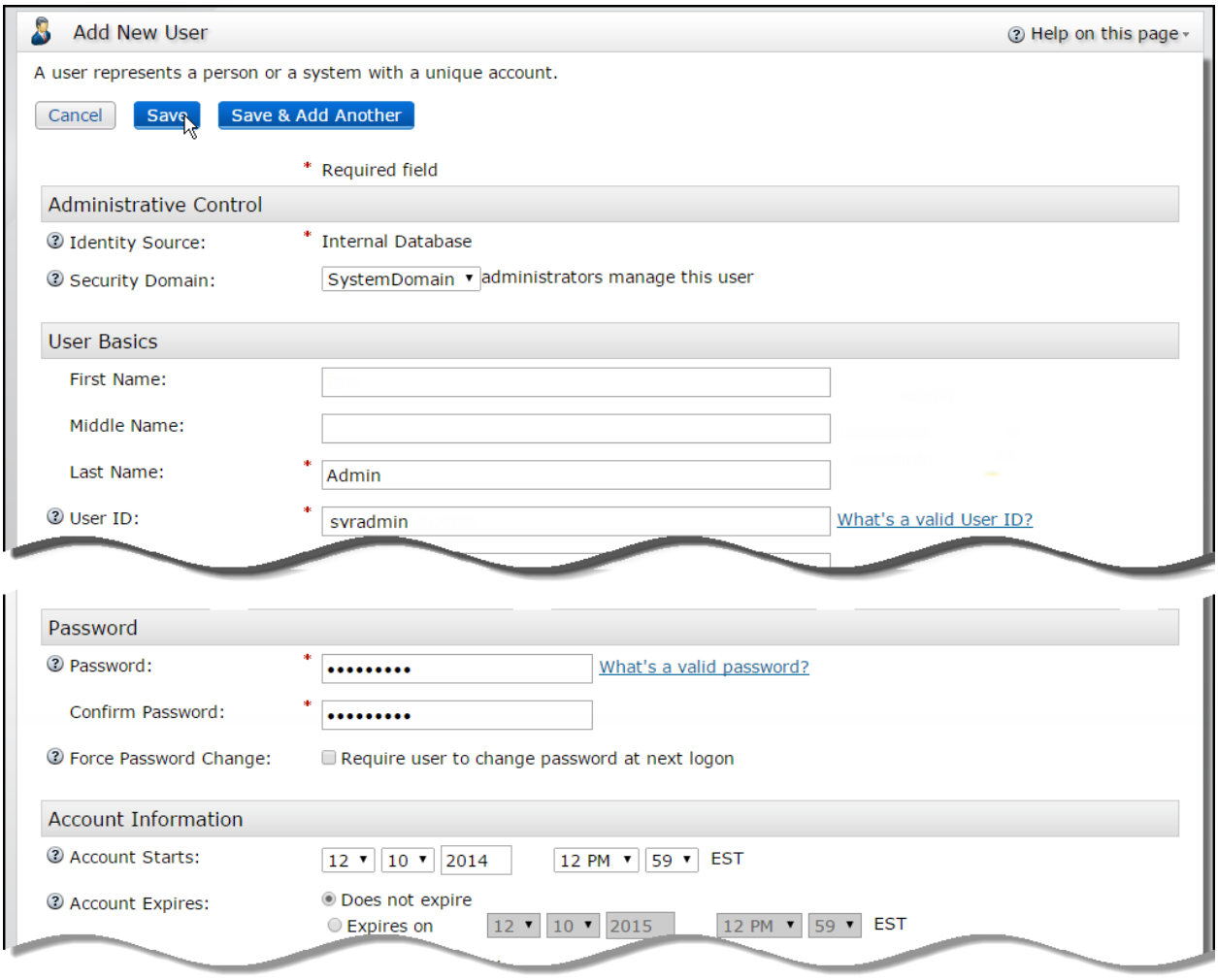
Note: The role in the example below applies to the top-level *SystemDomain*, which gives it unlimited privileges to manage all RSA Authentication Manager resources.

