# Barracuda Networks
## SSL VPN

# 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. |

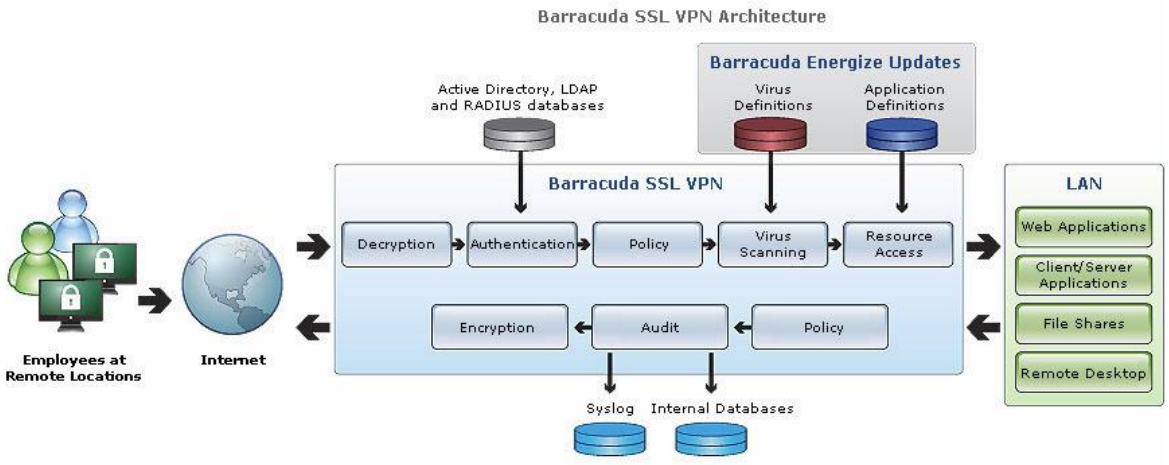
# Solution Summary

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<br>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*

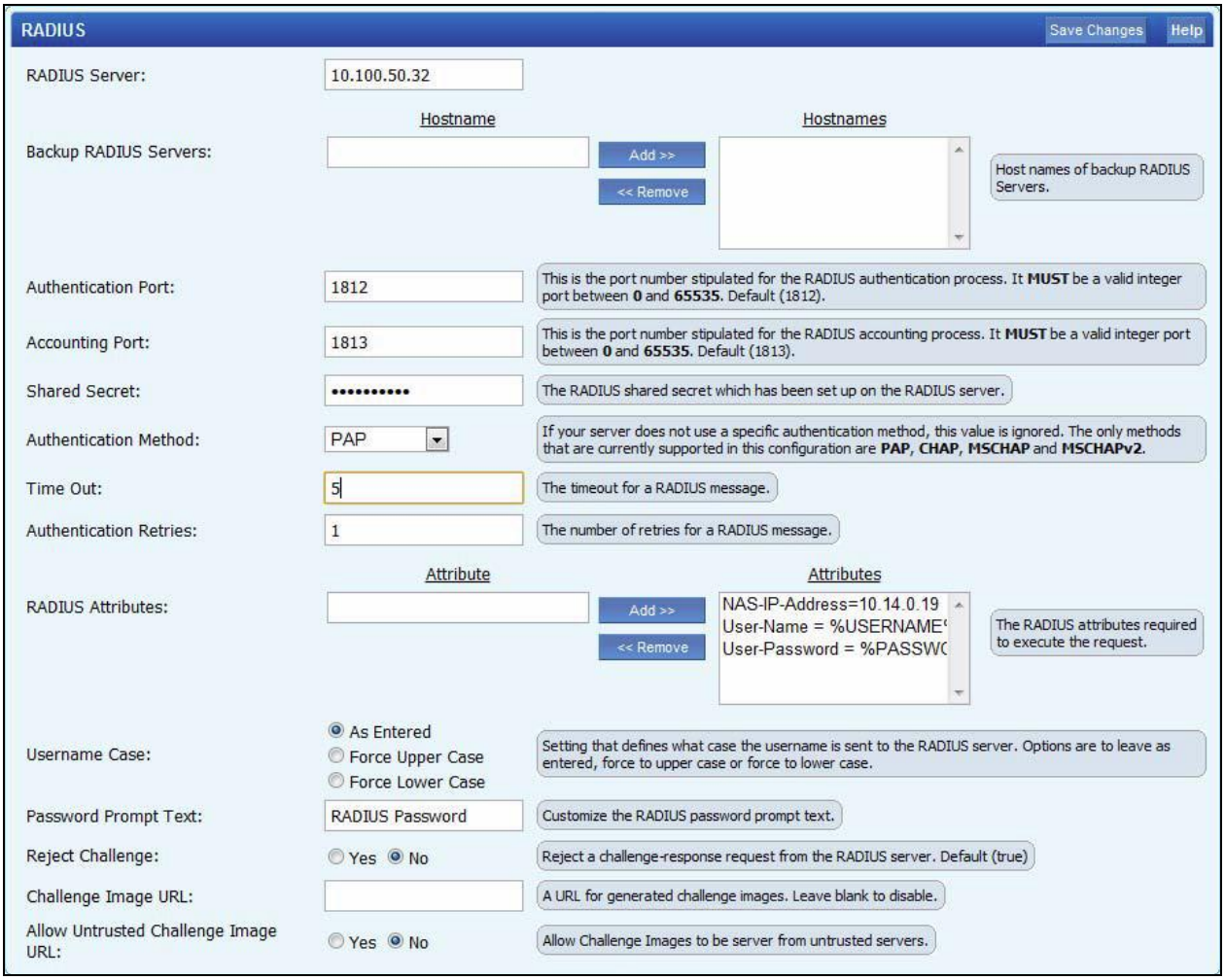
This section provides instructions for configuring the Barracuda SSL VPN with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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

