



## RSA SecurID Ready Implementation Guide

Last Modified: March 14, 2008

### Partner Information

---

Product Information	
Partner Name	Nortel Networks
Web Site	<a href="http://www.nortelnetworks.com">www.nortelnetworks.com</a>
Product Name	VPN Gateway 3050
Version & Platform	7.0.1.0
Product Description	The Nortel Networks VPN Gateway 3050 is a remote access security solution that extends the reach of enterprise applications and resources to remote users. The gateway performs on-the-fly content transformation to instantly convert most intranet resources into externally-viewable, secure HTML pages and employs an advanced network address and port translation (NAPT) utility to build SSL-secured VPN tunnels for client/server communications
Product Category	Perimeter Defense (VPN, Firewalls & Intrusion Detection)





## Solution Summary

The Nortel Networks VPN Gateway 3050 is a remote access security solution that extends the reach of enterprise applications and resources to remote employees, partners, and customers. By using the native capability of widely deployed Web browsers, the SSL VPN Gateway offers a convenient clientless alternative for securely provisioning resources for remote users, without the need to install and manage client tunneling software on their PCs.

Due to the clientless nature of this solution, Strong two factor authentication is essential to ensure the identity of users connecting to your Enterprise from the internet. For this reason, Nortel Networks VPN Gateway 3050 provides support for the RSA Authentication Manager as a method of strong authentication for users using RSA SecurID Authentication.

For enterprises maintaining IPsec VPN environments, the Nortel VPN Gateway 3050 provides a new level of deployment flexibility and end-user support by incorporating IPsec VPN client termination to remove the network administrator's challenge of managing multiple devices to deliver both types of remote access service.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS
List Library Version Used	5.0.3
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes Support for 2 Secondary Serves
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users,
RSA SecurID Protection of Administrative Users	Yes via RADIUS. See Known issues.
RSA Software Token and RSA SecurID 800 Automation	No





## Product Requirements

---

Partner Product Requirements: Nortel VPN Gateway 3050	
Firmware Version	7.0.1.0

Hardware Platform	
Platform	Required Patches
VPN 3050, ASA 310, ASA 410, ASA 310 FIPS	N/A

Additional Software Requirements	
Application	Additional Patches
Internet Explorer	5.0, 5.5 and 6.0

## RSA SecurID files

---

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

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

---



## 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 Nortel VPN Gateway and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and the RADIUS server database if using RADIUS. The Agent Host record identifies the Nortel VPN Gateway within its database and contains information about communication and encryption.

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 Nortel VPN Gateway as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Nortel VPN Gateway 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 records.



# 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.

## ***Nortel VPN Gateway 3050 Agent configuration***

Administrative tasks can be performed in the Command Line Interface (CLI) as well as the Web Administration GUI. All configuration steps and screenshots in this guide will refer to GUI administration. Please refer to Nortel Administrative documentation for more complete details on CLI and GUI Administration tasks.

## **RSA SecurID Authentication Configuration Overview**

1. Create a User Group
2. Configure the RSA Server record
3. Configuring the RSA SecurID Authentication Servers

## **RADIUS Authentication Configuration Overview**

1. Create a User Group
2. Configuring the RADIUS Authentication Servers



## Creating and Configuring a RSA SecurID or RADIUS User Group

1. From the admin console, expand **VPN Gateways** and click **Add** to add a VPN Gateway.
2. Click **Create VPN**.
3. Now click on the VPN Gateway you just created and click on **Groups**.
4. Click on the button **Add New Group**.
5. Fill out the form with the desired group name, user type and description.
6. Click **Update** and then **Apply** to add the new group to the configuration.

