Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 AppGate Security Server

2 Introduction

This document describes steps to configure a AppGate Security Server from Cryptozone 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.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page.

3 Prerequisites

AppGate Security Server Appliance

AppGate documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

3.1 Login Page customisation prerequisites

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

4 Baseline

AppGate Security Server Appliance

Swivel 3.8

5 Architecture

The AppGate Security Server makes authentication requests against the Swivel server by RADIUS.

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

6 Swivel Configuration

6.1 Configuring the RADIUS server

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

6.1.1 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.

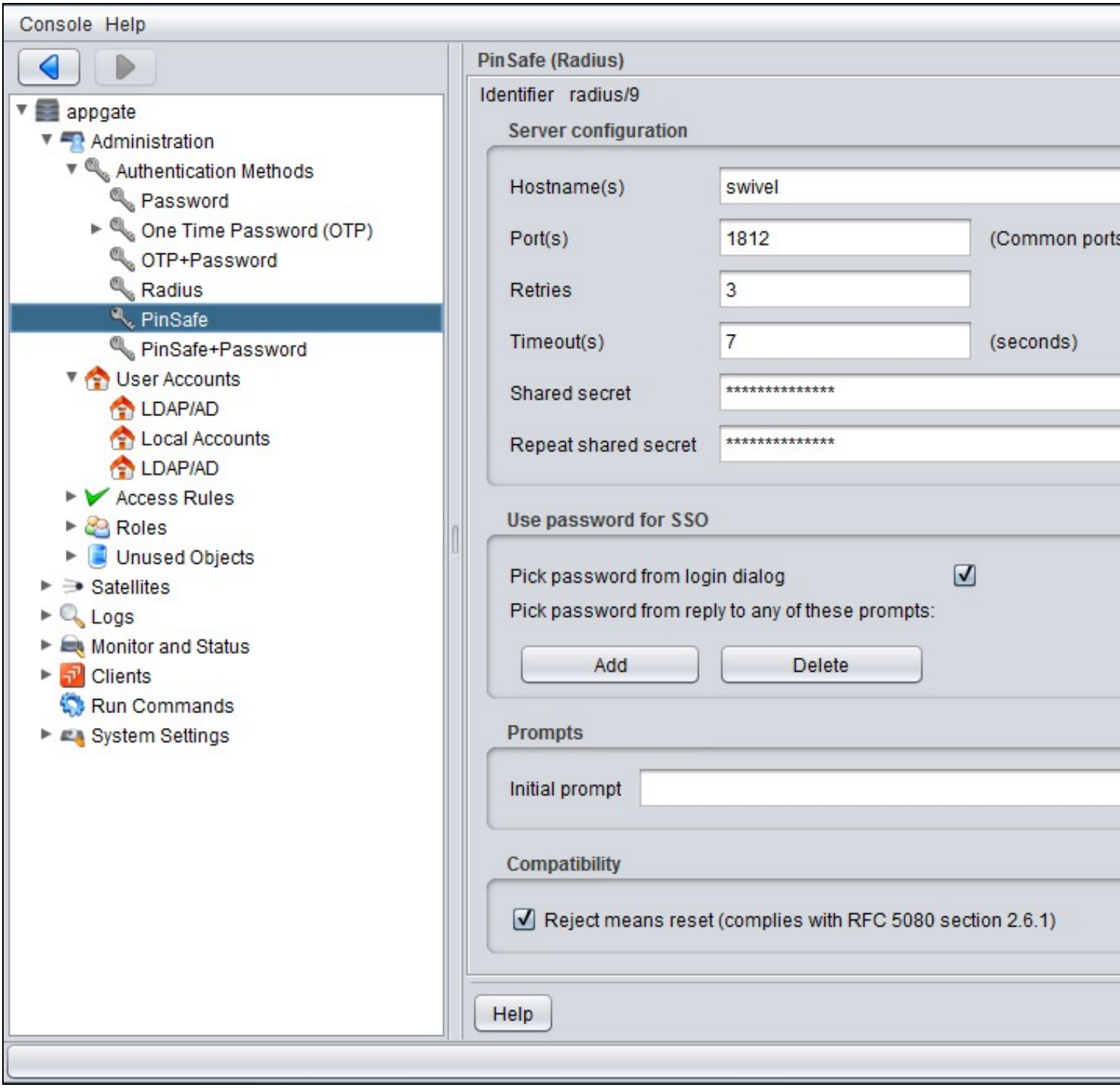
6.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

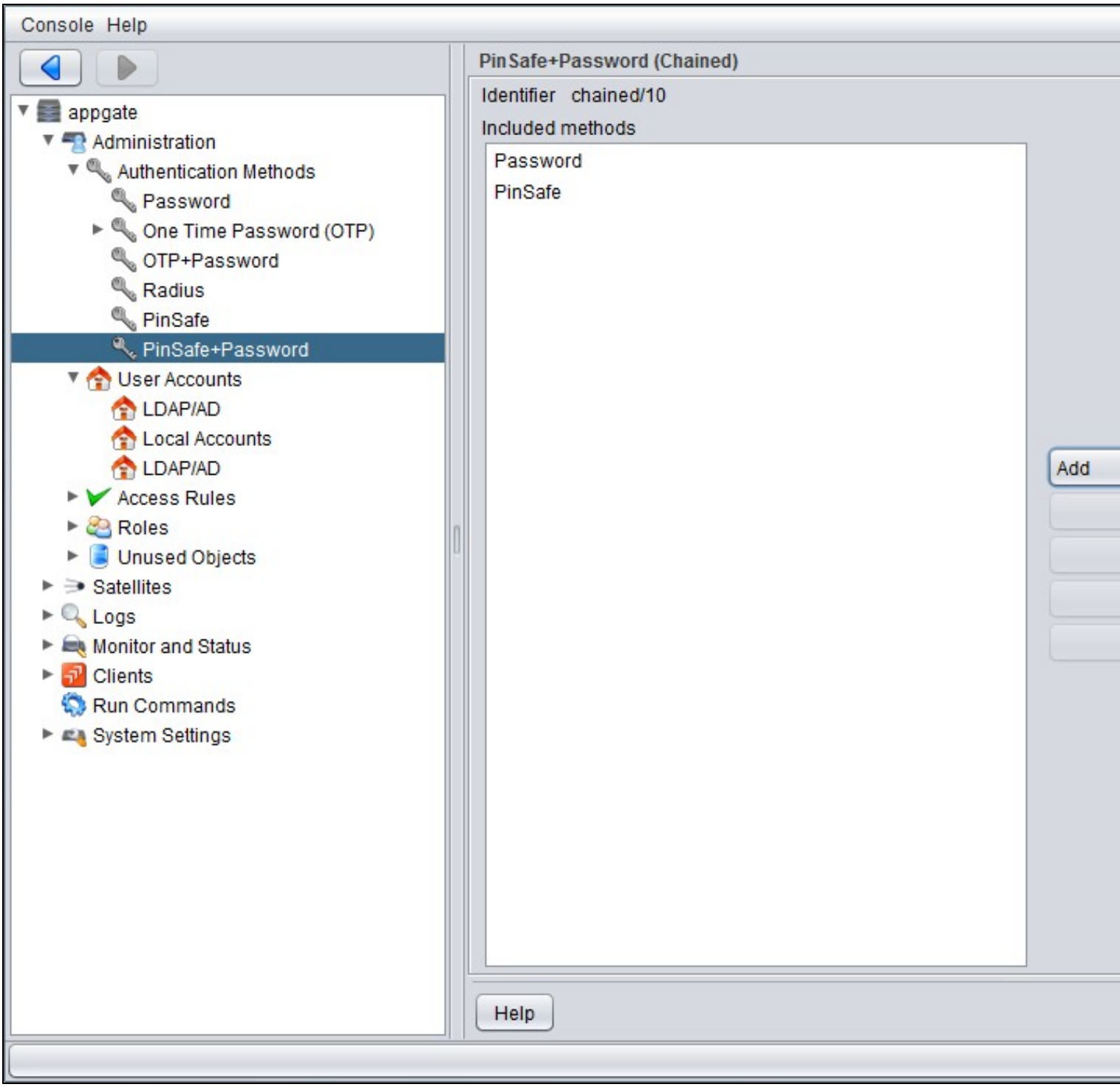
7 AppGate Security Server Configuration

7.1 Adding a Swivel RADIUS server

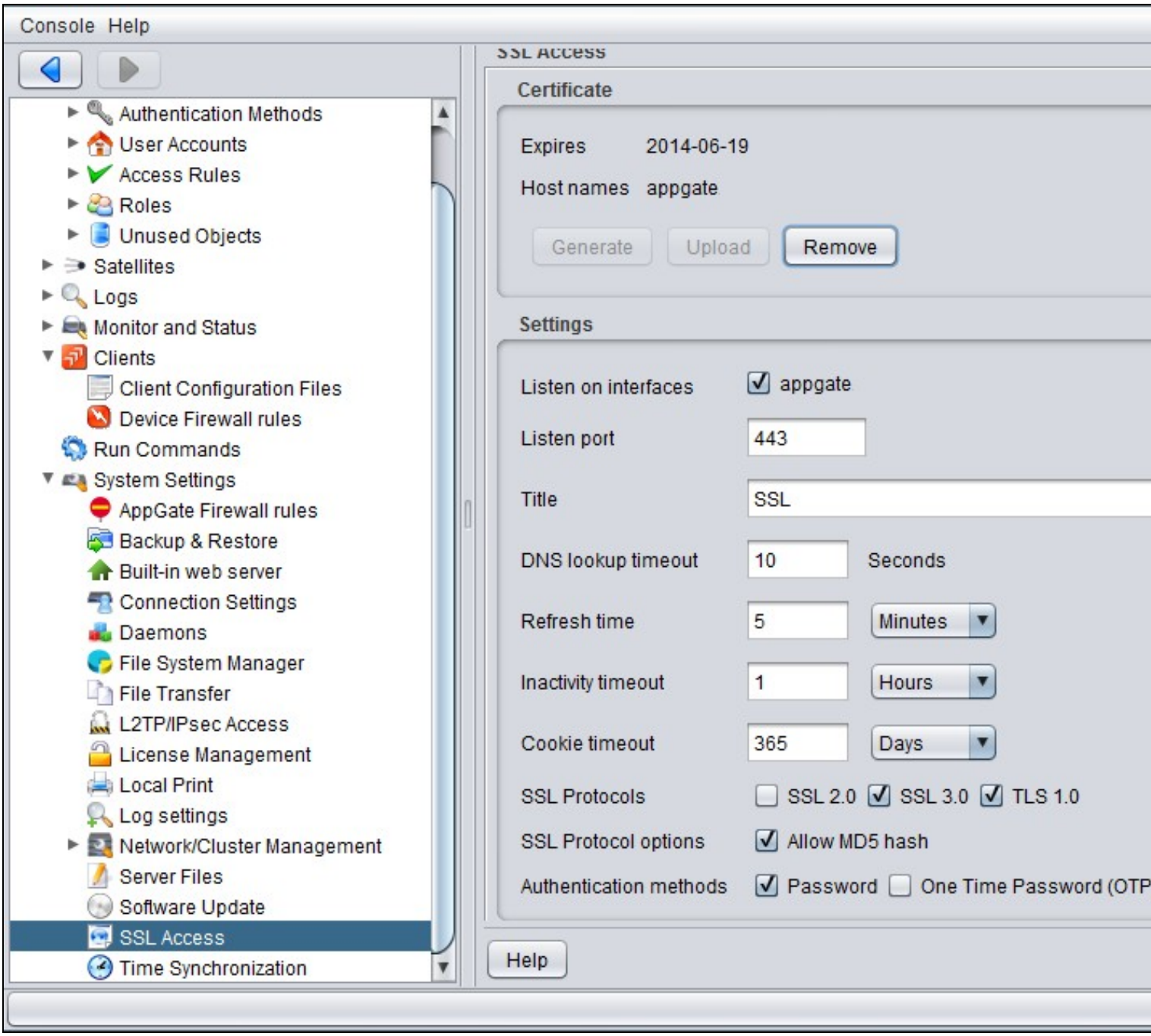
On the AppGate Security Server select Administration/Authentication Methods then Add Authentication Method.



It is recommended to use a password in combination with the OTC and this can be done by using a chained password.



On the AppGate Security Server select Administration/System Settings/SSL Access then select the required Authentication Methods allowed.



7.2 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.

7.3 Optional: Login Page Customisation

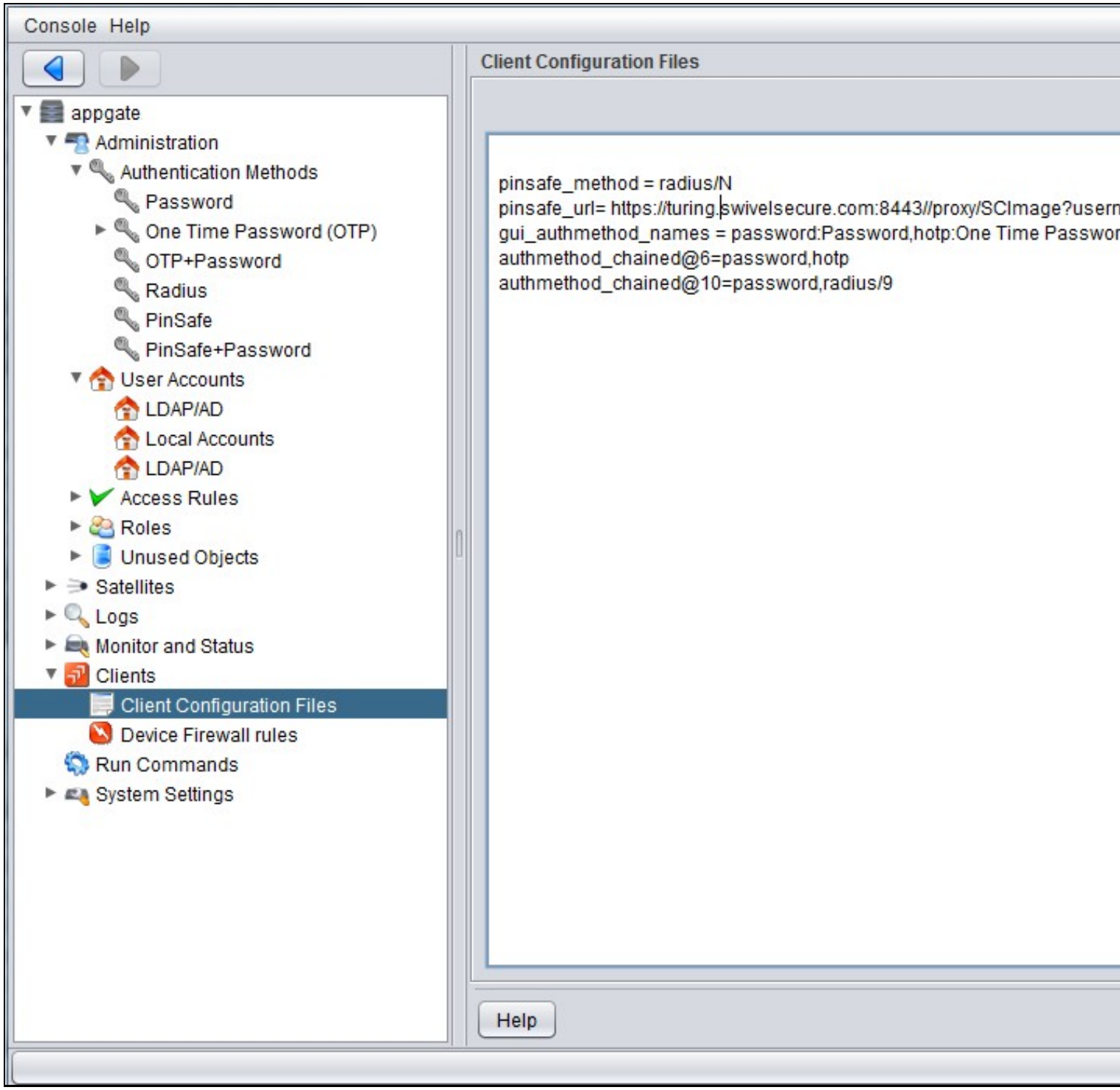
On the AppGate Security Server select Administration/User Accounts and for the required access account type ensure that RADIUS authentication is selecetd under the Authentication tab.

On the AppGate Security Server select Administration/Clients then Client Configuration Files and add the following lines:

pinsafe_method = radius/N

pinsafe_URL = http://server:port//pinsafe/SCImage?username=%u

where server is the Swivel sever public NAT and port the port to the Swivel server, usually 443 for a Swivel appliance. For further informationn refer to the AppGate Security Server documentation under RADIUS/Pinsafe.



8 Testing

9 Additional Configuration Options

10 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

11 Known Issues and Limitations

None

12 Additional Information

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

13 Array Networks SPX Integration

14 Introduction

This configuration document outlines how to integrate Swivel with the Array Networks SPX using password authentication in addition to the Swivel authentication.

15 Additional Contributors

Swivel Secure would like to thank Wender Putters from Connect Data Solutions

16 Prerequisites

Array Network SPX 8.2, 8.3, 8.4

Swivel 3.x

If the TURing is required to be used a NAT is required to the Swivel virtual or hardware appliance

Website to host custom login page, this can be the Swivel virtual or hardware appliance.

Custom login page, this can be downloaded from here: here

17 Baseline

Array Networks SPX 8.2.2.0 and also 8.4.4.2 Build 9

Swivel 3.5 and Swivel 3.7

18 Architecture

The Array Networks SPX makes authentication requests against the Swivel virtual or hardware appliance by RADIUS. The login page is redirected from the Array Networks SPX onto another web server. The Swivel virtual or hardware appliance can be used to host this page. The hosted page must be accessible from the internet.

If the AD password is required to be used then these are added together into the RADIUS request, and Swivel has to have the *require password* and *check password with repository set to yes*. Remember that in Swivel 3.7 and earlier this is a global setting. In Swivel 3.8 it is possible to set password checks by NAS devic rather than being a global setting.

19 Installation

20 Swivel Configuration

20.1 Configuring the RADIUS server

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

20.2 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.

20.3 Configure Password

Swivel 3.7 and earlier

If the AD Password is required to be used, on the Swivel Administration Console select Policy/Password, enable *Require Password* and *check password with repository*

Swivel 3.8 and later

If the AD Password is required to be used, on the Swivel Administration Console select RADIUS NAS, enable *check password with repository*

21 Configure the custom login page

21.1 Editing the Login Page

Edit the file login.html with the required values

The externally accessible IP address of the Swivel virtual or hardware appliance needs to be set for the following lines:

_AN_base_host = "http://192.168.100.100:8080";

_AN_base_path = "http://192.168.100.100:8080/login";

sUrl = "https://192.168.100.100:8443/proxy/SCImage?username=";

Change the IP address for that of the public URL. For a Swivel virtual or hardware appliance the sURL also needs to be changed as follows:

For a Virtual or hardware appliance:

sUrl = "https://IP:8443/proxy/SCImage?username=";

For a software only install see Software Only Installation

21.2 Copy the login page files

The login page can be hosted on a web server. Note that this page needs to be accessible from the internet by the client.

To use Swivel as a to host the login page:

Copy login.html to one of the following locations:

Swivel Virtual or hardware Appliance: create the folder ROOT in /usr/local/tomcat/webapps2 using a program such as WinSCP, see the WinSCP How To Guide, then ensure that the ownership/group of the folder and file are *swivel* and permissions for the ROOT folder are rwxrwxr-x. Copy in the file login.html and ensure the permissions are rw-rw-r--, and it is owned by the swivel user.

Software only install: <path to Tomcat>/webapps/ROOT

Test that the web page is accessible

Virtual or hardware appliance: http://IP of Swivel server:8443/login.html

For a software only install see Software Only Installation

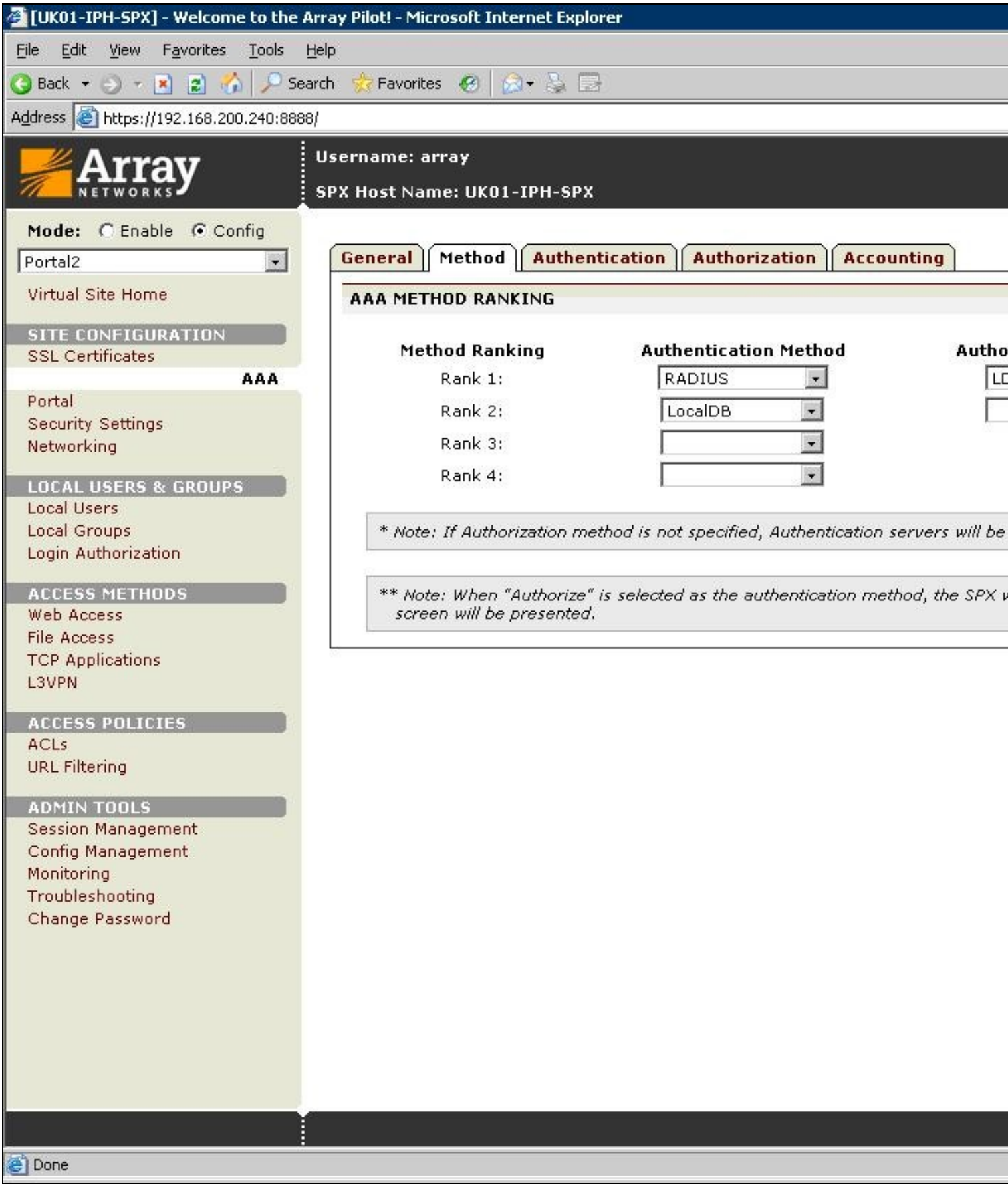
21.3 Create a Failed Login Page

When a login fails, the page redirects, to ensure that this is a Swivel login page either redirect the login failure back to the Swivel login.html, or make a copy of that file and edit it as required, such as to indicate that a login has failed.

22 Configure the Array Networks SPX

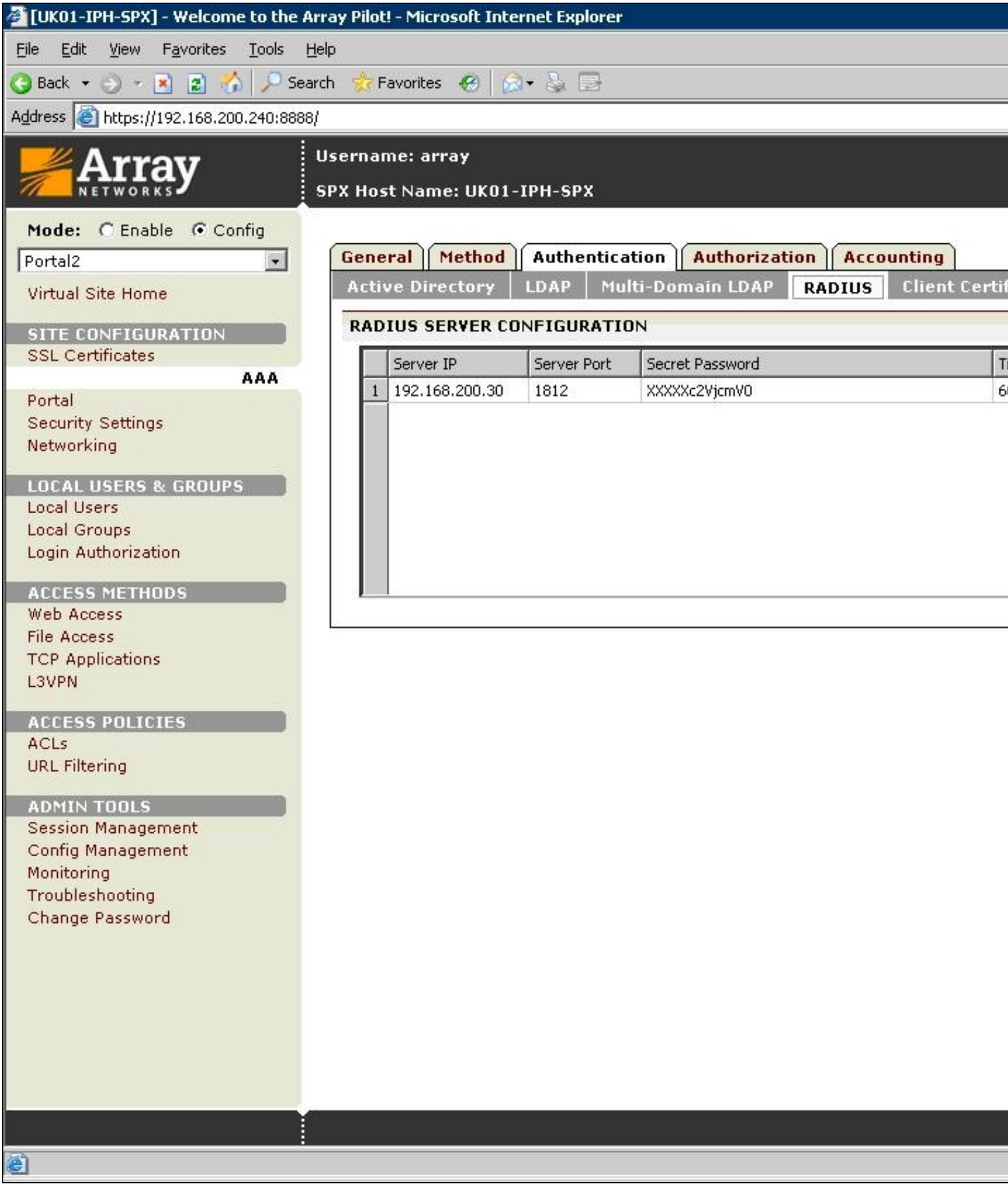
22.1 Configure RADIUS authentication

On the Array Networks SPX Select under Site Configuration AAA, then method. Configure the RADIUS server on the authentication menu. Set the authentication method to RADIUS



On the Authentication tab, Swivel needs to be configured as the RADIUS server for the VPN, ensuring that the shared secret matches that set on the RADIUS->NAS screen on Swivel.

If you want to configure more RADIUS servers for failover, add more servers.


[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal2
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
General Method Authentication Authorization Accounting
Active Directory LDAP Multi-Domain LDAP RADIUS Client Certif
RADIUS SERVER CONFIGURATION
Server IP Server Port Secret Password
1 192.168.200.30 1812 XXXXXc2VjcmV0

22.2 Link custom page to URL for login

The custom log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, enter the path to the Swivel virtual or hardware appliance. Note that this page needs to be accessible from the internet by the client.

The required settings are:

URL: Full address of where the login page can be reached

Username: default: uname, the username attribute used in the login page

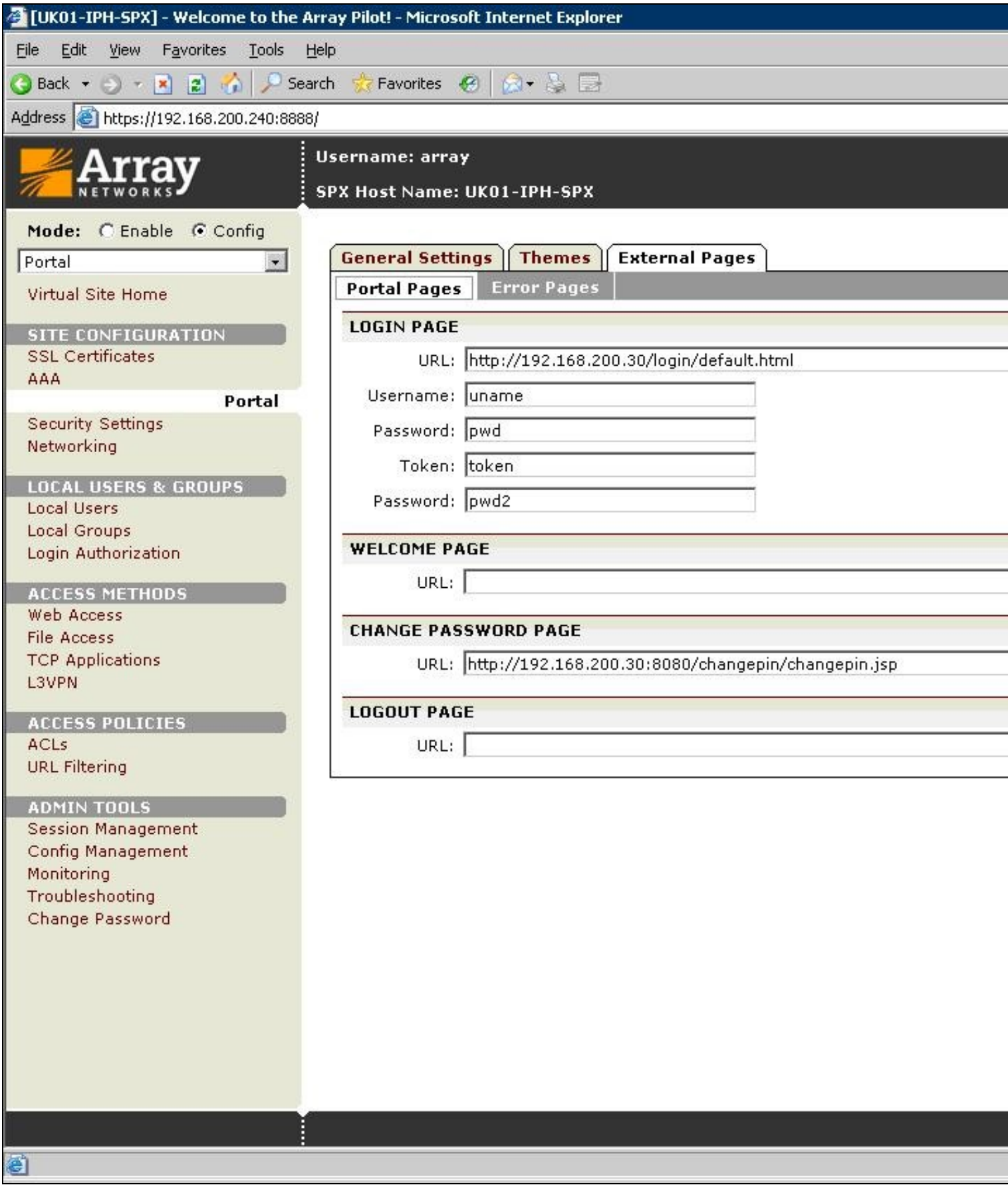
Password: default: pwd, the password attribute used in the login page

Token: default: token, the token attribute used in the login page

Password: default: pwd2, the secondary password attribute

Other options

Change Password Page Full address of the ChangePIN page

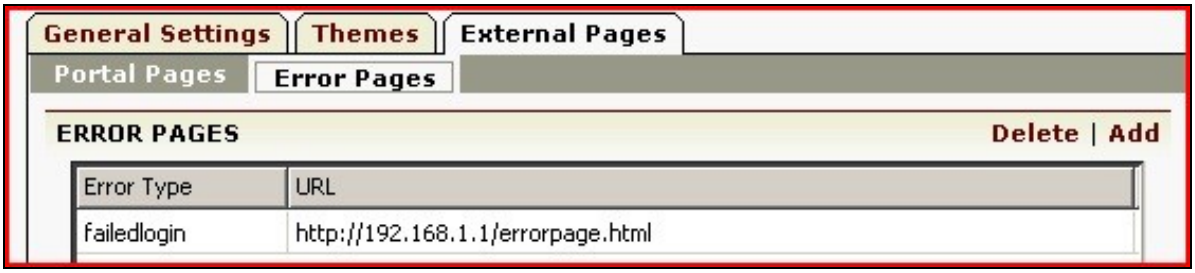

[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
General Settings
Themes
External Pages
Portal Pages
Error Pages
LOGIN PAGE
URL: http://192.168.200.30/login/default.html
Username: uname
Password: pwd
Token: token
Password: pwd2
WELCOME PAGE
URL:
CHANGE PASSWORD PAGE
URL: http://192.168.200.30:8080/changepin/changepin.jsp
LOGOUT PAGE
URL:

22.3 Link custom page to URL for failed login

The custom failed log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, select Error Pages, and for error type select failed login, enter either the path to the Swivel page or to a custom failed login page. Note that this page needs to be accessible from the internet by the client. Click save and the login page will now be listed.

Custom page for failed login:

The custom login page should be listed under Error Pages



22.4 Link custom page to URL for generic login error

It is also recommended to create another error page (as above) using the same custom login page URL (as above) but for a **generic login error**, which is a selectable Error Type. This prevents the default localhost login page of the Array being presented in the event of a generic login error.

22.5 Configure URL Policy

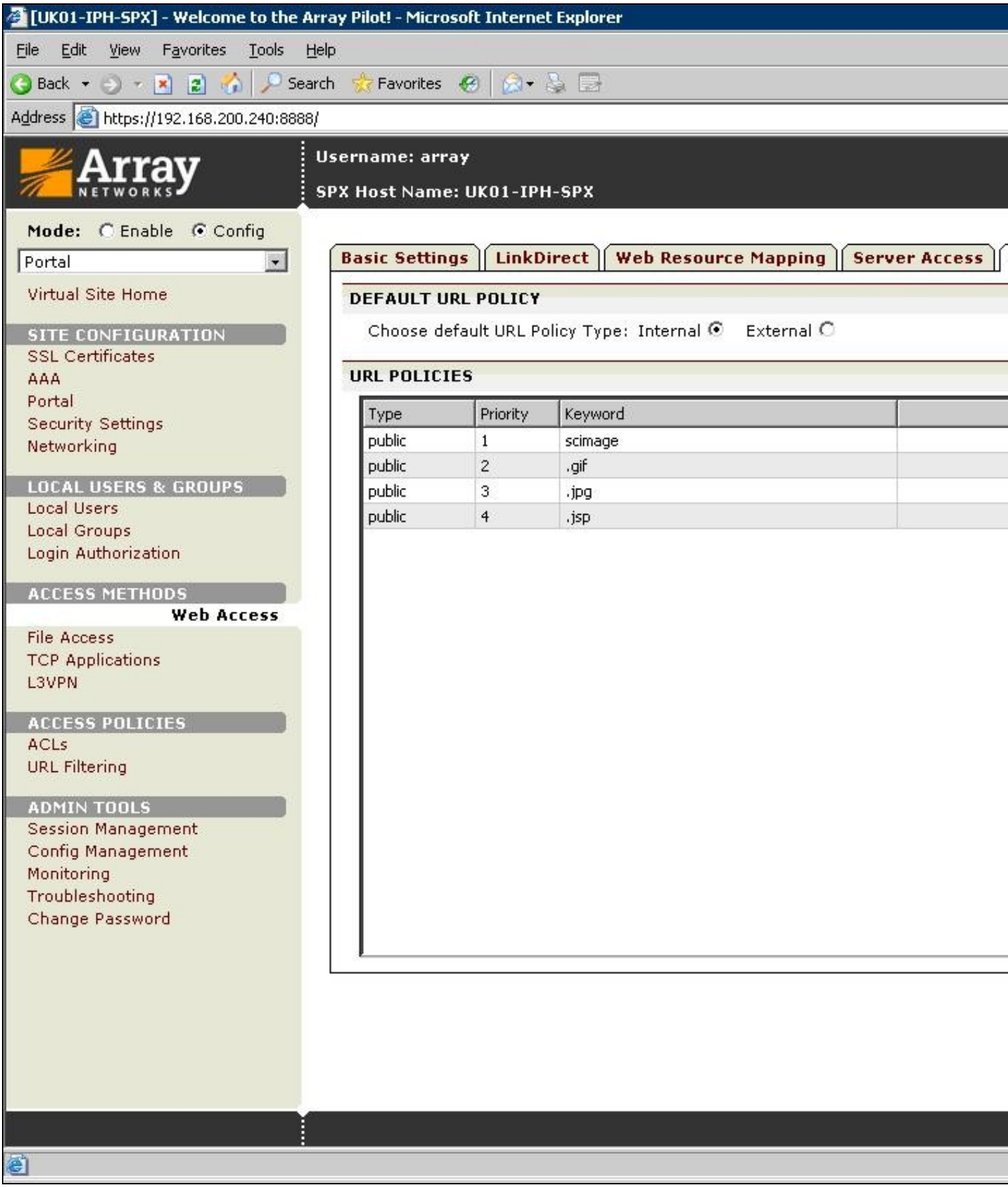
This page allows certain attributes to be used in the login page. On the Array Networks SPX Select under access methods/Web Access then URL Policies. Create the following policies:

Priority: 1 Type Public: keyword: SCImage

Priority: 2 Type Public: keyword: .gif

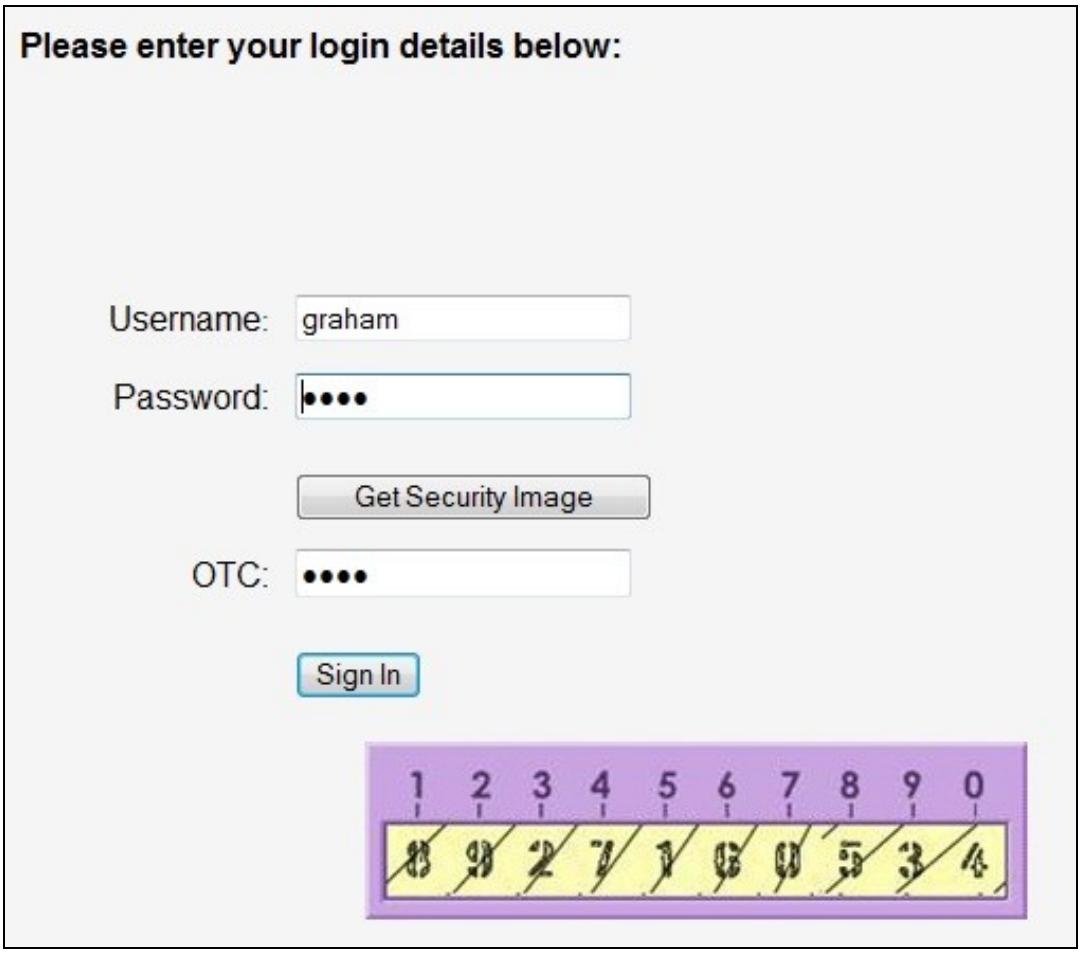
Priority: 3 Type Public: keyword: .jpg

Priority: 4 Type Public: keyword: .jsp


[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
Basic Settings
LinkDirect
Web Resource Mapping
Server Access
DEFAULT URL POLICY
Choose default URL Policy Type: Internal External
URL POLICIES
Type Priority Keyword
public 1 scimage
public 2 .gif
public 3 .jpg
public 4 .jsp

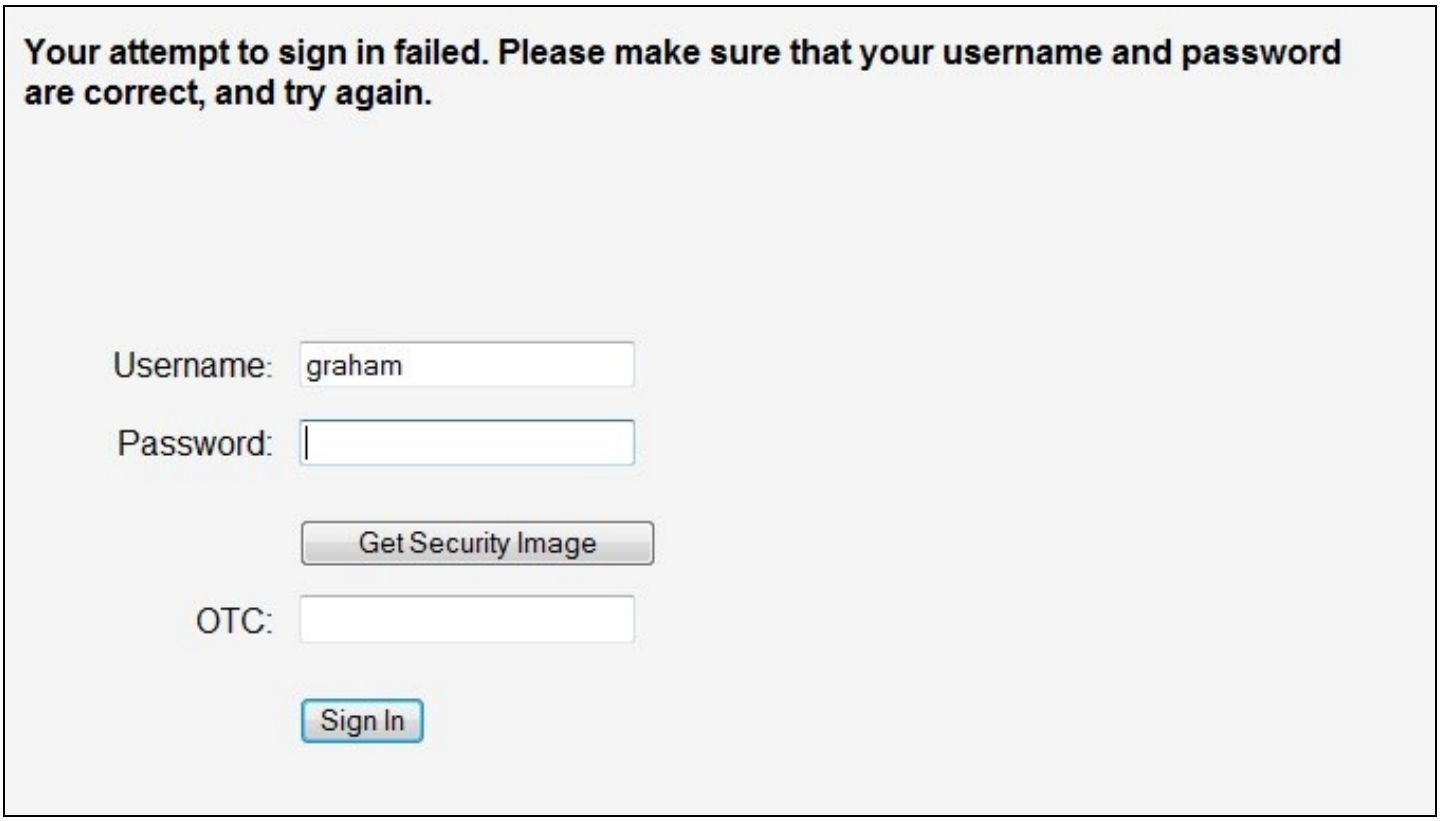
23 Verifying the Installation

Browse to the login page, enter a username, click on the Request Turing button and the Turing image should appear. Check for Session requests with that username on Swivel, and RADIUS requests.



