Avaya
VPN Gateway 3000 Series

RSA SecurID Ready Implementation Guide

Last Modified: May 30th, 2014

Partner Information

Product Information	
Partner Name	Avaya
Web Site	www.avaya.com
Product Name	VPN Gateway 3000 Series
Version & Platform	9.1 Virtual Appliance
Product Description	The Nortel VPN Gateway portfolio is an SSL VPN remote access security solution that extends the reach of enterprise applications to remote/mobile employees, contractors, partners and customers. The VPN Gateway provides flexible access options including browser based, on demand and installed SSL clients, and IPsec client support. Its comprehensive set of security features protects enterprises from malware attacks and prevents loss or theft of confidential information.

Solution Summary

Avaya's VPN Gateway 3000 series integrates with RSA SecurID to provide strong two-factor authentication for users accessing corporate resources from remote networks. The VPN Gateway can be configured to communicate with RSA Authentication Manager via both RADIUS and the RSA native SecurID authentication protocols. SecurID Authentication can be configured for users that attempt to access secured resources via the Avaya VPN Client or the clientless SSL VPN portal. Avaya VPN client can be configured to use an installed RSA Software Token or USB-attached hardware authenticator so the user only needs to enter the SecurID PIN when authenticating. The VPN client then retrieves the tokencode from the installed authenticator.

RSA Authentication Manager supported features	
Avaya VPN Gateway 3000 Series	
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	Yes
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	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	Yes
RSA SecurID SD800 Token Automation	Yes
RSA SecurID Protection of Administrative Interface	Yes*

**RADIUS only—see Known Issues section of this document*

Agent Host Configuration

To facilitate communication between the Avaya VPN Gateway 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 Avaya VPN Gateway and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Avaya VPN Gateway will occur.

If Avaya VPN Gateway will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

> **Note: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Avaya VPN Gateway with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

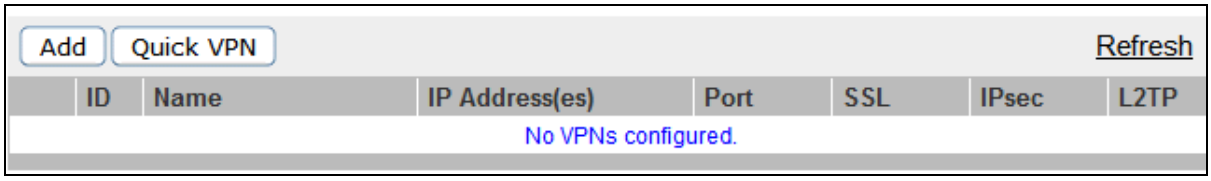
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Avaya VPN Gateway components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

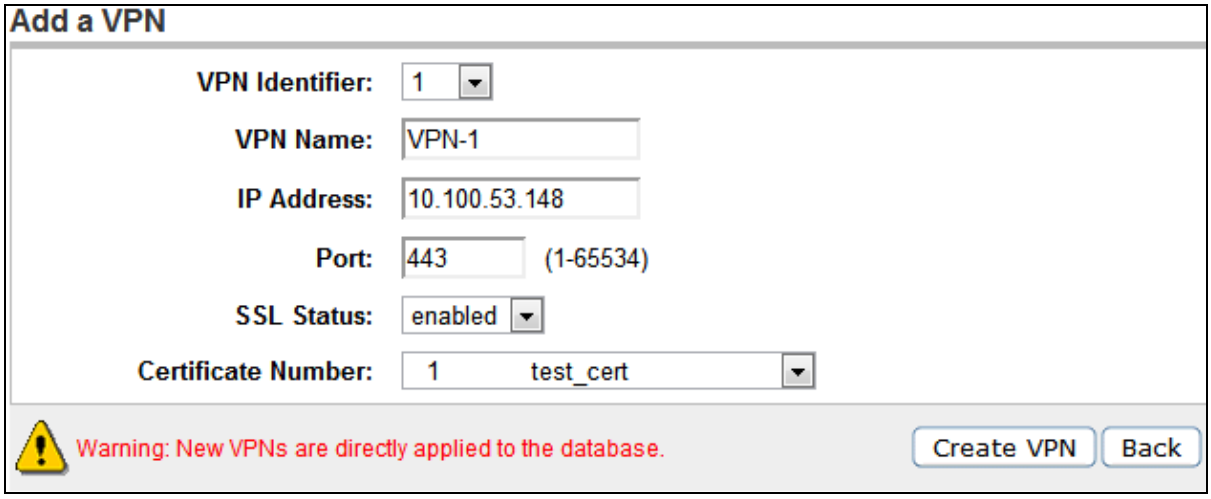
Configure the VPN Gateway for SSL VPN

Log in to the browser-based management interface and complete the following instructions to configure a VPN Gateway that accepts SSL VPN connections.

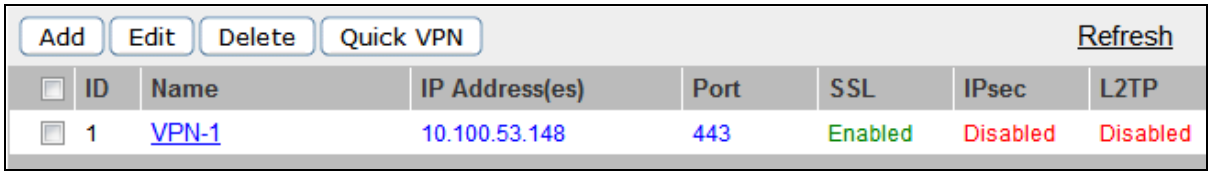
1. In the left navigation pane, click the **Config** tab, then **VPN Gateways**. Click **Add** to create a new VPN Gateway.



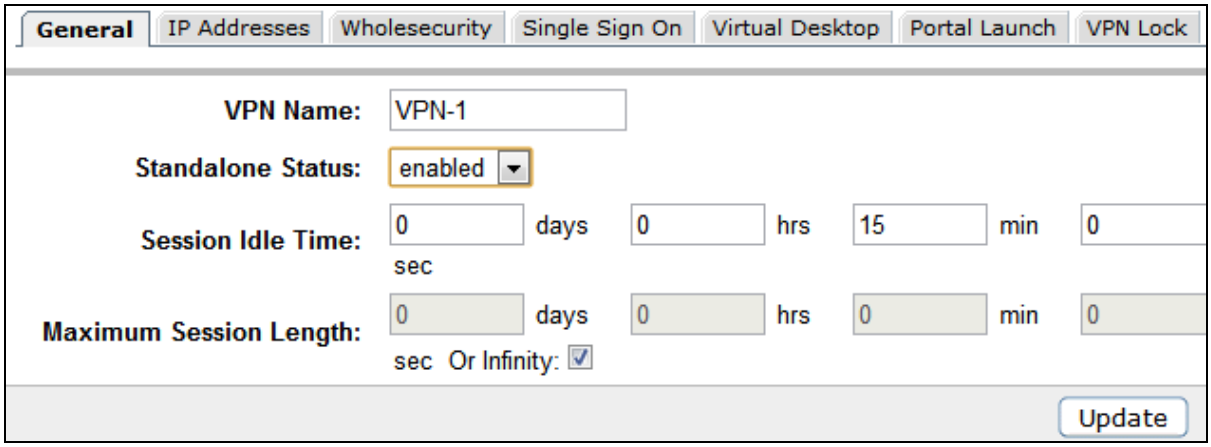
2. Enter the **VPN Name**, **IP Address**, select which **Certificate Number** to use and click **Create VPN**.



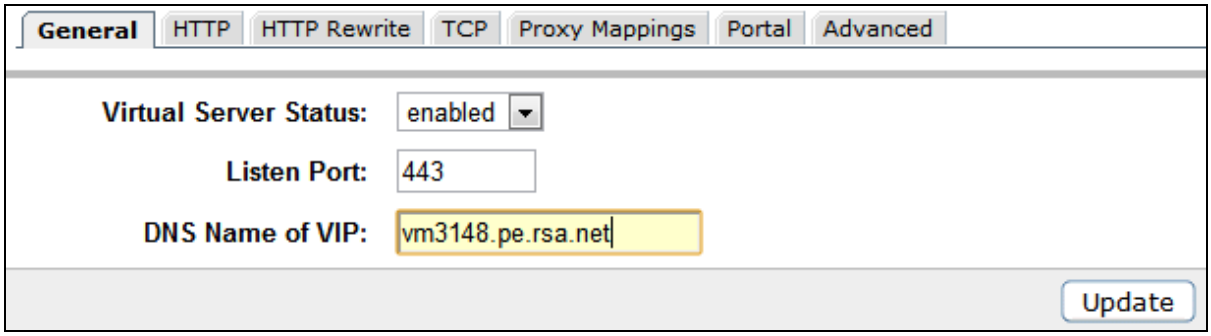
3. Click on the newly created VPN Gateway to edit it.



4. Click the **General** settings link in the VPN Summary. Select **enabled** from the **Standalone Status** dropdown list and click **Update**.



