



RSA SecurID Ready Implementation Guide

Last Modified: October 20th, 2009

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	SA SSL VPN Appliance
Version & Platform	6.3R4 (build 14121)
Product Description	Juniper Networks SA Series devices lead the market with a complete range of SSL VPN appliances, with the form factors and features tailored to meet the needs companies of all sizes. Juniper SSL VPNs are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks SSL VPN appliances combine the overall category benefit of a lower total cost of ownership compared to traditional solutions, with unique end-to-end security features. Dynamic access privilege management adds granular access control for each user and for each resource.
Product Category	Perimeter Devices (Firewalls, VPNs & ID)





Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, and RADIUS
RSA SecurID Library Version Used	5.3.1
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes (2)
RSA Authentication Agent Host Type for 6.1	Communication Server
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	Yes

* = Mandatory Function when using Native SecurID Protocols

Product Requirements

Partner Product Requirements: Juniper Networks Netscreen SA	
Self-contained appliance	
Firmware Version	6.3R4 (build 14121)



Agent Host Configuration

!> Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.

!> Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.

To facilitate communication between the Juniper Networks SA SSL VPN Appliance 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 the Juniper SA SSL VPN within its database and contains information about communication and encryption. You will also need to configure a RADIUS client.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the Juniper SA SSL VPN as a **Standard Agent**. This setting is used by the RSA Authentication Manager to determine how communication with the Juniper SA SSL VPN will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host, and RADIUS client records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	In Memory
Node Secret	See appendix
sdstatus.12	See appendix
sdopts.rec	Not implemented

Note: Go to the appendix of this document to get detailed information regarding these files.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Juniper SA SSL VPN for RSA SecurID Authentication

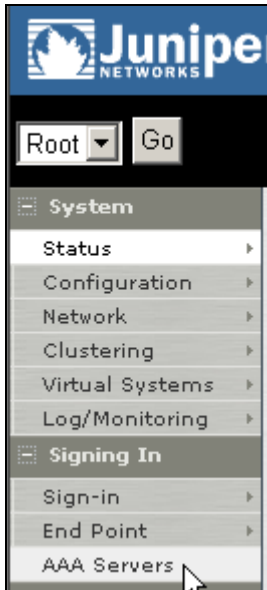
A. Native RSA SecurID Authentication Support

1. Get the `sdconf.rec` file from the RSA Authentication Manager and store it on the machine from which you will manage the Juniper Networks SA SSL VPN.
2. Log into the Juniper Networks SA Administrator Console. The administrator console can be reached via a web browser by entering the following URL <https://hostname/admin>.

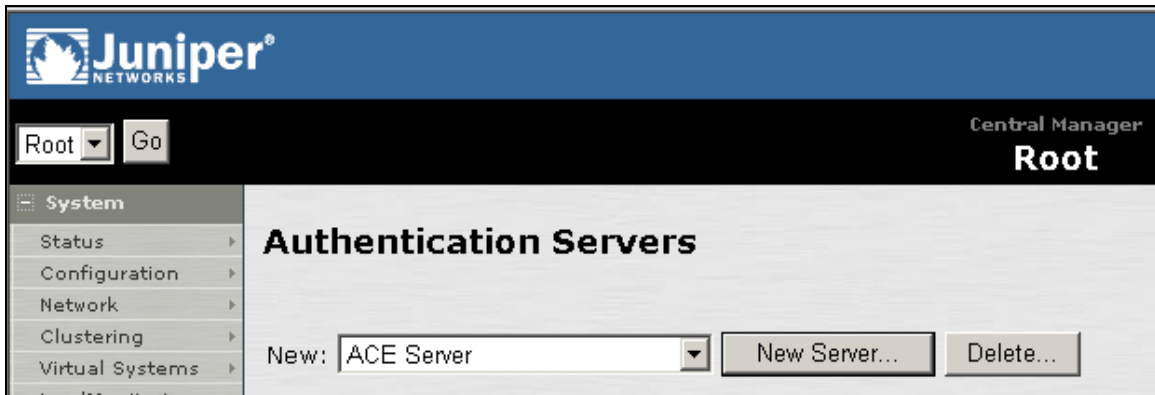




3. In the Administrator Console, choose **Signing In > AAA Servers**.



4. From the drop-down list, choose **ACE Server**.





5. Click **New Server**. The configuration page for Authentication Manger “ACE Server” appears.
6. Fill in the appropriate information:

Juniper® NETWORKS

Root Go Central Manager
Root

System
Status
Configuration
Network
Clustering
Virtual Systems
Log/Monitoring

Signing In
Sign-in
End Point
AAA Servers

Administrators
Authentication
Delegation

Users
Authentication
Roles
New User

Resource Policies

Auth Servers >
New ACE Server

Name: Label to reference this server.

