Table of Contents

1 Cisco AnyConnect

2 Introduction

The Cisco AnyConnect client allows authentication using the following methods from Swivel:

- SMS Text
- Mobile Phone Client
- Token
- Taskbar Utility

This document describes a custom AnyConnect Windows client with built-in support for single channel Swivel authentication, both TURing and Pinpad. For the IPSEC client see Cisco IPSEC Client Integration.

Our custom Cisco AnyConnect clients are available for versions 2.4, 3.1, 4.4 and 4.7 of AnyConnect. Note that the 4.4 client has been successfully tested with version 4.5 as well.

3 Cisco AnyConnect Integration

Product Integration

Product	SMS Text	SMS On Demand	Mobile Phone Client	Token	Taskbar Utility	TURing Image	Pinpad	Index number display
Standard Cisco AnyConnect 2.4	Yes	No	Yes	Yes	Yes	No	No	No
Swivel modified AnyConnect 2.4	Yes	No	Yes	Yes	Yes	Yes	No	No
Standard Cisco AnyConnect 3.1	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.4/5	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.7	Yes	No	Yes	Yes	Yes	Yes	Yes	No

The Cisco AnyConnect client should be downloaded from the Cisco website. The Swivel AnyConnect modifications, where available, can be downloaded below.

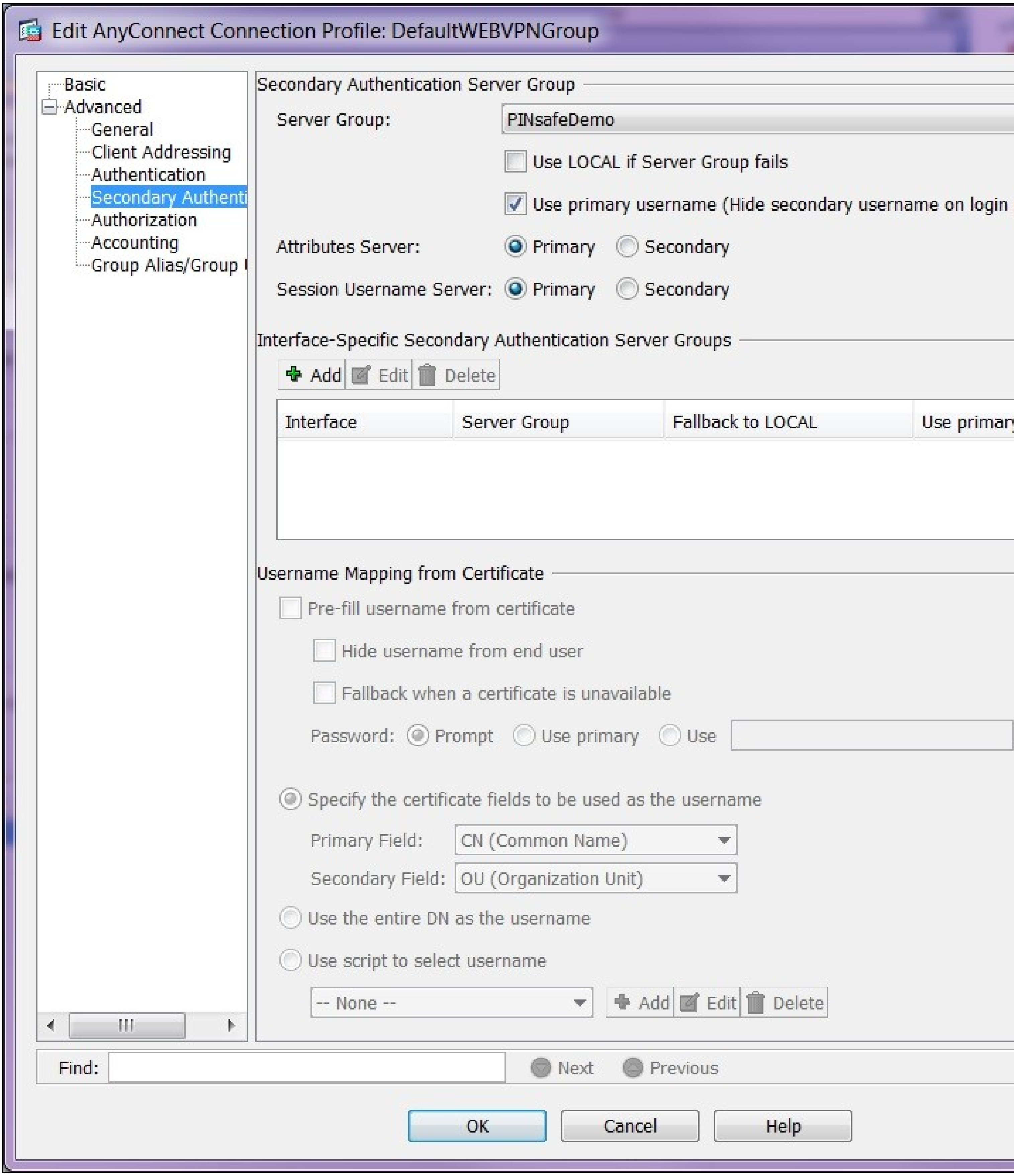
4 Cisco AnyConnect Client Integration

4.1 Configure the Cisco ASA

In order to use Swivel authentication, you need to follow the instructions in Cisco ASA Integration, creating a RADIUS server for Swivel authentication within the Cisco AnyConnect configuration. However, ignore the section on Login Page Customisation, as it is not relevant for the AnyConnect client.

The basic steps for AD Primary and Swivel RADIUS secondary are:

- Configure the ASA for Primary authentication server access, such as AD, and test that it works.
- From Remote Access VPN > AAA/Local Users > AAA Server Groups, create a Swivel group, and add the Swivel RADIUS servers.
- From Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles open the required Connection Profile, and under Advanced Secondary Authentication, set the Secondary Authentication Server Group to the Swivel group.



Edit AnyConnect Connection Profile: DefaultWEBVPNGroup

Secondary Authentication Server Group

Server Group: PINsafeDemo

□ Use LOCAL if Server Group fails

☑ Use primary username (Hide secondary username on login

Attributes Server: ● Primary ○ Secondary

Session Username Server: ● Primary ○ Secondary

Interface-Specific Secondary Authentication Server Groups

Interface	Server Group	Fallback to LOCAL	Use primar

Username Mapping from Certificate

□ Pre-fill username from certificate

□ Hide username from end user

□ Fallback when a certificate is unavailable

Password: ● Prompt ○ Use primary ○ Use

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

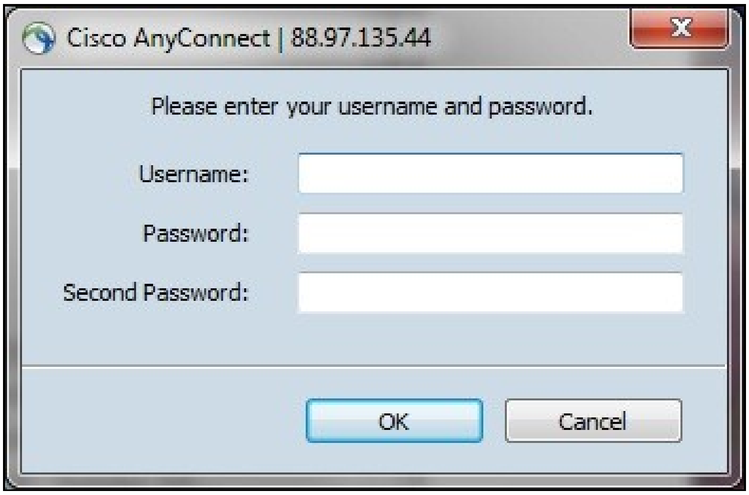
-- None --

When using a Primary authentication service such as Active Directory and a secondary authentication service such as Swivel, the AnyConnect client will display an extra password field, allowing entry of username, password and One Time Code.

4.2 Install the Cisco AnyConnect Client

Download and install the normal Cisco AnyConnect client from your Cisco VPN.

The client should connect and allow authentication using SMS, Mobile Phone Client, Token, and the Taskbar Utility. For PINpad and TURing the below modification is available for testing.



Cisco AnyConnect | 88.97.135.44

Please enter your username and password.

Username:

Password:

Second Password:

5 Swivel modified AnyConnect Client for TURing and PINpad

5.1 Download the client modifications

You can download the 4.7 client from here.

You can download the 4.4 client from here.

You can download the 3.1 client from here.

You can download the 2.4 client from here.

5.2 Prerequisites for the modified client

The client machine must be running a recent Microsoft Windows operating system. This client will not work on non-Windows systems. It has been tested on Windows 7 and XP, but we would expect it to work on any Windows system supported by Cisco.

The client machine must have the Microsoft.Net Framework version 3.5 or later installed. Windows 7 and later will probably have this installed by default.

Your Cisco VPN must support version 2.4, 3.1 or 4.4 of the AnyConnect client.

You must have Swivel 3.4 or later. For Pinpad support, you must either have Swivel 3.9.2 or later, or an appliance with the latest release of the Proxy application.

The client makes a direct call to request the TURing or Pinpad images, so you must have direct access to the Swivel server, or else have a proxy set up to redirect requests. The current version always adds "SCImage" to the URL for TURing images and "SCPinPad" to the Pinpad URL, so you cannot at present use our ASP, ASP.Net or PHP proxy solutions. This will be rectified before the product is released.

5.3 Installation of the Cisco AnyConnect client modifications

Locate the installation directory: by default this is **C:\Program Files\Cisco\Cisco AnyConnect VPN Client**. If you have a 64-bit operating system, the folder will probably be **C:\Program Files (x86)...**.

Take a copy of the file vpnui.exe and rename it or store it in a safe place. You will need to restore this to use the default AnyConnect client again.

Copy the files vpnui.exe, Interop.vpnapi.dll and SwivelSettings.xml from the downloaded zip file into the AnyConnect folder. Alternatively, if you want to keep both clients alongside each other, you can rename the new vpnui.exe to something else.

Run the AnyConnect client. If you get an error at this point, check that you have the right Microsoft.Net Framework library installed.

5.4 Cisco Modified AnyConnect Configuration for PINpad and TURing

The first time you run the client, you will need to configure it. Click the arrow to the right of the **Options** button and select **Preferences** from the pop-up menu.

Fill in the correct settings in the dialog box. For a Swivel Appliance, the Swivel URL should be **https://*<Swivel Server>*:8443/proxy/**. For a software only install see Software Only Installation. If you are using a proxy, or a software-only installation, use the URL appropriate for your installation.

Note the option **PINsafe is primary authentication**. This should be checked if Swivel is the only form of authentication, or is the primary authentication. It should be unchecked if you are using PINsafe as secondary authentication. This option is only relevant for Pinpad, as it determines which password field is populated by the pad.

To add new Cisco VPNs, if yours is not shown, right-click on the box labelled **Use PINsafe for the following connections**, and select **Add Server...**. Note that you can specify that the Swivel security string is not shown for certain VPNs.

Now you have entered the preferences, you should be able to click **Connect** and see the login prompt. After you enter a username, or if you have checked the option to remember the last username, immediately, you should see either a TURing image, or a Pinpad. Use these to enter the Swivel one-time code.

Assuming you have entered the correct credentials, you will be connected to the Cisco VPN, and the client will minimize to the system tray. Click on the tray icon to restore the dialog.

6 Cisco ASA Integration

7 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

7.1 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.

8 Prerequisites

Cisco ASA 8.03 or higher

Cisco documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

8.1 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**.

