Stonesoft Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
 5.1 Configuring the RADIUS server
 5.2 Setting up the RADIUS NAS
 5.3 Enabling Session creation with username
- 6 Stonesoft Configuration

 - 6.1 Create a Radius Authentication Method
 6.2 Optional: Create a Secondary Authentication Server
 - ◆ 6.3 Login Page Customisation
- 7 Testing
- 8 Additional Configuration Options
 - ◆ 8.1 Two Stage Authentication
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

Introduction

This document describes steps to configure a Stonesoft Firewall SSL VPN with Swivel as the authentication server.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page. Depending on your needs, you can modify the default customization object or create a new customization object. There are many ways to configure it to work with Swivel.

To use the Single Channel Image such as the TURing Image and PINpad, the Swivel server must be made accessible. The client requests the images from the Swivel server, and is usually configured using a NAT (Network Address Translation), often with a proxy server. The Swivel appliance is configured with a proxy port to allow an additional layer of protection.

Prerequisites

Stonesoft Firewall

Swivel 3.x

Modified login page for TURing

Modified login page for PINpad

Baseline

Stonesoft 4.9.9|1050

Swivel 3.9

Architecture

Stonesoft makes authentication requests against the Swivel server by RADIUS.

The client makes TURing requests against the Swivel server using HTTP/HTTPS

Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank (or use 0.0.0.0) to allow RADIUS requests on any interface.

For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances

RADIUS>Server	<u> </u>
KAD105/Server	
Please enter the details for t	he RADIUS server.
Server enabled:	Yes▼
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 🔻
Filter ID:	No 🔻
Additional RADIUS logging:	Both
Enable debug:	Yes 🔻
Radius Groups:	Yes 🕶
Radius Group Keyword:	POLICY
	Apply Reset

Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the Swivel server and VPN RADIUS configuration.

RAD	IUS>NAS 🎯	
	enter the details for an RADIUS interface.	y RADIUS network access servers. A NAS is permitted to access the auther
NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel server can be configured to return an image containing a TURing image by presenting the username via the XML API or the SCImage servlet.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installation

Stonesoft Configuration

Create a Radius Authentication Method

On the Stonesoft management console select the Manage System tab and then Authentication Methods, select Add Authentication Method...

STONESOFT

			Help	Browse	Restore	Publish
Monitor System	Manage Accounts and Storage	Manage Resou	rce Acce	ss	Manage Sy	stem
Manage System						
Authentication Methods	Manage Authentication Method	S				
Certificates	Overview					
Abolishment		You can view, add, edit, and delete authentication methods. Registered methods are listed by To edit or delete an authentication method, click the appropriate link in the list.				
Assessment	To edit or delete an authentication	n method, click the	арргорпа	të link in the	list.	
RADIUS Configuration	Add Authentication Method	Registered Authentication Methods				
Notification Settings						
Device Definitions						
Access Points	Display Name Stonesoft Web			1000	atus abled	
Policy Services	Stonesoft Password				En	abled
Authentication Services						
Administration Service						
Directory Service						
OATH Configuration						
Log Off						

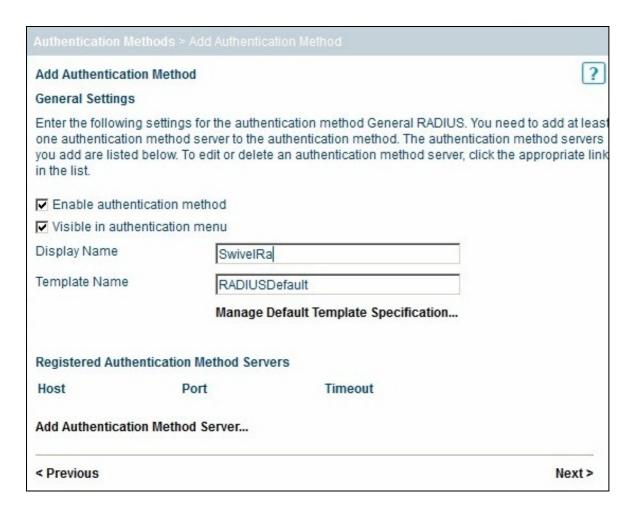
Select the General RADIUS authentication method



Ensure the following are checked:

- Enable authentication methodVisible in authentication menu

Enter a Display Name, then click on Next.