5. Back on the VPN Summary page, click the **SSL** settings link. Enter the **DNS Name of VIP** and click **Update**.



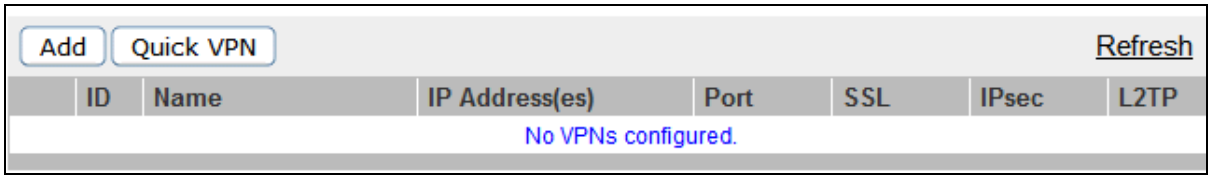
6. Click **Apply** in the browser-based management interface header to apply the change.

The VPN Gateway is now configured to accept SSL VPN connections. Refer to the instructions on enabling SecurID authentication via native SecurID and RADIUS protocols later in this document.

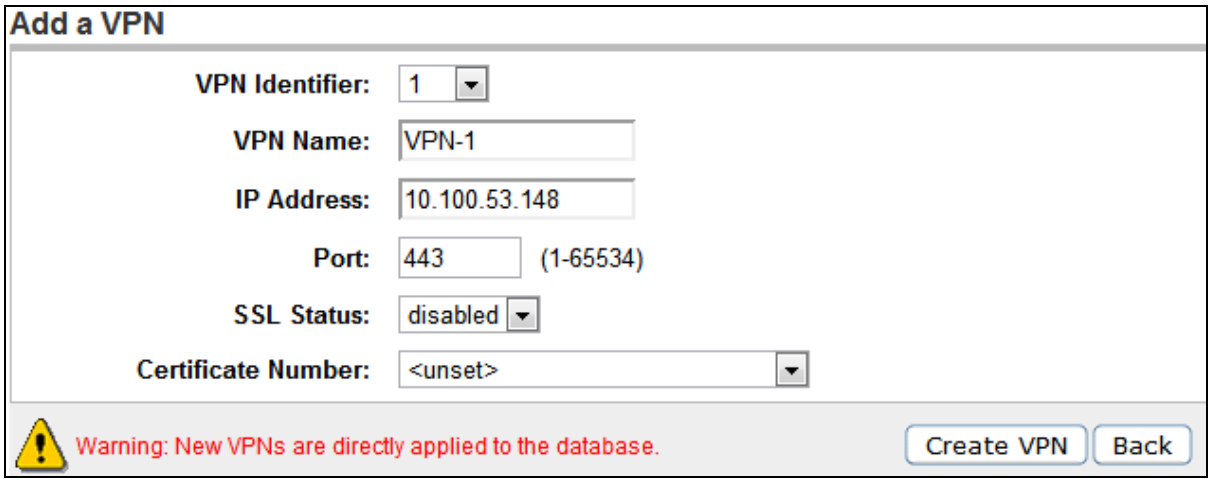
Configure the VPN Gateway for IPSec VPN

Log in to the browser-based management interface and complete the following instructions to configure a VPN Gateway that accepts IPSec VPN connections.

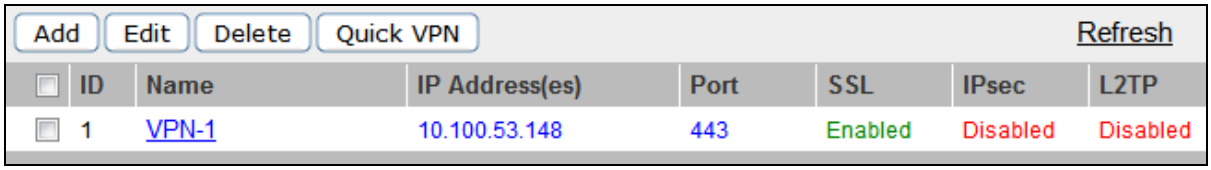
1. In the left navigation pane, click the **Config** tab, and then click **VPN Gateways**. Click **Add** to create a new Gateway.



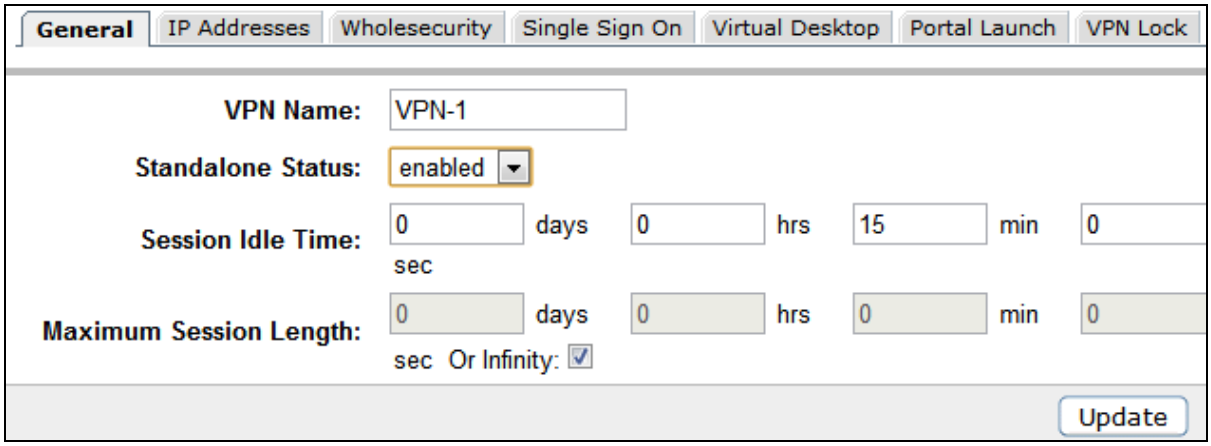
2. Enter the **VPN Name** and **IP address**. Click **Create VPN**.



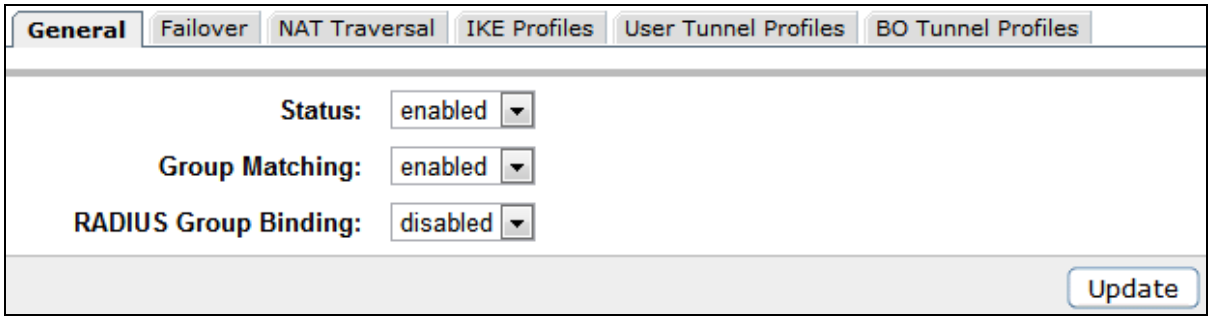
3. Click on the newly created VPN Gateway to edit it.



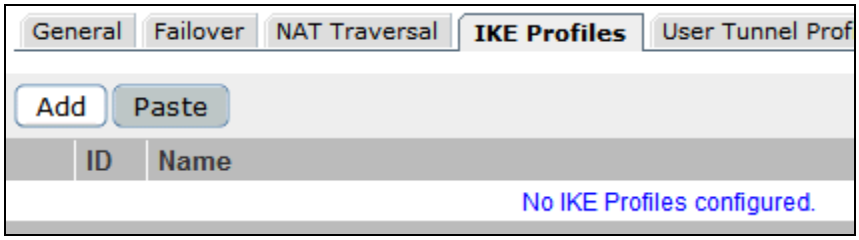
4. Click the **General** settings link in the VPN Summary. Select **enabled** from the **Standalone Status** dropdown list and click **Update**.



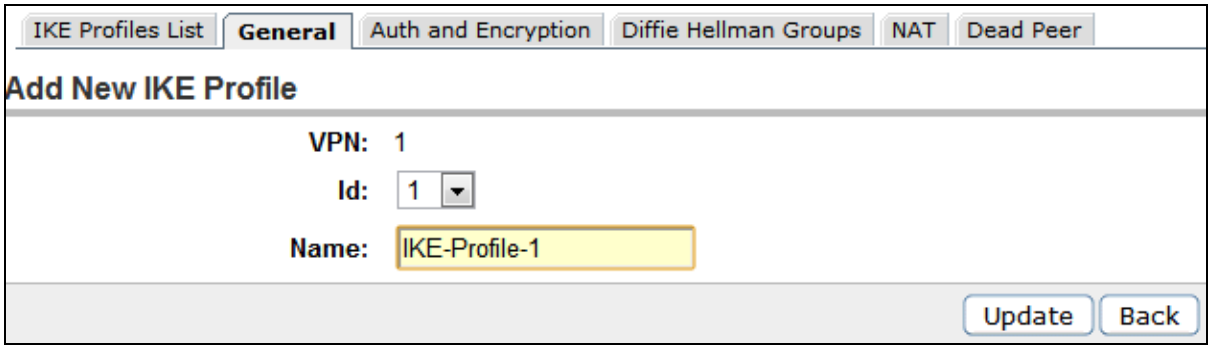
5. Back on the VPN Summary Page, click the **IPSec** settings link. Set the **Status** and **Group Matching** settings to **enabled** and click **Update**.



