



RSA SecurID Ready Implementation Guide

Last Modified: April 18, 2005

Partner Information

Product Information	
Partner Name	F5 Networks
Web Site	http://www.f5.com/
Product Name	FirePass
Version & Platform	v5.4.1
Product Description	<p>F5's FirePass controller enables enterprises to provide secure, reliable and intuitive remote access to corporate applications and data using standard web browser technology, without the headaches associated with time-consuming client software installation and configuration, or changes to server-side applications.</p> <p>FirePass is the first SSL VPN solution with complete cross-platform support. Extending its support for any IP application to Apple Macintosh, PocketPC and Linux clients, in addition to Microsoft Windows, and expanding client and application security for web, email and file application access, FirePass delivers the industry's most ubiquitous solution for secure network access.</p> <p>It also offers the only open API and SDK that enables 3rd party application vendors to build seamless, secure remote access into their client applications.</p>
Product Category	Perimeter Devices (Firewalls, VPNs and ID)

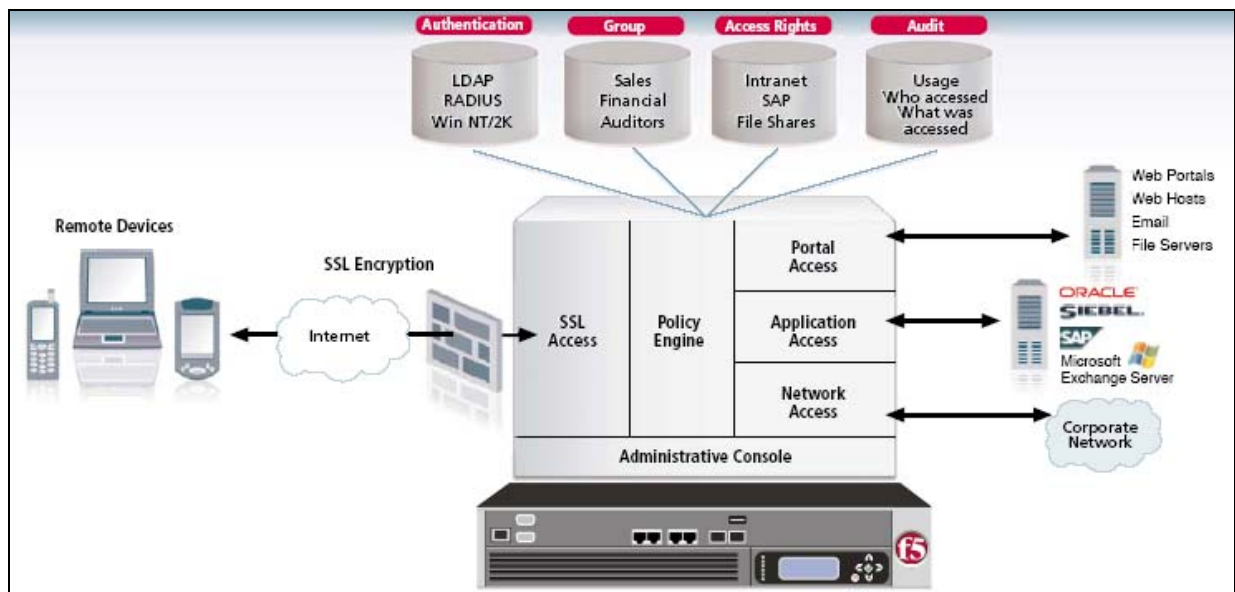


Solution Summary

The FirePass controller features broad, flexible authentication options. The FirePass device can easily be configured to work with RADIUS, and its Native Protocol support for RSA SecurID Authentication allows the FirePass to be deployed without requiring configuration changes on the existing authentication deployment. The FirePass controller also supports RSA advanced features. Organizations using the FirePass controller with RSA SecurID benefit from increased security, easier management, and a lower total cost of ownership.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS
List Library Version Used	5.03
RSA Authentication Manager Name Locking *	Yes
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes (3)
Location of Node Secret on Agent	/usr/local/uroam/var/ace/server_name
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

* = Mandatory Function when using Native SecurID Protocols



Product Requirements

Partner Product Requirements: FirePass Appliance	
Firmware Version	5.4.1

Agent Host Configuration

To facilitate communication between the FirePass Appliance 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 FirePass Appliance within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the FirePass Appliance as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the FirePass Appliance will occur.