ACE Port:

Configuration File

Current config file:
Imported on:

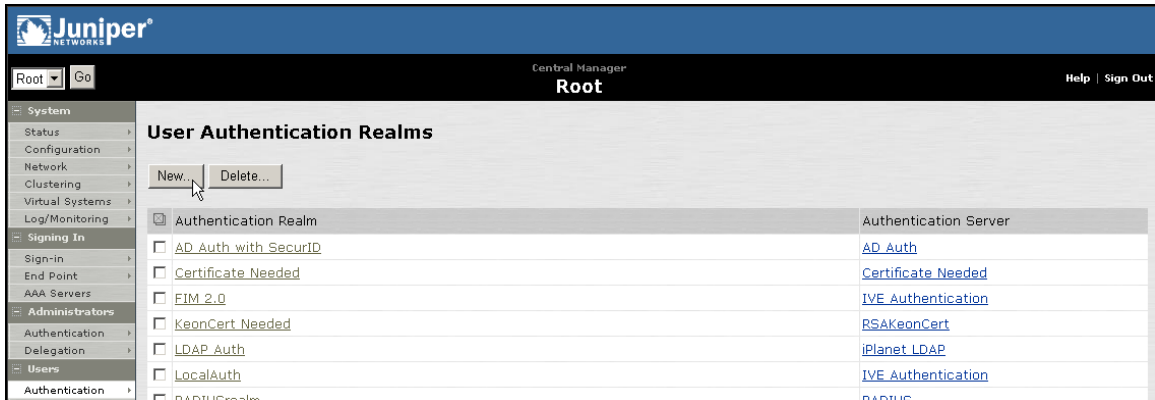
Import new config file:

Save Changes ?

- **Name:** Enter a name to identify the ACE Server instance. Because users may not readily understand the concept of signing into an authentication server, it is recommended that you use a familiar name that conveys a group to which the user belongs, such as “corporate” or “bostonoffice”.
 - **Port:** Change if needed but default is 5500.
 - **Import new config file:** Click the Browse button to browse to the RSA Authentication Manger configuration file (sdconf.rec) saved in Step 1 above.
7. Click **Save Changes**.
 8. Go to **Users – Roles** and create a role for your RSA SecurID authentication users based on your policies.

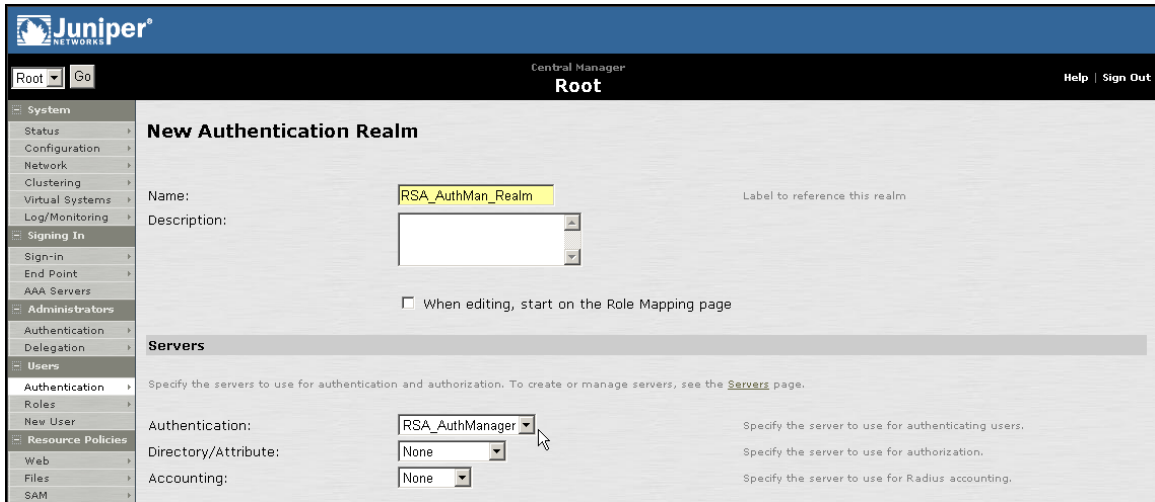


9. Go to **Users > Authentication**.



10. Click **New**.

11. Enter the appropriate information for this Authentication Realm.



- **Name:** Give the Realm a Name.
- **Authentication Server:** Select the RSA Authentication Manager definition defined in step 6 above.



