



RSA SecurID Ready Implementation Guide

Last Modified: February 1, 2011

Partner Information

Product Information	
Partner Name	Stonesoft Corp.
Web Site	www.stonesoft.com
Product Name	StoneGate SSL VPN
Version & Platform	StoneGate SSL VPN 1.4.4 [1437], StoneGate Virtual Appliance StoneGate Management Center (SMC) 5.2.2 [8257], CentOS 5.5
Product Description	StoneGate SSL VPN solution offers a flexible and secure remote access to enterprise information, appliances and networking resources. The solution guards the security of the network via an encrypted VPN tunnel while providing access from anywhere, and with any device.

STONESOFT
Network Security



Solution Summary

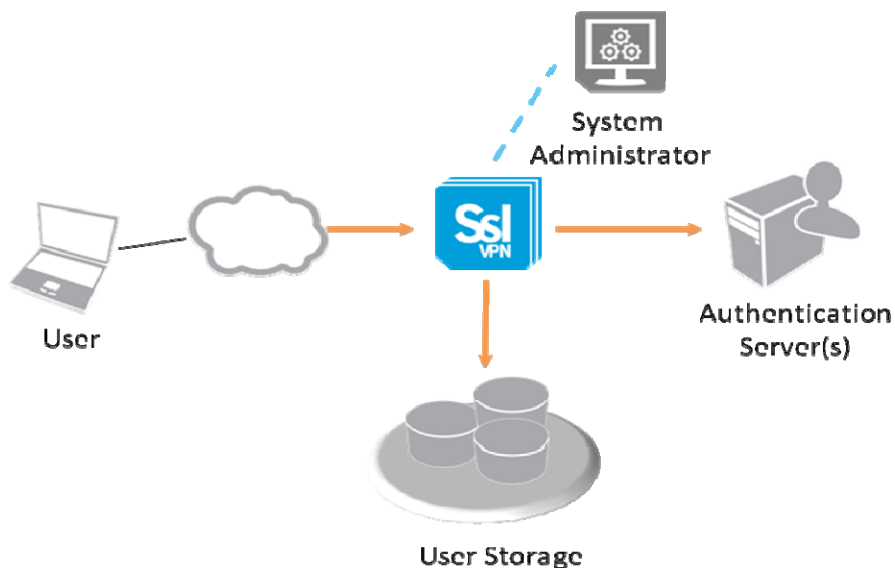
StoneGate SSL VPN offers secure remote access. It is a virtual private network (VPN) solution that can be used with a standard Web browser. Contrary to the traditional IPsec (Internet Protocol Security) VPN, SSL VPN does not require the installation of specialized client software on the end user device.

StoneGate SSL VPN provides employees with flexibility to access the network securely from any location and from any Web-enabled devices such as laptop, PDA or mobile phone. The applications can include e-mail, intranet, extranet, client/server applications, VoIP, terminal services, and much more.

RADIUS is a back-end protocol used by StoneGate to communicate with external authentication servers. RADIUS protocol can be used together with RSA Authentication Manager to provide StoneGate users secure two-factor authentication.

RSA SecurID supported features	
StoneGate SSL VPN 1.4.4	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
On-Demand Authentication via API	Yes
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

StoneGate System Architecture





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 StoneGate SSL VPN will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for StoneGate 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.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	None stored
Node Secret	None stored
sdstatus.12	N/A
sdopts.rec	N/A



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the StoneGate 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.

