RSA SecurID Ready Implementation Guide

Last Modified November 29, 2001

1. Partner Information

Partner Name	Stonesoft Corp.
Web Site	www.stonesoft.com
Product Name	StoneGate Firewall
Version & Platform	Version 1.6.3
Product Description	StoneGate is the first firewall and VPN solution offering high security, high performance and availability. It features: An embedded OS for increased security. Multiple ISP and VPN load balancing to ensure continuous network connectivity. Advanced centralized administration tools for enterprise - wide management of the firewall infrastructure.
Product Category	Firewall

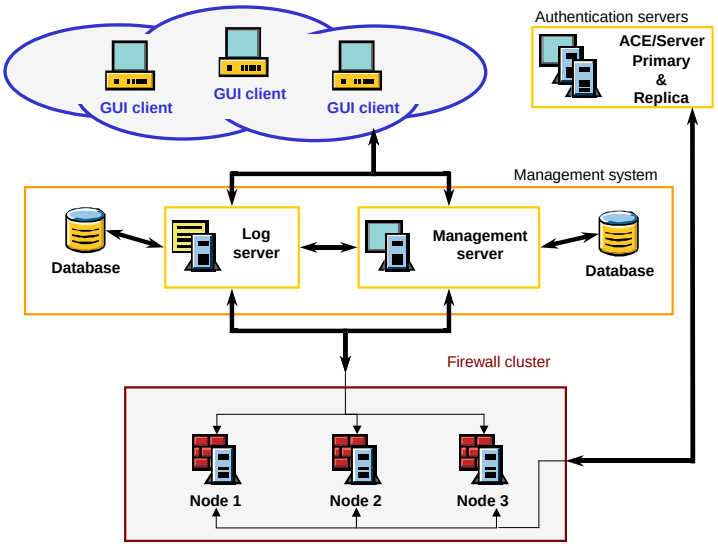
2. Contact Information

	Sales Contact	Support Contact
E-mail	sales@stonesoft.com	support@stonesoft.com
Phone	+358 9 4767 11	+358 9 4767 11
Web	www.stonesoft.com	www.stonesoft.com

3. Solution Summary

Feature	Details
Authentication Methods Supported	RADIUS, TACACS+.
ACE/Agent Library Version	N/A
ACE 5 Locking	N/A
Replica ACE/Server Support	N/A
Secondary RADIUS/TACACS+ Server Support	Yes (up to 10 supported)
Location of Node Secret on Client	None stored
ACE/Server Agent Host Type	UNIX Agent
SecurID User Specification	Designated users, all users, SecurID as default.
SecurID Protection of Administrators	No

StoneGate system architecture.



4. Product Requirements

- ***Hardware requirements***

Component Name: StoneGate Management system	
CPU make/speed required	Pentium processor, suggested minimum processor speed 500 MHz
Memory	128 MB minimum, 256 MB or more recommended
HD space	4GB for evaluation (20 GB or more for production use).

Component Name: StoneGate Firewall Engine	
CPU make/speed required	Pentium processor, suggested minimum processor speed 300 MHz
Memory	128 MB
HD space	1 GB

- ***Software requirements***

Component Name: StoneGate Management System	
Operating System	**Version (Patch-level)**
Windows NT 4.0	Service Pack 6a, English language version
Windows 2000	Service Pack 2, English language version
Sun Solaris	2.6 & 2.7
RedHat Linux	7.0 and 7.1, English language version

Component Name: StoneGate Firewall engine	
Operating System	**Version (Patch-level)**
Linux–based, provided with product	1.6.3

5. Partner ACE/Agent configuration

Supported authentication types with RSA SecurID product

Client-initiated authentication

Client initiated authentication means that the user starts the authentication process. It can be done with two tools: Authentication Client software (part of StoneGate VPN Client software) or using Telnet to connect to the firewall cluster on port 2543.

It is possible to authorize the client's IP address for a period of time with client initiated authentication. It is also possible to authorize the next opening connection from the client. The authorization part is specified in the access rule base.

Firewall-initiated authentication

Firewall-initiated authentication means that the firewall cluster starts the authentication process. It can be used only with the Authentication Client software. This software is part of StoneGate VPN Client software.

In firewall initiated authentication the firewall makes the connection to the client. This naturally requires that the client is reachable, e.g. there can't be NAT between firewall engine and the client.

With firewall initiated authentication it is also possible to authorize either the client's IP address or the current connection.