9 Baseline

Cisco ASA 8.03, Also tested with 8.21

Swivel 3.5, 3.6, 3.7, 3.8, 3.9

10 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

11 Swivel Configuration

11.1 Configuring the RADIUS server

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

11.1.1 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.

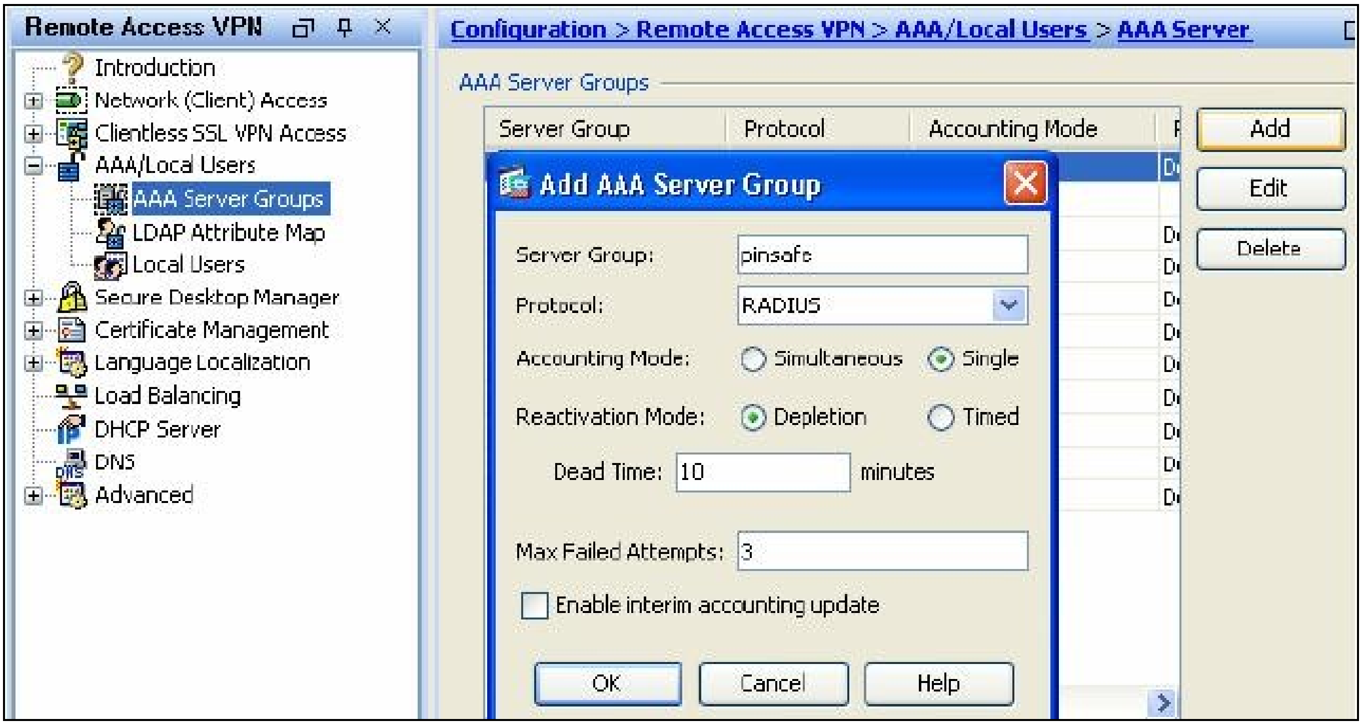
11.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

12 Cisco ASA Configuration

12.1 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.



Add AAA Server Group

Server Group: pinsafe

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

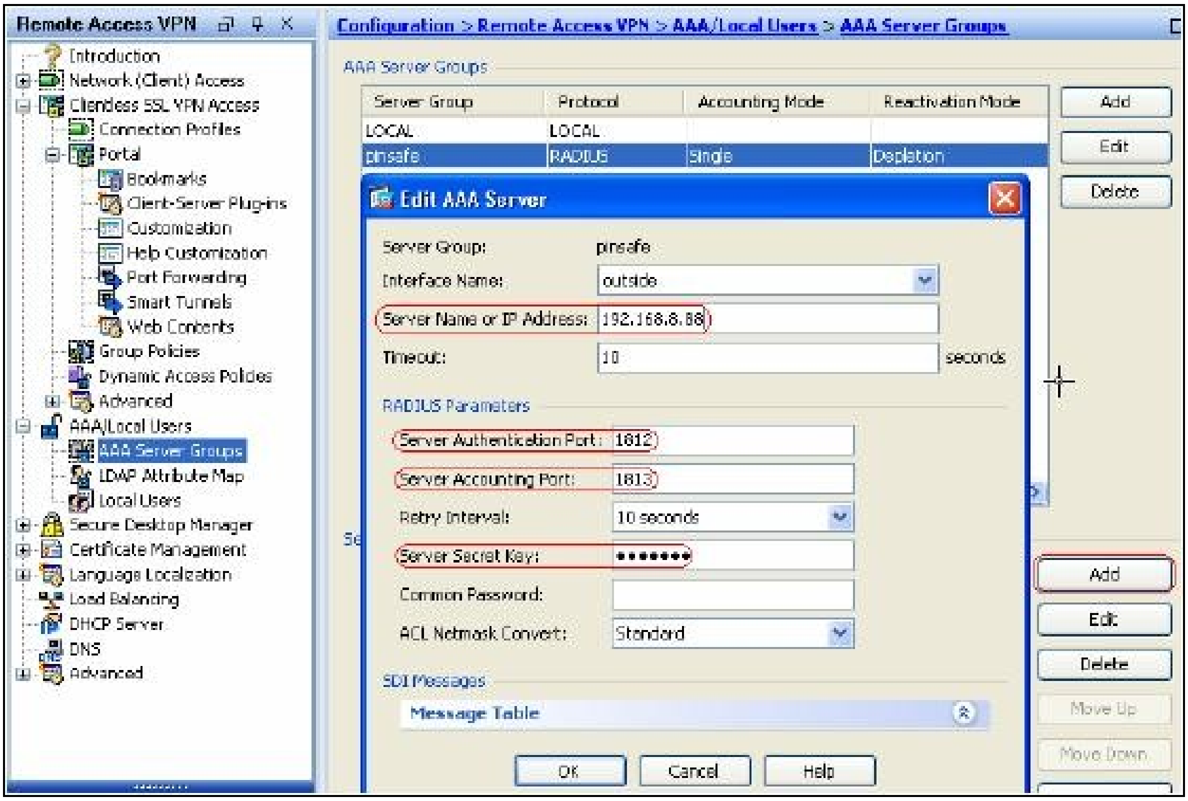
Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

□ Enable interim accounting update

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.



Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		
pinsafe	RADIUS	Single	Depletion

Edit AAA Server

Server Group: pinsafe

Interface Name: outside

Server Name or IP Address: 192.168.8.88

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1812

Server Accounting Port: 1813

Retry Interval: 10 seconds

Server Secret Key: •••••••

Common Password:

ACL Netmask Convert: Standard

SDI Messages

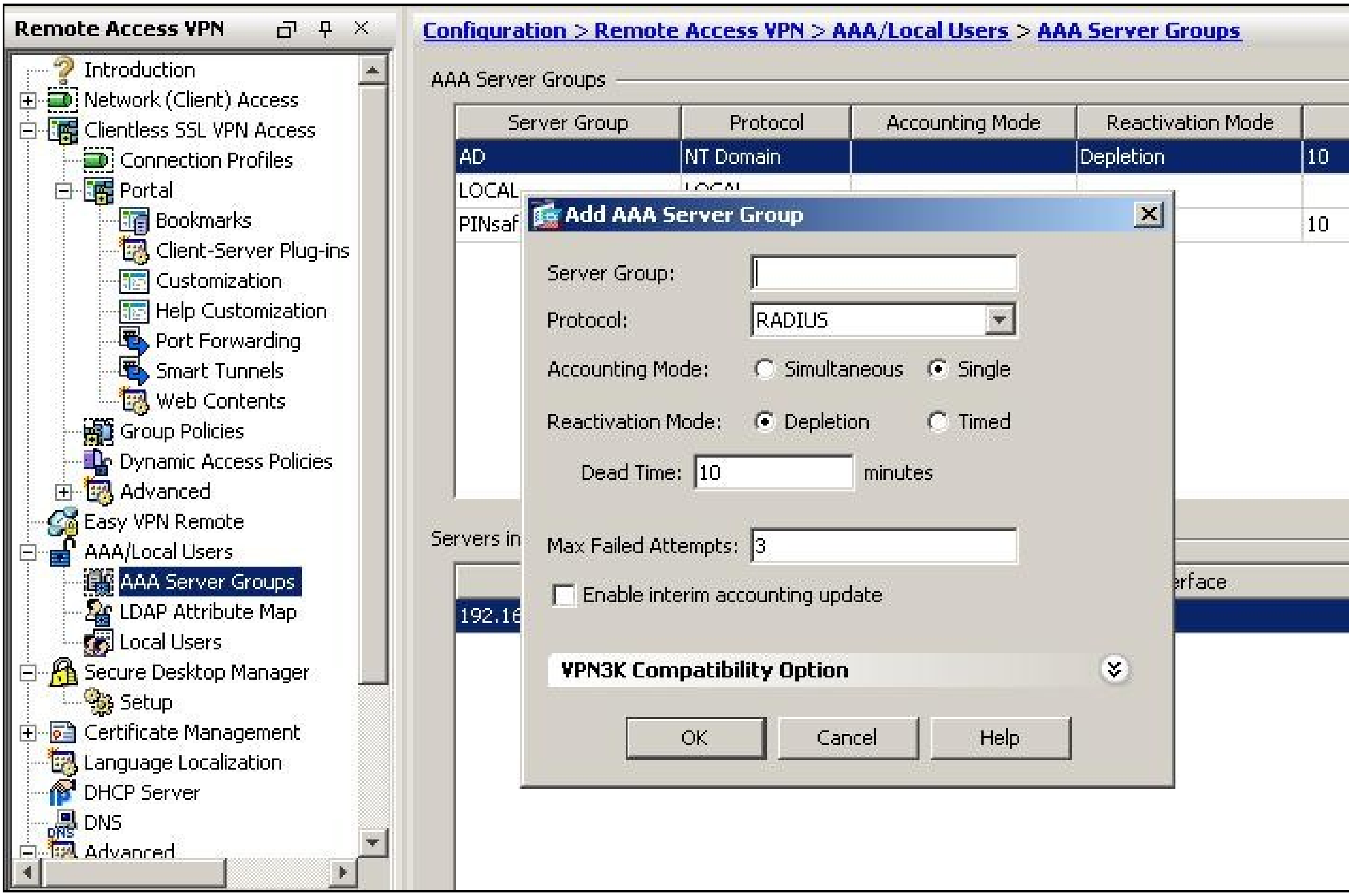
Message Table

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

12.2 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.