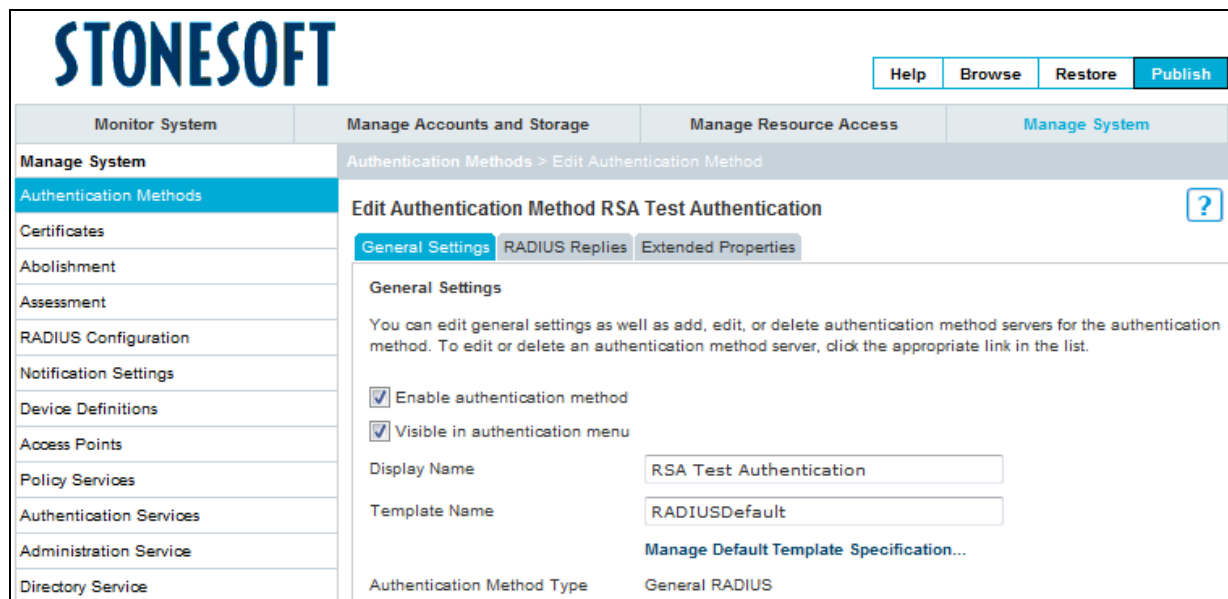
All StoneGate SSL VPN components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

StoneGate SSL VPN / RSA SecurID Authentication Configuration

The following steps are carried out using StoneGate SSL VPN Administration Portal.

1. Select **Authentication Methods** from the left hand navigation bar.
2. Click **Add Authentication Method** and select RADIUS or SecurID whichever is the correct method for your environment.
3. Complete the essential fields with the RSA Server information.

 **Note:** It is not possible to import `sdconf.rec` file to StoneGate SSL VPN, thus the used shared secret must be known.



The screenshot displays the StoneGate SSL VPN Administration Portal interface. At the top left is the 'STONESOFT' logo. On the top right, there are buttons for 'Help', 'Browse', 'Restore', and 'Publish'. Below the logo, there are four main navigation tabs: 'Monitor System', 'Manage Accounts and Storage', 'Manage Resource Access', and 'Manage System'. The 'Manage System' tab is active. On the left side, there is a vertical navigation menu with 'Authentication Methods' selected. The main content area shows the 'Edit Authentication Method RSA Test Authentication' page. It has three sub-tabs: 'General Settings', 'RADIUS Replies', and 'Extended Properties'. The 'General Settings' tab is active and contains the following configuration options:

- Enable authentication method
- Visible in authentication menu
- Display Name: RSA Test Authentication
- Template Name: RADIUSDefault
- Authentication Method Type: General RADIUS

There is also a link for 'Manage Default Template Specification...'.



4. Select the **Extended Properties** tab and select **Allow user not listed in any User Storage**. Defining Users is optional and can be configured under Manage Account and Storage.

The screenshot shows the STONESOFT web interface. At the top left is the STONESOFT logo. On the top right are buttons for Help, Browse, Restore, and Publish. Below the logo is a navigation menu with four tabs: Monitor System, Manage Accounts and Storage, Manage Resource Access, and Manage System. The Manage System tab is active, and the breadcrumb trail is Authentication Methods > Edit Authentication Method > Add Extended Property. The main content area is titled 'Edit Authentication Method RSA Test Authentication' and includes a help icon. Below the title is the 'Add Extended Property' section, which prompts the user to 'Enter the following information for the extended property.' There are two input fields: 'Key' and 'Value'. The 'Value' field has a dropdown menu open, showing several options: 'Lock user ID to session', 'Save credentials for SSO domain', 'Allow user not listed in any User Storage' (which is highlighted), 'Force create user', 'Create user on failed logon', and 'ActiveSync DeviceID Locking'. At the bottom left of the form is a '< Previous' button, and at the bottom right is an 'Add' button.