**Groups**

Lets you define the user groups that reside on the VPN Gateway. When a user logs in to the VPN (via the Portal, the SSL VPN client or the IPsec VPN client), the system tries to determine the user's group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's credentials in the authentication mechanism by which the user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database).. [?](#)

Default Group: 3 RADIUS Authentication

Anonymous Group: <unselected>

[Update](#)

[Add](#) [Edit](#) [Delete](#) [Copy](#) [Paste](#) [Refresh](#)

<input type="checkbox"/>	ID	Name	User Type	Comment
<input type="checkbox"/>	1	Password Users	advanced	Users authenticated by static passwords.
<input type="checkbox"/>	2	<a href="#">SecurID Users</a>	advanced	Users authenticated by RSA SecurID.
<input type="checkbox"/>	3	<a href="#">RADIUS Authentication</a>	advanced	Users authenticated by RSA RADIUS

7. From the **Groups** menu on the administration console, click on the group name.
8. Select the **Access List** tab.
9. Create an appropriate Access list based on your organizations configuration. In the example below you will see we have created a generic rule allowing all access for authenticated RSA SecurID or RADIUS users.

General **Access Lists** Linksets TG IPsec VPN Admin Net Direct Mobility Extended Profiles

[Add](#) [Edit](#) [Delete](#)

<input type="checkbox"/>	ID	Network	Service	Application	Allow	Comment	Reorder
<input type="checkbox"/>	1	*	*	*	accept		

10. Click **Update** to apply the Access rules.
11. Configure the user group for any necessary links or VPN Settings as required.
12. Click **Apply** to add the new information to the IOS configuration.

**Apply Pending Configuration Changes**

Apply Results

**Apply Succeeded**

[Back](#)




## Configure the RSA Server record

1. Open the Management Interface (MIP) of the Nortel VPN Gateway using a web browser. Authenticate with administrative user account and select the **Config** tab.
2. From the SSL-VPN admin menu select **Administration > RSA Servers** item.
3. Click the **Add** button and complete the form.
4. Click **Apply** to commit changes to the IOS configuration.

### Add New RSA Server

Id:


RSA Server IP/Hostname:

 **Note: You must Update and Apply the RSA Server Group entry before you import the sdconf.rec file**

5. To import your sdconf.rec file you will return to the **RSA Servers** menu and modify the entry for the sdconf.rec file you will be adding.

### Import sdconf.rec file

File:


 **Warning: The created RSA servers should be Applied before importing the sdconf.rec file**

6. Click **import** to upload the sdconf.rec file and then click **Apply** changes to the IOS configuration.

## Configuring the RSA SecurID Authentication Servers

1. From the admin console, select **VPN Gateways > Authentication**.
2. Click **Add**.
3. Enter information for the Authentication Server such as Name and Display Name. The Authentication Mechanism will be **RSA**. Then click **update** to complete additional RSA SecurID authentication options.
4. Select the Settings tab and fill in the appropriate information.
  - **RSA Server IP.Hostname:** Select the RSA Authentication Manger server you created.
  - **Group For RSA Authenticated Users:** Select The Group name you created for the.

### RSA Server Settings

Allows you to configure some of the RSA authentication method specific settings. 

General **Settings** Advanced

RSA Server IP/Hostname:

Group For RSA Authenticated Users:

5. Click **Update** and then **Apply** to add the new information to the IOS configuration.



## Configuring the RADIUS Authentication Servers

- From the admin console, select **VPN Gateways > Authentication**.
- Click **Add**.
- Enter information for the Authentication Server such as Name and Display Name. The Authentication Mechanism will be **RADIUS**. Then click **update** to complete additional RADIUS authentication options.
- Select the Servers tab and click **Add**.

### RADIUS Servers

#### Add New RADIUS Server

VPN: 1  
Auth Id: 3  
IP Address:  (format: 10.10.1.75)  
Port:   
Shared Secret:   
Shared Secret (again):

- Enter the appropriate information for you server and click **Update**.

 **Note:** You can add a maximum of three RSA RADIUS servers to this authentication server list.

General Settings Session Network Attributes <b>Servers</b> Macros Advanced				
<input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="checkbox"/>	ID	IP Address	Port	Reorder
<input type="checkbox"/>	1	<a href="#">10.100.50.37</a>	1812	↓
<input type="checkbox"/>	2	<a href="#">10.100.50.36</a>	1812	↓ ↑
<input type="checkbox"/>	3	<a href="#">10.100.50.35</a>	1812	↑

- Click **Apply** to add the new information to the IOS configuration.





