



RSA SecurID Ready Implementation Guide

Last Modified: October 24, 2013

Partner Information

Product Information	
Partner Name	Barracuda Networks
Web Site	https://www.barracuda.com/
Product Name	Barracuda SSL VPN
Version & Platform	2.4.0.9
Product Description	The Barracuda SSL VPN is an integrated hardware and software solution enabling secure, clientless remote access to internal network resources from any Web browser. Designed for remote employees and road warriors, the Barracuda SSL VPN provides comprehensive control over file systems and Web-based applications requiring external access. The Barracuda SSL VPN integrates with third-party authentication mechanisms to control user access levels and to provide Single Sign-On.



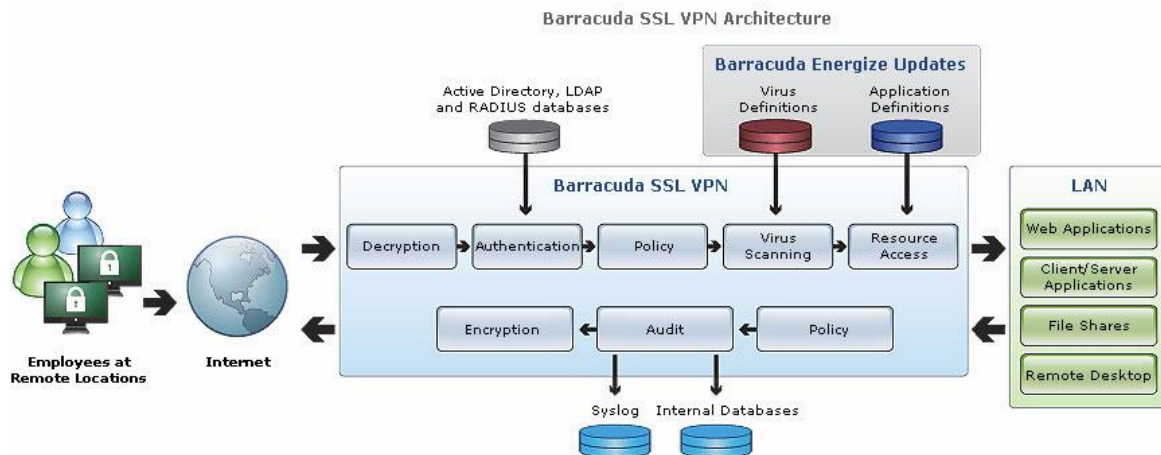
Solution Summary

The Barracuda SSL VPN can perform authentication to RSA Authentication Manager servers by using the RADIUS protocol. This is done by utilizing a Java based RADIUS client to send authentication requests to the Authentication Manager server and allowing or denying access to the SSL VPN unit based upon a success or failure message returned by the Authentication Manager server. This client also handles RADIUS challenge requests, allowing the Authentication Manager server to communicate and prompt for PIN change requests etc.

All that needs to be configured on the Barracuda SSL VPN is an Authentication Scheme which uses the RADIUS module and also to set the RADIUS server specific details such as hostname, shared secret etc.

This can be ideal if you already have an RSA Authentication Manager infrastructure in place and you wish to bring the same security to an internet facing product such as an SSL VPN. RSA authentication can be combined with any of the Barracuda SSL VPN's 7 other authentication methods, to create multi factor authentication for even greater security.

RSA Authentication Manager supported features Barracuda SSL VPN version 2.4.0.9	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 the Barracuda SSL VPN will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Barracuda SSL VPN to communicate with 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: 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 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 Barracuda SSL VPN 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 Barracuda SSL VPN components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Overview

1. Configure RADIUS settings. Log on to Barracuda SSL VPN as ssladmin, navigate to **Access Control > Configuration** and scroll down to the RADIUS section.

RADIUS Save Changes Help

RADIUS Server:

Backup RADIUS Servers: Add >> << Remove Hostnames
Host names of backup RADIUS Servers.

Authentication Port: This is the port number stipulated for the RADIUS authentication process. It **MUST** be a valid integer port between **0** and **65535**. Default (1812).

