Barracuda Networks
Web Application Firewall

RSA SecurID Ready Implementation Guide

Last Modified: November 27, 2013

Partner Information

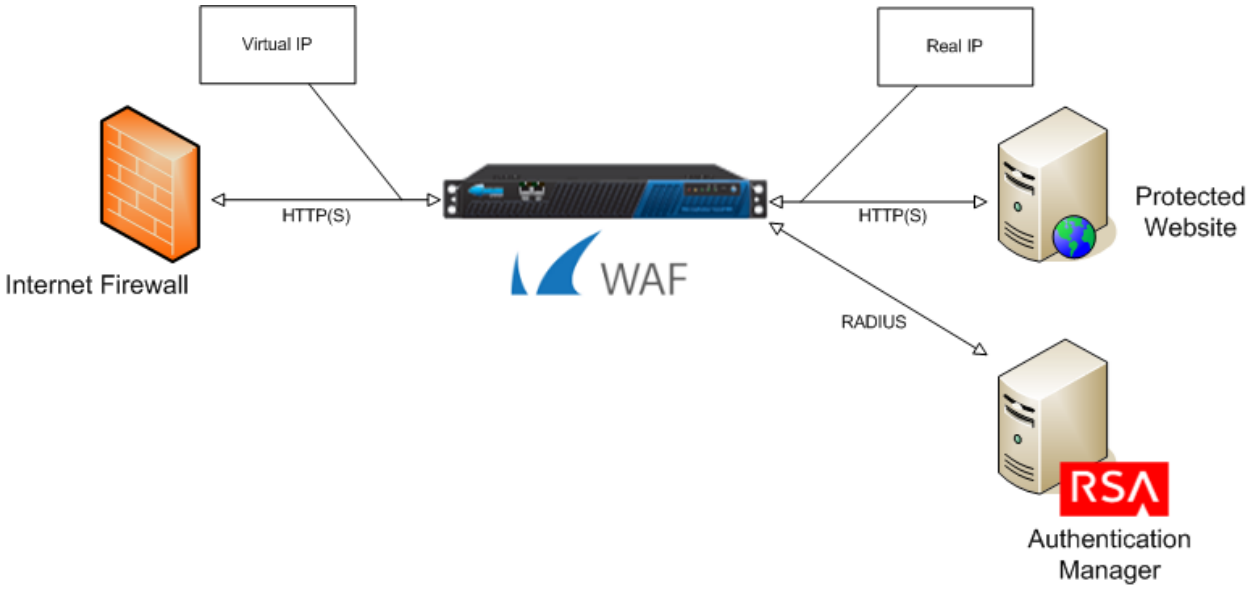
Product Information	
Partner Name	Barracuda Networks
Web Site	www.barracuda.com
Product Name	Web Application Firewall
Version & Platform	7.8.1, Model V660
Product Description	The Barracuda Web Application Firewall offers the capability to secure, deliver, and manage enterprise Web applications from a single appliance through an intuitive, real-time user interface.

Solution Summary

The Barracuda Web Application Firewall (WAF) protects websites from attackers leveraging protocol or application vulnerabilities including data theft, denial of service (DoS), unauthorized access and website defacement.

The Barracuda Web Application Firewall provides advanced protection via RSA two factor authentication. The Barracuda WAF is designed to enforce policies for both internal and external data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

RSA Authentication Manager supported features Web Application Firewall 7.8.1	
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	No
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 Web Application Firewall will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Web Application Firewall 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 Web Application Firewall 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 the Web Application Firewall components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Barracuda Web Application Firewall for SecurID Authentication