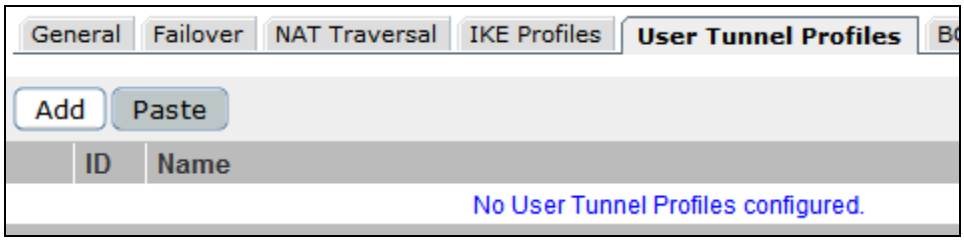
6. Click the **IKE Profiles** tab and click **Add** to create a new IKE Profile.



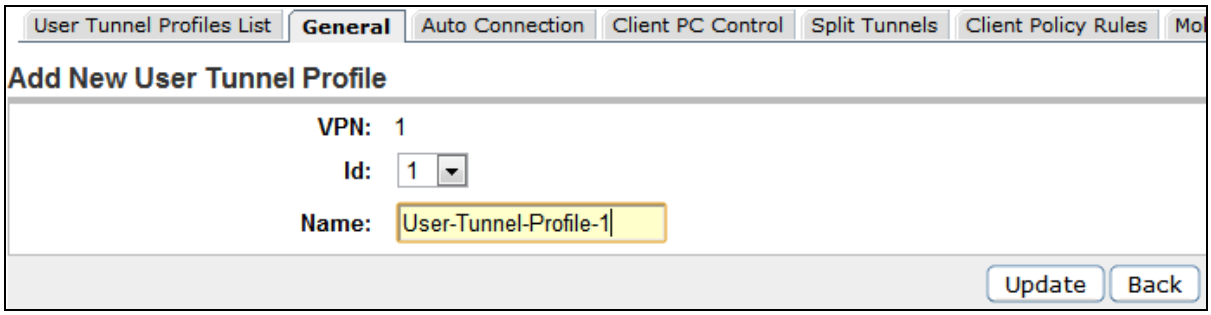
7. Enter a **Name** for the profile and click **Update**.



8. Return to the **IPSec** settings page. Click the **User Tunnel Profiles** tab and click **Add** to create a new profile.

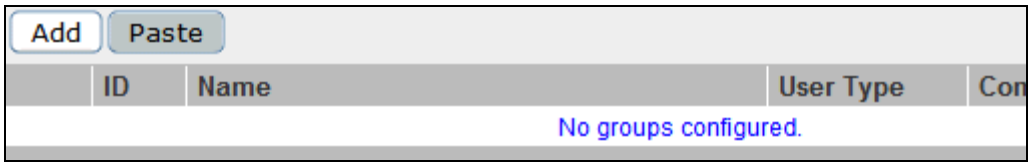


9. Enter a **Name** for the policy and click **Update**.

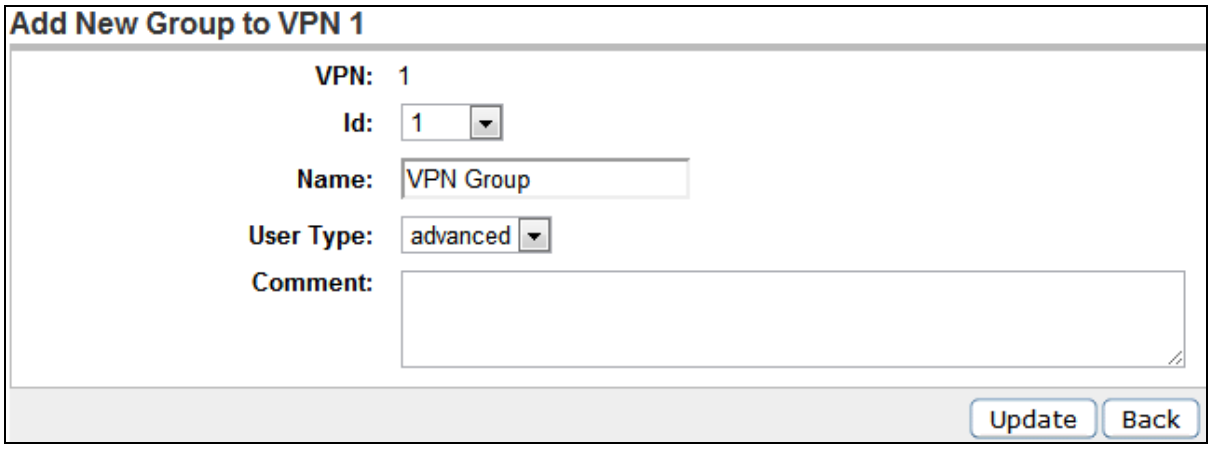


10. Select the previously created IKE Profile from the **IKE Profile** dropdown menu and click **Update**.

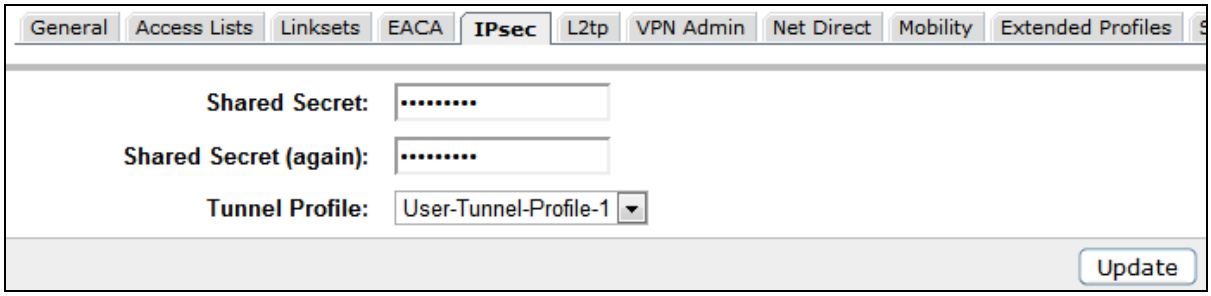
11. Return to the VPN Summary page and click the **Groups** settings link. Click **Add** to define a new group.



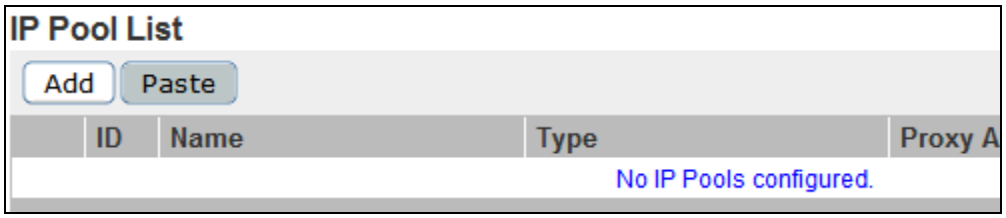
12. Enter a **Name** for the group and click **Update**.



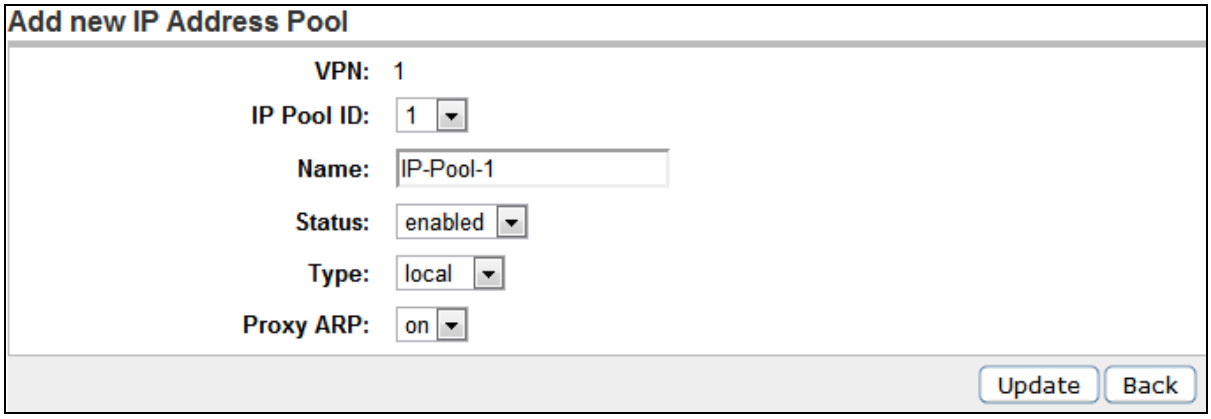
13. Click the **IPSec** tab. Enter the **Shared Secret** select the **Tunnel Profile** and click **Update**.



