

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

Please enter the details for the RADIUS server.

Server enabled:	<input type="text" value="Yes"/>
IP address:	<input type="text" value="0.0.0.0"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Maximum no. sessions:	<input type="text" value="50"/>
Permit empty attributes:	<input type="text" value="No"/>
Filter ID:	<input type="text" value="No"/>
Additional RADIUS logging:	<input type="text" value="Both"/>
Enable debug:	<input type="text" value="Yes"/>
Radius Groups:	<input type="text" value="Yes"/>
Radius Group Keyword:	<input type="text" value="POLICY"/>

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.

RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication via the RADIUS interface.

NAS: Identifier:	<input type="text" value="Device Name"/>
Hostname/IP:	<input type="text" value="192.168.0.1"/>
Secret:	<input type="password" value="••••••"/>
EAP protocol:	<input type="text" value="None"/>
Group:	<input type="text" value="---ANY---"/>
Authentication Mode:	<input type="text" value="All"/>
Change PIN warning:	<input type="text" value="No"/>

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...*

Monitor System	Manage Accounts and Storage	Manage Resource Access	Manage System						
Manage System	Authentication Methods								
Authentication Methods	Manage Authentication Methods ?								
Certificates	Overview								
Abolishment	You can view, add, edit, and delete authentication methods. Registered methods are listed below. To edit or delete an authentication method, click the appropriate link in the list.								
Assessment	Add Authentication Method...								
RADIUS Configuration	Registered Authentication Methods								
Notification Settings	<table border="1"><thead><tr><th>Display Name</th><th>Status</th></tr></thead><tbody><tr><td>Stonesoft Web</td><td>Enabled</td></tr><tr><td>Stonesoft Password</td><td>Enabled</td></tr></tbody></table>			Display Name	Status	Stonesoft Web	Enabled	Stonesoft Password	Enabled
Display Name	Status								
Stonesoft Web	Enabled								
Stonesoft Password	Enabled								
Device Definitions									
Access Points									
Policy Services									
Authentication Services									
Administration Service									
Directory Service									
OATH Configuration									
Log Off									

Select the *General RADIUS* authentication method

Stonesoft Web

Stonesoft Challenge

Stonesoft Synchronized

Stonesoft Mobile Text

Stonesoft Password

Stonesoft OATH

General RADIUS

SecurID

SafeWord

LDAP

Active Directory

IBM Tivoli

IBM RACF

Novell eDirectory

Windows Integrated Login

NTLM

Basic

User Certificate

Extended User Bind

Form-Based Authentication

E-ID

E-ID Signer

Confidence Online

Custom-defined

Copy of

Ensure the following are checked:

- *Enable authentication method*
- *Visible in authentication menu*

Enter a Display Name, then click on Next.

Authentication Methods > Add Authentication Method

Add Authentication Method ?

General Settings

Enter the following settings for the authentication method General RADIUS. You need to add at least one authentication method server to the authentication method. The authentication method servers you add are listed below. To edit or delete an authentication method server, click the appropriate link in the list.

Enable authentication method
 Visible in authentication menu

Display Name
 Template Name
[Manage Default Template Specification...](#)

Registered Authentication Method Servers

Host	Port	Timeout
Add Authentication Method Server...		

[< Previous](#)

[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

Authentication Methods > Add Authentication Method

Add Authentication Method Server ?

General Settings

Enter the following settings for the authentication method server and click Next to add it to the authentication method.

Host
 Port
 Time-out milliseconds
 Shared Secret

[< Previous](#)

[Next >](#)

Leave the RADIUS Reply settings as default unless a specific RADIUS configuration is required

Authentication Methods > Add Authentication Method

Add Authentication Method ?

General Settings

Enter the following settings for the authentication method General RADIUS. You need to add at least one authentication method server to the authentication method. The authentication method servers you add are listed below. To edit or delete an authentication method server, click the appropriate link in the list.

Enable authentication method
 Visible in authentication menu

Display Name
 Template Name
[Manage Default Template Specification...](#)

Registered Authentication Method Servers

Host	Port	Timeout
172.16.205.235	1812	15000

[Add Authentication Method Server...](#)

[< Previous](#) [Next >](#)

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.

Authentication Methods > Edit Authentication Method > Add Extended Property

Edit Authentication Method SwivelRadius ?

Add Extended Property

Enter the following information for the extended property.

Key
 Value

[< Previous](#) [Add](#)

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

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

Authentication Methods

Manage Authentication Methods ?

Added Authentication Method SwivelRadius

Overview

You can view, add, edit, and delete authentication methods. Registered methods are listed below. To edit or delete an authentication method, click the appropriate link in the list.

Add Authentication Method...