12. Click **Save Changes**.

Juniper NETWORKS
Central Manager
Root
Help | Sign Out

Created realm successfully. Add role mapping rules here.

User Authentication Realms >
RSA_AuthMan_Realm

General Authentication Policy Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete ↑ ↓ Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	▶ When users meet these conditions			

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

13. Click **New Rule** and create a rule.

New Rule... Duplicate Delete ↑ ↓ Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	▶ When users meet these conditions			
<input type="checkbox"/>	1. <u>username</u> is "***"	→ <u>Users</u>		

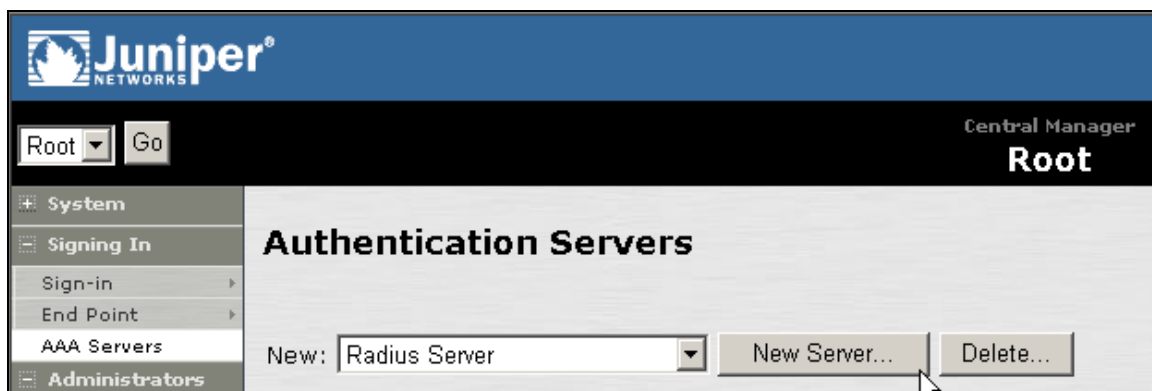
14. Click the **Save Changes** button to save your configuration.

After successfully configuring the server, RSA SecurID authentication is enabled on the Juniper Networks SA SSL VPN. The server doesn't have to be restarted. Users who are configured to use RSA SecurID authentication can sign in with their username and their RSA SecurID PASSCODE.

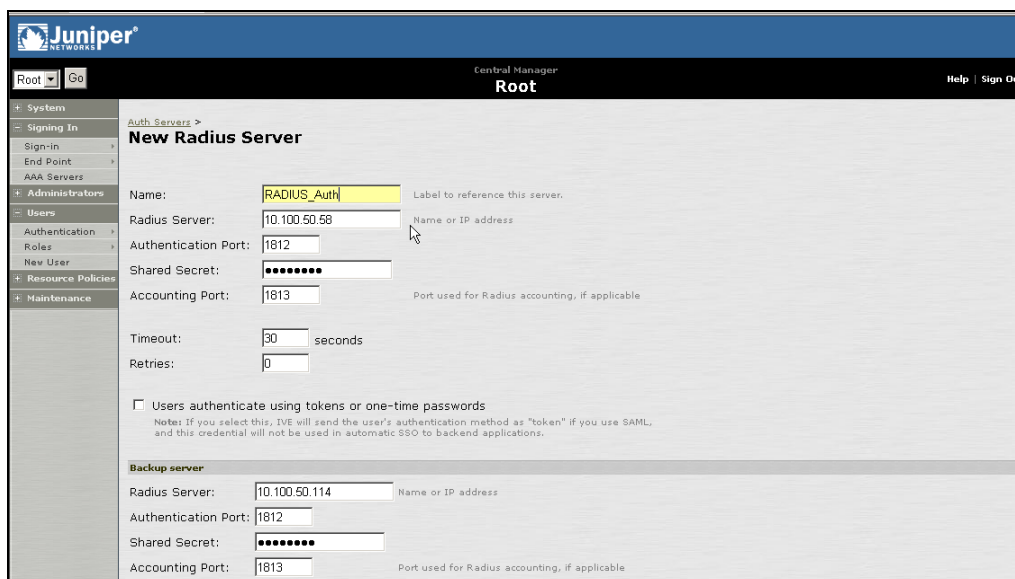


B. RADIUS Authentication Support

1. Log into the Juniper Networks SA Administrator Console. The administrator console can be reached via a web browser by entering the following URL `https://hostname/admin`.
2. From the main menu, choose **Signing In > AAA Servers**.