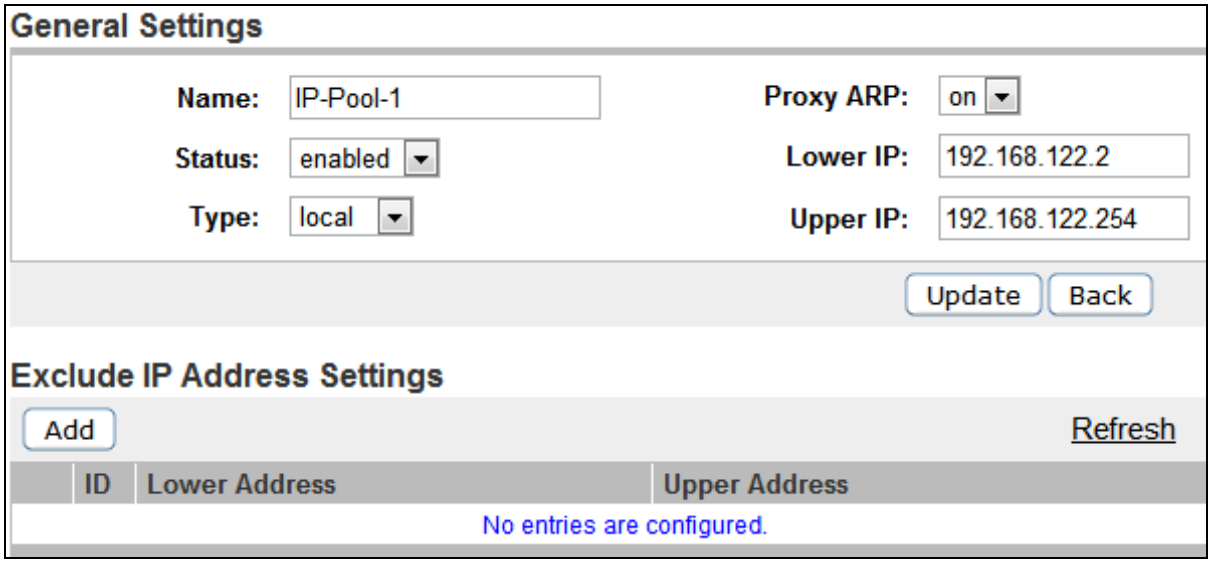
14. Return the VPN Summary page and click the **IP Pool** settings link. Click **Add** to create a new IP Pool.



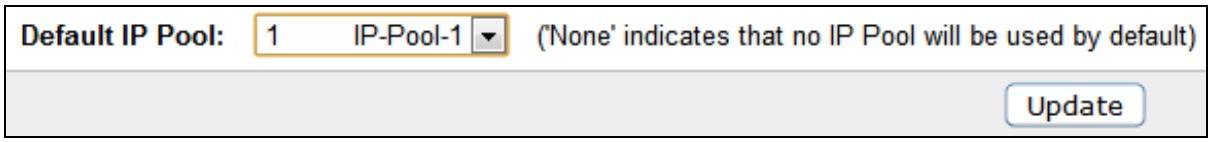
15. Enter a **Name** for the IP Pool, set its **Status** to **enabled**, and click **Update**.



16. Configure the IP Address Pool properties to fit your requirements. Additional attributes can be set from the **Network Attributes** tab. Click **Update** when finished.



17. Return to the **IP Pool** settings page. Select the new IP Pool from the **Default IP Pool** dropdown list and click **Update**.



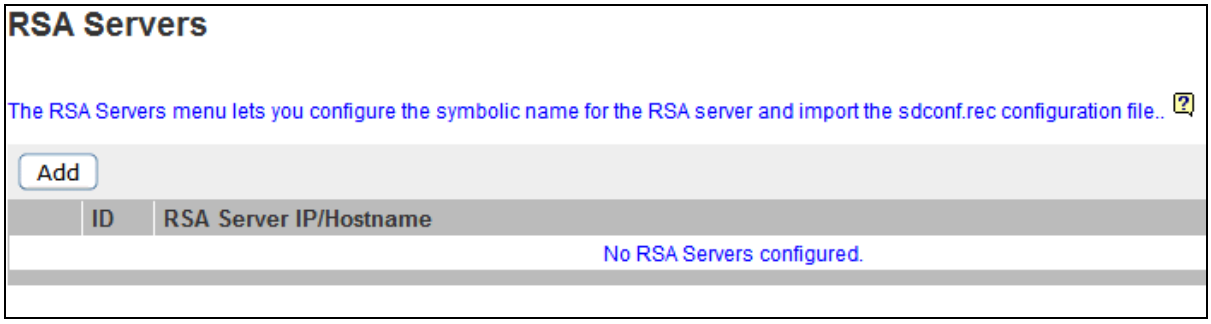
18. Click **Apply** in the browser-based management interface header to apply the change.

The VPN is now configured to accept IPSec VPN connections. Refer to the instructions on enabling SecurID authentication via native SecurID and RADIUS protocols later in this document.

Enable SecurID Authentication via Native RSA Protocol

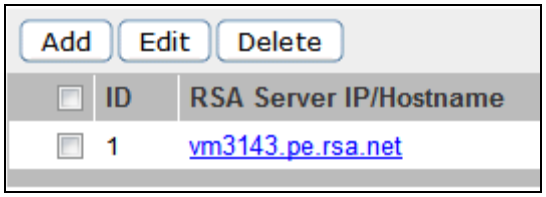
Log in to the browser-based management interface and complete the following instructions to configure SecurID authentication over the native protocol on the VPN Gateway.

1. In the left navigation pane, click the **Config** tab, expand **Administration** and click **RSA Servers**. Click **Add** to add new servers.



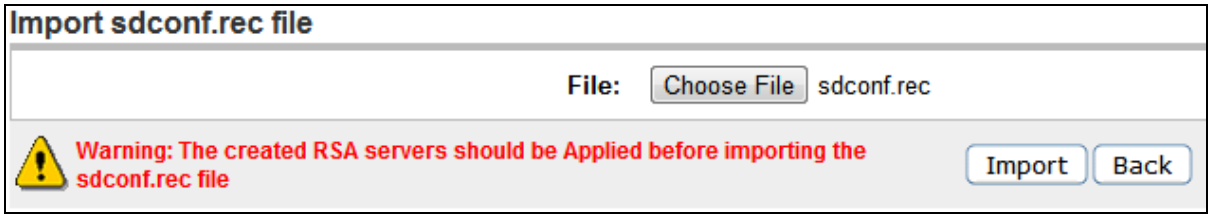
2. Enter the **RSA Server IP/Hostname** and click **Update**. Click **Apply** in the browser-based management interface header to apply the change.

3. Click on the newly configured RSA Server to edit it.

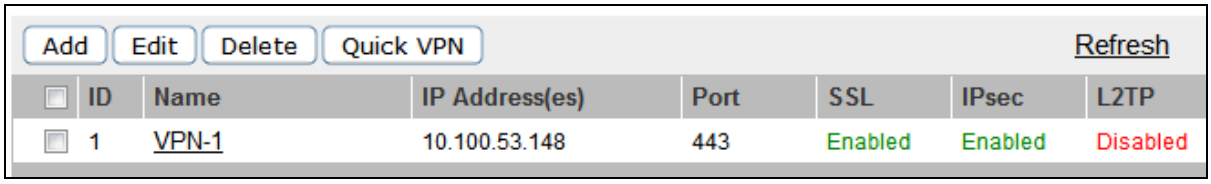


4. Browse to the **sdconf.rec** file obtained from the RSA Security Console and click **Import** to upload the configuration file to the VPN Gateway.