Test using the SMS option without clicking on the Turing button. Note: If the Single Channel Turing image is clicked it will expect a Single Channel login for the length of the session request (usually 2 minutes). Check for RADIUS requests on Swivel.

Ensure that the failed login redirects to a Swivel login page.



24 Troubleshooting

Check the Swivel logs and system event logs for any errors or lack of communication as well as the Array Networks SPX logs.

25 Known Issues and Limitations

26 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

27 AuthControl Desktop

28 Introduction

AuthControl Desktop is the brand name for Swivel Secure's custom Windows Credential Provider.

The detailed article can be found under Windows Credential Provider.

29 Aventail Integration

SonicWall Aventail clientless SSL VPN Gateway

Integration Guide

30 Introduction

This document outlines the steps required to integrate the SonicWALL Aventail SSL VPN with Swivel. SonicWALL Aventail SSL VPN appliances are able to use external RADIUS servers for providing authentication and Swivel provides RADIUS authentication, so this forms the basis for the integration approach. This document is designed for use with version 10.x of the SonicWALL Aventail and is significantly different to 9.x and earlier versions.

Swivel users can use either Swivel?s Single Channel (TURing, Pattern) or Dual Channel (SMS, J2ME) methods to retrieve Security Strings, which are applied against the user?s PIN to extract a One-Time Code (OTC) which represents the password for an authentication request.

With Dual Channel methods, the user already holds one or more Security Strings on their mobile device (and can request more at any time) so with the Aventail VPN configured to use the matching Swivel server for RADIUS authentication, no further integration is required. However if Swivel is set to send many security strings in a single text message, then the login page can be modified to indicate to the user which string to use. For details of this refer to the additional details section. (The Authentication configuration section below describes how to achieve the RADIUS configuration).

However with Single Channel methods, the user must be presented with a Turing or Pattern image at sign-in time (representing a single time-limited Security String), so they can extract their OTC. The SonicWall Aventail makes a proxy request to Swivel so a NAT rule is not required to Swivel, see below for details.

31 Prerequisites

SonicWall Aventail 10.5.2

or SonicWall Aventail 10.5.3 Client Hot Fix 003

Swivel 3.x

Aventail login page script

32 Baseline

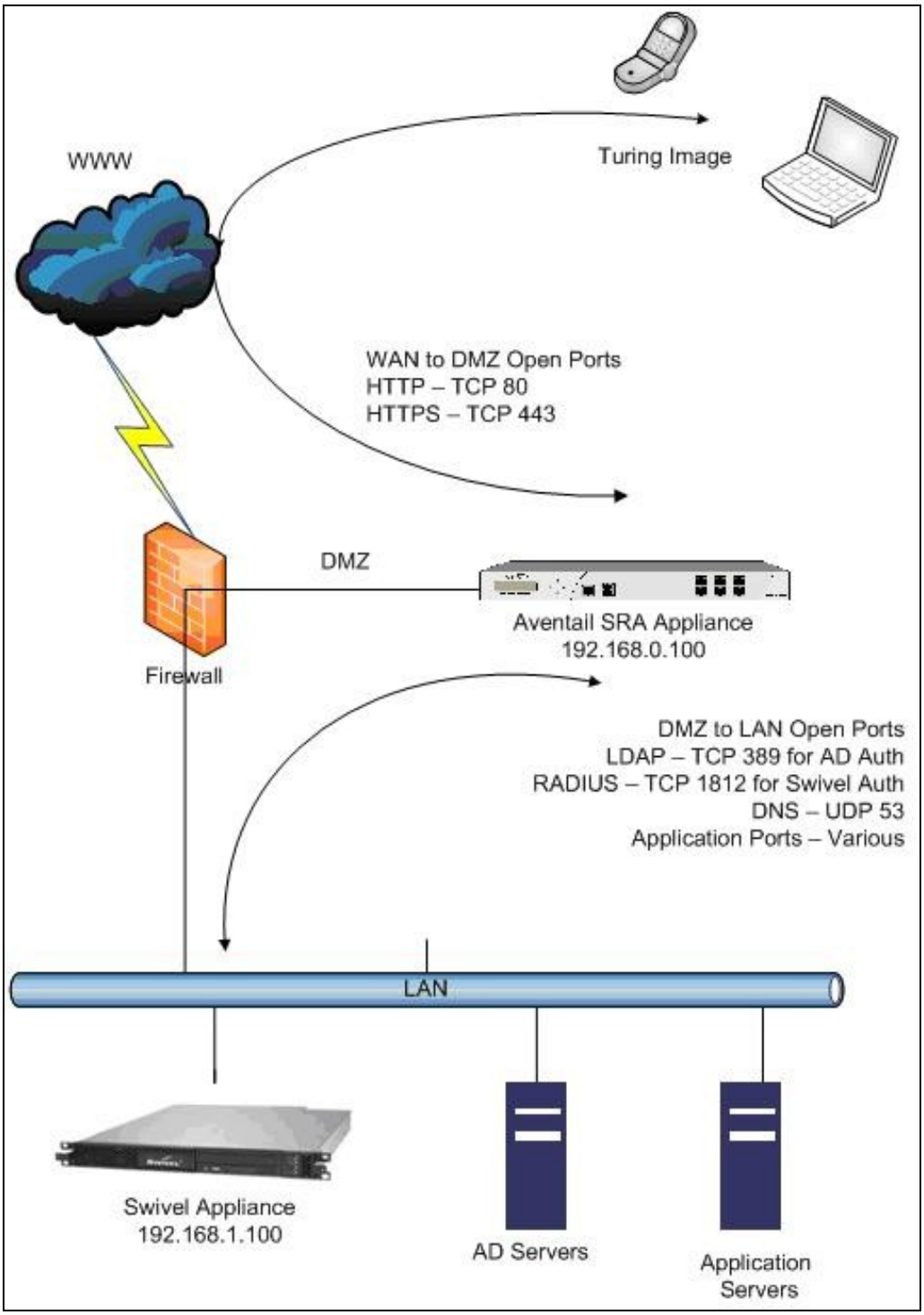
SonicWall Aventail 10.5.2 and 10.6.2-196

Swivel 3.7

33 Architecture

The user connects to the SonicWALL Aventail VPN using a web browser, pointing to the appropriate sign-in URL for the VPN in question.

The SonicWALL Aventail VPN is configured to use Swivel for radius authentication. Users are stored and maintained in Swivel.



34 Swivel Configuration

34.1 Configuring the RADIUS server

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

34.2 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.

34.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

35 SonicWall Aventail Integration

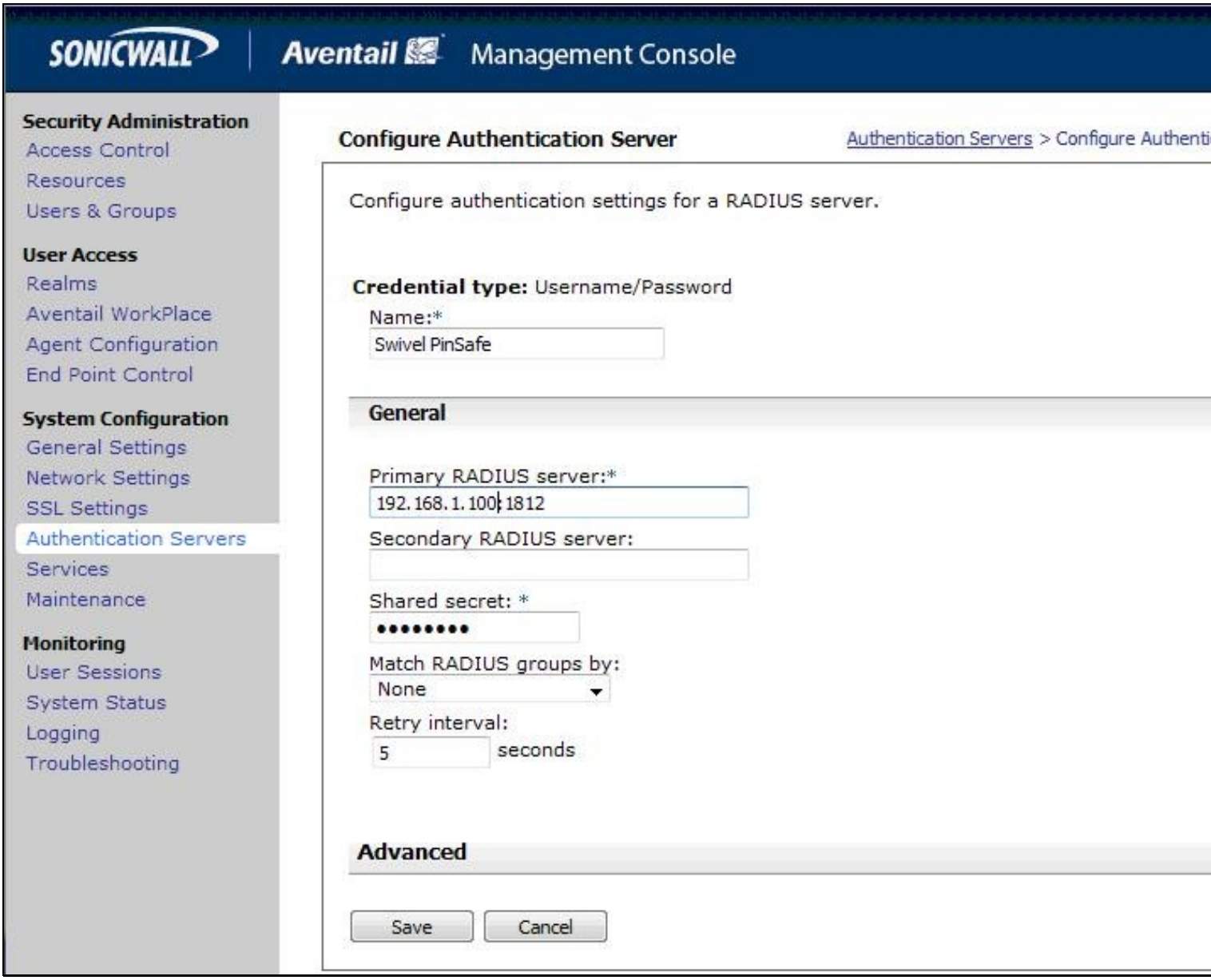
35.1 Configuring The Sonicwall Aventail for RADIUS Authentication

A new Authentication Server needs to be set up with RADIUS username/password authentication. The Primary RADIUS server needs to be set to the IP address of the Swivel virtual or hardware appliance followed by the authorisation port (see below). The secret needs to match the secret set on the NAS configuration screen.

If you want to configure a secondary Swivel RADIUS server for failover you would add the details of the server in the ?Secondary RADIUS server? section on this page.

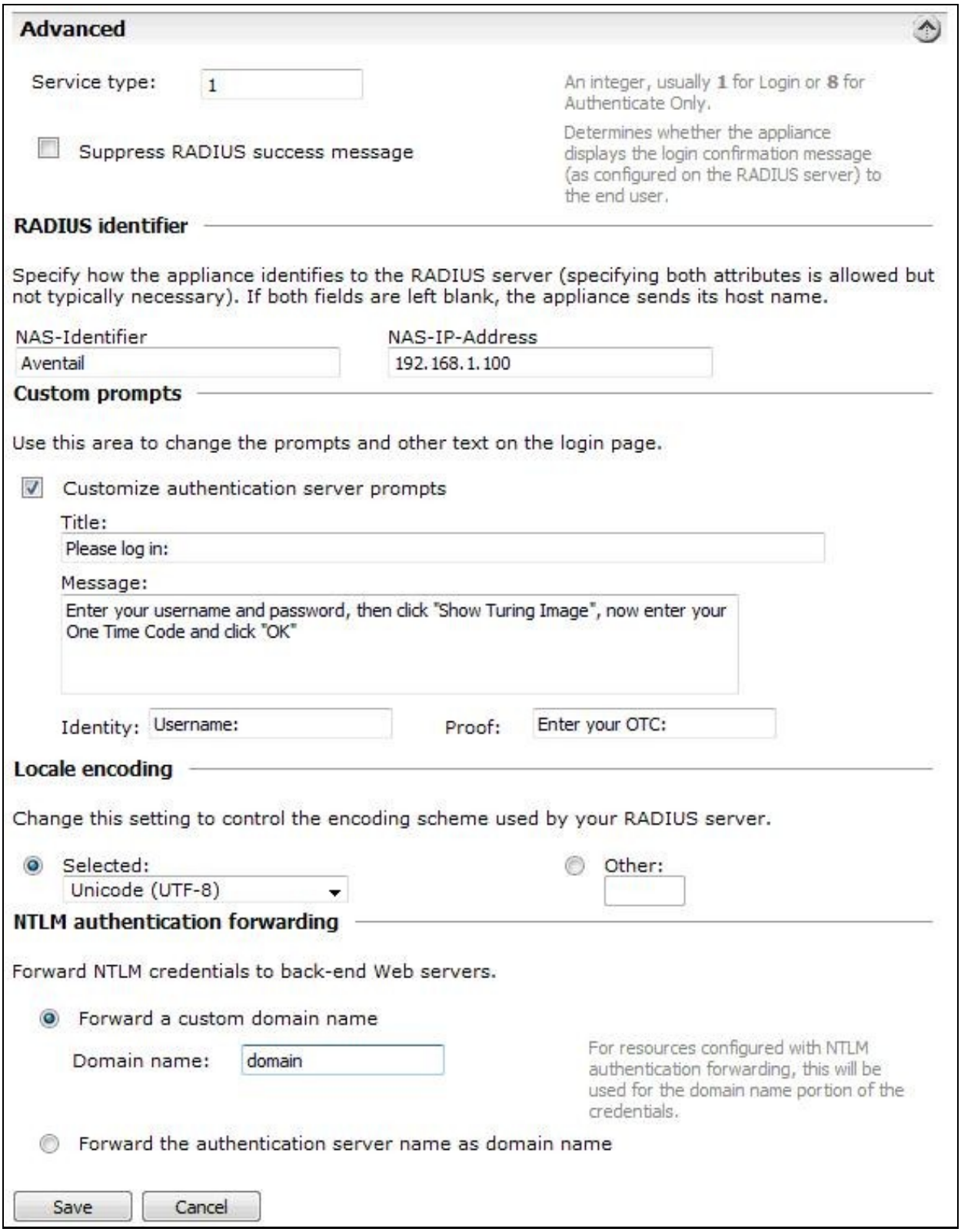
Swivel can be configured as the Primary Authentication Server or the Secondary Authentication server using *Chained Authentication*, typically AD will be the Primary authentication server and Swivel as the secondary authentication server. To configure this on the SonicWall Aventail Administration console click on Realms, then click on the name of the realm to be modified, or click New and select an authentication server in the drop down list. Click Advanced and select a Secondary Authentication server (If it has not yet been defined click on New to create it).

SonicWALL Aventail Authentication Server RADIUS Configuration



Under the Advanced section you should specify the NAS settings and you can also customise the password prompt to show ?Enter your OTC:? or whatever is you preference.

Advanced RADIUS settings



35.2 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.

35.3 Modifying the Aventail Sign-In Page for Turing

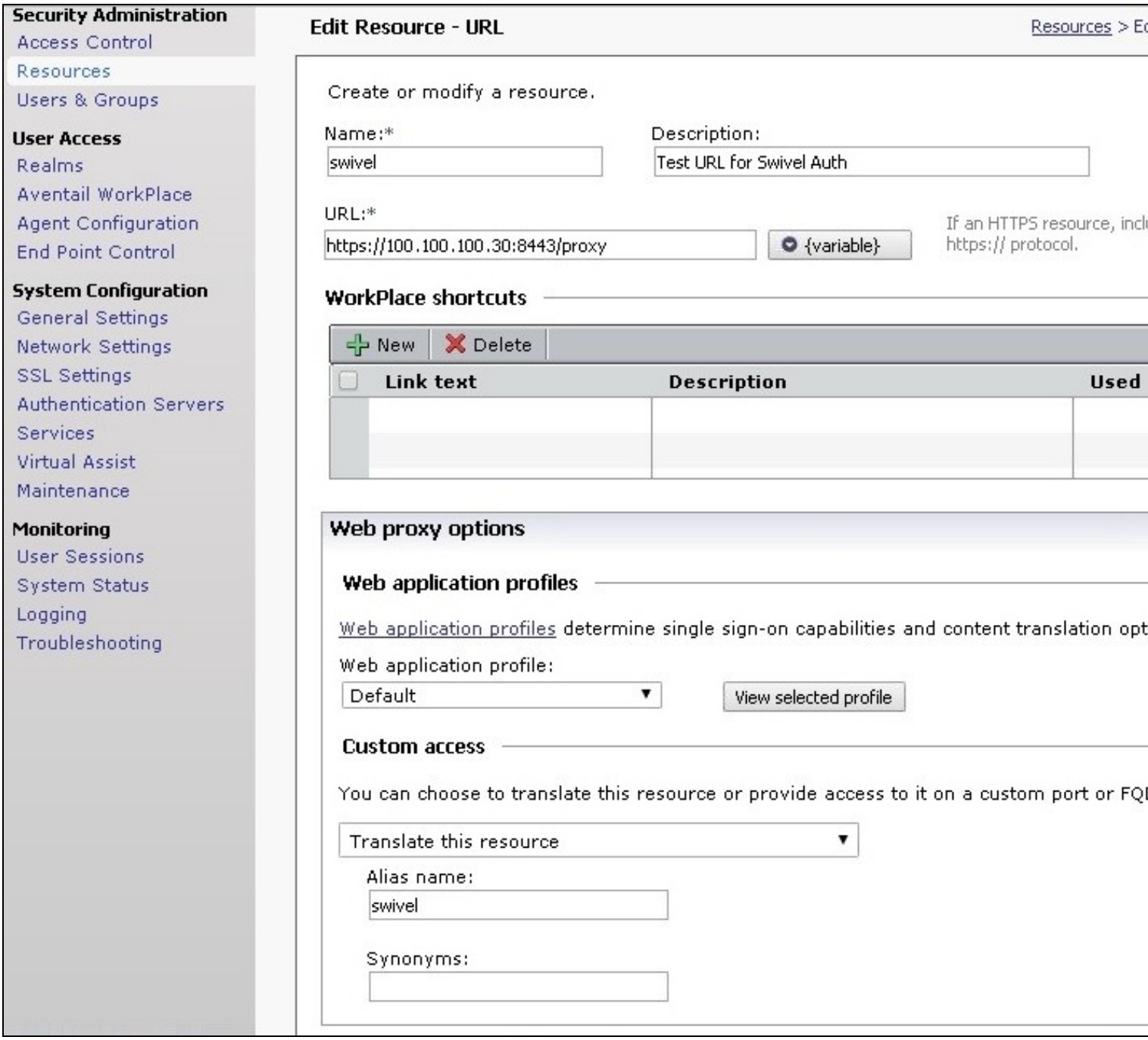
Note: When working with an Aventail Active Passive pair, the Master and Slave may need to be both configured, or shutdown the Slave whilst the master is configured for the changes to be evident.

Swivel sends Security Strings to users via SMS, J2ME (Dual Channel) or through a Turing image (Single Channel). The user extracts their One Time Code (OTC) from the Security String and enters that (preceded by their static Swivel password if they have one) into the SSL VPN log-in page.

If they were using Dual Channel (SMS or J2ME) they would have a security string ready and waiting on their mobile device. For Single Channel, we need some way of presenting a Turing image on the SSL VPN?s sign-in page.

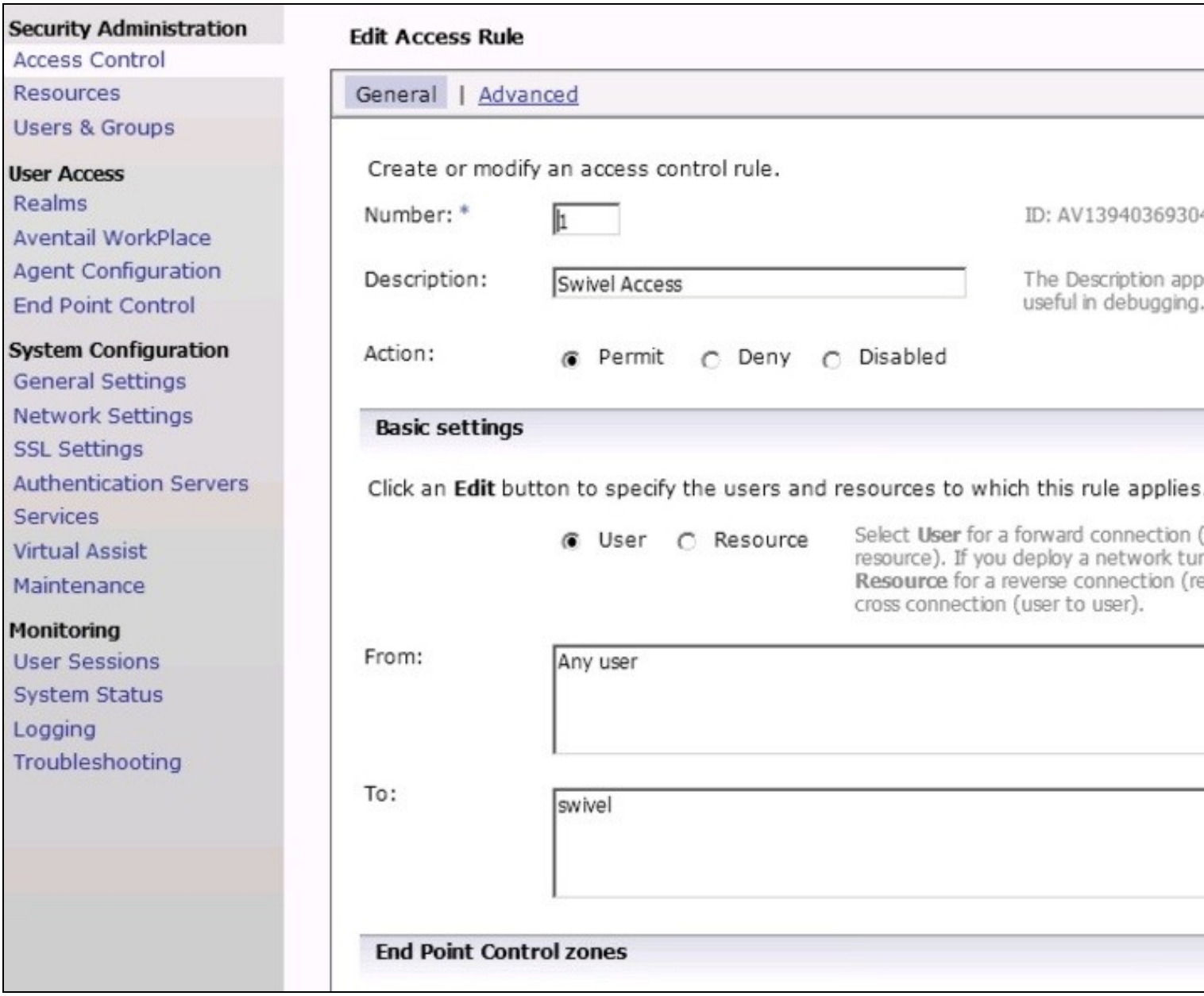
Using the Aventail AMC, it is necessary to create a URL resource for the Swivel virtual or hardware appliance and then make it available to un-authenticated users. It is also necessary to create a custom authentication page to present the ?Turing? button and also the image. The following steps describe how this is achieved.

1. Create a URL resource and give it the name ?swivel? with the URL of the Swivel virtual or hardware appliance. URL = https://swivel_server:8443/proxy for a Swivel hardware or virtual virtual or hardware appliance, for a software only install see Software Only Installation. Do not create a workplace shortcut. Under Custom access select Translate this resource with an Alias = ?swivel?. Creating an alias means the real URL of the Swivel virtual or hardware appliance is hidden from any user attempting to log in.



2. Create an ACL which allows all users access to the resource created in step 1. Select Access Control and New Rule with Permit access for type User

with access from Any User to the Swivel Resource.



3. The Swivel resource is behind and therefore protected by the Aventail appliance. It is necessary to allow un-authentication access to the URL created in step 1, this is NOT the same as adding an ACL.

a. Using an SSH client such as PUTTY or WinSCP connect to the Aventail appliance as ?root? with the admin password.

b. Then using Vi or an editor in WinSCP edit the file : /usr/local/app/mgmt-server/datastore/pending/sysconf/avconfig.xml

c. Find the resource id for the resource you just created (search for ?swivel?): <webURL id="AV1193773540220KE" name="swivel" scope="all_descendants">

d. Then, find the following line: <webAuthRule enabled="true" id="WebSSLNullAuthRule" managed="system">

e. Add your resource id to the ?destinations? block: <destinations_item refId="AV1193773540220KE"/>

f. Restart the management console: /etc/init.d/mgmt-server restart

g. Log in to the management console again and add/edit something; it doesn?t really matter what, you just want to get the ?Pending changes? and then apply the changes.

h. Changes to the avconfig.xml file will not get replicated to a HA secondary appliance so the settings need to made on this appliance. Also, during firmware upgrades the changes to avconfig.xml may not be retained.

4. For the given workplace site it is necessary to create a customised authentication request page. The section below describes this in detail.

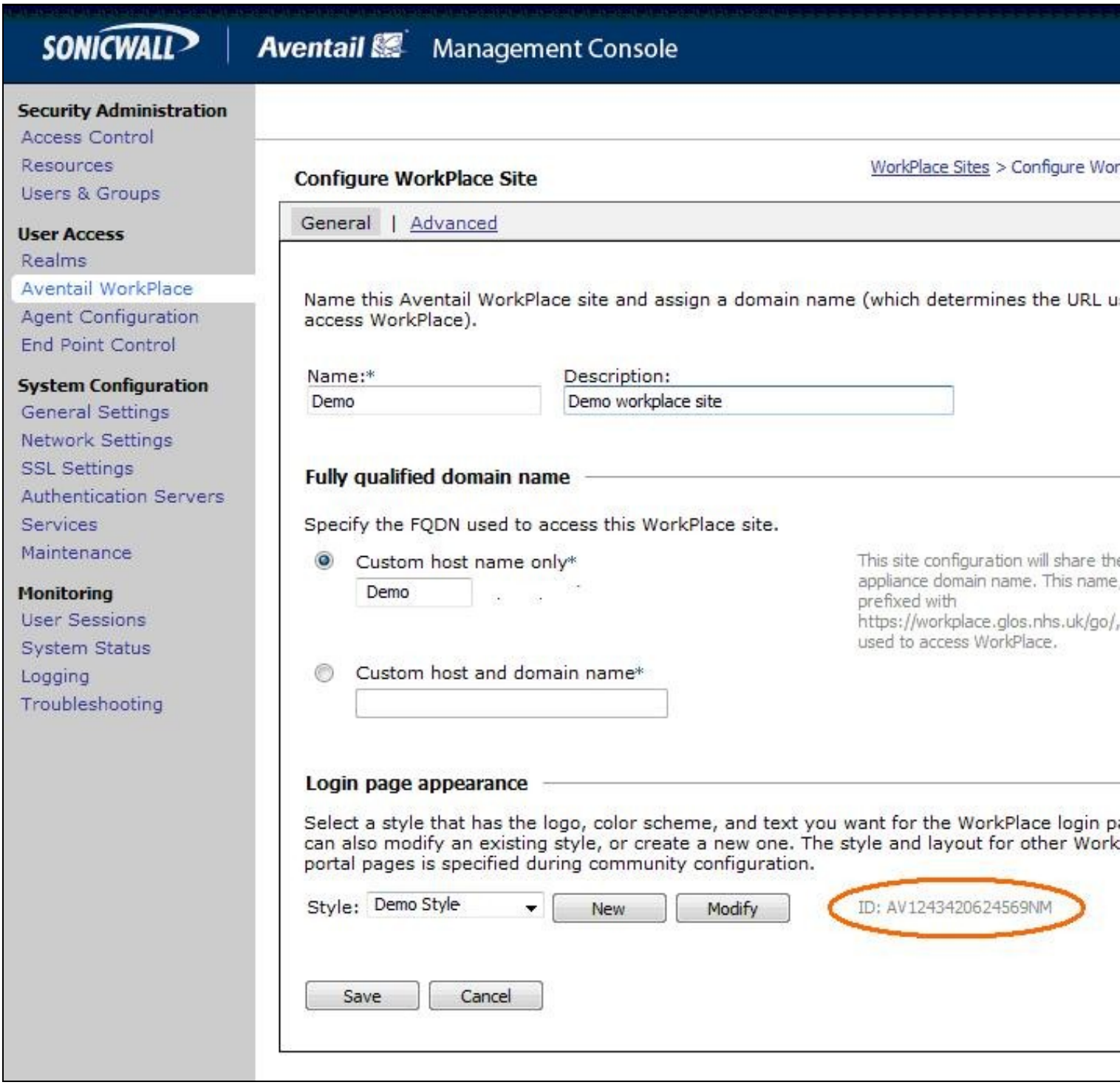
35.4 Creating A Custom Authentication Request Page

In order to have the TURing image displayed on the authentication page it is necessary to create and customise an ?authentication-request.tmpl? file.

In version 10.0.0 and later the default WorkPlace template files contain only plain HTML: the rendering is done using cascading style sheets. The content has also been streamlined with the help of tags that define more general divisions on the workplace portal pages (for example, , , , and so on).

1. For the required workplace, create a new style (or use one already created) to be used only for this workplace. Make a note of the styles ID num. The style needs to be used for the SSL VPN login point for which Swivel authentication will be used.

Configure Workplace and record Style ID



The default WorkPlace template files should be used as a starting point for customized templates, and never edited directly, because your changes will be overwritten the next time you customize WorkPlace in AMC. The default templates are as follows (one for each supported display size):

```
/usr/local/extranet/templates/extraweb.tmpl
```

```
/usr/local/extranet/templates/compact-extraweb.tmpl
/usr/local/extranet/templates/micro-extraweb.tmpl
```

When you create a workplace site, you specify a style for the login pages, which include realm selection, realm error, licensing error, and so on.

Copy the basic template from your v10 appliance: transfer /usr/local/extranet/templates/extraweb.tmpl (using WinSCP, for example) to your local computer. Log in using root and the admin password.

2. Save a copy of the extraweb.tmpl as authentication-request.tmpl.

Insert the following code into the new file directly below

```
<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position:

<img id=imgTuring name=imgTuring style="visibility:hidden;position: relative; left:40;top:70;">

<script language="JavaScript">


// Add on-blur method to username field so that
// TURing image appears automatically
if(document.getElementsByName("data_0")[0] != null) {
  document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
}


function ShowTuring() {

sUser=document.getElementsByName("data_0")[0].value;

 if (sUser=="") {
  alert ("Please enter your username first!");
  document.getElementsByName("data_0")[0].focus()
 }  else {
//The IP address below must be the External IP of the Aventail VPN
sUrl="https://FQDN_of_workplace/swivel/SCImage?username=";

//Find the image using Mozilla compatible pproach...
varImg = document.getElementById("imgTuring");

//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
varImg.style.visibility = "visible";

//Alternative approach - show image in Popup
//window.showModalDialog(sUrl + sUser,null,"dialogWidth=305px;dialogHeight=110px;status:no;scroll:no;help:no;")

//Set focus to the OTC input
document.getElementsByName("data_2")[0].focus()
 }
}


</script>
```

The customization first adds a button to the page to allow the user to request a TURing image and a placeholder for the image so that it can be displayed.

<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position: relative; left:50;top:60;width:75;"> When the user presses the TURing button it calls the showTuring function that retrieves the image from Swivel via the alias that has been set up and makes the TURing image visible. The customisation also adds an "onblur" action to the username field. This means that when the user tabs away from the username field a TURing image will be automatically requested.

3. The newly customised authentication-request.tmpl needs to be saved to the correct location on the Aventail. Again using WinSCP, copy the file to the folder /usr/local/extranet/templates/AV(ID identified in Figure 7). The ID folder should have been created automatically when the style was created.

4. Make a change in the Aventail AMC such that ?pending changes? can be applied.

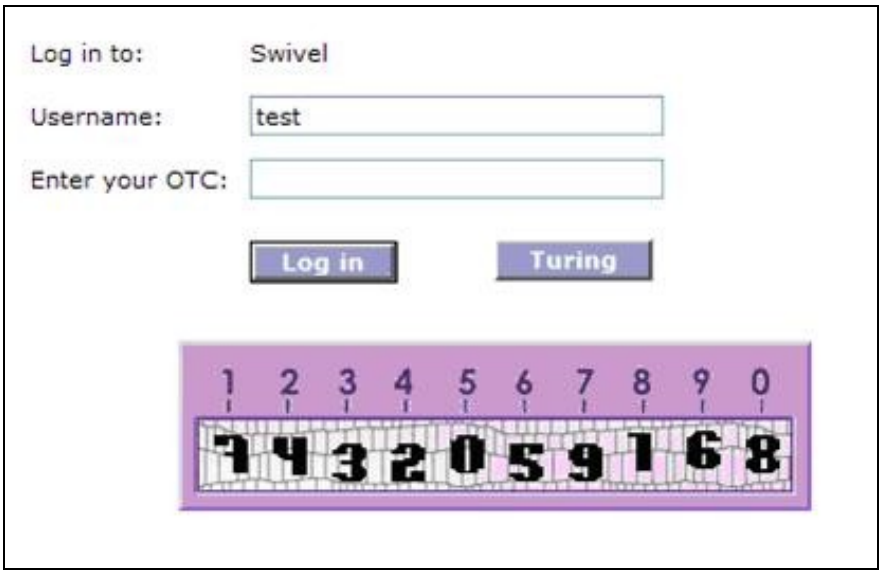
5. The newly configured workplace configuration should now be available.

If your Aventail appliance is part of a HA pair then copy the customised authentication-request.tmpl file across to the backup appliance.

36 Verifying the Installation

Login using the Turing or SMS.

Example of a modified SonicWALL Aventail sign-in page



37 Known Issues and Limitations

None

38 Configuration Options

38.1 Turing Image Size

Change the line:

<img id=imgTuring name=imgTuring style="visibility:hidden;">

to

<img id=imgTuring name=imgTuring width="450" style="visibility:hidden;">

A width of 450 to gives a 50% larger image (300 is standard). Different values may be used.

38.2 Security String Index

To modify the login page to display the required Security String index rather than a TURing image use the following modifications. See also Multiple Security Strings How To Guide

1) The button that is used for TURing needs to be changed to request the index and rather than an image tag a text field is required to display the result.

```
<tr>
 <td>
  <input type=button name=btnTuring value="Get Index" onclick=ShowIndex()
  class='submitbutton' style="visibility:visible;width:100;">
 </td>
 <td >
  Use index : <INPUT class="indextext" TYPE="text" id="indextext" name="indextext" size = "3">
  to select your security string.
 </td>
</tr>
```

Similarly the onblur action should be changed

```
if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0].onblur = function () {ShowIndex();};
}
```

2) The ShowIndex function then needs adding

```
function ShowIndex() {
{
  sUrl="https://FQDN_of_workplace/swivel/SCImage?username="
  sUser=document.getElementsByName("data_0")[0].value;
  if (sUser=="") {
   alert ("Please enter your username first!");
   document.getElementsByName("data_0")[0].focus()
 }
 else
 {
  updateindex(sUrl,sUser);
  document.getElementsByName("data_1")[0].focus()
 }
}

function updateindex(sUrl,sUser)
{
 //this means call the getText function and when callback is called,
 // call setIndex
 getText(sUrl  + sUser, setIndex) + "&random=" + Math.round(Math.random()*1000000);
}

 function getText (url, callback) {
 var request = null;
 //Initialize the request variable.
 if (window.XMLHttpRequest) {
 // Are we working with mozilla?
 request=new XMLHttpRequest();
 }
 else
 {
 //Not Mozilla, must be IE
 request=new ActiveXObject("Microsoft.XMLHTTP");
 }
 if (request==null) {
  //If we couldn't initialize request...
  alert("Your browser doesn't support the Get Index Button, sorry.");
  return false;
  }
   request.onreadystatechange = function() {
   if (request.readyState == 4 && request.status == 200)
   {
     callback(request.responseText);
   }
 }

   request.open("GET", url);
   request.send(null);
}

function setIndex(text){
 index = document.getElementById("indextext");
 if(text.length < 3){
  index.value = text;
 } else {
  index.value = "";
 }
```

```
}
```

38.3 TURing and SMS

To support TURING and SMS Index you need to include both buttons and both sets of scripts.

But not have any onBlur action on the username, as the user may choose either option.

38.4 Manual Turing Display

To stop the automated Turing display remove the **.onblur** entry. Note you would use this where dual channel authentication is required. The starting of a single channel session makes the Swivel server expect a single channel login:

```
// Remove on-blur method to username field so that
// TURing image appears automatically
 if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0] = function () {ShowTuring();};
 }
```

38.5 Automated Turing Display

To automate the Turing display we can add the below lines of code. Note you would not use this where dual channel authentication is required as the starting of a single channel session makes the Swivel server expect a single channel login:

```
// Add on-blur method to username field so that
// TURing image appears automatically
 if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
 }
```

Example:

```
<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position:

<img id=imgTuring name=imgTuring style="visibility:hidden;position: relative; left:40;top:70;">

<script language="JavaScript">


// Add on-blur method to username field so that
// TURing image appears automatically
if(document.getElementsByName("data_0")[0] != null) {
  document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
}


function ShowTuring() {

{
 sUser=document.getElementsByName("data_0")[0].value;

 if (sUser=="") {
  alert ("Please enter your username first!");
  document.getElementsByName("data_0")[0].focus()
 }

else

{
//The IP address below must be the External IP of the Aventail VPN
sUrl="https://FQDN_of_workplace/swivel/SCImage?username=";

//Find the image using Mozilla compatible pproach...
varImg = document.getElementById("imgTuring");

//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
varImg.style.visibility = "visible";

//Alternative approach - show image in Popup
//window.showModalDialog(sUrl + sUser,null,"dialogWidth=305px;dialogHeight=110px;status:no;scroll:no;help:no;")

//Set focus to the OTC input
document.getElementsByName("data_2")[0].focus()
 }
}
}

</script>
```

39 Troubleshooting

Check the Swivel logs for TURing images and RADIUS requests.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

This can be caused by the following:

- If the Swivel server sends the reply but it is not received by the access device, the access device may try to resend the RADIUS request. This can be caused by the Access device sending a RADIUS request from an external interface, but not accepting the response through that external interface.

If a red cross appears instead of the TURing image it is likely that a self signed certificate may be preventing the image from appearing. To verify this, in I.E. right click on the red cross and click on properties, copy the URL into the URL bar and see if a certificate error occurs with an image. The URL will be similar to:

virtual or hardware Appliance: https://<VPN URL>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

To overcome this install a valid certificate on the Swivel virtual or hardware appliance. Using non SSL communication will likely result in the web browser creating a pop up about SSL and non SSL communications in the web page.

40 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

41 Barracuda SSL VPN Integration

42 Introduction

This document describes steps to configure a Barracuda SSL VPN 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.

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 appliance is configured with a proxy port to allow an additional layer of protection.

43 Prerequisites

Barracuada SSL VPN 380 or higher. Note the SSL VPN 280 does not support RADIUS authentication.

Barracuda Documentation

Swivel 3.x, 3.5 for RADIUS groups

The Swivel server must be accessible from the Barracuda SSL VPN using RADIUS.

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

44 Baseline

Barracuda SSL VPN 2.2.2.203 and 2.2.2.115

Swivel 3.9

45 Architecture

The Barracuda SSL VPN makes authentication requests against the Swivel server by RADIUS.

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

46 Swivel Configuration

46.1 Configuring the RADIUS server

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

46.2 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.

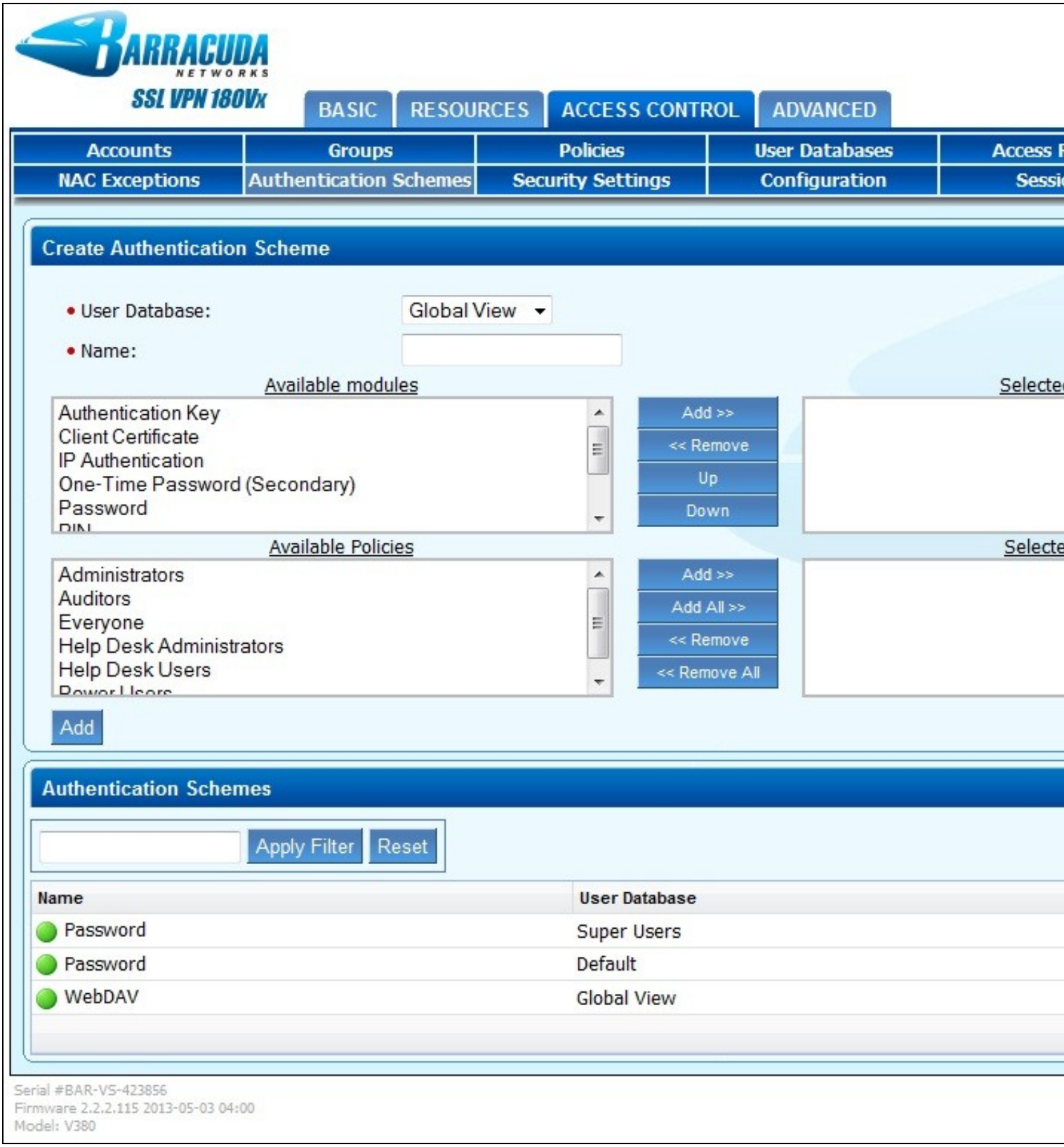
47 Barracuda SSL VPN Configuration

Login to the Barracuda SSL VPN administration console, usually through the ssladmin login.