## Configuring RADIUS Authentication Servers for Administrative Access

1. From the admin console, select **Administration > RADIUS**.
2. Click **Add**.
3. Enter information for the RADIUS Authentication Server.

### RADIUS

#### Add RADIUS Authentication Server

IP Address:	<input type="text" value="10.100.50.37"/>
Port:	<input type="text" value="1812"/>
Shared Secret:	<input type="password" value="••••••••"/>
Shared Secret (again):	<input type="password" value="••••••••"/>

4. Click **update**.
5. Enable authentication by selecting **enabled** for RADIUS Authentication Status.

Managing: SSL-7.0.1.0 on 3050  
Administration » RADIUS Authentication

Wed, Sep 26, 2007 12:14:15 PM Logged as admin

### RADIUS

RADIUS menu is used to configure RADIUS authentication of system users. Authentication applies to both CLI and WebUI users.

**RADIUS Servers** | Group Attributes

RADIUS Authentication Status:	<input type="text" value="enabled"/>	Enable/Disable RADIUS authentication of system users (disabled by default).
RADIUS Server Timeout:	<input type="text" value="10"/>	(seconds)
Use Local Password As Fallback:	<input type="text" value="yes"/>	

#### RADIUS Servers

<input type="checkbox"/>	ID	IP Address	Port
<input type="checkbox"/>	1	10.100.50.37	1812

6. Click update then **Apply**.

**NEW-PIN mode does not work via the admin console. See the Known issues section of this guide for more information.**




## Testing the configuration

1. Open a web browser and point to the portal address.
2. For user credentials enter a SecurID username and Passcode.
3. From the **Login Service** list select your RSA SecurID or RSA RADIUS challenge group.
4. Click **Login** to authenticate and enter the Portal Server.

A screenshot of a web browser displaying the Nortel Networks login portal. The page features the Nortel Networks logo in the top left corner. Below the logo is a blue header bar. In the center, there is a white login form titled "Login". The form contains the following elements: a welcome message "Welcome to the RSA Security Partner Lab SSL VPN 3050...", a login status indicator "Login Status: not logged in" in red text, a "Username:" label followed by a text input field, a "Password:" label followed by a text input field, a "Login Service:" label followed by a dropdown menu currently set to "default", and a "Login" button. The background of the page is a light blue gradient.

---

 **Note:** The user name does not need to exist on the VPN Gateway 3050 in order to be authenticated. The VPN Gateway 3050 will pass off authentication to the RSA Authentication Manager as a trusted authentication source.

---

# Certification Checklist

Date Tested: September 26, 2007

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003 Server
RSA RADIUS Server	6.1	Windows 2003 Server
VPN Gateway 3050	7.0.1.0	IOS Router

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<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"/>
<b>PASSCODE</b>			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Credential Functionality</b>			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

SWA / BSD

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

# Certification Checklist For RSA Authentication Manager 7.x

Date Tested: March 14, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003
RSA RADIUS Server	7.1	Windows 2003
VPN Gateway 3050	7.0.1.0	IOS Router

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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"/>
<b>Passcode</b>			
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"/>
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
<b>Load Balancing / Reliability Testing</b>			
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"/>
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
PIN Expiration	<input type="checkbox"/> N/A	PIN Expiration	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
PIN Expiration	<input type="checkbox"/> N/A	PIN Expiration	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

