CA Technologies
CA Identity Manager 12.6

Secured by RSA Implementation Guide for Administrative Interoperability

Last Modified: June 9, 2015

Partner Information

Product Information	
Partner Name	CA Technologies
Web Site	http://www.ca.com/us/securecenter/ca-identity-manager.aspx
Product Name	CA Identity Manager
Version & Platform	12.6
Product Description	CA Identity Manager delivers a unified solution for user provisioning and user management that manages users' identities throughout their entire lifecycle, providing them with timely, appropriate access to applications and data. The user provisioning and identity management solutions that CA offers can give users access to what they want when they need it.

Solution Summary

CA Identity Manager provides a single point of entry to manage user identities throughout their entire lifecycle, allowing users timely, appropriate access to applications and data. The Identity Manager connector platform simplifies the task of building Identity Manager provisioning integrations with third party products. A connector runs as part of the wider Provisioning Server architecture, acts as a gateway to a native endpoint system or application and manages its endpoint's resources.

The CA Identity Manager RSA SecurID connector permits Identity Manager administrators to provision users, groups, RSA SecurID tokens and resources directly to RSA Authentication Manger. You can use the connector to provision the following RSA Authentication Manager resources:

Accounts (Local and trusted)
Administrative roles
RADIUS profiles
RSA SecurID Tokens
Security domains
Trusted groups
User groups

You can also use the connector to view read-only information about the following object types:

Authentication agents
Authentication grade policies
Identity sources
Lockout policies
Authentication policies
Token policies
Self-service policies
Trusted realms

Important: This guide contains instructions to configure the connector. See the *CA Identity Management & Governance Connectors: RSA SecurID Connector* guide for a complete list of the connector's features and comprehensive instructions on how to use them.

CA Identity Manager 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
Enable/disable RSA SecurID tokens	Yes
Reset RSA SecurID token PINs	Yes
Enable Risk-Based Authentication (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

Configuration

Before You Begin

Important: You must Install or upgrade CA IAM Connection Server and register it with the CA Provisioning Server. For information about installing and configuring the CA IAM Connector Server, see *the CA Identity Manager Connectors Guide* or visit the *CA Identity Management & Governance Connectors* wiki page (https://wiki.ca.com/pages/viewpage.action?pageId=120917235).

This section provides instructions for enabling CA Identity Manager to provision RSA Authentication Manager resources. You should have working knowledge CA Identity Manager, the CA IAM Connector Server and RSA Authentication Manager, as well as access to the appropriate administrative documentation. Ensure that these products are running properly prior to configuring the integration.

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

Configure RSA Authentication Manager

Prerequisites

You must complete the following prerequisites on your Identity Manager host to configure RSA Authentication Manager 8.1 API security settings. Consult your *RSA Authentication Manager 8.1 Developer's Guide* for 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.

- Set the required Java system properties.
- Set the required system environment settings.
- Export the root certificate from the RSA Authentication Manager server.
- 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 randomly generates a user name and password for securing API connections to the RSA API command server. You will need these credentials when you configure the connector. Follow the procedure below to obtain the them.