No software, other than StoneGate Management system and StoneGate firewall -engine are required to support Client initiated authentication, though the Authentication Client software included in the StoneGate VPN Client can be used.

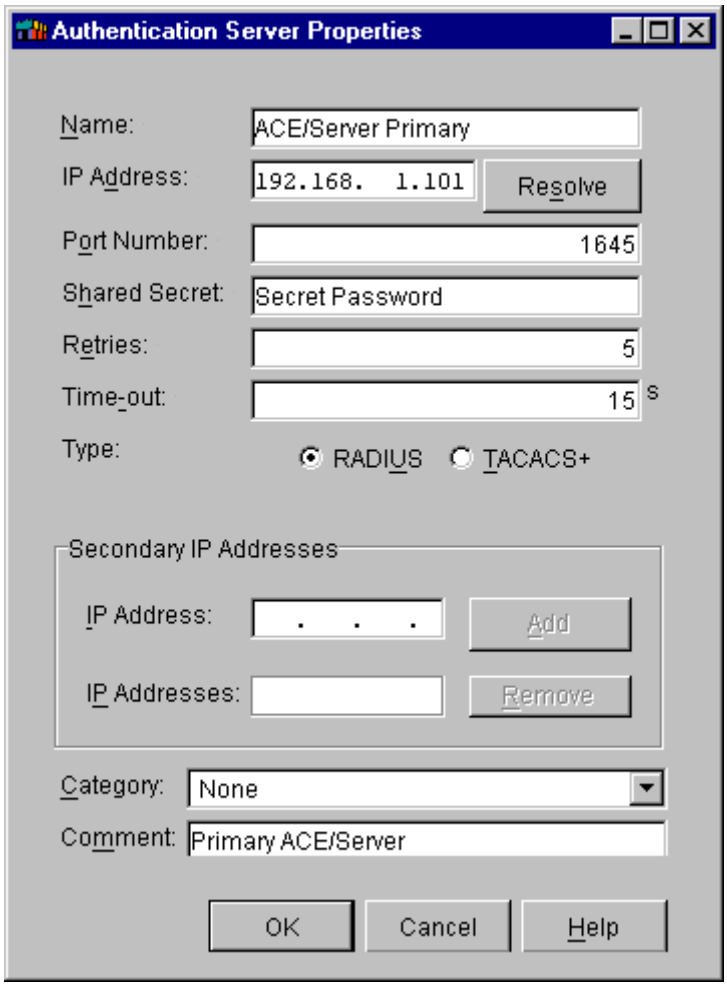
For Firewall initiated authentication support the StoneGate Authentication Client software MUST be used.

StoneGate Firewall / RSA SecurID Configuration – *User Authentication*

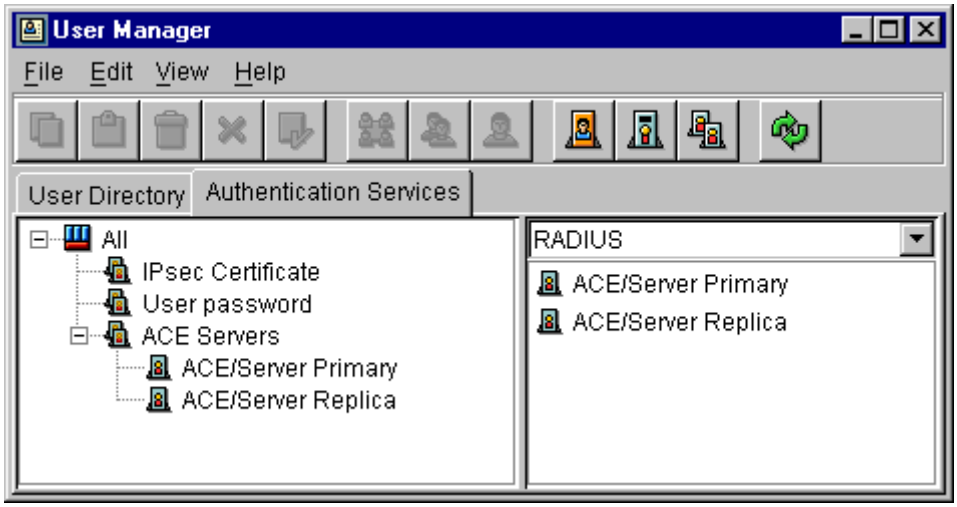
The following steps can be carried out using the Stonegate **User Manager** GUI:

- Create an Authentication service (type can be Radius or Tacacs+).