 **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 records.

Partner Authentication Agent 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.

RADIUS Authentication Support

1. Log into the FirePass Administrator Console. The administrator console can be reached using the following syntax: **https://firepass.mycompany.xyz/admin/**.
2. From the left navigation, click **Users > Groups > Master Groups**, and then click the **Create New Group** button. The Create New Group screen opens.
3. In the **Name** box, type a name for this group.
4. From the **Users in Group** list, select the setting appropriate for your configuration. For this guide, we select **External**.
5. From the **Authentication method** list, select **RADIUS**.
6. Leave the **Copy settings from** list at the **Do not copy** option. Click the **Create** button. The Master Group configuration screen opens.
7. From the Master Group configuration page, click the **Authentication** tab.
8. In the Primary Radius Server section, in the **Server** box, type the IP address of the Primary RADIUS Server.
9. In the **Port** box, type the RADIUS port number (**1645** by default on RSA servers, it can be changed to **1812** which is the RFC default port for RADIUS).
10. In the **Shared Secret** boxes, type and then confirm the shared secret.

The screenshot displays the 'Users : Groups : Master Groups' configuration page. The 'Authentication' tab is selected, showing 'RADIUS Authentication' settings. The 'RADIUS settings' section includes 'Timeout' (5), 'Retries' (5), and 'Service Type (optional)' (Default). The 'Primary RADIUS server' section includes 'Server' (10.4.11.26), 'Port' (1645), and 'Shared Secret' (masked with asterisks). There are checkboxes for 'Retrieve Single Sign On Password from RADIUS attribute' and 'Use a secondary RADIUS server'.

11. If applicable to your configuration, click a check in the Use a secondary RADIUS server box to configure a secondary RADIUS server. After configuring the secondary server, you can also click Use a tertiary RADIUS server to configure a tertiary RADIUS server.

After successfully configuring the server, RADIUS authentication is enabled. Users who are configured to use RADIUS authentication can sign in with their username and password.

Native RSA SecurID Authentication Support

Configure the FirePass controller to use the Authentication Manager.

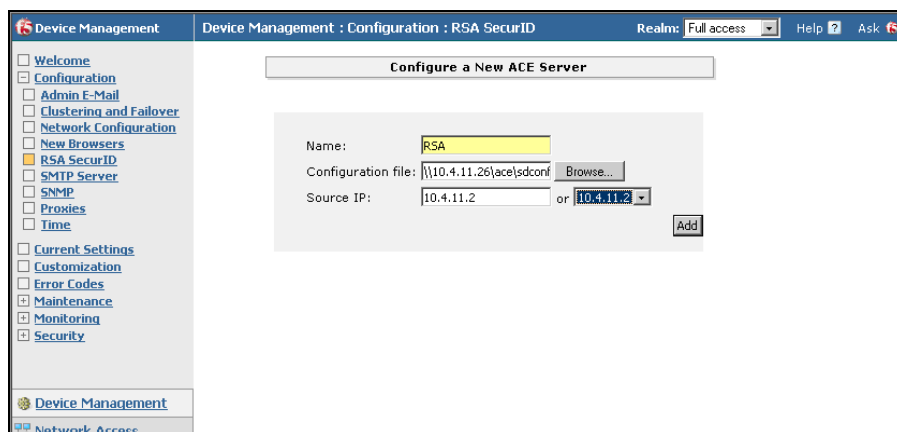
1. From the RSA Authentication Manger, locate and save the **sdconf.rec** file to a location you can access from the FirePass device.
2. Log into the FirePass Administrator Console. The administrator console can be reached using the following syntax: **https://firepass.mycompany.xyz/admin/**.
3. From the left navigation, click Device Management > Configuration > RSA SecurID screen. The Configure a New Ace Server screen opens.
4. In the Name box, type a name for identifying the RSA Authentication Manager configuration on the FirePass controller.
5. In the **Configuration file** box, click the **Browse** button to locate the RSA Authentication Manger configuration file (by default named **sdconf.rec**), in the location you saved it to in Step 1.
6. In the Source IP section, specify the **Source IP** address to be used for communicating with RSA Authentication Manager.

