



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.

Add	Quick VPN						Refresh
ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP	
No VPNs configured.							

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

Add a VPN

VPN Identifier:


VPN Name:

IP Address:

Port: (1-65534)

SSL Status:

Certificate Number:

 **Warning: New VPNs are directly applied to the database.**

[Create VPN](#) [Back](#)

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

		Quick VPN			Refresh		
<input type="checkbox"/>	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP
<input type="checkbox"/>	1	VPN-1	10.100.53.148	443	Enabled	Disabled	Disabled

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

General	IP Addresses	Wholesalesecurity	Single Sign On	Virtual Desktop	Portal Launch	VPN Lock
<p>VPN Name: <input type="text" value="VPN-1"/></p> <p>Standalone Status: <input type="text" value="enabled"/></p> <p>Session Idle Time: <input type="text" value="0"/> days <input type="text" value="0"/> hrs <input type="text" value="15"/> min <input type="text" value="0"/> sec</p> <p>Maximum Session Length: <input type="text" value="0"/> days <input type="text" value="0"/> hrs <input type="text" value="0"/> min <input type="text" value="0"/> sec <input checked="" type="checkbox"/> Or Infinity</p> <p style="text-align: right;"><input type="button" value="Update"/></p>						

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

General	HTTP	HTTP Rewrite	TCP	Proxy Mappings	Portal	Advanced
<p>Virtual Server Status: <input type="text" value="enabled"/></p> <p>Listen Port: <input type="text" value="443"/></p> <p>DNS Name of VIP: <input type="text" value="vm3148.pe.rsa.net"/></p> <p style="text-align: right;"><input type="button" value="Update"/></p>						

- 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.

Add		Quick VPN						Refresh
ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP		
No VPNs configured.								

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

Add a VPN

VPN Identifier:


VPN Name:

IP Address:

Port: (1-65534)

SSL Status:

Certificate Number:

 **Warning: New VPNs are directly applied to the database.**

[Create VPN](#) [Back](#)

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

Add		Edit	Delete	Quick VPN				Refresh
<input type="checkbox"/>	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP	
<input type="checkbox"/>	1	VPN-1	10.100.53.148	443	Enabled	Disabled	Disabled	

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

General | IP Addresses | Wholesecurity | Single Sign On | Virtual Desktop | Portal Launch | VPN Lock

VPN Name:

Standalone Status:

Session Idle Time: days hrs min sec

Maximum Session Length: days hrs min sec Or Infinity:

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

General | Failover | NAT Traversal | IKE Profiles | User Tunnel Profiles | BO Tunnel Profiles

Status:

Group Matching:

RADIUS Group Binding:

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

General | Failover | NAT Traversal | **IKE Profiles** | User Tunnel Prof

ID	Name
No IKE Profiles configured.	

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

IKE Profiles List **General** Auth and Encryption Diffie Hellman Groups NAT Dead Peer

Add New IKE Profile

VPN: 1
Id: 1
Name: IKE-Profile-1

Update Back

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

General Failover NAT Traversal IKE Profiles **User Tunnel Profiles** B...

Add Paste

ID	Name
No User Tunnel Profiles configured.	

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

User Tunnel Profiles List **General** Auto Connection Client PC Control Split Tunnels Client Policy Rules Mo...

Add New User Tunnel Profile

VPN: 1
Id: 1
Name: User-Tunnel-Profile-1

Update Back

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

The screenshot shows the 'General Settings' configuration page. It includes the following fields:

- IKE Profile:** A dropdown menu with 'IKE-Profile-1' selected.
- Enable Banner:** A dropdown menu with 'disabled' selected.
- Banner Display:** A text area containing the text 'SSL-VPN banner ...'.
- Client DNS Registration:** A dropdown menu with 'enabled' selected.

An 'Update' button is located at the bottom right of the form.

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

The screenshot shows the 'Groups' settings page. At the top, there are 'Add' and 'Paste' buttons. Below them is a table with the following columns: 'ID', 'Name', 'User Type', and 'Con'. The table is currently empty, and a blue message 'No groups configured.' is displayed in the center.