- Create Authentication Server/Servers with correct type.

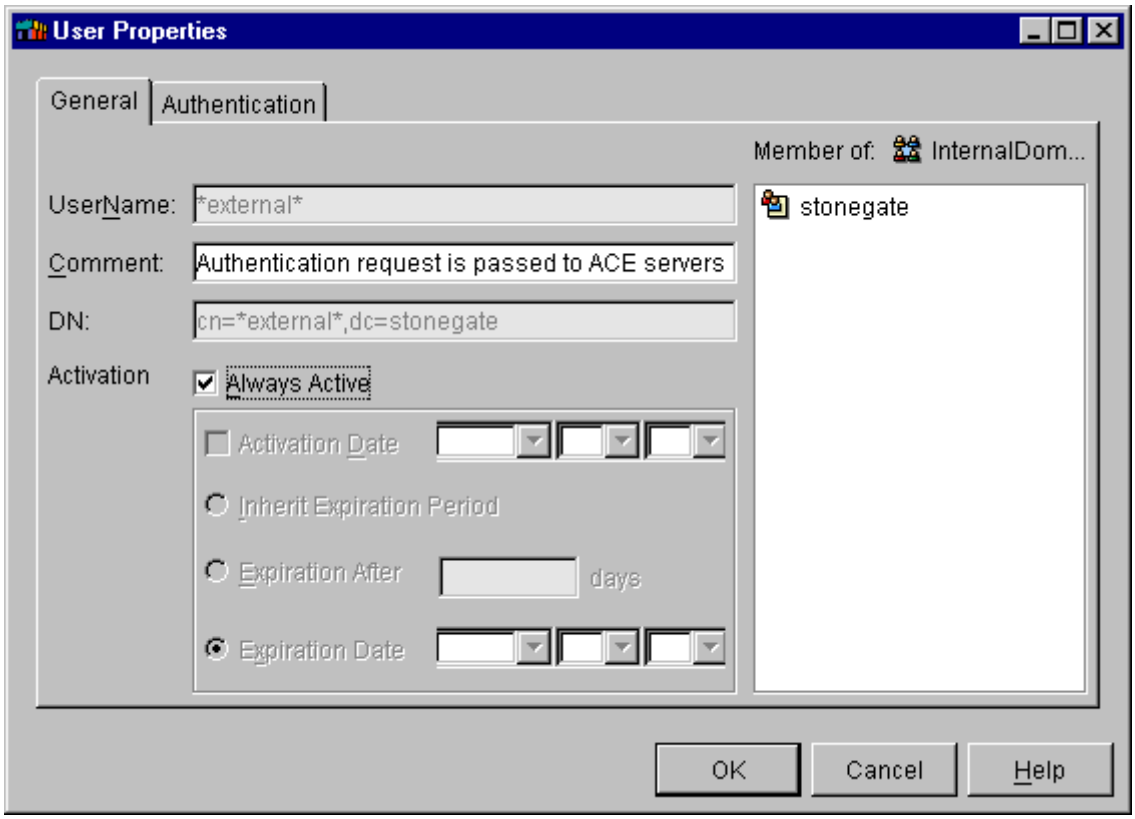


- All Created Authentication Servers must be bound to the Authentication Service.