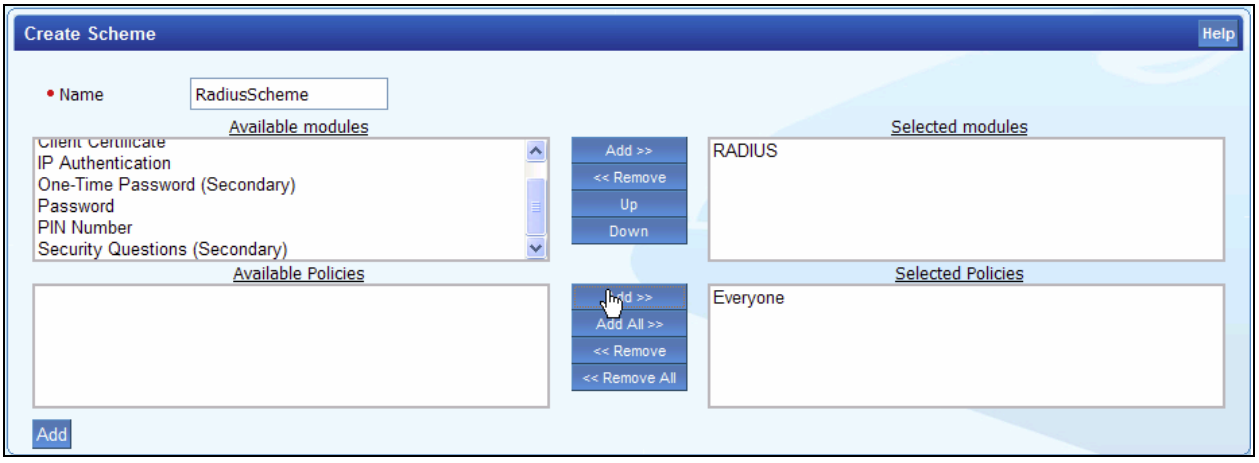
1. Configure RADIUS settings. Log on to Barracuda SSL VPN as ssladmin, navigate to **Access Control > Configuration** and scroll down to the RADIUS section.