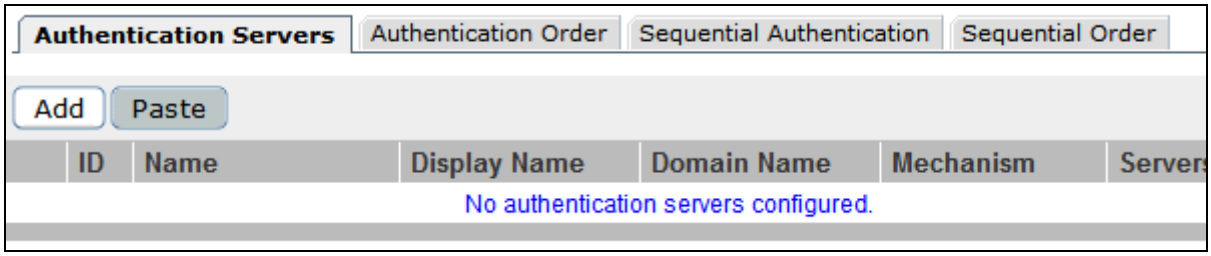
> **Important: You may get the error, "Import failed: The sdconf.rec file size is incorrect, should be 1024 bytes" if your sdconf.rec file is from an Authentication Manager 8.x. See the Known Issues section of this guide for remediation.**



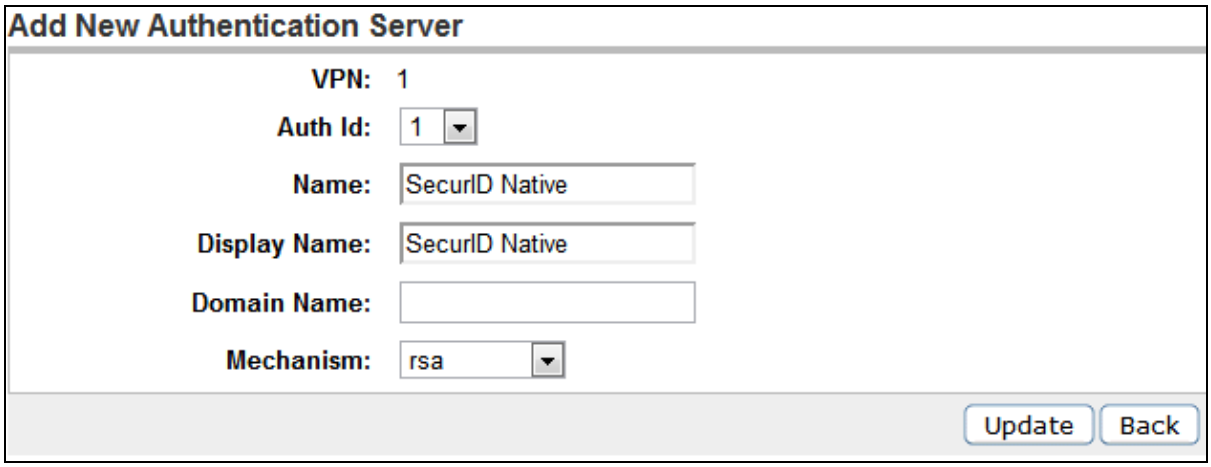
5. In the left navigation pane, click **VPN Gateways**. Click on the gateway for which you plan to enable RSA SecurID Authentication.



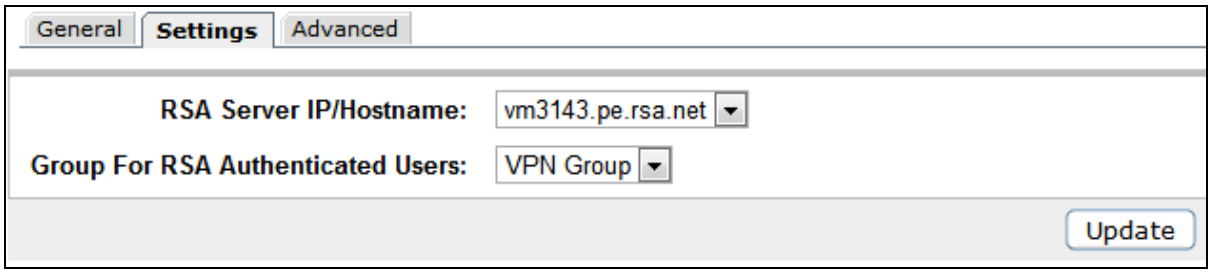
6. Click on the **Authentication** section to open the authentication options for the VPN Gateway. Click **Add** to add an authentication server.



7. Enter a **Name** for the authentication server, select **rsa** from the **Mechanism** dropdown list, and click **Update**.



8. Click the **Settings** tab. Select the **RSA Server IP/Hostname** you configured earlier. Choose the appropriate **Group For RSA Authenticated Users** from the dropdown list. Click **Update**.



9. Return to the VPN Gateway's **Authentication** settings page. Click the **Authentication Order** tab. Move the newly created Authentication Server over to the **Selected** list. Click **Update**.

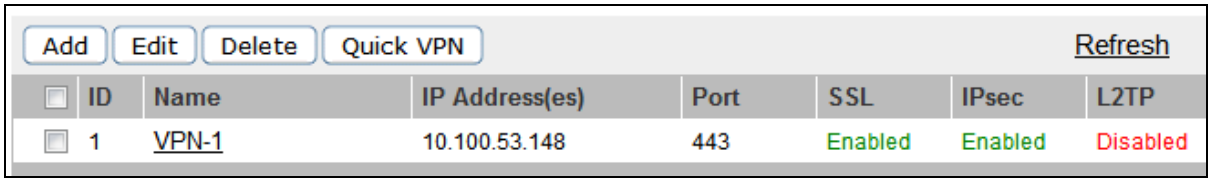
10. Click **Apply** in the browser-based management interface header to apply the change.

RSA SecurID Authentication is now configured for the VPN Gateway using the native RSA protocol.

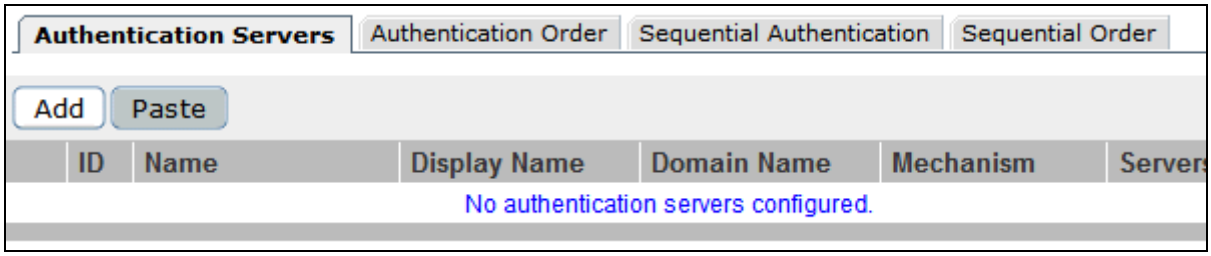
Enable SecurID Authentication via RADIUS Protocol

Log in to the browser-based management interface and complete the following instructions to enable RSA SecurID authentication over RADIUS.

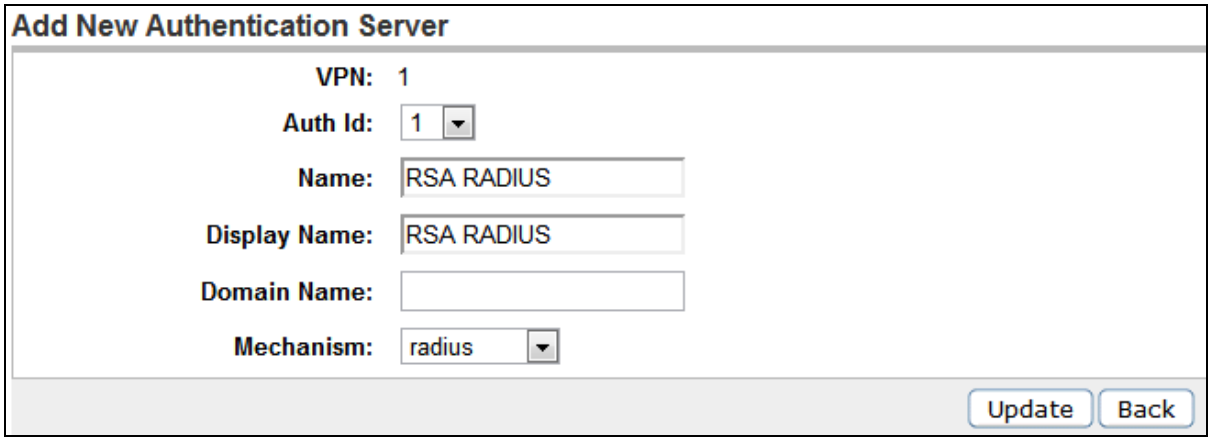
1. In the left navigation pane, click the **Config** tab, and then click **VPN Gateways**. Click on the VPN Gateway for which you plan to enable RSA SecurID Authentication.



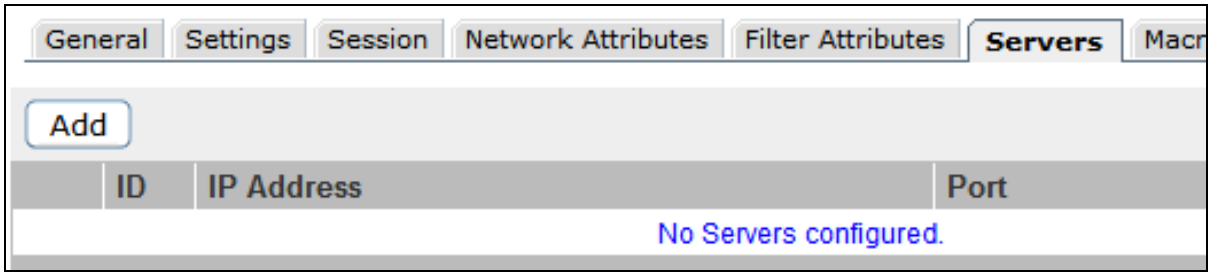
2. Click on the **Authentication** section to open the authentication options for the VPN Gateway. Click **Add** to add an authentication server.