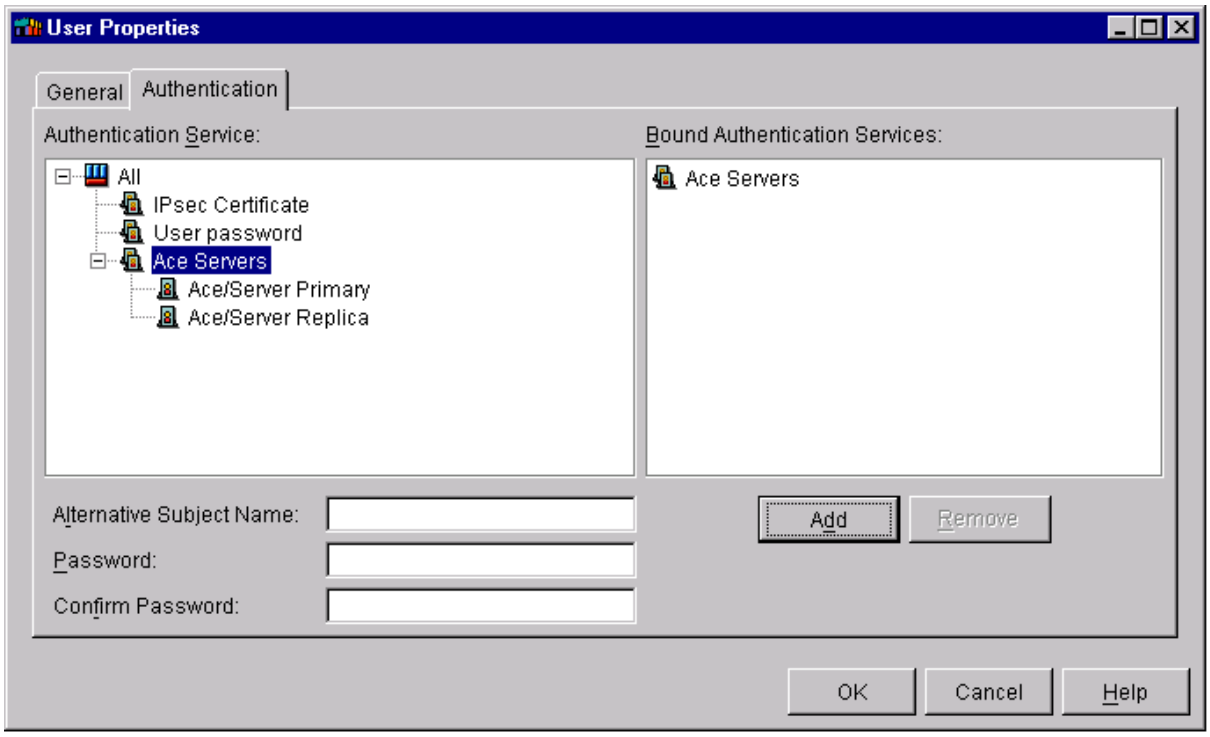
Having created your Service(s) and Server(s), you must now create users within the StoneGate user Database.

If you want to use ACE/Server authentication as your default Authentication Service for all users, create a special user with the **UserName: **external**** within the StoneGate user database and bind it to the previously created Authentication Service.

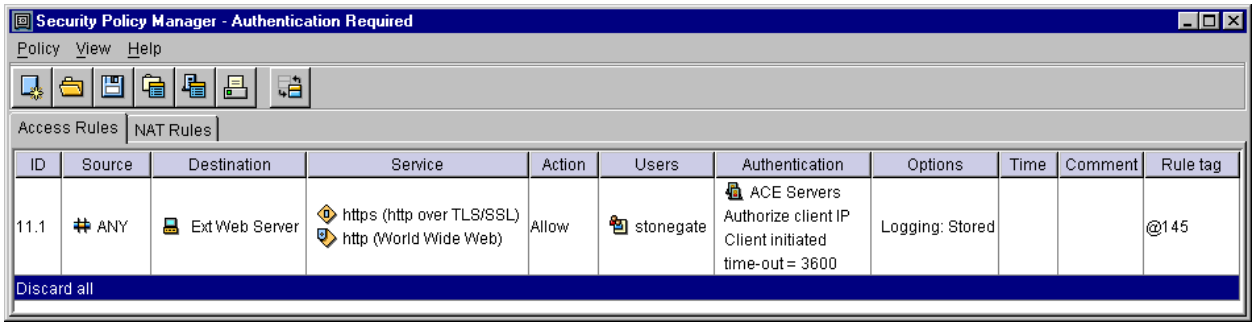


Using this generic method of authentication, ***external*** is the only user you will be required to create within the StoneGate user database.

If there is a need to configure Authentication Services on a per user basis, it can be done by creating individual user records within the StoneGate user database and binding them to the appropriate Authentication Service.



