Stonesoft Corp.
StoneGate SSL VPN

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

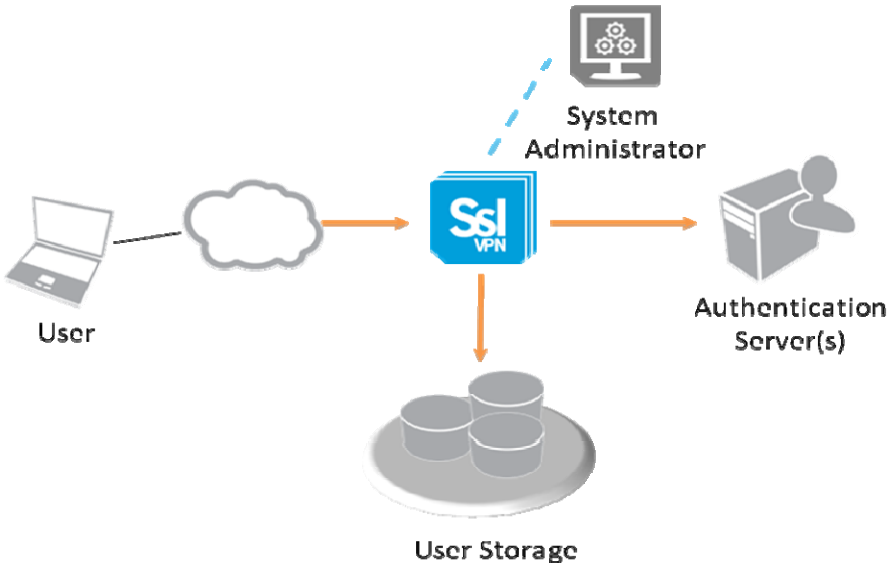
StoneGate SSL VPN offers secure remote access. It is a virtual private network (VPN) solution that can be used with a standard Web browser. Contrary to the traditional IPSec (Internet Protocol Security) VPN, SSL VPN does not require the installation of specialized client software on the end user device.

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.

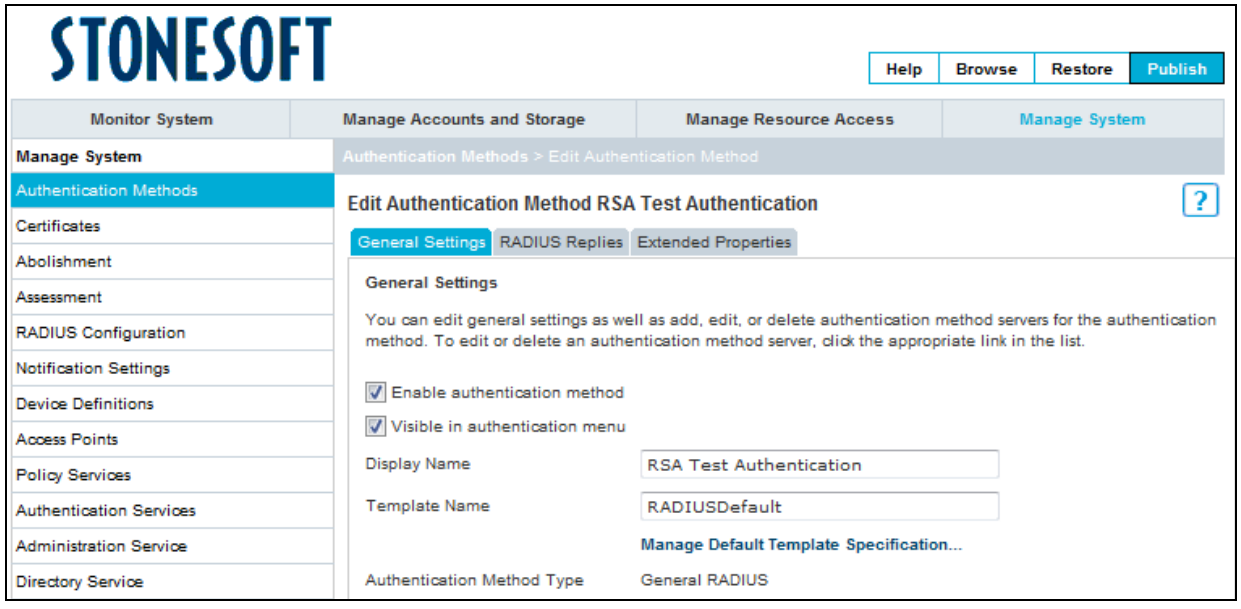
All StoneGate SSL VPN components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