! Important: Because the FirePass controller is a multi-homed appliance with multiple IP addresses, this setting is very important. It must be the same address as the IP address you specified in the Network address field you entered while configuring FirePass as an agent host on RSA Authentication Manager.

To specify the Source IP

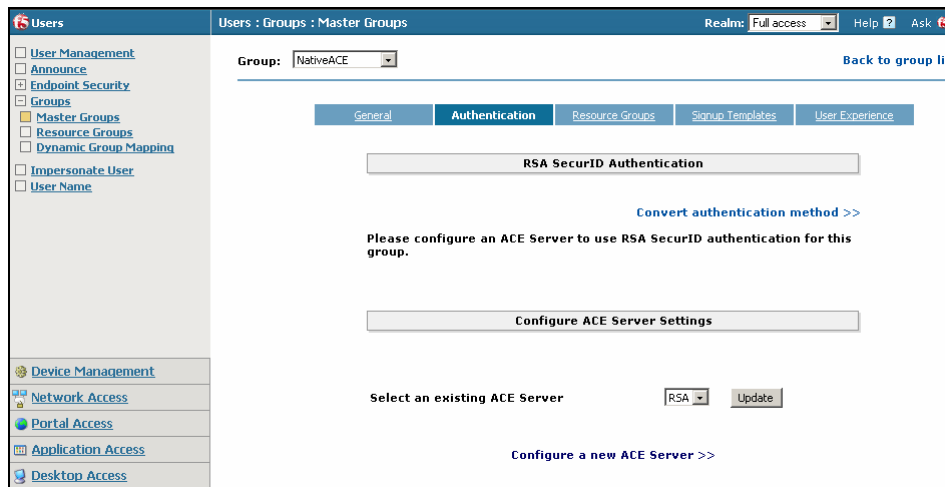
- If there is a NAT device in the network path between the FirePass and the RSA Authentication Manager, type the address as translated by the NAT device.
- Otherwise, select the IP address from among those configured on the FirePass controller.

Note: In all cases, this IP address *must match* the Source IP address in the IP packets received by the RSA Authentication Manager.

