# Caradigm
## Single Sign-On and Context Management 6.2.7

# RSA Ready Implementation Guide for RSA SecurID

# Caradigm Single Sign-On and Context Management 6.2.7

John Sammon, RSA Partner Engineering
Last Modified: March 1, 2016

RSA READY

# Solution Summary

Caradigm customers integrate Caradigm's Electronic Prescriptions for Controlled Substances (EPCS) offering into their clinical applications. Administrated by the Drug Enforcement Administration, EPCS permits physicians to electronically prescribe drugs for their patients that are classified as controlled substances.

Caradigm's Single Sign-On and Context Management (SSO & CM) offering includes Multi-Factor Authentication supporting RSA SecurID authentication in two modes – Local RSA Client and Vault RSA Client. When an end-user launches a customer's EPCS application, the user must submit RSA SecurID credentials in order to complete the process of prescribing controlled substances.

A Caradigm RSA client is a workstation or a collection of workstations that is protected by RSA Authentication Manager. There are two types of Caradigm RSA clients: local RSA client and vault RSA client.

The local RSA client is a single workstation that communicates with RSA Authentication Manager. The client software is installed on a workstation, and the workstation is registered on the RSA server as an authentication agent.

The vault RSA client is a proxy to several workstations, and it serves as a single endpoint to RSA Authentication Manager. The client software is installed on the Caradigm vault cluster that maintains the Single Sign-On and Context Management information for users who access these workstations.

The primary vault must be registered on the RSA server as an authentication agent. The secondary vault may also be registered on the RSA server as an authentication agent as well. Doing so will enable the secondary vault to serve as the authentication agent in the event the primary vault is offline. You may also choose to register backup vaults in the cluster with the RSA server.

| RSA Authentication Manager supported features | |
|---|---|
| **Caradigm Single Sign-On and Context Management 6.2.7** | |
| **RSA SecurID Authentication via Native RSA SecurID UDP Protocol** | Yes |
| **RSA SecurID Authentication via Native RSA SecurID TCP Protocol** | No |
| **RSA SecurID Authentication via RADIUS Protocol** | No |
| **RSA SecurID Authentication via IPv6** | No |
| **On-Demand Authentication via Native SecurID UDP Protocol** | Yes |
| **On-Demand Authentication via Native SecurID TCP Protocol** | No |
| **On-Demand Authentication via RADIUS Protocol** | No |
| **Risk-Based Authentication** | No |
| **RSA Authentication Manager Replica Support** | Yes |
| **Secondary RADIUS Server Support** | No |
| **RSA SecurID Software Token Automation** | No |
| **RSA SecurID SD800 Token Automation** | No |
| **RSA SecurID Protection of Administrative Interface** | No |

# RSA Authentication Manager Configuration

## *Agent Host Configuration*

To facilitate communication between Caradigm SSO & CM and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies a Caradigm RSA client and contains information about communication and encryption. Use the RSA Security Console to create an agent record for each Caradigm local client or each cluster of vault RSA clients in your environment.

For each local RSA client, you'll need the following information:

- The local RSA client's hostname
- IP addresses for all of the local RSA client's network interfaces

**! Important: The agent's hostname must resolve to the IP address specified.**

For each cluster of vault RSA clients, you'll need the following information:

- The cluster's hostname
- The cluster's virtual IP address and IP addresses for all vaults chosen to be authentication agents.

**! Important: The agent's hostname must resolve to the cluster's Virtual IP address.**

When you add the authentication agent, set the agent type to "Standard Agent". This setting is used by the RSA Authentication Manager to determine how communication with Caradigm SSO & CM will occur.

# Partner Product Configuration

## *Before You Begin*

This section provides instructions for configuring Caradigm SSO & CM with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that you have both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Caradigm SSO & CM components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## *Caradigm Single Sign-On and Context Management Configuration*

After verifying that the Caradigm SSO & CM components are properly installed and functioning, follow the steps in the appropriate section below based on the type of Caradigm RSA Client you wish to configure.

- Caradigm RSA Local Client Configuration
- Caradigm RSA Vault Client Configuration

### Caradigm RSA Local Client Configuration

If you are configuring a local RSA, download your agent's *sdconf.rec* file to your workstation and save it in the EPCS EMR installation folder. Refer to the *RSA Authentication Manager Administrator's Guide* for instructions to generate an *sdconf.rec* file.

