

# Table of Contents

<b>1 McAfee IPsec.....</b>	<b>1</b>
<b>2 Overview.....</b>	<b>2</b>
<b>3 Demos.....</b>	<b>3</b>
<b>4 Stonesoft Integration.....</b>	<b>4</b>
<b>5 Introduction.....</b>	<b>5</b>
<b>6 Prerequisites.....</b>	<b>6</b>
<b>7 Baseline.....</b>	<b>7</b>
<b>8 Architecture.....</b>	<b>8</b>
<b>9 Swivel Configuration.....</b>	<b>9</b>
9.1 Configuring the RADIUS server.....	9
9.2 Setting up the RADIUS NAS.....	9
9.3 Enabling Session creation with username.....	10
<b>10 Stonesoft Configuration.....</b>	<b>11</b>
10.1 Create a Radius Authentication Method.....	11
10.2 Optional: Create a Secondary Authentication Server.....	17
10.3 Login Page Customisation.....	17
<b>11 Testing.....</b>	<b>18</b>
<b>12 Additional Configuration Options.....</b>	<b>20</b>
12.1 Two Stage Authentication.....	20
<b>13 Troubleshooting.....</b>	<b>21</b>
<b>14 Known Issues and Limitations.....</b>	<b>22</b>
<b>15 Additional Information.....</b>	<b>23</b>

# 1 McAfee IPsec

## 2 Overview

Swivel can provide strong and two factor authentication to the McAfee IPsec solution.

### 3 Demos

TURing	SMS	Mobile App.
McAfee IPsec & Swivel TURing	McAfee IPsec & Swivel SMS	McAfee IPsec & Swivel Mobile App.

## 4 Stonesoft Integration

## 5 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.

## 6 Prerequisites

Stonesoft Firewall

Swivel 3.x

[Modified login page for TURing](#)

[Modified login page for PINpad](#)

## 7 Baseline

Stonesoft 4.9.9|1050

Swivel 3.9



## 8 Architecture

Stonesoft makes authentication requests against the Swivel server by RADIUS.

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

## 9 Swivel Configuration

### 9.1 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"/>

### 9.2 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 server 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.

### 9.3 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](https://Swivel_server_IP:8443/proxy/SCImage?username=testuser)

For a software only install see [Software Only Installation](#)

# 10 Stonesoft Configuration

## 10.1 Create a Radius Authentication Method

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

The screenshot shows the Stonesoft management console interface. At the top left is the 'STONESOFT' logo. On the right, there are buttons for 'Help', 'Browse', 'Restore', and 'Publish'. Below these are four main navigation tabs: 'Monitor System', 'Manage Accounts and Storage', 'Manage Resource Access', and 'Manage System' (which is highlighted in blue). Under the 'Manage System' tab, there is a sub-menu with 'Authentication Methods' selected and highlighted in blue. The main content area is titled 'Authentication Methods' and contains the following sections:

- Manage Authentication Methods** (with a help icon)
- 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

On the left side of the console, there is a vertical navigation menu with the following items: 'Manage System', 'Authentication Methods', 'Certificates', 'Abolishment', 'Assessment', 'RADIUS Configuration', 'Notification Settings', 'Device Definitions', 'Access Points', 'Policy Services', 'Authentication Services', 'Administration Service', 'Directory Service', 'OATH Configuration', and '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
<a href="#">Add Authentication Method Server...</a>		

---

[< 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
<b>Manage System</b>	Authentication Services		
Authentication Methods	<b>Manage Authentication Services</b>		
Certificates	<b>Overview</b>		
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	<b>Add Authentication Service...</b>		
Notification Settings	<b>Registered Authentication Services</b>		
Device Definitions	Service ID	Display Name	Internal Host
Access Points	4	Authentication Service	127.0.0.1
Policy Services	<b>Manage Global Authentication Service Settings...</b>		
<b>Authentication Services</b>			
Administration Service			
Directory Service			
OATH Configuration			
<b>Log Off</b>			

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



Authentication Services > Global Settings

### 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			
<b>Log Off</b>	<b>Configuration Published</b>				
	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.				
	Published content - All files synchronized.				
	<b>Access Points</b>				
	<b>Display Name</b>	<b>Host</b>			<b>Status</b>
Access Point	127.0.0.1			Successful publi	
<b>Policy Services</b>					
<b>Display Name</b>	<b>Host</b>			<b>Status</b>	
Policy Service	127.0.0.1			Successful publi	
<b>Authentication Services</b>					
<b>Display Name</b>	<b>Host</b>			<b>Status</b>	
Authentication Se...	127.0.0.1			Successful publi	