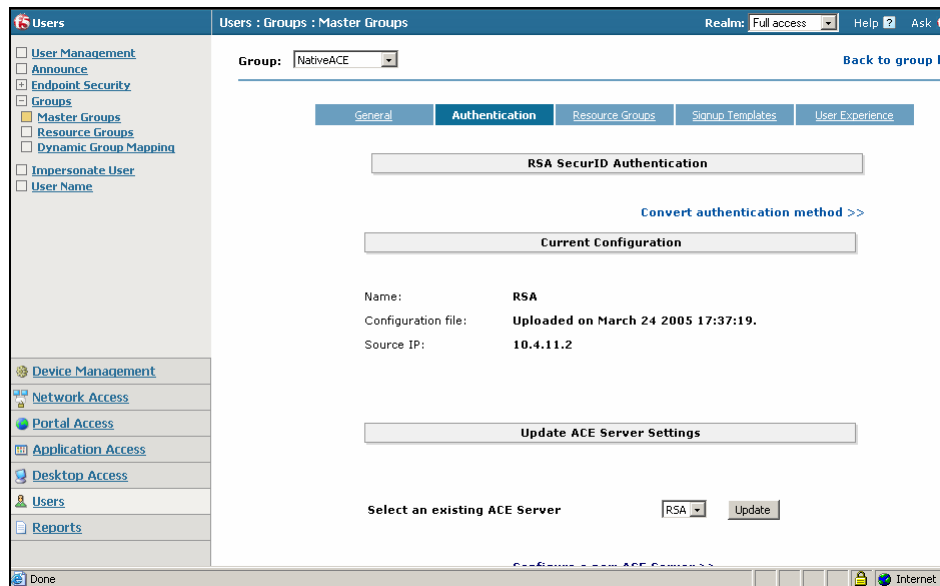


7. Click the **Add** button.

8. From the left navigation, click **Users > Groups > Master Groups**, and then click the **Create New Group** button. The Create New Group screen opens.
9. In the **Name** box, type a name for this group.
10. From the **Users in Group** list, select the setting appropriate for your configuration. For this guide, we select **External**.
11. From the **Authentication method** list, select **Native Ace**.
12. Leave the **Copy settings from** list at the **Do not copy** option. Click the **Create** button. The Master Group configuration screen opens.



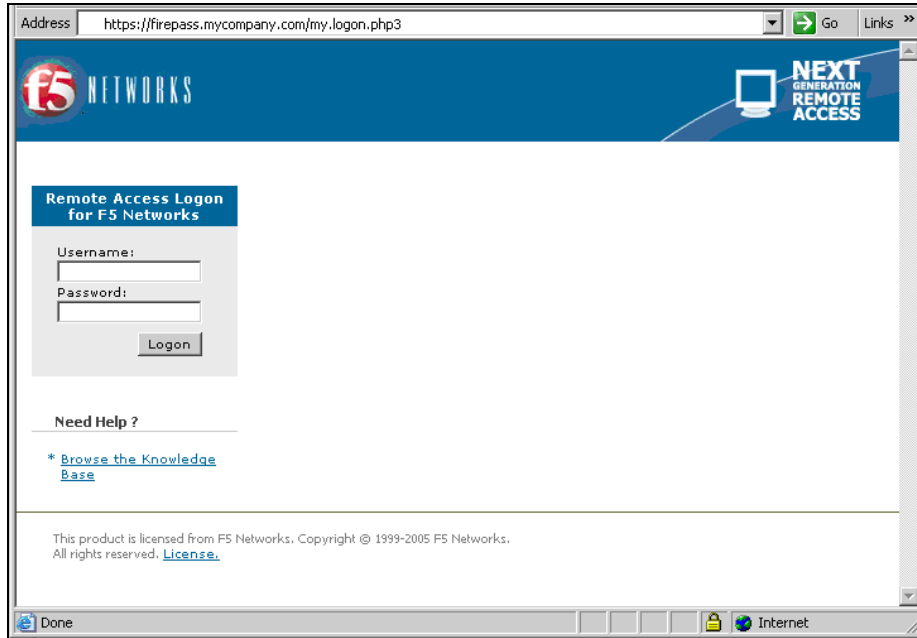
13. Click the **Authentication** tab.
14. Select an existing ACE Server from the list and click **Update**.



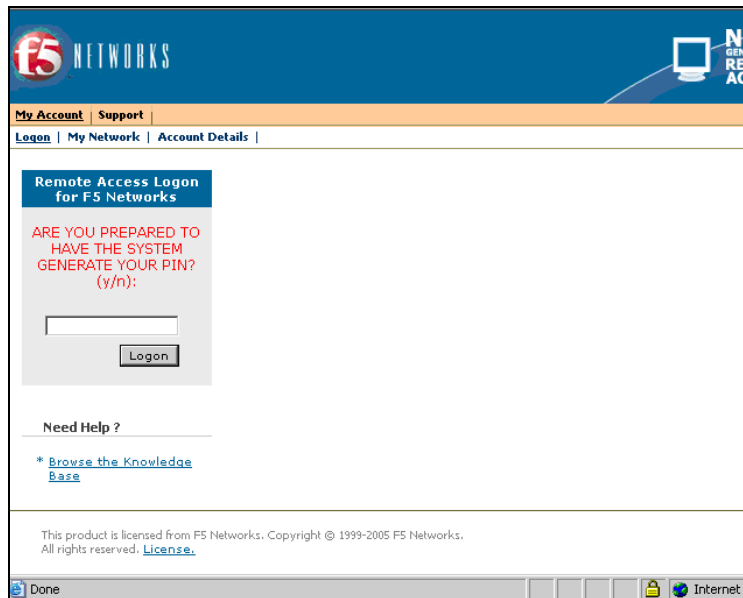
After successfully configuring the server, RSA SecurID Authentication is enabled on the FirePass controller. The server does not have to be restarted. The users configured to use RSA SecurID Authentication can login with their username and their SecurID PASSCODE, accordingly.