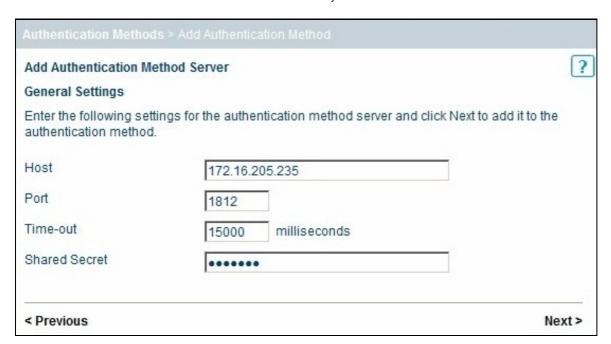
Enter the following information and when complete click Next:

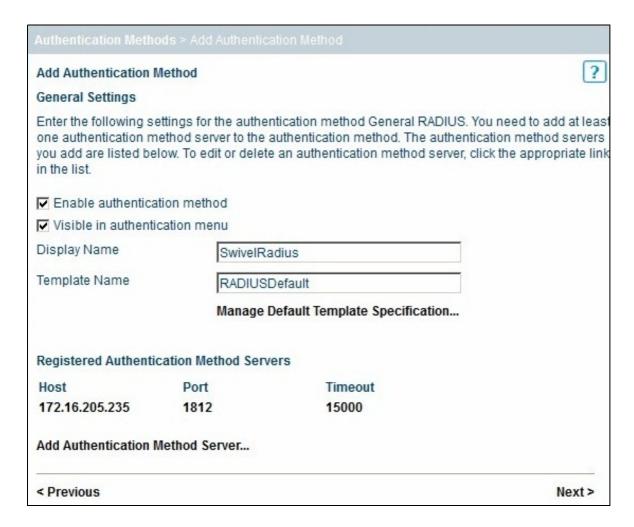
Host: Hostname/IP address of the Swivel server

Port: RADIUS authentication port, 1812 is the default for Swivel

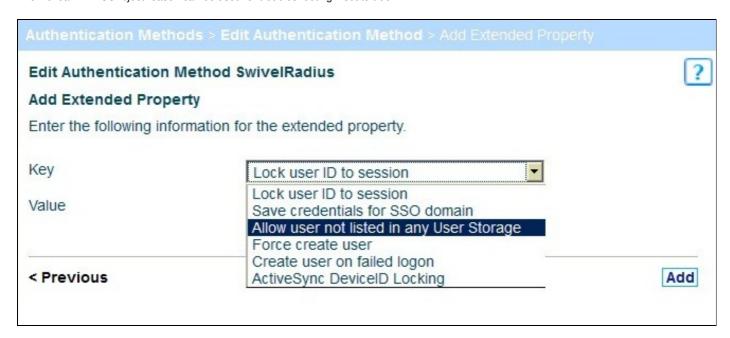
Time-out: default 15000 milliseconds

Shared Secret: The shared secret entered on the Swivel NAS entry for the Stonesoft server



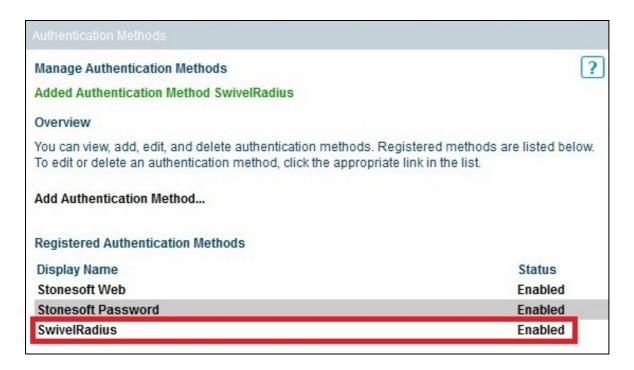


On the Extended Properties page click on Add Extended Property then select *Allow user not listed in any User Storage* and set it to *true*The *Reveal RADIUS reject reason* can be used for troubleshooting if set to true.



possibly not use: Stonesoft Authentication Method RADIUS Extended Properties.jpg

The configured RADIUS authentication method will appear under the list of Registered Authentication Methods.



Select Authentication Services then Add Authentication Service

Monitor System	Manage Accounts and Storage	Manage Resource Access	Manage System
Manage System	Authentication Services		
Authentication Methods	Manage Authentication Service	s	
Certificates	Overview		
Abolishment		te Authentication Services, as well as m	anage global RADIU
Assessment	authentication and password/PI	N settings.	
RADIUS Configuration		es are listed below. To edit or delete an	
Notification Settings	Service Settings.	st. To manage global settings, click Man	age Global Authentio
Device Definitions	Add Authentication Service		
Access Points	Aud Audientication Service		1
Policy Services	Registered Authentication Serv	ices	
Authentication Services	Service ID	Display Name	Internal Hos
Administration Service	4	Authentication Service	127.0.0.1
Directory Service		The or the second	
OATH Configuration	Manage Global Authentication S	ervice Settings	
Log Off			

On the RADIUS Authentication tab, ensure that *Proxy unknown users* is checked.