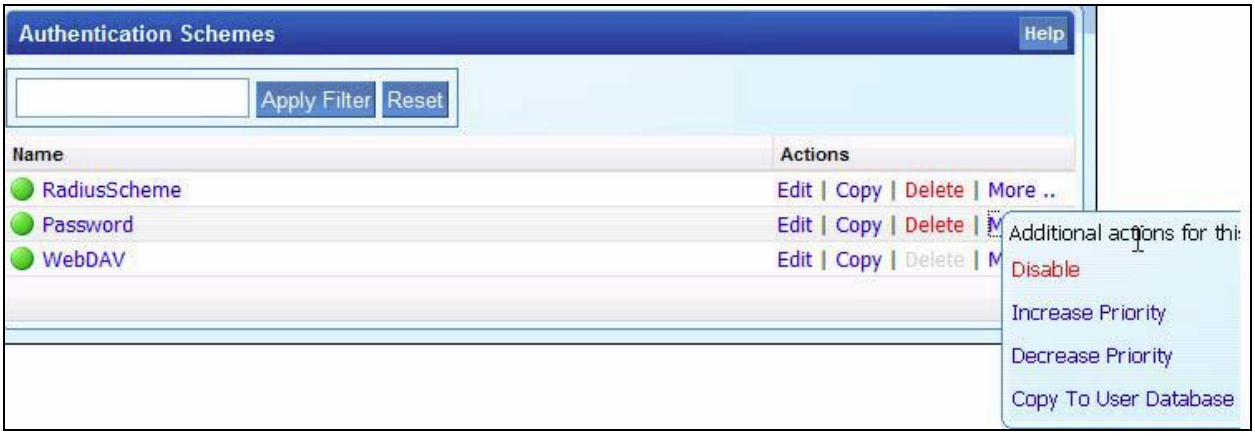
2. Enter appropriate details for the SecurID server such as **RADIUS Server, Shared Secret, Authentication Method**.

> **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.**

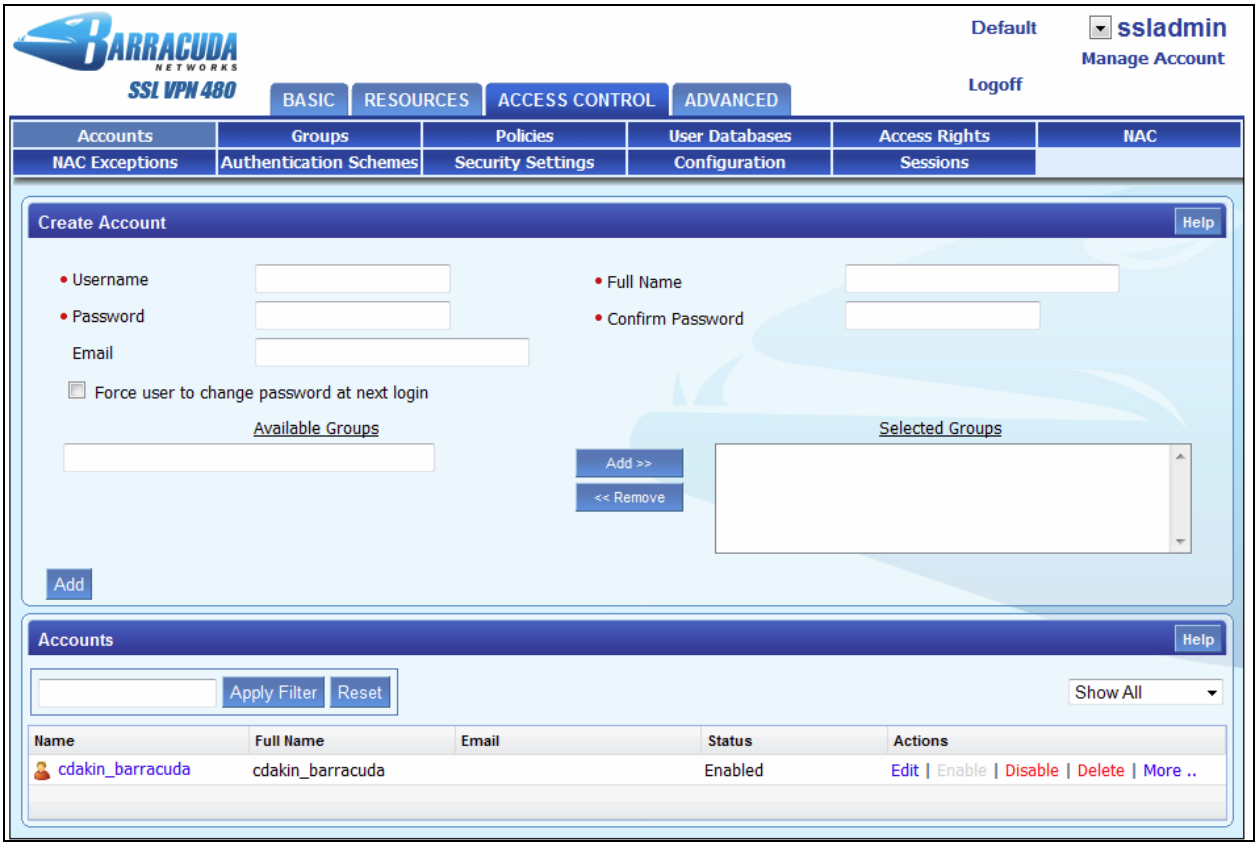
3. Create an Authentication Scheme using the RADIUS module. As ssladmin, navigate to **Access Control > Authentication Schemes** and create a new Authentication Scheme, this must contain at least the RADIUS module, but you may add more if you wish to have multi factor authentication. Assign this to a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