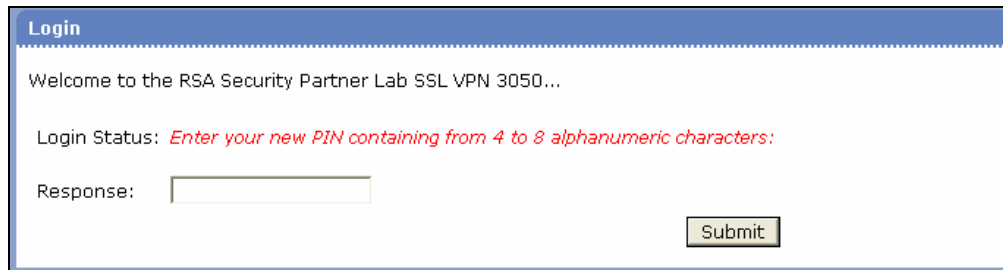
SWA

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

## Known Issues

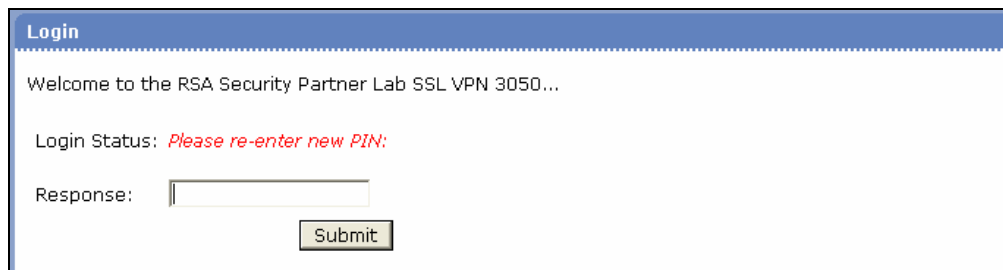
**PIN Rejection:** When a PIN is rejected by the Authentication Manager Server the user is questioned by the client to try a different PIN but the program flow is not intuitive.

1. The user first authenticates using either Token or Password. The user is next prompted to create a new PIN.



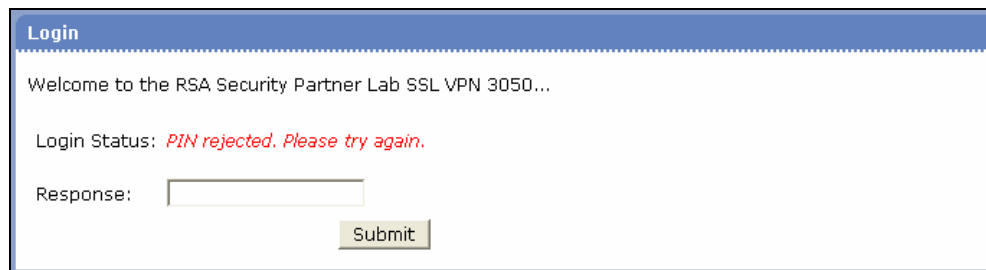
The screenshot shows a login window titled "Login" with a blue header. Below the header, it says "Welcome to the RSA Security Partner Lab SSL VPN 3050...". The "Login Status" is "Enter your new PIN containing from 4 to 8 alphanumeric characters:". There is a "Response:" label followed by an empty text input field and a "Submit" button.

2. The user must re-enter the new PIN to validate input from the previous step.



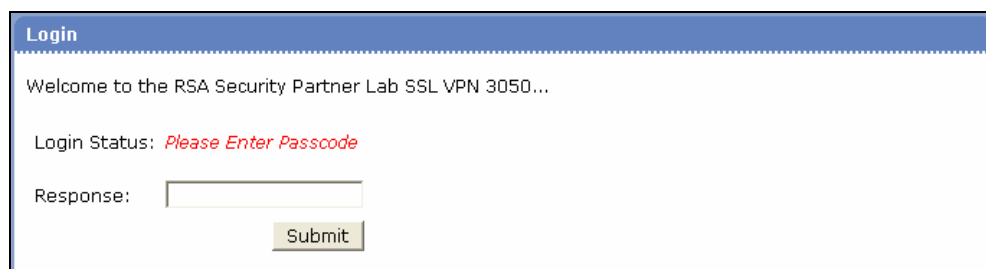
The screenshot shows the same login window. The "Login Status" is "Please re-enter new PIN:". There is a "Response:" label followed by an empty text input field and a "Submit" button.

3. If rejected, the client displays the question to the user with an empty text box for input.



The screenshot shows the same login window. The "Login Status" is "PIN rejected. Please try again.". There is a "Response:" label followed by an empty text input field and a "Submit" button.

4. The client will accept any input by the user and then prompt for a new Passcode to restart the authentication process.