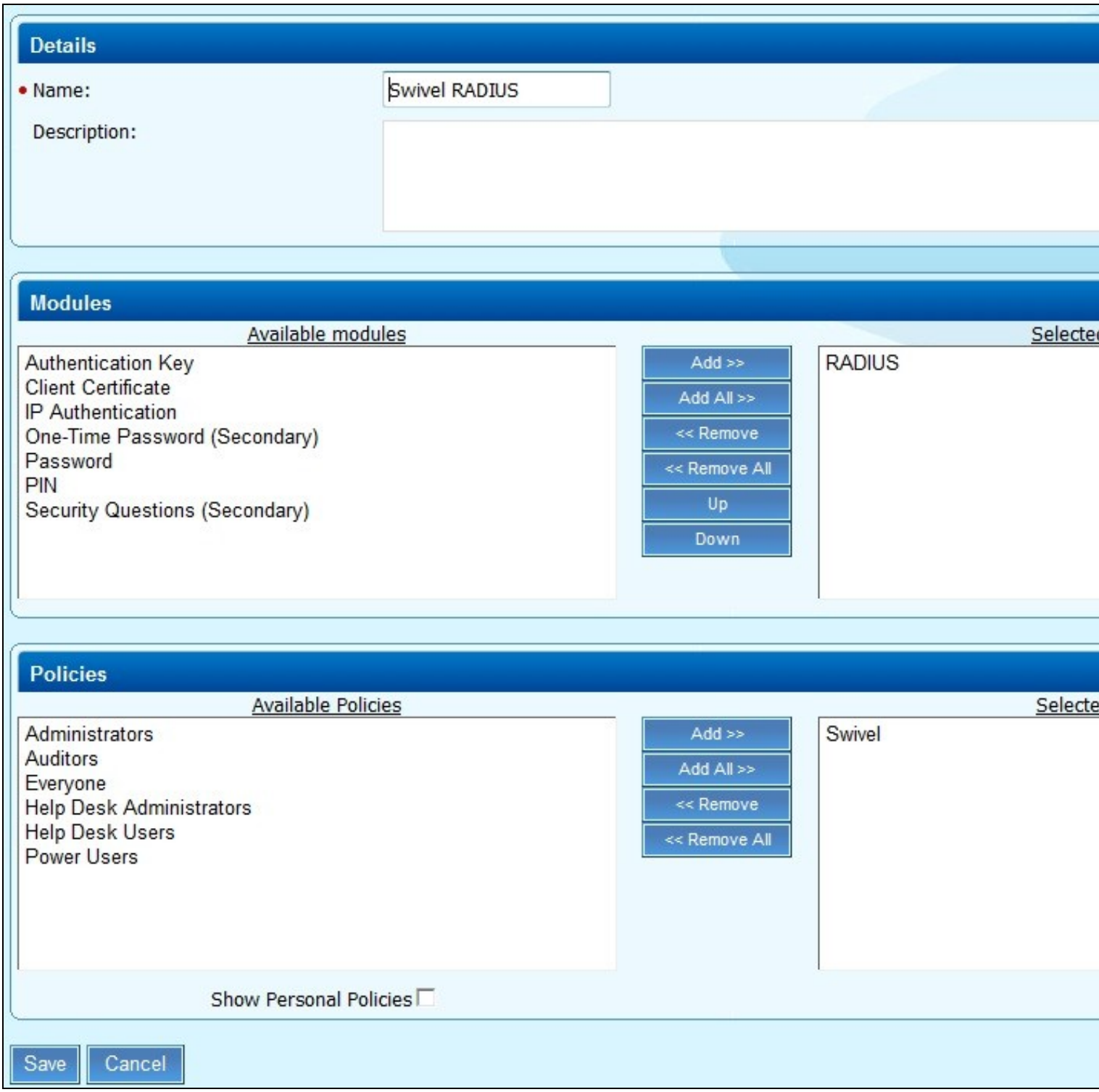
The user must exist as a user on the Barracuda SSL VPN, the user can be created through the Access Control Tab then select Accounts. Other user data sources may be configurable such as AD.

47.1 Create an authentication scheme

From the Access Control tab select Authentication schemes.



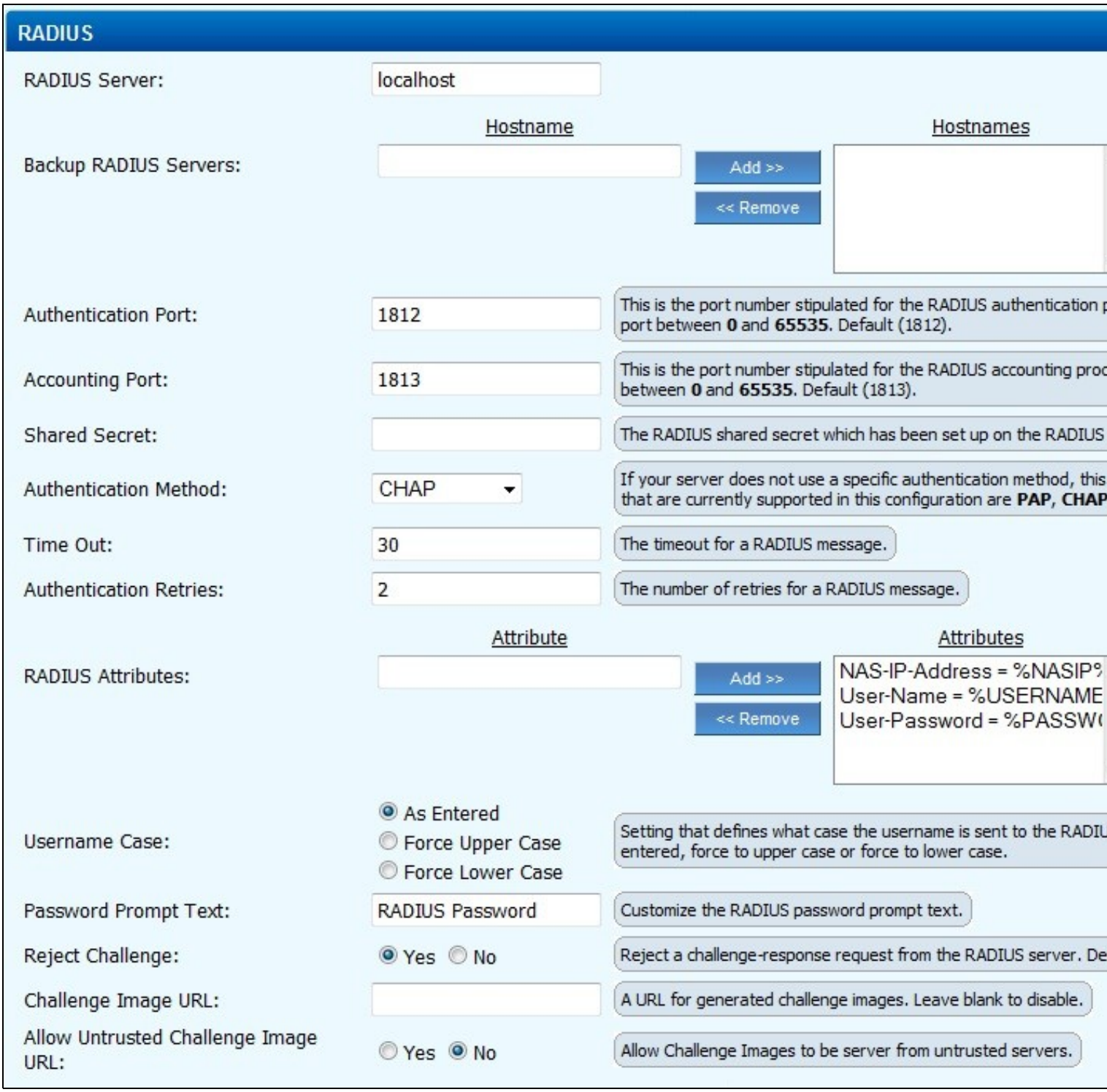
Enter a name for Authentication Scheme, such as **Swivel RADIUS**. From Available Modules select RADIUS then click on Add >>, so it appears on the right as a Selected module., and then select from Available policies the policy required and click Add >>. When complete click Add. A default policy can be used, in this example it is using a custom policy created under Access Control/Policies.



If required move the **Swivel RADIUS** authentication scheme to the top of the list, the top entry is the default entry presented to the user at login, click More to change the priority.

47.2 Barracuda RADIUS Configuration

On the SSL VPN administration console select the Access Control tab then select configuration.



Enter the following information:

RADIUS Server: Swivel RADIUS server hostname or IP (Note do not use the Swivel VIP address if this is being used, but the real IP address, see VIP on PINsafe Appliances).

Backup RADIUS Servers: Additional Swivel RADIUS instances as required.

Authentication Port: The Swivel server RADIUS authentication port, default 1812.

Accounting Port: The Swivel server RADIUS accounting port, default 1813.

Shared Secret: The shared secret entered into the NAS entry on the Swivel server.

Authentication Method: Use PAP for Challenge and Response/Two Stage Authentication and mobile clients.

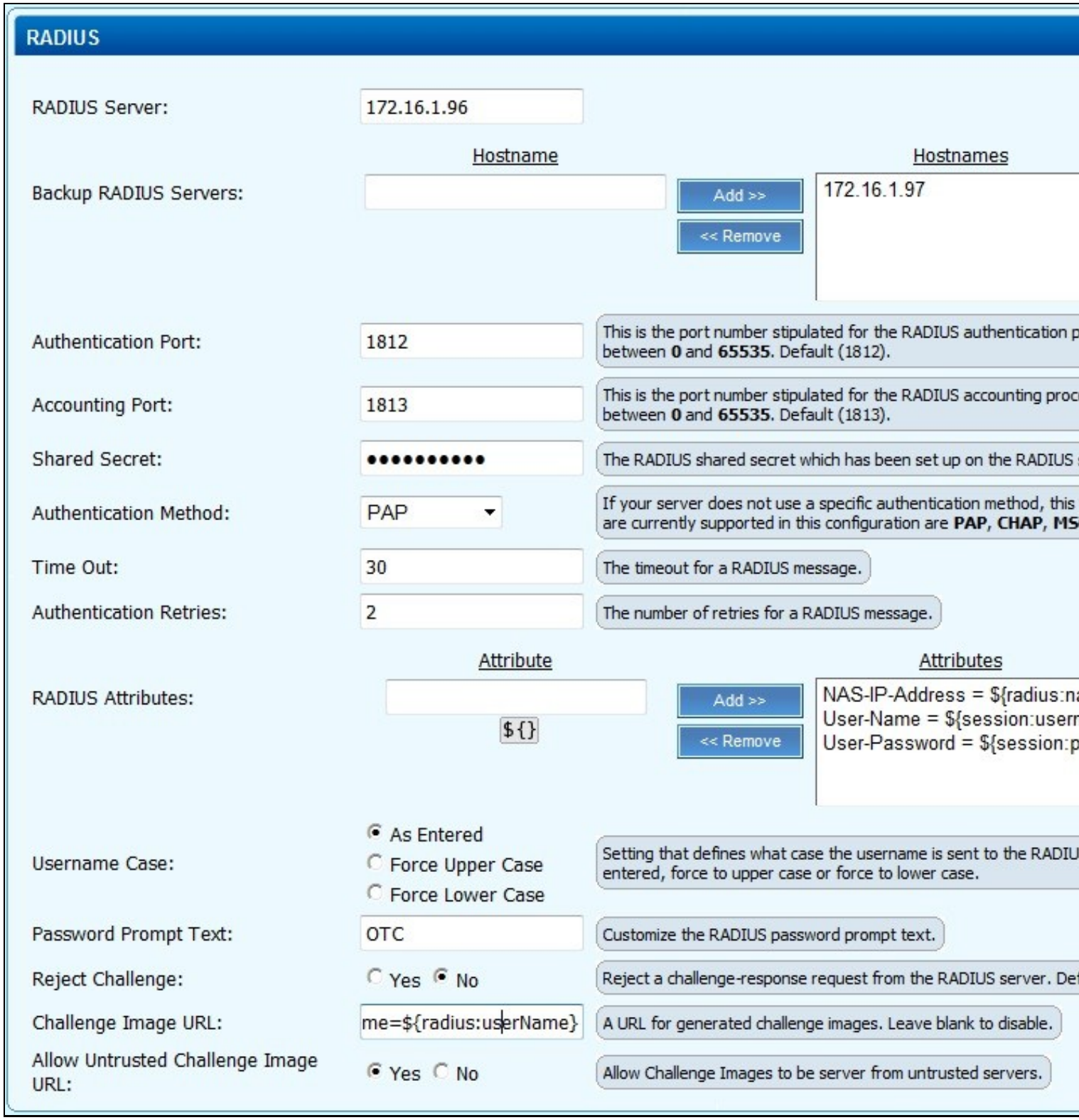
Password Prompt Text: The text to be displayed in the login field, usually set to OTC or One Time Code.

Reject Challenge: Set to No if Two Stage Authentication/Challenge and Response is to be used.

Challenge Image URL: Enter Swivel server details for graphical images to be used for authentication.

See options below for different configuration options.

Allow Untrusted Challenge Image URL: Set to Yes.



Save the RADIUS settings.

47.3 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.

47.4 Additional Configuration options

47.4.1 Additional RADIUS configuration Options: Single Channel TURing graphical image

This allows the graphical single channel TURing image to be displayed to the user for authentication. If this is not required, such as if SMS and Mobile Phone Client authentication is to be used, then this step should be skipped and the **Challenge Image URL:** left blank.

To configure the single channel graphical image set **Challenge Image URL:** to:

For an Appliance

```
https://Swivel_server_public_hostname:8443/proxy/SCImage?username=${radius:userName}
```

For a software only install see Software Only Installation

Allow Untrusted Challenge Image URL: Set to Yes.

Save the RADIUS settings.

47.4.2 Additional RADIUS configuration Options: Multiple String delivery index display

When a user logs in the user can be displayed an image telling them which of their security strings to use for authentication. See also Multiple Security Strings How To Guide

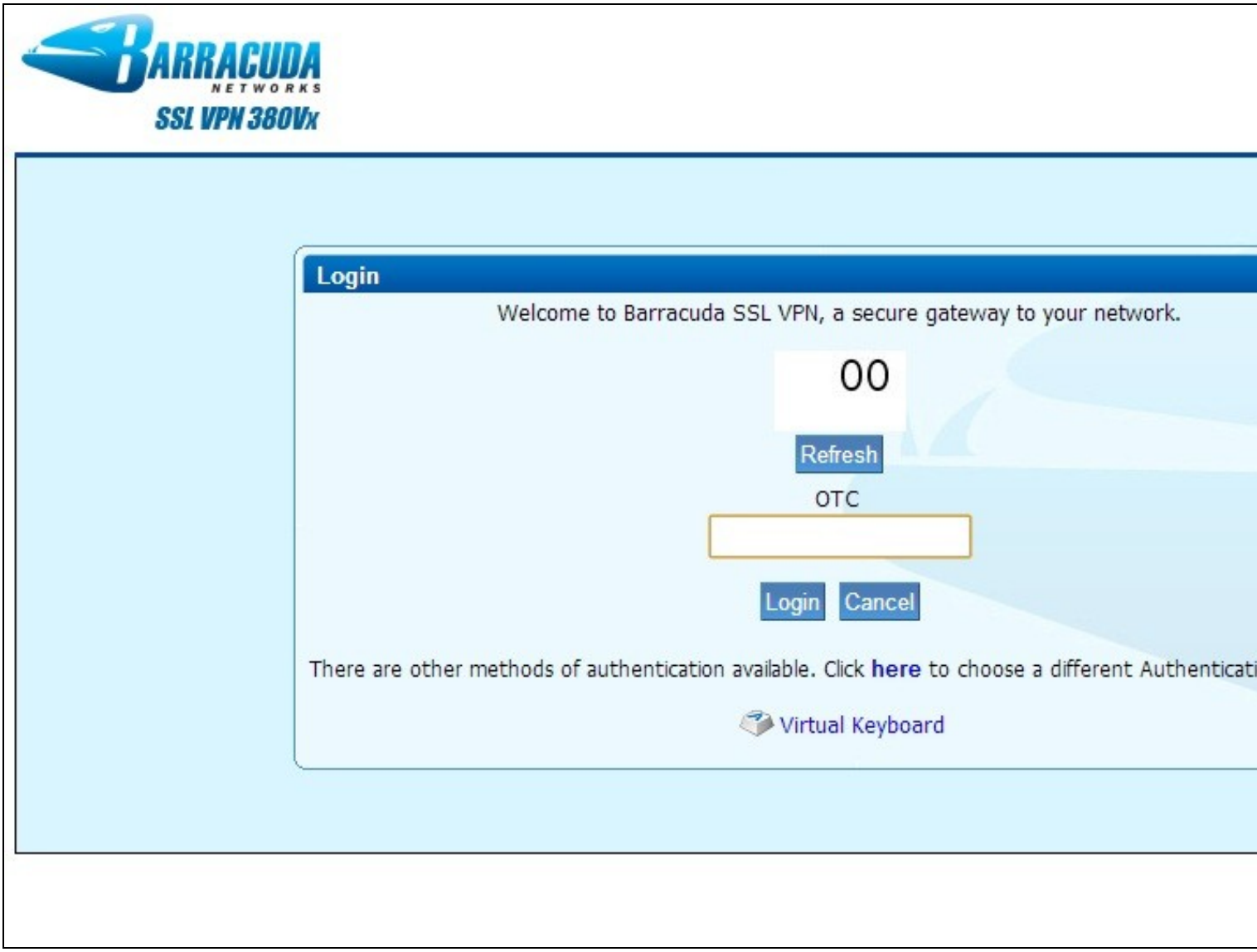
Set **Challenge Image URL:** to:

For an Appliance

```
https://Swivel_server_public_hostname:8443/proxy/DCIndexImage?username=${radius:userName}
```

For a software only install see Software Only Installation

Save the RADIUS settings.



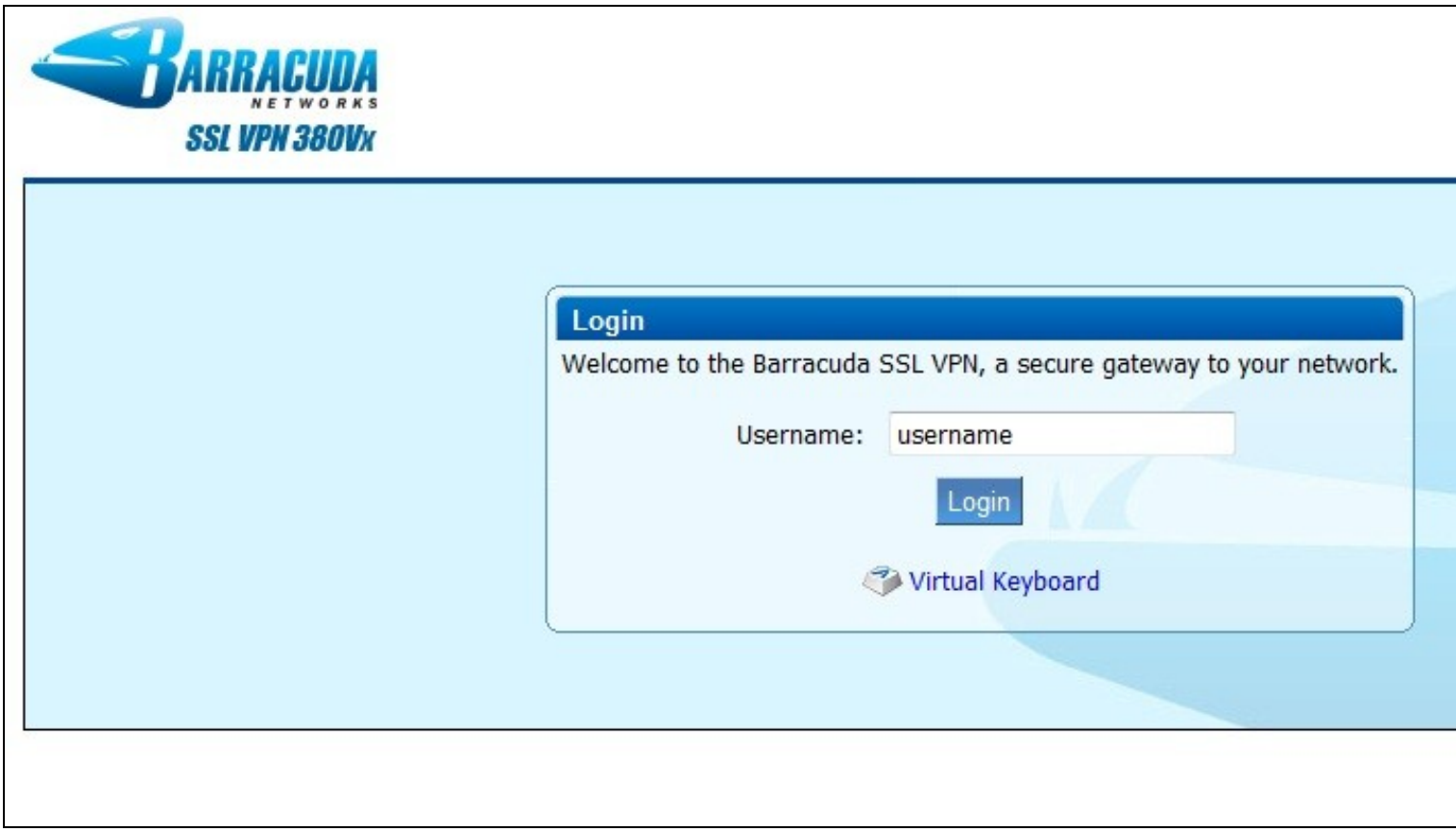
47.4.3 Additional RADIUS configuration Options: Two Stage Authentication

This allows the user to enter a username, then on the second screen a password and then on the third screen will be required to enter their One Time Code. Note that where the graphical TURing image or other image is used, then this will be displayed on the second and third screens even though it is not required on the second screen. See also Two Stage Authentication How to Guide

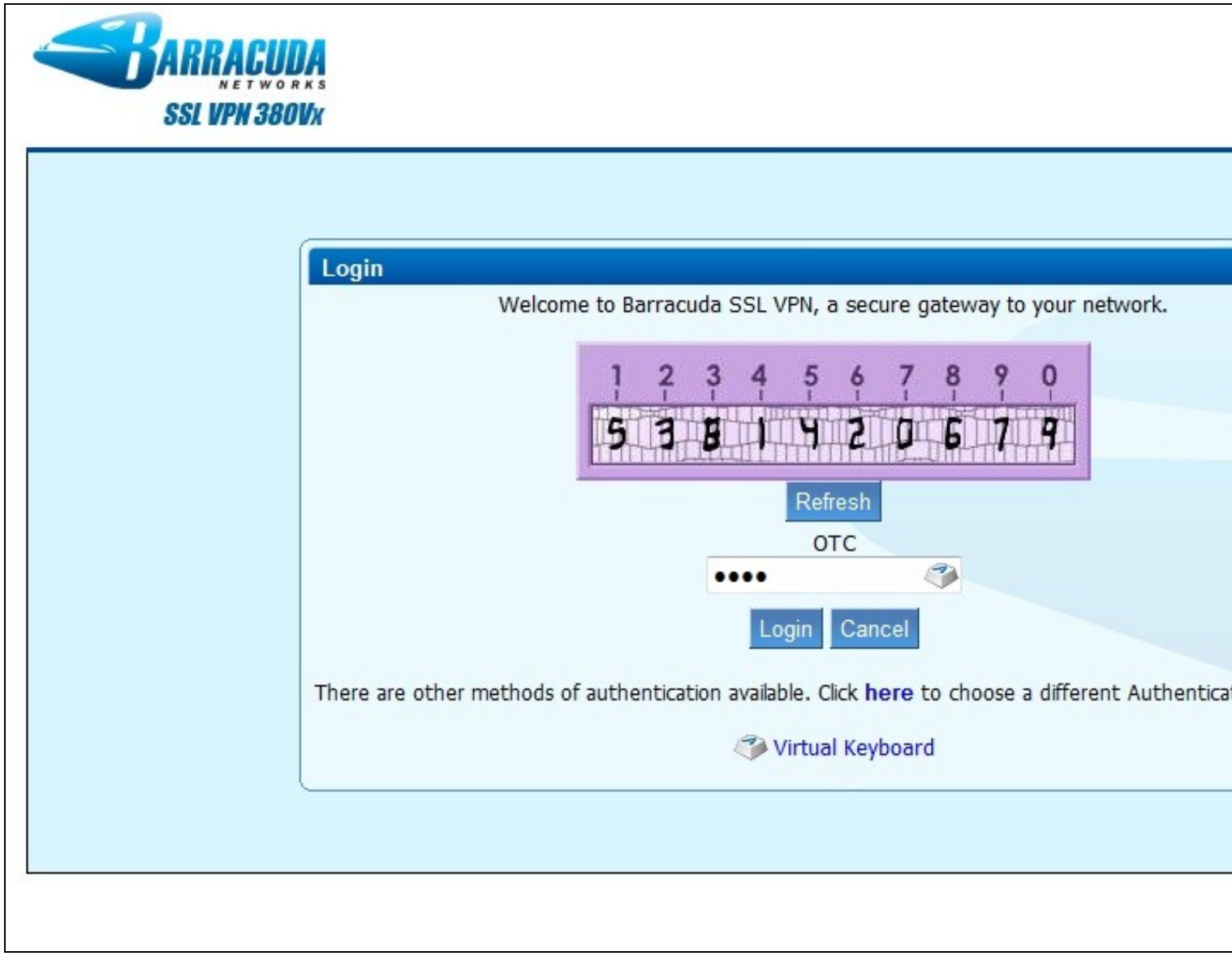
This requires the Barracuda SSL VPN setting **Reject Challenge:** to be set to No if Two Stage Authentication/Challenge and Response is to be used, and **Authentication Method:** should be set to PAP, save the RADIUS settings. On the Swivel administration console the RADIUS/NAS/Two stage authentication needs to be set to Yes, then click Apply. The user also needs to have a repository password, see Password How to Guide.

48 Testing

Select the Barracuda SSL VPN login page, enter a username, then select login.



Enter the One Time Code and click login.


BARRACUDA
NETWORKS
SSL VPN 380Vx
Login
Welcome to Barracuda SSL VPN, a secure gateway to your network.
1 2 3 4 5 6 7 8 9 0
5 3 8 1 4 2 0 6 7 9
Refresh
OTC
Login
Cancel
There are other methods of authentication available. Click here to choose a different Authentica
Virtual Keyboard

49 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

50 Known Issues and Limitations

Two Stage authentication will display an image at each stage.

Change PIN is not currently supported to redirect to a Swivel Change PIN page.

51 Additional Information

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

52 Bomgar

53 Introduction

This document describes the steps to configure Bomgar with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client, It is not currently possible to embed the TURing or Pinpad within the login page/client but these can be provided instead by Taskbar or User Portal for strong Single Channel Authentication.

54 Prerequisites

Bomgar Account

Bomgar Documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

To use the Single Channel Image such as the TURing Image, the Swivel server must be made accessible and the security string provided through the Taskbar, User Portal or other web page, usually through a NAT.

55 Baseline

Bomgar Product Version 14.2.2, Product Build 51805, API Version 1.12.0

Swivel 3.10.1

56 Architecture

The Bomgar software makes authentication requests against the Swivel server by RADIUS.

57 Swivel Configuration

57.1 Configuring the RADIUS server

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

57.2 Configuring Two Stage Authentication

The Bomgar client software supports Two Stage Authentication. It is suggested to initially configure just with an OTC and if Two stage authentication is required, configure this once everything has been tested and proven to be working.

See Challenge and Response How to Guide

57.2.1 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.

57.3 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

58 Bomgar Configuration

The following document provided by Bomgar outlines the integration setting on Bomgar: Bomgar RADIUS Integration.

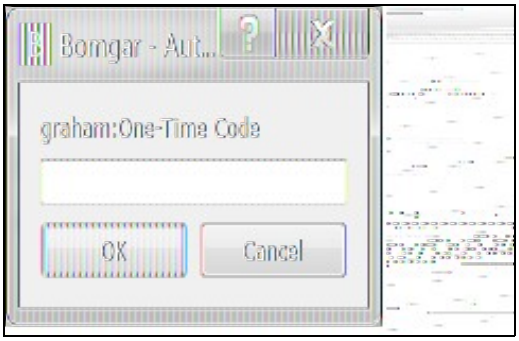
58.1 Test the RADIUS authentication

The Bomgar configuration has a test tool, and 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. Either using the test tool or through the the web 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 OTP prompt 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, and is contactable.

If this works then the client software login can be tested.

Bomgar Client login

Bomgar client login uisng Two Stage Authentication



58.2 Optional

59 Testing

60 Additional Configuration Options

61 Troubleshooting

62 Known Issues and Limitations

None

63 Additional Information

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

64 Checkpoint EndPointSecurityVPN Integration

Place Holder

65 Checkpoint Mobile Access

Please refer to the Checkpoint Connectra Integration page.

66 Checkpoint SecureClient Integration

Checkpoint SecureClient

Integration Guide

Version 1.1 March 2010, Updated March 2014

67 Introduction

This document outlines the steps required to integrate the Checkpoint SecureClient VPN software with Swivel.

Swivel users can use Swivel?s Token, SMS, Mobile Phone Client, as well as the single channel TURing and Pinpad methods to retrieve a One Time Code or a Security string.

With Single Channel methods, the user must be presented with a TURing or Pinpad at sign-in time, so they can extract their OTC such as the TURing using the Taskbar.

The settings and software can be configured for larger deployments within an msi file to ease installation.

67.1 Prerequisites

Checkpoint SecureClient E75. This solution is not compatible with E80.

Swivel 3.x. Where the Single Channel image is to be used, this should be presented to the user through a Network Address Translation to the Swivel server.

Swivel SecureClient software

- The file extensions have been changed to prevent them being blocked by filters etc .dll files to .dlx, and .reg to .rex. These need to be renamed back again.

67.2 Baseline

Checkpoint SecureClient R60 and R77,

Checkpoint SecureClient E75.10 (tested for Token, SMS, Mobile App, Taskbar)

Checkpoint VPN server R75.45 (tested for Token, SMS, Mobile App, Taskbar)

Swivel 3.6, 3.9.7, 3.10

67.3 Architecture

The user connects to the Checkpoint VPN by using the SecureClient software. The Checkpoint is configured to use a Swivel server for radius authentication. Users are stored and maintained in Swivel.

68 Swivel Configuration

68.1 Configuring the RADIUS server

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

68.2 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.

68.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

69 Configuring the Checkpoint VPN-1/Firewall-1

69.1 Checkpoint VPN-1/Firewall-1 configuration Overview

The steps for enabling SecureClient users on the Checkpoint VPN-1/Firewall-1 is outlined below. For further details refer to the VPN-1/Firewall-1 Administration Guides.

1. Install the SecureClient license.

2. Create SecureClient users.

3. Define a SecureClient authentication method using PINsafe as a RADIUS server

4. Create a SecureClient group.

5. Add SecureClient users to the SecureClient group.

6. Define a Remote Access Community and participants.

7. Create SecureClient rule for the Remote Access Community.

8. Create the Desktop Security Policy rules.

9. Install Security Policy.

69.1.1 Configure Checkpoint VPN-1/Firewall-1 to use the Swivel RADIUS server

Create a RADIUS server entry on the Checkpoint Policy Editor

Select Manage/Network Objects' then Click on New then Workstation. In the Workstation Properties window, enter the, Swivel server IP Address, choose 'Host' for Type. For the Comment enter enter "PINsafe authentication". When complete, click OK. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

Select Manage/Servers then click on New and from the menu select Radius. In the RADIUS Server Properties window enter the following:

Name RADIUS server name

Comment information e.g. PINsafe RADIUS server

Colour A colour for the object (we like orange!)

Host hostname of the Swivel server created above

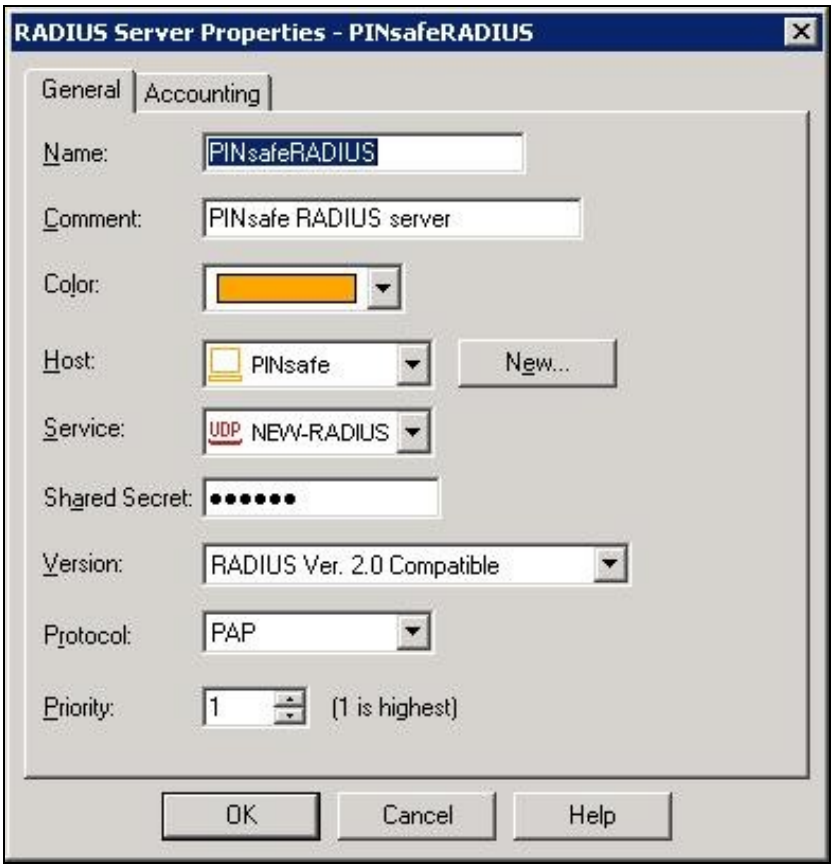
Service select New Radius (Uses port 1812)

Shared secret enter the shared secret that is also entered on the Swivel server

Version select the RADIUS version required

Protocol select the required RADIUS version

Priority The priority for authentication to multiple RADIUS devices



69.1.2 To configure External Checkpoint VPN-1/Firewall-1 users to authenticate by RADIUS

External User Profiles There are two different types of External User Profiles available in the Check Point VPN-1/Firewall-1 product, either match all users or match by domain, whereby users are differentiated by their domain name.

The steps below will configure an External Profile of Match All Users.

1. On the Checkpoint VPN-1/Firewall-1 configuration select Manage/Users and Administrators/New/Match All Users/Default.

2. The user generic* is created and greyed out.

3. Select the Authentication tab.

4. From the drop down box choose RADIUS as the user?s Authentication Method.

For further details on the available user authentication methods, configuration and setup, refer to the VPN-1/Firewall-1 Administration Guides.

The SecureClient is now ready for two factor authentication using standard SMS delivery or the Mobile Phone Client.

69.2 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. Open the Secureclient, 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 SecureClient 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. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

69.3 Modifying the Checkpoint SecureClient for Single Channel and Advanced SMS features

Note that all .dll files have been renamed to .dlx, and .reg files to .rex, to avoid problems with email filters. You will need to change the names back before deploying the files.

Stop the SecureClient or ensure it is not running.

Copy PINsafeAuthGUI.dll, and copy it to the SecuRemote\bin folder

Edit SecuRemote\database\userc.C. and add the below to the :options section

```
:guilibs (
: ("C:\Program Files\CheckPoint\SecuRemote\bin\PINsafeAuthGUI.dll")
)
```

Edit RegSettings.reg. to set the correct Swivel server and possibly the port and context. Double-click RegSettings.reg to install the registry settings the DLL needs.

The options are:

PINsafeServer: The IP address of the Swivel server. This should be a NAT address of the Swivel server and accessible from the client.

PINsafeProtocol: 1 for https, or 0 for http

PINsafePort: The port used to retrieve single channel images from the Swivel server, usually 8443 for a Swivel virtual or hardware appliance. For a software only install see Software Only Installation

PINsafeContext: The installation instance of the pinsafe server, usually pinsafe or proxy for a Swivel virtual or hardware appliance

PINsafeAllowSelfCert: 1 to allow self signed certificates on the Swivel server, 0 to not allow them to be used

PINsafeSecret:

PINsafeUser: The user for authentication can be pre-configured. Do not set this value if this is a template to be used for deployment to multiple users.

PINsafeChannelType: single or dual channel communications. Setting dual, requests an SMS security string by the on demand method. The On Demand authentication must be enabled on the Swivel server.

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="localhost"
"PINsafeProtocol"="1"
"PINsafePort"="8080"
"PINsafeContext"="pinsafe"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Swivel virtual or hardware Appliance Values:

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="External NAT IP of PINsafe server"
"PINsafeProtocol"="1"
"PINsafePort"="8443"
"PINsafeContext"="proxy"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Verify that winhttp.dll is present in C:\Windows\System32

Start SecureClient. Click connect. Under Options, Change Authentication to Secure Authentication API.

When you click Connect, you should now either see a dialog with a TURing on it, or "CONFIRMED" for dual channel, in which case a security string will be sent by the appropriate transport. The password field has been left in case you want a password as well as a OTC, but this can be removed if required. Enter the OTC, and hopefully it will authenticate.

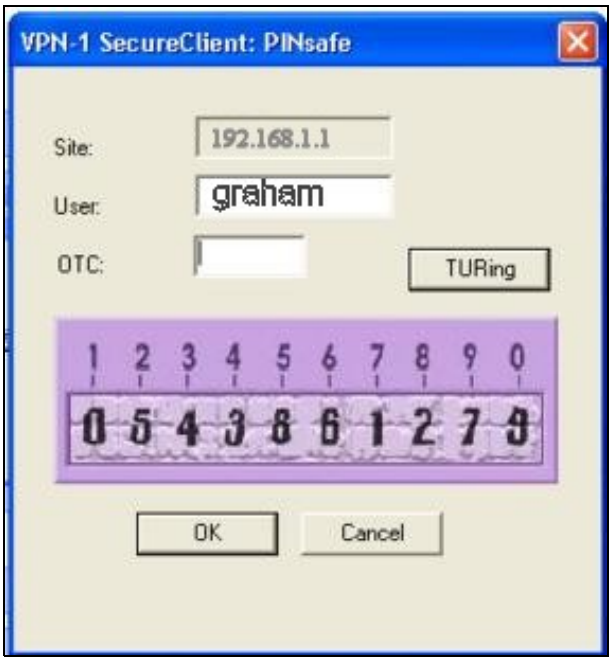
70 Removing the Swivel SecureClient

To remove the Swivel authentication remove the earlier added content in Edit SecuRemote\database\userc.C.

then restart the client

71 Verifying the Installation

Login using the Turing or SMS.



72 Bulk deployment

With a tested deployment, it is possible to take these settings and create a msi file that will install the Swivel SecureClient software.

For further information see [[1]]

73 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Check the Checkpoint Firewall Logs

radius not supported

This can be seen when using local policies, switch to a Global Policy for RADIUS authentication and test, or for individual users use RADIUS authentication.

74 Known Issues and Limitations

Checkpoint will not accept RADIUS passwords greater than 16 characters in length. If check password with repository is used, then the PIN length will also need to be taken into account, i.e. for a 4 digit PIN, this restricts the length to 12 characters. Two stage RADIUS authentication will bring this back to 16 characters.

75 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

76 Cisco AnyConnect

77 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.

78 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.

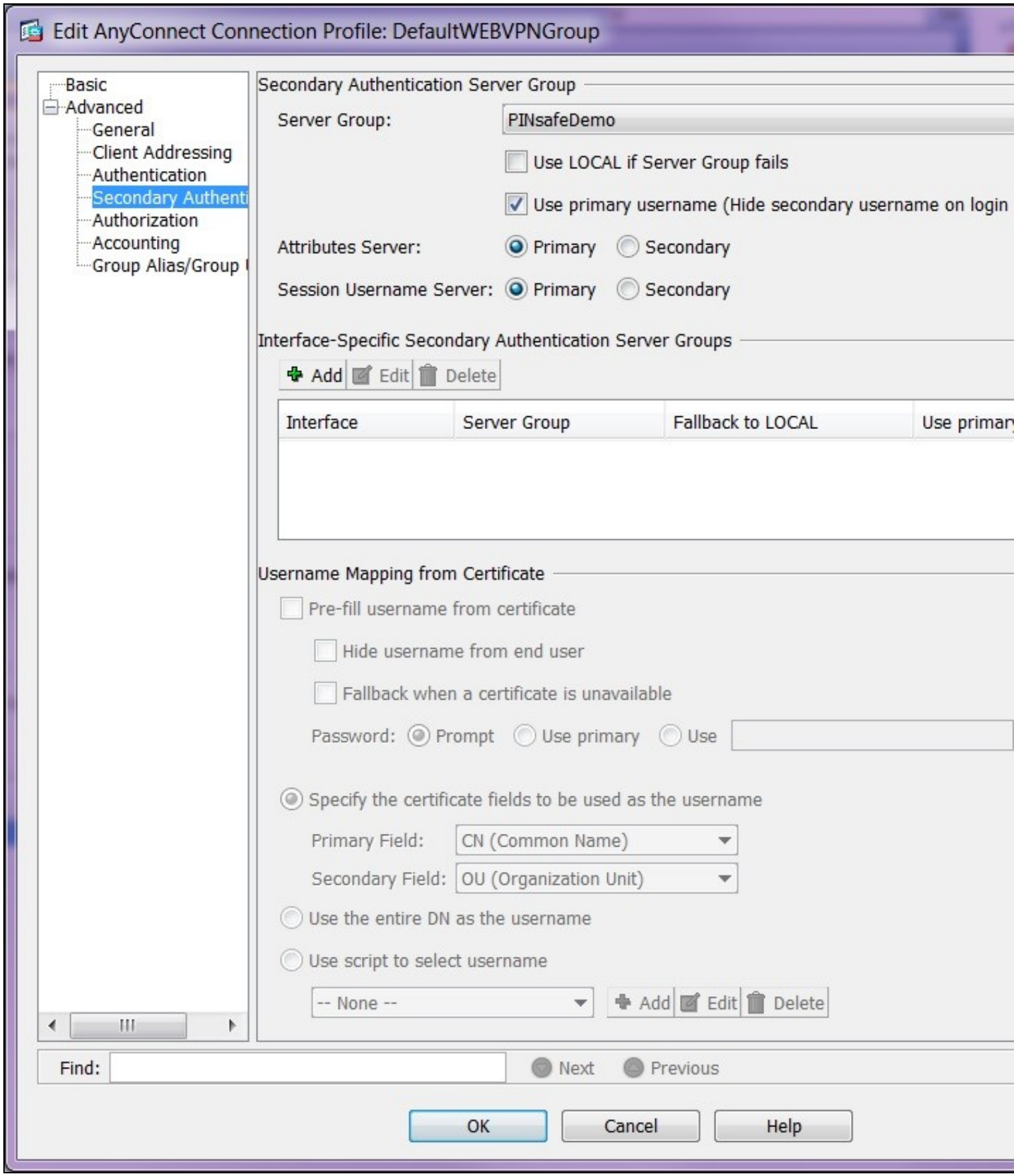
79 Cisco AnyConnect Client Integration

79.1 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.

