## Cisco ASA Integration

#### Contents

- 1 Introduction
  - 1.1 Configuration steps overview
- 2 Prerequisites 2.1 Login Page customisation prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
  - ♦ 5.1 Configuring the RADIUS server
    - ♦ 5.1.1 Enabling Session creation with username
- 5.2 Setting up Swivel Dual Channel Transports
- 6 Cisco ASA Configuration
  - ♦ 6.1 Create a Radius Authentication Server Group
  - 6.2 Optional: Create a Secondary Authentication Server
    6.3 Create a Connection Profile (Tunnel Group)
  - ♦ 6.4 Optional: Create a Secondary Authentication for the Connection Profile (Tunnel Group)
  - 6.5 Test the RADIUS authentication
  - ♦ 6.6 Optional: Login Page Customisation
- 7 Testing
- 8 Additional Configuration Options ◆ 8.1 Customisation for One Touch / Push
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

## Introduction

This document describes steps to configure a Cisco ASA with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS. AnyConnect works with Swivel if started in the portal.

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 such as:

- Username AD Password and Swivel Authentication (The most common method with AD authentication made against the LDAP server and OTC checked against Swivel using RADIUS)
- Username AD Password and Swivel Authentication (AD authentication and OTC checked against Swivel using RADIUS)
- Username and OTC (OTC checked against Swivel using RADIUS authentication)

And various other options including local password.

To use the Single Channel Image such as the TURing Image, 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 virtual appliance or hardware appliance is configured with a proxy port to allow an additional layer of protection.

For the Cisco IPSEC client Swivel integration see Cisco IPSEC Client Integration

#### Configuration steps overview

- Configuring the Swivel server
- Create a customization object to hold the attached Javascript.
- Create an authentication server group with RADIUS protocol.
- Create a connection profile (tunnel group) to link login URL, authentication server and custom login page together.

## Prerequisites

Cisco ASA 8.03 or higher

Cisco documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

#### Login Page customisation prerequisites

Cisco ASA 8 customisation Script Note: beware if opening this in Wordpad or similar in case the text editor wraps the text onto a new line. This script can be used for TURing, SMS, Token or Mobile Phone Client. There is an alternative customisation for Pinpad, available from here.

For Single Channel TURing images some editing of the script is required.

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image or Pinpad, and security string number, for external access this is usually through a NAT.

## Baseline

Cisco ASA 8.03, Also tested with 8.21 Swivel 3.5, 3.6, 3.7, 3.8, 3.9

# Architecture

The Cisco ASA 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**

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

#### **Enabling Session creation with username**

To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

### Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

# **Cisco ASA Configuration**

### **Create a Radius Authentication Server Group**

Authentication Server Group is used to hold necessary information about the Swivel server. Go to Remote Access VPN -> AAA/Local users -> AAA Server. Click on Add to add an AAA Server Group.

Remote Access VPN $\Box  + \times$	Configuration > Remote	Access VPN > /	AAA/Local Users > [	AAA Se	rver E
P Introduction	AAA Server Groups				
E Clientless SSL VPN Access	Server Group	Protocol	Accounting Mode	F	Add
AAA/Local Users	🖆 Add AAA Serve	Edit			
LDAP Attribute Map	Server Group:	pinsafe		D, C	Delete
🕀 🔏 Secure Desktop Manager	Protocol;	RADIUS	~	Di	
Load Balancing     DHCP Server	Accounting Mode:	O Simultaneous	i 💽 Single	D	
	Reactivation Mode:	Oppletion		Di	
Advanced	Dead Time: 10	minu	ites	Di	
	Max Failed Attempts:	3			
	Enable interim acc	counting update	10		
		Cancel	Help		
				>	

Enter a name for Server Group, select RADIUS for Protocol and click OK. With the newly created server group name selected, click on Add on the right bottom to add a Swivel server.