Registered Authentication Methods

Display Name	Status
Stonesoft Web	Enabled
Stonesoft Password	Enabled
SwivelRadius	Enabled

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 Services		
Certificates	Overview		
Abolishment	You can view, add, edit, and delete Authentication Services, as well as manage global RADIUS authentication and password/PIN settings.		
Assessment	Registered Authentication Services are listed below. To edit or delete an Authentication Service, click the appropriate link in the list. To manage global settings, click Manage Global Authentication Service Settings.		
RADIUS Configuration	Add Authentication Service...		
Notification Settings	Registered Authentication Services		
Device Definitions	Service ID	Display Name	Internal Host
Access Points	4	Authentication Service	127.0.0.1
Policy Services	Manage Global Authentication Service Settings...		
Authentication Services			
Administration Service			
Directory Service			
OATH Configuration			
Log Off			

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

Manage Global Authentication Service Settings ?

- RADIUS Authentication
- Password/PIN Settings
- E-mail Messages
- SMS/Screen Messages

Manage RADIUS Authentication

Add or edit global settings for RADIUS authentication here.

When both "Drop unknown users" and "Proxy unknown users" are selected, the latter takes precedence over the former.

- Drop unknown sessions
- Drop unknown users
- Proxy unknown users
- Reveal reject reason

Session time-out seconds

RADIUS encoding

[Save](#)

When the configuration is complete then select publish

		Help	Browse																		
		Restore	Pub																		
Monitor System	Manage Accounts and Storage	Manage Resource Access	Manage System																		
	Publish Version																				
Log Off	<p>Configuration Published</p> <p>When the configuration has been published successfully, it is distributed to all servers in the Stonesoft network. For detailed information, please view the system log.</p> <p>Published content - All files synchronized.</p> <p>Access Points</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Display Name</th> <th style="width: 20%;">Host</th> <th style="width: 20%;">Status</th> </tr> </thead> <tbody> <tr> <td>Access Point</td> <td>127.0.0.1</td> <td style="color: green;">Successful publi</td> </tr> </tbody> </table> <p>Policy Services</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Display Name</th> <th style="width: 20%;">Host</th> <th style="width: 20%;">Status</th> </tr> </thead> <tbody> <tr> <td>Policy Service</td> <td>127.0.0.1</td> <td style="color: green;">Successful publi</td> </tr> </tbody> </table> <p>Authentication Services</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Display Name</th> <th style="width: 20%;">Host</th> <th style="width: 20%;">Status</th> </tr> </thead> <tbody> <tr> <td>Authentication Se...</td> <td>127.0.0.1</td> <td style="color: green;">Successful publi</td> </tr> </tbody> </table>			Display Name	Host	Status	Access Point	127.0.0.1	Successful publi	Display Name	Host	Status	Policy Service	127.0.0.1	Successful publi	Display Name	Host	Status	Authentication Se...	127.0.0.1	Successful publi
Display Name	Host	Status																			
Access Point	127.0.0.1	Successful publi																			
Display Name	Host	Status																			
Policy Service	127.0.0.1	Successful publi																			
Display Name	Host	Status																			
Authentication Se...	127.0.0.1	Successful 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*

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

	Name	Size	Type
	[..]		
<input type="checkbox"/>	Applet.html	1.93 KB	.html
<input type="checkbox"/>	Dialog.html	1.97 KB	.html
<input type="checkbox"/>	Dialog.pda.html	1.10 KB	.html
<input type="checkbox"/>	Dialog.wml	541 bytes	.wml
<input type="checkbox"/>	GenericForm.html	2.92 KB	.html
<input type="checkbox"/>	GenericForm.pda.html	2.09 KB	.html
<input type="checkbox"/>	GenericForm.wml	1.34 KB	.wml
<input type="checkbox"/>	SelfServiceForm.html	5.80 KB	.html
<input type="checkbox"/>	SelfServiceFormPIN.html	5.55 KB	.html
<input type="checkbox"/>	SelfServiceUserChallenge.html	3.05 KB	.html
<input type="checkbox"/>	setFocus.js	733 bytes	.js
<input type="checkbox"/>	setFocus.pda.js	660 bytes	.js
<input type="checkbox"/>	Web.jar	30.95 KB	.jar
<input type="checkbox"/>	Web.js	5.45 KB	.js
<input type="checkbox"/>	WebActiveX.cab	216.27 KB	.cab
<input type="checkbox"/>	WebSkin.zip	14.13 KB	.zip

Select all

Download selected files as zip Delete selected files

 Create Dir Create File Rename File

 Browse... Upload

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 SSL VPN

SwivelRadius

User Name

Password

Submit

Clear

Stonesoft login page with Single Channel TURING image



Stonesoft SSL VPN

SwivelRadius

User Name

Password

Get OTC

1	2	3	4	5	6	7	8	9	0
4	2	7	8	0	6	1	5	9	3

Submit

Clear

Stonesoft login page with PINpad



Stonesoft
SSL VPN

User
Name

Password

 Get OTC

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