3. Select **RADIUS Server** from the drop-down menu and click **New Server**.
4. Enter the RADIUS Server IP address, port number, and shared secret.



5. Click **Save changes** to save the configuration.
6. Go to **Users – Roles** and create a role for your RSA SecurID Authenticated users based on your policies.



7. Go to **Users – Authentication**.

8. Click **New**.

9. Enter the appropriate information for this Authentication Realm.

- **Name:** Give the Realm a Name.

- **Authentication Server:** Select the RADIUS definition defined in step 5 above.

10. Click **Save Changes**.



11. Click **New Rule** and create a rule.

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is ***	→ Users		

12. Click the **Save Changes** button to save your configuration.

After successfully configuring the server, RADIUS authentication is enabled. Users who are configured to use RADIUS authentication can sign in with their username and PASSCODE.

Authentication Examples

The user will see the following user interface when authenticating against the RSA Authentication Manager Server.

- **Standard sign-in screen.** To access sign-in screen, enter the Juniper machine's URL in a browser.

Juniper NETWORKS

Welcome to the
Instant Virtual Extranet

Username Please sign in to begin your secure session.


Password

Realm

- The user enters their username and RSA SecurID PASSCODE and selects the RSA Authentication Manager Server from the drop-down menu.
 - On success, the user is successfully logged in.
 - On failure, the user is returned to the sign-in page



- **New PIN screens.**



Welcome to the
Instant Virtual Extranet

New PIN Required


You must create a new Personal Identification Number (PIN) before you can sign in. Your PIN should be 4 to 8 characters long.

New PIN:

Confirm PIN:

- Be sure to remember your PIN, because you need it to sign in.
- If you prefer, the system can [generate a PIN](#) for you. Generated PINs are typically more secure.
- If you decide not to create a new PIN now, click Cancel.

- **User created PIN.**



Welcome to the
Instant Virtual Extranet

New PIN Required

You must create a new Personal Identification Number (PIN) before you can sign in. Your PIN should be 4 to 8 characters long.


New PIN:

Confirm PIN:

- Be sure to remember your PIN, because you need it to sign in.
- If you decide not to create a new PIN now, click Cancel.



- **Pin Accepted.**




Welcome to the
Instant Virtual Extranet

Your new PIN has been saved. Be sure to remember your PIN, because you need it each time you sign in.

Username Please sign in to begin your secure session.
Password
Realm


- **System Generated PIN.**



Welcome to the
Instant Virtual Extranet

Generate New PIN?

The system will now generate a PIN for you. Make sure that no one else can see your screen and then click Generate PIN to continue.




Welcome to the
Instant Virtual Extranet

New PIN Generated

Your new PIN is **rvx9**. Be sure to remember it, because you need your PIN each time you sign in. When you have memorized it, click Continue to return to the sign-in page.

- Next TOKENCODE Screen.



The screenshot shows the Juniper Networks logo at the top left. Below it, the text reads "Welcome to the Instant Virtual Extranet". A yellow warning box contains the text: "Token Resync Required. Please enter an additional token code to continue. The server requires that you enter an additional token code to verify that your credentials are valid. To continue, wait for the token code to change and then enter the new code in the SecurID Token Code field." Below the warning box is a text input field labeled "SecurID Token Code:" with "Enter" and "Cancel" buttons.

Integration with the RSA Software Token/SD800

The Juniper SA Series SSL VPN allows administrators to customize login pages for use with the RSA Software Token and SD800. When the end-user browses to the URL of the SoftID custom sign-in page, the page prompts the user to enter a PIN by way of the SecurID application on their local machine. If the application accepts the PIN, the end-user is logged in.

For detailed information about enabling custom sign-in pages, please see the Juniper SA Admin Guide.