Network (Client) Access	Same Group	Prote		Arrest mitten Made	Reation	aking Made	1
Clencess 55L YPN Access	Local	LOCAL		Accounting Mode	REGLIV	austribue	AGO
- Tortal	pinsafe	RADIL	JG	angle	Deplation	n'	Edit
Bookmarks	🔂 Edit AAA Sei	VEF					Deleb
	Server Group:		pirsafe				
Port Forwarding	Interface Name:		outside		Y		
Web Contents	Server Name or B	Address:	192,168,8,8	8)			
- Group Policies	Timeout:		10			seconds	15
Advanced	RADIUS Paramete	rs					††
AAA/Local Users	(Server Authent	ication Port	1812)		j.		
LDAP Attribute Map	Server Account	ng Port:	1813)			8	
Secure Desktop Manager	Retry Interval:		10 second	; 👻		Ē	3
Certificate Management	Server Secret k	ау:	••••••			1	odd
Canguage Editateauth	Common Passw	ord:				4	AUO
DHCP Server	ACL Netmask C	onv <del>a</del> t:	Standard	*			Edit
Advanced	SDI Messages —						Delete
	Message Ta	ble				8	Move Up

Enter Swivel server?s IP, authentication port and server secret key as indicated. Click on OK then Apply to save the AAA server group.

### **Optional: Create a Secondary Authentication Server**

The login page can be configured to display Swivel as a primary or secondary authentication server. To use multiple authentication servers, they must be configured under Remote Access VPN -> AAA/Local users -> AAA Server. This example shows an AD Server being added.

Go to Remote Access VPN -> AAA/Local users -> AAA Server. Click on Add to add an AAA Server Group.

Remote Access VPN 리 무 ×	<b>Configurat</b>	ion > Remot	e Access VI	N > AAA/L	ocal Users > <u>A/</u>	AA Server	<u>Groups</u>	
	AAA Server	Groups						
H·      H·	Se	rver Group	Protoc	ol A	ccounting Mode	Reactiv	vation Mode	
Connection Profiles	AD		NT Domain		-	Depletion		10
Portal	LOCAL		LOCAL				1	
	PINsaf	🙀 Add AAA	Server Grou	ıp		×		10
Client-Server Plug-ins								1
- Iso Customization		Server Group	);					
		Protocol:	RA	DIUS	-			
Port Forwarding					0 - 1			
Smart Tunnels		Accounting M	lode: (O	Simultaneous	s (• Single			
Web Contents		Reactivation	Mode: 💿	Depletion	C Timed			
Group Policies								
		Dead Tim	e: 10	minu	utes			
Resolution Provide Advanced								
	Servers in	Max Failed Al	ttempts: 3					
AAA Server Groups							erface	
- 2 LDAP Attribute Map	192.16	Enable in	terim account	ing update				
🗄 🔏 Secure Desktop Manager		VPN3K Cor	npatibility (	Option		*		
Setup								
🗄 📴 Certificate Management			ОК	Cancel	Help			
- B Language Localization					1	-		
DHCP Server	-							
DNS								
Advanced								

Enter a name for Server Group, select NT Domain or Kerberos for Protocol and click OK. With the newly created server group name selected, click on Add on the right bottom to add a NT Domain Server.

🚰 Add AAA Server	Group	×
Server Group:	AD	
Protocol:	NT Domain	
Reactivation Mode:	• Depletion C Timed	
Dead Time: 10	minutes	
Max Failed Attempts:	3	
OK	Cancel Help	

Enter the AD server?s IP, Server port and Domain Controller hostname. Click on OK then Apply to save the AAA server group.

Server Group:	AD	
Interface Name:	inside 💌	]
Server Name or IP Address:	192.168.0.100	
Timeout:	10	seconds
NT Domain Parameters		
NT Domain Parameters Server Port: 139 Domain Controller: 192.1	68.0.100	

This secondary authentication server then needs to be linked to the Connection Profile (see below).

## **Create a Connection Profile (Tunnel Group)**

Swivel can be defined as a Primary Authentication server or as a Secondary authentication server.

Connection Profile is used to link authentication server group, URL used to access the ASA, and login page customization together. Go to Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles. Click on Add to add a connection profile.