### Caradigm RSA Vault Client Configuration

To configure a vault RSA client, perform the following steps:

1. Download the *sdconf.rec* file and save it in to a temporary folder. Refer to the *RSA Authentication Manager Administrator's Guide* for instructions to generate an *sdconf.rec* file.
2. Log in to the SSO & CM Administrator at the URL below using a Microsoft Internet Explorer browser:

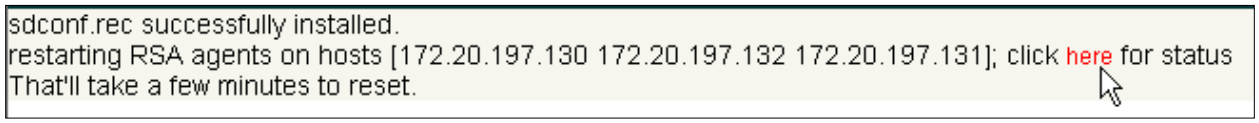
   **https://*VIP_Or_Vault_Identifier*:10000**

3. Click the **Appliance** tab.

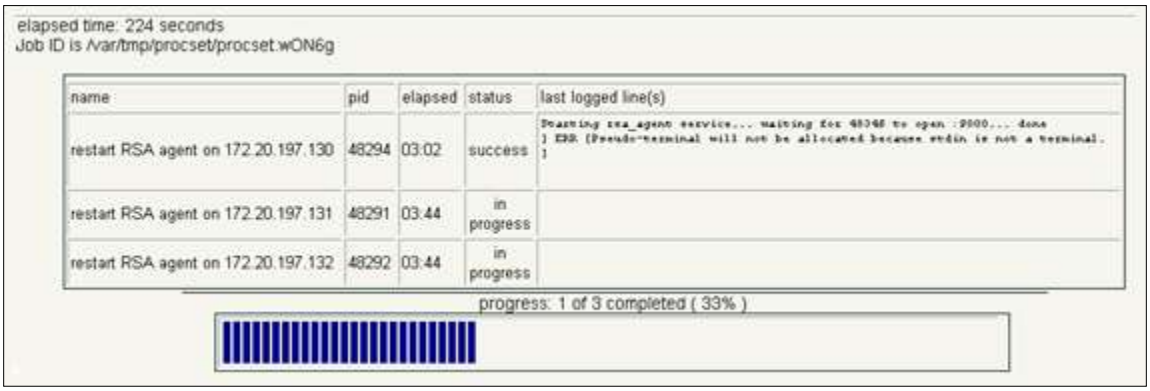

4. Click the **RSA Agent Management** link.


5. Click the **Browse...** button, locate and select your *sdconf.rec* file, and click the **Install** button

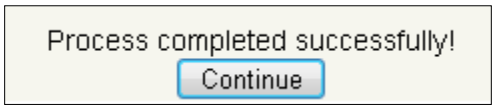

6. The console will display a message that the *sdconf.rec* file has been successfully installed and that the RSA *rsa_agent* service is restarting. You may click the **here** link to observe this process.



**Note: It takes approximately five minutes for the *rsa_agent* service to restart, but the time may vary depending on the number of vaults in your cluster.**




7. When the service has finished restarting, click the **Continue** button.

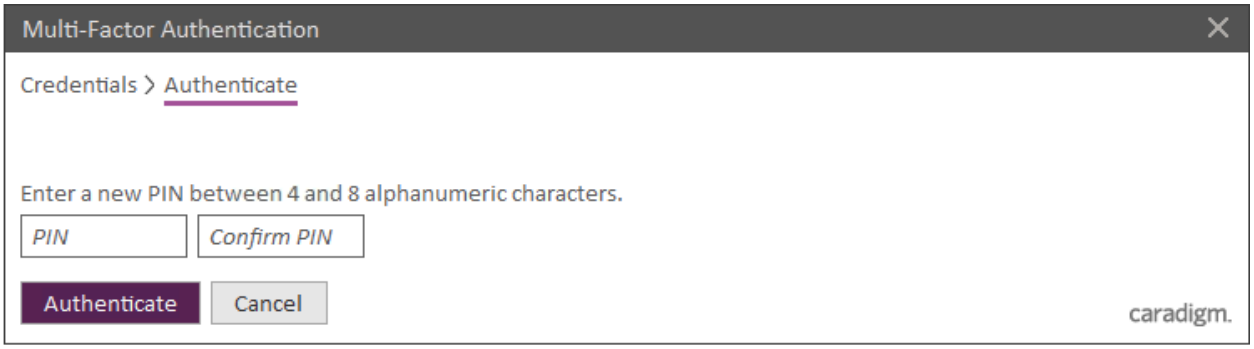



8. You may now log out of the SSO and Context Management Administrator console.

# RSA SecurID Login Screens

Login screen:


User-defined New PIN:




System-generated New PIN:

Next Tokencode:

# Certification Checklist for RSA Authentication Manager

Date Tested: January 19, 2016

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 8.1.1 | Virtual Appliance |
| **RSA Authentication Agent API** | Vault –Java API 8.1.3<br>Local Client – C API 8.1.2 | Vault – CentOS 6.5<br>Local Client – C API 8.1.2 |
| **Caradigm Single Sign-On and Context Management** | 6.2.7 | Vault – CentOS 6.5<br>Local Client - Win7/8.1 |