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

   rsautil manage-secrets --action list

2. When prompted, enter your RSA Operations Console administrator's username and password. 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_txtrvjoc
Command Client User Password ..............: e9SHbK0W4i
```

Create an RSA Authentication Manager Account for Connector Operations

The connector must use an RSA Authentication Manager administrative account with a *superadmin* role in order to perform operations with RSA Authentication Manager Server API. Follow the steps below to create the account:

1. Log in to the RSA Security Console, select the **Identity→Users→Add New** menu item and enter values for the required fields. You will need the username and password you choose when you configure Identity Manager.
2. Uncheck the **Force Password Change** checkbox, select the **Does not expire** radio button in the **Account Expires** options group and click the **Save** button.

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.

3. When you return to the **Users** page, click the down arrow to the right of the new user's name and select the **Administrative Role** menu item.
4. Click the **Assign Role** button, select the **SuperAdminRole** checkbox and click the **Assign Role** button at the bottom of the page.

Configure CA Identity Manager

Prerequisites

You must complete the following prerequisites before configuring you connector.

- Obtain a copy of the RSA SecurID CA Identity Manager Connector
- Obtain a copy of the RSA SecurID Attributes List for CA Identity Manager Connector
- Generate/update an OSGI bundle for the connector that includes the RSA Authentication Manager 8.1 API JAR files.
- Use the Connection Server to deploy the OSGI bundle

Important: Visit the CA Identity Management & Governance Connector Download page to download attribute lists and connectors. You will need CA Support credentials to access the page.

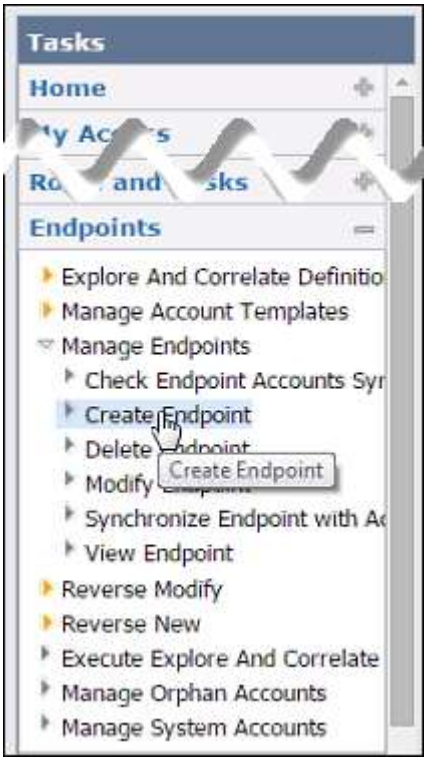
See the *CA Identity Management & Governance Connectors: RSA SecurID Connector* guide for instructions to upgrade an older RSA SecurID Connector OSGI bundle or to generate a new one.

See the *CA Identity Manager Connectors Guide* or visit the *CA Identity Management & Governance Connectors* wiki page (https://wiki.ca.com/pages/viewpage.action?pageId=120917235) for instructions to deploy OSGI bundles with the CA IAM Connection Server.

Acquire an RSA SecurID Endpoint

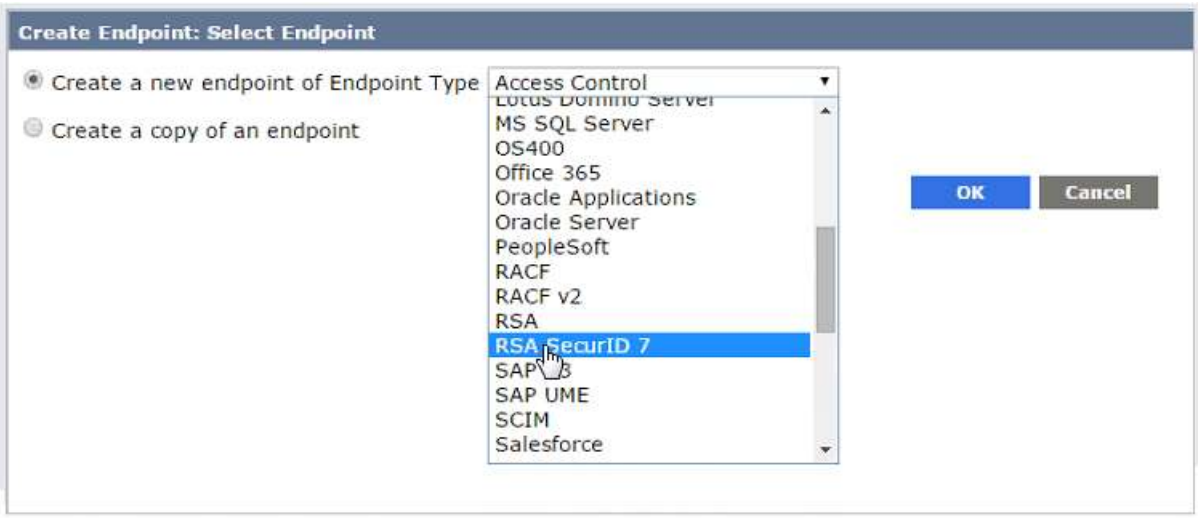
Follow the instructions below to acquire an RSA SecurID endpoint.