Remote Access VPN 🗗 🕀 🗙	Configuration > Remote Acc	ess VPN > Clientles	ss SSL VPN Access > Con	nection Profiles			
ntroduction	Access Interfaces						
Network (Client) Access	Enable interfaces for clientless	SSL VPN access.					
Clientless SSL VPN Access	TabayEsca	Interface Allow Access					
	Internace						
- Portai	oucside						
Cliept-Server Plug.ips	inside	inside 🗌					
	Access Port: 443						
Web Contents	Click here to Assign Certificate	e to Interface.					
Group Policies							
Dynamic Access Policies	Login Page Setting						
🕀 📆 Advanced	Allow user to select connect	ction profile, identifie	d by its alias, on the login pa	age, Otherwise, Defa			
				-			
🖻 🚽 🔓 AAA/Local Users	🔲 Allow user to enter interna	I password on the log	gin page.				
AAA Server Groups							
- 🎥 LDAP Attribute Map	Connection Profiles						
- 🕼 Local Users	Connection profile (tunnel grou	up) specifies how use	r is authenticated and other	parameters.			
🖻 🚮 Secure Desktop Manager	a						
🚽 🖓 Setup		3Ce					
🗄 🔂 Certificate Management	Namo	Enabled	Aliacos				
Language Localization		Chabled	Allases	Adu			
DHCP Server		<u> </u>		AAA(LOCAL)			
	DefaultRAGroup		10% 0445-	AAA(LOCAL)			
E 😳 Advanced	DefaultWEBVPNGroup		pinsafe	AAA(PINsafe)			
🐳 🐳 Connection Gateway		18 44		01			

In Basic panel, enter a name, alias and select the AAA Server Group created. Swivel can be configured as the Primary authentication server or the secondary authentication server.

Basic	Name:	DefaultWEBVPNGroup	
Advanced	Aliases:	pinsafe	]
Authentication Secondary Authenticat	Authentication		
Authorization Accounting	Method:	(• AAA () Certificate () Both	-
-NetBIOS Servers	AAA Server Group:	PINsafe 💌	Manage
-Clientless SSL VPN		🔲 Use LOCAL if Server Group fails	
	DNS		
	Server Group:	DefaultDNS	Manage
		(Following fields are attributes of the DNS server	group selected a
		Servers: 192.168.0.100	
		Domain Name: swivel.local	
	Default Group Policy	N	
	Group Policy:	DfltGrpPolicy	] Manage
		(Following field is an attribute of the group policy	selected above.
		✓ Enable clientless SSL VPN protocol	
·		Next O Previous	
IDO: L		Griona Grionada	

Click on Advanced then Clientless SSL VPN. Select the customization object created and add a Group URL used to access the ASA with Swivel authentication.

Basic Advanced General Authentication Authorization Accounting NetBIOS Servers Clientless SSL VPN	Portal Page Customization: pinsafe Denable the display of Radius Reg Denable the display of SecurId me Connection Aliases Add Z Delete	Manage ect-Message on the login screen when authentication essages on the login screen
	Alias	Enabled
	Group URLs  Add  Delete  URL  https://pinsafe.cisco.com/pinsafe	Enabled

Click on OK then Apply to save the Connection Profile.

#### **Optional: Create a Secondary Authentication for the Connection Profile (Tunnel Group)**

This option has been configured using the Secondary Authentication server option available in ASA 8.21

Go to Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles, select the connection profile created above then select Edit. Expand the Advanced option list and select Secondary Authentication. Enter the Secondary server group required and if the username should be reused.

Ensure the box "Use primary username (Hide secondary username on login page)" is ticked. Click on OK to save the settings. If AD is defined as the Primary authentication server then Swivel can be defined as the secondary AD server.