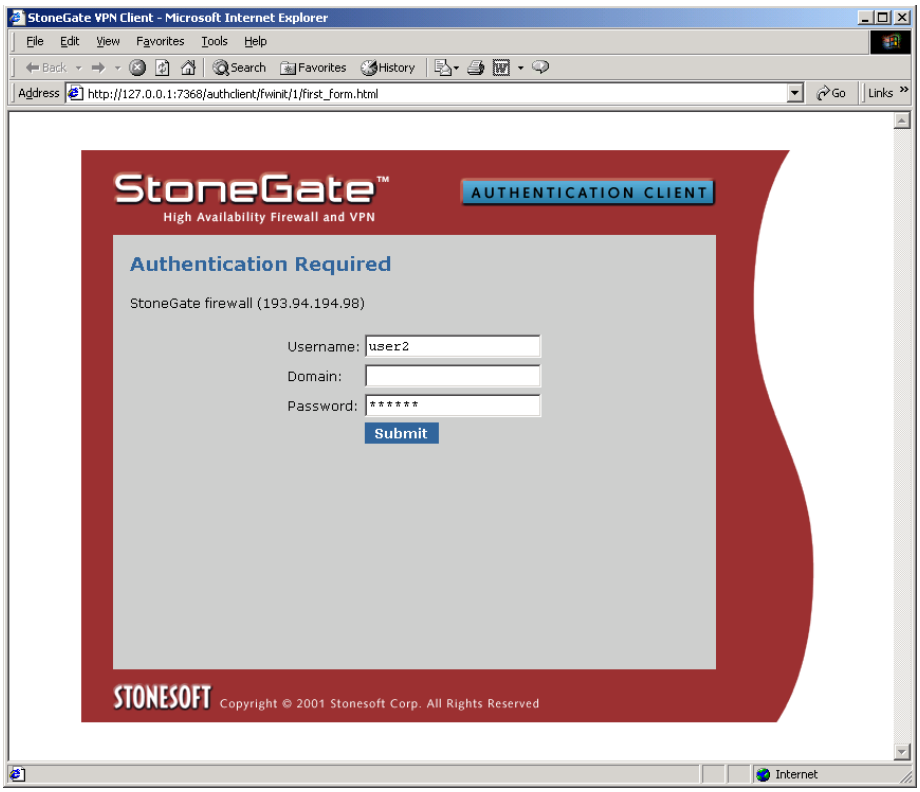
Using the **Security Policy Manager**, associate the appropriate access rules to the users or user group being authenticated by the RSA ACE/Server.