SA Series SSL VPN Configuration

1. Create Sign-in page

To configure the SoftID custom sign-in page, first download the Samples.zip and SoftID.zip template files. These files are downloadable from the SA IVE. Go to Authentication > Signing In > Sign-in Pages > Upload Custom Pages.

Sample Templates Files

The following sample templates may be useful in producing your own customized sign-in page templates. Click to download the sample files, edit them to fit your needs, and then upload them.

- [Sample](#)
This is a basic set of templates that works for most cases.
- [Softid](#)
This is a set of templates for ACE Authentication.
- [Kiosk Example](#)
This is an example which demonstrates how to protect against hardware keystroke loggers.
- [Meeting](#)
This is a set of pages for joining a meeting.

Unzip **Samples.zip** to a directory first, and then unzip the SoftID.zip file to the same location, overwriting any duplicates. Once you have customized the files to your liking, zip the entire set of files and upload them to the device.



Signing In >
Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages that may appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-In Pages

Name:
Label to reference the custom sign-in pages.

Page Type: Access

Templates File:
Zip file containing the custom templates and assets.
Current Template File:
 Size 70983 bytes Uploaded on Fri Apr 7 09:35:27 2006

Save Changes?

skip validation checks during upload

2. Create Sign-in policy

Signing In >
***/softid/**

User type: Users Administrators

Sign-in URL: Format: <host>/<path> Use * as wildcard in the beginning of the host name.

Description:

Sign-in page:
To create or manage pages, see [Sign-In pages](#).

Meeting URL:

Authentication realm

Specify how to select an authentication realm when signing in.

User types the realm name
The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [User Authentication page](#) or the [Administrator Authentication page](#).

Available realms:

Selected realms:

Save changes?

! Important: It is important that you enforce the RSA Authentication configured Authentication Realm as shown in the screenshot.

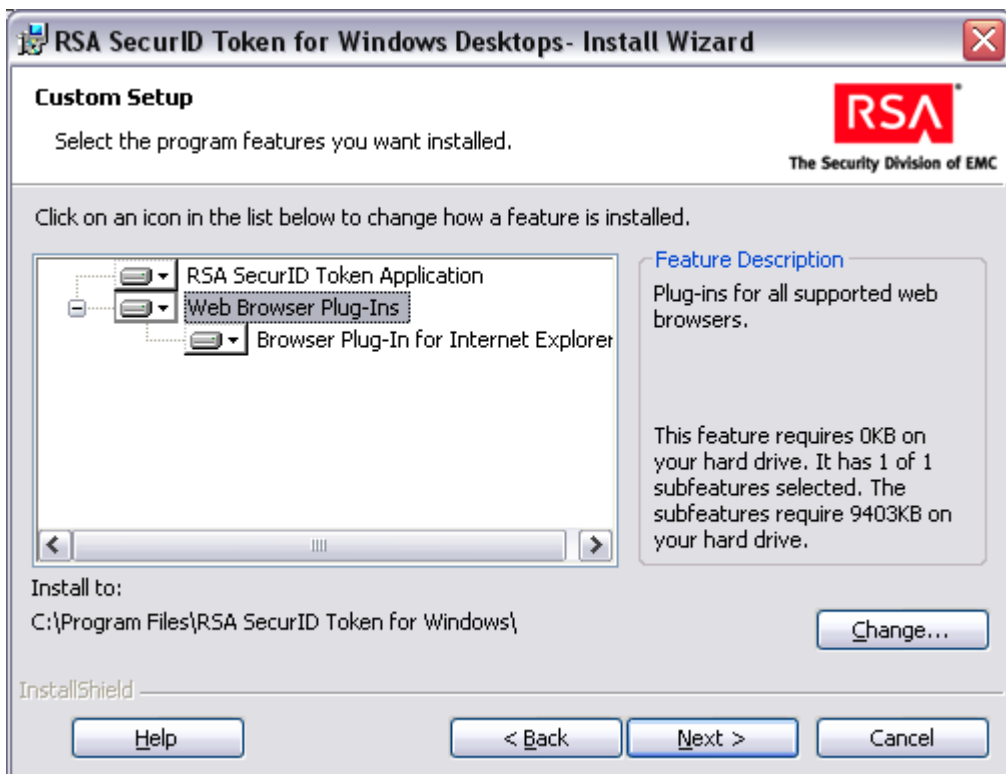


Client Configuration – Software Token

1. Install the RSA Software Token for Windows Desktops 4.0.

 **Note:** RSA Software Token needs to be installed on the client PC prior to attempting to connect to the “SoftID” URL.

2. Ensure that the Web Browser Plug-In for Internet Explorer has been installed. This is only available via the “Custom Setup” option.