4. Optionally, enter the administrator's first name in the **First Name** field.
5. Optionally, enter the administrator's middle name in the **Middle Name** field.
6. Enter the administrator's last name in the **Last Name** field.
7. Choose a username for the administrator and enter it in the **User ID** field.
8. Optionally, enter the user's email address in the **Email** field.
9. Optionally, enter notes about the account in the **Notes** field.

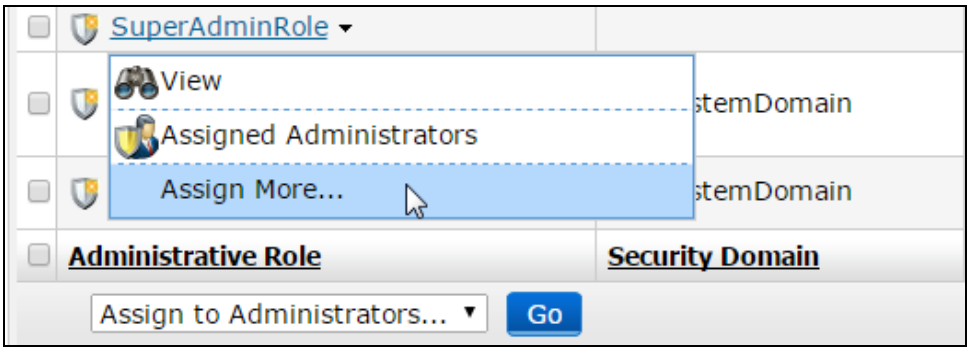
10. Enter a password for the administrator's account into the **Password** field and again in the **Confirm Password** field.

Note: You must enter the new administrator's credentials when you configure the Password Management Module. See the PrivilegedUser and PrivilegedUserPwd variables.

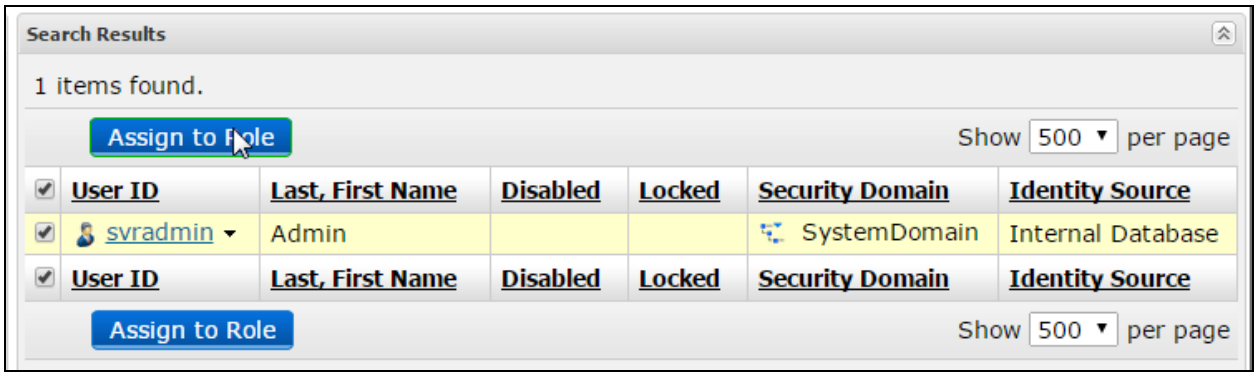
11. Uncheck the **Force Password Change** checkbox.
12. Select the **Does not expire radio** button in the **Account Expires** option group.
13. Click the **Save** button.



14. Click the **Administration** menu, click the **Administrative Roles** submenu and select the **Manage Existing** menu item.
15. Click the **SuperAdminRole** link and select the **Assign More…** item from the context menu.