and the second sec	Secondary Authentication	Server Group		La restance
Advanced Server Group:		AD		👻 Mana
General Authentication		Lise LOCAL if Serv	ver Group fails	
Secondary Authentica	at	-		
Authorization		Use primary user	name (Hide secondary usernam	e on login page)
-Accounting -NetBIOS Servers	Attributes Server:	Primary C Second Primary C Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second Second	ondary	
ntless SSL VPN	Session Username Serv	er: 🖲 Primary 🔿 Seco	ondary	
	Interface-Specific Second	lary Authentication Server	r Groups	
	Add Call Edit	👕 Delete		
	Interface	Server Group	Fallback to LOCAL	Use primary usernar
			20	10
	Username Mapping from (	Lertificate		
	Pre-fill Username fr	om Certificate		
	📕 Hide username	from end user		
	Specify the certification	to fields to be used as the	e liceroame	
		are tields to be daed da rit	c uscillanic	
	Duine and Tradal	Ne rielas to be asea as th		
	Primary Field:	IN (Common Name)		
	Primary Field: C	IN (Common Name) DU (Organization Unit)		
	Primary Field: Secondary Field:	IN (Common Name) DU (Organization Unit) is the username		
	Primary Field: Secondary Field: C Use the entire DN a	IN (Common Name) IN (Organization Unit) Is the username		
	Primary Field: Secondary Field: C Use the entire DN a C Use script to select	IN (Common Name) DU (Organization Unit) is the username username		
	Primary Field: Secondary Field: C Use the entire DN a C Use script to select	IN (Common Name) DU (Organization Unit) as the username username		
	Primary Field: Secondary Field: C Use the entire DN a C Use script to select	CN (Common Name) CN (Organization Unit) as the username username	Edit Delete	
	Primary Field: Secondary Field: C Use the entire DN a C Use script to select	IN (Common Name) DU (Organization Unit) is the username username	Edit Delete	
	Primary Field: C Secondary Field: C C Use the entire DN a C Use script to select	IN (Common Name) DU (Organization Unit) as the username username Add 1 Next © Previous	Edit Delete	
nd:	Primary Field: Secondary Field: C Use the entire DN a C Use script to select None	IN (Common Name) DU (Organization Unit) Is the username Username I Add 1 Next OPPrevious	Edit Delete	

#### **Test the RADIUS authentication**

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

#### **Optional: Login Page Customisation**

If the Swivel Single Channel Image is to be used, then the login page needs to be customised. If single channel authentication is not required, or other page modifications such as for SMS on Demand buttons, then this section can be skipped. The login page customization is used to insert necessary Javascript to retrieve Swivel Turing image. In ASDM, go to Remote Access VPN ->Clientless SSL VPN Access -> Portal -> Customization. Click on Add to add a new customization object.

Remote Access VPN 🗗 🗜 🗙	Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Cus
<ul> <li>Introduction</li> <li>Network (Client) Access</li> <li>Clientless SSL VPN Access</li> <li>Connection Profiles</li> <li>Portal</li> </ul>	Customization Objects Configure customization objects that the security appliance uses to customize the SSL Add C Edit C Delete T Import C Export
Bookmarks	Customization Objects
Client-Server Plug-ins	Template
Customization	DfltCustomization
Port Forwarding	🖆 Add Customization Object 🛛 🔀
Group Policies	This will create a copy of default customization object and save it with the specified name.
AAA/Local Users     AAA/Local Users     Action Manager	Customization Object Name: pinsafe
Certificate Management     Language Localization	OK Cancel Help

Enter a name for the object, click on OK then Apply.

💠 Ad	ld 🗹 Edit	: 前 Delete
Custo	mization C	bjects
Templa	te	
DfltCus	tomization	i
pinsafe	;	

With the new object selected, click on Edit to enter the Customization Editor. Click on the Information Panel menu item. Note: If the information panel has been moved to a different location then the script can be added to the Copyright panel instead.

# CISCO SSL VPN Customization Editor

Logon page	pinsafe : Logon Page > Browser Window
<ul> <li>Browser Window</li> <li><u>Title Panel</u></li> <li><u>Languages</u></li> <li><u>Language Selector</u></li> <li><u>Logon Form</u></li> <li><u>Information Panel</u></li> <li><u>Copyright Panel</u></li> <li><u>Full Customization</u></li> </ul>	Title SSL VPN Service default customization

Logon page	pinsafe : Logon Page > Information Panel
<ul> <li>Browser Window</li> <li><u>Title Panel</u></li> <li><u>Languages</u></li> <li><u>Language Selector</u></li> <li><u>Logon Form</u></li> <li><u>Information Panel</u></li> <li><u>Copyright Panel</u></li> </ul>	Mode Enable  Panel Position Right  Text Image URL

Change Mode to ?Enable?. Modify the pinsafeurl variable in the Cisco ASA 8 customisation Script to reflect your Swivel server?s URL. (The scripts are located at the top of the page under prerequisites). Paste the modified content into the Text box. Click on Save on the top right corner of the Customization Editor to save the object.

WARNING: the Panel Position must be set to Right for the script to work. This is so that the customisation script is rendered after the logon form. If you particularly need the information panel to be on the left, put the Swivel customisation script in the Copyright Panel instead, as that is always rendered at the bottom.