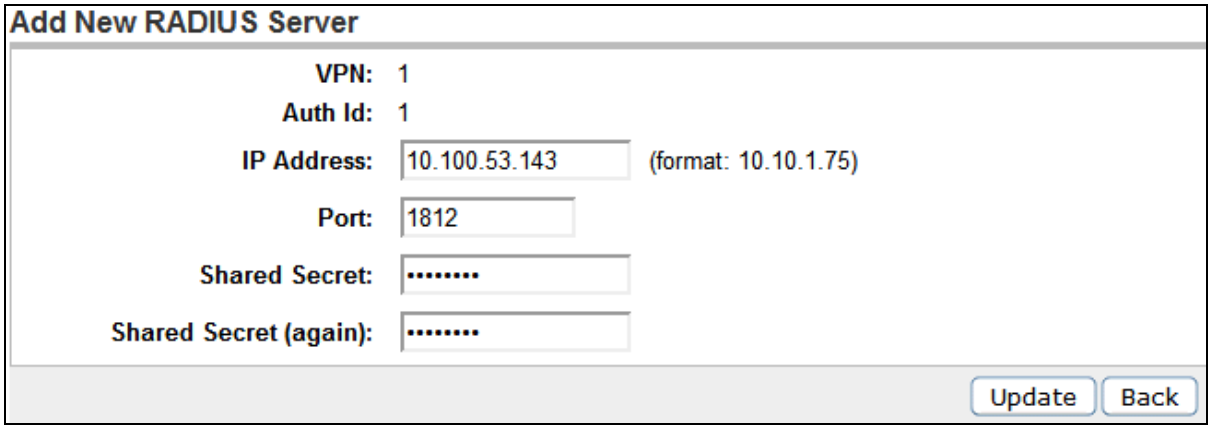
3. Enter a **Name** for the new authentication server, select **radius** from the **Mechanism** dropdown list and click **Update**.



4. Open the **Servers** tab and click **Add** to add a new RADIUS server.

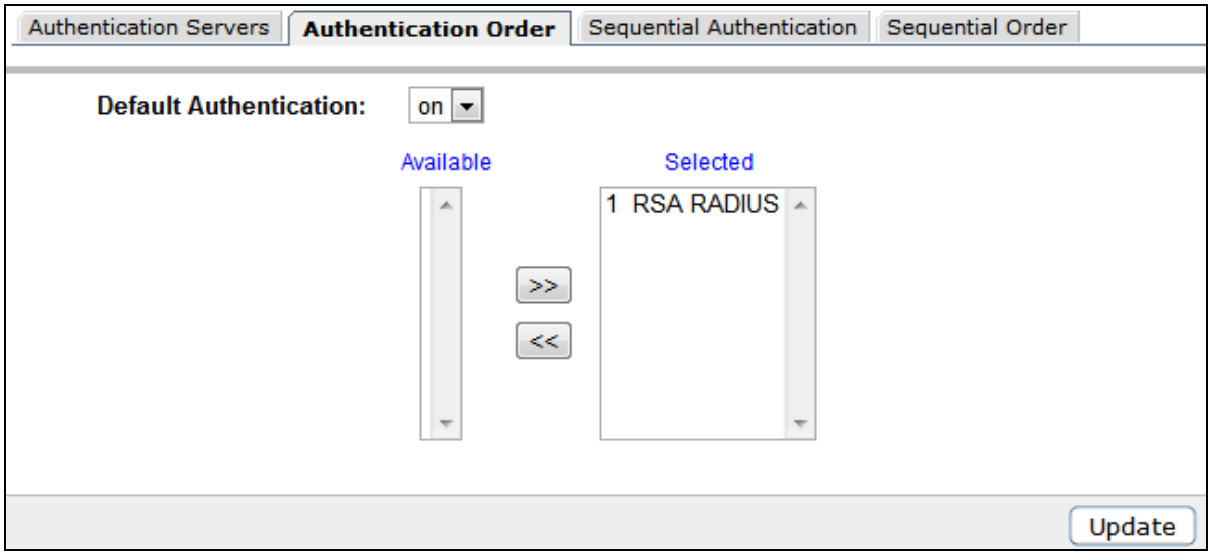


5. Supply the **IP Address** and RADIUS **port** of your Authentication Manager server. Enter the **Shared Secret** and click **Update**.

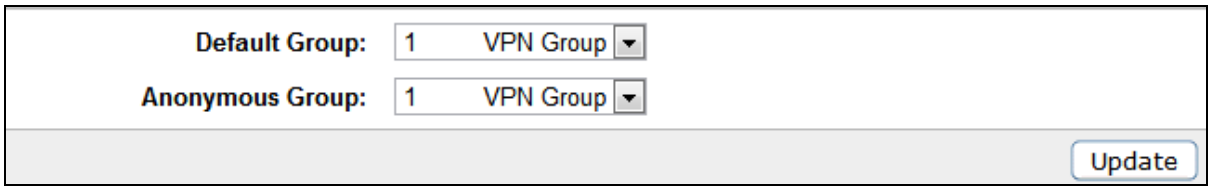


Note: Repeat steps 4 and 5 to add RADIUS replica servers.

6. Return to the Authentication settings page. Click the **Authentication Order** tab and move the RADIUS server entry into the **Selected** column. Click **Update**.



7. Return to the VPN Summary page. Click on the **Groups** link. Set the **Default Group** and click **Update**.

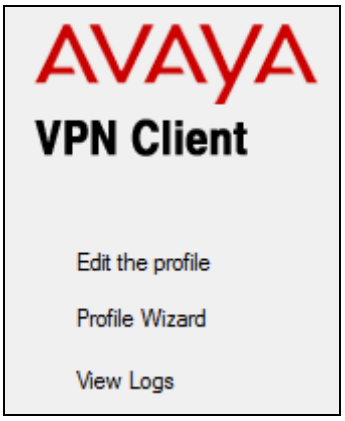


8. Click **Apply** in the browser-based management interface header to apply the change.

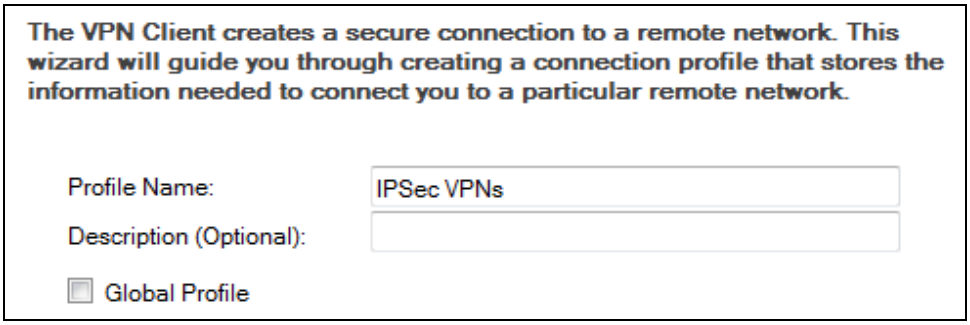
RSA SecurID Authentication is now configured for the VPN Gateway using RADIUS.

Configure the VPN Client

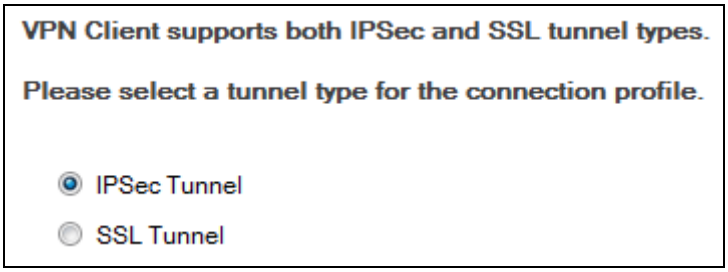
1. Launch the **Avaya VPN Client** and click **Profile Wizard**.



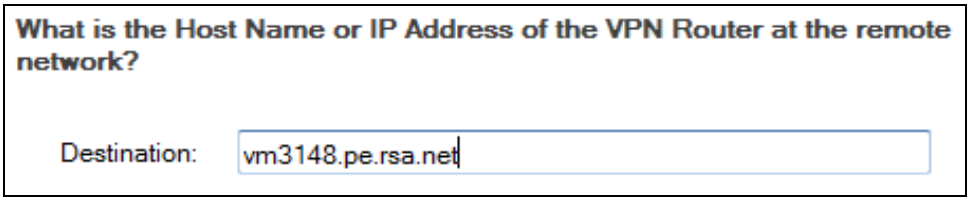
2. Enter the **Profile Name** and click **Next**.