Create a New Service on the Barracuda Web Application Firewall

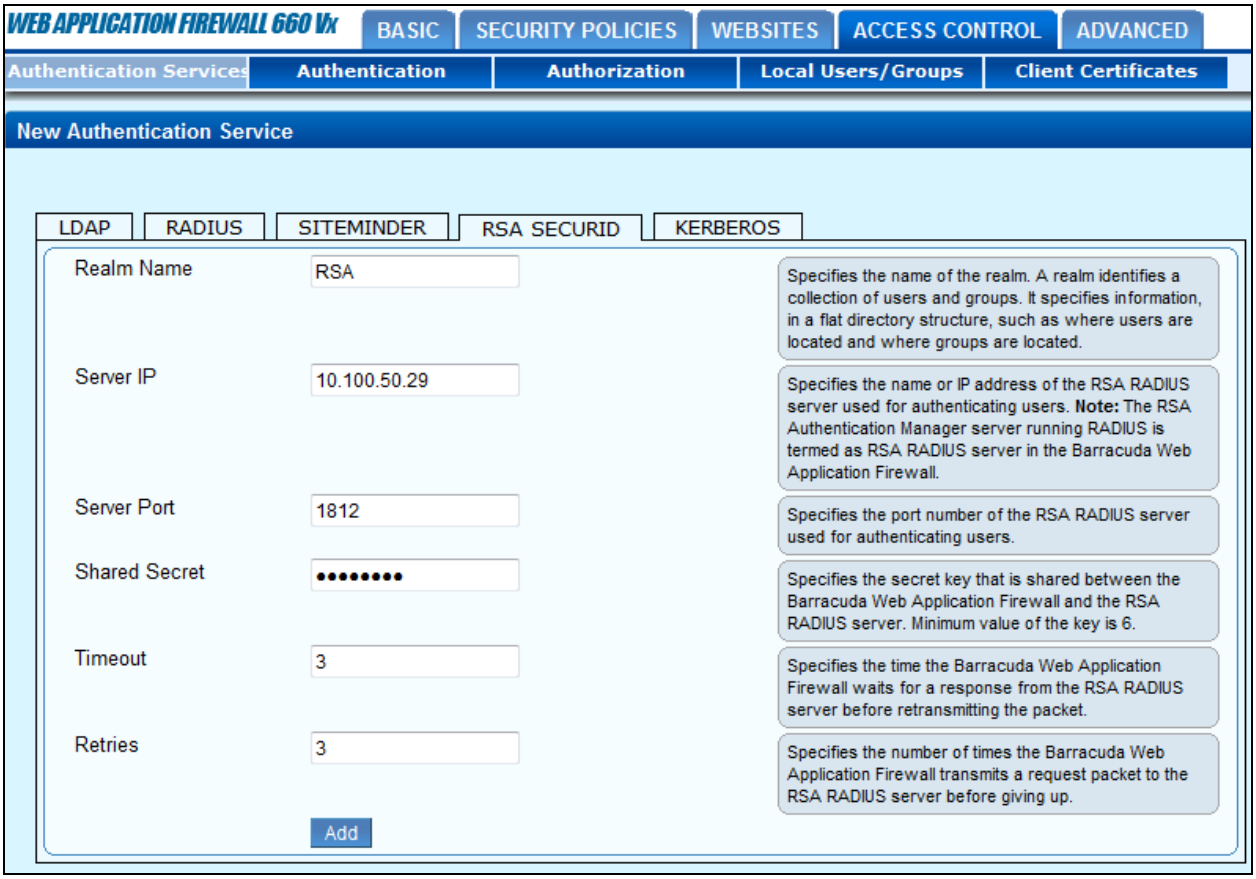
1. Log on to the Barracuda Web Application Firewall by using a supported Web browser.
2. From the **BASIC** tab, select the **Services** page.
3. In the **Add New Service** section, specify values for the following fields:

   - **Service Name**: Enter the name to identify this service on the Barracuda Web Application Firewall.
   - **Type**: Select HTTP from the drop-down list.
   - **Virtual IP**: Enter the IP address of the service. If the IP address is specified for the first time, a new Virtual IP is created and a Netmask will be automatically assigned based on the class of the IP address specified. If the Netmask is inappropriate, you need to create the Virtual IP first (where you can specify the Netmask) and then use that IP address in the service creation. The Virtual IPs can be added or managed on the **ADVANCED** > **Advanced IP Config** page.
   - **Port**: Enter the port number for the service. Port 80 is the default port for the HTTP Service.
   - **Real Server**: Enter the IP address of the server that hosts the service.

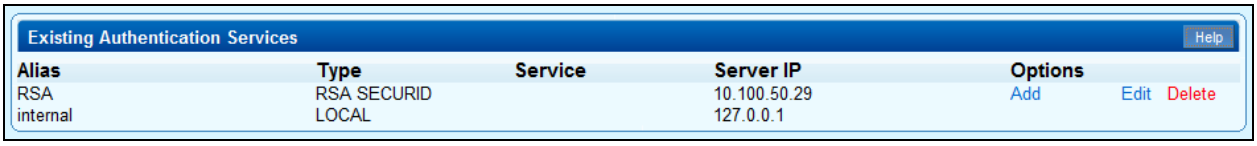
4. Click **Add** to add the service.