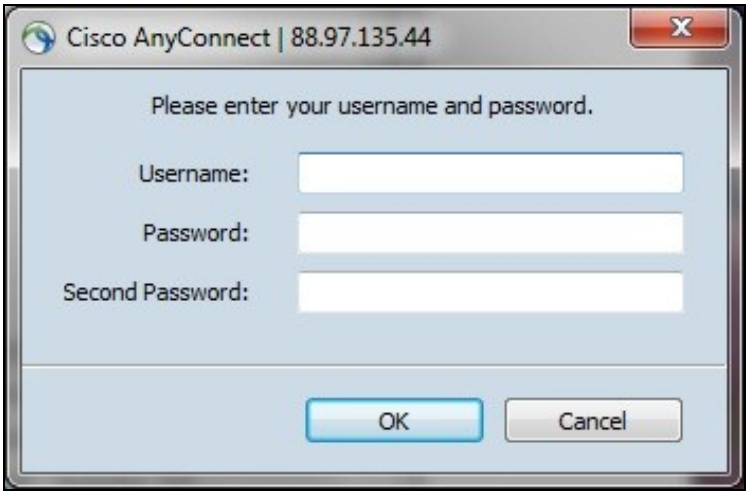


When using a Primary authentication service such as Active Directory and a secondary authentication service such as Swivel, the AnyConnect client will display an extra password field, allowing entry of username, password and One Time Code.

79.2 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.



80 Swivel modified AnyConnect Client for TURing and PINpad

80.1 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.

80.2 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.

80.3 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.

80.4 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.

81 Cisco ASA Integration

82 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

82.1 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.

83 Prerequisites

Cisco ASA 8.03 or higher

Cisco documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

83.1 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**.

84 Baseline

Cisco ASA 8.03, Also tested with 8.21

Swivel 3.5, 3.6, 3.7, 3.8, 3.9

85 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

86 Swivel Configuration

86.1 Configuring the RADIUS server

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

86.1.1 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.

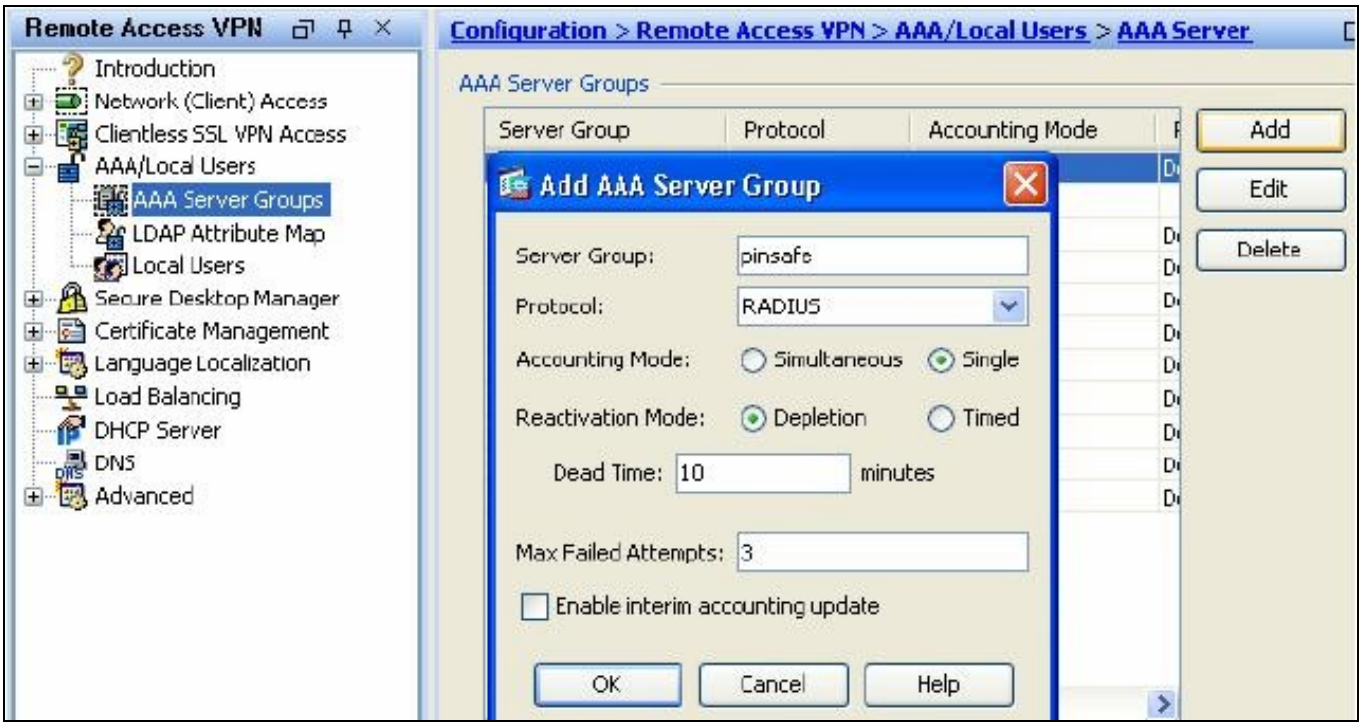
86.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

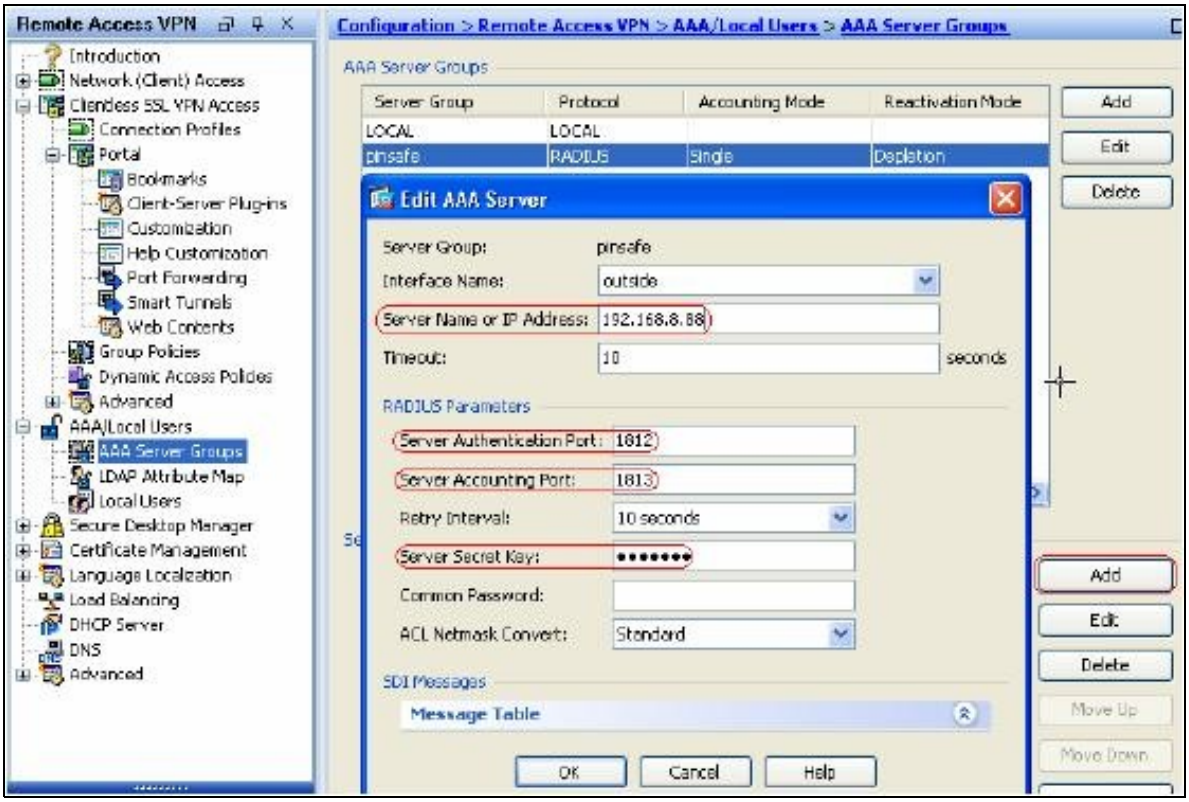
87 Cisco ASA Configuration

87.1 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.



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.

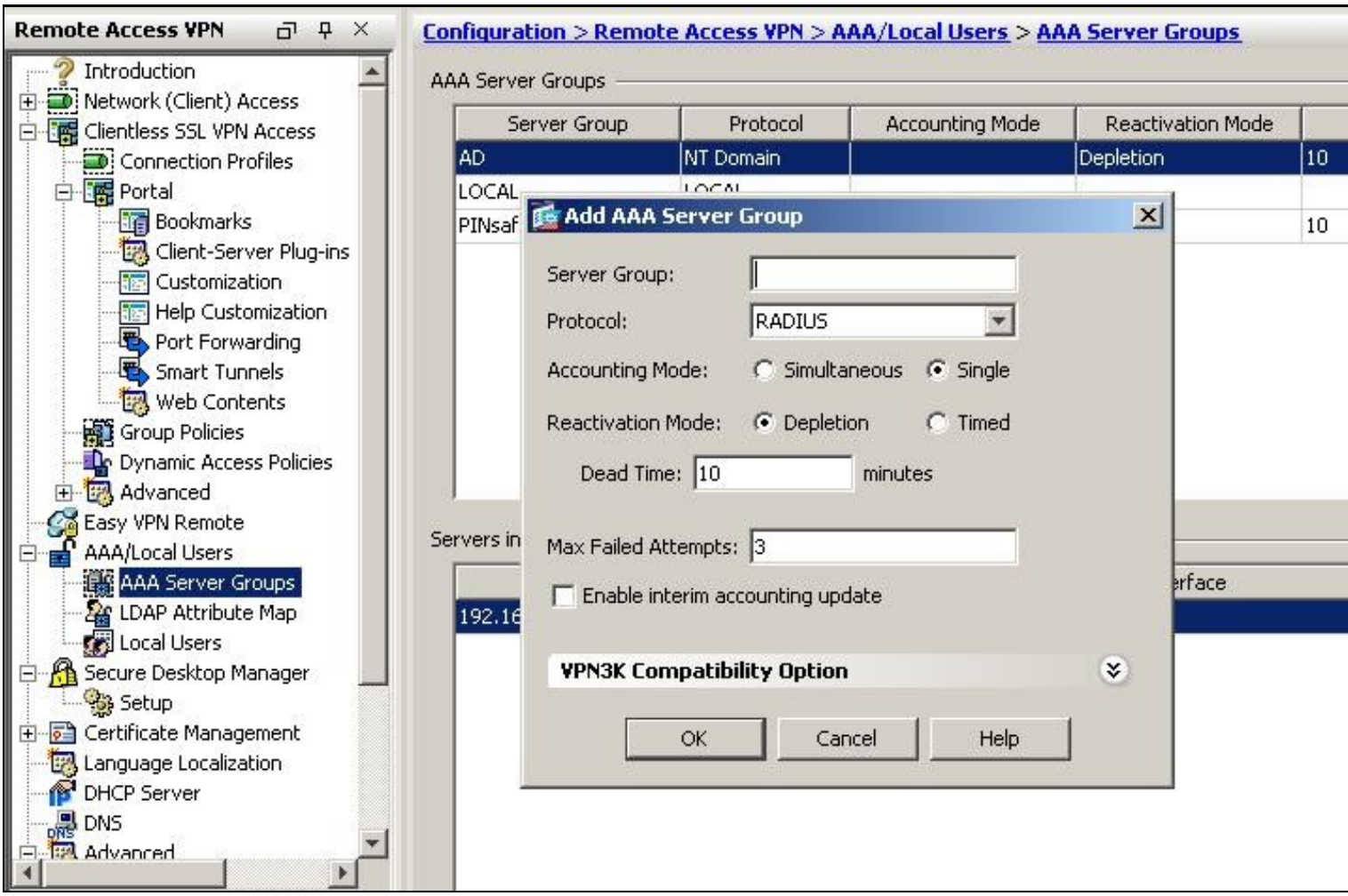


Enter Swivel server?s IP, authentication port and server secret key as indicated. Click on OK then Apply to save the AAA server group.

87.2 Optional: Create a Secondary Authentication Server

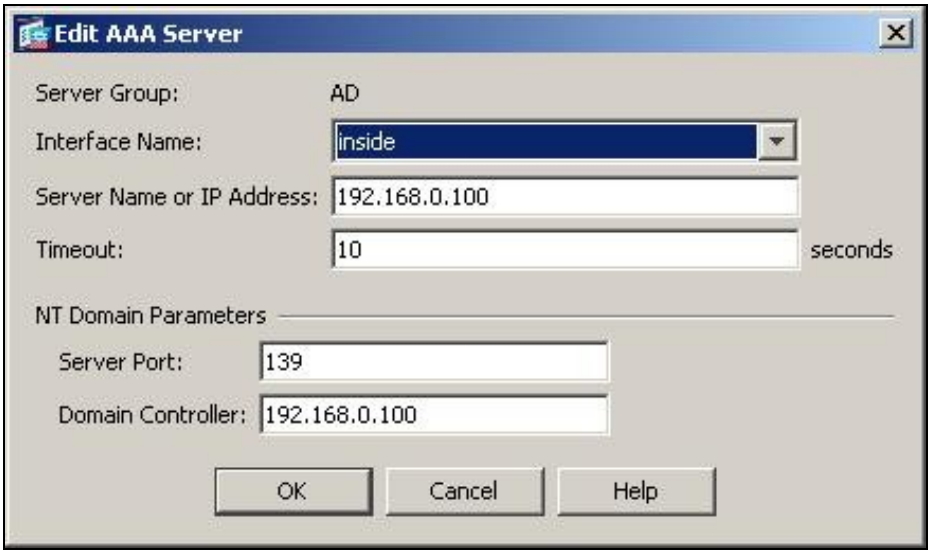
The login page can be configured to display Swivel as a primary or secondary authentication server. To use multiple authentication servers, they must be configured under Remote Access VPN -> AAA/Local users -> AAA Server. This example shows an AD Server being added.

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



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.

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

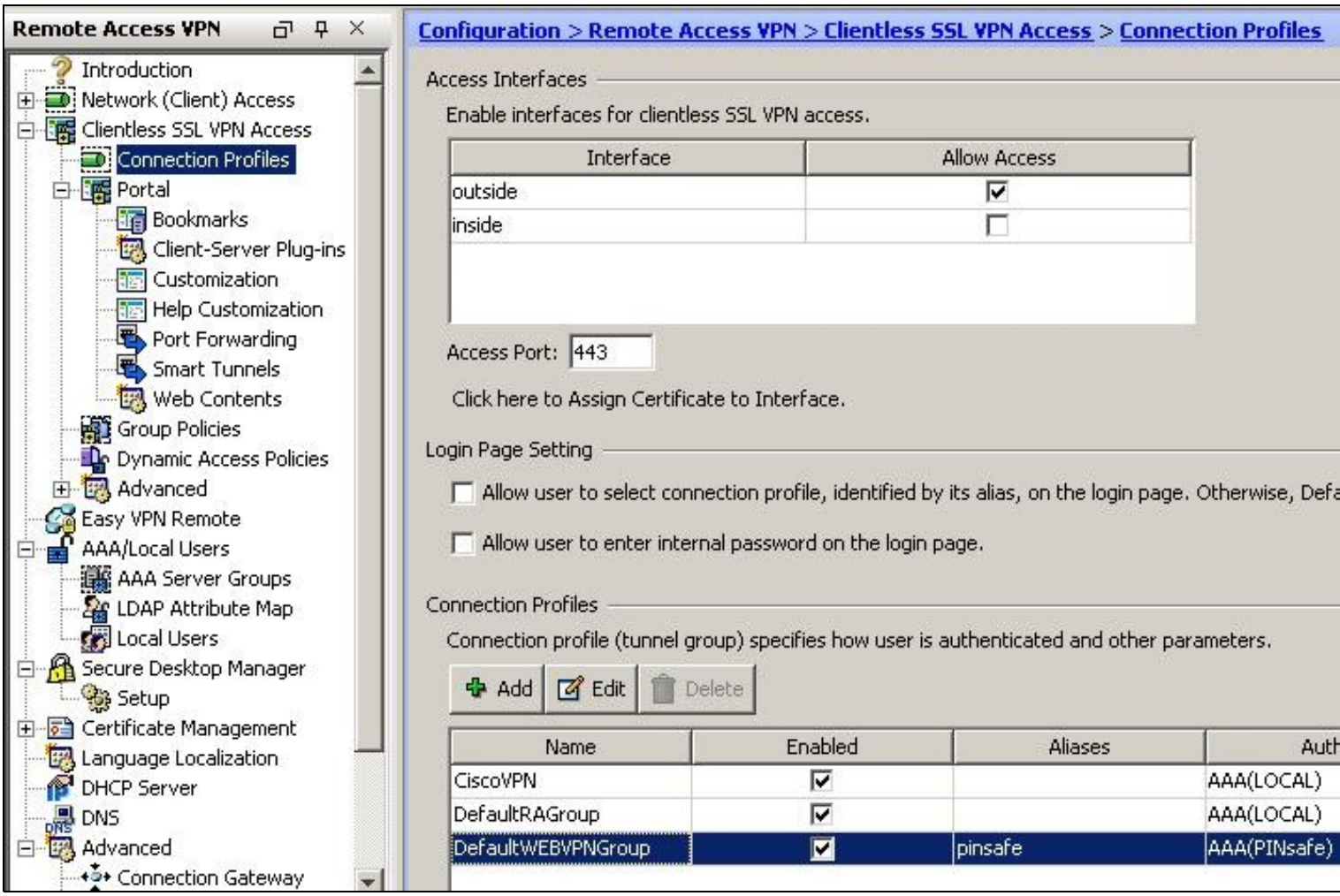


This secondary authentication server then needs to be linked to the Connection Profile (see below).

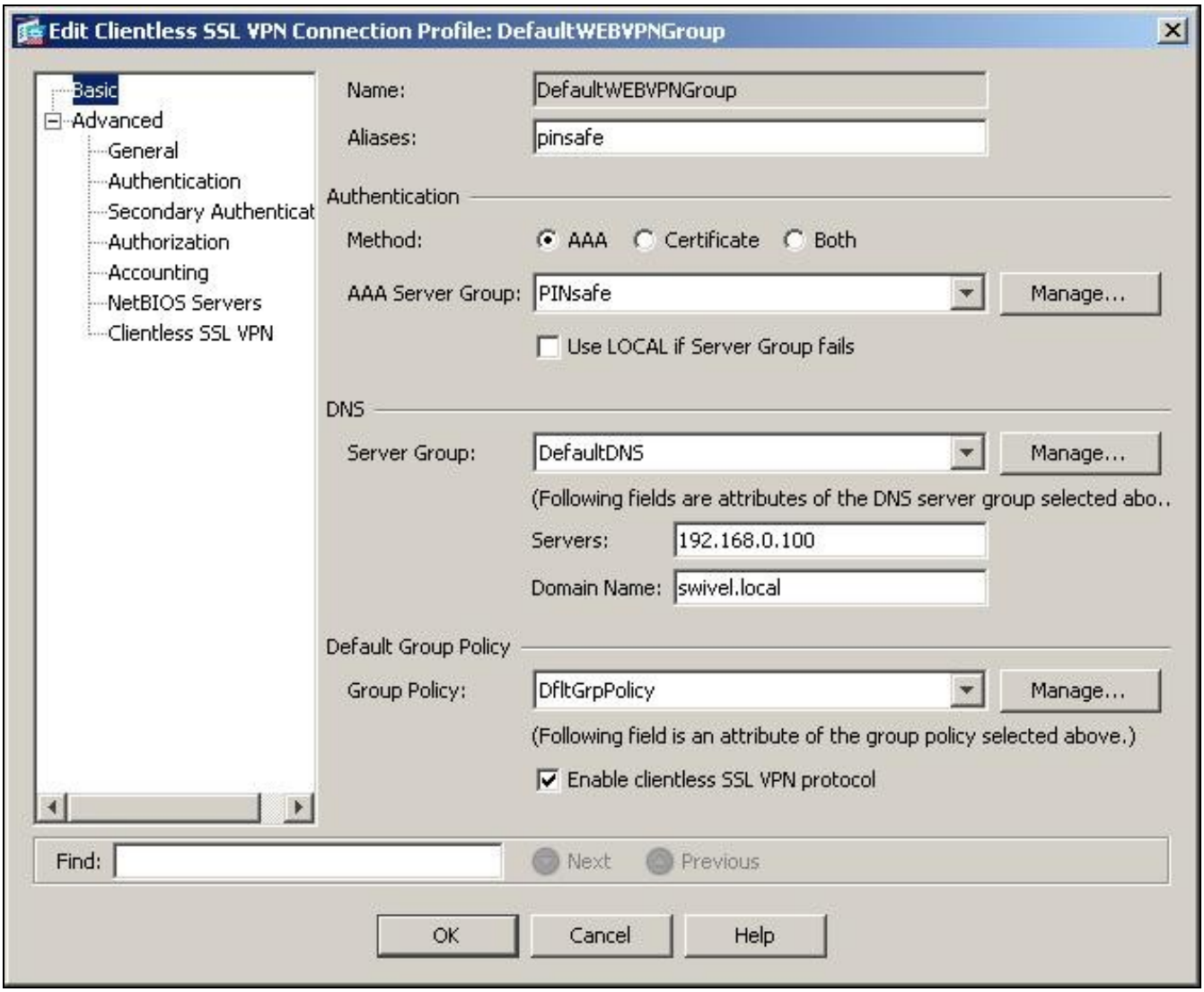
87.3 Create a Connection Profile (Tunnel Group)

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

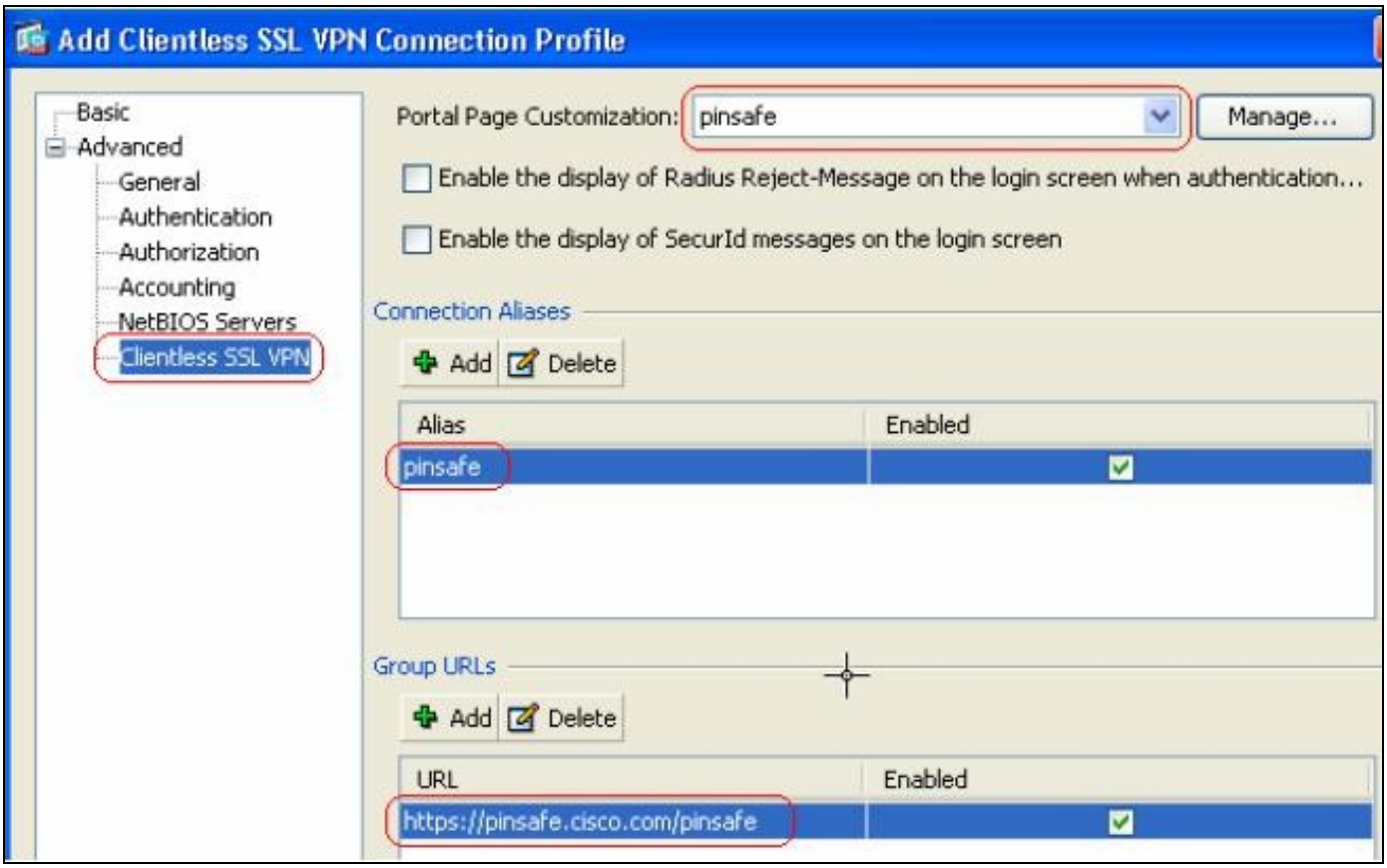
Connection Profile is used to link authentication server group, URL used to access the ASA, and login page customization together. Go to Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles. Click on Add to add a connection profile.



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.



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.



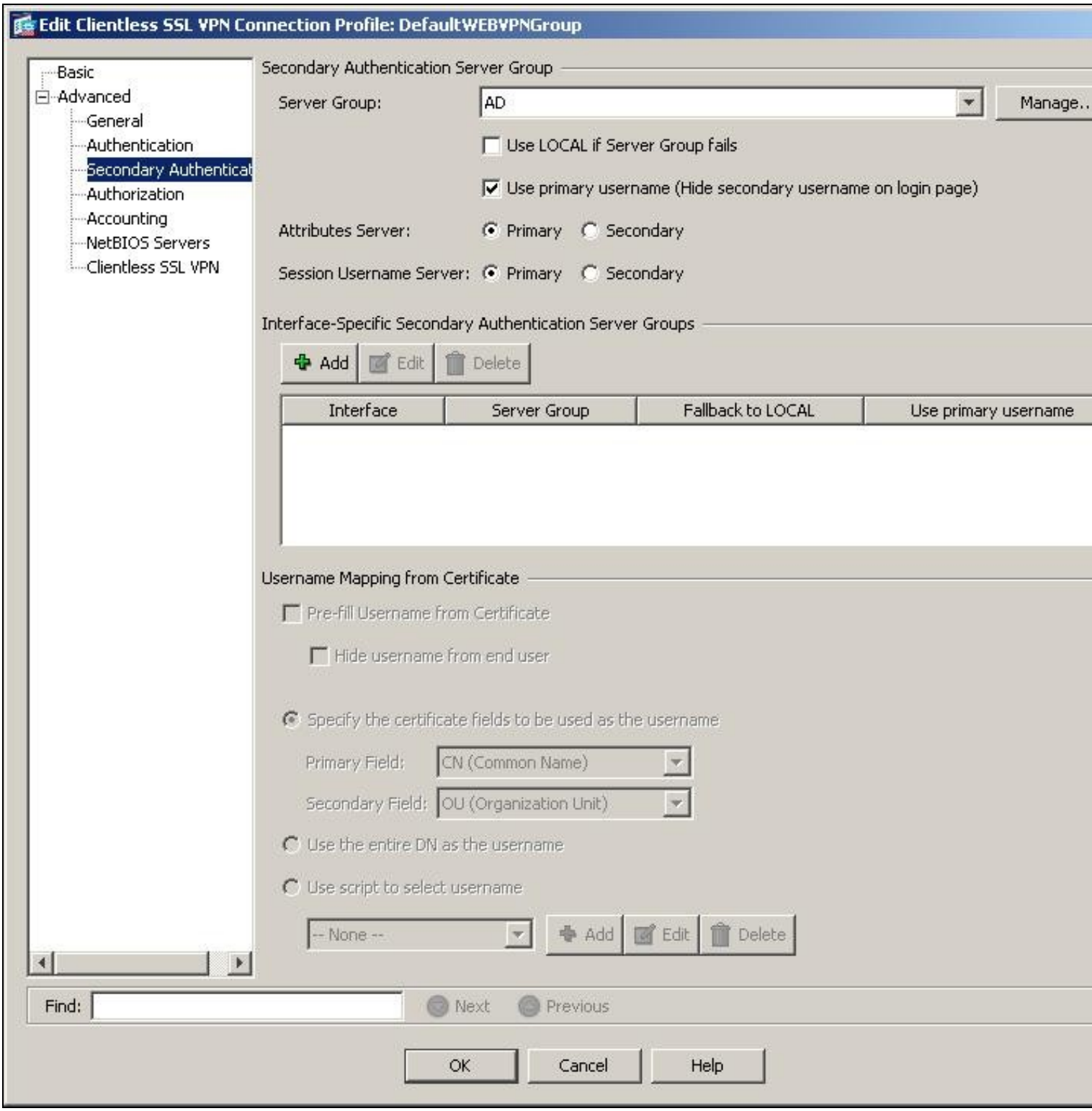
Click on OK then Apply to save the Connection Profile.

87.4 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.



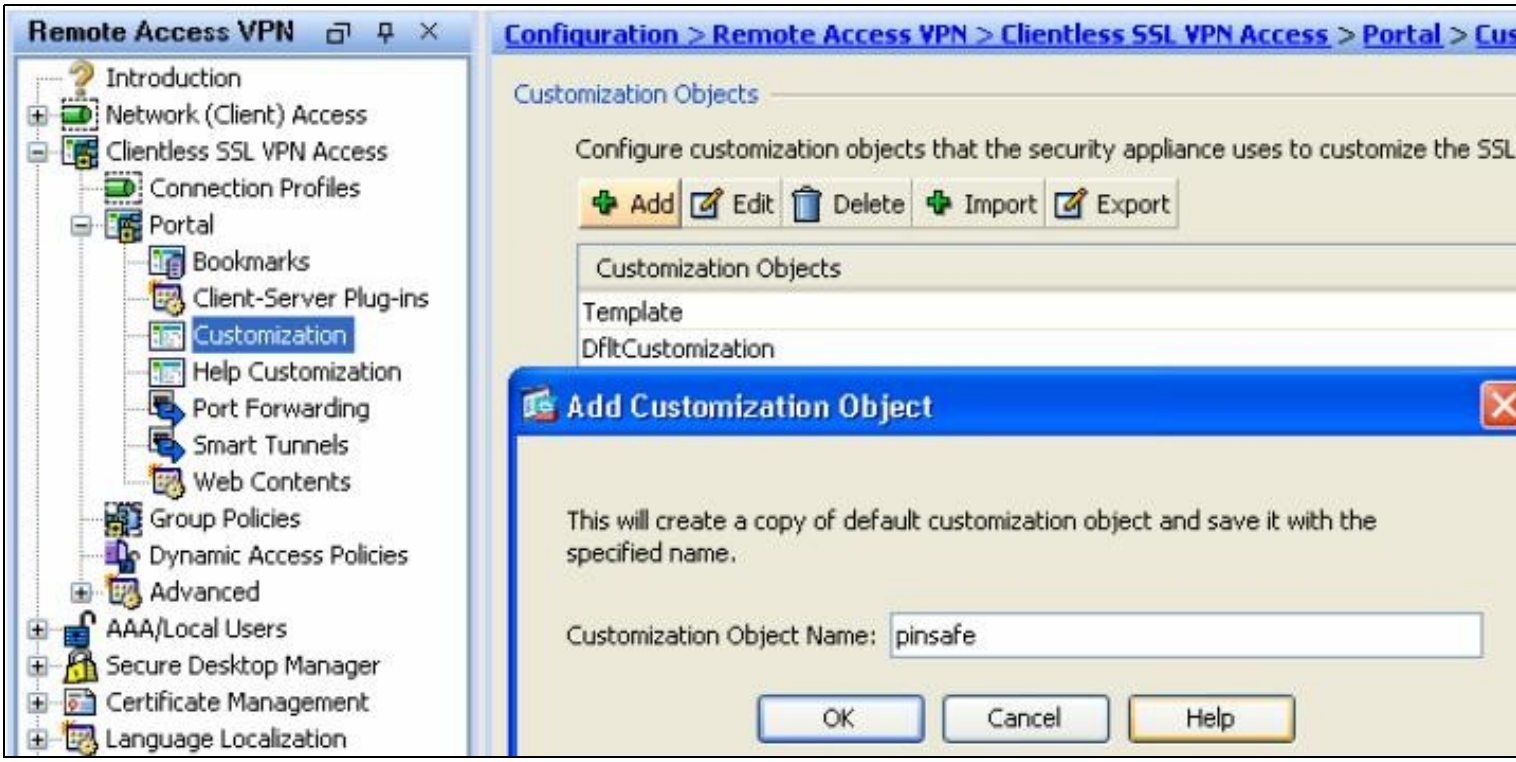
87.5 Test the RADIUS authentication

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.

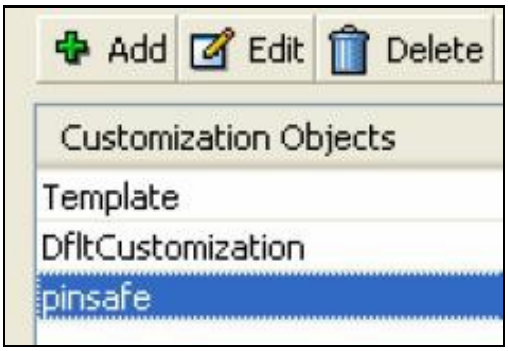
87.6 Optional: Login Page Customisation

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

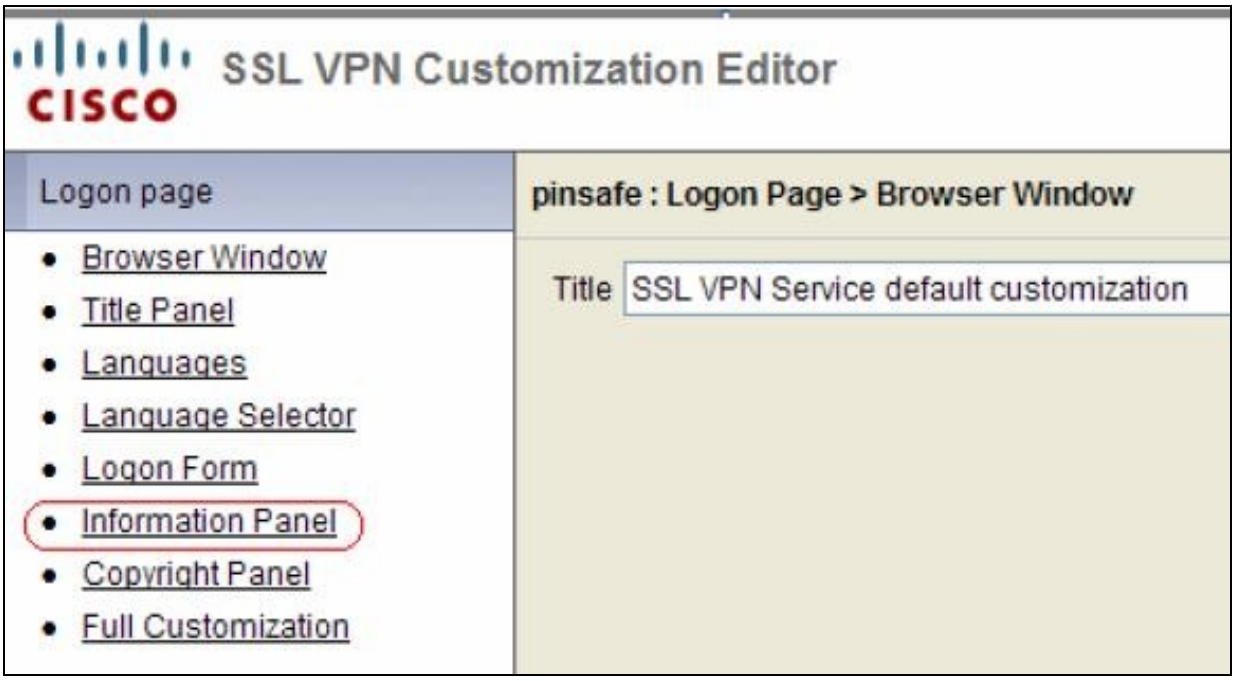
Javascript to retrieve Swivel Turing image. In ASDM, go to Remote Access VPN ->Clientless SSL VPN Access -> Portal -> Customization. Click on Add to add a new customization object.

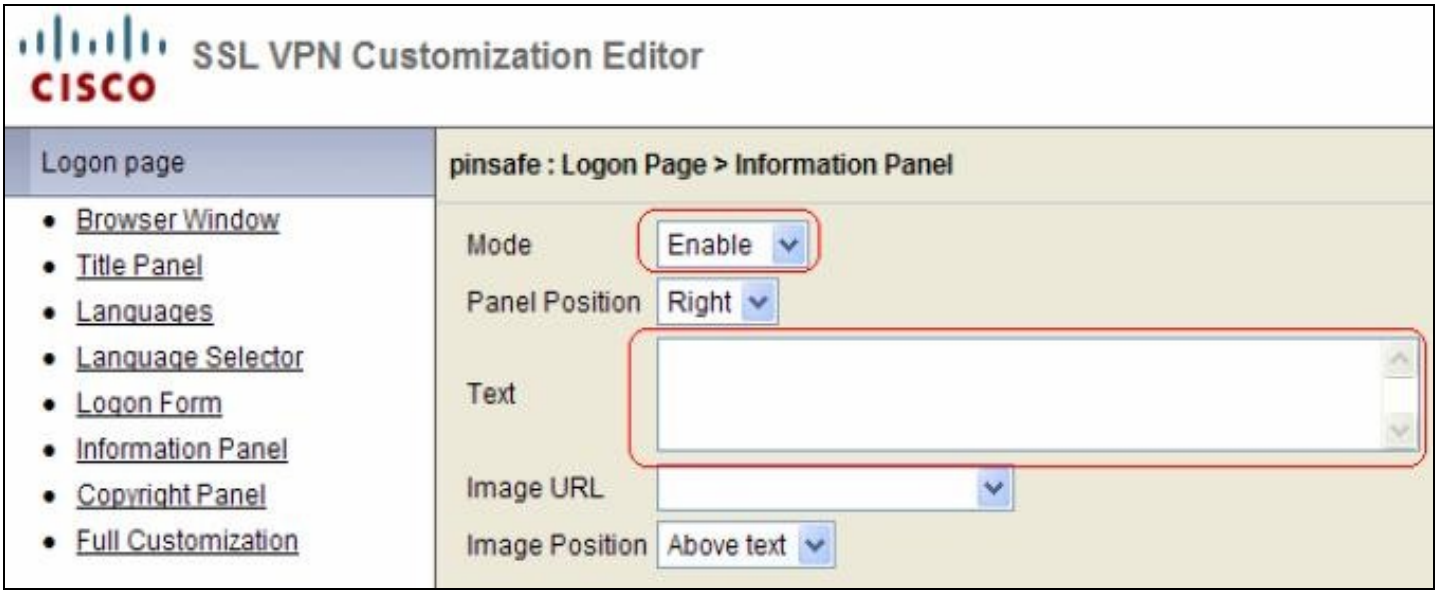


Enter a name for the object, click on OK then Apply.



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.





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

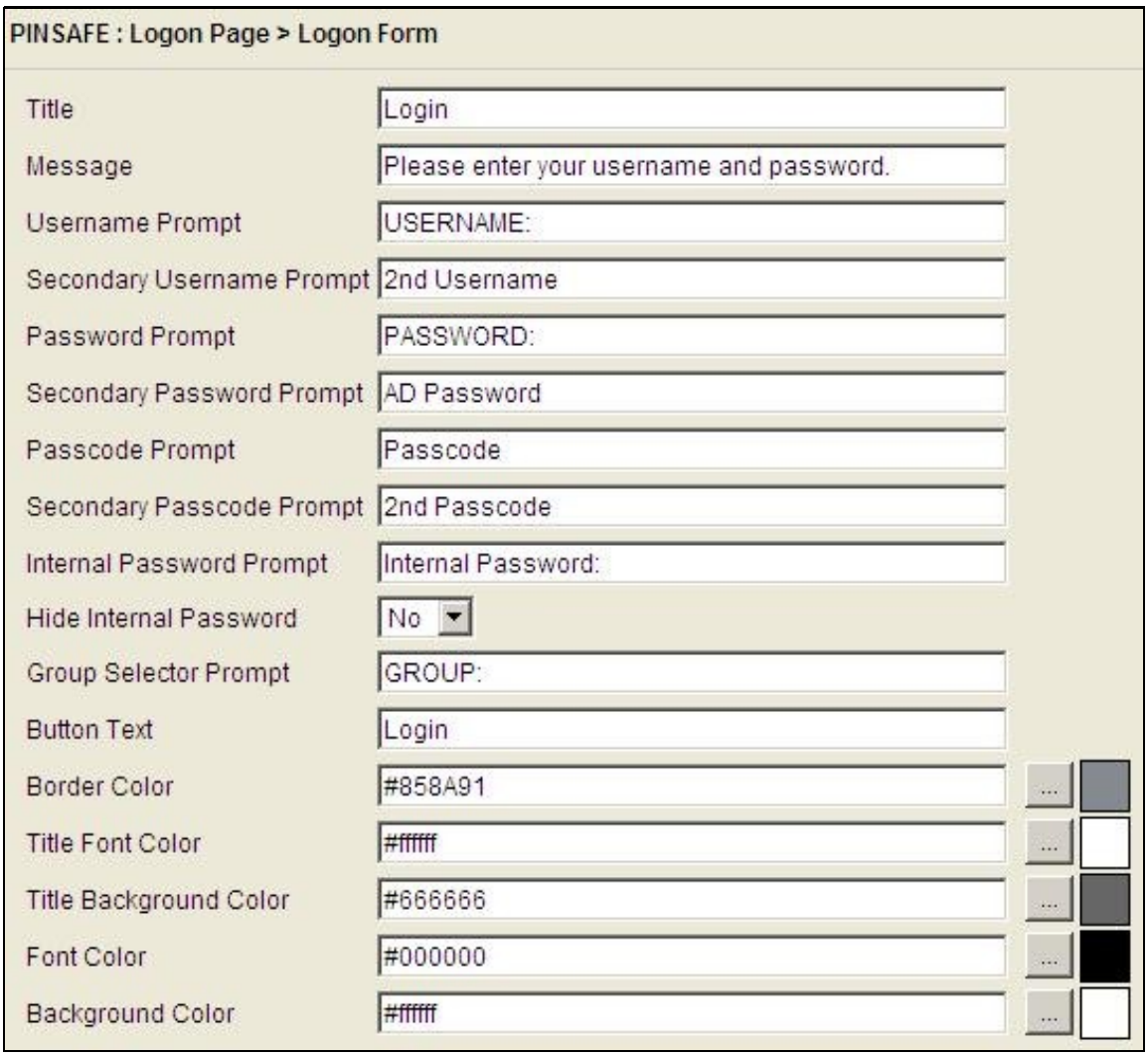
```
"Please enter your user name and click on Get OTP Index";
```

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.



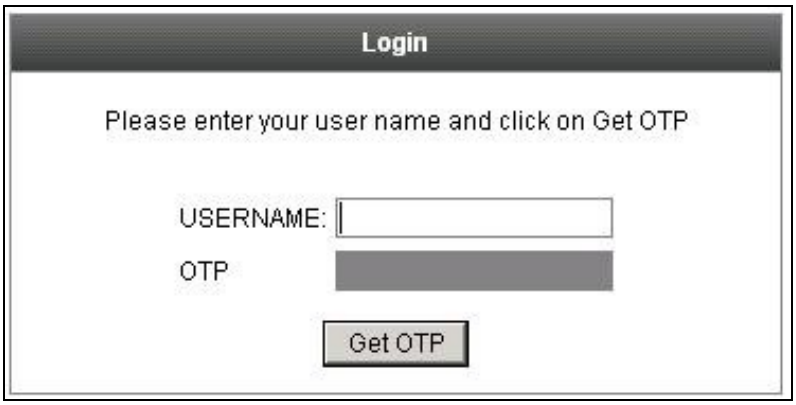
AD as the primary authentication server, Swivel as the secondary authentication server.