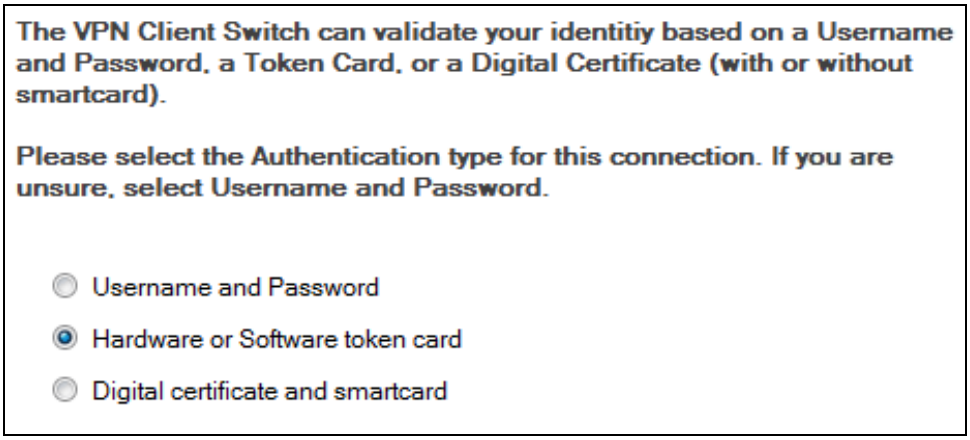
3. Select **IPSec Tunnel** and click **Next**.



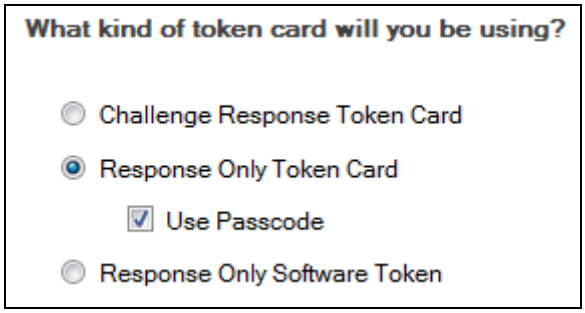
4. Enter the **Host Name** or **IP Address** of the VPN Gateway and click **Next**.



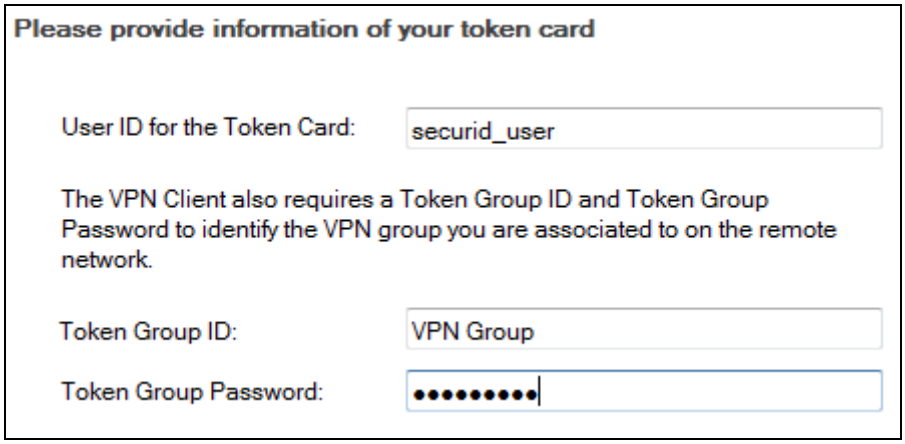
5. Select **Hardware or Software token card** as the authentication type and click **Next**.



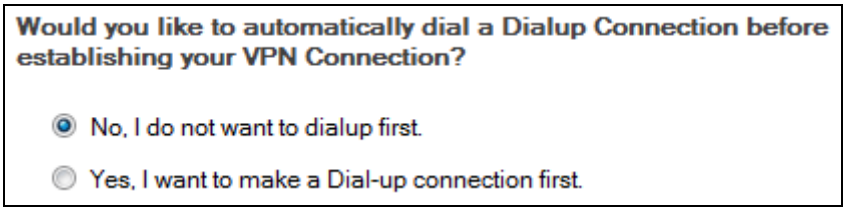
6. Select **Response Only Token Card** if the user will be authenticating with a hardware authenticator or **Response Only Software Token** if the user will be authenticating using an installed RSA Software Authenticator. Click **Next**.



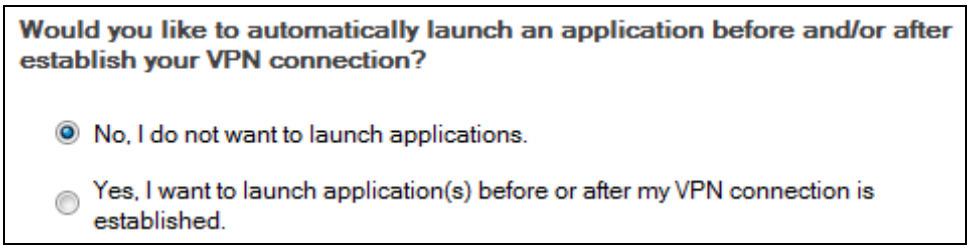
7. Enter the **User ID**, **Token Group ID**, and **Token Group Password** and click **Next**.



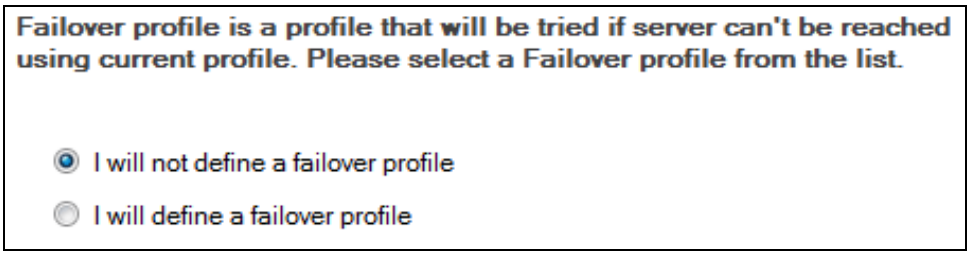
8. Configure the Dialup information as required by your organization and click **Next**.



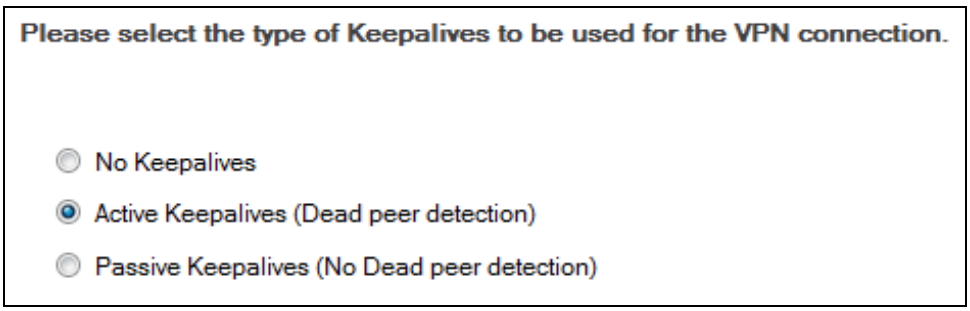
9. Configure application launch options as required by your organization and click **Next**.



10. Define failover options as required by your organization and click **Next**.

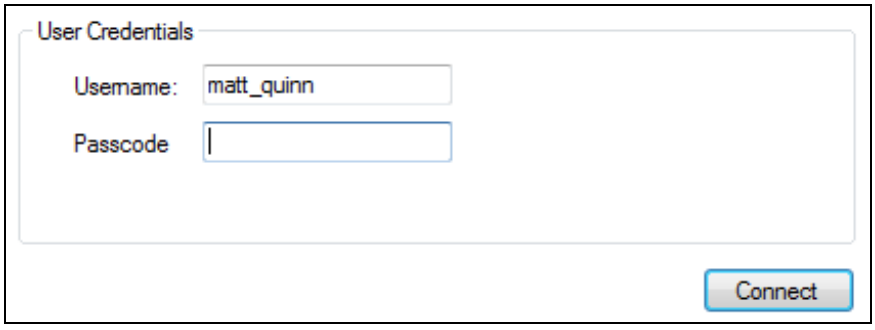


11. Define Keepalive settings as required by your organization and click **Next**. Click **Finish** to complete the wizard.