Configure the Authentication Service on the Barracuda

1. From the **ACCESS CONTROL** tab, select the **Authentication Services** page.
2. Select **RSA SecurID** under the **New Authentication Service** section.

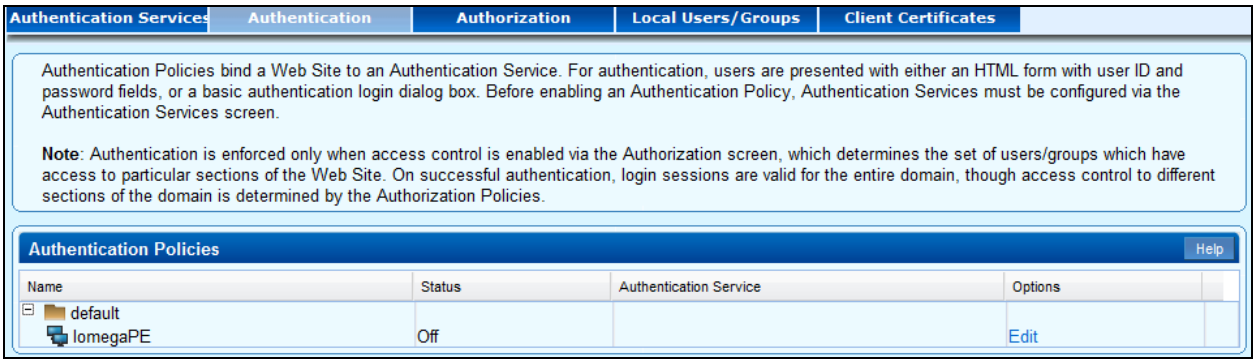


3. Enter values for all the fields.
4. Click **Add**.
5. The Authentication Services will appear in the Exiting Authentication Services table, click **Add** under **Options** to add a secondary RADIUS server to this service.