16. Search for the user you created above, select the user' row in the **Search Results** table and click the **Assign Role** button.



Retrieve the RSA Command Client Credentials

During the RSA Authentication Manager installation process, the system generates credentials that each API client must use to connect to the RSA API Command Server. Follow the instructions below to obtain the command client user name and password for the connector:

1. Connect to your RSA Authentication Manager server virtual appliance using an SCP or SSH client, navigate to the *%RSA_AM_HOME%/utils* directory and enter the following command:

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

2. Enter the RSA Authentication Manager super user's master password when you are prompted.
3. The system will display a list of internal system passwords that includes the command client user name and password. Locate them in the list and copy them for later use. For example:

```
Command Client User Name ..................: CmdClient_1mhw9dqk
Command Client User Password ..............: e9SHbKOW4i
```

Important: Take note of the command client user name and password. You will need them when you configure the Password Management Module. See the *CommandUser* and *CommandUserPwd* variables.

PasswordCourier Password Management Module Configuration

The integration's Password Management Module communicates with an RSA Authentication Manager server using the server's administrative API. Follow the instructions below to provide the PPM access to the API, the server's location and the proper credentials.

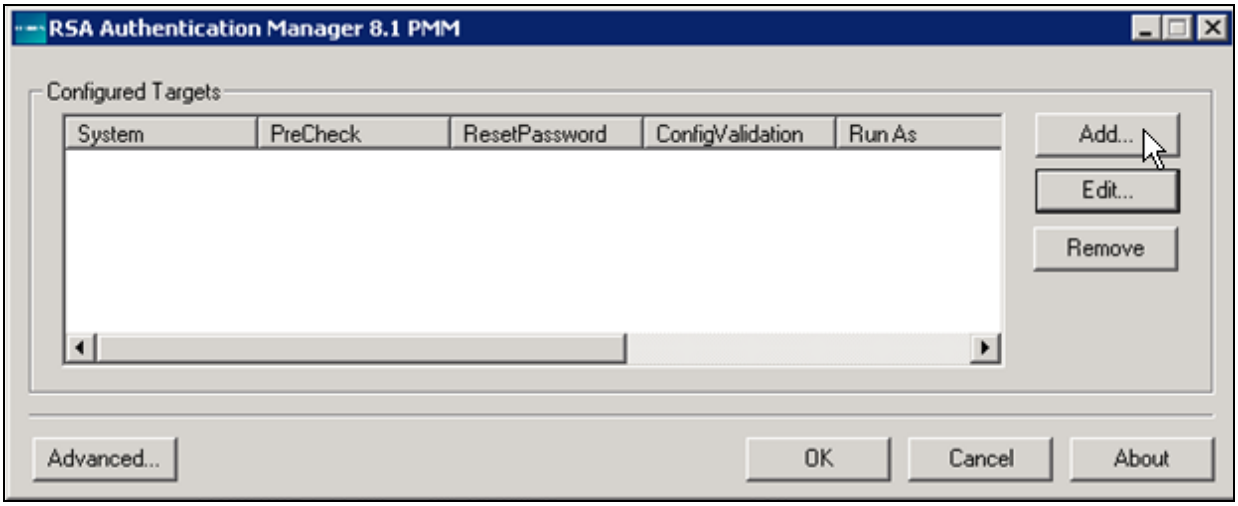
Note: This section uses the variables listed in the table below.