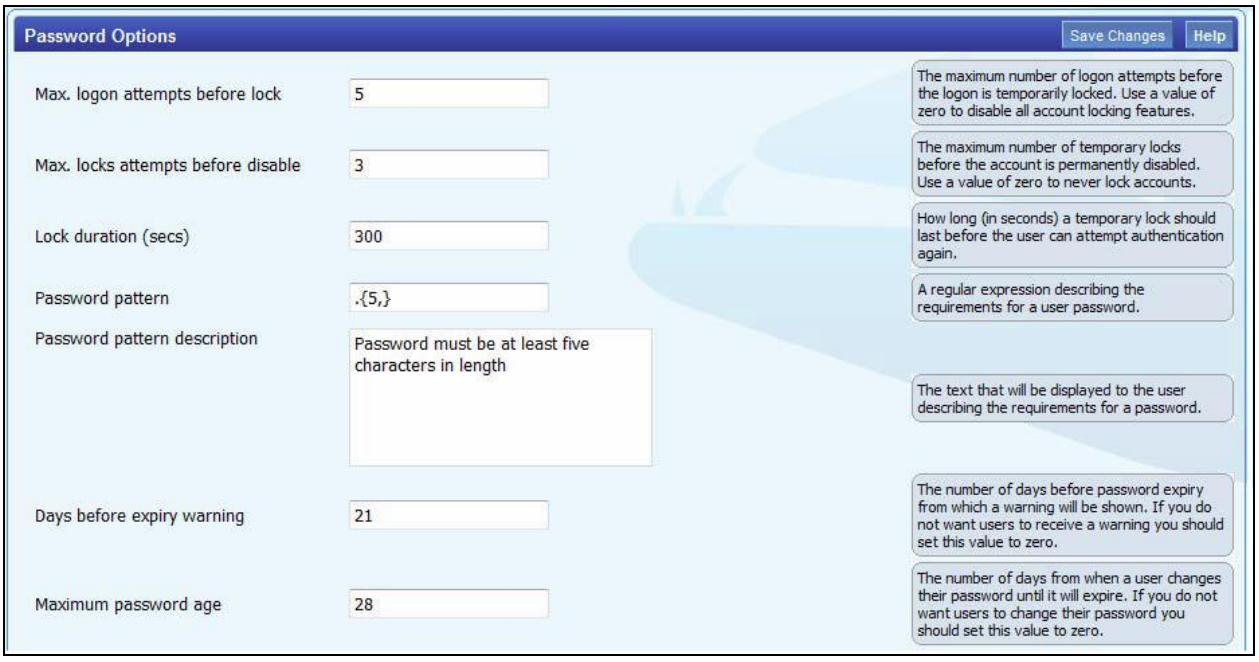

4. Once created, if you wish this new scheme to be the default, click **More**... next to its name and move it to the top of the list.



5. 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.
6. Enter a **username** and **password** and click **add.** You are now ready to test the RADIUS login account.

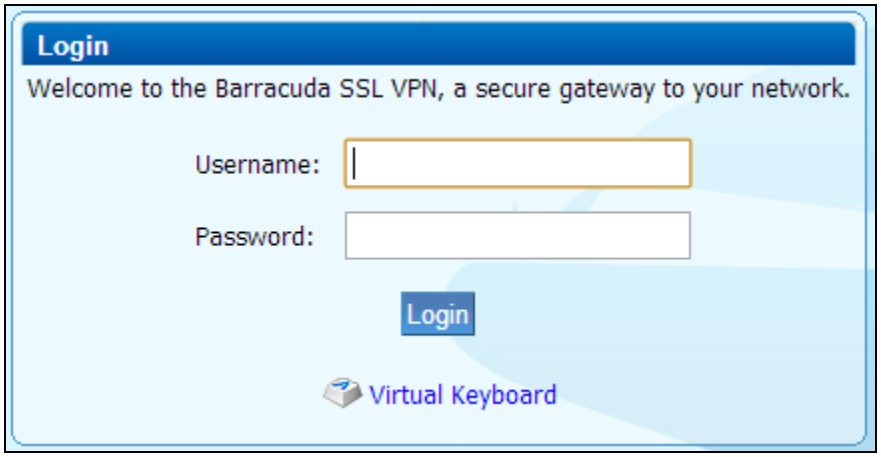


7. To successfully get prompted for SecurID Next Tokencode Mode you will need to increase the number of failed logon attempts. Navigate to **Access Control > Security Settings**. In the Password Options section, increase the value of **Max. logon attempts before lock** to at least 5 .