StoneGate SSL VPN / RSA SecurID Authentication Configuration

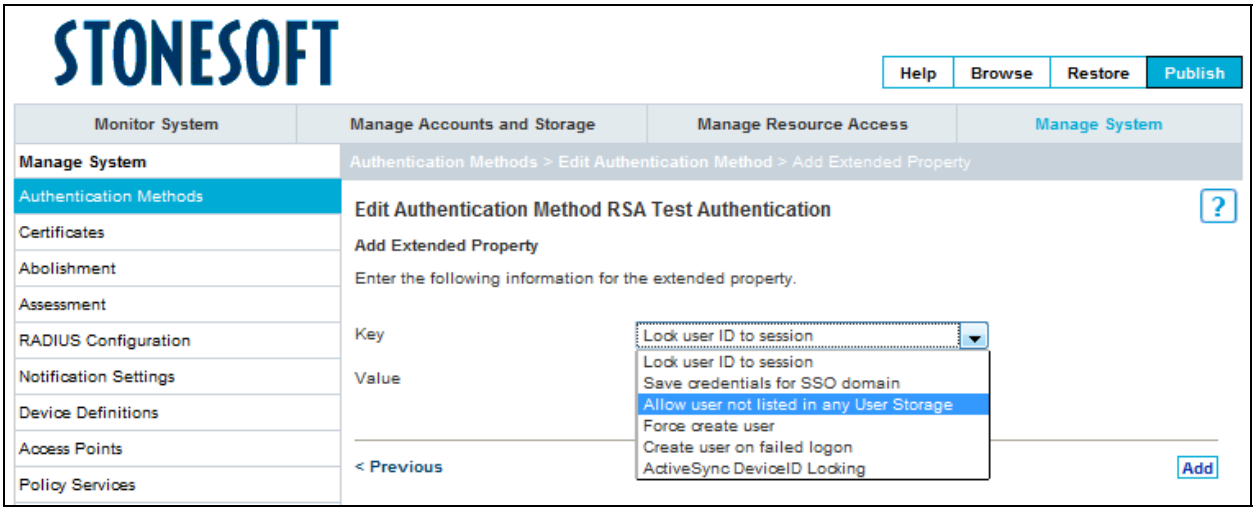
The following steps are carried out using StoneGate SSL VPN Administration Portal.

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.



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.

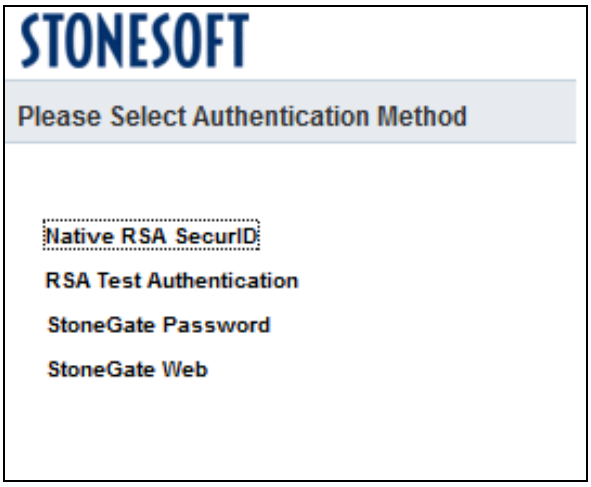


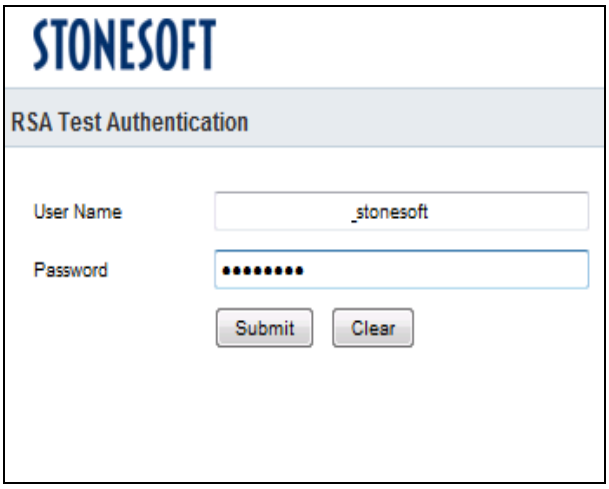
5. Next you can define access rules. Access Rules are optional and can be define under the Manage Resource Access tab.