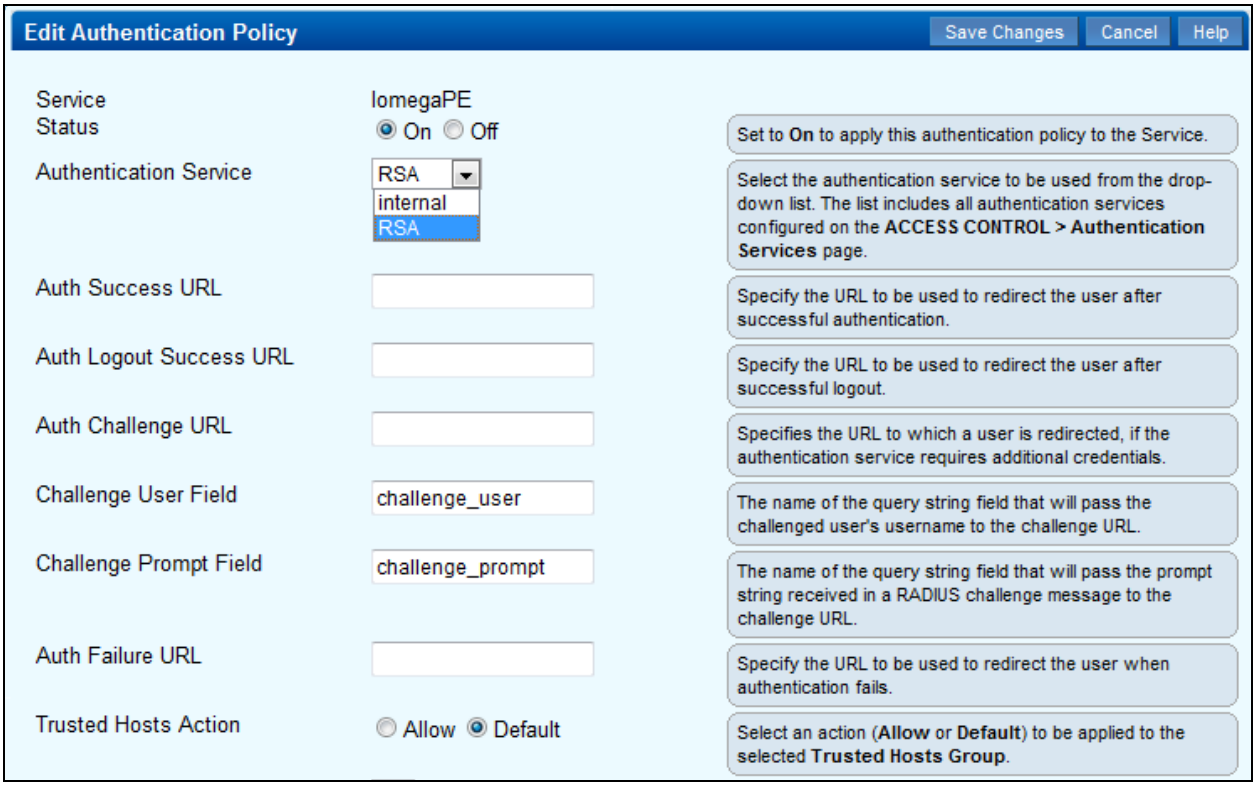


Bind the New Service with the Authentication Service

1. From the **ACCESS CONTROL** tab, select the **Authentication** page.
2. Under the **Authentication Policies** section, click **Edit** against the service for which you want to configure RSA SecurID authentication.



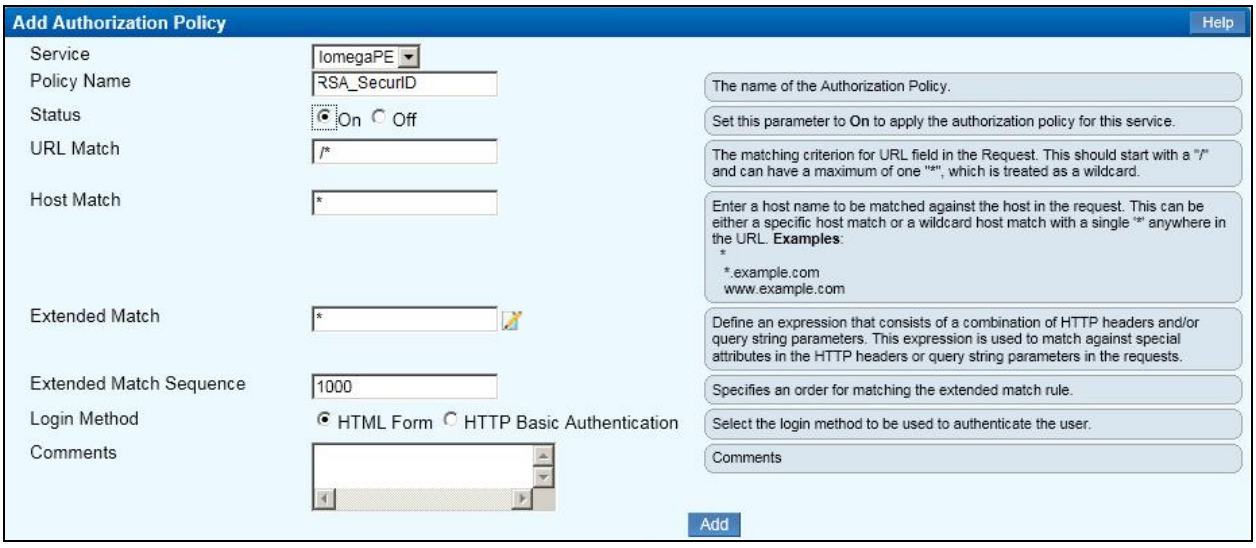
3. The **Edit Authentication Policy** window appears. Specify values for the following fields:
   - Set the **Status** '**On**' to enable authentication for this service.
   - Select the RSA Authentication Service you created on the **ACCESS CONTROL** > **Authentication Services** > **RSA SecurID** page from the **Authentication Service** drop-down list.
   - Specify value for other parameter(s). Click the help button to get more information about how to configure an authentication policy.



4. Click **Save Changes**.

Configure the Authorization Policy for the Service

1. From the **ACCESS CONTROL** tab, select the **Authorization** page.
2. In the **Add Authorization Policy** window, enter a **Policy Name**.
3. Change the **Status** to **On**.
4. Enter a **URL Match** value.