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

The screenshot shows the 'Add New Group to VPN 1' configuration page. It includes the following fields:

- VPN:** A dropdown menu with '1' selected.
- Id:** A dropdown menu with '1' selected.
- Name:** A text input field containing 'VPN Group'.
- User Type:** A dropdown menu with 'advanced' selected.
- Comment:** A text area.

'Update' and 'Back' buttons are located at the bottom right of the form.

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

General Access Lists Linksets EACA **IPsec** L2tp VPN Admin Net Direct Mobility Extended Profiles

Shared Secret:

Shared Secret (again):

Tunnel Profile: User-Tunnel-Profile-1

Update

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

IP Pool List

Add Paste

ID	Name	Type	Proxy A
No IP Pools configured.			

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

Add new IP Address Pool

VPN: 1

IP Pool ID: 1

Name: IP-Pool-1

Status: enabled

Type: local

Proxy ARP: on

Update Back

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

General Settings

Name: <input type="text" value="IP-Pool-1"/>	Proxy ARP: <input type="button" value="on"/> ▼
Status: <input type="button" value="enabled"/> ▼	Lower IP: <input type="text" value="192.168.122.2"/>
Type: <input type="button" value="local"/> ▼	Upper IP: <input type="text" value="192.168.122.254"/>

Exclude IP Address Settings

[Refresh](#)

ID	Lower Address	Upper Address
No entries are configured.		

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

Default IP Pool: ▼ (None indicates that no IP Pool will be used by default)

- 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.

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

RSA Servers

The RSA Servers menu lets you configure the symbolic name for the RSA server and import the sdconf.rec configuration file.. [?](#)

ID	RSA Server IP/Hostname
No RSA Servers configured.	

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

Add New RSA Server

Id:

RSA Server IP/Hostname:

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


<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	ID	RSA Server IP/Hostname
<input type="checkbox"/>	1	vm3143.pe.rsa.net

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.

Import sdconf.rec file

File: sdconf.rec

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

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

<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Quick VPN"/>					<input type="button" value="Refresh"/>
<input type="checkbox"/>	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP	
<input type="checkbox"/>	1	VPN-1	10.100.53.148	443	Enabled	Enabled	Disabled	

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

ID	Name	Display Name	Domain Name	Mechanism	Server
No authentication servers configured.					

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

VPN: 1

Auth Id: 1

Name: SecurID Native

Display Name: SecurID Native

Domain Name:

Mechanism: rsa

Update Back

- 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**.