Authentication Examples

Login Screenshot



New PIN Mode – System Generated PIN Screenshots



f5 NETWORKS NE
GENI
REN
ACC

My Account | **Support**

[Logon](#) | [My Network](#) | [Account Details](#) |

Remote Access Logon for F5 Networks

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


Need Help ?

* [Browse the Knowledge Base](#)

f5 NETWORKS NE
GENI
REN
ACC

My Account | **Support**

System Generated PIN




The system will generate a new PIN for you. Click to see your PIN when you are ready.

Or press Cancel to return to sign-on page.

Done Internet

My Account | **Support**

System Generated PIN

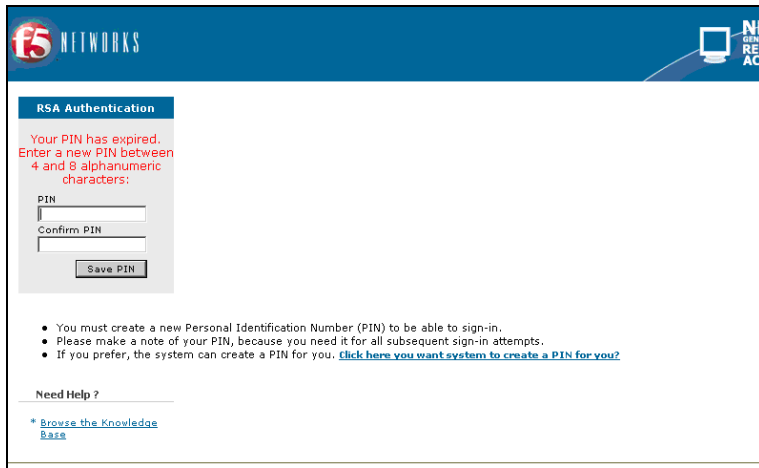


Your System Generated PIN is **kdi8**.

Please make a note of your new PIN because you need it for all subsequent sign-in attempts.

After you have memorized the new PIN, click continue to return to the sign-on page

New PIN Mode – User Generated PIN Screenshots



f5 NETWORKS NE
GENE
REP
ACT

RSA Authentication

Your PIN has expired.
Enter a new PIN between
4 and 8 alphanumeric
characters:

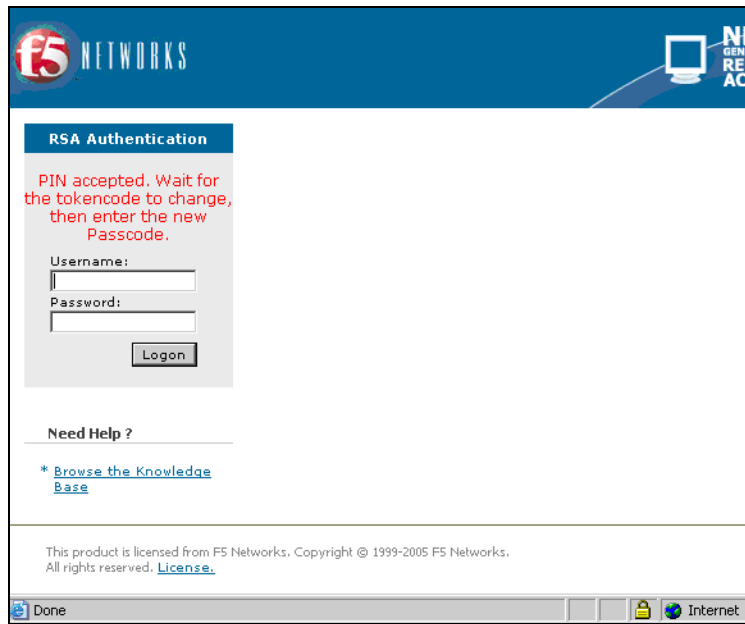
PIN

Confirm PIN

- You must create a new Personal Identification Number (PIN) to be able to sign-in.
- Please make a note of your PIN, because you need it for all subsequent sign-in attempts.
- If you prefer, the system can create a PIN for you. [Click here you want system to create a PIN for you?](#)

Need Help ?

