

RSA SecurID Ready Implementation Guide

Last Modified: 09/01/2009

Partner Information

Product Information	
Partner Name	SonicWALL
Web Site	www.sonicwall.com
Product Name	SonicWALL SonicOS
Version & Platform	Enhanced 5.2.0.1
Product Description	SonicOS Enhanced is the most powerful SonicOS operating system designed for SonicWALL security appliances.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

Partner Integration Overview	
Authentication Methods Supported	RADIUS
RSA SecurID Library Version Used	N/A
RSA Authentication Manager Replica Support *	N/A
Secondary RADIUS Server Support	Yes (1)
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, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No

Product Requirements

Partner Product Requirements: SonicWALL UTM Products	
Firmware Version	SonicOS Enhanced 5.2.0.1
Additional Software Requirements	
SonicWALL Global VPN Client	4.2.6



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 SonicOS Enhanced 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 SonicOS Enhanced 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 SonicOS Enhanced as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the SonicOS Enhanced 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	N/A
Node Secret	N/A
sdstatus.12	N/A
sdopts.rec	N/A




Partner Product 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.

 **Note: SonicWALL recommends that customers update to the latest version of SonicOS Enhanced prior to completing this configuration.**

Configuring SonicOS Enhanced

SonicWALL UTM products running SonicOS Enhanced support secure two-factor authentication for Global VPN Client tunnels via the RADIUS protocol. The following configuration steps must be performed in order implement this solution.

On the SonicWALL security appliance:

- Set up the User's Authentication Method
- Create new GroupVPN Policy for the Global VPN Client

On the computer requiring secure remote access via SonicWALL Global VPN Client:

- Install SonicWALL Global VPN Client
- Create a Profile for Connecting to the SonicWALL security appliance
- Connect to the Sonicwall Security Appliance Using the GVC
- Verify that applications function properly through the tunnel

Configuring RADIUS

1. In **Users > Settings** under **User Login Settings**, set the Authentication Method to **RADIUS** from the drop-down menu, and click the **Configure** button.



The screenshot shows a web interface titled "User Login Settings". Below the title, there is a label "Authentication method for login:" followed by a dropdown menu currently displaying "RADIUS" and a "Configure..." button to its right.

 **Note: After the RADIUS authentication method is enabled the SonicWALL security appliance can only be accessed using HTTPS Management.**

2. In the **Primary Server: Name or IP Address** field, enter the RSA Authentication Manager Servers IP Address.
3. Create a **Shared Secret** to authenticate the SonicWALL to the RSA Authentication Manager Server. This same secret will be used when you create the Agent Host records in the RSA Authentication Manager Server configuration.
4. Set the **Port Number** to 1812.



Settings | **RADIUS Users** | Test

Global RADIUS Settings

RADIUS Server Timeout (seconds): Retries:

RADIUS Servers

Primary Server:

Name or IP Address:

Shared Secret:


Port Number:

Secondary Server:

Name or IP Address:

Shared Secret:

Port Number:

 **Note:** RSA recommends a RADIUS Server Timeout of 60 seconds or greater.

5. Select the **RADIUS Users** tab, and select the **Use Radius Filter-ID** attribute on Radius Server.
6. Select **Trusted User** from the drop-down box under **Default user group** to which all RADIUS users belong.

Settings | **RADIUS Users** | Test

RADIUS User Settings

Allow only users listed locally

Mechanism for setting user group memberships for RADIUS users:

Use SonicWALL vendor-specific attribute on RADIUS server

Use RADIUS Filter-Id attribute on RADIUS server

Use LDAP to retrieve user group information


Local configuration only

Memberships can be set locally by duplicating RADIUS user names

Default user group to which all RADIUS users belong:

▼

7. Click **OK**.

 **Note:** The RADIUS testing tool may not work due to encryption type mismatches. Please use the RSA Log Monitor application for testing and debugging purposes.



Configuring Global VPN Client Settings

1. In **VPN > Settings**, click the **Configure** icon for the **WAN GroupVPN**, and select the **Advanced** Tab.
2. Select **Require Authentication of VPN Clients via XAUTH**, and select the **Trusted Users** group as the User Group for XAUTH users.

The screenshot shows the 'Advanced' tab of the VPN Client Settings window. It features four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'Advanced Settings' section includes checkboxes for 'Enable Windows Networking (NetBIOS) Broadcast' and 'Enable Multicast'. Below these are options for 'Management via this SA' with checkboxes for 'HTTP', 'HTTPS', and 'SSH'. A 'Default Gateway' field is set to '0.0.0.0'. The 'Client Authentication' section has a checked checkbox for 'Require Authentication of VPN Clients via XAUTH'. The 'User Group for XAUTH users' dropdown is set to 'Trusted Users', and the 'Allow Unauthenticated VPN Client Access' dropdown is set to '--Select Local Network--'.

3. Select the **Client** Tab, and set the following parameters:
 - Set **Cache XAUTH User Name and Password on Client** to **Single Session**.
 - Set **Virtual Adapter settings** to **DHCP Lease** (or **DHCP Lease** or **Manual Config** if you wish to statically address the virtual adapter).
 - Select the **Use Default Key for Simple Client Provisioning** checkbox.

The screenshot shows the 'Client' tab of the VPN Client Settings window. It features four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'User Name and Password Caching' section has a dropdown for 'Cache XAUTH User Name and Password on Client' set to 'Single Session'. The 'Client Connections' section has a dropdown for 'Virtual Adapter settings' set to 'DHCP Lease' and another dropdown for 'Allow Connections to' set to 'Split Tunnels'. There is an unchecked checkbox for 'Set Default Route as this Gateway'. The 'Client Initial Provisioning' section has a checked checkbox for 'Use Default Key for Simple Client Provisioning'.