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

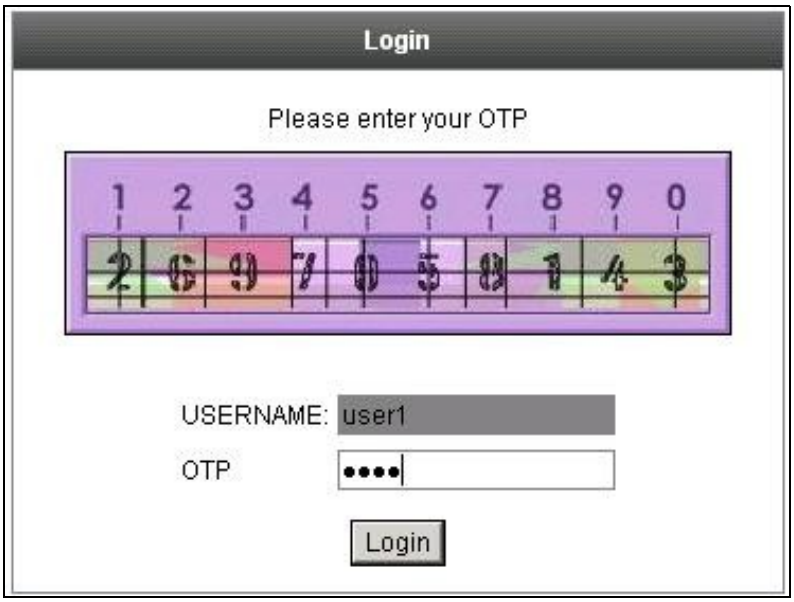
88 Testing

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

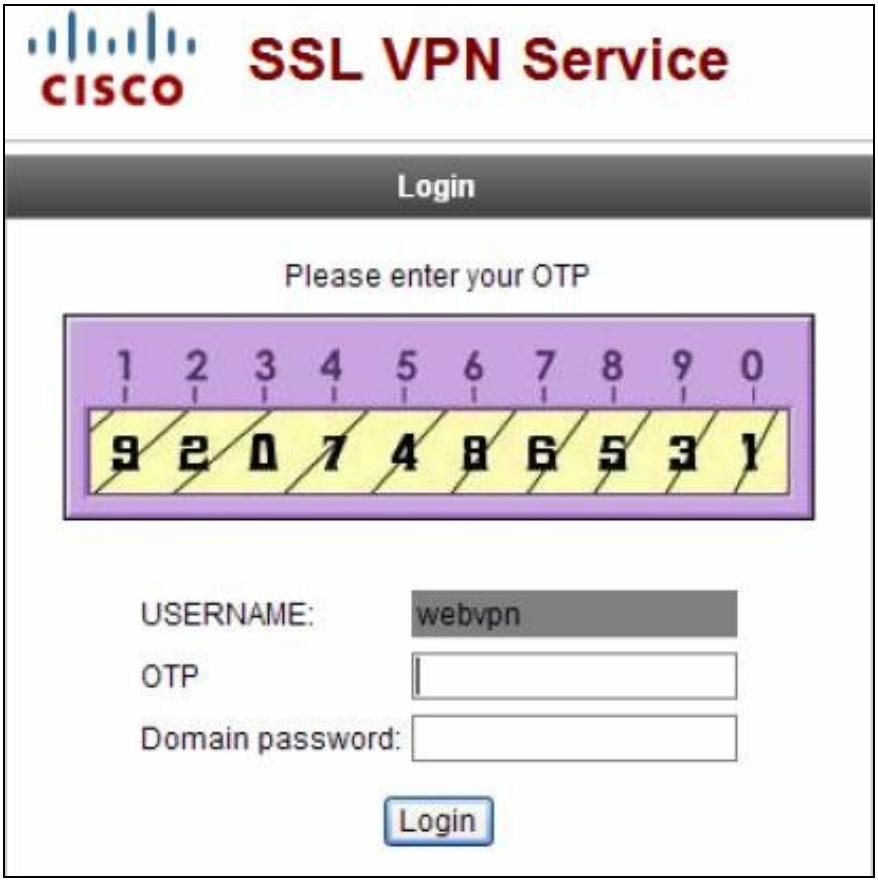


If configured, a Domain Password prompt will appear.

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

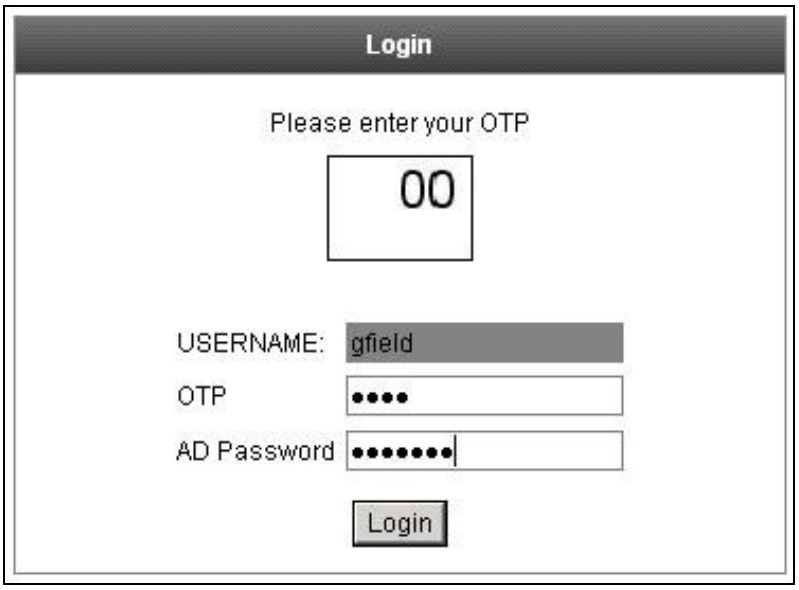


OTP login with Domain Password

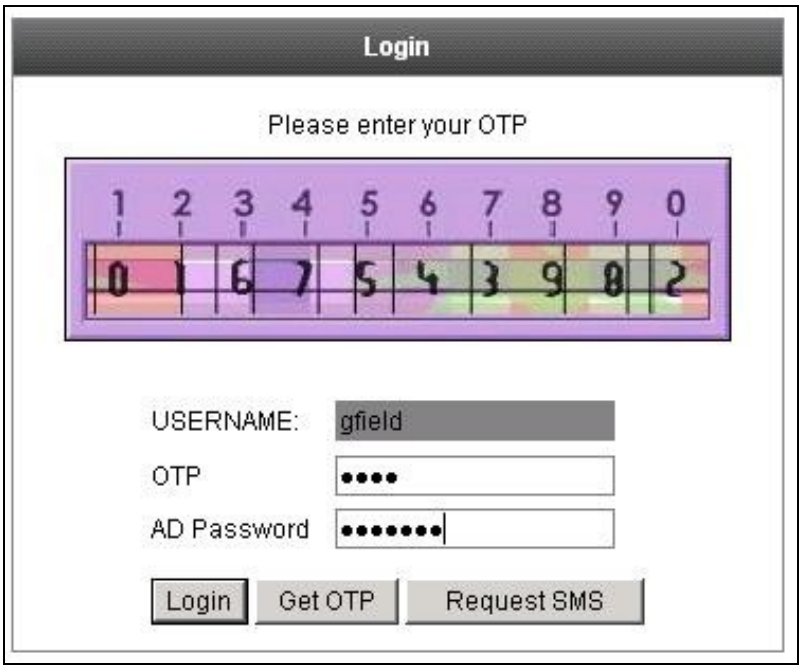


Use your PIN to extract the OTP and enter it in the OTP field. If everything is configured correctly, you will see the portal page after clicking on Login. Please note that the Javascript to retrieve the Turing image is executed at the user?s browser. Therefore, the user?s PC must have access to the 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.



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




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

89 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";
}
```

89.1 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>
```

90 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.

91 Known Issues and Limitations

None

92 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

93 Cisco IPSEC Client Integration

93.1 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

93.2 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

93.3 Baseline

PINsafe 3.5

Cisco IPSEC VPN Client 5.0.02

PINsafe Taskbar 1.3.01

93.4 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.

94 Swivel Configuration

94.1 Configuring the RADIUS server

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

94.2 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.

94.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

94.3 PINsafe Client Configration

94.3.1 PINsafe Dual Channel Configuration

No specific client requirements for Dual Channel integration.

94.3.2 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.

94.4 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.

94.5 Cisco IPSEC Client Configuration

94.5.1 Cisco IPSEC Client with Dual Channel Authentication

No further configuration is required for the Cisco IPSEC client

94.5.2 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.

94.5.3 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.

94.6 Additional Configuration Options

94.7 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.

94.8 Known Issues and Limitations

None

94.9 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

95 Cisco SA 520

95.1 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.

95.2 Prerequisites

Cisco SA 520

Cisco documentation

PINsafe 3.x, 3.5 for RADIUS groups

95.3 Baseline

Cisco SA 520 firmware version 2.1.51

PINsafe 3.8

PAP Authentication was tested in this setup

95.4 Architecture

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

96 Swivel Configuration

96.1 Configuring the RADIUS server

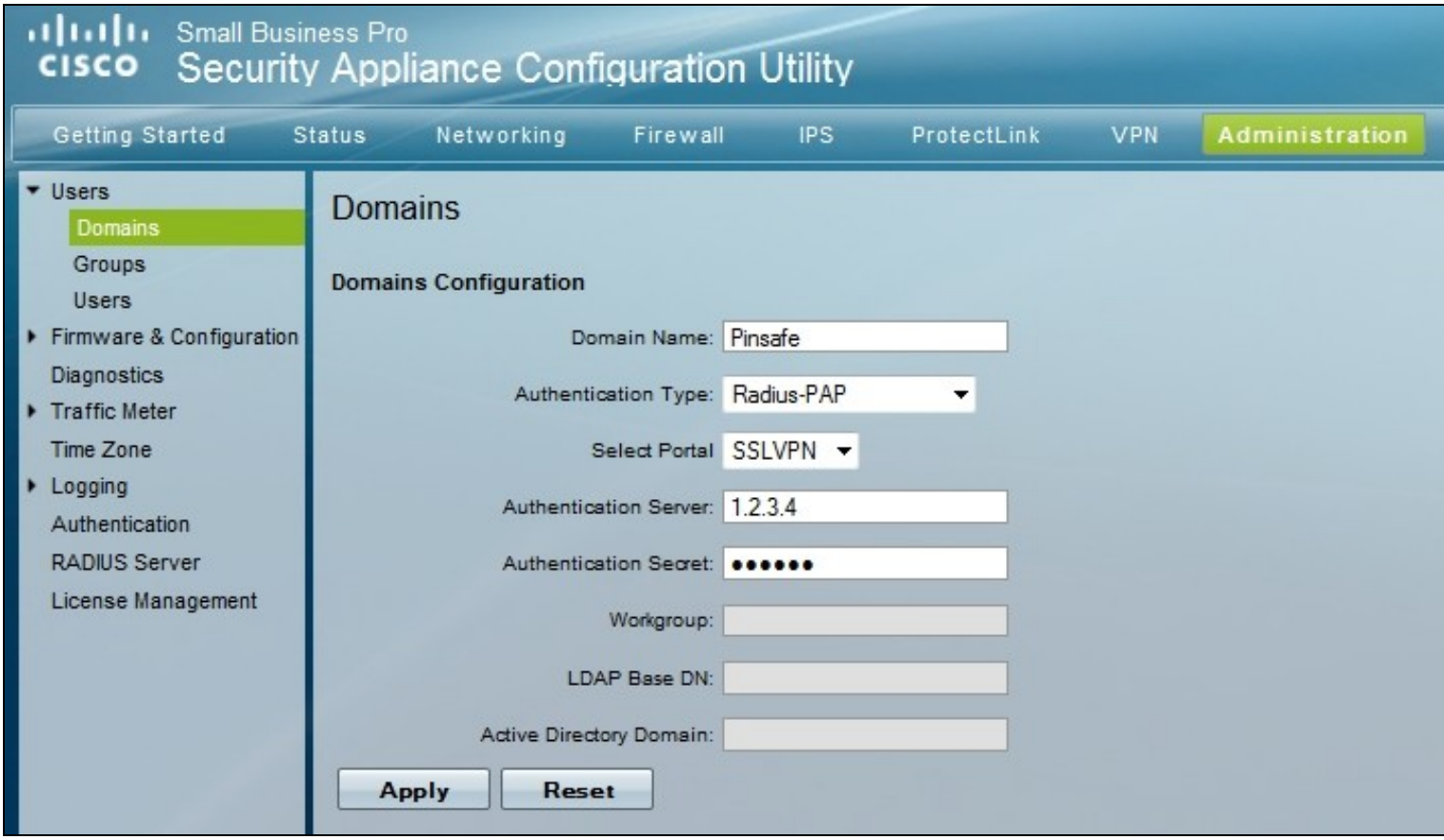
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

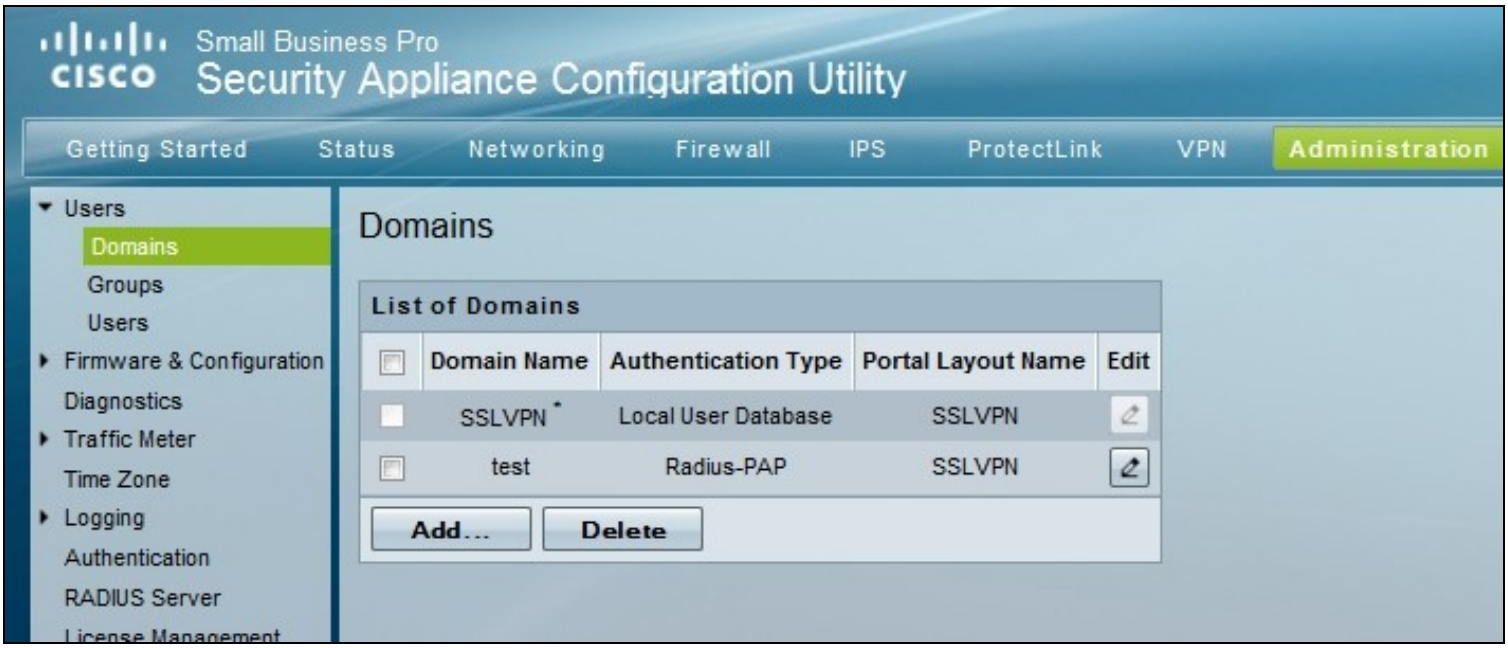
96.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

96.3 Cisco SA 520 Configuration

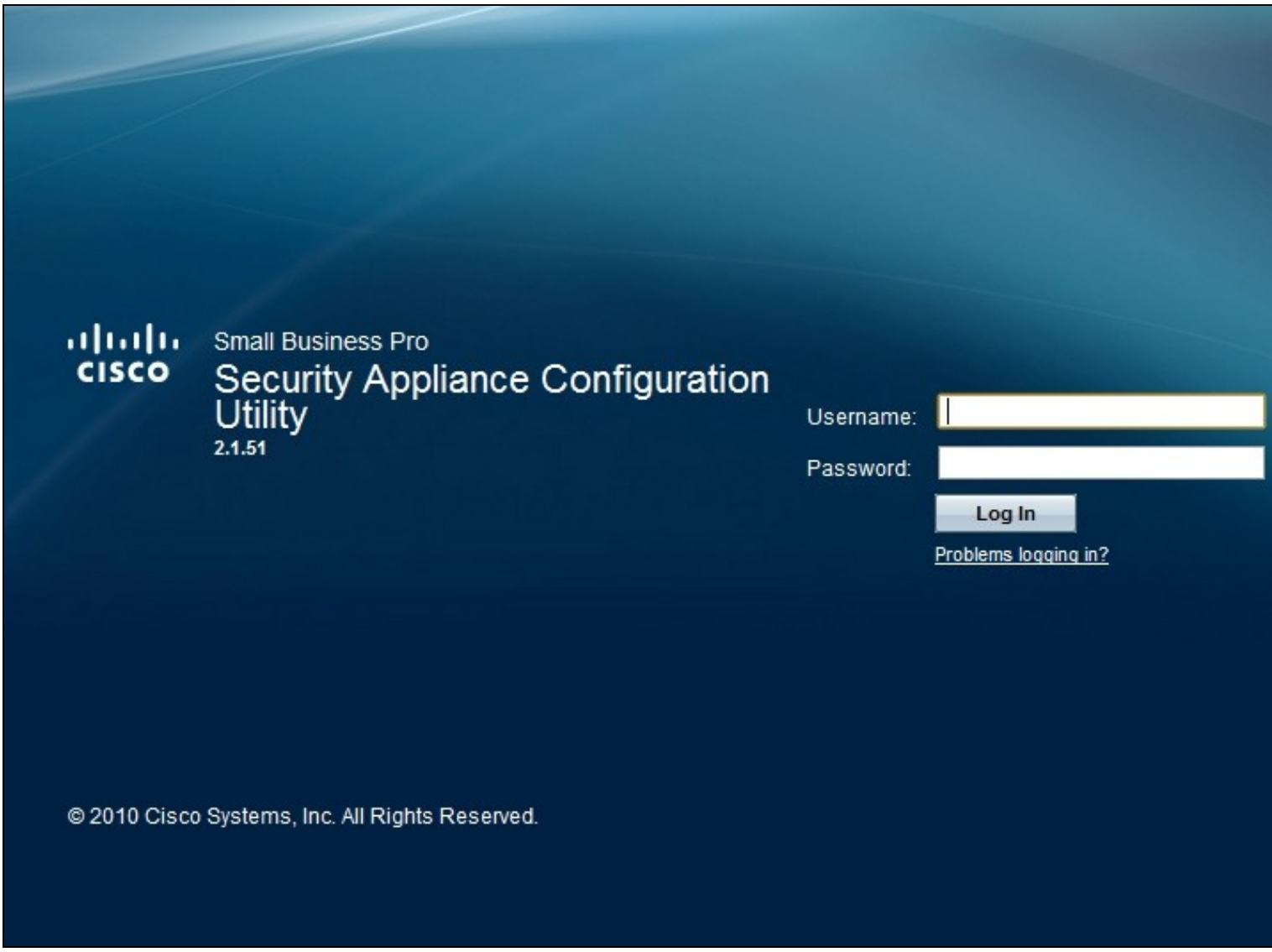
On the Cisco SA 520 Administration console select the Administration tab then users and domains. Click on Add, and enter the PINsafe RADIUS server authentication details for the portal.





96.4 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.



96.5 Additional Configuration Options

96.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

96.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

96.8 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

97 Citrix Access Gateway 5 VPX

97.1 Introduction

Please refer to the documentation located at:

Citrix Access Gateway Standard 5.x

98 Citrix Access Gateway Access Controller 5.0

PINsafe integrates with the Access Controller 5.0 using RADIUS authentication. The following authentication methods are supported:

- SMS
- Mobile Phone Client
- Email
- Taskbar utility

Please refer to the Citrix Access Controller Administration guide for further information on configuring the Access Controller.

The single Channel graphical TURing image cannot currently be embedded into the login page when using the Access Controller 5.0, but we hope to offer this enhancement at a future date. Please contact Swivel Secure to register your interest.

99 Citrix Access Gateway Advanced 4.x

100 Introduction

This document covers the integration of Citrix Access Gateway Advanced edition 4.x.

101 Prerequisites

PINsafe 3.x

The CAG 4.5 integration guide is available here: Citrix Access Gateway Advanced edition 4.5

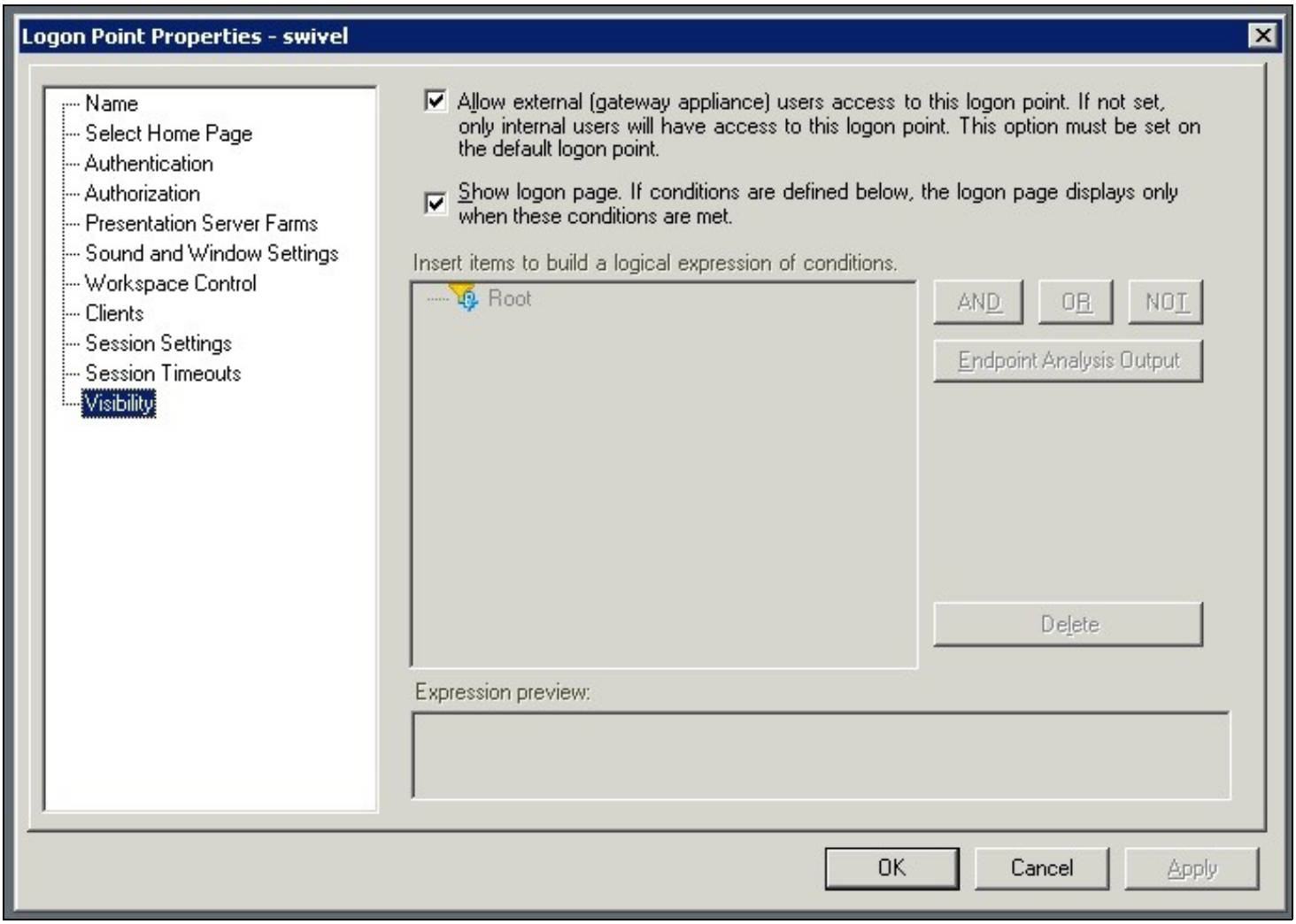
The CAG 4.5.8 integration guide is available here: Citrix Access Gateway Advanced edition 4.5.8

Note: For PINsafe Single Channel authentication the PINsafe server IP needs to be reachable by the client (i.e. this means an external IP address or a NAT for the PINsafe server IP). An SSL certificate is usually installed on the PINsafe server to prevent the browser from displaying errors regarding self signed certificates or sites without SSL certification. Swivel Secure can assist with the deployment of the certificate, but this must be purchased and applied for by the end user or their reseller.

Additional Integration supplementary documentation is provided below

102 Installation

Ensure on the Logon Point Properties, that under Visibility, the check box is ticked for 'Allow external (gateway appliance) users access to this logon point. If not set, only internal users will have access to this logon point. This option must be set on the default logon point.'



103 Additional Installation Options

103.1 Remove automatic TURing image automatically displaying

To prevent the auto-loading, remove (or comment out) the onBlur method on username:

```
//     userField.onblur = ShowTuring;
```

to

```
userField.onblur = ShowTuring;
```

103.2 Prevent browser caching TURing image

To stop image caching, add a random number to the image request **+ "&random=" + Math.round(Math.random()*1000000);**

Example:

```
//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
```

103.3 Prevent the cursor from automatically entering the OTC field

Remove the following line from Login.ascx

```
//Set focus to the OTC input
document.getElementById(sNameOfOTCText).focus();
```

103.4 Change the TURing button text

To change the prompt for Turing, edit the Login.ascx file and look for the line:

```
turingBtn.value = "Turing";
```

and change it to

```
turingBtn.value = "Refresh Image";
```

103.5 Verifying the Installation

103.6 Uninstalling the PINsafe Integration

103.7 Troubleshooting

103.8 Known Issues and Limitations

103.9 Additional Information

104 Citrix Access Gateway Enterprise Edition 10

105 Introduction

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 10.0 (Netscaler VPN).

For version 10.1 refer to Citrix Netscaler Gateway 10.x

For versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8,

For other versions of 9.x see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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 Network Address Translation, often with a proxy server. The Swivel appliance is configured with a proxy port to allow an additional layer of protection.

106 Prerequisites

Access Gateway Enterprise Edition firmware version 10.x

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or Swivel files for version 10.

107 Baseline

Tested with Swivel 3.8, 3.9, 3.9.4

Citrix Access Gateway Enterprise Edition Version NS10.0 Build 70.7, and NS10.1 Build 119.7.

108 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

109 Swivel Configuration

109.1 Configuring the RADIUS server

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

109.2 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.

109.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

110 Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. If the single Channel TURing image is not to be used, then the login page does not need to be modified, unless other functions are required such as the Get Security String Index. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the Swivel server to be accessible from the internet, usually with a NAT.

110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. Note: for appliances, the Swivel VIP should not be used as the RADIUS server IP address, see VIP on PINsafe Appliances

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS

Authentication type RADIUS

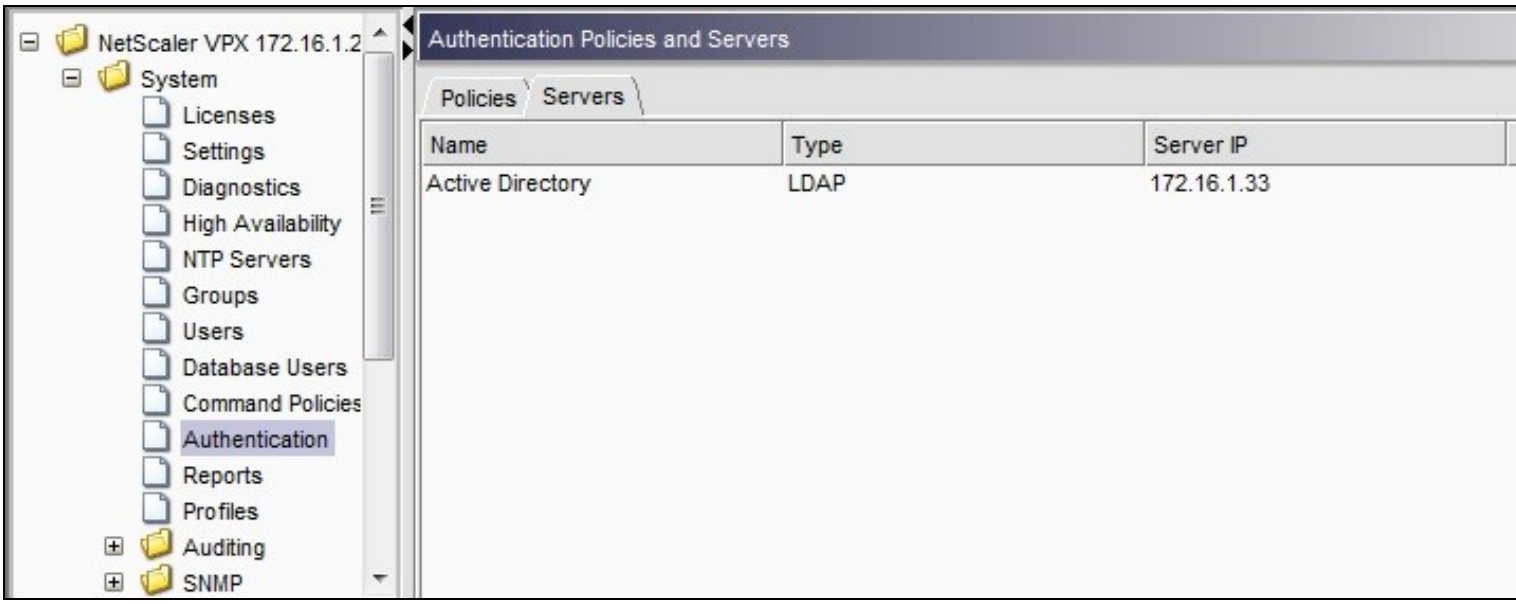
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

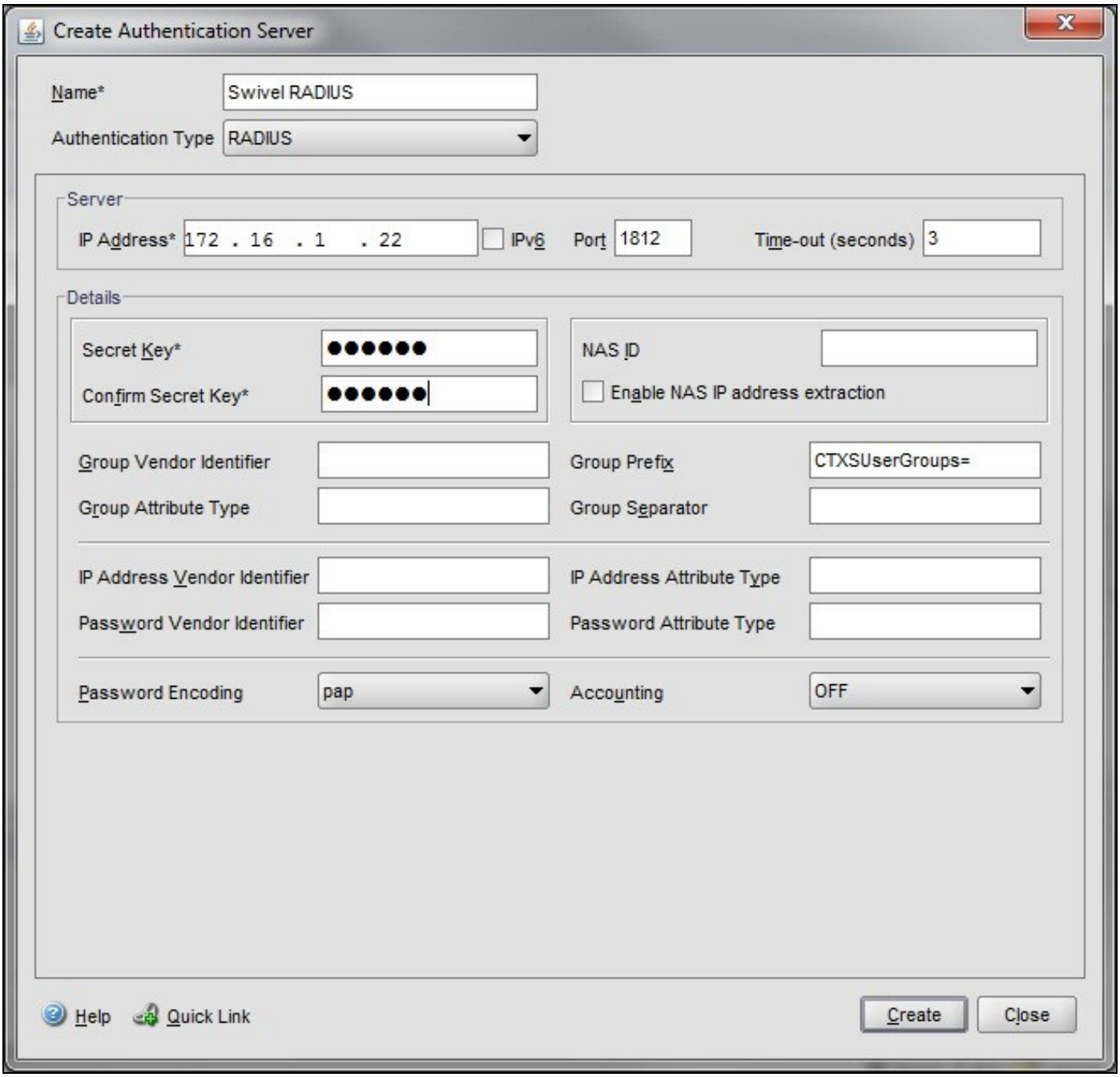
Group Prefix CTXSUserGroups=

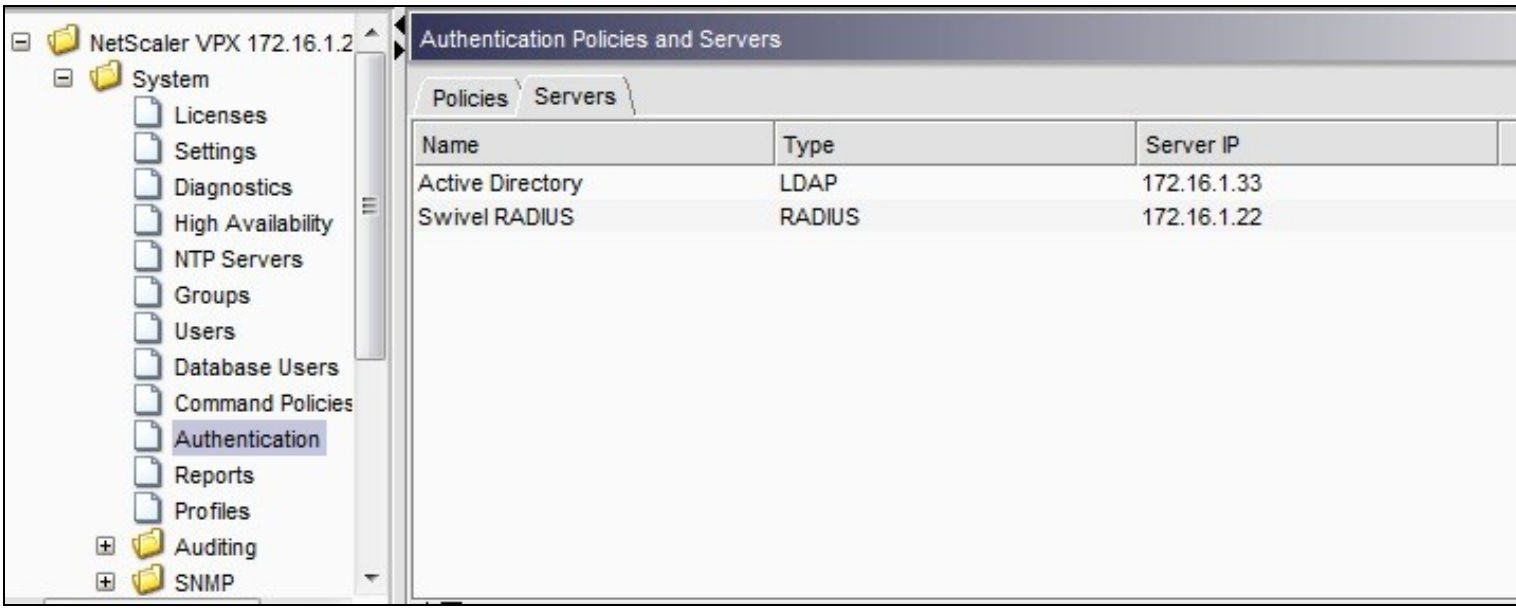
Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.




Create Authentication Server
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
IP Address*
172 . 16 . 1 . 22
IPv6
Port
1812
Time-out (seconds)
3
Details
Secret Key*
Confirm Secret Key*
NAS ID
Enable NAS IP address extraction
Group Vendor Identifier
Group Prefix
CTXSUserGroups=
Group Attribute Type
Group Separator
IP Address Vendor Identifier
IP Address Attribute Type
Password Vendor Identifier
Password Attribute Type
Password Encoding
pap
Accounting
OFF
Help
Quick Link
Create
Close



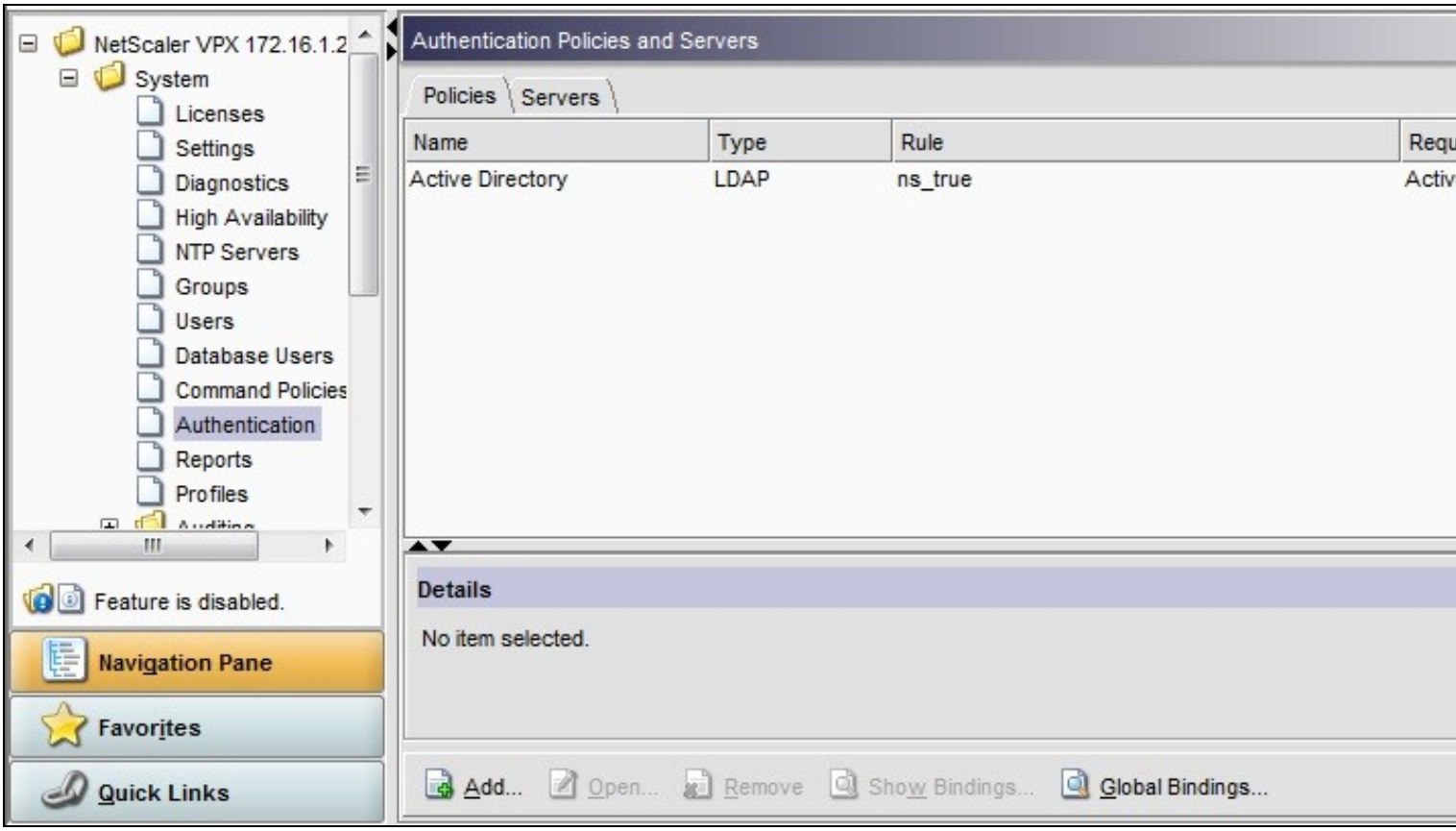
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