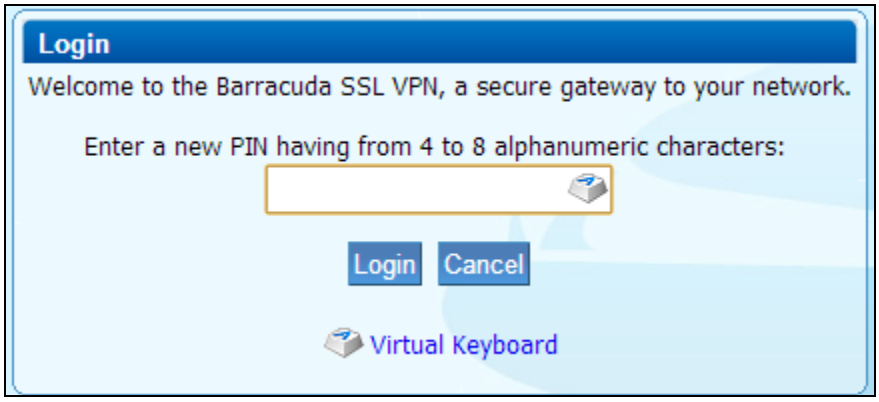


## RSA SecurID Login Screens

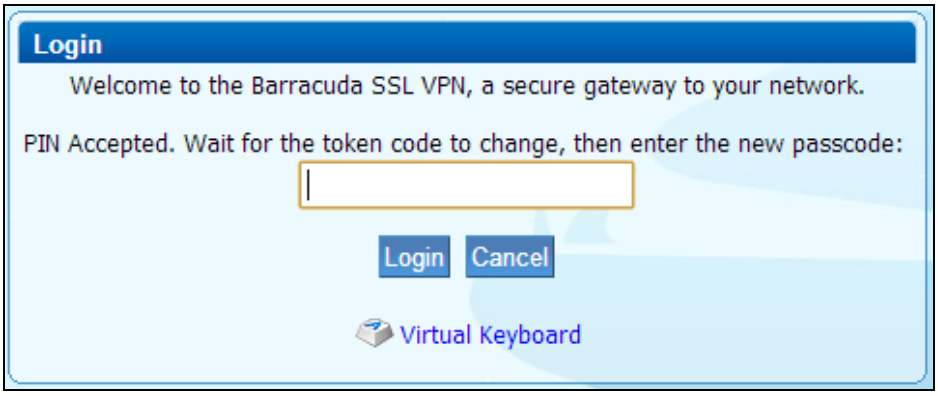
Login screen:



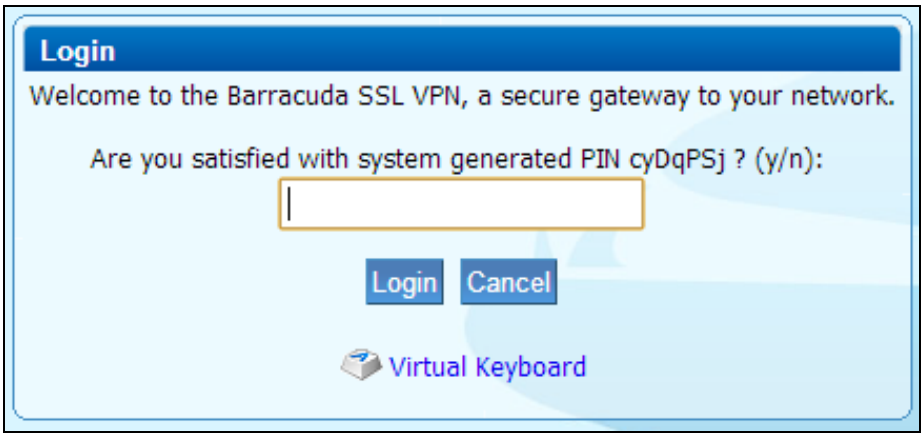

User-defined New PIN:



PIN Accepted, wait for change:




System-generated New PIN:




Next Tokencode:

# 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