Accounting Port: This is the port number stipulated for the RADIUS accounting process. It **MUST** be a valid integer port between **0** and **65535**. Default (1813).

Shared Secret: The RADIUS shared secret which has been set up on the RADIUS server.

Authentication Method: If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are **PAP**, **CHAP**, **MSCHAP** and **MSCHAPv2**.

Time Out: The timeout for a RADIUS message.

Authentication Retries: The number of retries for a RADIUS message.

RADIUS Attributes: Add >> << Remove Attributes
The RADIUS attributes required to execute the request.

Username Case: As Entered Force Upper Case Force Lower Case Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.


Password Prompt Text: Customize the RADIUS password prompt text.

Reject Challenge: Yes No Reject a challenge-response request from the RADIUS server. Default (true)

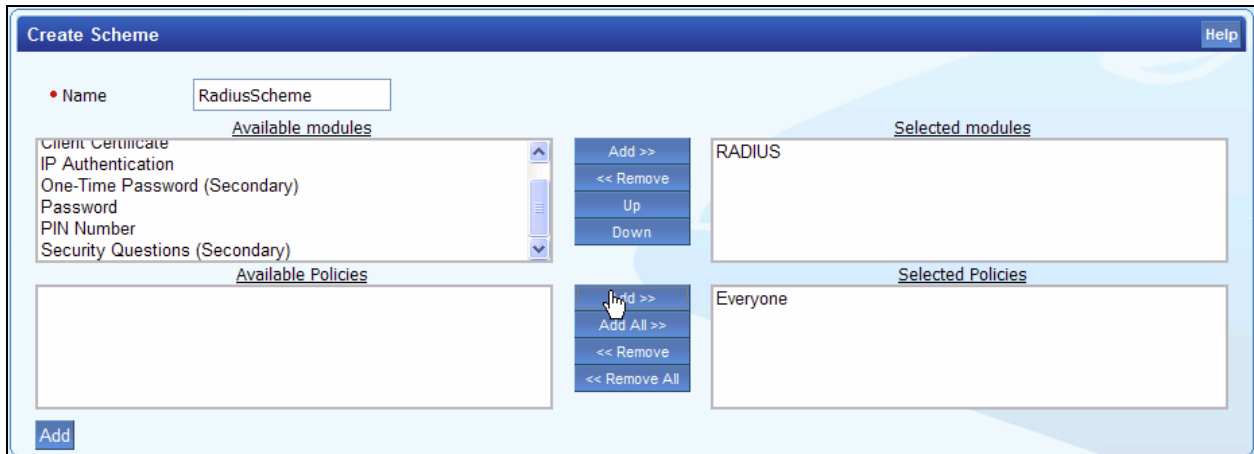
Challenge Image URL: A URL for generated challenge images. Leave blank to disable.

Allow Untrusted Challenge Image URL: Yes No Allow Challenge Images to be server from untrusted servers.

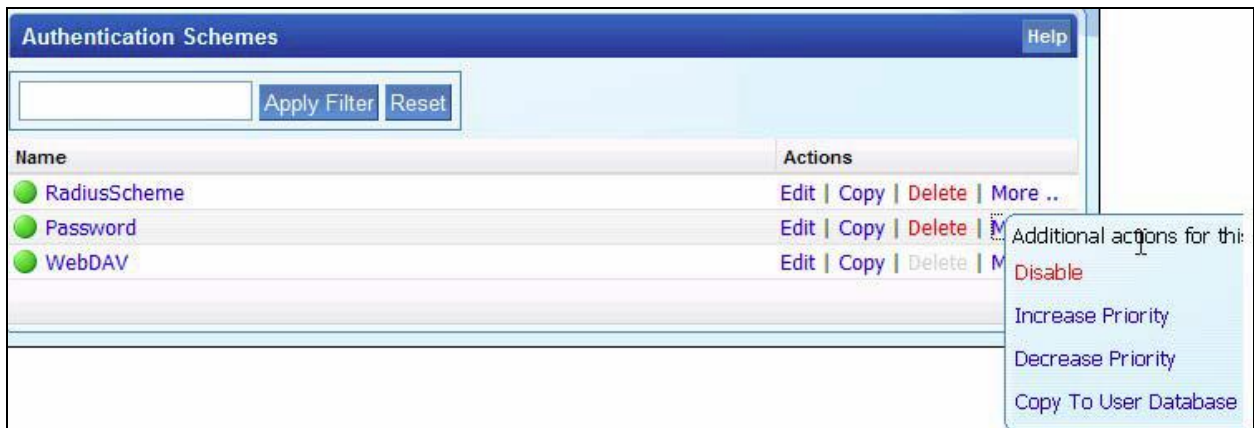
2. Enter appropriate details for the SecurID server such as **RADIUS Server, Shared Secret, Authentication Method**.