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	
AD	NT Domain		Depletion	10
LOCAL	LOCAL			
PINsaf				10

Servers in

192.16

rface

Add AAA Server Group

Server Group:

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

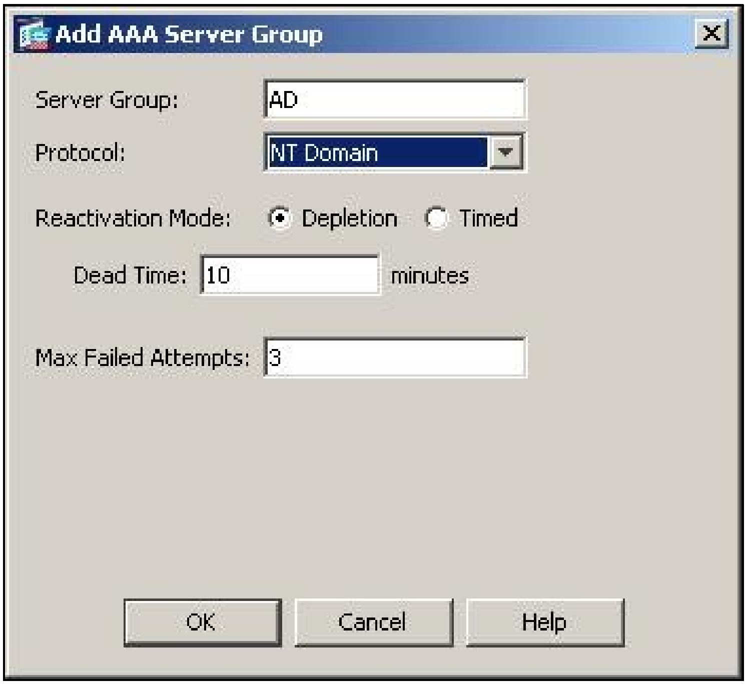
Dead Time: 10 minutes

Max Failed Attempts: 3

□ Enable interim accounting update

VPN3K Compatibility Option

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

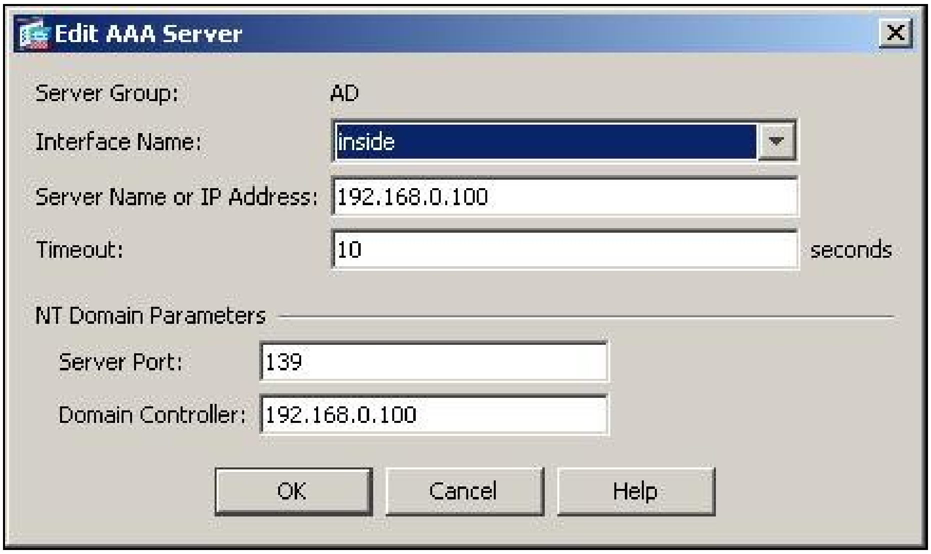
Protocol: NT Domain

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

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


Edit AAA Server

Server Group: AD

Interface Name: inside

Server Name or IP Address: 192.168.0.100

Timeout: 10 seconds

NT Domain Parameters

Server Port: 139

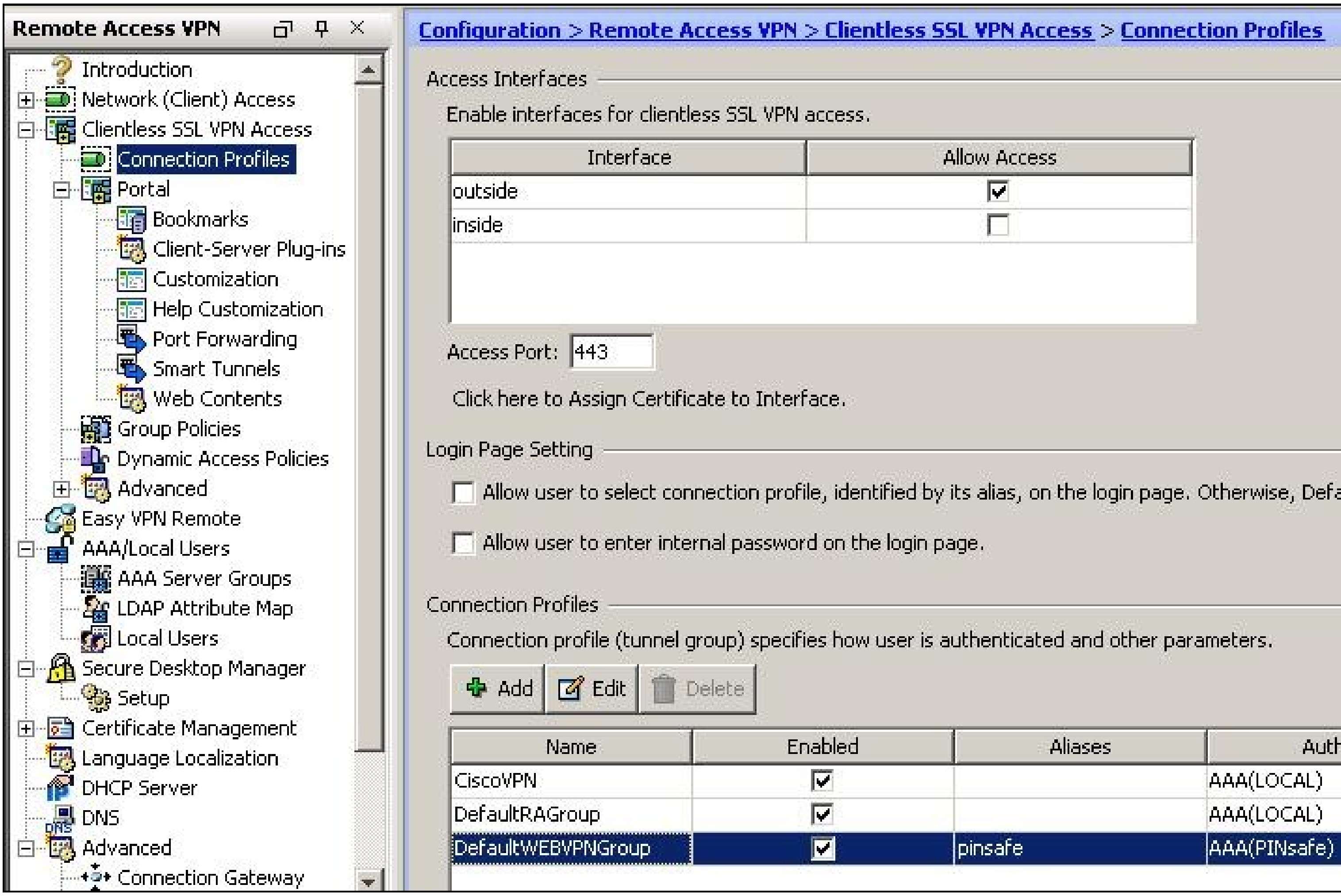
Domain Controller: 192.168.0.100

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

12.3 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.



Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
inside	□

Access Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

□ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, Defa

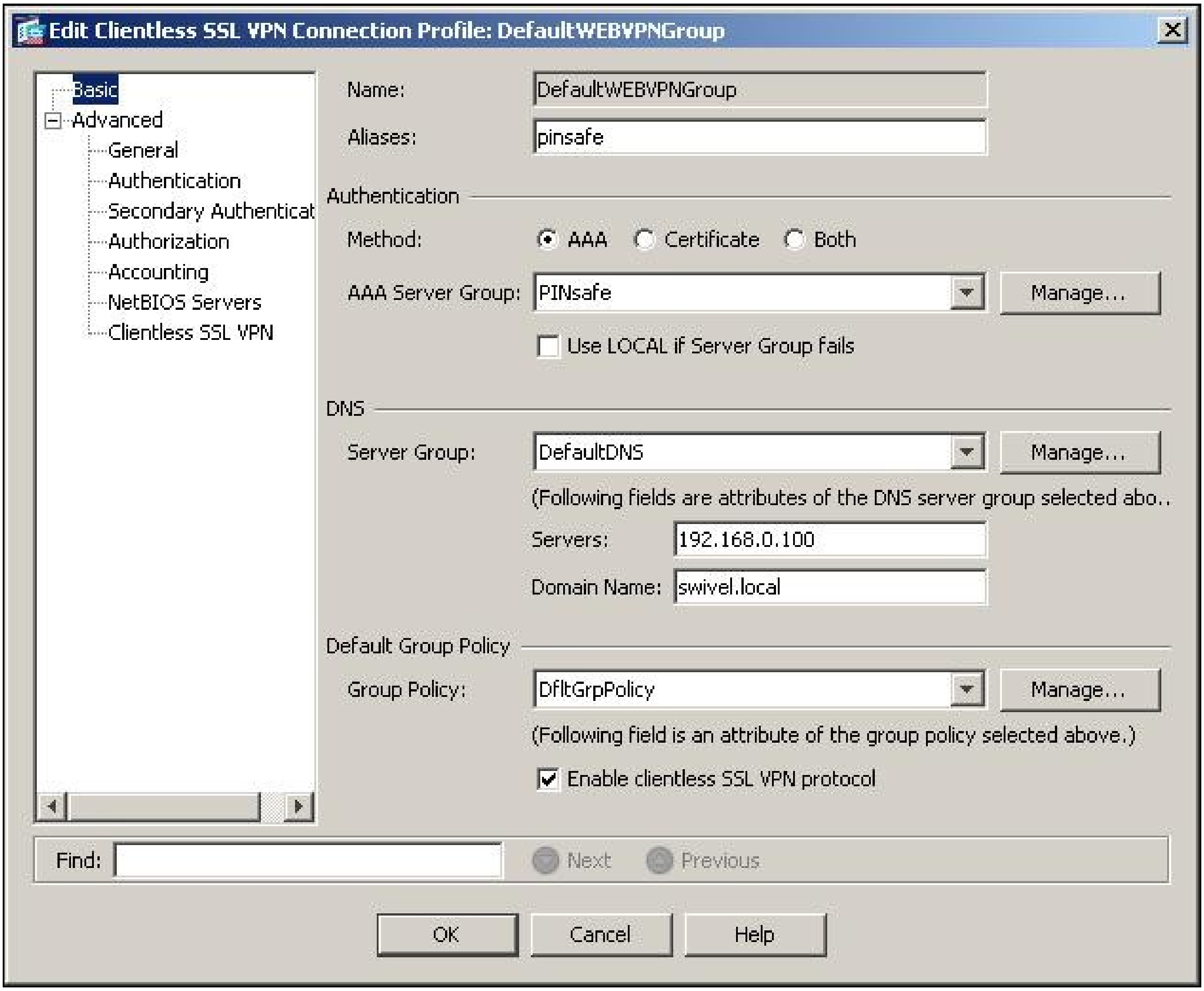
□ Allow user to enter internal password on the login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	Enabled	Aliases	Auth
CiscoVPN	☑		AAA(LOCAL)
DefaultRAGroup	☑		AAA(LOCAL)
DefaultWEBVPNGroup	☑	pinsafe	AAA(PINsafe)

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.



Name: DefaultWEBVPNGroup

Aliases: pinsafe

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: PINsafe

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected abo..