Variable Name	Description
%COURION_RSA_API_HOME%	The RSA Authentication Manager SDK installation directory on the Connector Framework and the Connector Framework Server. The default directory is: *C:\Program Files\ Courion Corporation\CourionService*
%DOT_NET_VER%	The version of the .NET framework installed in your Courion environment. (.NET 2.0, .NET 3.5 or .NET 4.0). Consult your Courion documentation for details.
%RSA _SDK_DIST_FILE%	A file named *rsa-am-extras-8.1.0.0.0.zip* that contains the RSA Authentication Manager 8.1 server SDK, documentation and utilities. It is bundled with the RSA Authentication Manager 8.1 distribution kit.
%RSA_AM_HOME%	The RSA Authentication Manager server's installation directory
%RSA_HOST%	The RSA Authentication Manager server's host name
%RSA_DOT_NET_API_ROOT%	The path to the RSA Authentication Manager 8.1 Administrative .NET API library that the PPM will use to communicate with RSA Authentication Manager. You will copy the API from this path to the *%COURION_RSA_API_HOME%* directory on the Connector Framework and the Connector Framework Server. **Note**: The path is relative to *the %RSA _SDK_DIST_FILE%* file's (unzipped) root directory. There are three versions of the library, one for each .NET framework version listed in the *%DOT_NET_VER%* description above. Each library has its own root directory: • *\RSA Authentication Manager SDK\lib\dotnet20* • *\RSA Authentication Manager SDK\lib\dotnet35* • *\RSA Authentication Manager SDK\lib\dotnet40*
%TEMP_DIR%	A temporary directory.

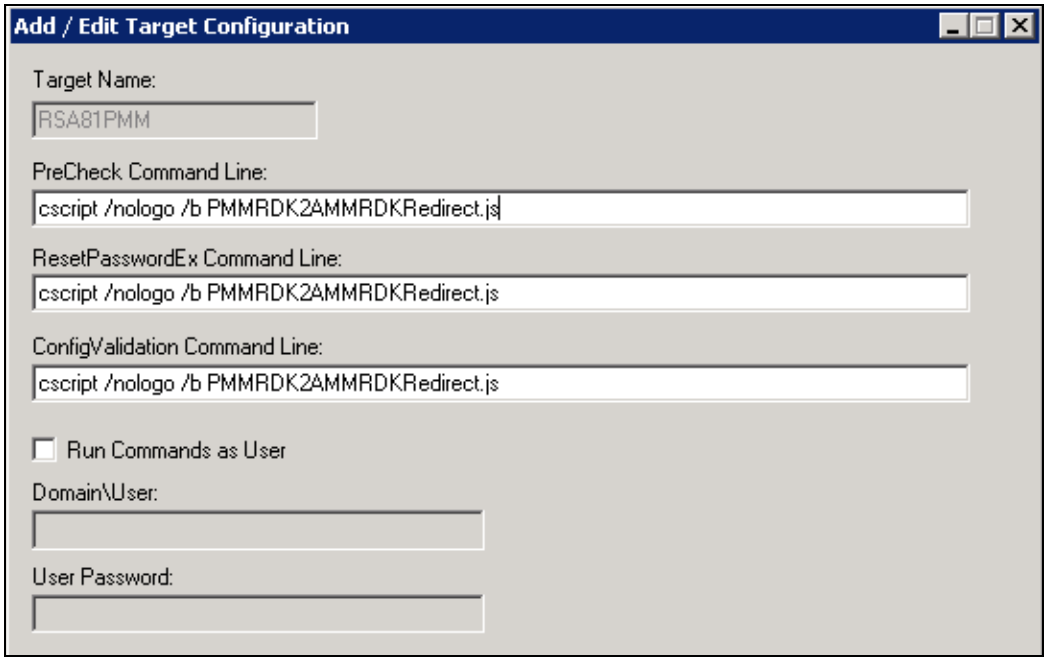
Follow the step below to configure a Password Management Module for RSA Authentication Manager:

1. The standard RSA Authentication Manager 8.1 virtual appliance distribution kit is bundled with a *ZIP* file named *rsa-am-extras-8.1.0.0.0.zip*, which contains various utilities, documentation, and the RSA Authentication Manager 8.1 Administrative SDK. Unzip this file into a temporary directory (*%TEMP_DIR%*).
2. Navigate to the *%TEMP_DIR%\%RSA_DOT_NET_API_ROOT%* directory.