## 10.2 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.

## 10.3 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

## 11 Testing

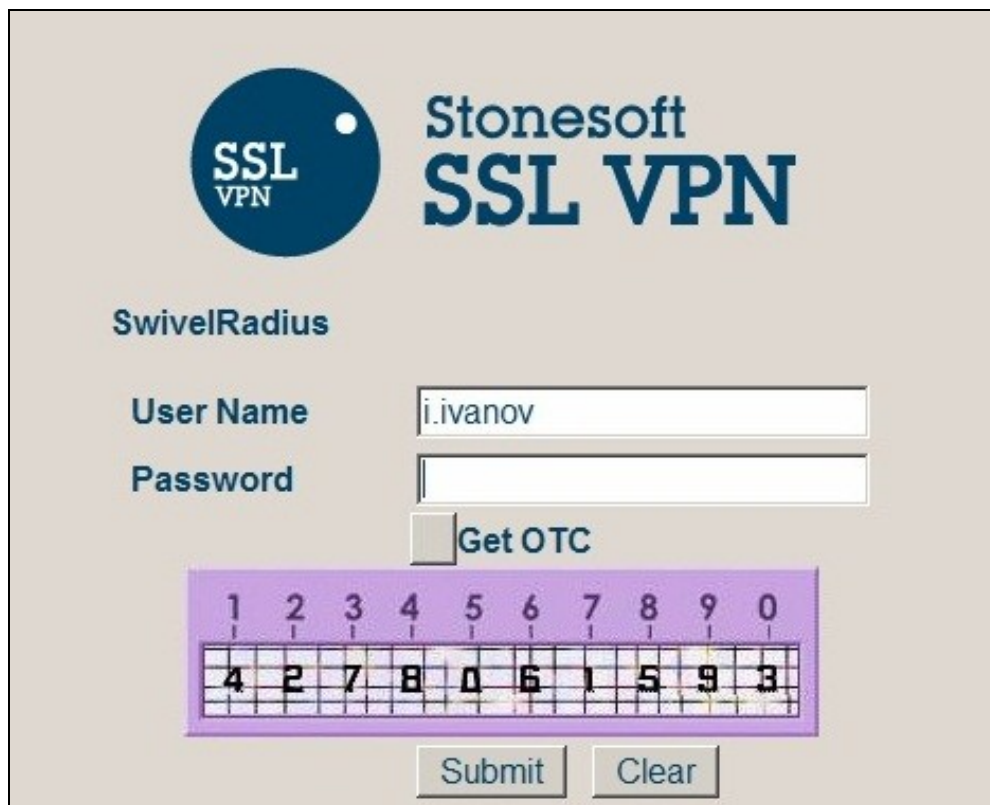
Browse to the login page and view the login page for the required configuration.

Stonesoft login page with Dual Channel using SMS, Mobile Client



The image shows the Stonesoft SSL VPN login page. At the top left is the logo, a dark blue circle with 'SSL VPN' in white. To its right is the text 'Stonesoft SSL VPN' in a dark blue font. Below the logo and text is the label 'SwivelRadius'. Underneath are two input fields: 'User Name' and 'Password'. Below the 'Password' field are two buttons: 'Submit' and 'Clear'.

Stonesoft login page with Single Channel TURing image



The image shows the Stonesoft SSL VPN login page with a single channel. It features the same logo and header as the previous image. Below the 'SwivelRadius' label are the 'User Name' and 'Password' input fields. The 'User Name' field contains the text 'i.ivanov'. Below the 'Password' field is a 'Get OTC' button. Underneath is a purple-bordered grid for a TURING image. The grid has 10 columns labeled 1 through 0. The first row of the grid contains the numbers 4, 2, 7, 8, 0, 6, 1, 5, 9, 3. Below the grid are 'Submit' and 'Clear' buttons.



# Stonesoft SSL VPN

User Name

Password

Get OTC



## 12 Additional Configuration Options

### 12.1 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.

## 13 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

## 14 Known Issues and Limitations

None

## 15 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](mailto:support@swivelsecure.com)