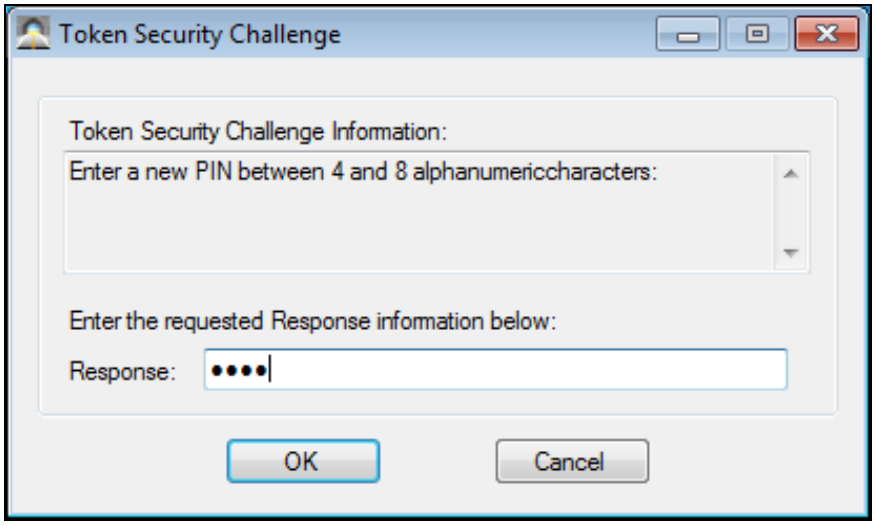


RSA SecurID Login Screens

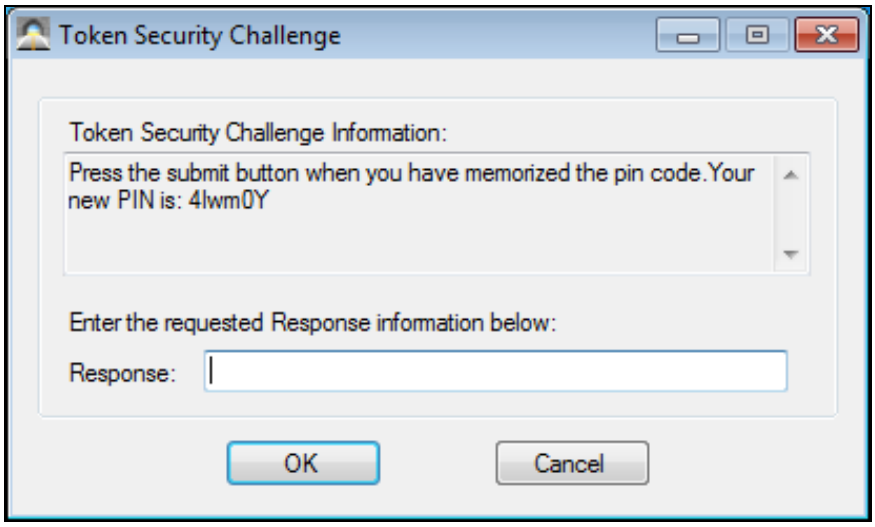
Login screen:



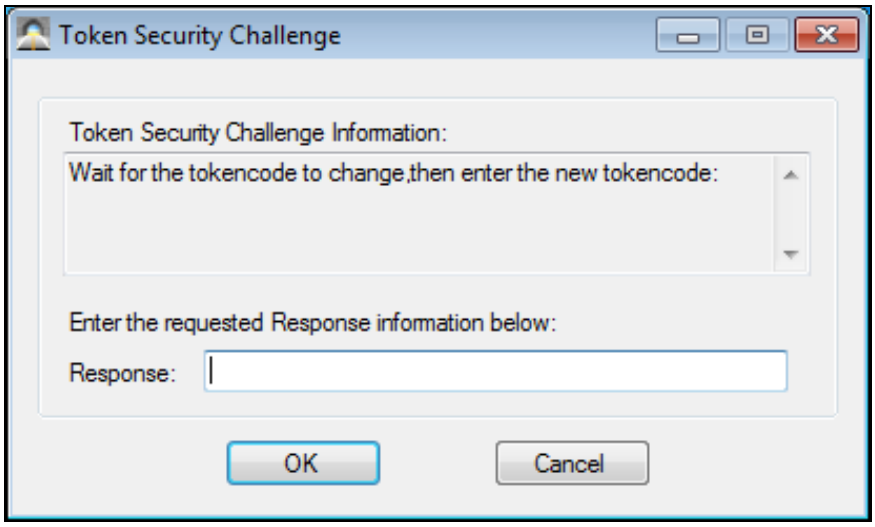
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
RSA Software Token	4.1.1.836	Windows 7 32bit
RSA Remote Authentication Client	3.6	Windows 7 32bit
Avaya VPN Gateway	SSL-9.1.3.1	3050-VM
Avaya VPN Client	10.06.500	Windows 7 32bit

RSA SecurID Authentication

Date Tested: May 28th, 2014

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

PEW

✓= Pass ✗ = Fail N/A = Not Applicable to Integration

Certification Test Checklist for RSA Authentication Manager

Software Token Automation

Date Tested: May 29, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
PINless Token			
Next Tokencode Mode	✓	N/A	✓
PINpad-style Token			
Deny Alphabetic PIN	✓	N/A	✓
Next Tokencode Mode	✓	N/A	✓
Fob-style Token			
16 Digit Passcode	✓	N/A	✓
Alphanumeric PIN	✓	N/A	✓
Next Tokencode Mode	✓	N/A	✓
Other			
System Generated PIN	✓*	N/A	✓*
Password Protected PIN	✓	N/A	✓

SID800 Token Automation

Date Tested: May 29, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
PINless Mode			
PINless Token	✓	N/A	✓
New PIN Mode			
User Defined PIN	✓	N/A	✓
System Generated PIN	✓*	N/A	✓*
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	✓

PEW

✓= Pass ✗ = Fail N/A = Not Applicable to Integration

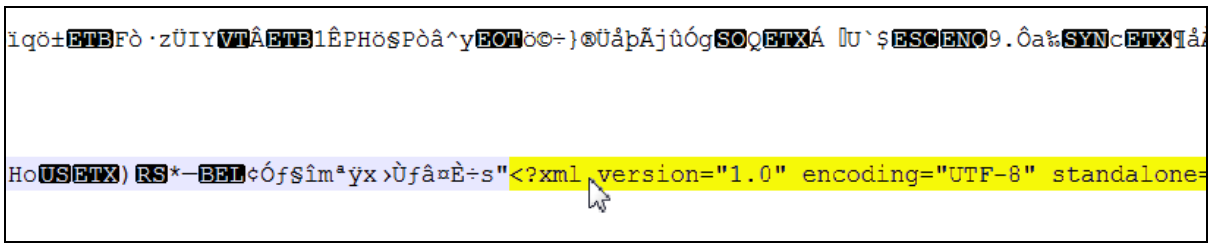
* See known issues section

Known Issues

The sdconf.rec file size is incorrect, should be 1024 bytes

If you're using Authentication Manager 8.x, you may get the error, "Import failed: The sdconf.rec file size is incorrect, should be 1024 bytes." To remediate, you must edit the sdconf.rec file and remove the XML from the end of the file and then save the file. Notepad++ was used to edit the sdconf.rec to accomplish this during the course of this certification.

Example:



Browser Based Management Interface Logon

If you configure the VPN Gateway device to require SecurID authentication when administrators log in using the browser-based management console and the user's authenticator is in New PIN mode, authentication will fail and the user will be unable to log in. The user will be prompted to create or accept a PIN but the PIN is never sent to Authentication Manager. Instead, the user receives the following error message:

"Login failed: a password must be specified"

To work around this issue, the user must set their new PIN using some alternative method, such as the RSA Self-Service Console.

Software / SID 800 Token Automation System Generated PIN

The user experience for accepting a new system generated PIN using Software / SID 800 Token automation is not as expected. After the user accepts the new system-generated PIN, the Avaya VPN Gateway will display an access denied page even though the PIN is accepted. Subsequent authentications using the new PIN will function as expected.

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	In memory
sdopts.rec	Not implemented
Node secret	In memory
sdstatus.12 / jastatus.12	In memory
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

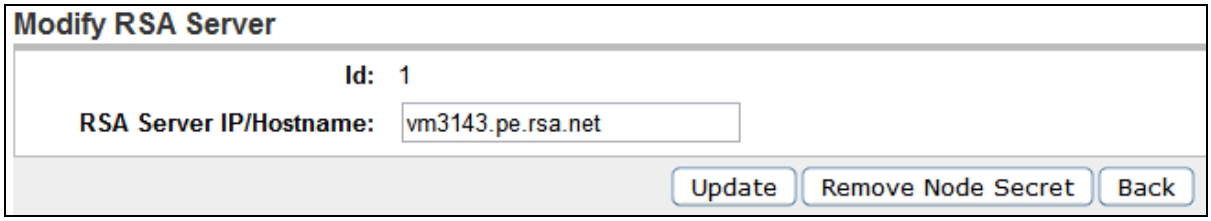
Partner Integration Details	
RSA SecurID UDP API	5.0.3.2
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

The node secret file is created on the agent after the first successful authentication with Authentication Manager. At times, the node secret may need to be reset, which requires an administrator to clear the secret in Authentication Manager and on the agent.

To clear the node secret on the VPN Gateway using the browser-based management console:

1. Browse to **Config > Administration > RSA Servers**.
2. Click the RSA Server that corresponds to your Authentication Manager deployment.
3. Click **Remove Node Secret**.



sdconf.rec:

To update the sdconf.rec configuration file on the VPN Gateway:

1. Browse to **Config > Administration > RSA Servers**.
2. Click the RSA Server that corresponds to your Authentication Manager deployment.
3. Browse to the sdconf.rec file obtained from the RSA Security Console and click **Import**.