Servers: 192.168.0.100

Domain Name: swivel.local

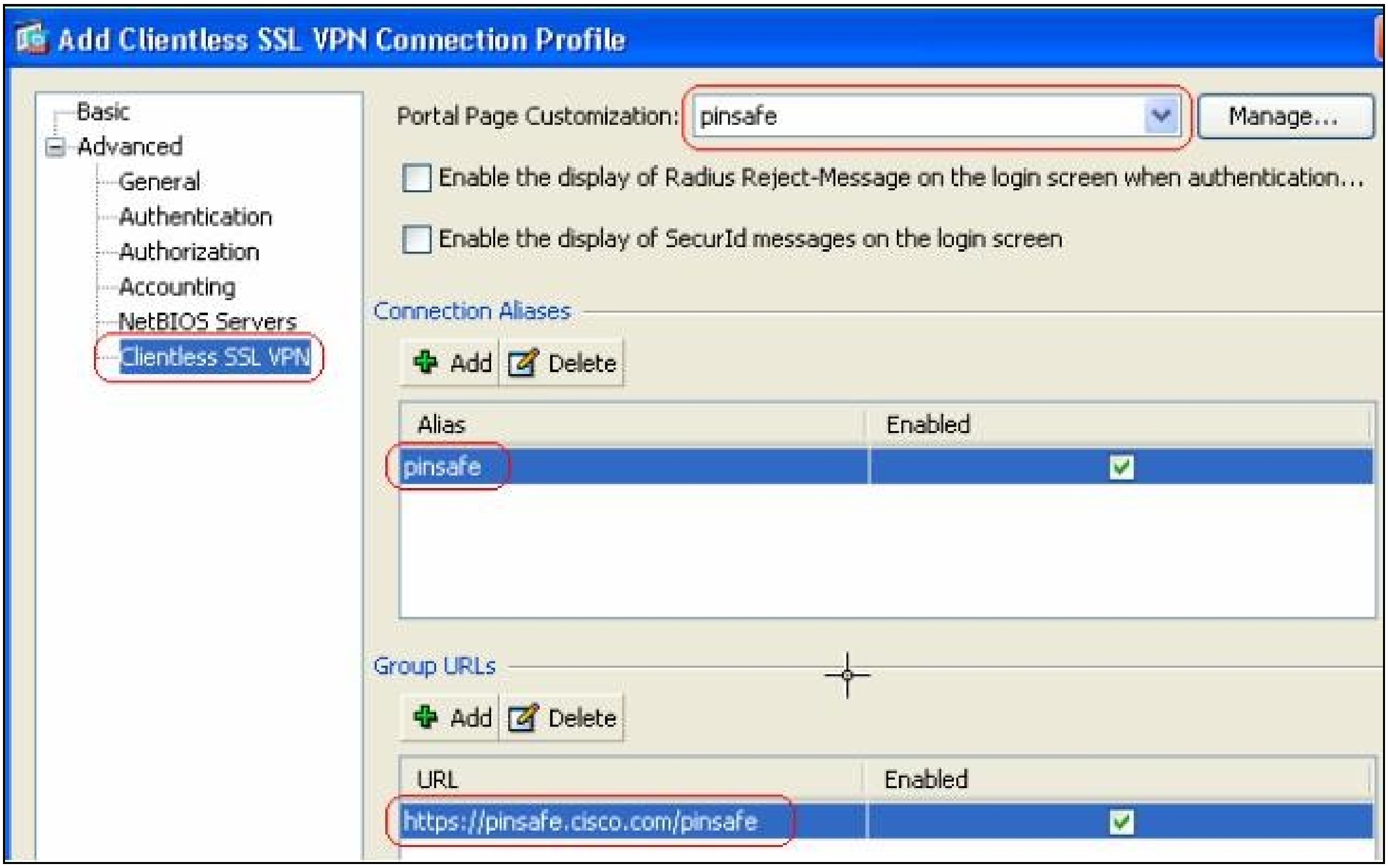
Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

☑ Enable clientless SSL VPN protocol

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.



Portal Page Customization: pinsafe

□ Enable the display of Radius Reject-Message on the login screen when authentication...

□ Enable the display of SecurId messages on the login screen

Connection Aliases

Alias	Enabled
pinsafe	☑

Group URLs

URL	Enabled
https://pinsafe.cisco.com/pinsafe	☑

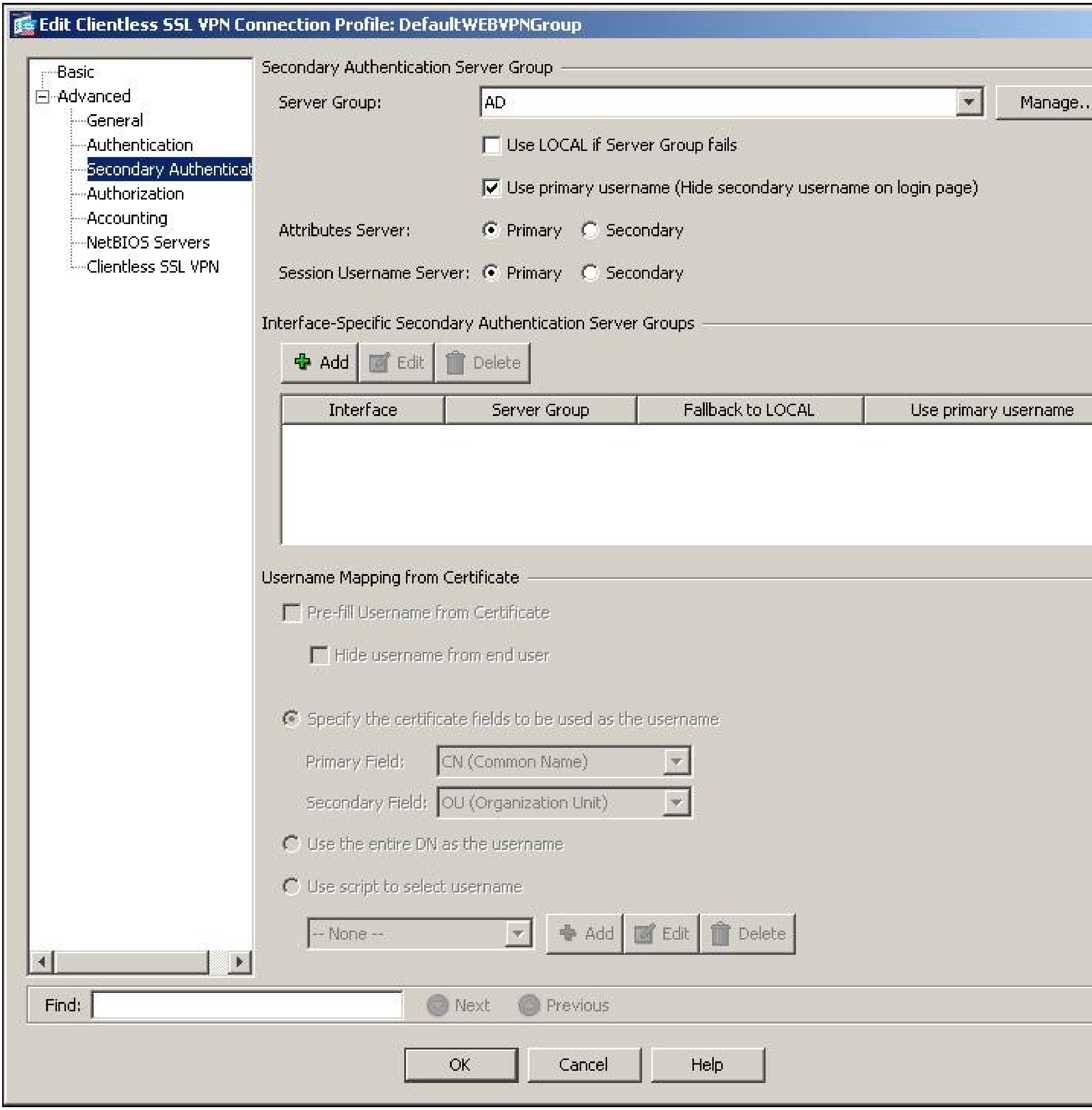
Click on OK then Apply to save the Connection Profile.

12.4 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.


Edit Clientless SSL VPN Connection Profile: DefaultWEBVPNGroup
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Manage..
Interface-Specific Secondary Authentication Server Groups
Add
Edit
Delete
Username Mapping from Certificate
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

Server Group: AD

☐ Use LOCAL if Server Group fails

☑ Use primary username (Hide secondary username on login page)

Attributes Server: ● Primary ○ Secondary

Session Username Server: ● Primary ○ Secondary

Interface	Server Group	Fallback to LOCAL	Use primary username

☐ Pre-fill Username from Certificate

☐ Hide username from end user

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --

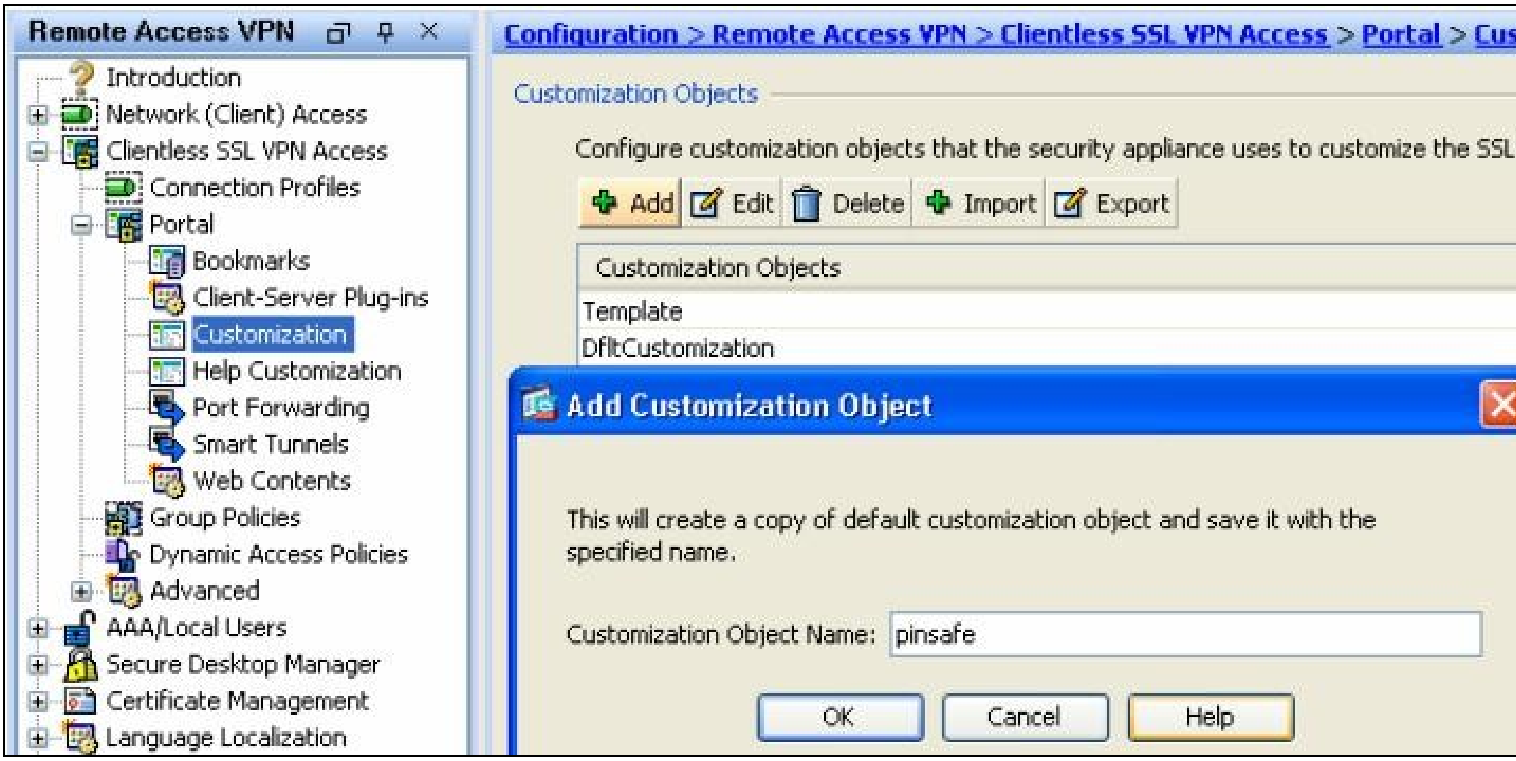
12.5 Test the RADIUS authentication

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.