#### The following elements need to be modified in the script:

//Modify the value of primary to reflect the URL of your PINsafe server //if using on-demand SMS, url will need to be DCMessage rather the SCImage //if using an HA pair and you wish the page to try one server then the other to receive a TURING //set standby to be the url of the standby swivel virtual or hardware appliance and set ha to true; var primary='https://demo.swivelsecure.com:8443/proxy/SCImage?username='; var standby='https://demo.swivelsecure.com:8443/proxy/SCImage?username='; var pinsafeurl = primary; var ha = false ; //set HA to true if you want the page to try two servers var loadTimeout = 2500; //how long the page waits (in milliseconds) for the image to be served from the main server before trying the second var button = true; // set to true if you want to show a button that requests a security string var autoShow = true; // set to true to show the TURing image automatically after entering the username

Note that for the Pinpad version, SCImage will be replaced with SCPinPad.

The primary and standby should be modified. If a standby is not used then set var secondaryAuth = false

#### For a virtual or hardware appliance

var primary='https://demo.swivelsecure.com:8443/proxy/SCImage?username=';

For a software only install see Software Only Installation

To use multiple security strings in an SMS message, this can be modified to show the next security string which should be entered.

For a virtual or hardware appliance

var pinsafeurl='https://demo.swivelsecure.com:8443/proxy/DCIndexImage?username=';

For a software only install see Software Only Installation

The text can also be changed to reflect the request for a security string index number. See also Multiple Security Strings How To Guide

"Please enter your user name and click on Get OTP Index";

The Button to request the Security String Index can also be edited

obj[0].value="Get OTP Index";

The Logon Form can be edited to suit the language and secondary authentication password message. Select the Logon Form to display the fields available.

Swivel as the primary authentication server, AD as the secondary authentication server.

PINSAFE : Logon Page > Logon	Form	
Title	Login	
Message	Please enter your username and password.	
Username Prompt	USERNAME:	
Secondary Username Prompt	2nd Username	
Password Prompt	PASSWORD:	
Secondary Password Prompt	AD Password	
Passcode Prompt	Passcode	
Secondary Passcode Prompt	2nd Passcode	
Internal Password Prompt	Internal Password:	
Hide Internal Password	No 💌	
Group Selector Prompt	GROUP:	
Button Text	Login	
Border Color	#858A91	
Title Font Color	#mm	
Title Background Color	#666666	
Font Color	#000000	
Background Color	(#mm	

AD as the primary authentication server, Swivel as the secondary authentication server.

pinsafe : Logon Page > Logon F	orm			
Title	Login			
Message	Please enter your username and password.			
Username Prompt	USERNAME:			
Secondary Username Prompt	2nd Username			
Password Prompt	AD Password			
Secondary Password Prompt	OTC			
Passcode Prompt	Passcode			
Secondary Passcode Prompt	Passcode			
Internal Password Prompt	Internal Password:			
Hide Internal Password	No 🔻			
Group Selector Prompt	GROUP:			
Button Text	Login			
Border Color	#858A91			
Title Font Color	#11111			
Title Background Color	#666666			
Font Color	#000000			
Background Color	#11111			

# Testing

Now the configuration is complete. You can use the configured Group URL to access the ASA with Swivel authentication.

Login
Please enter your user name and click on Get OTP
USERNAME:
OTP
Get OTP

If configured, a Domain Password prompt will appear.

	Login			
L	Joyin			
lease enter your user	name and click on Get OTF			
USERNAME:				
OTP				

Before the user name is entered, the OTP (One Time Password) field is grayed out. Enter a user name and click on Get OTP.

				Lo	gin				
			Pleas	e ent	er you	ır OTF	2		
1	2	3	4	5	6	7	8	9	0
2	6	9)	7	10	-	83	1	4	3
	US	BERN	AME:	user	1				
	ОТ	Έ		••••	1				
				Lo	gin				

OTP login with Domain Password

_	Login
Plea	se enter your OTP
1 2 3 4	5 6 7 8 9 0
9 2 0 1	4 B 6 5 3 Y
USERNAME:	webvpn
OTP	
Domain passw	vord:

Use your PIN to extract the OTP and enter it in the OTP field. If everything is configured correctly, you will see the portal page after clicking on Login. Please note that the Javascript to retrieve the Turing image is executed at the user?s browser. Therefore, the user?s PC must have access to the Swivel URL. It is highly recommended that you configure your Swivel server to use SSL/https to protect the session. Also if you are using a Swivel virtual or hardware appliance, the image can be requested via the built-in image proxy.