3. Copy the *rsaws.dll* library to the *%COURION_RSA_API_HOME%* directory on the on the Connector Framework and the Connector Framework Server.
4. Open the Windows **Start** menu and select the **Programs → Courion Access Assurance Suite → Password Management Modules→ RSA Authentication Manager** menu item to launch the RSA Authentication Manager PPM target configuration dialog box.



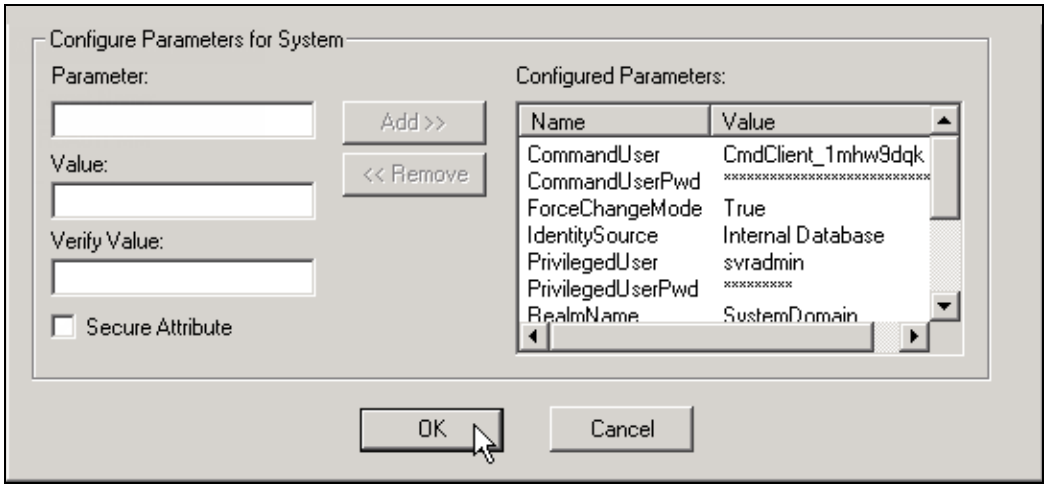
5. Click the **Add** button to open the RSA PPM configuration page. If you already created an RSA PPM, you will see it listed in the **Configured Targets** table. To change a value, select the target, click the **Edit** button and add the variable and new value to the **Configuration Parameters** list.
6. Enter a name for the RSA Authentication Manager target system in the **Target Name** field.
7. Enter *cscript /nologo /b PPMRDK2AMMRDKRedirect.js* in the **PreCheck Command Line**, **ResetPasswordEx Command Line** and **ConfigValidation Command Line** fields.
8. Uncheck the **Run Command as User** checkbox.



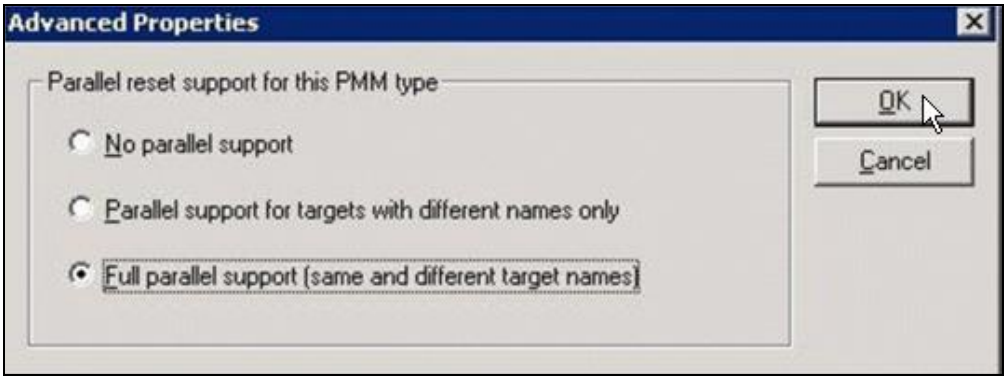
9. For each of the key value pairs in the following table:
    a. Enter the parameter name in the **Parameter** field.
    b. Enter the parameter value in the in the **Value** and **Verify Value** fields.
    c. When you add the *CommandUser* parameter and the *CommandUserPwd* parameter, check the **Secure Attribute** checkbox. Otherwise, leave the checkbox unchecked.
    d. Click the **Add** button.