* [Browse the Knowledge Base](#)



f5 NETWORKS NE
GENE
REP
ACT

RSA Authentication

PIN accepted. Wait for
the tokencode to change,
then enter the new
Passcode.

Username:

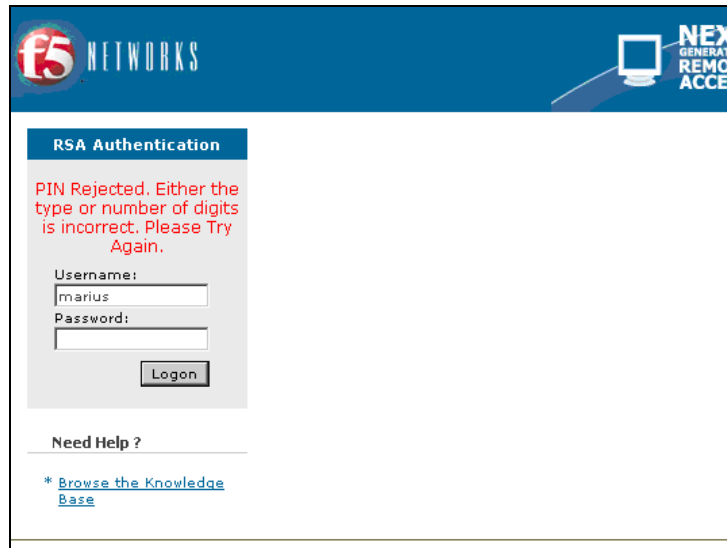
Password:

Need Help ?

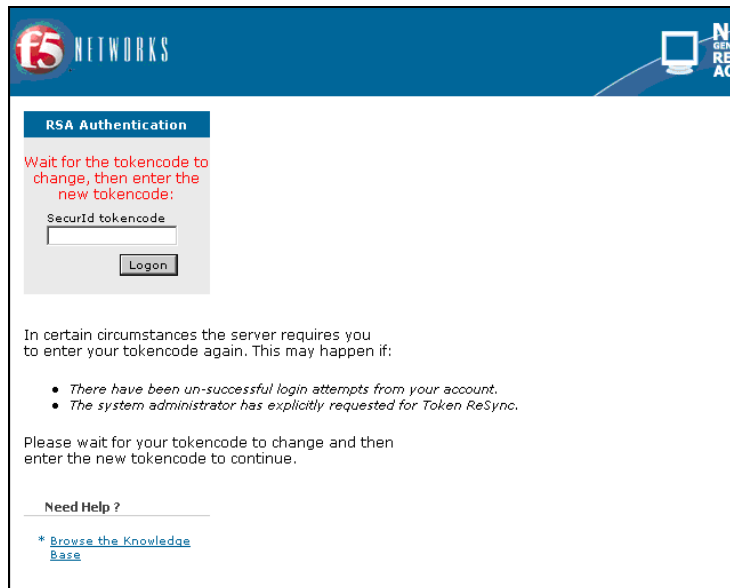
* [Browse the Knowledge Base](#)

This product is licensed from F5 Networks. Copyright © 1999-2005 F5 Networks.
All rights reserved. [License.](#)

Done Internet



Next Tokencode Mode Screenshot



Certification Checklist

Date Tested: April 7, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.0	Windows 2003 Server
F5 FirePass	5.4.1 Release	Integrated IOS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

PAR / EF

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

Known Issues

FirePass supports one primary and two back-up RADIUS servers. If the primary server is not available, first the secondary server, and then tertiary server, will be used.