 **Note:** If you are using **Secondary failover servers**, it is recommended to **decrease the timeout to 10 seconds from the default 30** and **decrease the number of retries to 1** also set the **Reject Challenge** option to **No**. Without this, you will not get prompts to change PINs etc.

3. Create an Authentication Scheme using the RADIUS module. As ssladmin, navigate to **Access Control > Authentication Schemes** and create a new Authentication Scheme, this must contain at least the RADIUS module, but you may add more if you wish to have multi factor authentication. Assign this to a Policy to provide access to this scheme for your users and click **Add**.



4. Once created, if you wish this new scheme to be the default, click **More...** next to its name and move it to the top of the list.



- Next, create a user account to match the RADIUS login name. Navigate to the **ACCESS CONTROL** tab and select **Accounts**. Alternatively if you're using an Active Directory or LDAP server, ensure this account exists on that user database.
- Enter a **username** and **password** and click **add**. You are now ready to test the RADIUS login account.

The screenshot displays the Barracuda Networks SSL VPN 480 web interface. At the top left is the Barracuda Networks logo. The top right shows the user 'ssladmin' with a 'Logoff' link and a 'Manage Account' link. Below the logo are navigation tabs: 'BASIC', 'RESOURCES', 'ACCESS CONTROL' (selected), and 'ADVANCED'. A secondary navigation bar contains 'Accounts', 'Groups', 'Policies', 'User Databases', 'Access Rights', and 'NAC'. Underneath this are sub-tabs: 'NAC Exceptions', 'Authentication Schemes', 'Security Settings', 'Configuration', and 'Sessions'. The main content area is divided into two sections. The first section, 'Create Account', includes input fields for Username, Password, Email, Full Name, and Confirm Password. There is a checkbox for 'Force user to change password at next login' and a list of 'Available Groups' with an 'Add >>' button. A 'Selected Groups' list is also present with a '<< Remove' button. An 'Add' button is at the bottom left of this section. The second section, 'Accounts', features a search filter with 'Apply Filter' and 'Reset' buttons, and a 'Show All' dropdown. Below this is a table of accounts:

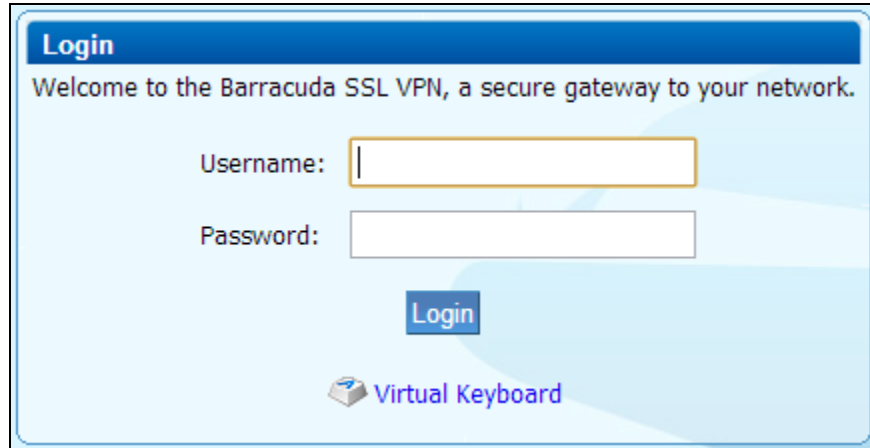
Name	Full Name	Email	Status	Actions
cdakin_barracuda	cdakin_barracuda		Enabled	Edit Enable Disable Delete More ..