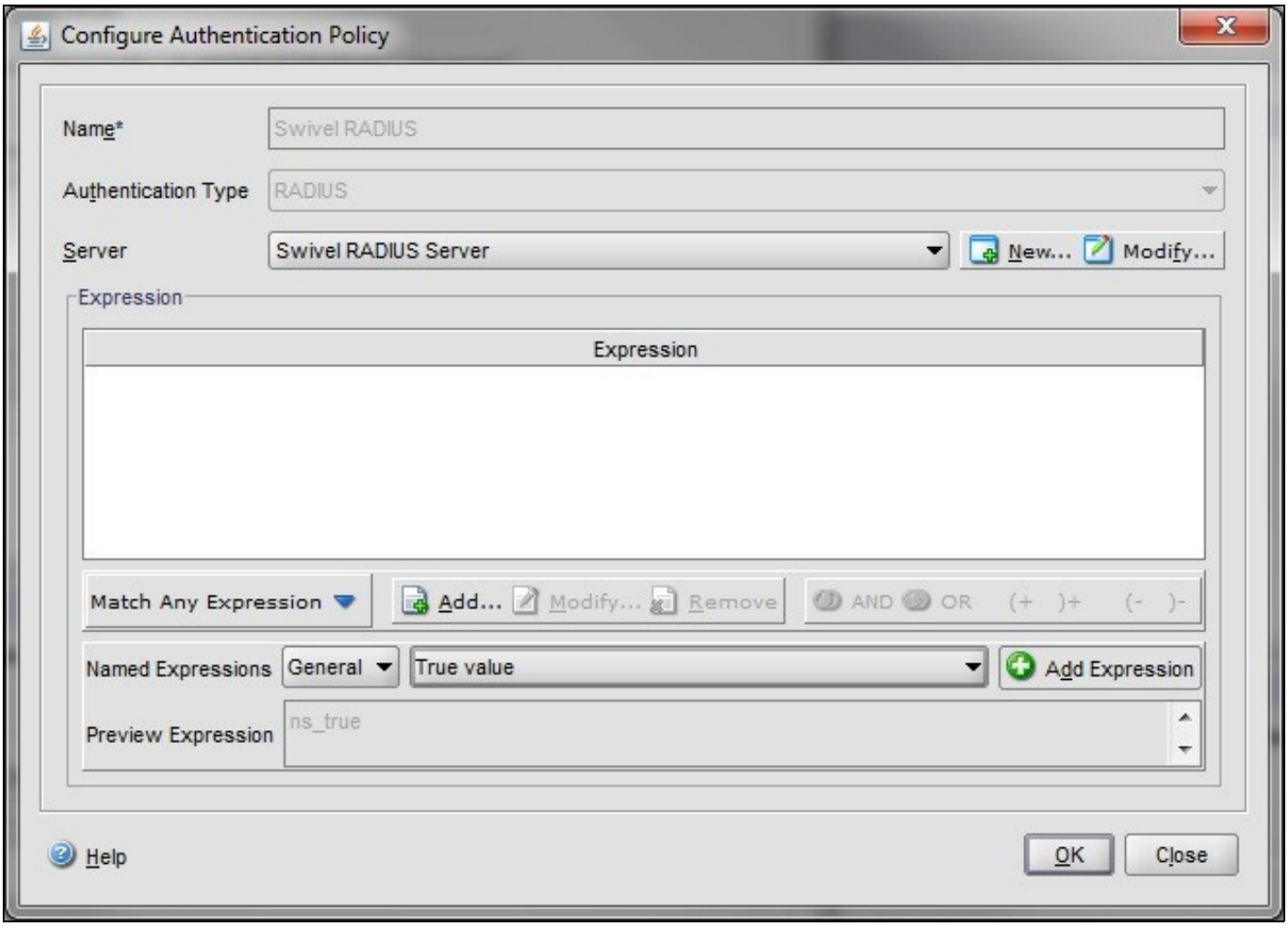
Name Swivel RADIUS Policy

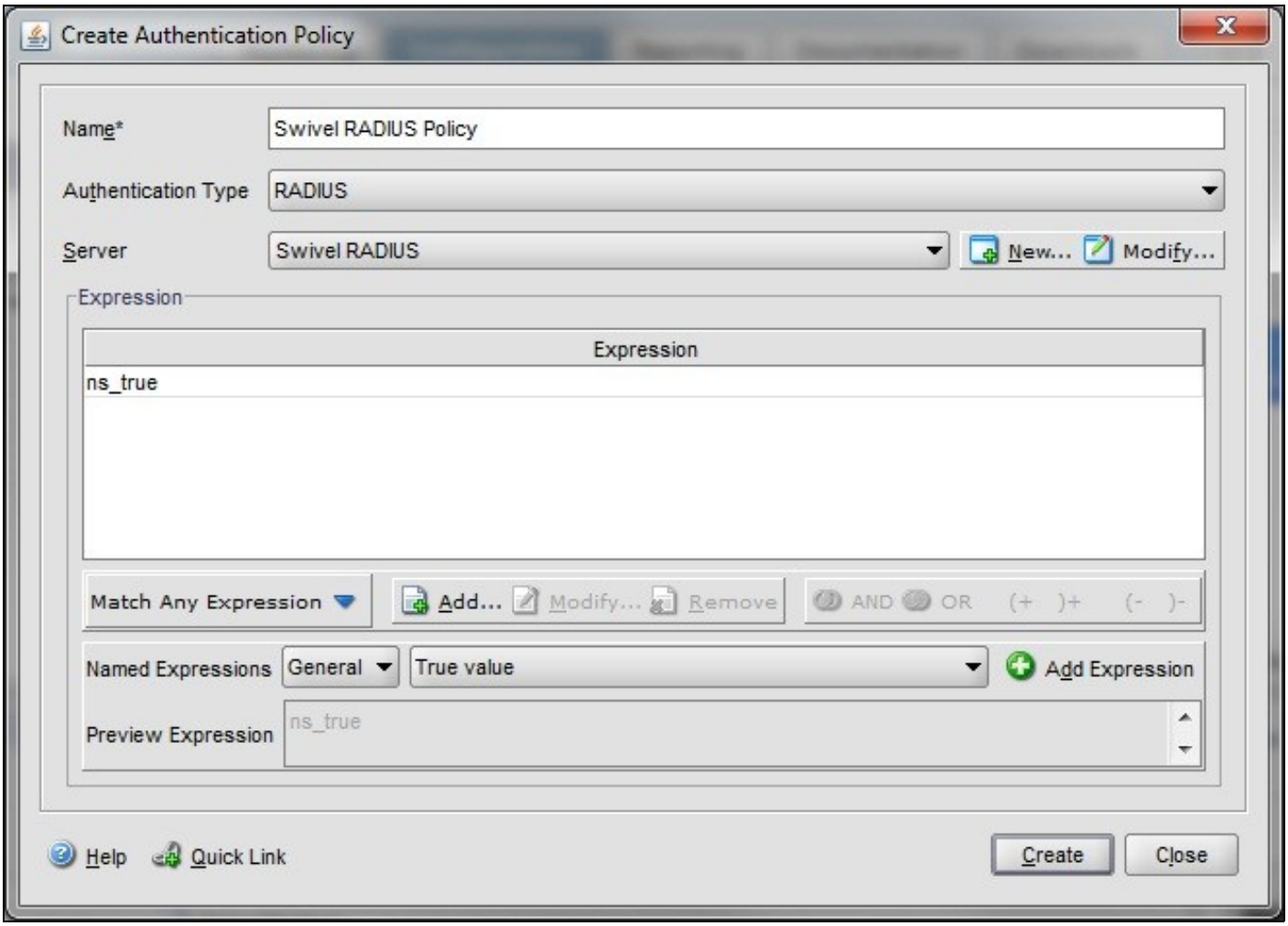
Authentication Type RADIUS

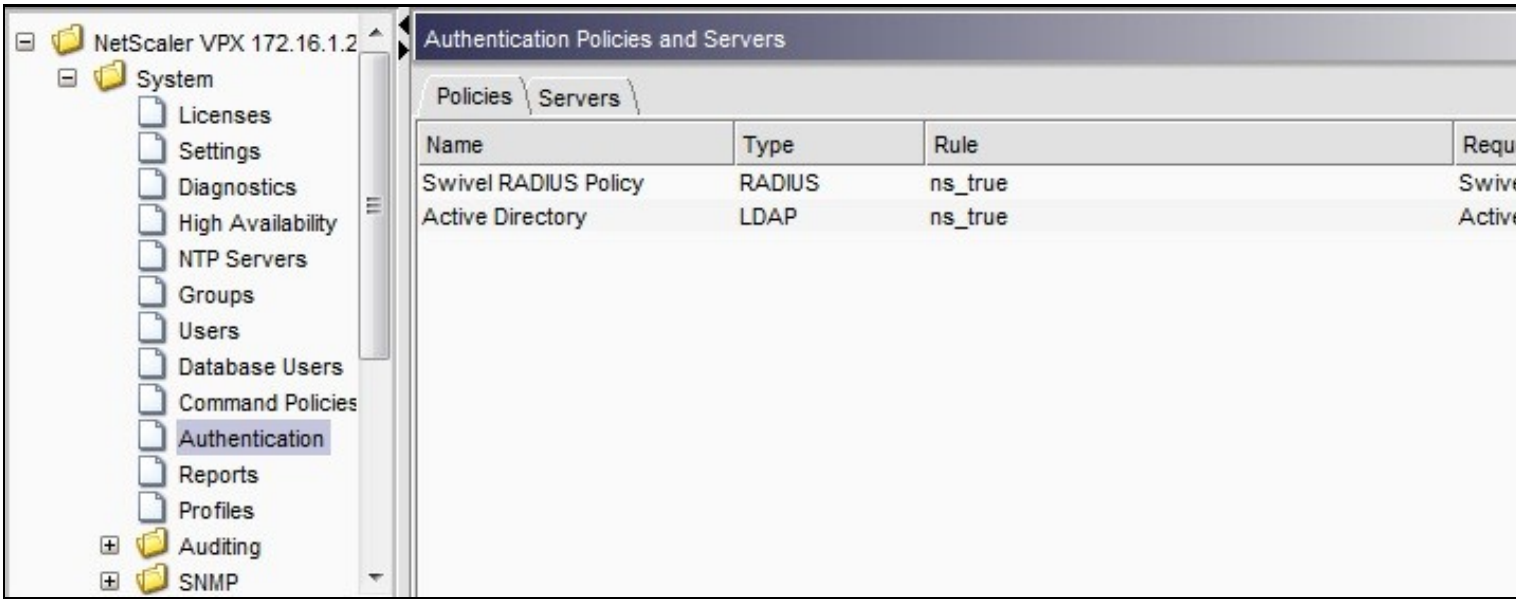
Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

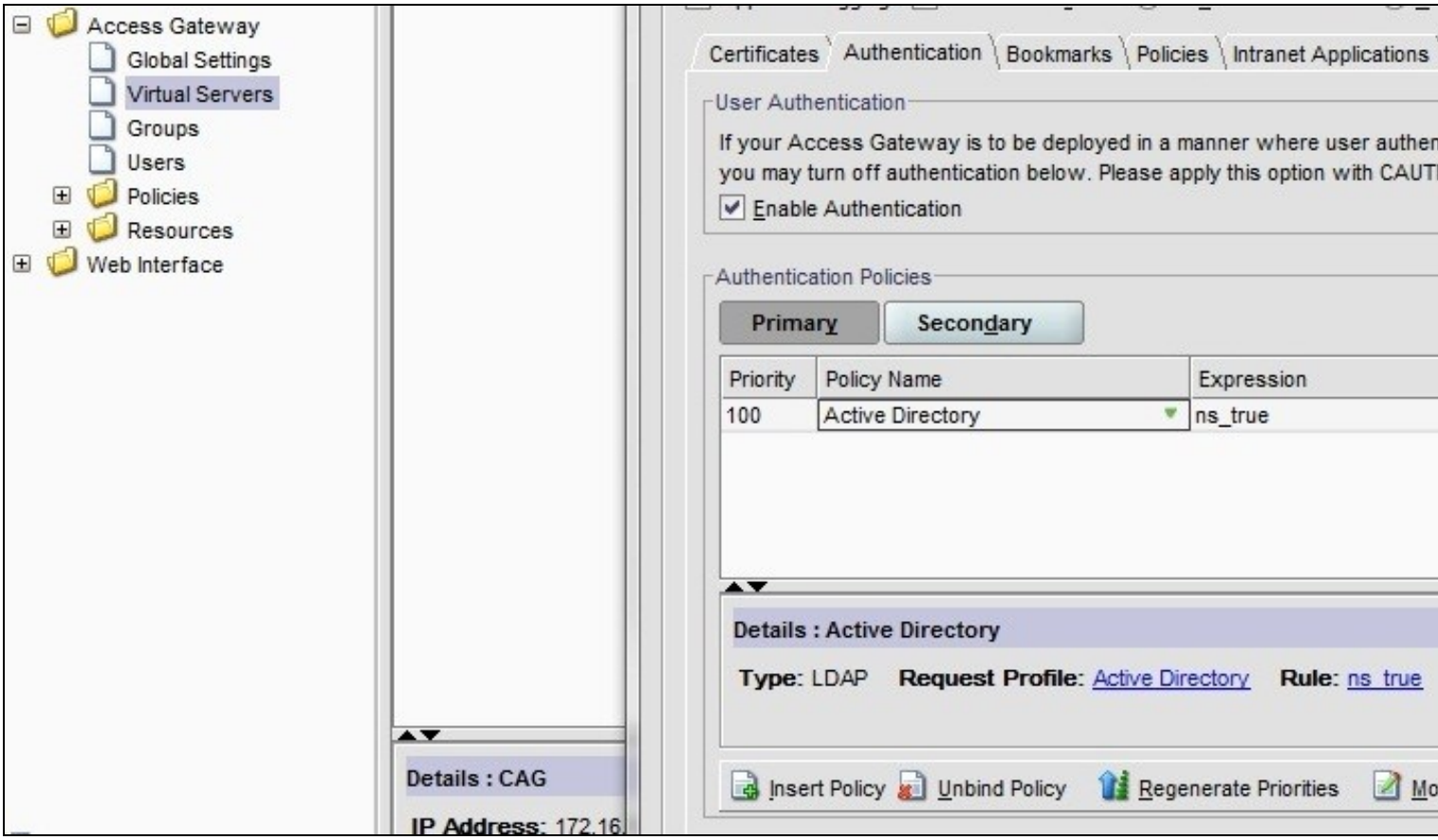


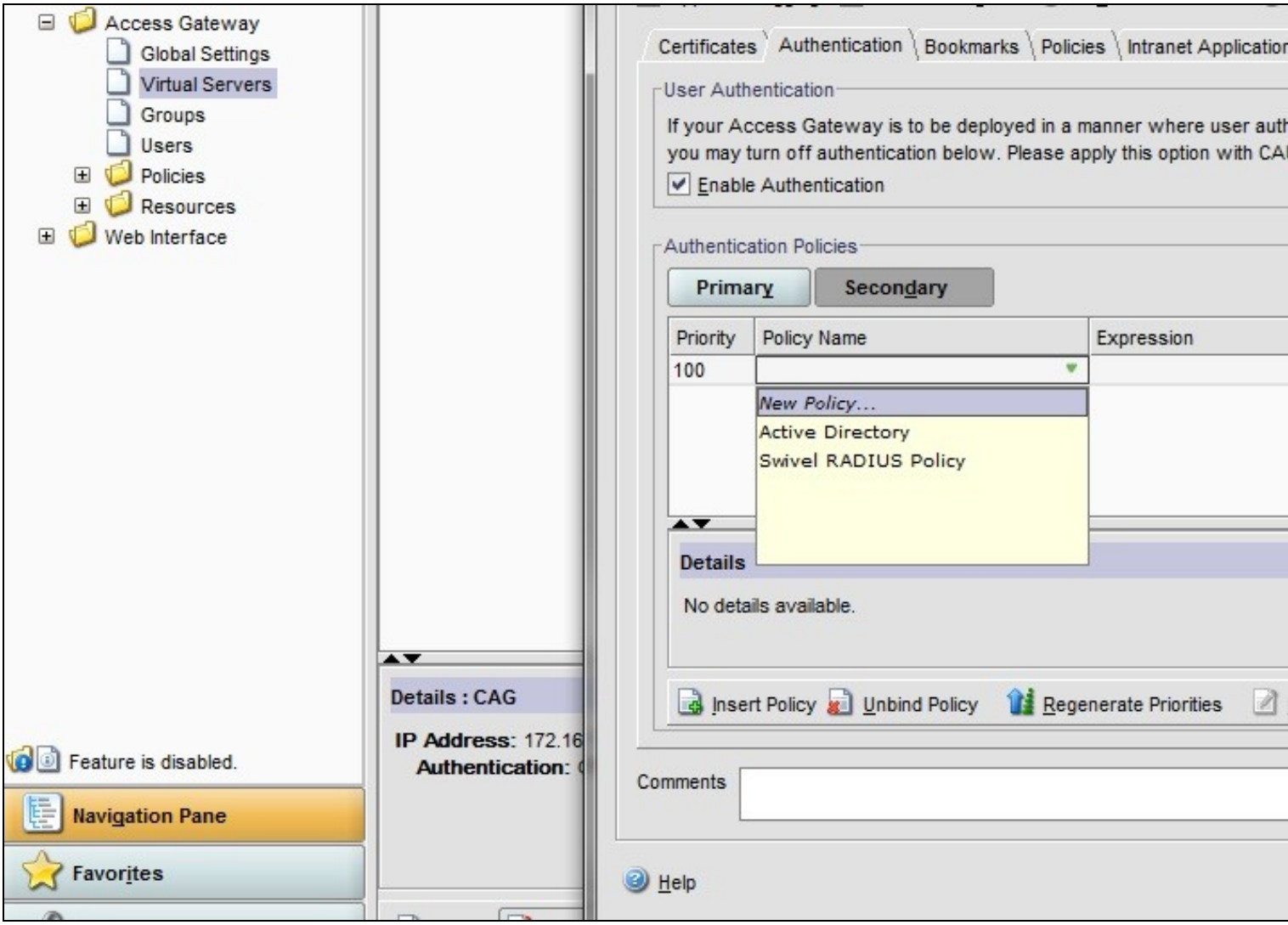

Configure Authentication Policy
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
Swivel RADIUS Server
New...
Modify...
Expression
Expression
Match Any Expression
Add...
Modify...
Remove
AND
OR
(+)+
(-)-
Named Expressions
General
True value
Add Expression
Preview Expression
ns_true
Help
OK
Close





The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.


Access Gateway
Global Settings
Virtual Servers
Groups
Users
Policies
Resources
Web Interface
Details : CAG
IP Address: 172.16
Certificates
Authentication
Bookmarks
Policies
Intranet Applications
User Authentication
If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUT
Enable Authentication
Authentication Policies
Primary
Secondary
Priority
Policy Name
Expression
100
Active Directory
ns_true
Details : Active Directory
Type: LDAP
Request Profile: Active Directory
Rule: ns_true
Insert Policy
Unbind Policy
Regenerate Priorities



110.2 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.

111 Additional Configuration Options

111.1 Login Page Customisation

The login page can be modified to display the TURing image, PINpad or String Index as outlined in the following sections.

111.1.1 Customisation Overview

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Winsdows based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
- Display Security String Index
- Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, the script /nsconfig/rc.netscaler copies at boot the required files from /var/mods to /netscaler/ns_gui.

111.1.2 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

111.1.3 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /netscaler/ns_gui/vpn
cp index.html index.html.bak
cd /netscaler/ns_gui/vpn/resources
mkdir bak
cp *.xml bak
```

111.1.4 Customise the login script

111.1.4.1 Requesting a TURing image

These files can be modified before uploading

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the Hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

111.1.5 Customise the login prompt

Modify the language resource files in /netscaler/ns_gui/vpn/resources. If you are only using the English language, then edit en.xml and search for

```
<String id="Password2">
```

this should be around line 59.

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password" with a value of "AD Password". You should therefore have 2 lines as follows:

```
<String id="Password">AD Password</String>
<String id="Password2">OTC:</String>
```

(Note that Password has no colon at the end, whereas Password2 has a colon).

111.1.5.1 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.

Edit the file rc.netscaler to copy across any modified language pages, as for English which is included in the script.:

```
cp /var/mods/en.xml.mod /netscaler/ns_gui/vpn/resources/en.xml
```

111.1.6 Upload files to Netscaler

Download the files under the prerequisites and copy them to the following locations:

index.html to /netscaler/ns_gui/vpn/index.html

pinsafe.js to /netscaler/ns_gui/vpn/pinsafe.js

rc.netscaler to /nsconfig/rc.netscaler

Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere regularly to prevent work in progress being lost during development. How to manage these pages is covered later.

111.1.7 Copy the modified files from run time to file storage

```
mkdir /var/mods
cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
cp /netscaler/ns_gui/vpn/resources/en.xml /var/mods/en.xml.mod
```

Also copy across any additional language files modified.

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle. At boot time the /nsconfig/rc.netscaler script copies /var/mods/ files back to /netscaler/ns_gui.

111.1.8 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time.

111.2 Additional Login Customisation options

111.2.1 Automated TURing Display

With the automated TURing display, when the user leaves the username field, the TURing will be automatically displayed. A login using the TURing image is expected for that user.

Edit the index.html file

```
search for onFocus="loginFieldCheck()"
```

Add a new attribute after this, as follows:

```
onBlur="showTuring()"
```

Example:

```
onFocus="loginFieldCheck()" onBlur="showTuring()" style="width:100%;"
```

111.2.2 Changing the button labels

If you want to want to change the button text such for sending security strings to SMS or email on-demand, rather than showing a TURing image, or change the GET Image text you may want to change the label of the button. You can do this as follows:

Edit the index.html file and locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

```
id="btnTuring" value="Get Image"
```

Change the value attribute to an appropriate alternative, such as "Send Message".

111.2.3 Requesting the string Index

See also Multiple Security Strings How To Guide

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/DCIndexImage?username=";
```

For a software only install see Software Only Installation

111.2.4 PINpad

Netscaler 93 PINpad is a version of the 9.3 customisation modified for Pinpad. Note that in order to use PINpad you will need a Swivel Appliance version 2.0.13 or higher. For earlier versions, you can get this from Downloads.

PINpad pre-req

111.2.5 Requesting an SMS

See also Challenge and Response below

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

111.3 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. RADIUS Challenge and Response can be optionally configured to enter a username and Password, which will then ask for a One Time Code. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

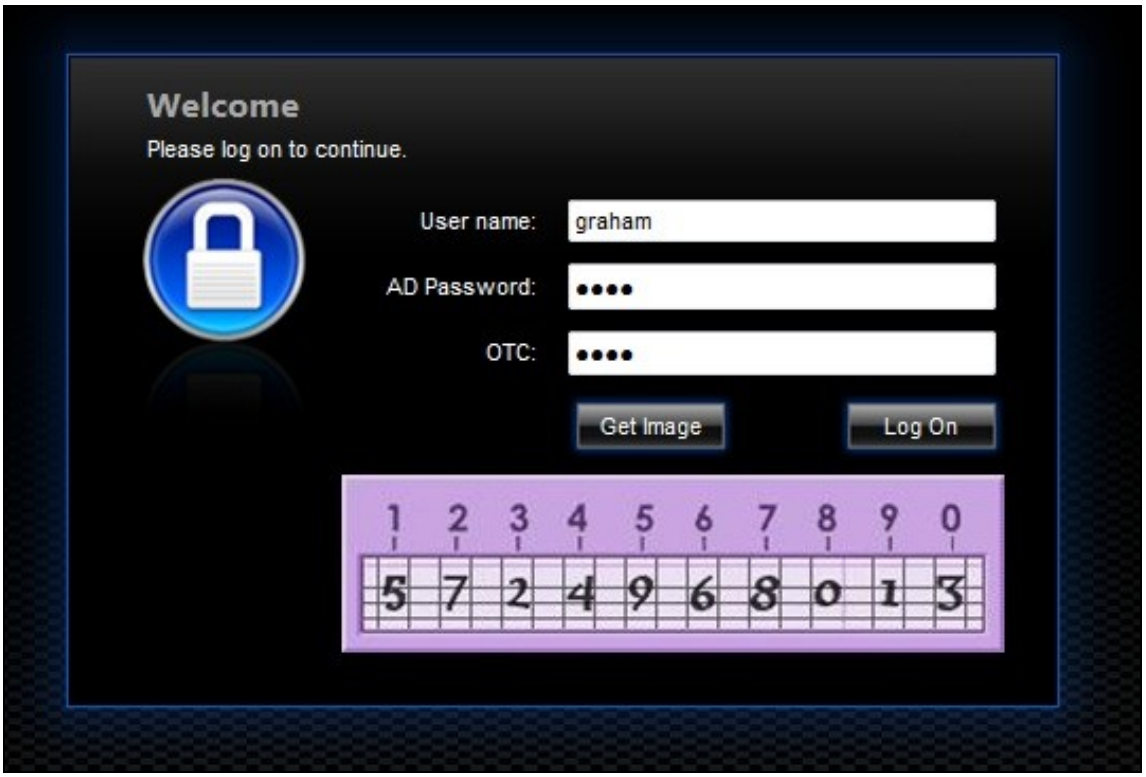
111.4 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

112 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.



For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

If the incorrect credentials are used then the login should fail

Where the TURing image is not used, then the Get Image page modification can be omitted

113 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

114 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

115 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see How To Modify Access Gateway Logon Fields

116 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

117 Citrix Access Gateway Enterprise Edition 8

117.1 Introduction

This document shows the steps required to integrate PINsafe with the Citrix Access Gateway Enterprise Edition (Formerly Netscaler VPN) version 8.x to 9.1. Version 9.2 is covered in a separate document see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring PINsafe to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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

117.2 Prerequisites

Access Gateway Enterprise Edition firmware version 8.x to 9.1.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

PINsafe 3.x

PINsafe server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the PINsafe server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or PINsafe files File:CAGEE_8_files.zip for versions 8 - 9.1

117.3 Baseline

PINsafe 3.5

Citrix Access Gateway Enterprise Edition 8.0. Also tested with 9.1.

117.4 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the PINsafe server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside if they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the pinsafe modifications.

118 Swivel Configuration

118.1 Configuring the RADIUS server

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

118.2 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.

118.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

118.3 Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the virtual or hardware appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the PINsafe server to be accessible from the internet, usually with a NAT. See also Multiple Security Strings How To Guide

118.3.1 Login Page Customisation

SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

Navigate to the location of the pages to be modified, and make a local backup copy of them

```
>cd /netscaler/ns_gui/vpn
>cp index.html index.html.bak
>cp login.js login.js.bak
```

Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere reguarlarly to prevent work in progress being lost during development. How to manage these pages is covered later.

The index.html file now needs to be edited (or replaced). The tool vi can be used to do this but an application such as WinSCP will make this easier. The required files can be found in the prerequisites.

A pinsafe.js file that is a modification of the existing login.js file is required. Make a copy of login.js called pinsafe.js The showTuring function shown below needs to be added to this file. Note the sUrl setting needs to be changed to reflect the IP address and port number of the relevant PINsafe server. There are other changes that can be made, eg changing the prompt to read One-Time code instead of password.

For a virtual or hardware appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, a script must be created that runs at startup to copy the modified files back to this location. The nsafter.sh or rc.netscaler shell scripts can be created or modified to accomplish this. For example via ssh:

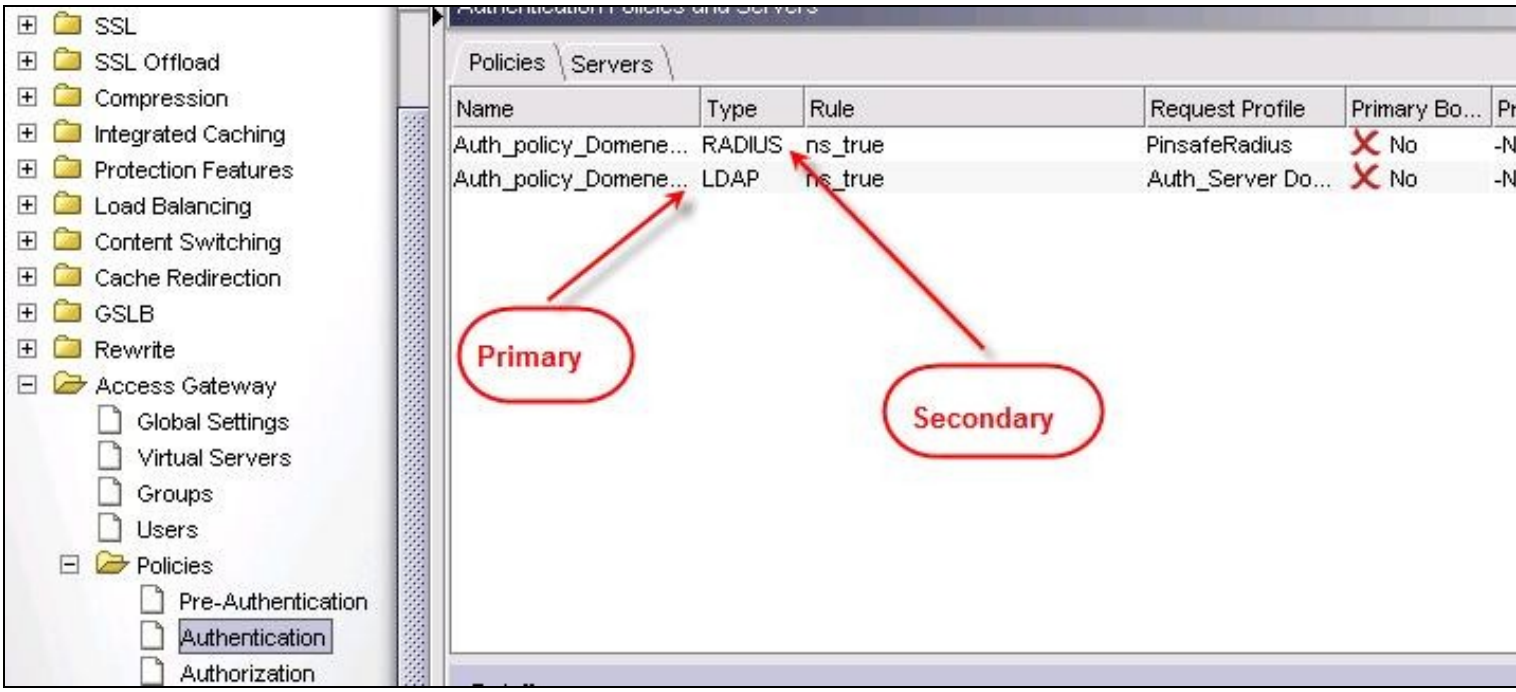
```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod /netscaler/ns_gui/vpn/pinsafe.js >> /nsconfig/rc.netscaler
```

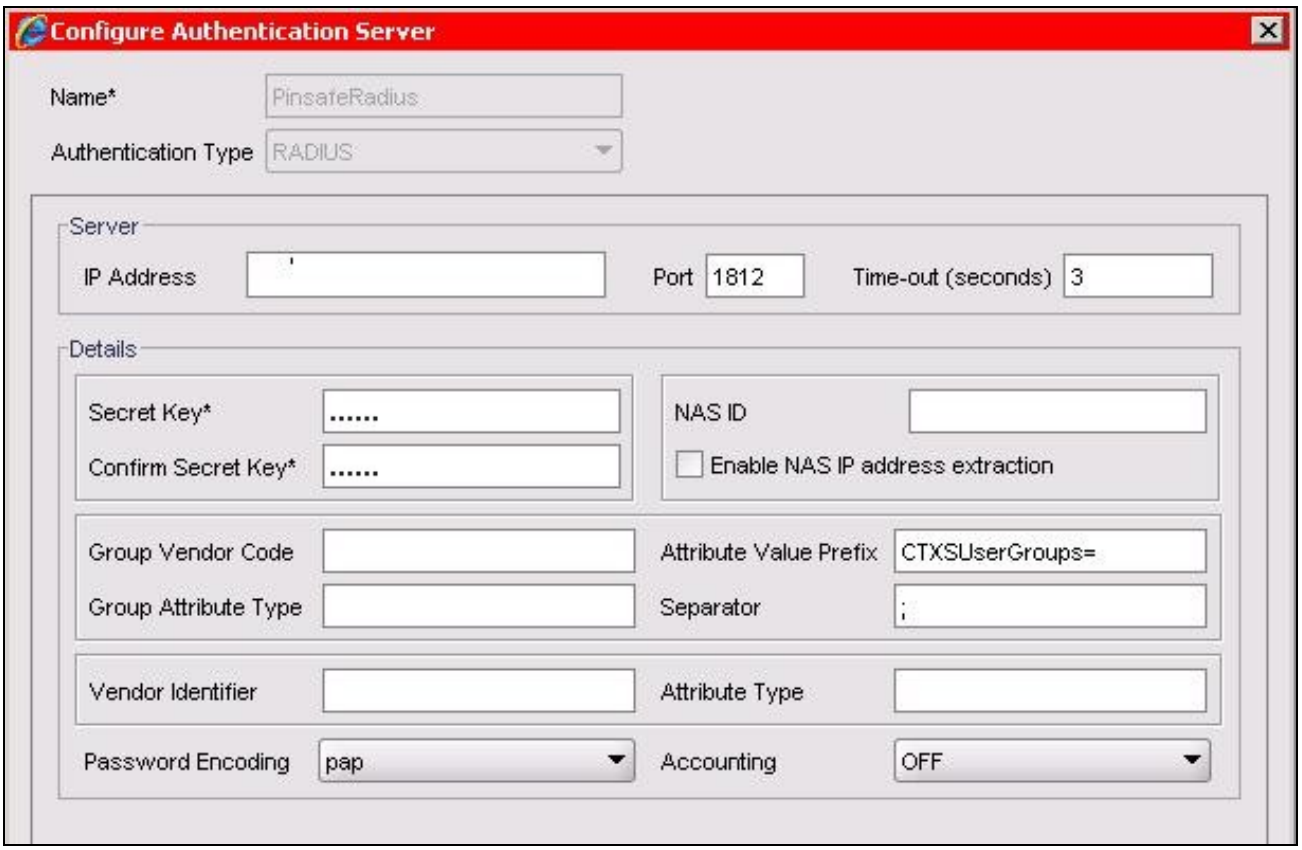
118.3.2 Citrix Advanced Access Gateway Enterprise Edition RADIUS Cofiguration

The CAGEE needs to be configured to use the PINsafe server as a RADIUS authentication server. Where a VIP is being used on the PINsafe server then configure the RADIUS request to be made against each of the PINsafe servers together with the use of Session Sharing.

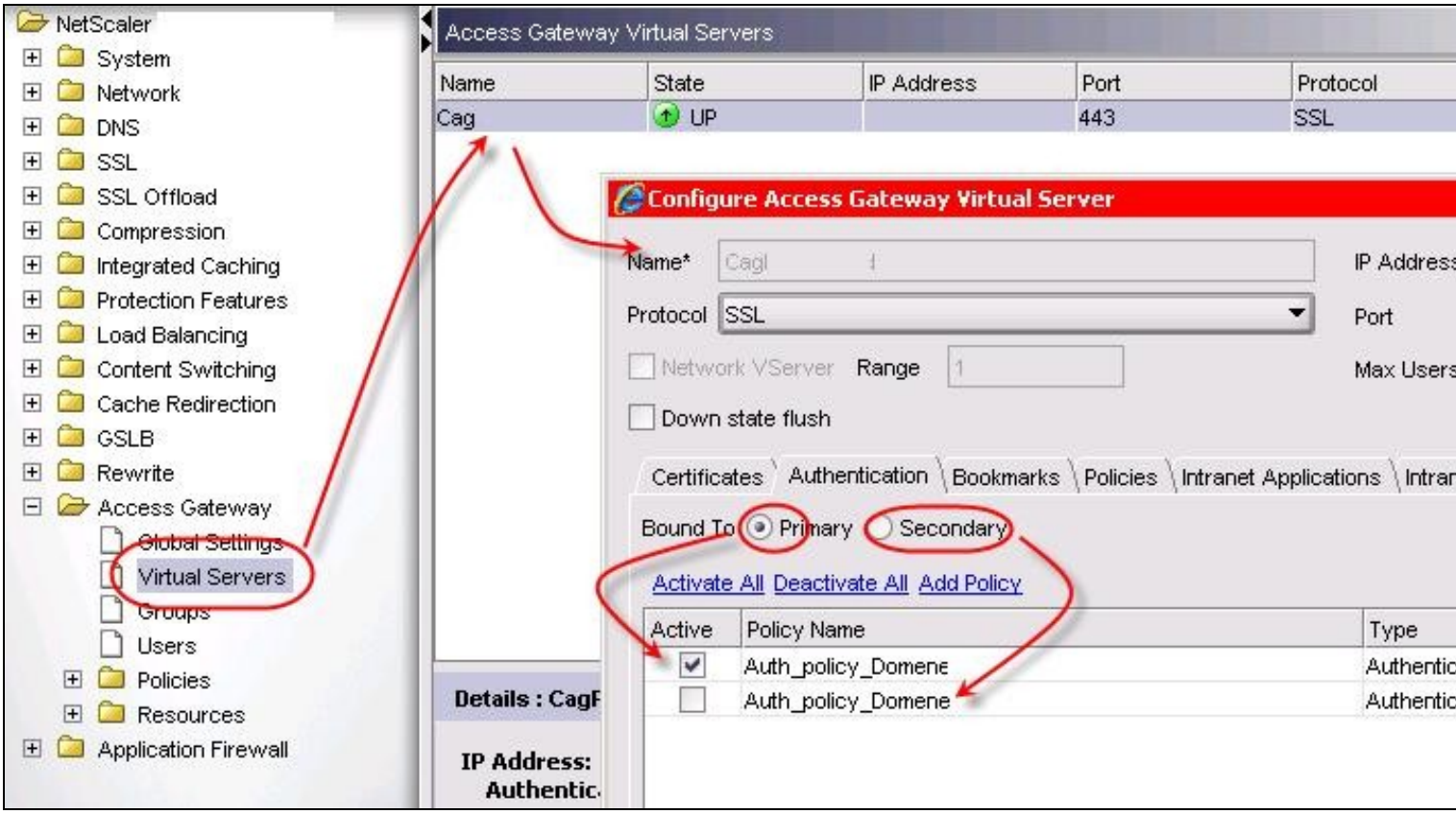
PINsafe can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Create a new Authentication policy (under the Netscaler->System->Authentication menu). The policy must specify RADIUS and then the PINsafe server must be added as a RADIUS server.





On the SSL-> Virtual Server menu, the created policy must be activated. If just PINsafe authentication is required then you ensure that only the PINsafe policy is active. If you require AD and PINsafe authentication then you need to make active the PINsafe policy as the secondary. Save the settings.



118.4 Additional Configuration Options

118.4.1 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.1 supports RADIUS Challenge and Response

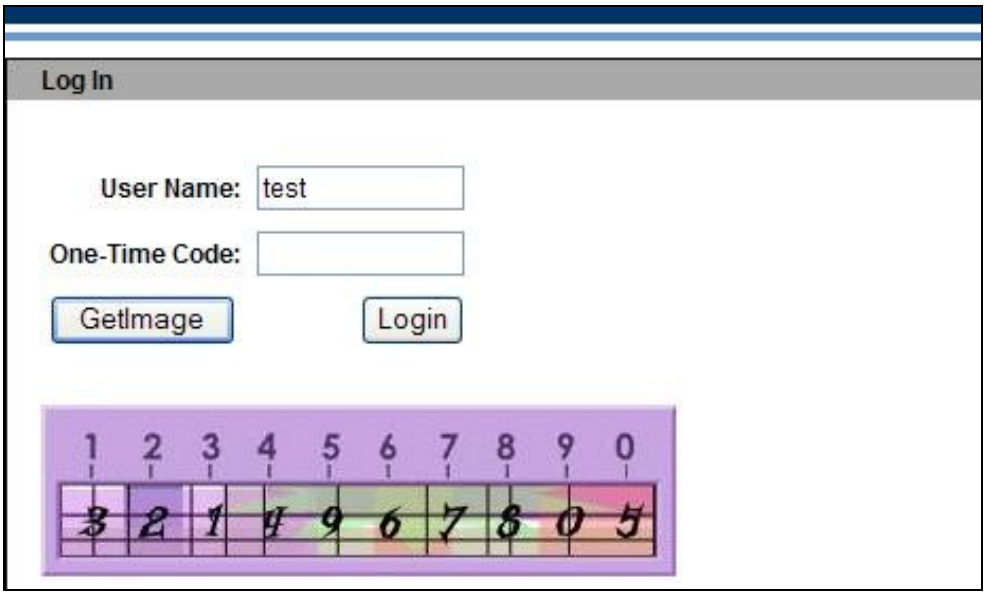
118.4.2 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required.

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

118.5 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.



118.6 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Image from PINsafe server absent

118.7 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

118.8 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

119 Citrix Access Gateway Enterprise Edition 9

119.1 Introduction

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 9.2 and 9.3 (Formerly Netscaler VPN). for versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

119.2 Prerequisites

Access Gateway Enterprise Edition firmware version 9.2 or 9.3

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or Swivel files for version 9.2 or version 9.3.

119.3 Baseline

Swivel 3.5

Citrix Access Gateway Enterprise Edition Version 9.2

and also Swivel 3.8

Citrix Access Gateway Enterprise Edition Version 9.3

119.4 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

120 Swivel Configuration

120.1 Configuring the RADIUS server

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

120.2 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.

120.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

120.3 Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the virtual or hardware appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. If the single Channel TURing image is not to be used, then the login page does not need to be modified, unless other functions are required such as the Get Security String Index. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the Swivel server to be accessible from the internet, usually with a NAT.

120.3.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where a VIP is being used on the Swivel server then configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing.

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS

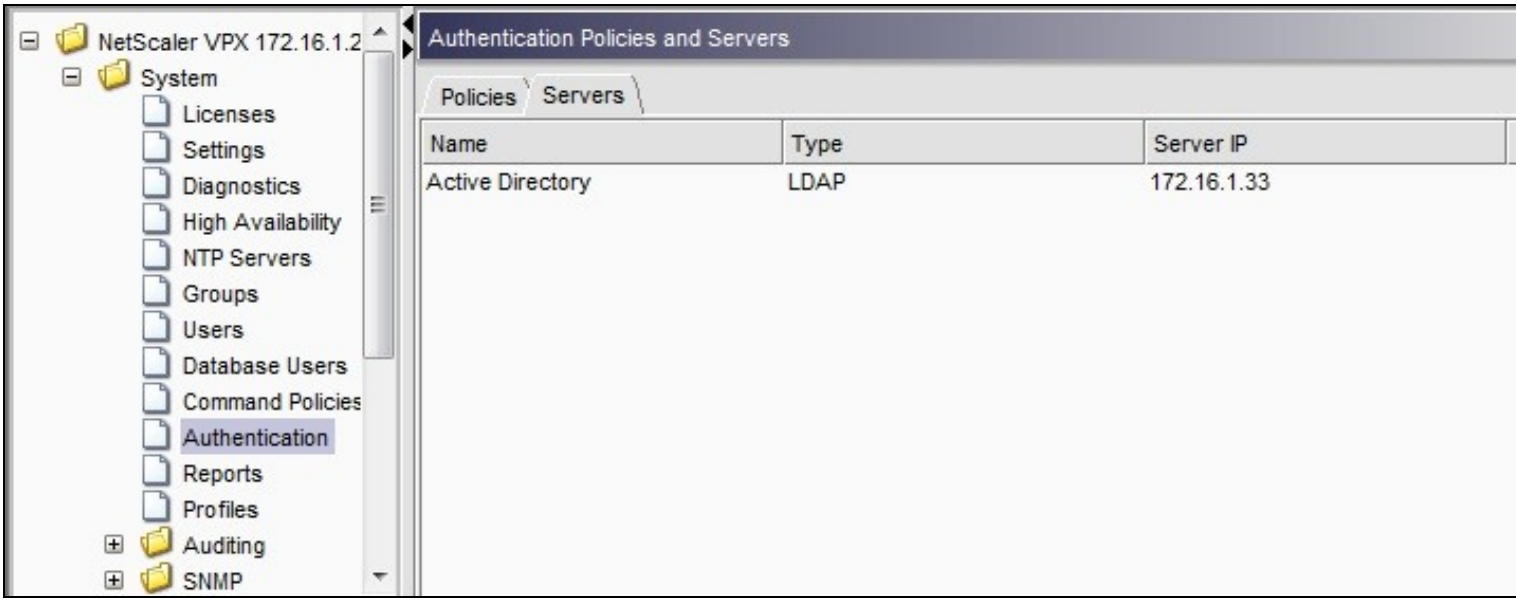
Authentication type RADIUS

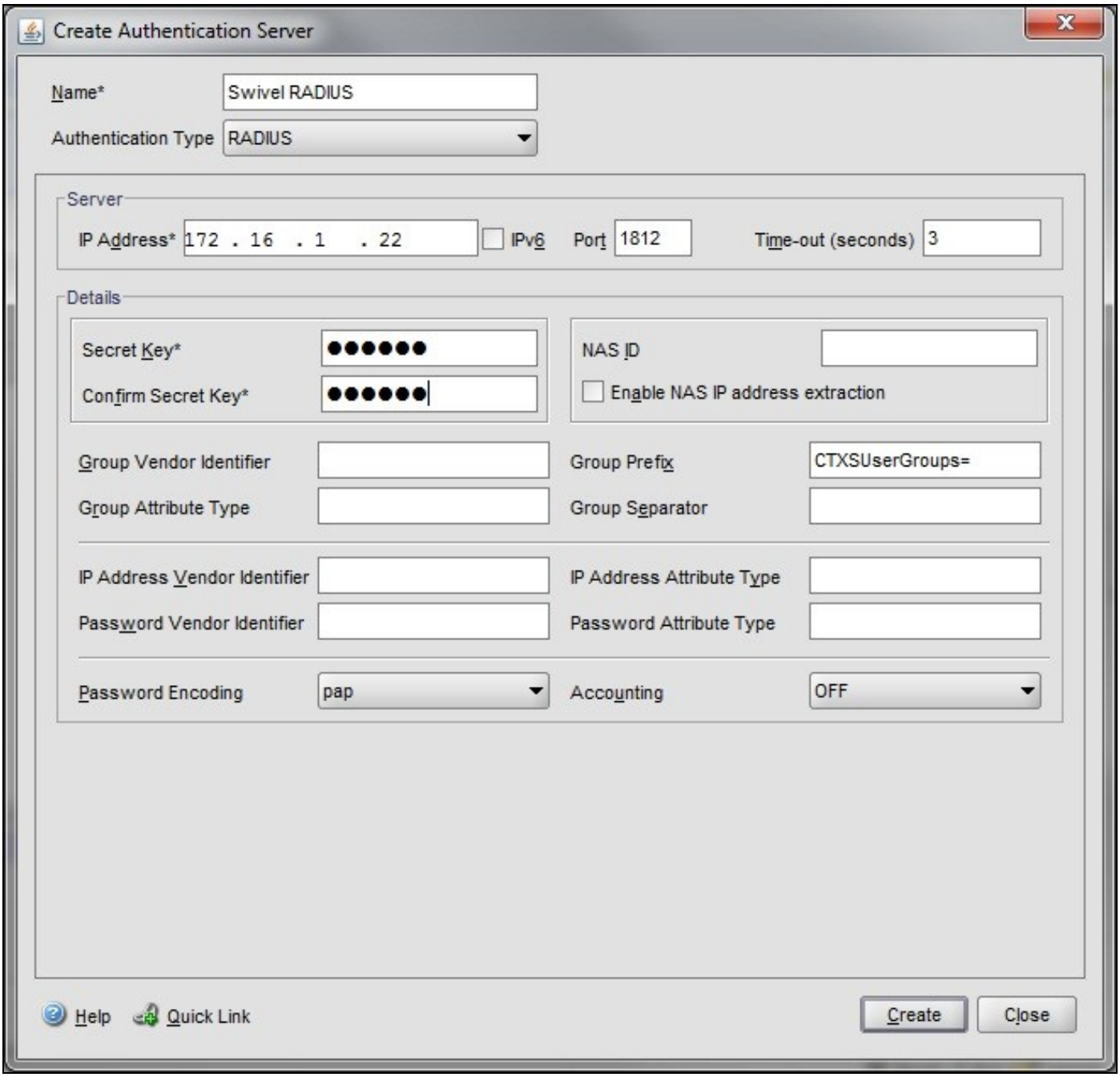
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

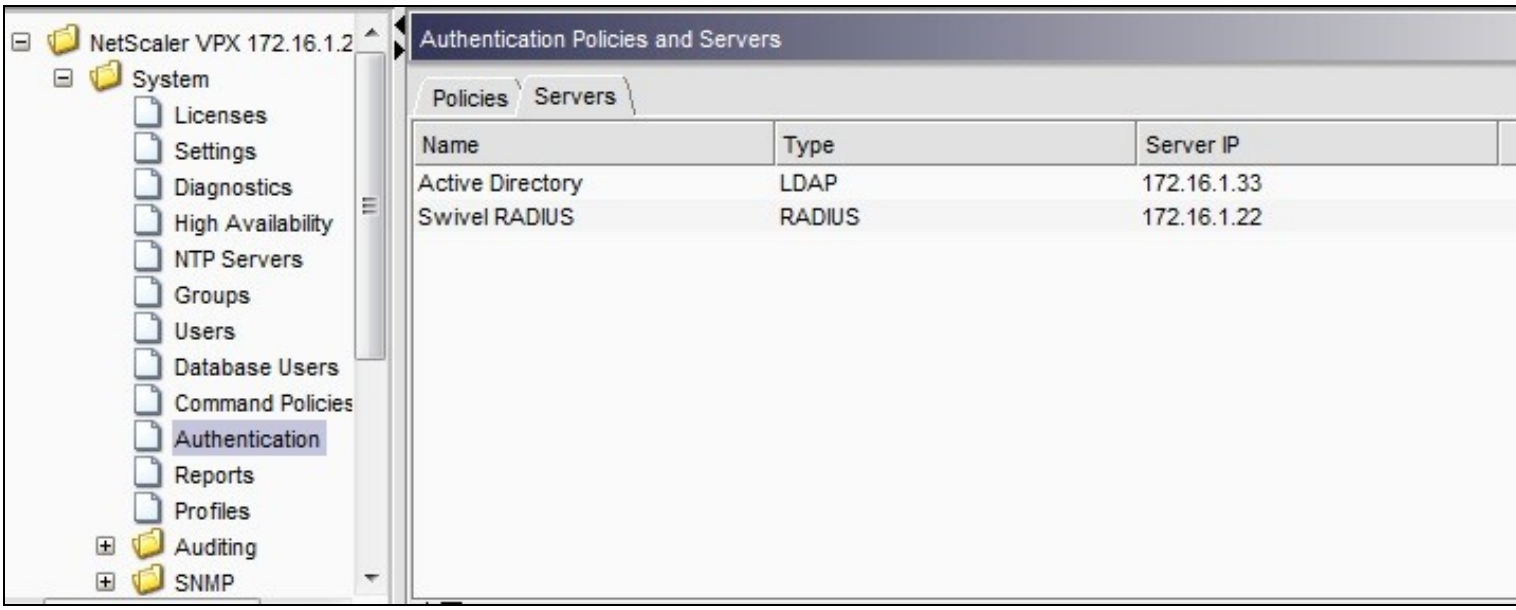
Group Prefix CTXSUserGroups=

Group Separator ;

When complete click on Create.