The below screen shot shows the use of the Security String Index to tell the user which of their multiple security Strings to use.

	Login
Pleas	e enter your OTP
	00
	ation
OTP	
AD Password	
	Login
AD Password	Login

The below security screen shows a login screen with Turing and SMS on Demand login options.

	Login
Please enter your use	r name and click on Get OTF
USERNAME:	
ОТР	
AD Password	72
Login Get OT	P Request SMS

Ple	ase ente	er you	r OTF			
1 2 3 4	1 5	6	7	8	9	0
0 67	5	4	3	9	8	2
USERNAME: OTP	gfield	]				
USERNAME: OTP AD Password	gfield	•••				

	Login		
Please enter your u	user name and click on Get OTI		
USERNAME:	gfield		
OTP	••••		
AD Password	•••••		
Login Get	OTP Request SMS		

## **Additional Configuration Options**

The Cisco server can be configured to use multiple authentication servers such as Active Directory.

Two Stage and Challenge/Response authentication can also be configured.

The integration uses Swivel as the primary authentication server and AD as the secondary authentication server. It would be possible to change this order.

If you need to reference the secondary password label or field, the IDs are "secondary\_password\_field" and "secondary\_password\_input" respectively.

For example, if you want to change the secondary password prompt from within the customised script, use the following:

## Customisation for One Touch / Push

This section describes how to customise the Cisco ASA login page to support Push authentication (previously One Touch). In order to use One Touch with Cisco ASA, you must have the Swivel software version 3.11.5 or later.

Before applying this customisation, read the article on One Touch to ensure that the Swivel Secure Appliance is prepared.

Follow the instructions on customisation above up to the point where the information panel is enabled. Now insert the following in the information panel:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js"></script>
 <script>
function redirect()
   window.location.replace("https://<swivel_server>:8443/onetouch/onetouch?returnUrl="
        encodeURIComponent(window.location.href) );
var QueryString = function () {
    // This function is anonymous, is executed immediately and
    // the return value is assigned to QueryString!
    var query_string = {};
var query = window.location.search.substring(l);
var vars = query.split("&");
for (var i=0;i<vars.length;i++) {
var pair = vars[i].split("=");
// If first entry with this name
if (typeof query_string[pair[0]] === "undefined") {
    query_string[pair[0]] = == "undefined") {
    yuery_string[pair[0]] === "string") {
    var arr = [ query_string[pair[0]] === "string") {
    var arr = [ query_string[pair[0]], pair[1] ];
    query_string[pair[0]] = arr;
    // If third or later entry with this name
    } else {
      var query_string = {};
           } else
                query_string[pair[0]].push(pair[1]);
           }
     return query_string;
1
    ();
$(document).ready(function(){
   usernamePassedIn = QueryString["username"];
   passwordPassedIn = QueryString["password"];
   claimPassedIn = QueryString["claim"];
   if(typeof claimPassedIn == 'undefined') {
     redirect();
     left claimPassedIn == 'undefined') {
     redirect();
   }
}
     } else {
          $('[name=password]').val(claimPassedIn);
$('[name=username]').val(usernamePassedIn);
document.getElementById("unicorn_form").submit();
});
```

</script>

## Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

#### Image from PINsafe server absent

#### Login page modifications absent

This can be caused if the script has been altered with line feeds inserted in a text editor from wrap around text. View the login page source and see if it contains the page modifications, and are not being displayed correctly.

#### TURing image doesn't change

If you are repeatedly shown the same TURing image for multiple logins, or after refreshing the page, this may be due to page caching settings in your browser. To avoid this problem, change one line in the customisation. Search for the string

```
obj.innerHTML += '
<img border="1" src="'+pinsafeurl+uname.value+'">';
```

and replace it with the following:

obj.innerHTML += '

<img border="1" src="'+pinsafeurl+uname.value+'&random='+Math.floor(Math.random()\*10000)+'">';

This results in a different URL every time the TURing image is displayed, thereby avoid problems with caching.

## **Known Issues and Limitations**

None

# **Additional Information**

We have a prototype customised AnyConnect VPN client available for testing. Please see here for more details.

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