4. Click **OK**.

Configuring DHCP over VPN

The user can configure an internal DHCP Server instead of using the built-in Sonicwall DHCP server.

1. Select **VPN > DHCP over VPN** and click the **Configure** icon for Central Gateway.



2. Select the **Use Internal DHCP Server** and **For Global VPN Client** check boxes.

DHCP Relay

Use Internal DHCP Server

For Global VPN Client

For Remote Firewall

Send DHCP requests to the server addresses listed below

IP Address

Add... Edit... Delete Delete All

Relay IP Address (Optional): 0.0.0.0

3. Click **OK**.

Configuring User Group Settings

1. Select **Users > Local Groups** and click the **Configure** icon for Trusted Users.
2. Select the **Members** tab, and confirm **All RADIUS Users** is in the **Members Users and Groups**.

Settings **Members** VPN Access CFS Policy

Group Memberships

Non-Member Users and Groups:

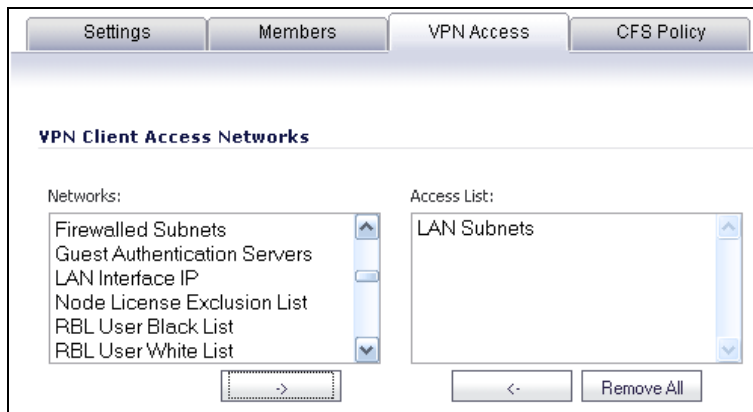
- Content Filtering Bypass
- Guest Services
- Limited Administrators
- SonicWALL Administrators
- SonicWALL Read-Only Admins
- SSLVPN Services

Member Users and Groups:

- All RADIUS Users

Add All -> <- Remove All

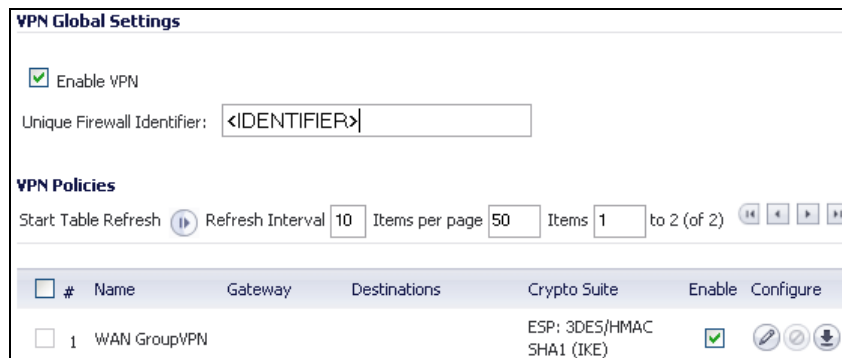
3. Select **VPN Access** tab, and add the **LAN Subnets** or the appropriate network resource(s) the remote users will need to access.



4. Click **OK**.

Enable Global VPN Client Connections

1. Select **VPN > Settings**.
2. Select the **Enable VPN** checkbox.
3. Select the **Enable** checkbox for the **WAN GroupVPN** policy.



SonicWALL Global VPN Client Configuration

Download and install the SonicWALL Global VPN Client by logging in to your mySonicWALL account at www.mysonicwall.com. Once installed, simply use the New Connection Wizard to create a connection to your SonicWALL as detailed below.

1. Create a new VPN Connection using the New Connection Wizard. Select the **File > New Connection** item to launch the wizard. Click **Next** to continue to the next screen of the wizard.



2. Select the **Remote Access** radio button and click the **Next** button.



3. Enter the WAN IP Address or the DNS address of the SonicWALL that you are going to connect to. Click the **Next** button when finished.



New Connection Wizard

Remote Access
To use the remote access scenario, specify the gateway's domain name or IP address.

Specify the domain name or IP address of the security gateway.
IP Address or Domain Name:

You may also specify a name for this connection.
Connection Name:

To continue, click Next.

< Back Next > Cancel

4. Click the **Finish** button to complete the wizard.

New Connection Wizard

 **Completing the New Connection Wizard**

Your new connection is ready to be added to your configuration. You can set the following options for this new connection:

- Create a desktop shortcut for this connection
- Enable this connection when the program is launched

To complete this wizard, click Finish.



< Back Finish Cancel

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: 08/17/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.3	Microsoft Windows 2003 Server
SonicWALL NSA	2400	SonicOS Enhanced 5.2.0.1-21o
SonicWALL Global VPN Client	4.2.6 (32-bit)	Microsoft XP Professional SP3 (32-bit)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

BSD

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 08/18/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1 SP2	Microsoft Windows 2003 Server
SonicWALL NSA	2400	SonicOS Enhanced 5.2.0.1-21o
SonicWALL Global VPN Client	4.2.6 (32-bit)	Microsoft XP Professional SP3 (32-bit)

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

BSD

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