The screenshot shows the same login window. The "Login Status" is "Please Enter Passcode". There is a "Response:" label followed by an empty text input field and a "Submit" button.

5. The user then inputs a valid Passcode.



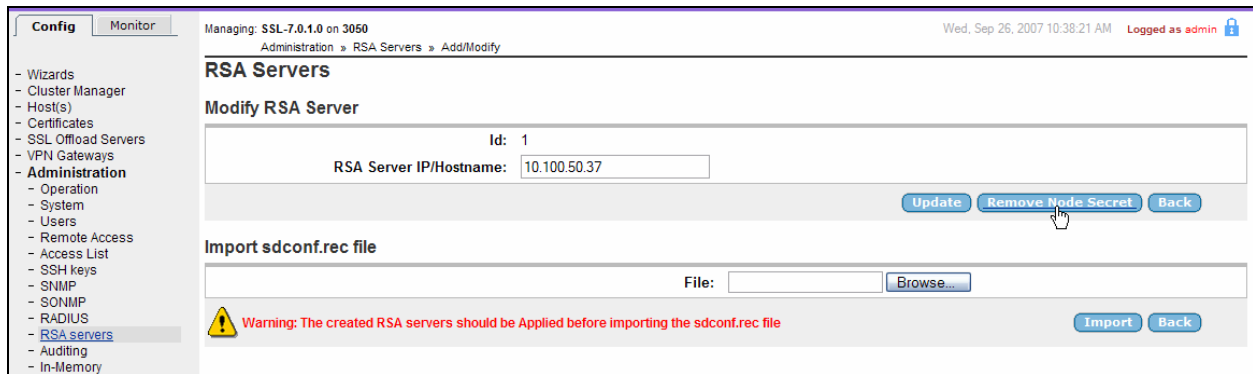
### **Administration Logon.**

NEW-PIN mode does not work via the admin console. The user is prompted to create or accept a PIN but the PIN never gets sent to the server and the user gets redirected to a blank web page.

# Appendix

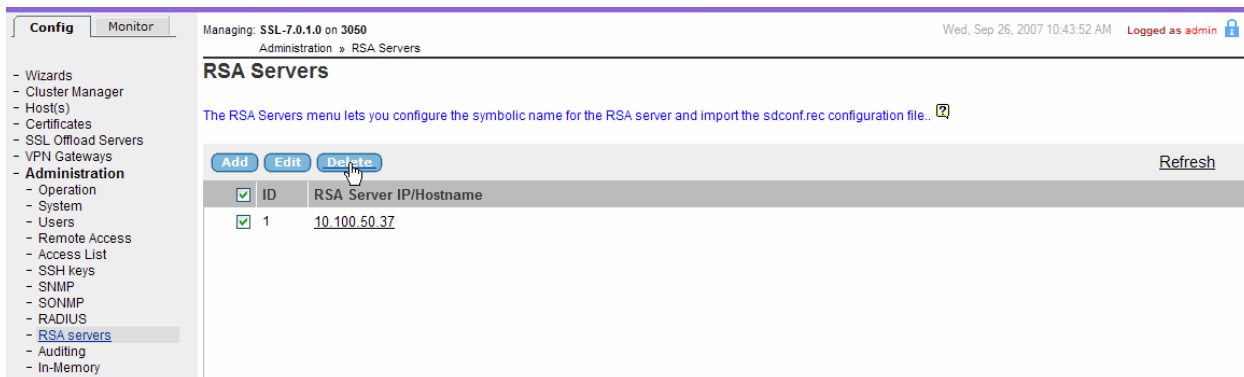
## Delete Node Secret

1. Navigate to **Config > Administration > RSA Servers** and click on the link for the RSA Authentication Server Label you created.
2. Click the button labeled **Remove Node Secret**.



## Remove sdconf.rec and sdstatus.12

1. Navigate to **Config > Administration > RSA Servers**.
2. Check the box for the RSA Authentication Server Label you created.
3. Click delete.



4. You now need to add a new record for an RSA Authentication Managers for authentication.