Create Authentication Server
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
IP Address*
172 . 16 . 1 . 22
IPv6
Port
1812
Time-out (seconds)
3
Details
Secret Key*
Confirm Secret Key*
NAS ID
Enable NAS IP address extraction
Group Vendor Identifier
Group Prefix
CTXSUserGroups=
Group Attribute Type
Group Separator
IP Address Vendor Identifier
IP Address Attribute Type
Password Vendor Identifier
Password Attribute Type
Password Encoding
pap
Accounting
OFF
Help
Quick Link
Create
Close



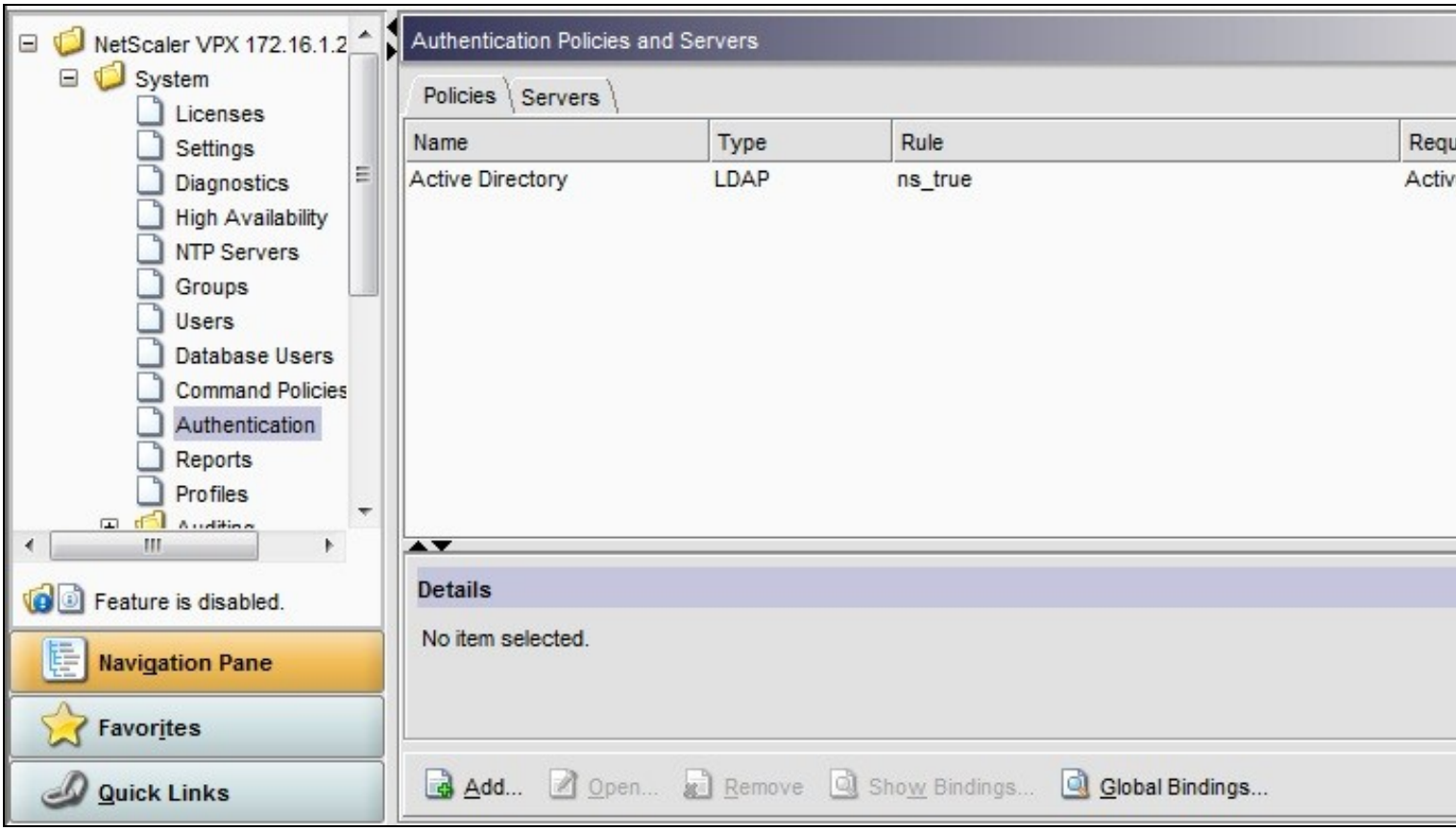
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

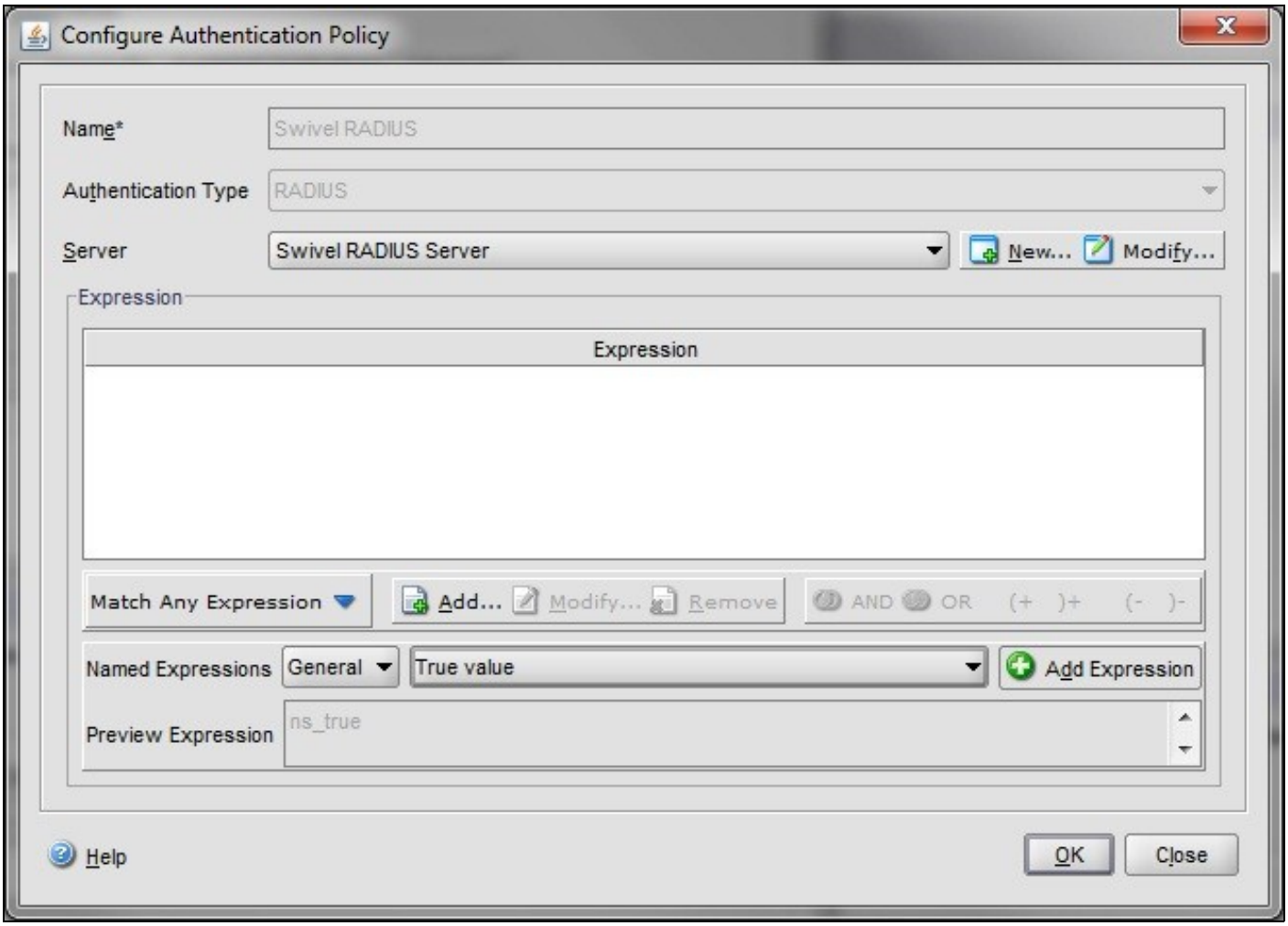
Name Swivel RADIUS Policy

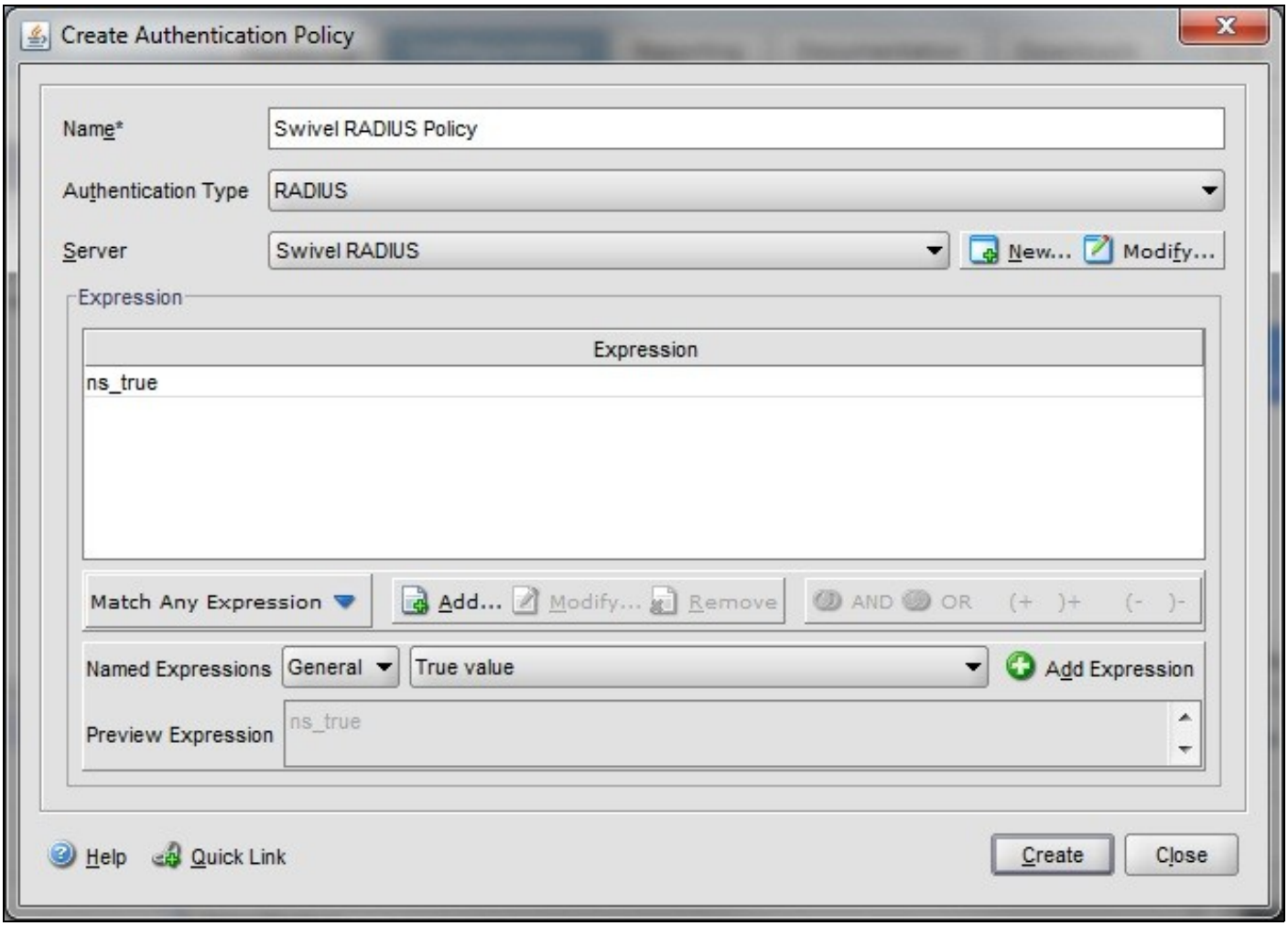
Authentication Type RADIUS

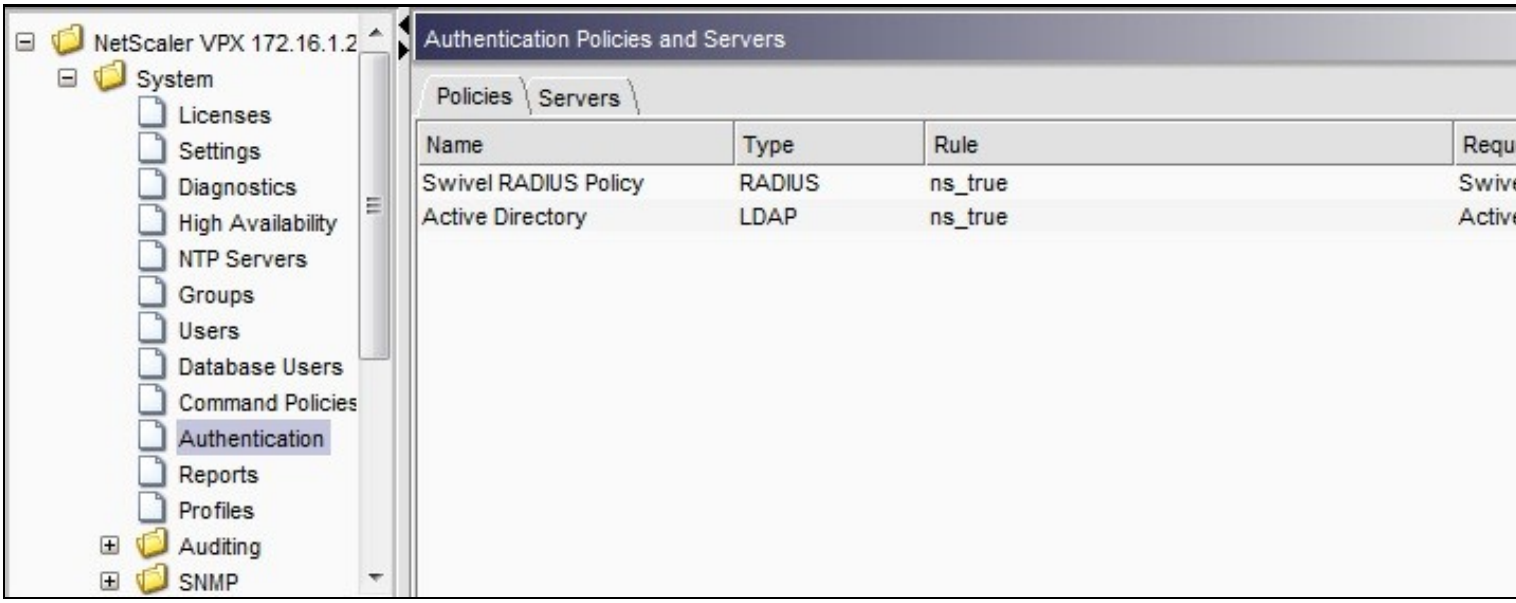
Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

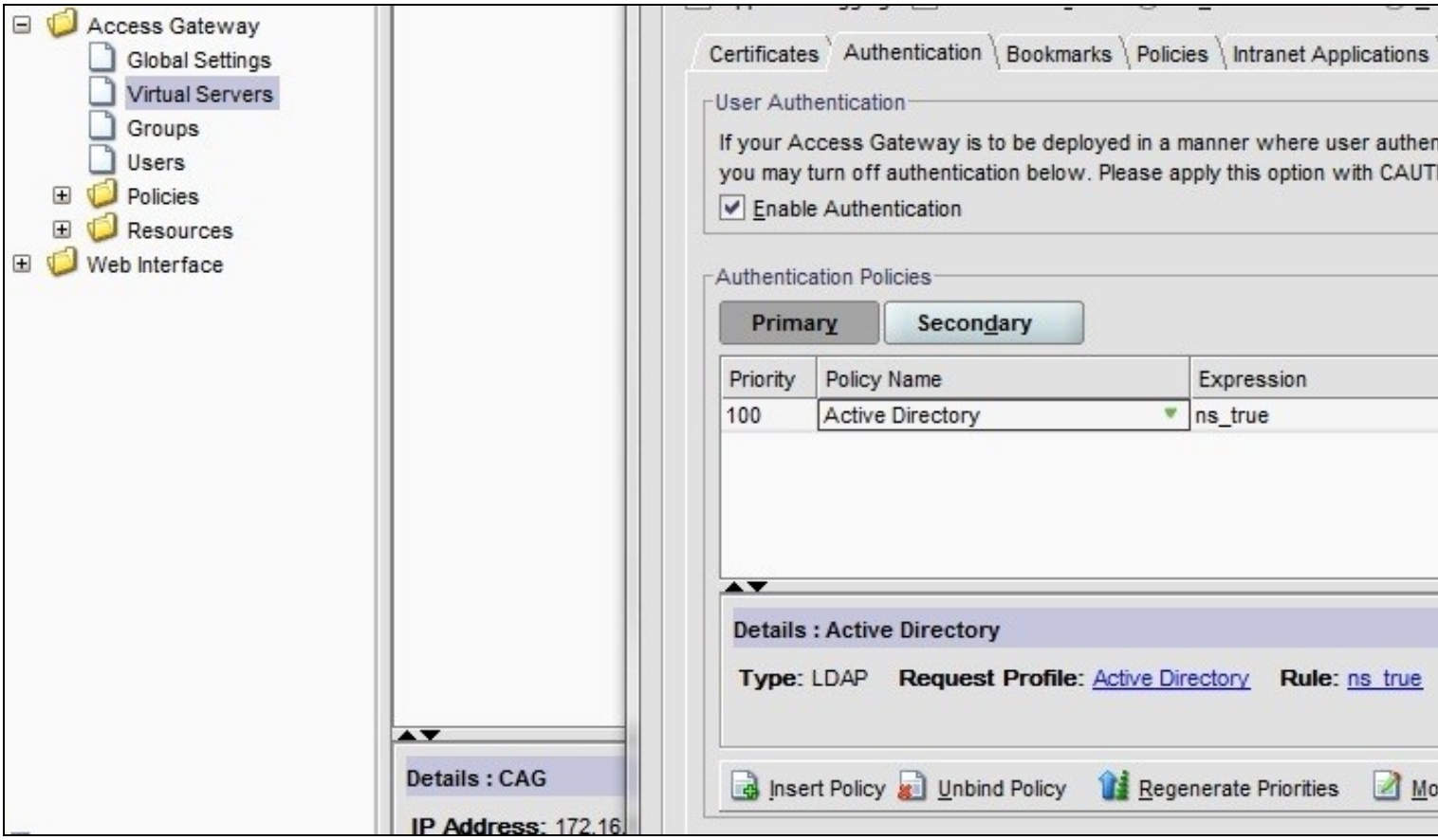


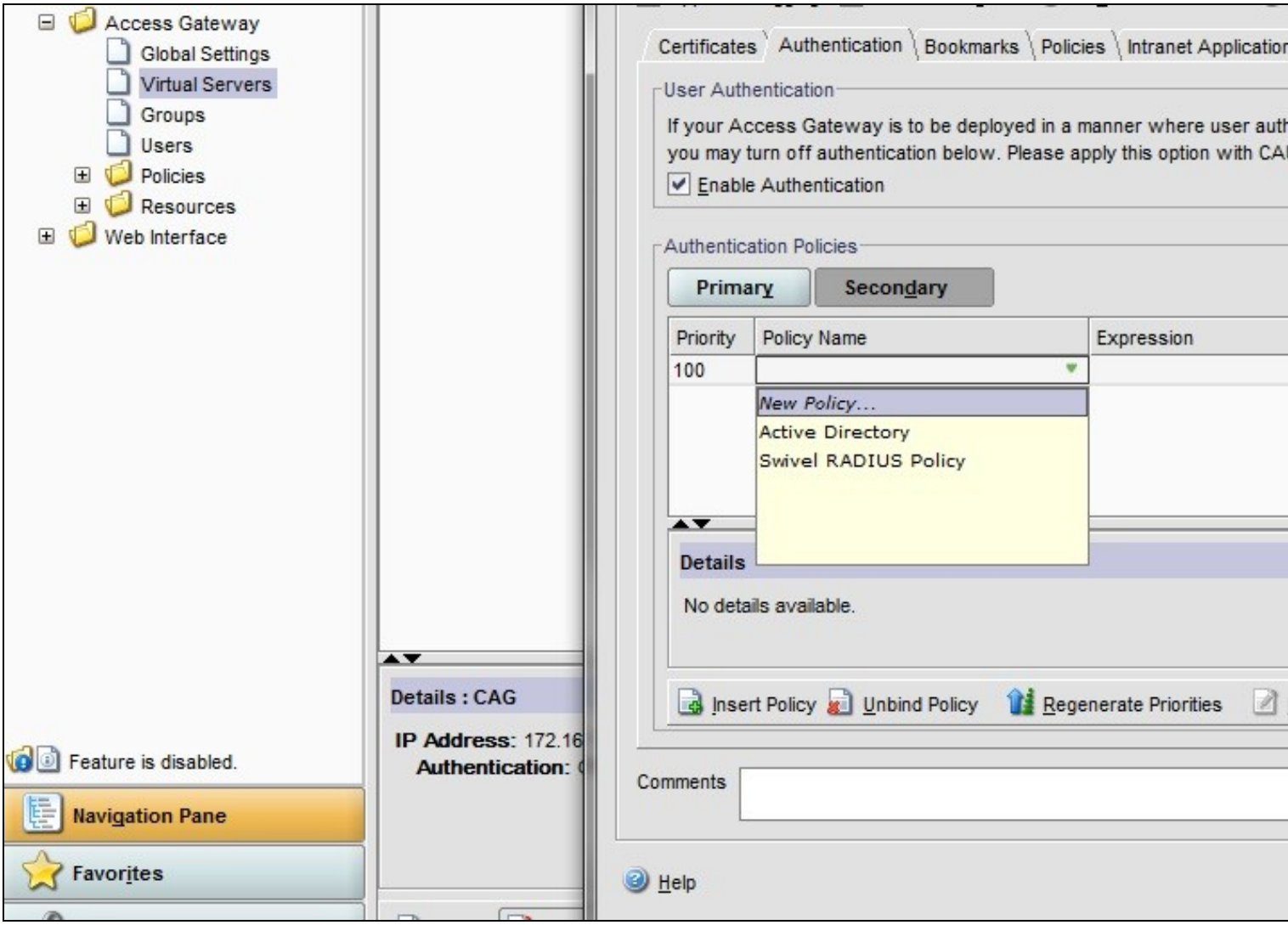

Configure Authentication Policy
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
Swivel RADIUS Server
New...
Modify...
Expression
Expression
Match Any Expression
Add...
Modify...
Remove
AND
OR
(+)+
(-)-
Named Expressions
General
True value
Add Expression
Preview Expression
ns_true
Help
OK
Close





The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.


Access Gateway
Global Settings
Virtual Servers
Groups
Users
Policies
Resources
Web Interface
Details : CAG
IP Address: 172.16
Certificates
Authentication
Bookmarks
Policies
Intranet Applications
User Authentication
If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUT
Enable Authentication
Authentication Policies
Primary
Secondary
Priority
Policy Name
Expression
100
Active Directory
ns_true
Details : Active Directory
Type: LDAP
Request Profile: Active Directory
Rule: ns_true
Insert Policy
Unbind Policy
Regenerate Priorities



120.4 Additional Configuration Options

120.4.1 Login Page Customisation

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
- Display Security String Index
- Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle we create a script that copies at boot the required files from /var/mods.

See under prerequisites for the modified files that need to be uploaded to the Netscaler.

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

Navigate to the location of the pages to be modified, and make a local backup copy of them

```
>cd /netscaler/ns_gui/vpn
>cp index.html index.html.bak
>cp login.js login.js.bak
```

In version 9.2 and 10.x, you will also need to modify any resource language files you use. After the above commands, do the following:

```
>cd resources
>mkdir bak
>cp *.xml bak
```

Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere regularly to prevent work in progress being lost during development. How to manage these pages is covered later.

120.4.1.1 index.html

The index.html file now needs to be edited (or replaced). The tool vi can be used to do this but an application such as WinSCP will make this easier. The required files can be found in the prerequisites.

Normally, you can use the index.html file as it is, but there are two possible modifications you may want to consider.

Currently, the TURing image is only shown (or security string sent) when you click on the appropriate button. You may prefer that this happens as soon as the username is entered. To do this, you need to add an attribute to the username field, as follows:

Firstly, find the field. If you search for "loginFieldCheck", you should locate the following:

```
onFocus="loginFieldCheck()"
```

Add a new attribute after this, as follows:

```
onBlur="showTuring()"
```

Make sure that you leave a space before and after the new attribute.

If you want to want to send security strings to SMS or email on-demand, rather than showing a TURing image, you may want to change the label of the button. You can do this as follows:

First, locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

```
id="btnTuring" value="Get Image"
```

Change the value attribute to an appropriate alternative, such as "Send Message".

120.4.1.2 pinsafe.js

A pinsafe.js file that is a modification of the existing login.js file is required. Make a copy of login.js called pinsafe.js The sUrl setting needs to be changed to reflect the IP address and port number of the relevant Swivel server.

For a virtual or hardware appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

To request a security string on demand, instead of a TURing image, replace SCImage with DCMessage, for example:

```
sUrl="https://IP_address:8443/proxy/DCMessage?username=";
```

Note that using message on demand will display a "CONFIRMED" image instead of a TURing image. If you prefer not to have this visual confirmation, remove the following line which you will find a little lower down:

```
varImg.style.visibility = "visible";
```

120.4.1.3 Language resource files

Modify the language resource files, which can be found in the resources sub-folder of the vpn folder. If you are only using the English language, then edit en.xml and search for

```
<String id="Password2">
```

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password1" with a value of "AD Password". You should therefore have 2 lines as follows:

```
<String id="Password1">AD Password</String>
<String id="Password2">OTC:</String>
```

(Note that Password1 has no colon at the end, whereas Password2 has a colon).

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, a script must be created that runs at startup to copy the modified files back to this location. The nsafter.sh or rc.netscaler shell scripts can be created or modified to accomplish this. For example via ssh:

```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod /netscaler/ns_gui/vpn/pinsafe.js >> /nsconfig/rc.netscaler
# cp /netscaler/ns_gui/vpn/resources/en.xml /var/mods/en.xml.mod
# echo cp /var/mods/en.xml.mod /netscaler/ns_gui/vpn/resources/en.xml >> /nsconfig/rc.netscaler
```

120.4.1.4 PINpad

This is a version of the 9.3 customisation modified for Pinpad. Currently in beta testing. Note that in order to use PINpad you will need a Swivel virtual or hardware Appliance with the latest proxy application installed. You can get this from here.

PINpad pre-req

120.4.2 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

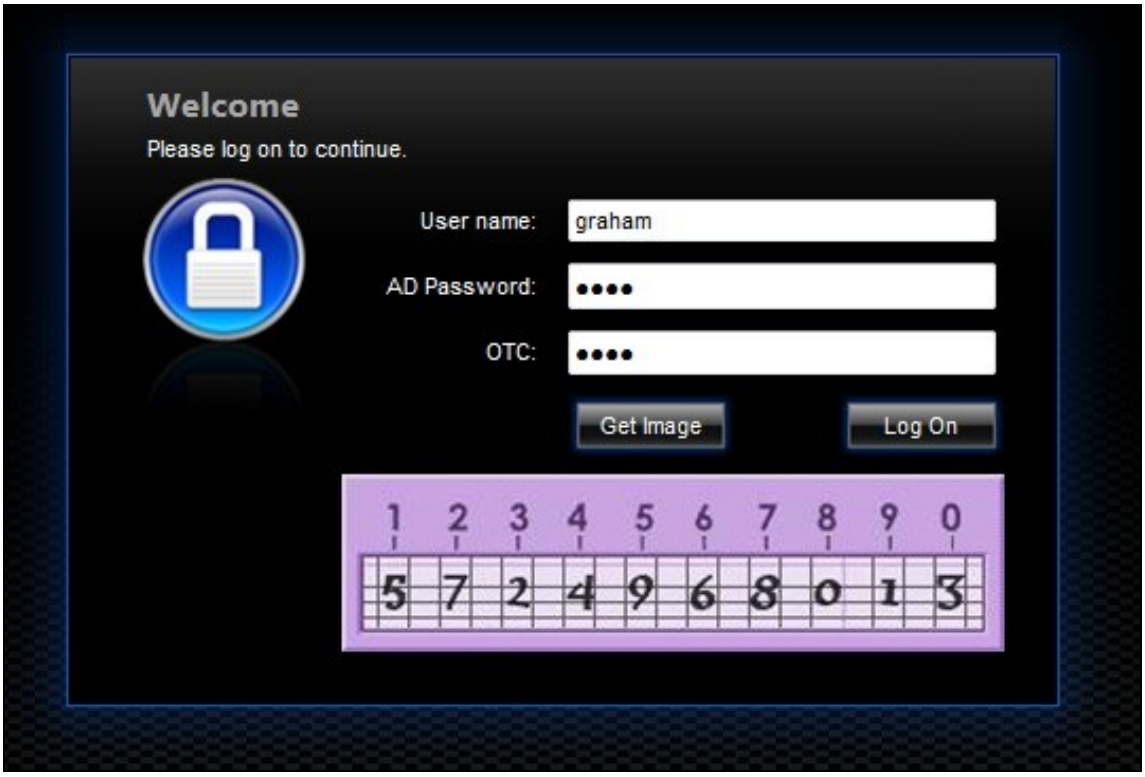
120.4.3 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

120.5 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.



For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

If the incorrect credentials are used then the login should fail

Where the TURing image is not used, then the Get Image page modification can be omitted

120.6 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

120.7 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

120.8 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

120.9 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

121 Citrix Access Gateway Standard 4.x

122 Introduction

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, PINsafe Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x

123 Prerequisites

Swivel 3.x

Citrix Access Gateway 4.x

124 Baseline

125 Architecture

Authentications are made against Swivel using RADIUS.

126 Installation

127 Swivel Configuration

127.1 Configuring the RADIUS server

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

127.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

127.3 Citrix Access Gateway Standard Edition Integration

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

128 Additional Information

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

129 Citrix Access Gateway Standard 5.x

130 Introduction

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, Swivel Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the following options are available:

- Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x
- Proxy the login request to a Web Interface login Citrix Access Gateway Web Interface Proxy

131 Prerequisites

Swivel 3.x

Citrix Access Gateway 5.x

132 Baseline

PINsafe 3.8

CAG Standard 5.0.3

133 Architecture

Authentications are made against Swivel using RADIUS.

134 Installation

135 Swivel Configuration

135.1 Configuring the RADIUS server

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

135.2 Setting up PINsafe Dual Channel Transports

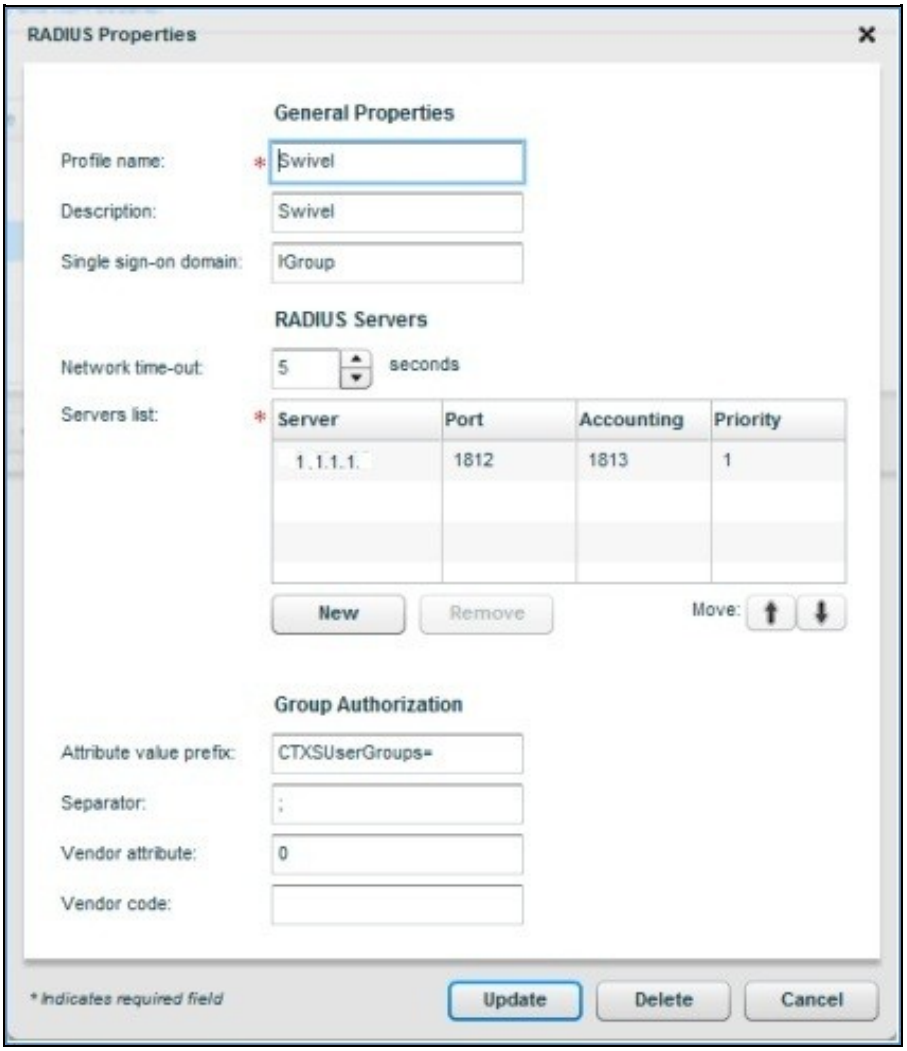
See Transport Configuration

136 Citrix Access Gateway Standard Edition Integration

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

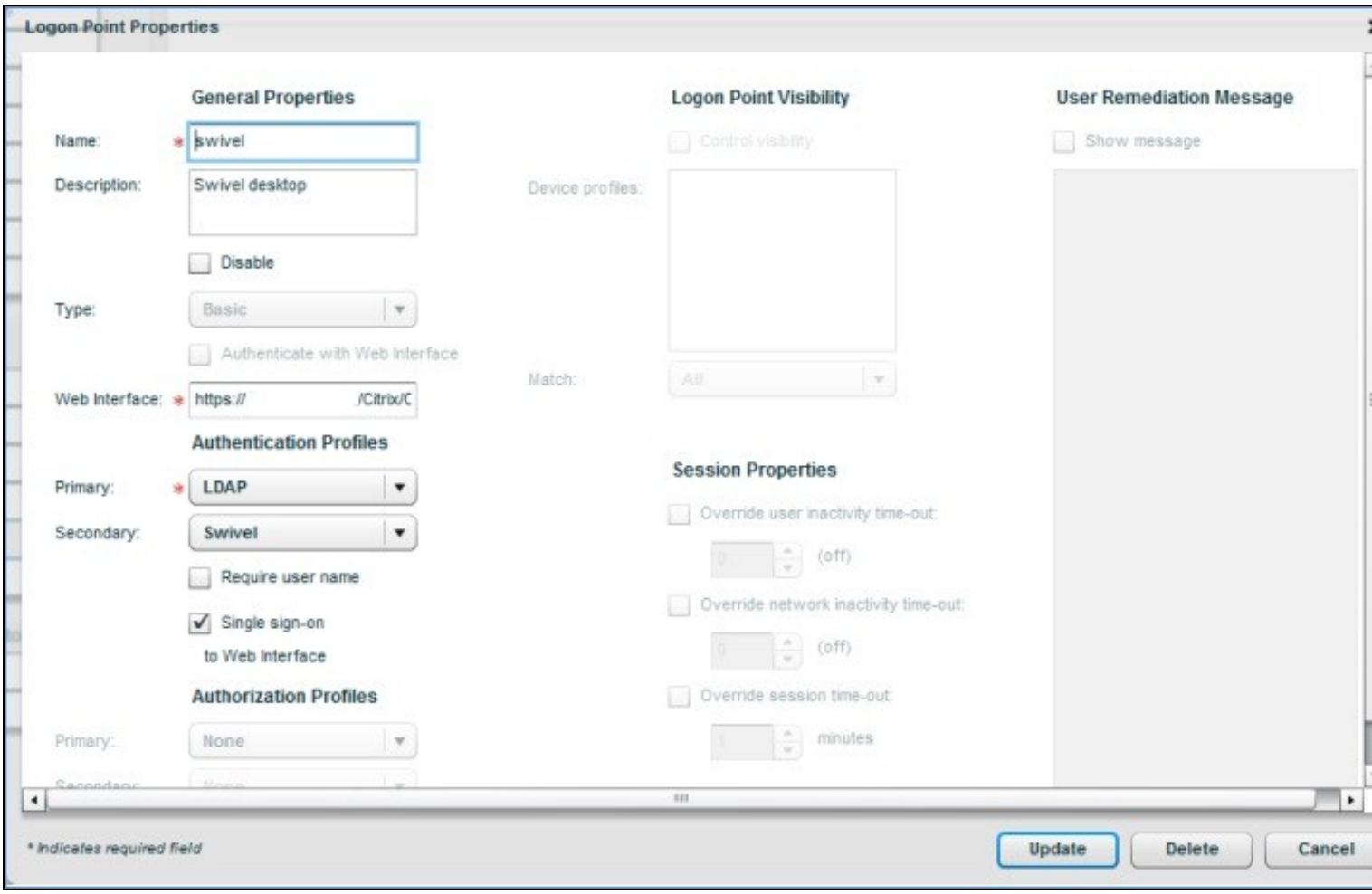
136.1 CAG RADIUS Properties

On the CAG Configuration, configure one or more PINsafe instances as a RADIUS server.