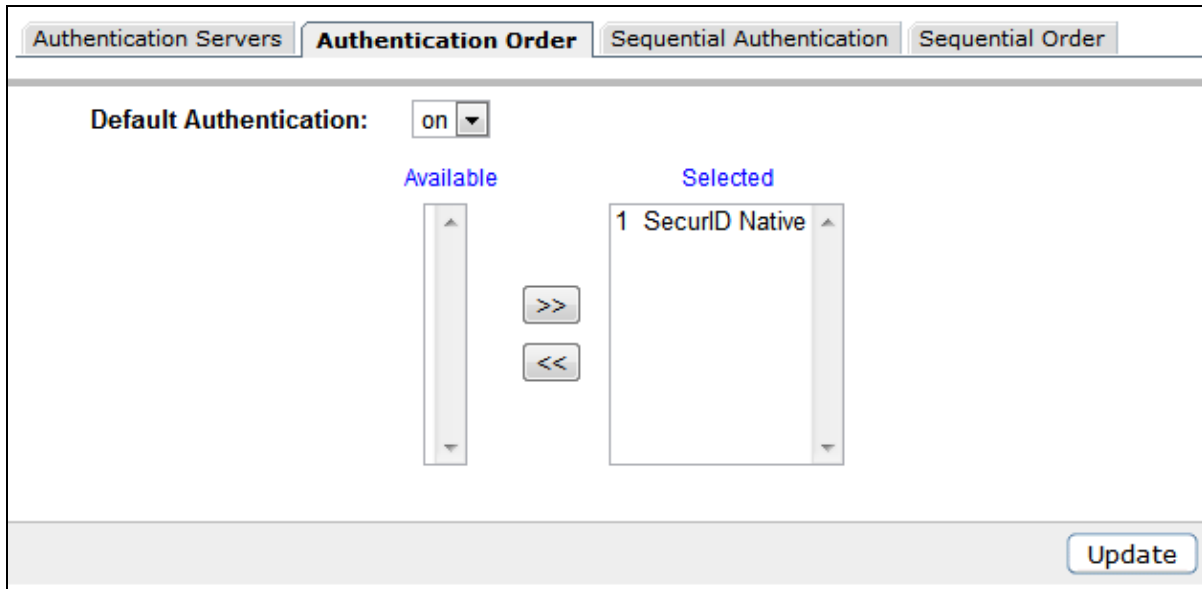
General **Settings** Advanced

RSA Server IP/Hostname: vm3143.pe.rsa.net

Group For RSA Authenticated Users: VPN Group

Update

- 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**.



- 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.

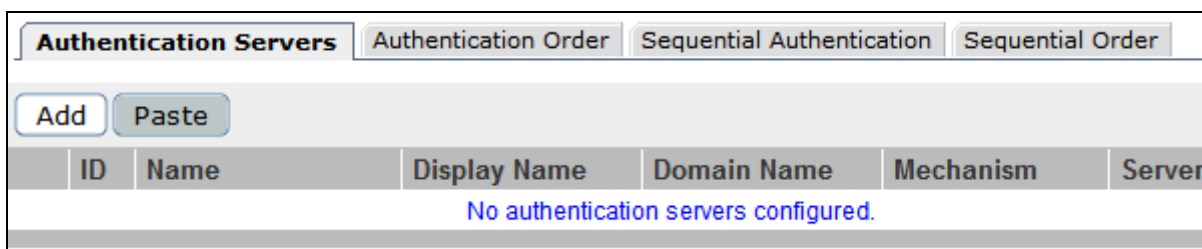
Enable SecurID Authentication via RADIUS Protocol

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

- 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.

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Quick VPN"/> <input type="button" value="Refresh"/>							
<input type="checkbox"/>	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP
<input checked="" type="checkbox"/>	1	<u>VPN-1</u>	10.100.53.148	443	Enabled	Enabled	Disabled

- 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**.

Add New Authentication Server

VPN: 1

Auth Id: 1

Name: RSA RADIUS

Display Name: RSA RADIUS

Domain Name:

Mechanism: radius

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

General Settings Session Network Attributes Filter Attributes **Servers** Macr

ID	IP Address	Port
No Servers configured.		

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

Add New RADIUS Server

VPN: 1

Auth Id: 1

IP Address: 10.100.53.143 (format: 10.10.1.75)

Port: 1812

Shared Secret:

Shared Secret (again):

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

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

Authentication Servers **Authentication Order** Sequential Authentication Sequential Order

Default Authentication: on ▼

Available Selected

1 RSA RADIUS

>> <<

Update

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

Default Group: 1 VPN Group ▼

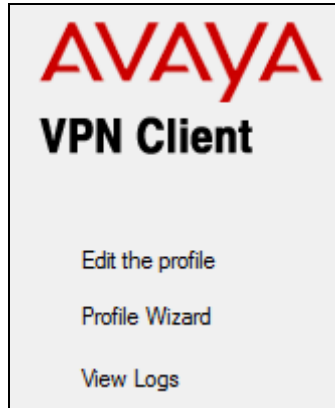
Anonymous Group: 1 VPN Group ▼

Update

- 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**.

The VPN Client creates a secure connection to a remote network. This wizard will guide you through creating a connection profile that stores the information needed to connect you to a particular remote network.

Profile Name:

Description (Optional):

Global Profile

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

VPN Client supports both IPSec and SSL tunnel types.

Please select a tunnel type for the connection profile.

IPSec Tunnel

SSL Tunnel

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

What is the Host Name or IP Address of the VPN Router at the remote network?

Destination:

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

The VPN Client Switch can validate your identity based on a Username and Password, a Token Card, or a Digital Certificate (with or without smartcard).

Please select the Authentication type for this connection. If you are unsure, select Username and Password.

Username and Password

Hardware or Software token card

Digital certificate and smartcard

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**.

What kind of token card will you be using?

Challenge Response Token Card

Response Only Token Card

Use Passcode

Response Only Software Token

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

Please provide information of your token card

User ID for the Token Card:

The VPN Client also requires a Token Group ID and Token Group Password to identify the VPN group you are associated to on the remote network.