VOID OF THE PARTY	D UDIN O III		011010
ADIUS Authentication	Password/PIN Settings	E-mail Messages	SMS/Screen Messages
Manage RADIUS Authe	ntication		
Add or edit global settin	gs for RADIUS authentic	ation here.	
When both "Drop unkno precedence over the for	And the state of t	nknown users" are s	selected, the latter takes
Drop unknown sess	ions		
Drop unknown users	3		
Proxy unknown user:	S		
Reveal reject reason			
Session time-out	180 seco	nds	
RADIUS encoding	UTF-8		

When the configuration is complete then select publish

			Help	Browse	Restore	Pul
Monitor System	Manage Accounts and Storage	Manage Resou	rce Acce	ss	Manage Sy	stem
	Publish Version					
Log Off	Configuration Published When the configuration has been Stonesoft network. For detailed in Published content - All files synctomatical Access Points Display Name	nformation, please v			o all servers i	in the
	Access Point	127.0.0.1			Successfu	l publi
	Policy Services					
	Display Name	Host			Status	
	Policy Service	127.0.0.1			Successfu	l publi
	Authentication Services					
	Display Name	Host			Status	
	Authentication Se	127.0.0.1			Successfu	l publi

Optional: Create a Secondary Authentication Server

These modifications are used only if some of the single channel features are required. The prerequisites section contains login pages for TURing and PINpad.

Login Page Customisation

The login page, GenericForm.html can be modified to allow a variety of different login methods.

To select a different login page browse to the files in:

/opt/portwise/administration-service/files/access-point/built-in-files/wwwroot/wa/authmech/base

select browse to select the source file, then click on Upload

	Name	Size	T
	[]		
	Applet.html	1.93 KB	.l
	Dialog.html	1.97 KB	.1
	Dialog.pda.html	1.10 KB	.1
	Dialog.wml	541 bytes	
	GenericForm.html	2.92 KB	.1
	GenericForm.pda.html	2.09 KB	٠,١
	GenericForm.wml	1.34 KB	54
	SelfServiceForm.html	5.80 KB	
	SelfServiceFormPIN.html	5.55 KB	
	SelfServiceUserChallenge.html	3.05 KB	2.
	setFocus.js	733 bytes	
	setFocus.pda.js	660 bytes	
	Web.jar	30.95 KB	
	Web.js	5.45 KB	
	WebActiveX.cab	216.27 KB	
П	WebSkin.zip	14.13 KB	

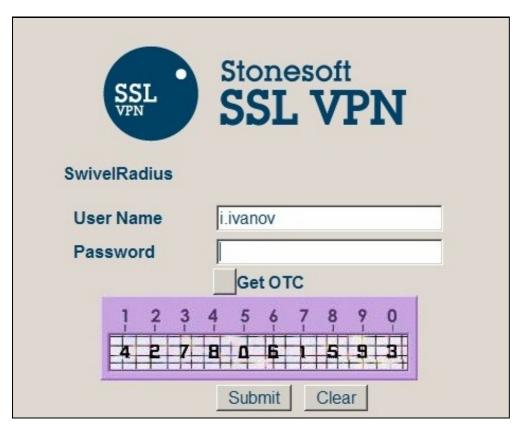
Testing

Browse to the login page and view the login page for the required configuration.

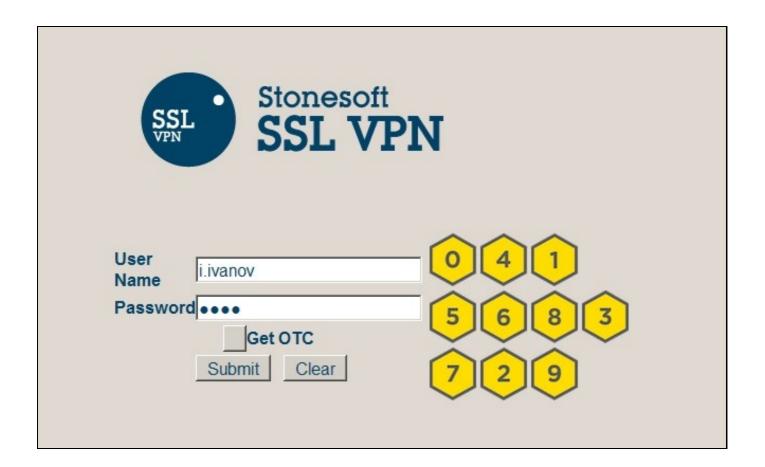
Stonesoft login page with Dual Channel using SMS, Mobile Client



Stonesoft login page with Single Channel TURing image



Stonesoft login page with PINpad



Additional Configuration Options

Two Stage Authentication

Swivel can be configured under the RADIUS/NAS settings to use Two Stage Authentication, whereby a password is entered and if correct the user is then prompted for a One Time Code, either from a graphical TURing image, mobile phone client or a Challenge and Response SMS sent to the user.

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

Known Issues and Limitations

None

Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com