1. Log in to CA Identity Manager as an administrator and select the **Tasks→Endpoints→Manage Endpoints→Create Endpoint** menu item.

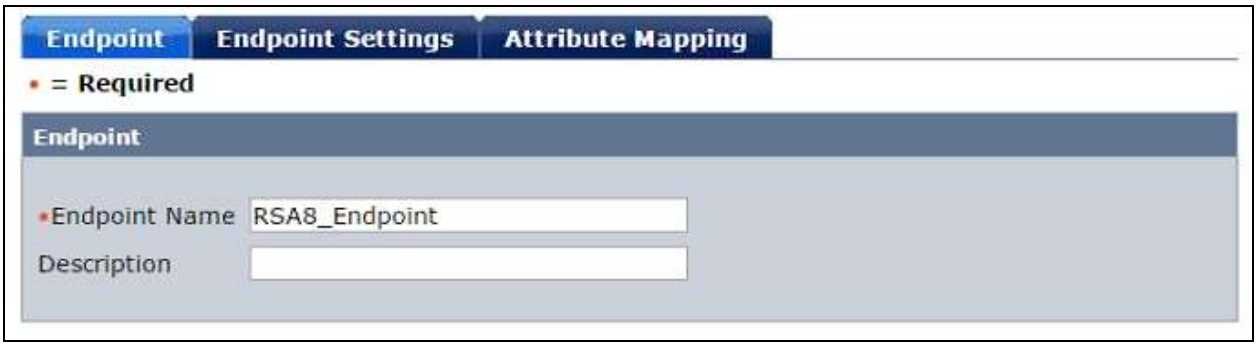


2. Select the radio button labeled **Create a new endpoint of Endpoint Type**, select *RSA SecurID 7* from the dropdown list and click the **OK** button.

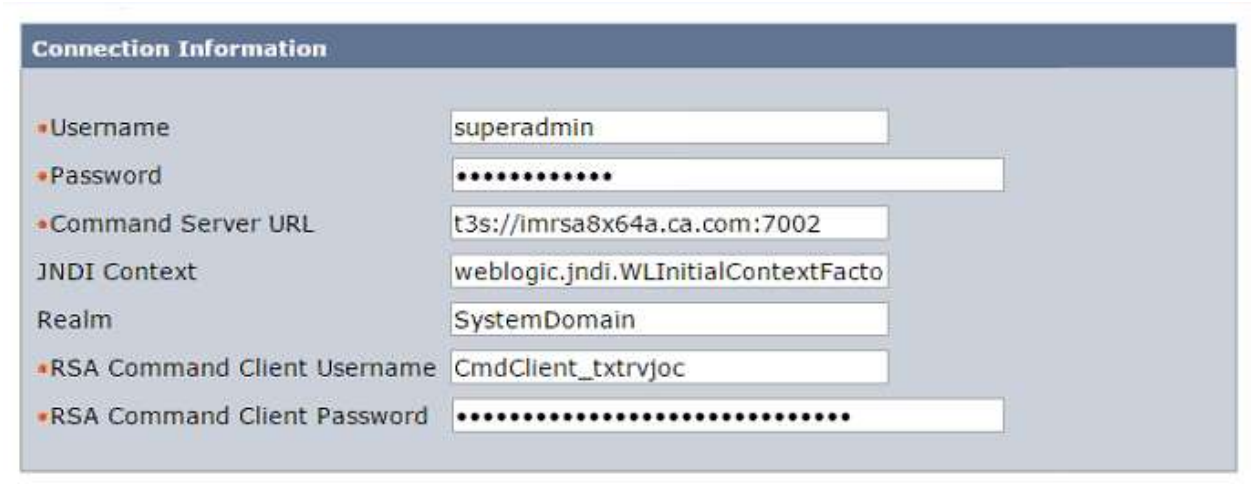
Important: The *RSA SecurID 7* endpoint type supports RSA Authentication Manager 8.x.



3. Select the **Endpoint** tab and enter a name for the endpoint in the **Endpoint Name** field.



4. Enter the RSA Authentication Manager Administrator's username in the **Username** field.
5. Enter the RSA Authentication Manager Administrator's password in the **Password** field.
6. Enter the RSA Authentication Manager Command Server's URL in the **Command Server URL** field.
7. Enter the RSA Command Client username in the **RSA Command Client Username** field.
8. Enter the RSA Command Client password in the **RSA Command Client Password** field.



9. Complete the remaining fields on the **Endpoint** tab based on your preferences or requirements and click the **Submit** button.

Once you have created the endpoint, you can use CA Identity Manager to explore, import and provision RSA Authentication Manager user accounts and resources. You have the choice of correlating existing RSA user accounts to Identity Manager global users or creating new Identity Manager global users and provisioning them to RSA Authentication Manager. See the *CA Identity Management & Governance Connectors: RSA SecurID Connector* guide for instructions.

Important: Instructions on how to use the connector are out of the scope of this document. See the *CA Identity Management & Governance Connectors: RSA SecurID Connector* guide for a complete list of the connector's features and comprehensive instructions on how to create new users, correlate existing user accounts and manage RSA Authentication resources.

Certification Checklist for RSA Authentication Manager

Date Tested: April 15, 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 R2 SP1 (64-bit)
CA Identity Manager	12.6 SP5 # 386	Windows 2008 R2 SP1 (64-bit)

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 user PIN	✓
Assign a password	✓
Change a user's authentication method	✓
Enable RBA	✗

JGS / PAR

✓ = Pass ✗ = Fail N/A = Not applicable

Known Issues

See the *CA Identity Management & Governance Connectors: RSA SecurID Connector* guide for an up-to-date list of know issues with the RSA SecurID Connector.