## *RSA SecurID Authentication*

Date Tested: : January 19, 2016

| Mandatory Functionality | Native UDP | Native TCP | RADIUS Client |
|---|---|---|---|
| **New PIN Mode** | | | |
| Force Authentication After New PIN | ✓ | N/A | N/A |
| System Generated PIN | ✓ | N/A | N/A |
| User Defined (4-8 Alphanumeric) | ✓ | N/A | N/A |
| User Defined (5-7 Numeric) | ✓ | N/A | N/A |
| Deny 4 and 8 Digit PIN | ✓ | N/A | N/A |
| Deny Alphanumeric PIN | ✓ | N/A | N/A |
| Deny PIN Reuse | ✓ | N/A | N/A |
| **Passcode** | | | |
| 16 Digit Passcode | ✓ | N/A | N/A |
| 4 Digit Fixed Passcode | ✓ | N/A | N/A |
| **Next Tokencode Mode** | | | |
| Next Tokencode Mode | ✓ | N/A | N/A |
| **On-Demand Authentication** | | | |
| On-Demand Authentication | ✓ | N/A | N/A |
| On-Demand New PIN | ✓ | N/A | N/A |
| **Load Balancing / Reliability Testing** | | | |
| Failover (3-10 Replicas) | ✓ | N/A | N/A |
| No RSA Authentication Manager | ✓ | N/A | N/A |

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

RSA READY

# Appendix

## *RSA SecurID Authentication Files*

| RSA SecurID Authentication Files | |
|---|---|
| **UDP Agent Files** | **Location** |
| sdconf.rec | Vault: /usr/local/rsa Local Client: Same folder as EPCS EMR. |
| sdopts.rec | Vault: /usr/local/rsa Local Client: Same folder as EPCS EMR. |
| Node secret | Vault: /usr/local/rsa Local Client: Same folder as EPCS EMR. |
| sdstatus.12 / jastatus.12 | Vault: /usr/local/rsa Local Client: Same folder as EPCS EMR. |
| | |

## *Node Secret:*

### Local RSA Client Node Secret

The node secret is stored in the EPCS EMR application's installation folder on local RSA clients. To clear the node secret a local RSA client, simply delete it.

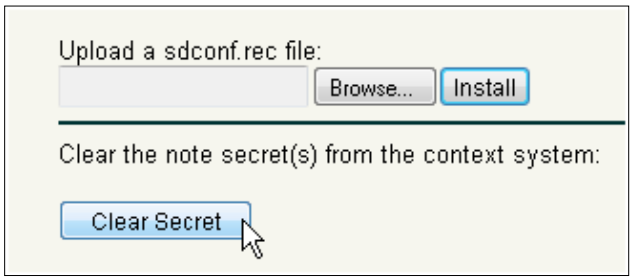
### Vault RSA Client Node Secret

The node secret is stored in the */usr/local/rsa* directory on vault RSA clients. To clear the node secret on vault RSA clients, follow the instructions below:

1. Click the **Appliance** tab on the SSO & Context Management Administrator.

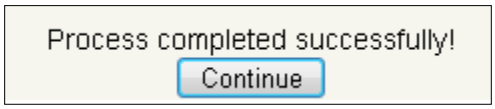

2. Click the **RSA Agent Management** link.

3. Click the **Clear Secret** button to delete the node secret on the vault cluster.




4. The console will display a message that the node secret has been deleted and that the RSA *rsa_agent* service is restarting. You may click the **here** link to observe this process.


5. When the service has finished restarting, click the **Continue** button.




## *sdconf.rec:*

The *sdconf.rec* file is stored in the */usr/local/rsa* directory on vault RSA clients and in the EPCS EMR application's installation folder on local RSA clients.

## *sdopts.rec:*

The sdopts.rec file is stored in the */usr/local/rsa* directory on vault RSA clients and in the EPCS EMR application's installation folder on local RSA clients.

## *sdstatus.12:*

The sdstatus.rec file is stored in the */usr/local/rsa* directory on vault RSA clients and in the EPCS EMR application's installation folder on local RSA clients.

## *Partner Integration Details*

| Partner Integration Details | |
|---|---|
| **RSA SecurID UDP API** | Vault Client –Java API 8.1.3;<br>Local Client – C API 8.1.2 |
| **RSA SecurID TCP API** | N/A |
| **RSA Authentication Agent Type** | NA |
| **RSA SecurID User Specification** | Designated Users |
| **Display RSA Server Info** | No |
| **Perform Test Authentication** | No |
| **Agent Tracing** | No |