12.6 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.

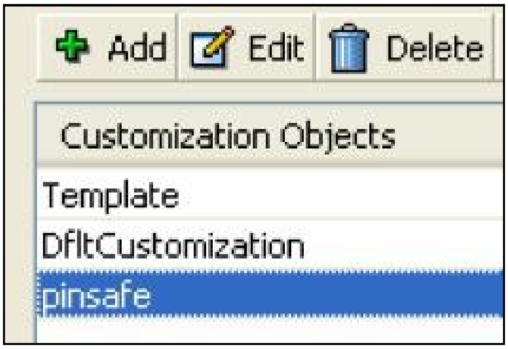


Configure customization objects that the security appliance uses to customize the SSL

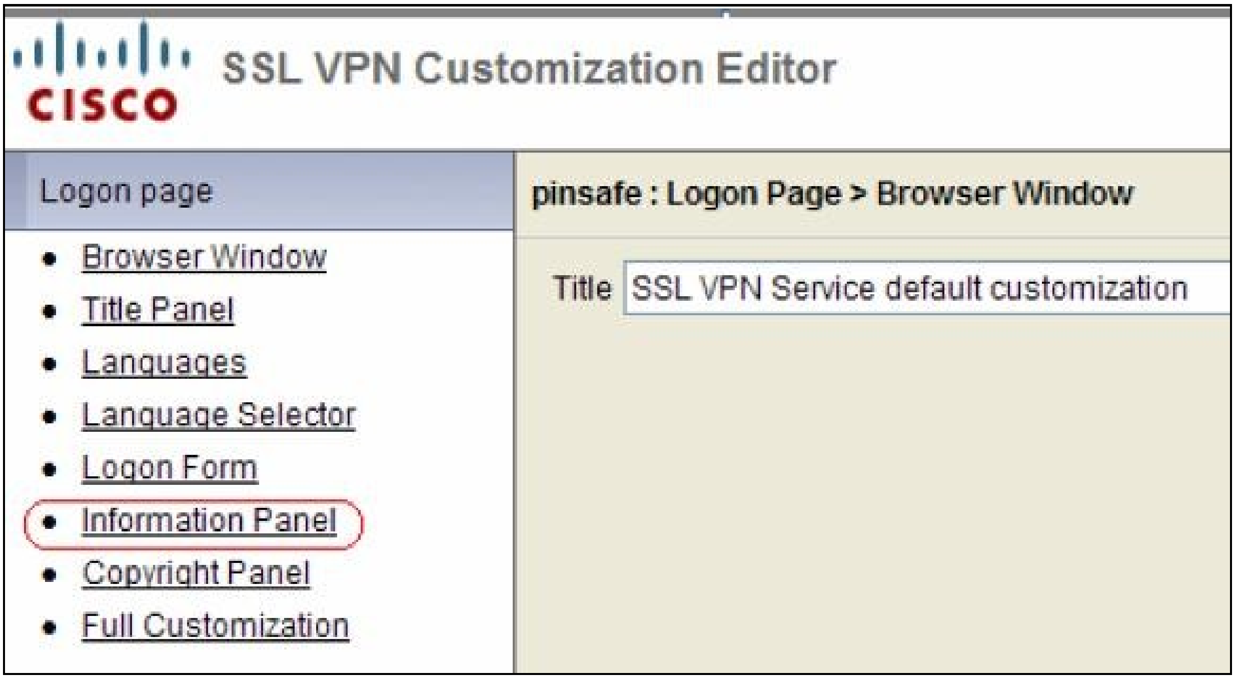
This will create a copy of default customization object and save it with the specified name.

Customization Object Name: pinsafe

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

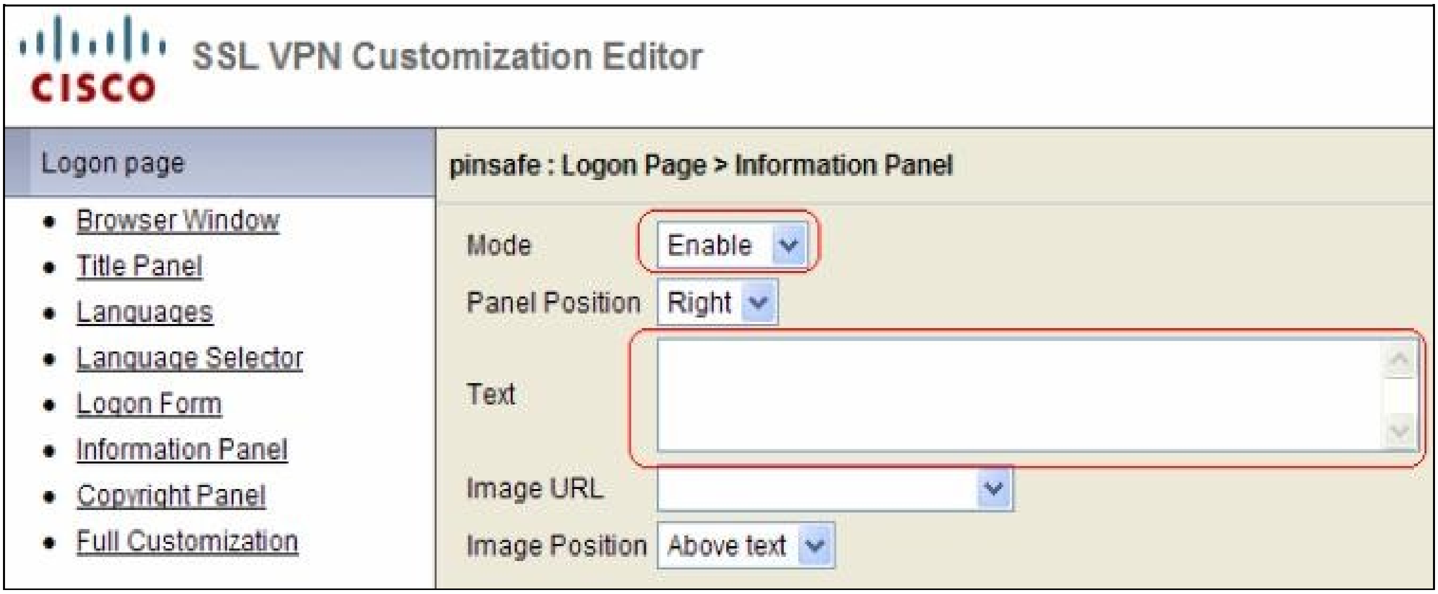


With the new object selected, click on Edit to enter the Customization Editor. Click on the Information Panel menu item. Note: If the information panel has been moved to a different location then the script can be added to the Copyright panel instead.



pinsafe : Logon Page > Browser Window

Title: SSL VPN Service default customization



pinsafe : Logon Page > Information Panel

Mode: Enable

Panel Position: Right

Text:

Image URL:

Image Position: Above text

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 secondaryAuth = true; // set to true if you want Swivel to be the secondary authentication option
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

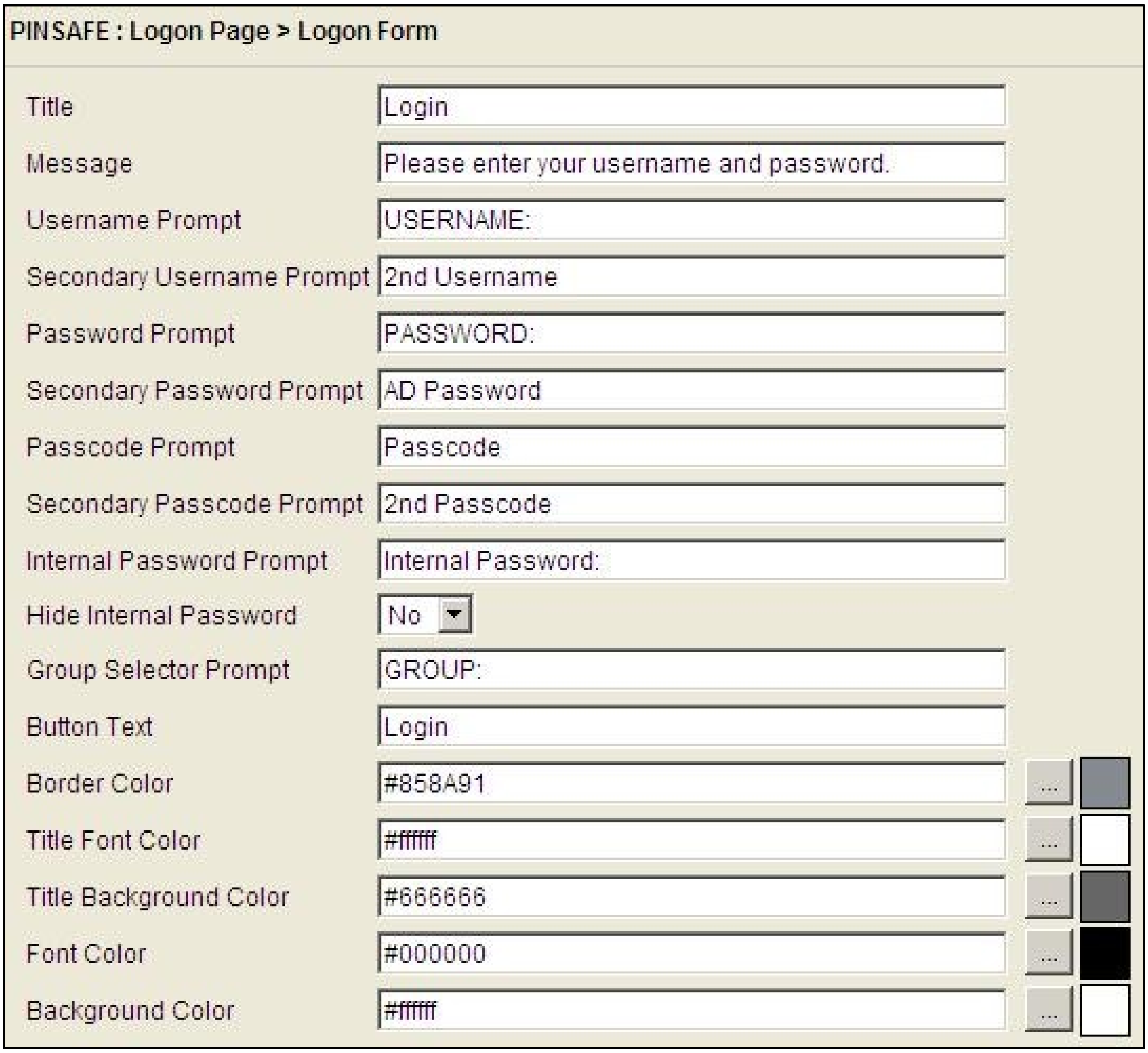
```
"Please enter your user name and click on Get OTP Index";
```

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.