Token Group ID:

Token Group Password:

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

Would you like to automatically dial a Dialup Connection before establishing your VPN Connection?

- No, I do not want to dialup first.
- Yes, I want to make a Dial-up connection first.

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

Would you like to automatically launch an application before and/or after establish your VPN connection?

- No, I do not want to launch applications.
- Yes, I want to launch application(s) before or after my VPN connection is established.

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

Failover profile is a profile that will be tried if server can't be reached using current profile. Please select a Failover profile from the list.

- I will not define a failover profile
- I will define a failover profile

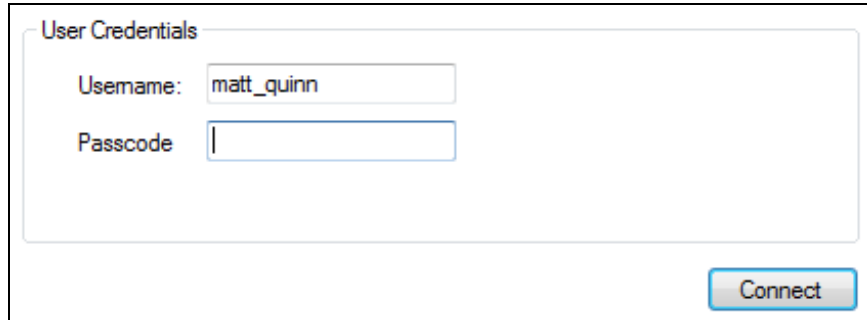
11. Define Keepalive settings as required by your organization and click **Next**. Click **Finish** to complete the wizard.

Please select the type of Keepalives to be used for the VPN connection.

- No Keepalives
- Active Keepalives (Dead peer detection)
- Passive Keepalives (No Dead peer detection)

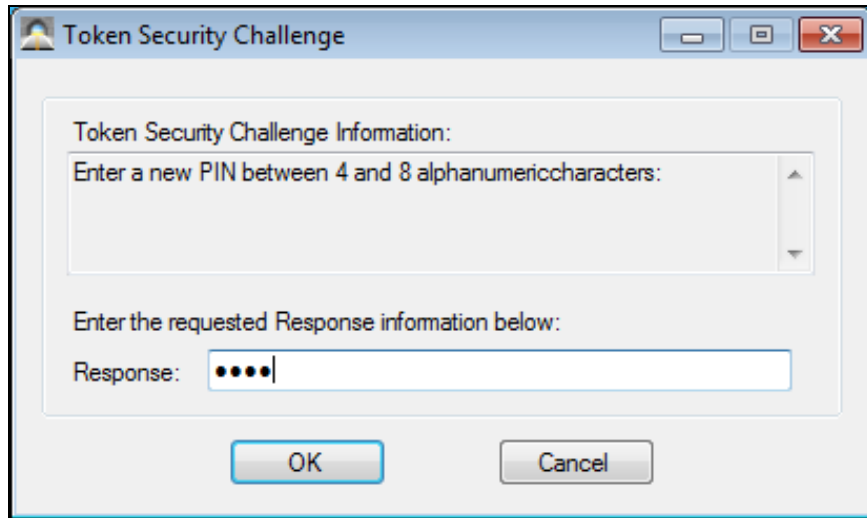
RSA SecurID Login Screens

Login screen:



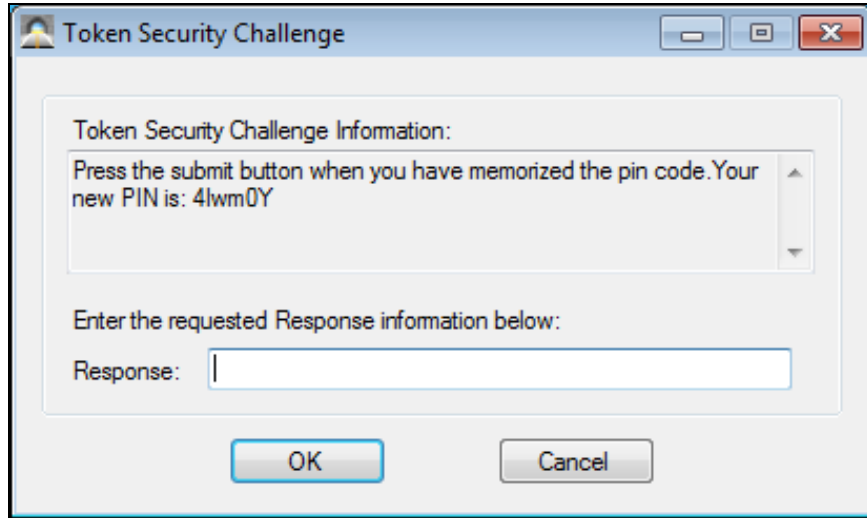
The screenshot shows a web-based login form titled "User Credentials". It contains two input fields: "Username" with the text "matt_quinn" and "Passcode" which is empty. A "Connect" button is located at the bottom right of the form.