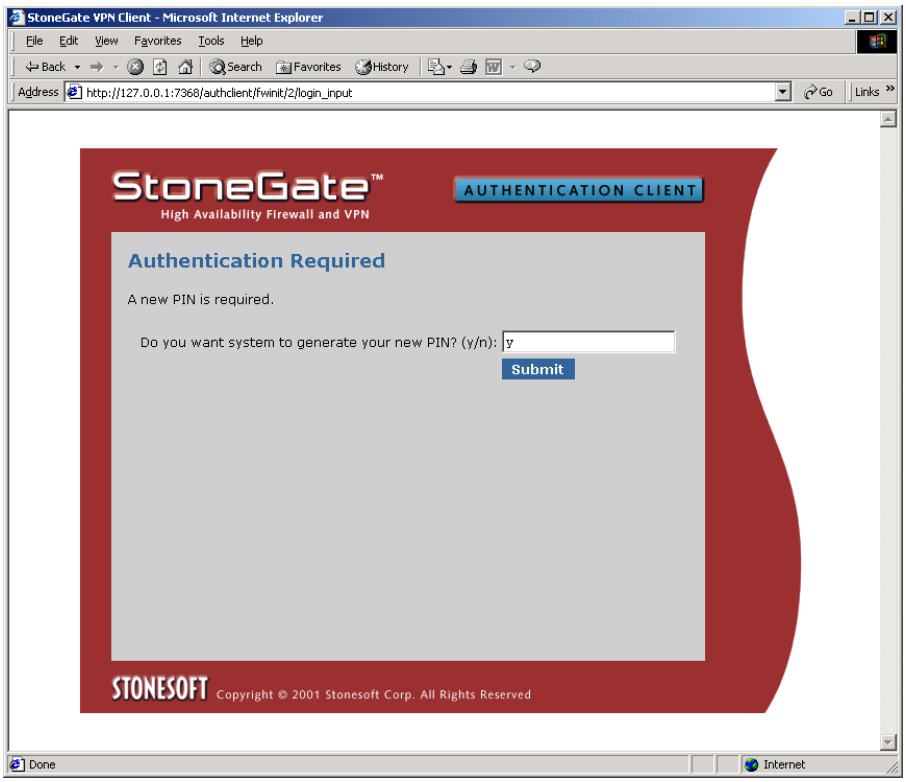


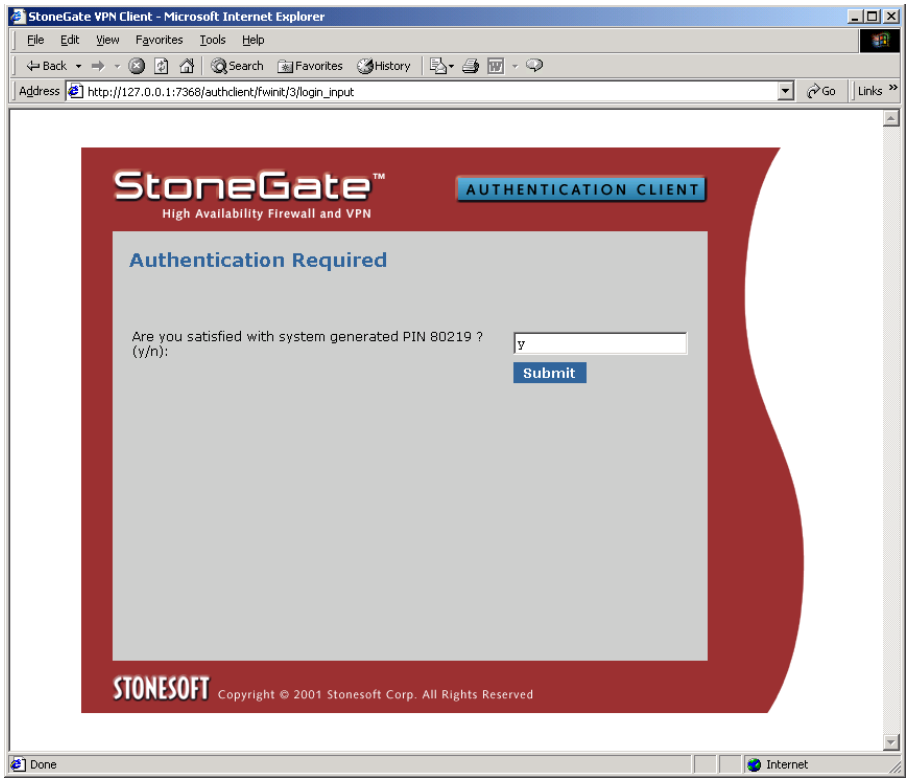
More detailed information on using StoneGate Firewall user Access and authentication rules can be found in the StoneGate Firewall Administrator's Guide. See Chapter 10: Defining users and user authentication.

Example SecurID enabled login sequences

Firewall initiated authentication with ACE/Server user account set to New PIN-mode.






StoneGate VPN Client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1:7368/authclient/fwinit/3/login_input
Go Links
StoneGate™
High Availability Firewall and VPN
AUTHENTICATION CLIENT
Authentication Required
Are you satisfied with system generated PIN 80219 ? (y/n):
y
Submit
STONESOFT Copyright © 2001 Stonesoft Corp. All Rights Reserved
Done
Internet


StoneGate VPN Client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1:7368/authclient/fwinit/5/login_input
Go Links
StoneGate™
High Availability Firewall and VPN
AUTHENTICATION CLIENT
Authentication Finished
PASSCODE Accepted
Access granted
STONESOFT Copyright © 2001 Stonesoft Corp. All Rights Reserved
http://127.0.0.1:7368/html/index.html
Internet

6. Certification Checklist

Date Tested: November 22, 2001

Product	Tested Version
ACE/Server	5.0.1
ACE/Agent	N/A
StoneGate firewall & VPN Client	1.6.3

Test	ACE	RADIUS
1st time auth. (node secret creation)	N/A	N/A
New PIN mode:		
System-generated		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
User-defined (4-8 alphanumeric)		
Non-PINPAD token	N/A	P
Password	N/A	P
User-defined (5-7 numeric)		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
SoftID token	N/A	P
Deny 4 digit PIN	N/A	P
Deny Alphanumeric	N/A	P
User-selectable		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
PASSCODE		
16 Digit PASSCODE	N/A	P
4 Digit Password	N/A	P
Next Tokencode mode		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
Replica Servers	N/A	P
User Lock Test (ACE Lock Function)	N/A	N/A
No ACE/Server	N/A	P

7. Known Issues

- If a clustered StoneGate firewall solution is used with RSA SecurID then an Agent Host entry must be defined within the ACE/Server database for each firewall cluster member.

- The Firewall cluster members share configured authentication service/server information. As a result of this when configuring Agents Hosts on the ACE/Server database, the same Shared Secret value must be used for each cluster member.