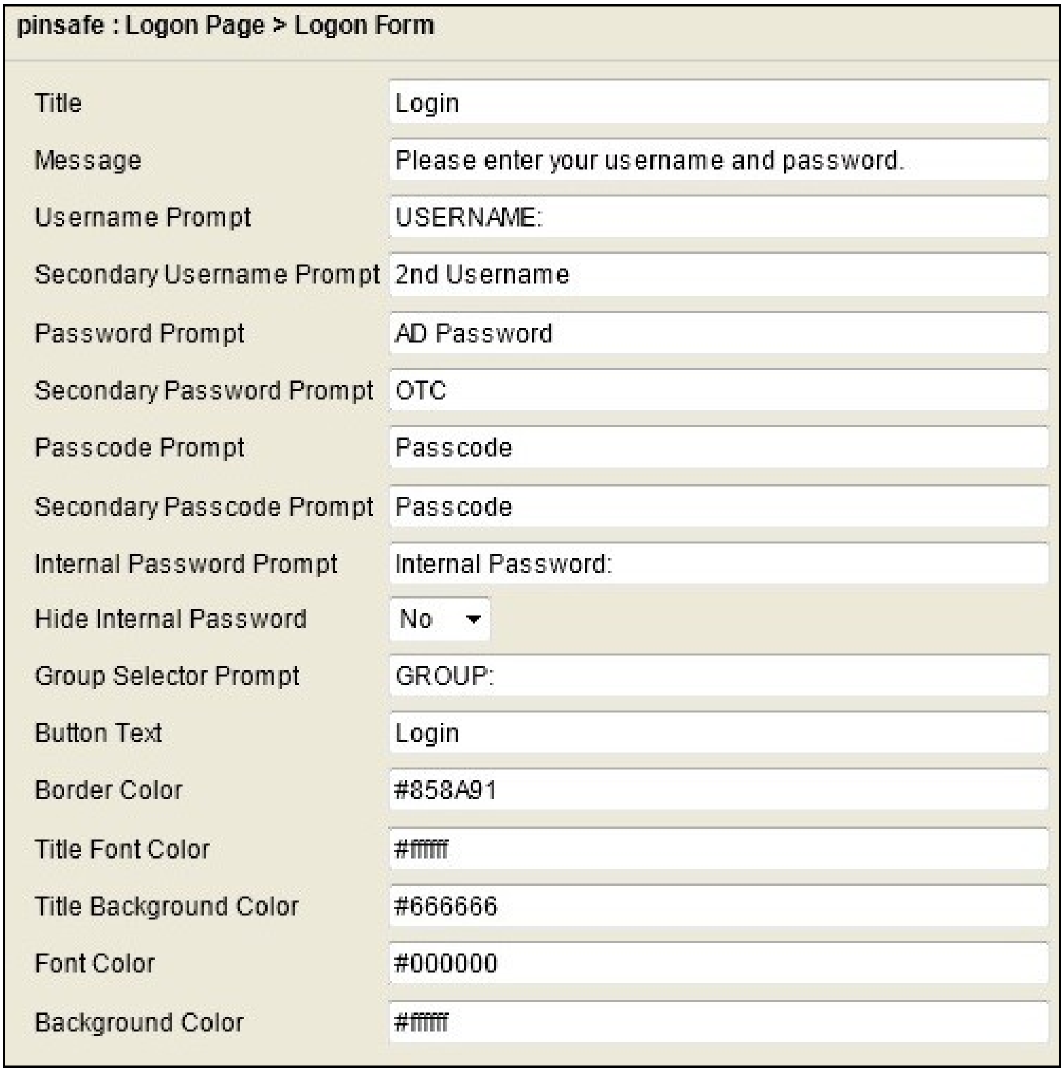
Swivel as the primary authentication server, AD as the secondary authentication server.



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	#ffffff	...
Title Background Color	#666666	...
Font Color	#000000	...
Background Color	#ffffff	...

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

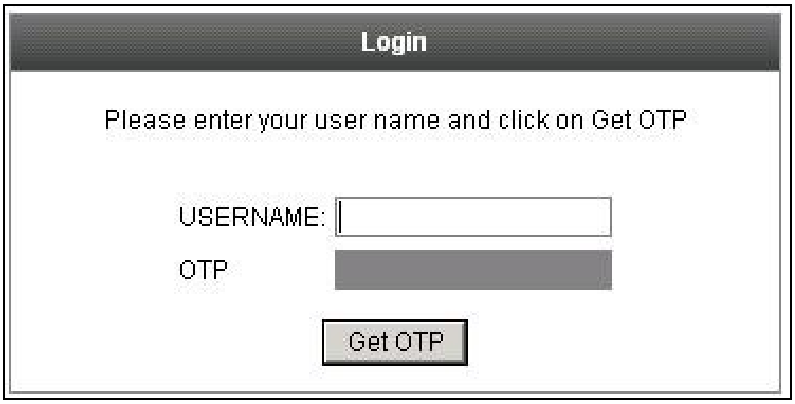


pinsafe : Logon Page > Logon Form

Title	Login
Message	Please enter your username and password.
Username Prompt	USERNAME:
Secondary Username Prompt	2nd Username
Password Prompt	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	#ffffff
Title Background Color	#666666
Font Color	#000000
Background Color	#ffffff

13 Testing

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



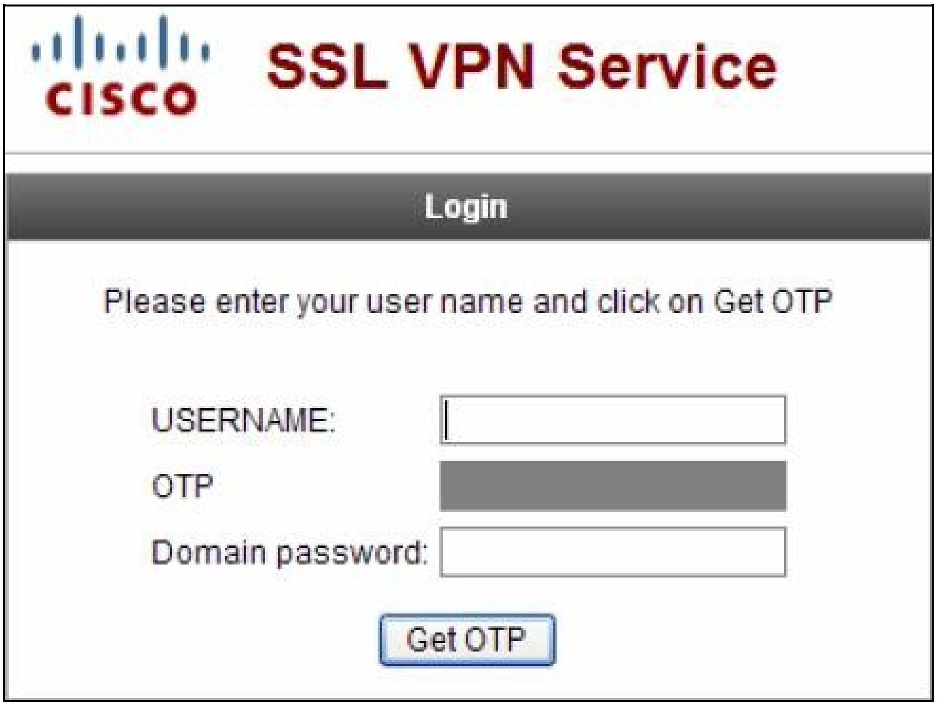
Login

Please enter your user name and click on Get OTP

USERNAME:

OTP

If configured, a Domain Password prompt will appear.



SSL VPN Service

Login

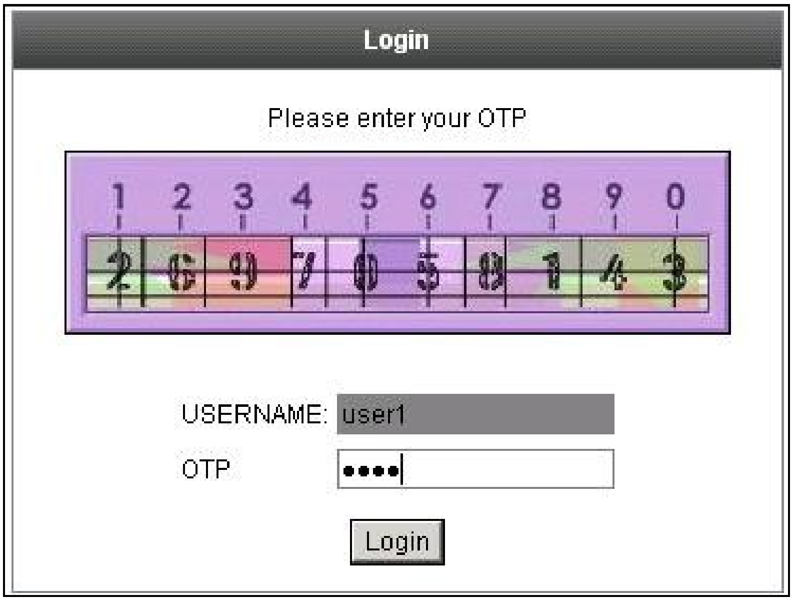
Please enter your user name and click on Get OTP

USERNAME:

OTP

Domain password:

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



Login

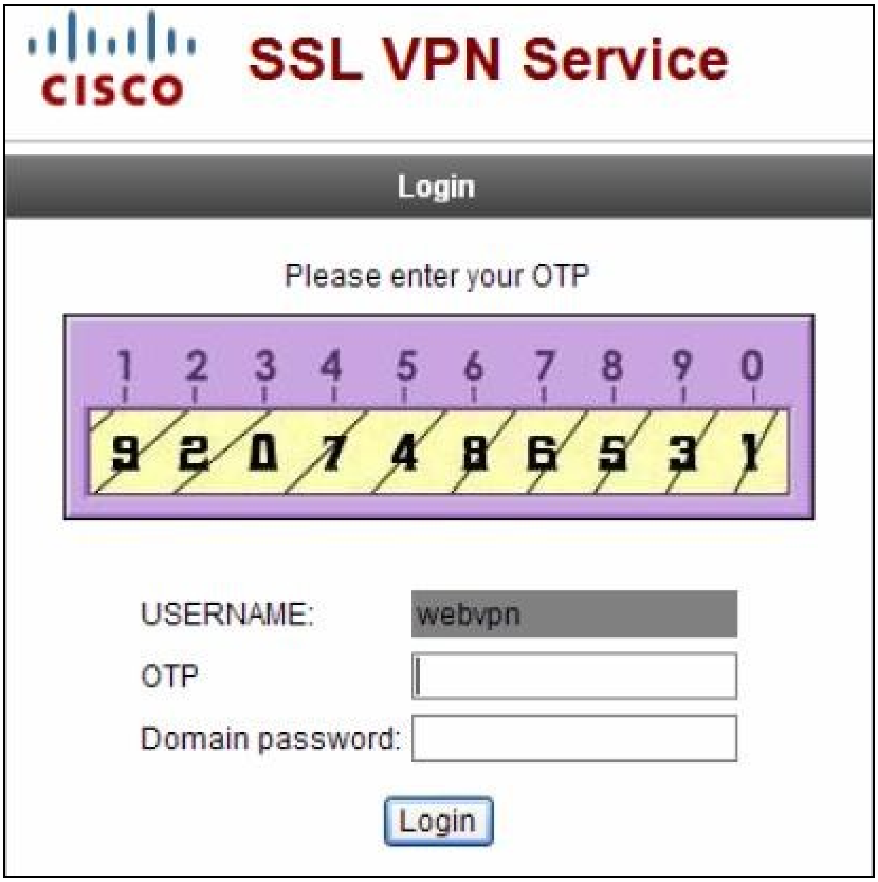
Please enter your OTP

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

USERNAME: user1

OTP ••••

OTP login with Domain Password



Login

Please enter your OTP

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

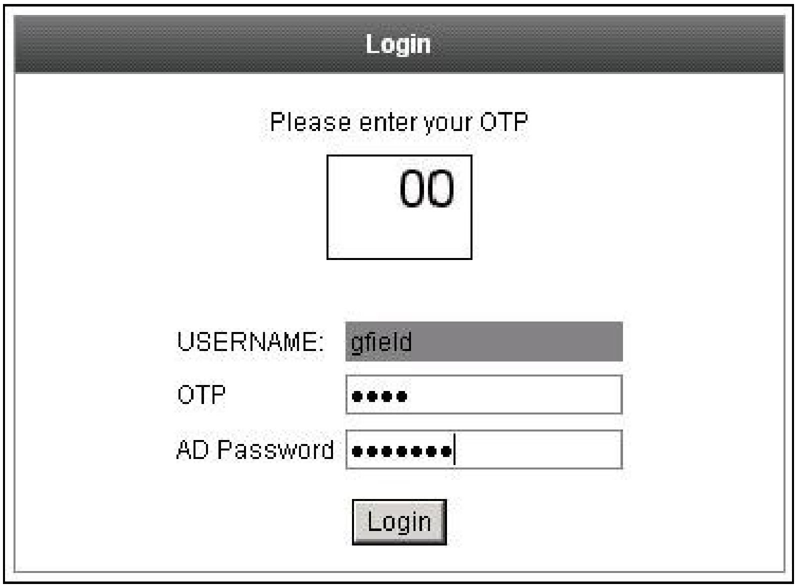
USERNAME: webvpn

OTP

Domain password:

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.



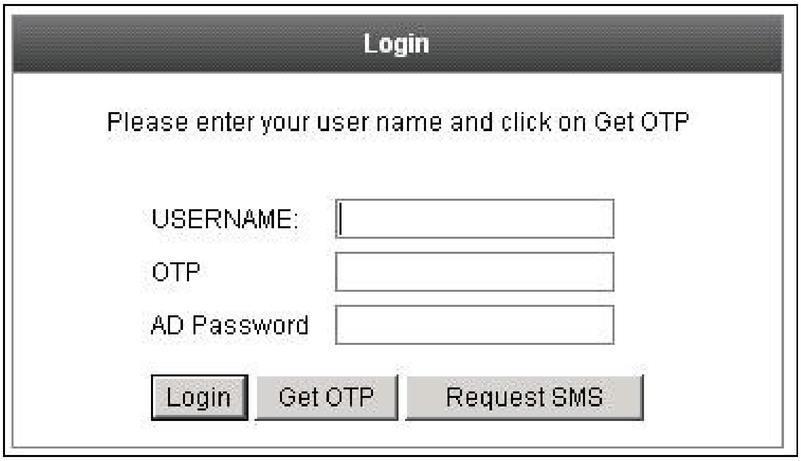
Please enter your OTP

USERNAME: gfield

OTP ●●●●

AD Password ●●●●●●●

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

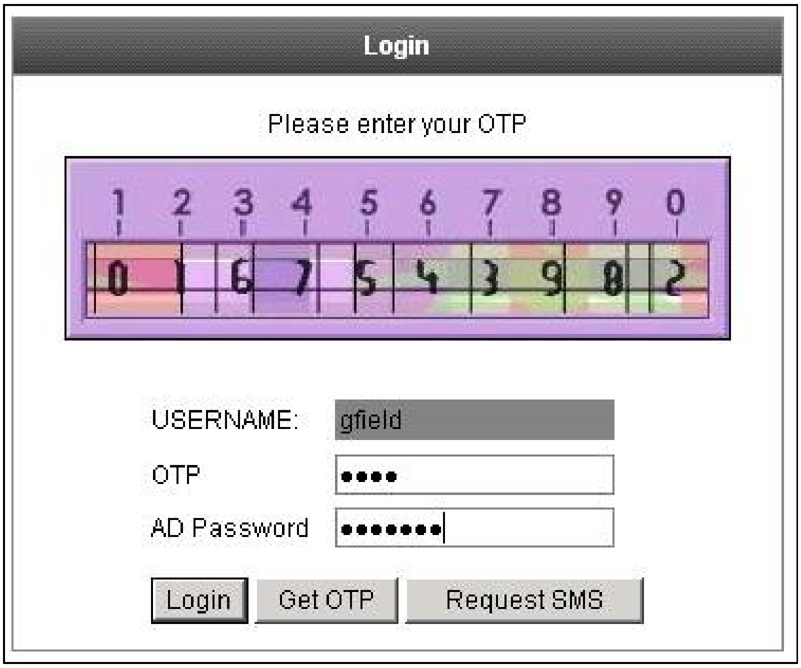


Please enter your user name and click on Get OTP

USERNAME:

OTP

AD Password

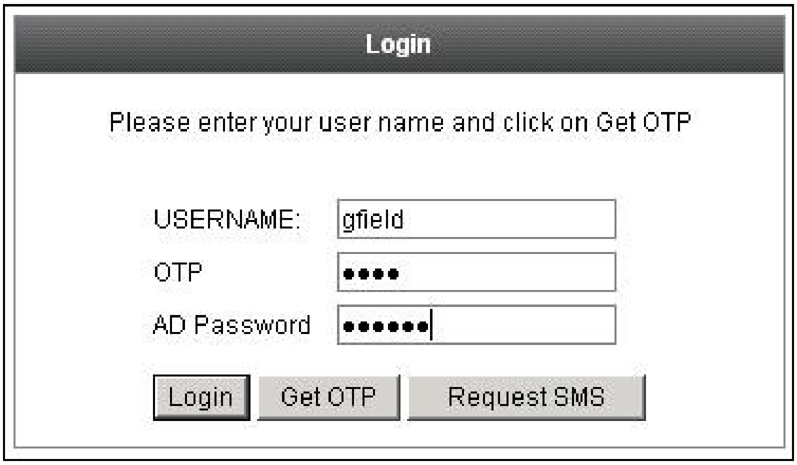


Please enter your OTP

USERNAME: gfield

OTP ●●●●

AD Password ●●●●●●●



Login

Please enter your user name and click on Get OTP

USERNAME: gfield

OTP ●●●●

AD Password ●●●●●●●

14 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:

```
 obj=document.getElementById("secondary_password_field");
 if(obj) {
  obj.innerHTML="AD password";
 }
```

14.1 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(1);
  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]] = pair[1];
    // If second entry with this name
    } else if (typeof 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 {
      query_string[pair[0]].push(pair[1]);
    }
  }
  return query_string;
} ();

$(document).ready(function(){
  usernamePassedIn = QueryString["username"];
  passwordPassedIn = QueryString["password"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
    redirect();
  } else {
    $('[name=password]').val(claimPassedIn);
    $('[name=username]').val(usernamePassedIn);
    document.getElementById("unicorn_form").submit();
  }
});