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

Screens

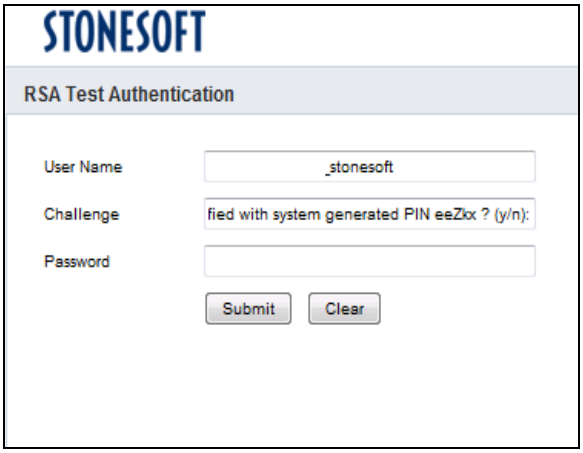
Login screen:





User-generated New PIN:

System-generated New PIN:



Next Tokencode:

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	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Deny Numeric PIN	✓	Deny Numeric PIN	✓
Deny PIN Reuse	✓	Deny PIN Reuse	✓
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	✓
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	✓
On-Demand New PIN	✓	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓

GLS / PAR

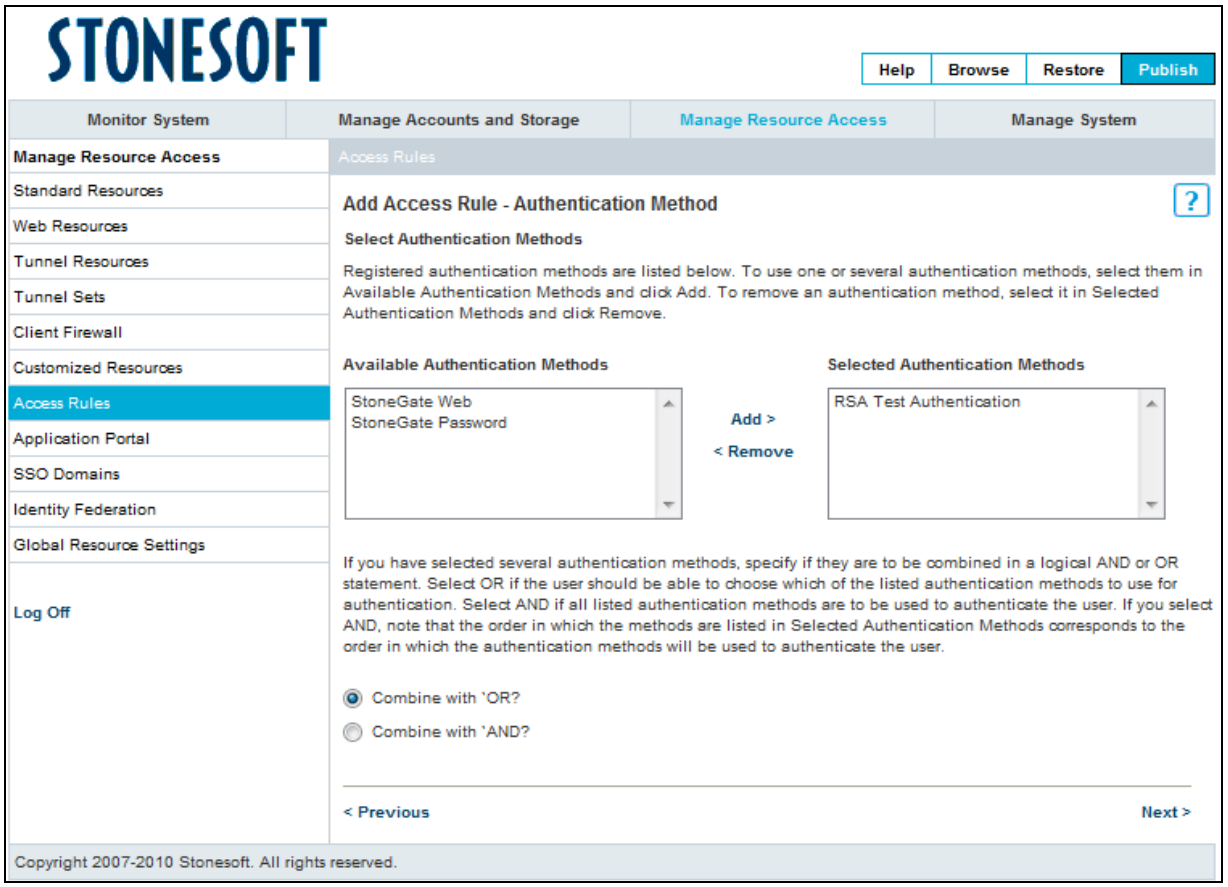
✓= Pass ✗= Fail N/A = Not Applicable to Integration