- To successfully get prompted for SecurID Next Tokencode Mode you will need to increase the number of failed logon attempts. Navigate to **Access Control > Security Settings**. In the Password Options section, increase the value of **Max. logon attempts before lock** to at least 5 .

Password Options		Save Changes	Help
Max. logon attempts before lock	<input type="text" value="5"/>	The maximum number of logon attempts before the logon is temporarily locked. Use a value of zero to disable all account locking features.	
Max. locks attempts before disable	<input type="text" value="3"/>	The maximum number of temporary locks before the account is permanently disabled. Use a value of zero to never lock accounts.	
Lock duration (secs)	<input type="text" value="300"/>	How long (in seconds) a temporary lock should last before the user can attempt authentication again.	
Password pattern	<input type="text" value=".{5,}"/>	A regular expression describing the requirements for a user password.	
Password pattern description	<div>Password must be at least five characters in length</div>	The text that will be displayed to the user describing the requirements for a password.	
Days before expiry warning	<input type="text" value="21"/>	The number of days before password expiry from which a warning will be shown. If you do not want users to receive a warning you should set this value to zero.	
Maximum password age	<input type="text" value="28"/>	The number of days from when a user changes their password until it will expire. If you do not want users to change their password you should set this value to zero.	

RSA SecurID Login Screens

Login screen:




Login

Welcome to the Barracuda SSL VPN, a secure gateway to your network.

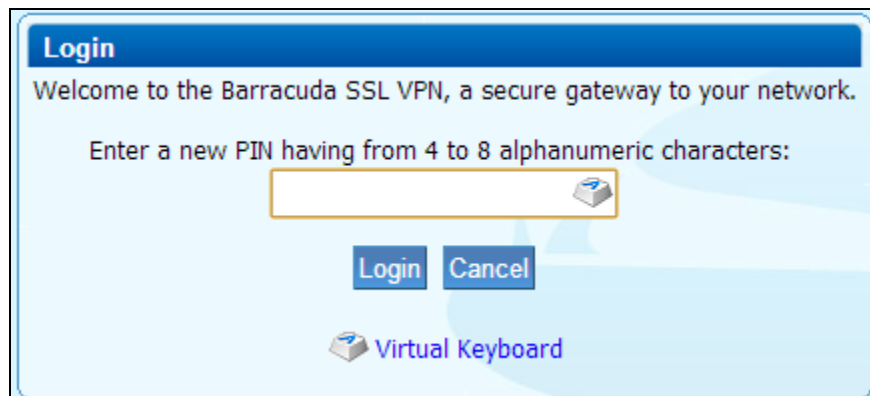
Username:

Password:

Login

 [Virtual Keyboard](#)


User-defined New PIN:




Login

Welcome to the Barracuda SSL VPN, a secure gateway to your network.

Enter a new PIN having from 4 to 8 alphanumeric characters:



Login **Cancel**

 [Virtual Keyboard](#)


PIN Accepted, wait for change:

Login

Welcome to the Barracuda SSL VPN, a secure gateway to your network.

PIN Accepted. Wait for the token code to change, then enter the new passcode:

[Login](#) [Cancel](#)

 [Virtual Keyboard](#)


System-generated New PIN:

Login

Welcome to the Barracuda SSL VPN, a secure gateway to your network.

Are you satisfied with system generated PIN cyDqPSj ? (y/n):

[Login](#) [Cancel](#)

 [Virtual Keyboard](#)


Next Tokencode:

Login

Welcome to the Barracuda SSL VPN, a secure gateway to your network.

Wait for token to change, then enter the new tokencode:

[Login](#) [Cancel](#)

 [Virtual Keyboard](#)

Certification Checklist for RSA Authentication Manager

Date Tested: October 24, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
Barracuda SSL VPN	2.4.0.9	Linux

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 PIN Reuse	N/A	Deny 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	✓
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

GLS / PAR

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