</script>
```

15 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.

16 Known Issues and Limitations

None

17 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

18 Cisco IPSEC Client Integration

18.1 Introduction

The Cisco IPSEC client allows authentication using the following methods from Swivel:

- SMS Text
- Mobile Phone Client
- Token
- Taskbar Utility

This document outlines how to integrate PINsafe Turing image using the PINsafe Taskbar for Microsoft Windows, with the Cisco IPSEC VPN Client. If SMS use is only required then the below Taskbar steps are not required.

For the Cisco ASA PINsafe integration see Cisco ASA Integration

18.2 Prerequisites

PINsafe 3.x, 3.5 for RADIUS groups

Turing image available to user from across internet

Cisco IPSEC VPN Client

A Cisco Authentication device using PINsafe as a RADIUS server

PINsafe Taskbar for Microsoft Windows

Cisco IPSEC Client

Cisco documentation

18.3 Baseline

PINsafe 3.5

Cisco IPSEC VPN Client 5.0.02

PINsafe Taskbar 1.3.01

18.4 Architecture

The user starts the Cisco IPSEC VPN client which starts up the PINsafe Taskbar utility and generates a Turing image for the user to use for the authentication.

19 Swivel Configuration

19.1 Configuring the RADIUS server

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

19.2 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.

19.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

19.3 PINsafe Client Configration

19.3.1 PINsafe Dual Channel Configuration

No specific client requirements for Dual Channel integration.

19.3.2 PINsafe Single Channel Configuration

Follow the installation notes to install the PINsafe Taskbar utility. Ensure that a Single Channel image can be generated. See Taskbar How to Guide. Note the intehgration has only been tested with the Turing Single Channel Image.

19.4 Cisco VPN Server Configuration

Configure the VPN server according to the Cisco Documentation, configuring the Cisco VPN server to use PINsafe as a RADIUS authentication server.

19.5 Cisco IPSEC Client Configuration

19.5.1 Cisco IPSEC Client with Dual Channel Authentication

No further configuration is required for the Cisco IPSEC client

19.5.2 Cisco IPSEC Client with Single Channel Authentication

Follow the Cisco installation notes. Then open the VPN Client Options menu and choose Application Launcher. The VPN Client displays a dialog, click on Enable and then enter the PINsafe Taskbar utility path and the required syntax:

Example: C:\Program Files\Swivel Secure Ltd\PINsafe Taskbar\PINsafeTaskbar.exe show

Click Apply to activate the application.

Note: The Cisco IPSEC VPN Client may need to be restarted.

19.5.3 Cisco IPSEC client with OTC and AD password

The Swivel server can be configured to use AD password and OTC. On the Swivel Administration console under RADIUS/NAS for the Cisco ASA set Check password with repository to Yes and apply the settings. The Password is entered first followed by the OTC, as passwordOTC. See also Password How to Guide.

19.6 Additional Configuration Options

19.7 Troubleshooting

Start the Cisco IPSEC VPN client, and click on connect. A Turing window should appear. A One Time Code can be obtained for authentication.

Check the PINsafe logs for Turing images and RADIUS requests.

No RADIUS connections seen

Check ports, Cisco uses 1645/1646 by default, Swivel uses 1812/1813 by default.

Cisco continues to use AD/other password instead of Swivel OTC

Rremove the Swivel RADIUS servers, apply the configuration then reenter them. Apply the configuration and then test to ensure RADIUS requests are seen in the Swivel logs.

19.8 Known Issues and Limitations

None

19.9 Additional Information

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

20 Cisco SA 520

20.1 Introduction

This document describes steps to configure a Cisco SA 520 with PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility.

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

Many Thanks to Brian Norrie of NCI Systems in contributing to this article.

20.2 Prerequisites

Cisco SA 520

Cisco documentation

PINsafe 3.x, 3.5 for RADIUS groups

20.3 Baseline

Cisco SA 520 firmware version 2.1.51

PINsafe 3.8

PAP Authentication was tested in this setup

20.4 Architecture

The Cisco 520 makes authentication requests against the PINsafe server by RADIUS.

21 Swivel Configuration

21.1 Configuring the RADIUS server

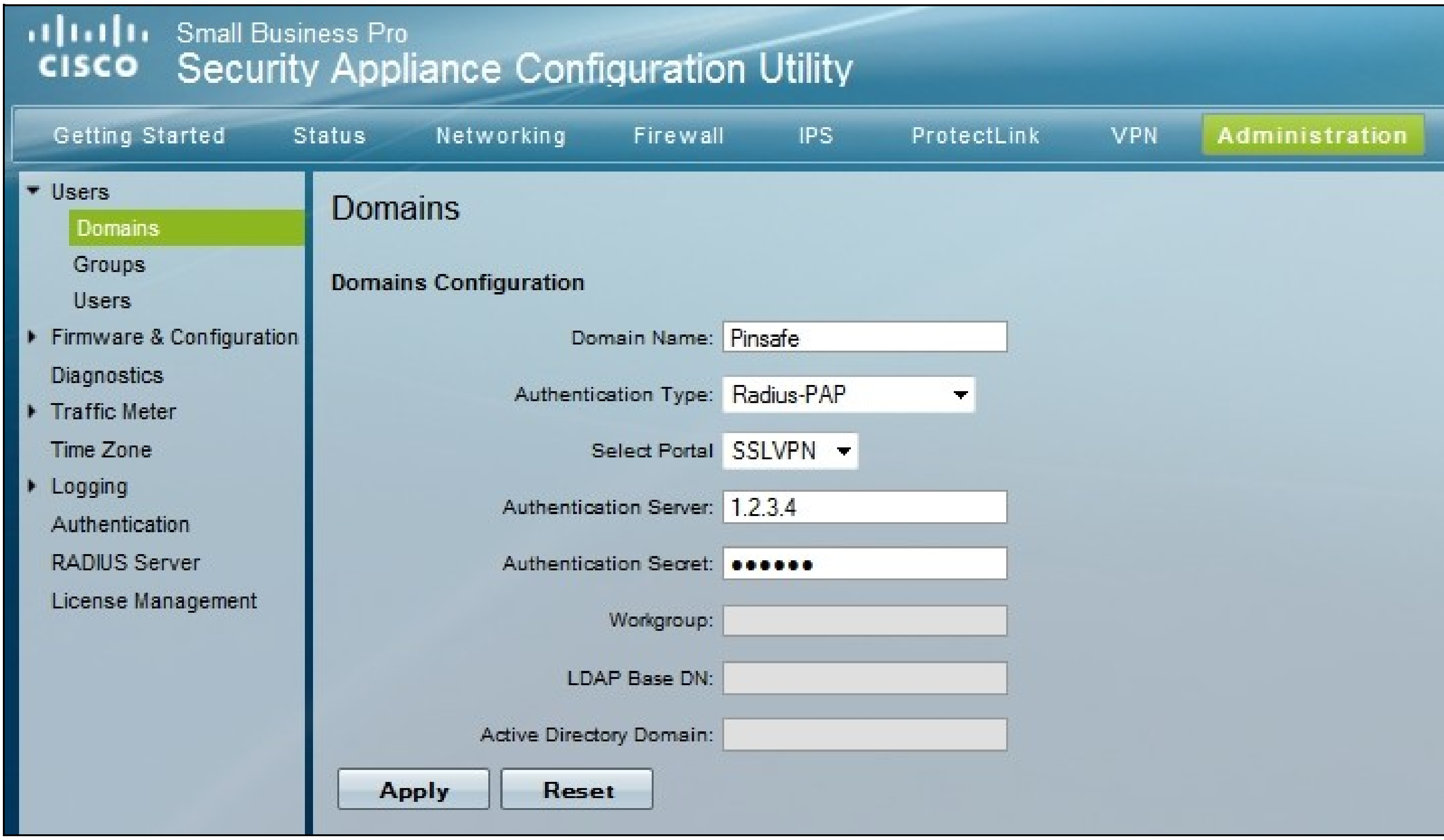
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

21.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

21.3 Cisco SA 520 Configuration

On the Cisco SA 520 Administration console select the Administration tab then users and domains. Click on Add, and enter the PINsafe RADIUS server authentication details for the portal.



Domains

Domains Configuration

Domain Name: Pinsafe

Authentication Type: Radius-PAP

Select Portal SSLVPN

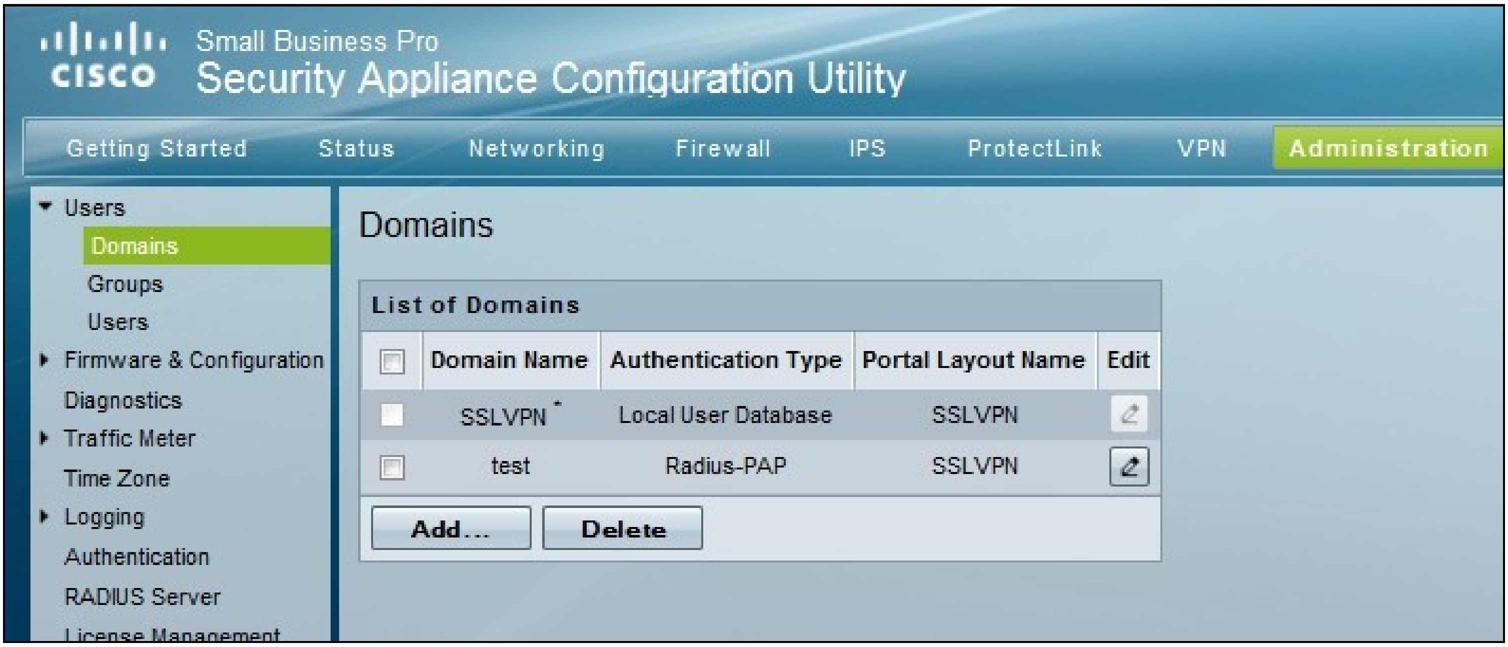
Authentication Server: 1.2.3.4

Authentication Secret: ●●●●●●

Workgroup:

LDAP Base DN:

Active Directory Domain:

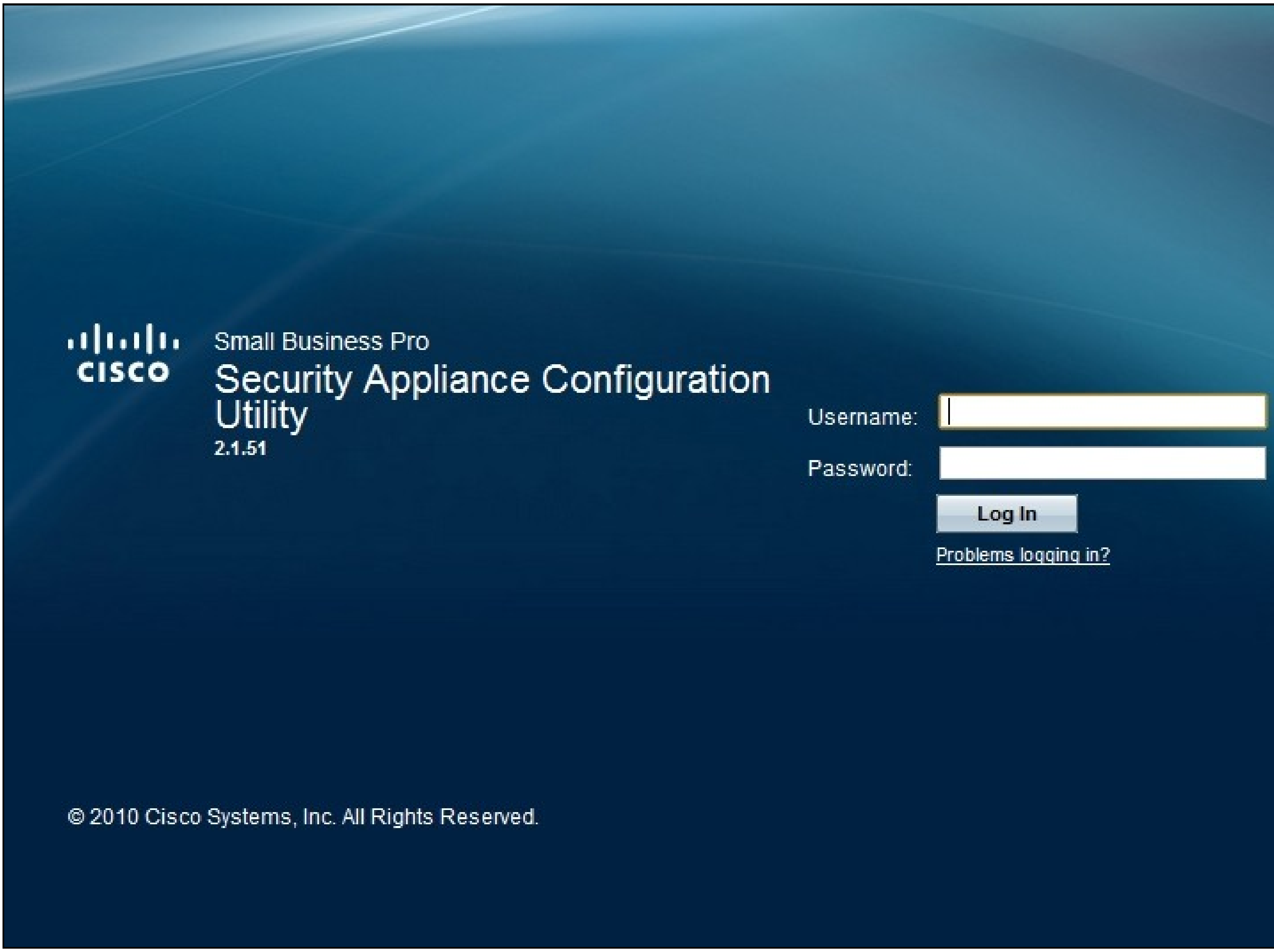


List of Domains

□	Domain Name	Authentication Type	Portal Layout Name	Edit
□	SSLVPN *	Local User Database	SSLVPN	✎
□	test	Radius-PAP	SSLVPN	✎

21.4 Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. You will need to enter your password followed immediately by the one time code into the Password field.


cisco
Small Business Pro
Security Appliance Configuration Utility
2.1.51
Username:
Password:
Log In
Problems logging in?
© 2010 Cisco Systems, Inc. All Rights Reserved.

21.5 Additional Configuration Options

21.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

21.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

21.8 Additional Information

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