User-defined New PIN:

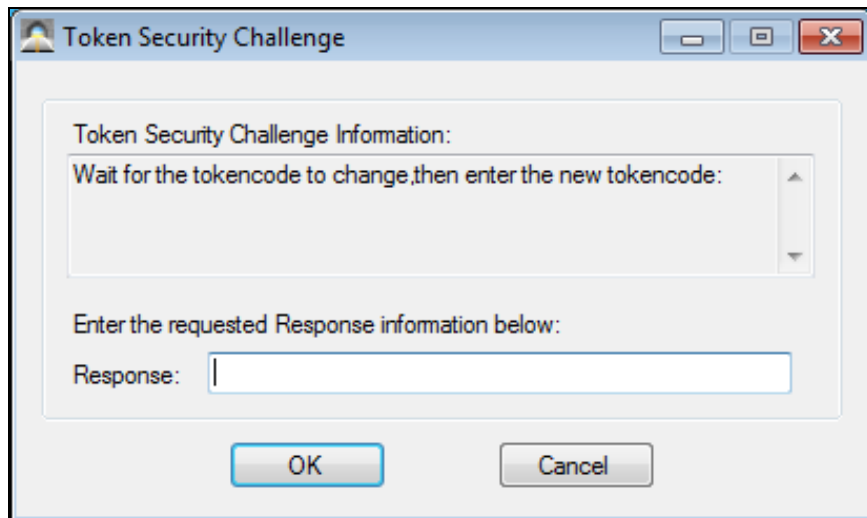


The screenshot shows a Windows-style dialog box titled "Token Security Challenge". It contains a text area with the text "Enter a new PIN between 4 and 8 alphanumeric characters:". Below this is a label "Enter the requested Response information below:" followed by a "Response:" input field containing four dots. "OK" and "Cancel" buttons are at the bottom.

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

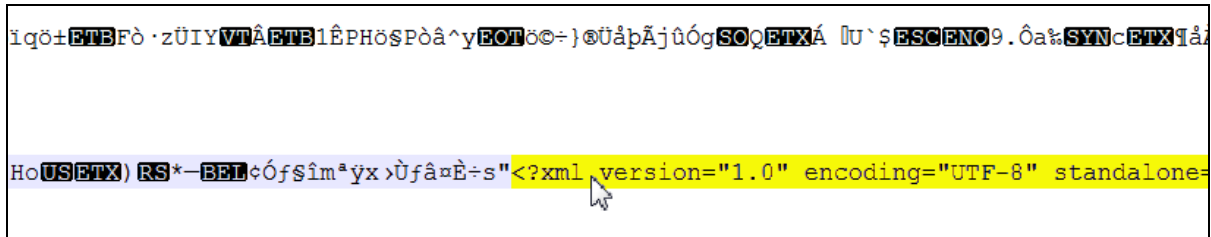
* See known issues section

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:



```
i qö±ETBFò·zÜIYVtÄETB1ÊPHöSPòâ^yEOTöc=)öÜápĀjûôgSOQETXÁ [U`$ESCENO9.ôa%SYNcETX1â  
Ho(US(ETX) RS*-BET)çófšîm^ÿx>Ûfâ=È÷s"<?xml version="1.0" encoding="UTF-8" standalone=
```

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**.

Modify RSA Server

Id: 1

RSA Server IP/Hostname:


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**.

Import sdconf.rec file

File: No file chosen

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