 **Note:** Ensure that the “Browser Plug-In for Internet Explorer is enabled as an installed feature as outlined in the screenshot above.



Authentication Example

When a user attempts to access the SoftID sign-in page, he or she will see the following RSA SecurID authentication dialog:



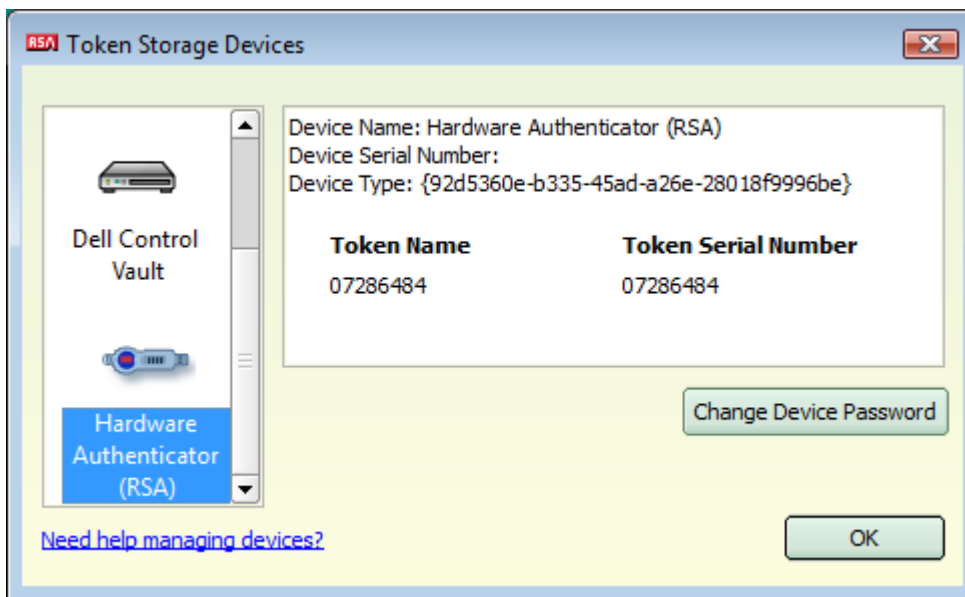
 **Note:** New PIN mode. The 'Enter PIN' field cannot be left blank. Therefore multiple '0's' need to be entered to satisfy this criteria.



Client Configuration – SID800 Token

The steps to configure the SID800 Token for use with the Juniper SA Series SSL VPN are as follows:

1. Install the appropriate version of the RSA Smart Card Middleware.
2. Ensure that the RSA Software Token for Windows shows the SID800 as a valid **Token Storage Device**:



3. Ensure that you have installed the Web Browser Plug-In for Internet Explorer as described above.

 **Note:** Authentication when in next tokencode mode can take up to two minutes due to the fact that a second code is required to successfully authenticate.

4. Users will then be prompted for their credentials via the RSA SecurID authentication dialog as demonstrated above. The end user should select the serial number for the SID800 token from the **Select Token:** dialog if there is more than one token installed.

Certification Checklist For RSA Authentication Manager 7.1

Date Tested: October 30, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 SP1
RSA RADIUS	7.1	Windows 2003 SP1
RSA Software Token for Windows	4.0	Windows Vista Enterprise SP1
Juniper SA SSL VPN Appliance	SA-2500	6.3R4 (build 14121)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
RSA SecurID 800 Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>

JEC

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

*See Known Issues Section for more information



Known Issues

1. **System Generated and User Selectable PIN:** System Generated and User Selectable PINs (Authentication Manager 6.1 only) do not work via RADIUS authentication.
2. **Next Tokencode mode with SID800:** Authentication when in next tokencode mode can take up to two minutes due to the fact that a second code is required to successfully authenticate. See the RSA Middleware readme file for more information on this condition.

Appendix

Managing the Node Secret

To delete the Node Secret: In the Administrator Console, choose **Signing In – AAA Servers**. Then under the **Authentication/Authorization Servers** heading select the name for the RSA Authentication Manger Server. In this guide it was called RSA_AuthManager. Now check the box next to **this node** and click **Delete**