Appendix

Access Rules

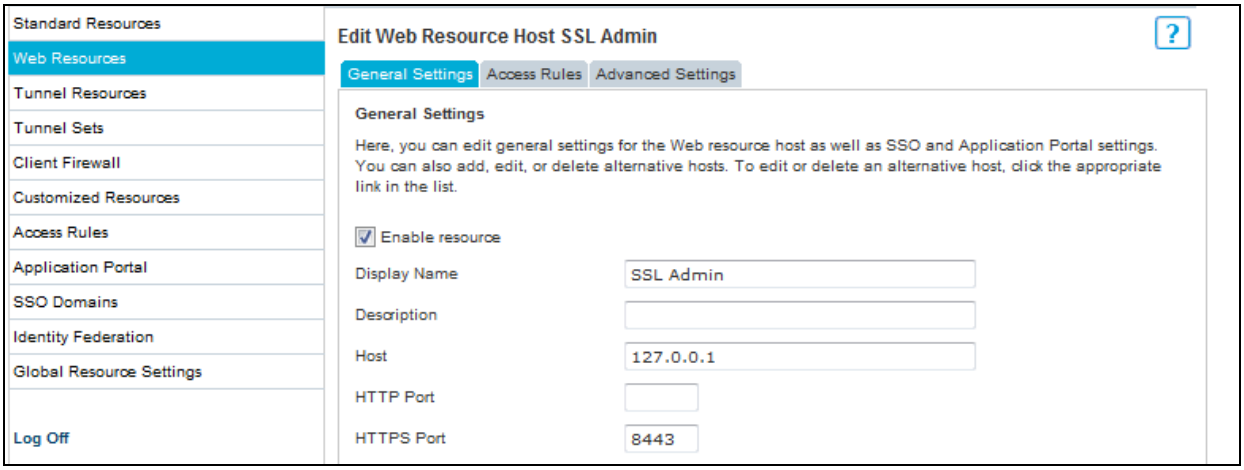
Access rules protect resources by allowing or denying access, and specify the requirements for a particular user, resource group, or communication channel. Additionally, business-related conditions can be customized for services. For example, only customers who are allowed credit are able to use the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

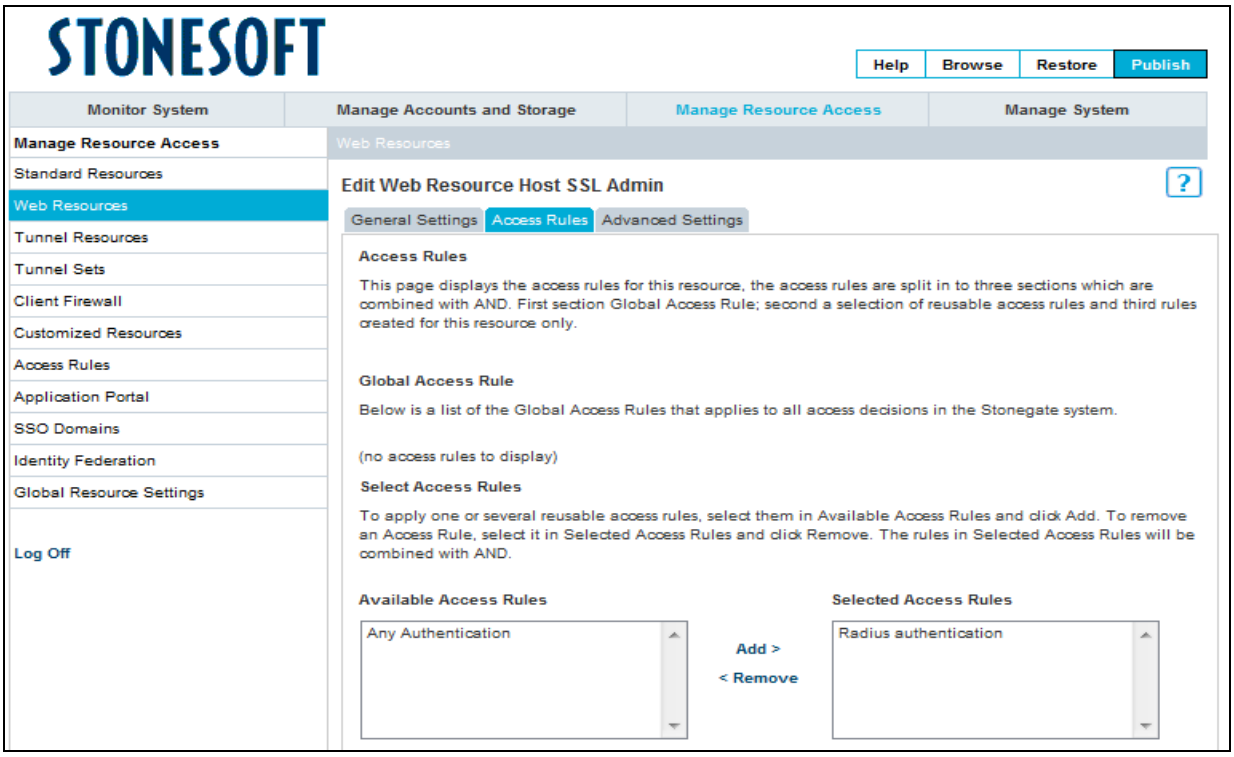


3. Select the **Next** button to defining resources. For users to be able to access a resource, you must configure a resource host.

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.