5. Next you can define access rules. Access Rules are optional and can be define under the Manage Resource Access tab.

 **Note:** Refer to the appendix of this document for more detailed information regarding Access Rules.



Screens

Login screen:

STONESOFT

Please Select Authentication Method

- Native RSA SecurID**
- RSA Test Authentication
- StoneGate Password
- StoneGate Web

STONESOFT

RSA Test Authentication

User Name:

Password:

User-generated New PIN:

STONESOFT

RSA Test Authentication

User Name:

Challenge:

Password:

Copyright© 2007-2010 Stonesoft. All rights reserved



System-generated New PIN:

STONESOFT

RSA Test Authentication

User Name

Challenge

Password

STONESOFT

Native RSA SecurID

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

Passcode

Next Tokencode:

STONESOFT

RSA Test Authentication

User Name

Challenge

Password

Copyright@ 2007-2010 Stonesoft. All rights reserved



Certification Checklist for RSA Authentication Manager

Date Tested: February 1, 2011

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1SP3	Windows 2003 Server R2
StoneGate SSL VPN	1.4.4 build 1437	StoneGate SSL VPN Virtual Appliance on VMWare ESXi 4.1.0

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"/>
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"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
Deny PIN Reuse	<input checked="" type="checkbox"/>	Deny PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
On-Demand Authentication			
On-Demand Authentication	<input checked="" type="checkbox"/>	On-Demand Authentication	<input checked="" type="checkbox"/>
On-Demand New PIN	<input checked="" type="checkbox"/>	On-Demand New PIN	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>

GLS / PAR

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

Appendix

Access Rules

Access rules protect resources by allowing or denying access, and specify the requirements for a particular user, resource group, or communication channel. Additionally, business-related conditions can be customized for services. For example, only customers who are allowed credit are able to use the ordering function.

1. Navigate to **Manage Resource Access** and select **Access Rules** from the left tool bar.
2. Select the Authentication Methods you want to apply the access rule to.

STONESOFT Help Browse Restore Publish

Monitor System Manage Accounts and Storage **Manage Resource Access** Manage System

Manage Resource Access Access Rules

Standard Resources

Web Resources

Tunnel Resources

Tunnel Sets

Client Firewall

Customized Resources

Access Rules

Application Portal

SSO Domains

Identity Federation

Global Resource Settings

Log Off

Add Access Rule - Authentication Method

Select Authentication Methods

Registered authentication methods are listed below. To use one or several authentication methods, select them in Available Authentication Methods and click Add. To remove an authentication method, select it in Selected Authentication Methods and click Remove.

Available Authentication Methods

- StoneGate Web
- StoneGate Password

Selected Authentication Methods

- RSA Test Authentication

Add > < Remove


If you have selected several authentication methods, specify if they are to be combined in a logical AND or OR statement. Select OR if the user should be able to choose which of the listed authentication methods to use for authentication. Select AND if all listed authentication methods are to be used to authenticate the user. If you select AND, note that the order in which the methods are listed in Selected Authentication Methods corresponds to the order in which the authentication methods will be used to authenticate the user.

Combine with 'OR?'
 Combine with 'AND?'

< Previous Next >

Copyright 2007-2010 Stonesoft. All rights reserved.

3. Select the **Next** button to defining resources. For users to be able to access a resource, you must configure a resource host.

 **Note:** In StoneGate SSL VPN, applications, folders, files, and URLs are registered as Web or tunnel resources. Web-enabled applications are registered as Web resources, and client-server applications that are not Web-enabled are registered as tunnel resources.

4. Access to a resource can be restricted with Access Rules.

 **Note:** For further details refer to the StoneSoft documentation.