Name	Value
RSAServerURL	- the RSA service command server URL *https:// %RSA_HOST%:7002/ims-ws/ services/CommandServer*
CommandUser	- the RSA Command Client username
CommandUserPwd	- the RSA Command Client password
PrivilegedUser	- the RSA Authentication Manager administrator's username
PrivilegedUserPwd	- the RSA Authentication Manager administrator's password
RealmName	- the name of the RSA security domain that the PPM will manage.
IdentitySource	- the RSA Authentication Manager security domain's identity source … Consult your *RSA Authentication Manager Administrator's Guide* for information about identity sources.
WeakValidation	- an optional, boolean variable that determines whether the PPM can connect to an RSA Authentication Manager server without using a certificate to authenticate … If you set this value to *False*, you must install your RSA Authentication Manager server's root certificate on your Courion server. Consult the *Courion PasswordCourier Administrator's Guide* for more information. The default value is *True*.
ForceChangeMode	- an optional, boolean variable that determines whether a user's RSA SecurID PIN will enter New PIN Mode whenever he/she uses PasswordCourier to change it. If you set this value to *True*, RSA Authentication Manager will force users to change their PINs the next time they authenticate. The default value is *False*.
ResourceType	- the type of RSA Authentication Manager resource that the PPM will manage Valid values are *Principal* (for user accounts) and *Token*. Consult the Courion PasswordCourier administrator's guide for more information
ScriptName	*RSAAuthMgr81Cnctr.js*

10. Click the **OK** button.



11. When you return to the PPM target configuration dialog box, select the RSA PPM target's row in the **Configured Targets** table and click the **Advanced** button.
12. Select the **Full Parallel Support (same and different target names)** radio button on the **Advanced Properties** dialog box.
13. Click the **OK** button.



14. Click the **OK** button on the **Add Target** dialog box.

Certification Checklist

Date Tested: December 9, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
PasswordCourier	8.3	Windows Server 2008 R2

Test	Result
Connect to RSA Authentication Manager Database for initial import	✓
User Management	
Add a user	N/A
Modify a user's information	N/A
Enable/Disable a user's account	N/A
Add a user to a group	N/A
Remove a user from a group	N/A
Token/Password Management	
Assign/unassign a token	N/A
Enable/Disable a user's token	N/A
Resynchronize a user's token	✓
Clear/Reset token's PIN	✓
Import Software token seed records	N/A
Assign/Reset user's password	✓
Reconciliation	
Reconcile entire RSA Authentication Manager user account data	N/A
Reconcile individual RSA Authentication Manager user account data	N/A

JGS / PAR

✓ = Pass ✗ = Fail N/A = Not Available

Known Issues

1. Although user names are case sensitive within RSA Authentication Manager, they are case-insensitive within the Courion IdentityMap(TM). For example, if you create an RSA Authentication Manager user account with a user ID of *issTest2*, and then create another with a user id of *ISSTEST2*, the Courion IdentityMap will replace the *issTest2* account with the *ISSTEST2* account.
2. Password reset functions are only supported for user accounts that are stored in the RSA Authentication Manager server's Internal Database identity source.
3. The integration displays a generic message if a user violates the current RSA Authentication Manager password policy's **minimum lifetime** setting. For example, if a user tries to reset his/her password twice in one day, and RSA Authentication Manager's password policy's **minimum lifetime** parameter is set to 1 day, PasswordCourier will display the following message: "Password policy not satisfied."