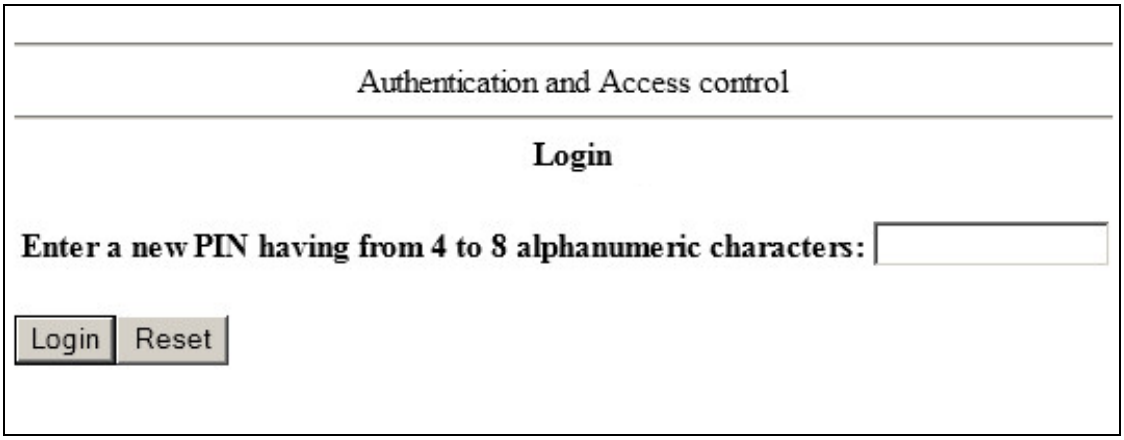
5. Click **Add** to add the Authorization policy configuration.

When a user attempts to access a protected resource, the Barracuda Web Application Firewall displays the login page to authenticate a user. If the URL Match is configured as “/*”, it will display the login page for any request sent to the service.

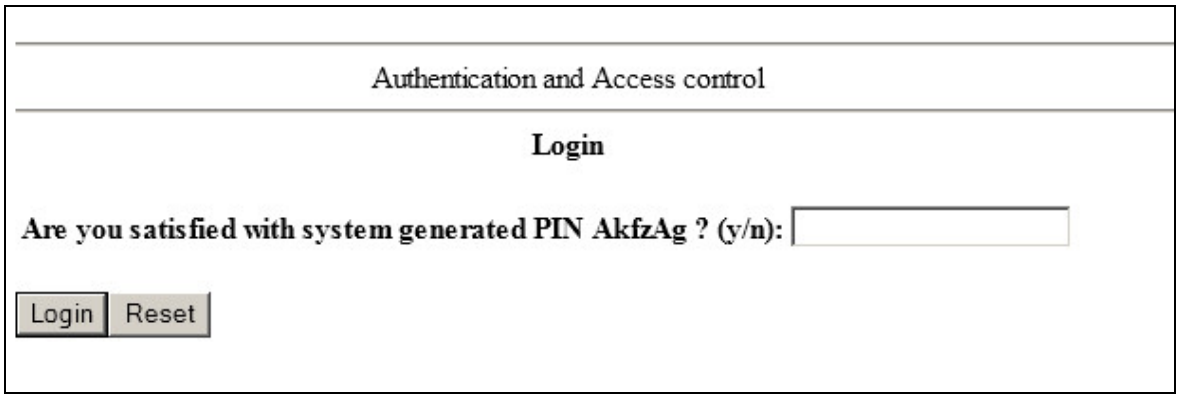
RSA SecurID Login Screens

Login screen:

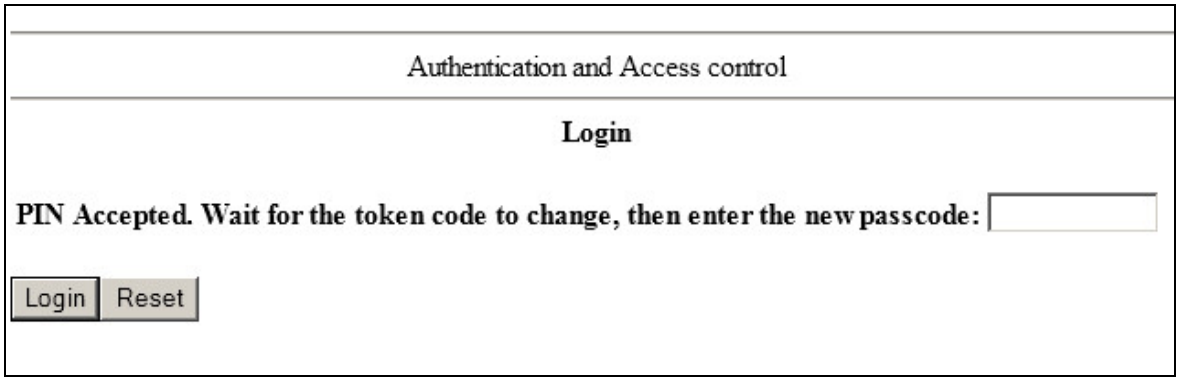
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: November 27, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Web Application Firewall	7.8.1	Proprietary OS

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

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