136.2 CAG logon Point Properties

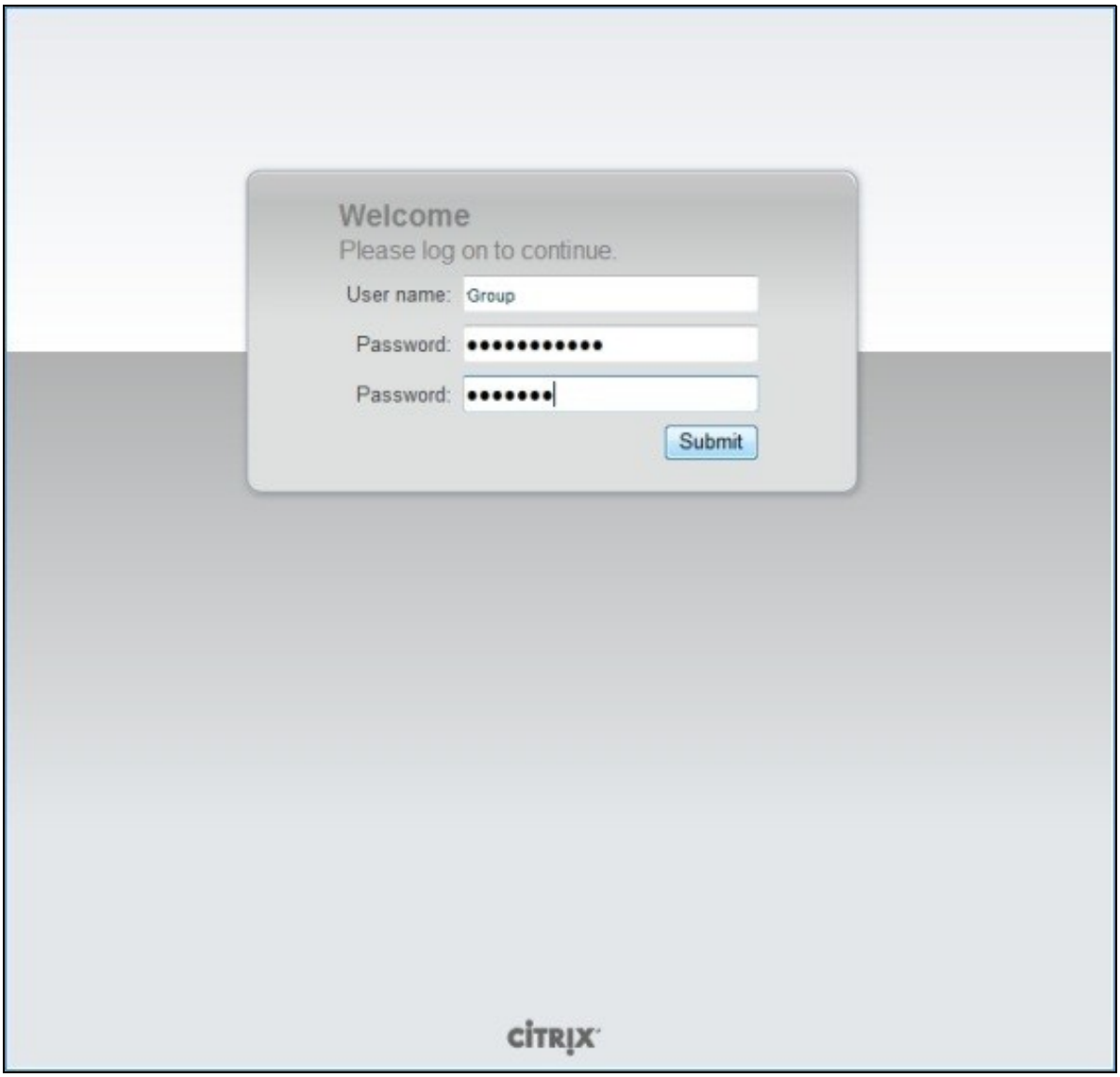
Configure Swivel as an authentication server. Swivel would usually be configured as a secondary authentication server with AD as the primary authentication server using RADIUS. In this example Single Sign ON is being used to the Citrix Web Interface, and has been created as a basic logon point.


Logon Point Properties
General Properties
Name:
swivel
Description:
Swivel desktop
Disable
Type:
Basic
Authenticate with Web Interface
Web Interface:
https://
/Citrix/C
Authentication Profiles
Primary:
LDAP
Secondary:
Swivel
Require user name
Single sign-on
to Web Interface
Authorization Profiles
Primary:
None
Logon Point Visibility
Control visibility
Device profiles:
Match:
All
Session Properties
Override user inactivity time-out:
(off)
Override network inactivity time-out:
(off)
Override session time-out:
minutes
User Remediation Message
Show message
* Indicates required field
Update
Delete
Cancel

137 Additional Installation Options

138 Verifying the Installation

Browse to the CAG login page and enter username, AD Password and OTC from the SMS or Mobile Phone Client. Check the PINsafe logs to ensure that a RADIUS request has been seen.



139 Uninstalling the PINsafe Integration

140 Troubleshooting

141 Known Issues and Limitations

142 Additional Information

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

143 Citrix Access Gateway Web Interface Proxy

144 Introduction

This document is to supplement the Citrix Access Gateway and Citrix Web Interface documentation for the deployment of PINsafe on the Web Interface and using the Secure Ticket Authority to pass authentication from the Citrix Access Gateway to the Citrix Web Interface.

145 Prerequisites

Citrix Access Gateway 5.x

Citrix Web Interface 5.x

PINsafe 3.x

146 Baseline

Citrix Access Gateway 5.0

Citrix Web Interface 5.4

PINsafe 3.8

147 Architecture

When a user authenticates to the Citrix Access Gateway, the authentication is passed to the Web Interface and the user may use PINsafe authentication.

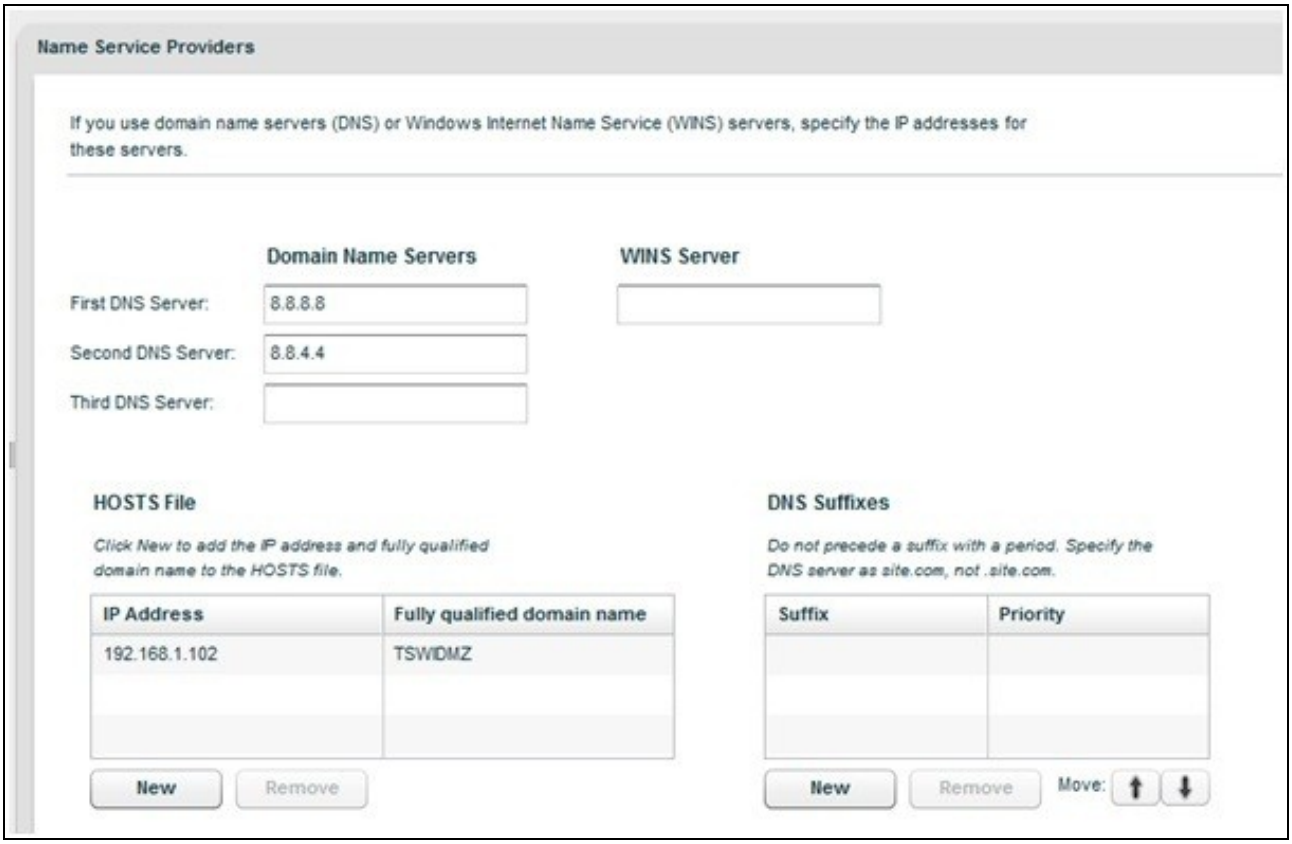
148 Installation

148.1 PINsafe and Web Interface Integration Configuration

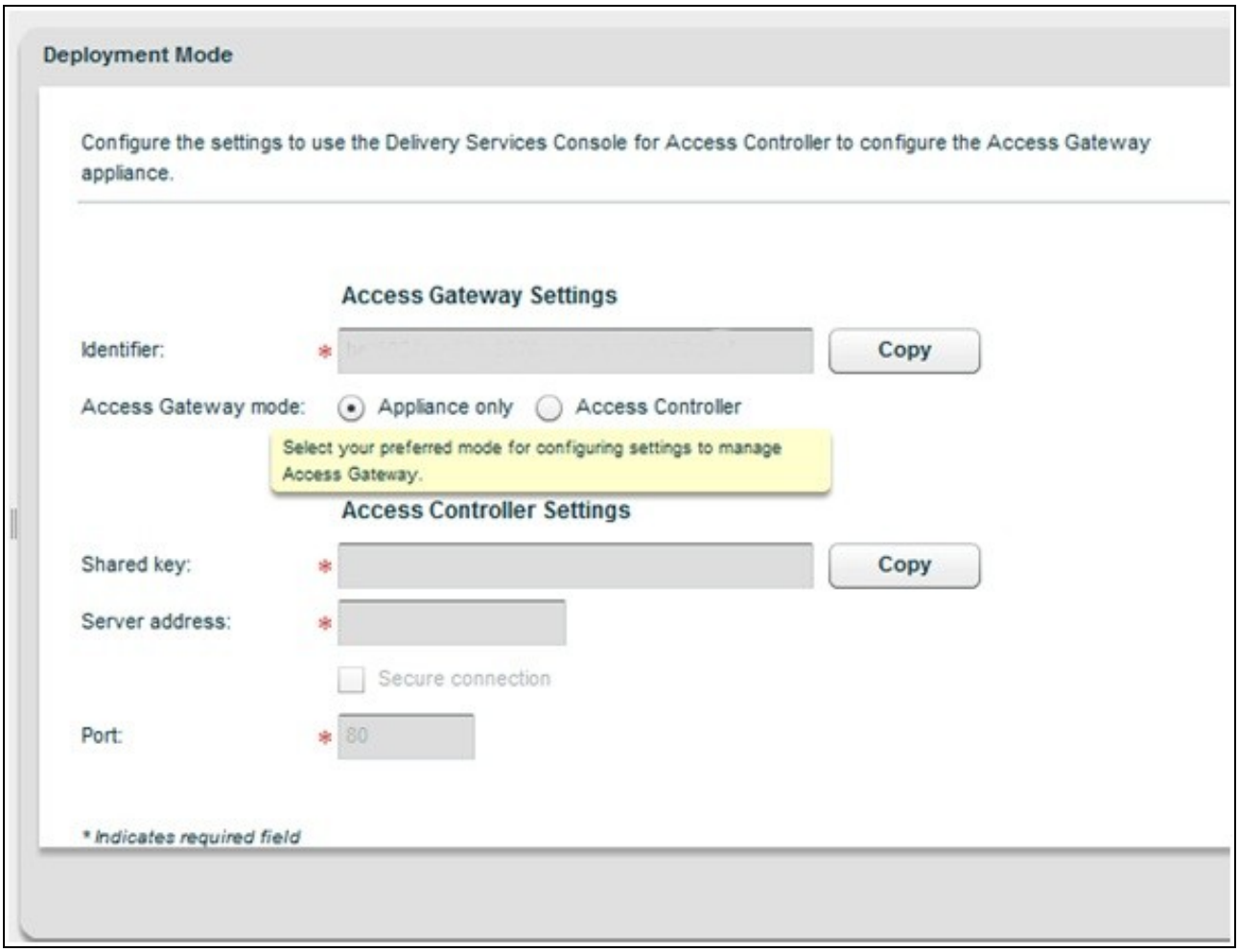
Follow the steps for the appropriate version of PINsafe Web Interface Integration on the PINsafe server see Integrations. Test that this integration is fully working.

148.2 CAG Standard and CAG VPX configuration and installation

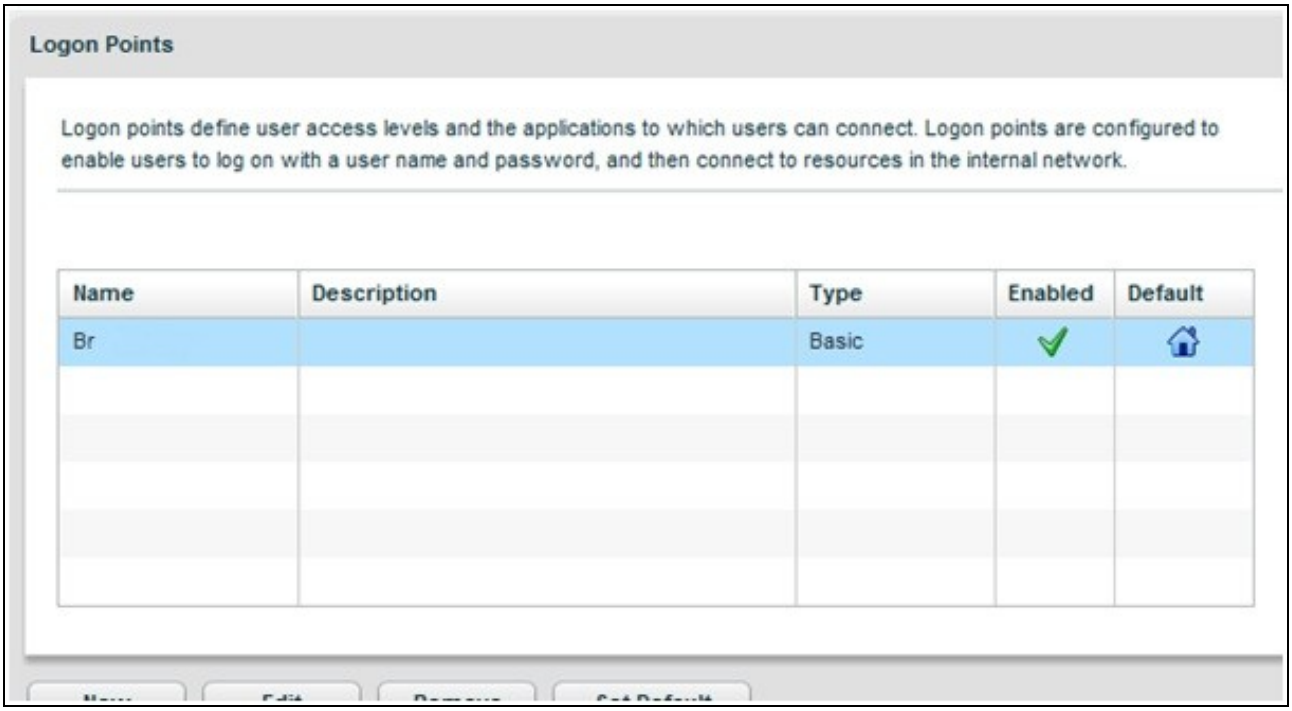
Configure the Access Gateway with networking information in the required deployment scenario. On the CAG enter under Name Service Providers the IP address and Fully Qualified Hostname of the Web Interface server under the section HOSTS File.



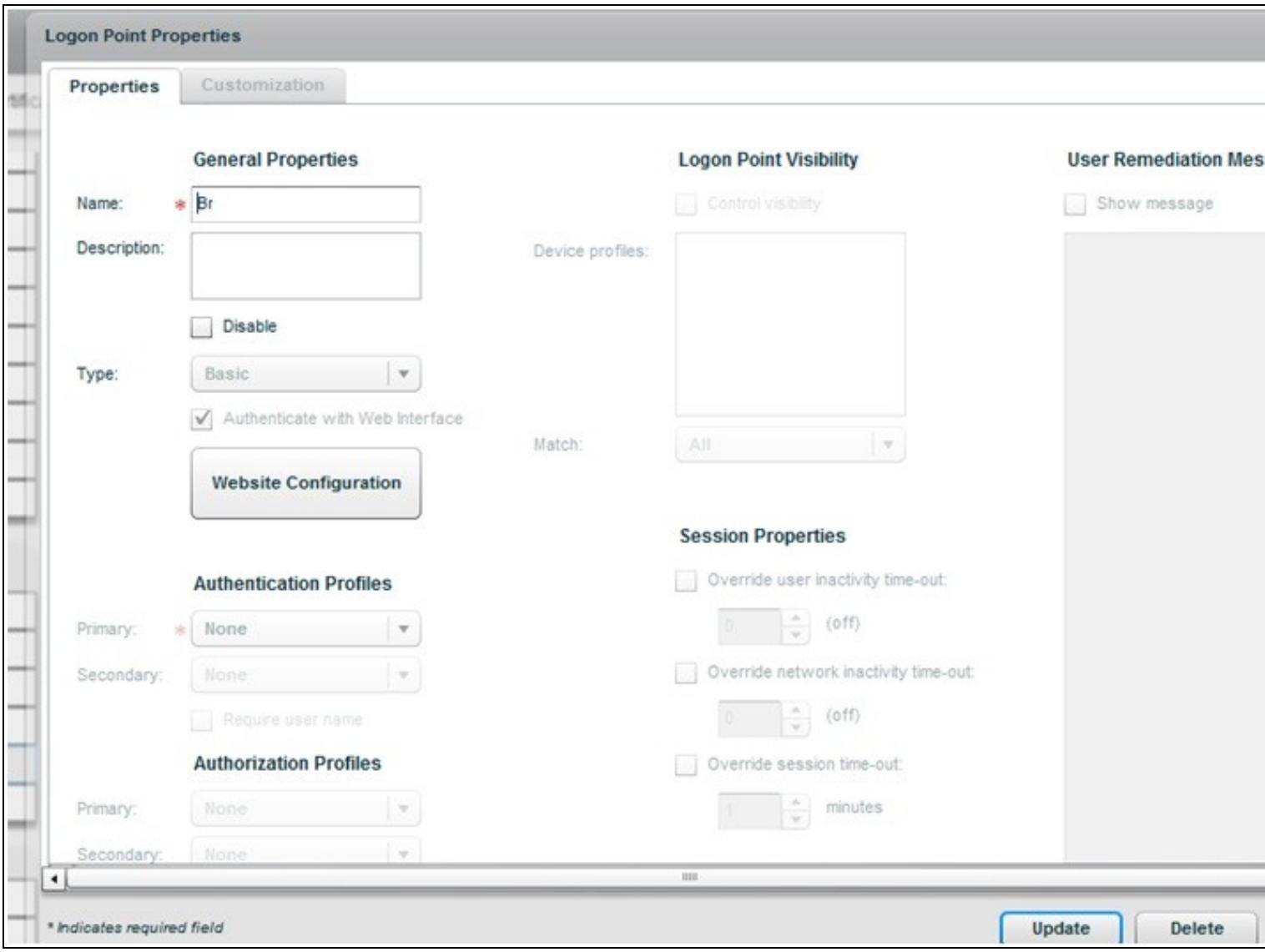
Under Deployment Mode set the Access Gateway Mode to Appliance Only.



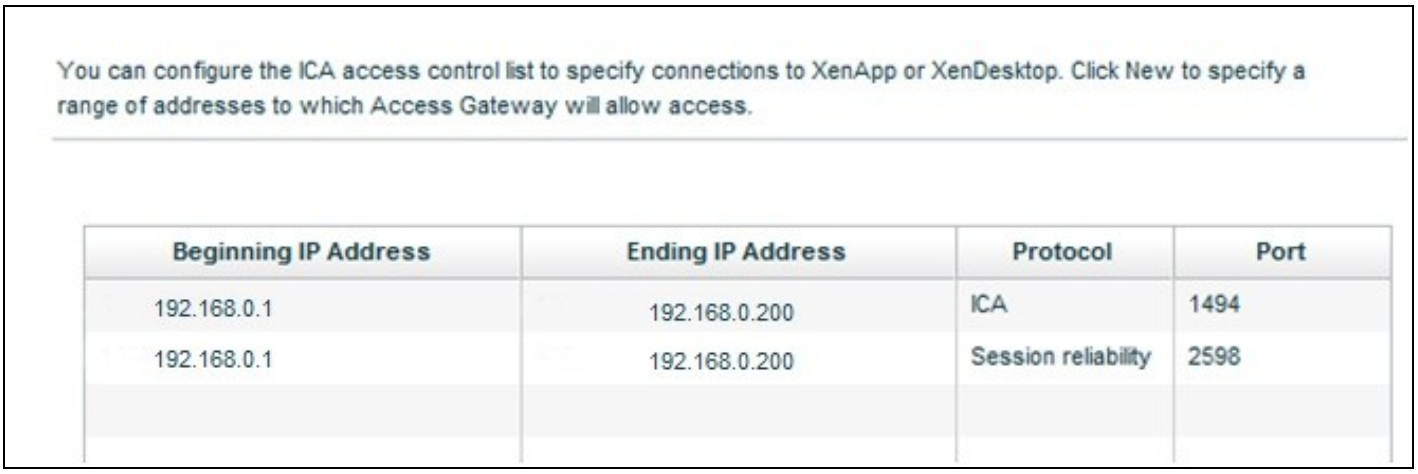
Set the Logon Point as home.



Configure the Logon Point Properties to authenticate with the Web Interface, using the hostname allows the DMZ IP address range to be hidden.



Enter the Web Interface server for the Web Address and Application Type should be WEBINTERFACE.



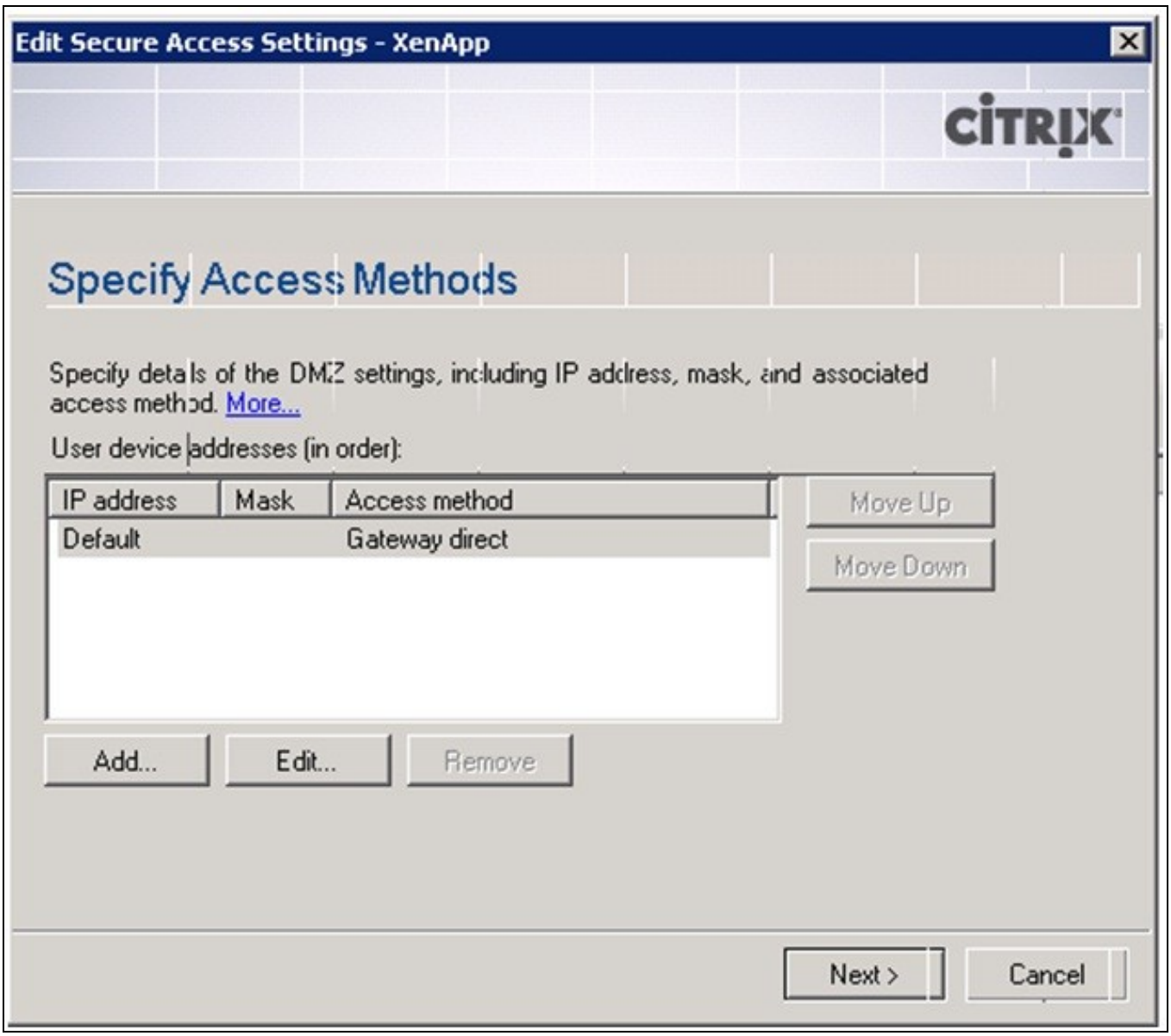
You can configure the ICA access control list to specify connections to XenApp or XenDesktop. Click New to specify a range of addresses to which Access Gateway will allow access.

Beginning IP Address	Ending IP Address	Protocol	Port
192.168.0.1	192.168.0.200	ICA	1494
192.168.0.1	192.168.0.200	Session reliability	2598

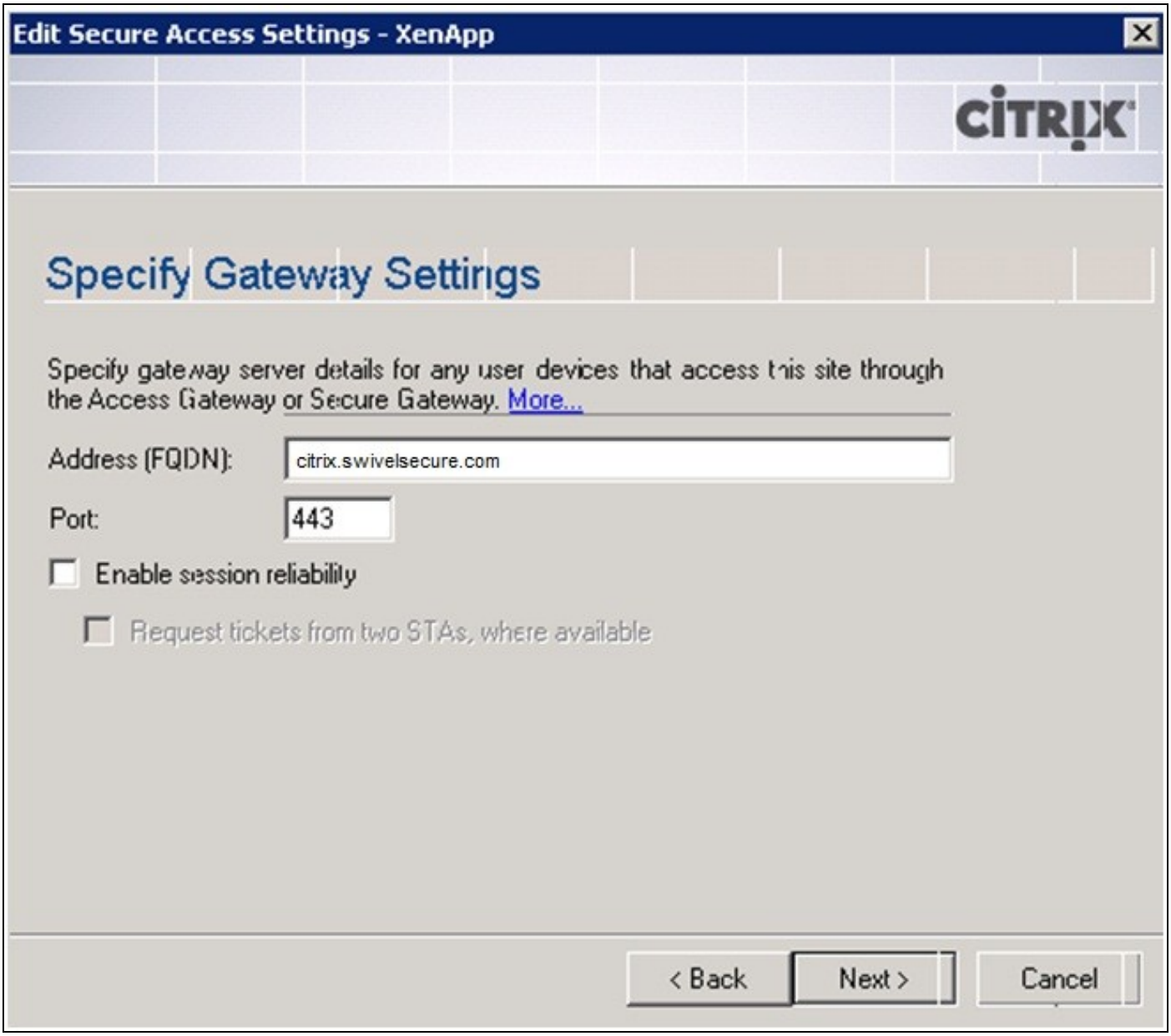
Configure the Web Interface as the STA (Secure Ticket Authority).

148.3 Citrix Web Interface configuration and installation

On the Citrix Web Interface edit the Secure Access Settings, Access Methods to be Gateway Direct.



The (FQDN) Fully Qualified Domain Name needs to be entered for the Gateway Settings



148.4 Additional Installation Options

149 Verifying the Installation

Browse to the login page and authenticate with PINsafe credentials.

150 Uninstalling the PINsafe Integration

151 Troubleshooting

152 Known Issues and Limitations

153 Additional Information

154 Citrix Netscaler Gateway 10.x

155 Introduction

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 10.1 and 10.5 (Netscaler VPN). 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.

For version 10.0 refer to Citrix Access Gateway Enterprise Edition 10

For versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8,

For other versions of 9.x see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad.

Citrix Netscaler 10.5 has a new HTML GUI interface for management, although the customisation pages using java script remains the same.

156 Prerequisites

Access Gateway Enterprise Edition firmware version 10.1 or higher

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

Netscaler pages to modify and/or Swivel files for version 10.x default theme or the Green Bubble 10.x theme

The following pages are for 10.5: only the language resources are different from 10.x. Version 10.5 default theme. Green Bubble 10.x theme.

156.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used upgrading Netscalers with Custom Pages

157 Baseline

Tested with Swivel 3.9.6

Citrix Netscaler Gateway NS10.1 Build 121.10

Citrix Netscaler Gateway NS10.5

158 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

159 Swivel Configuration

159.1 Configuring the RADIUS server

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

159.2 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.

159.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

160 Citrix Netscaler Gateway Configuration

The Swivel integration uses RADIUS authentication, and where the login page is modified it uses the Netscaler custom web pages which are configured and then copied into an archive file which is deployed at boot time.

160.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel virtual or hardware appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. Note: for virtual or hardware appliances, the Swivel VIP should not be used as the RADIUS server IP address, see VIP on PINsafe Appliances

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS

Authentication type RADIUS

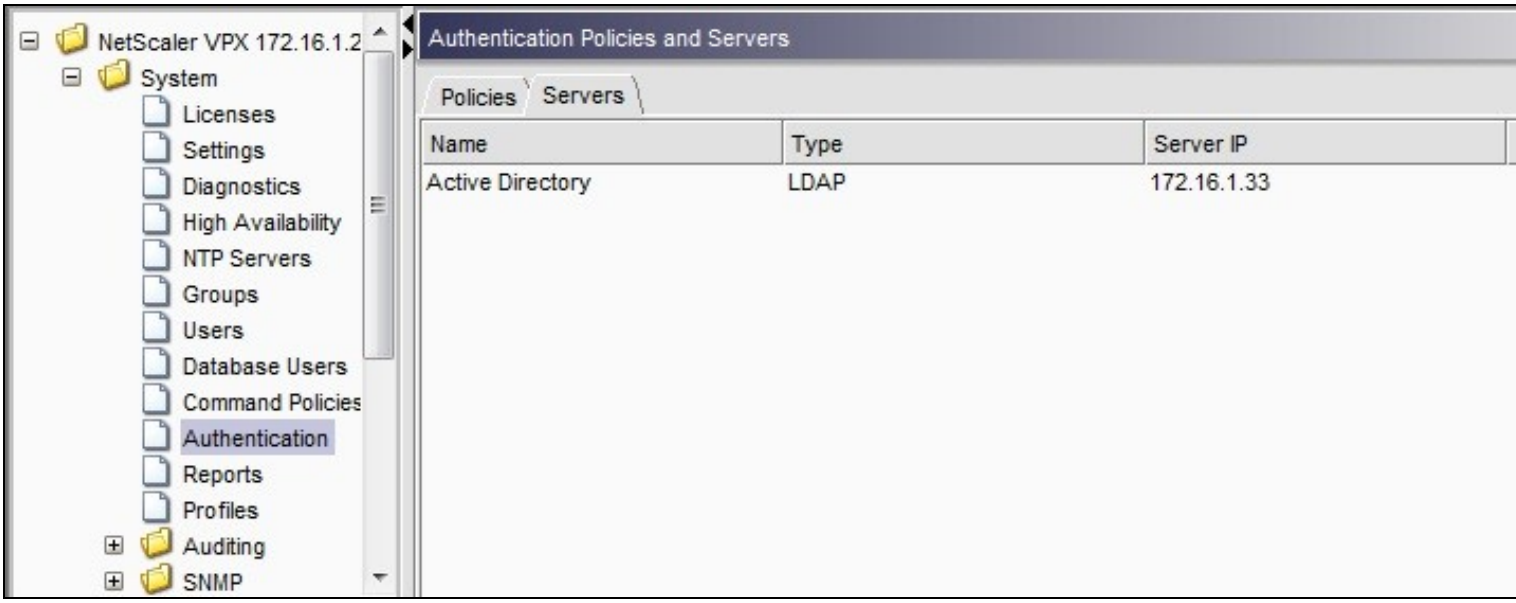
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

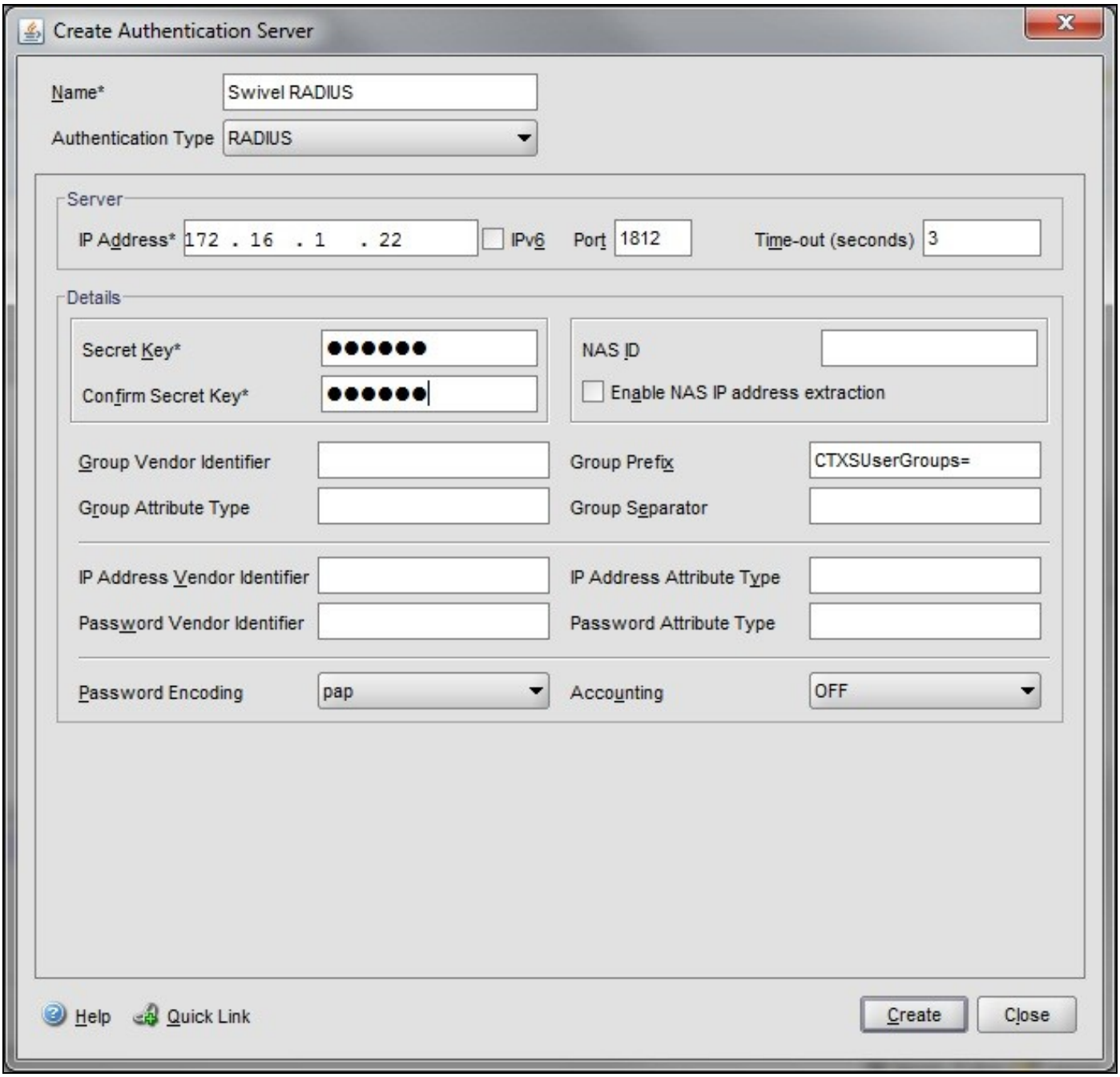
Group Prefix CTXSUserGroups=

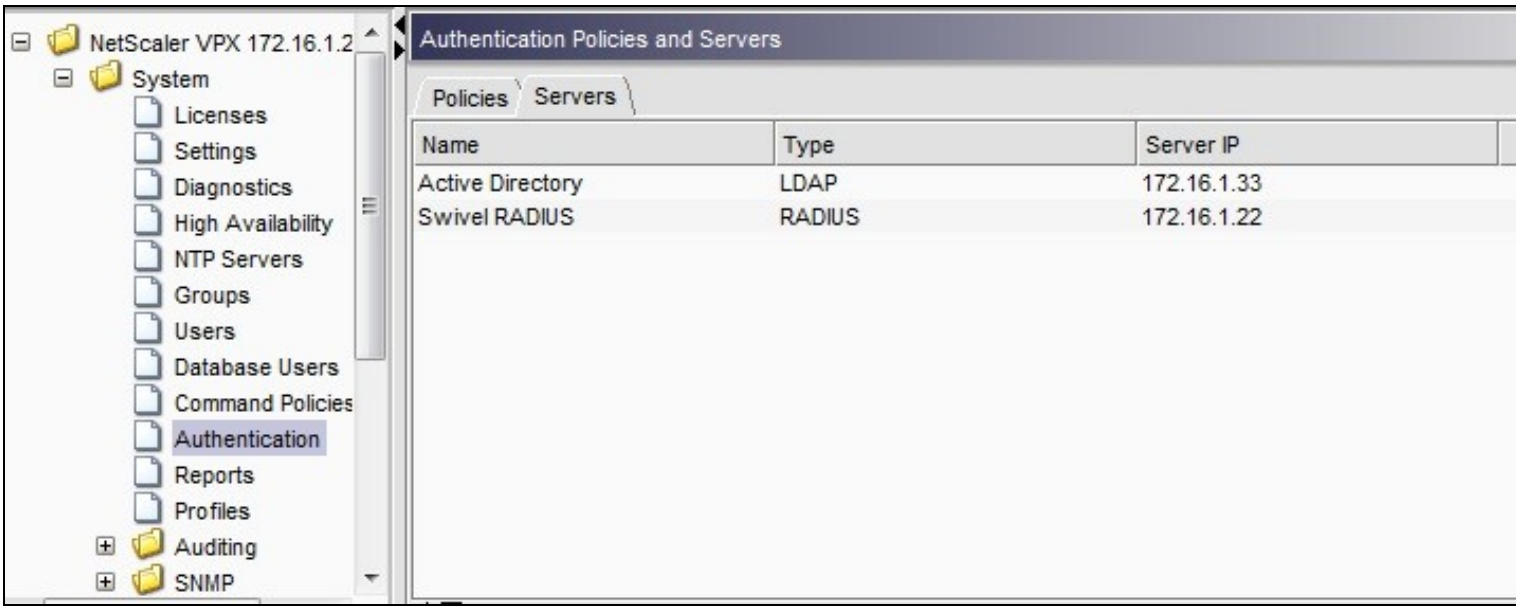
Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.




Create Authentication Server
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
IP Address*
172 . 16 . 1 . 22
IPv6
Port
1812
Time-out (seconds)
3
Details
Secret Key*
Confirm Secret Key*
NAS ID
Enable NAS IP address extraction
Group Vendor Identifier
Group Prefix
CTXSUserGroups=
Group Attribute Type
Group Separator
IP Address Vendor Identifier
IP Address Attribute Type
Password Vendor Identifier
Password Attribute Type
Password Encoding
pap
Accounting
OFF
Help
Quick Link
Create
Close



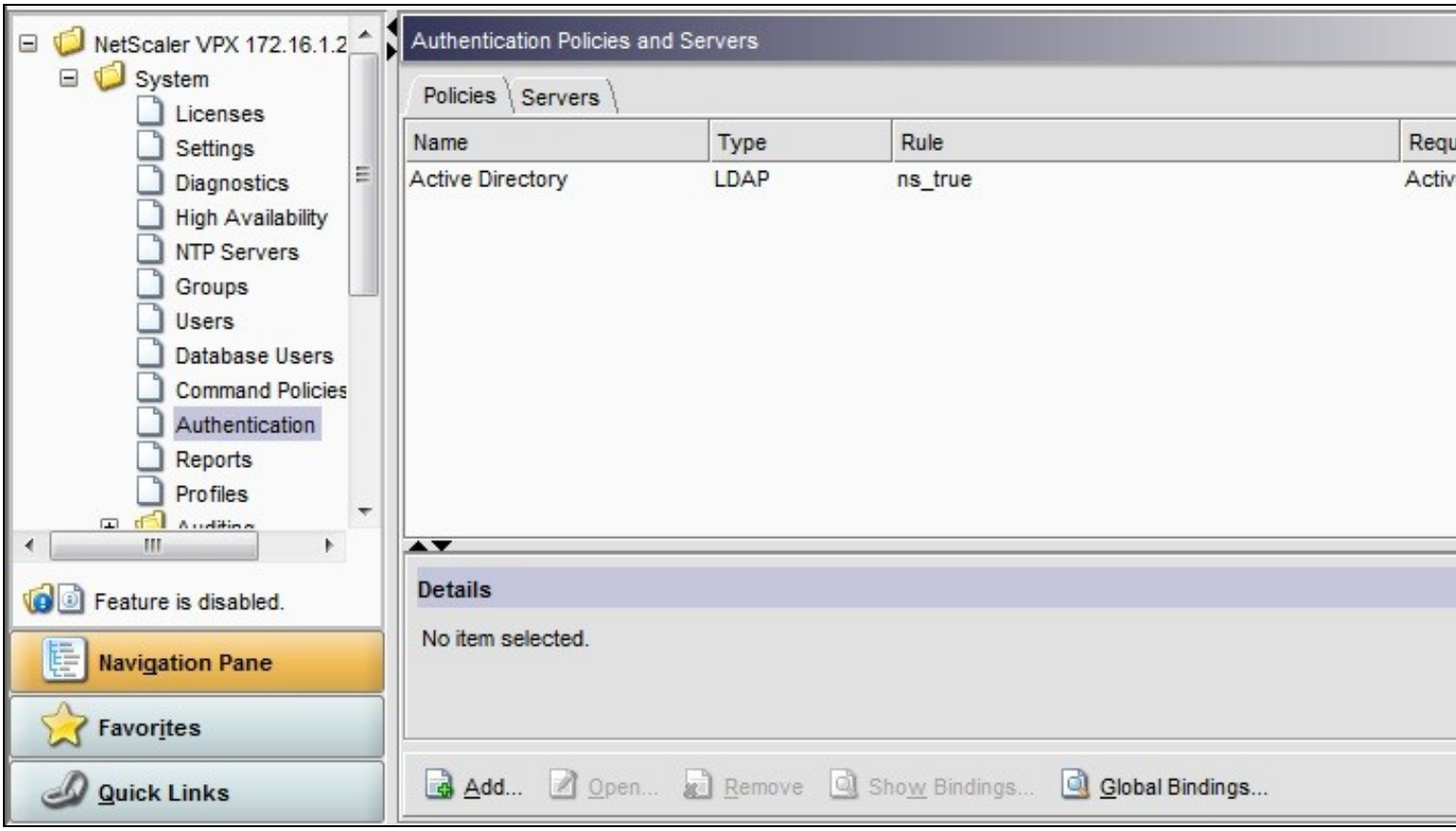
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

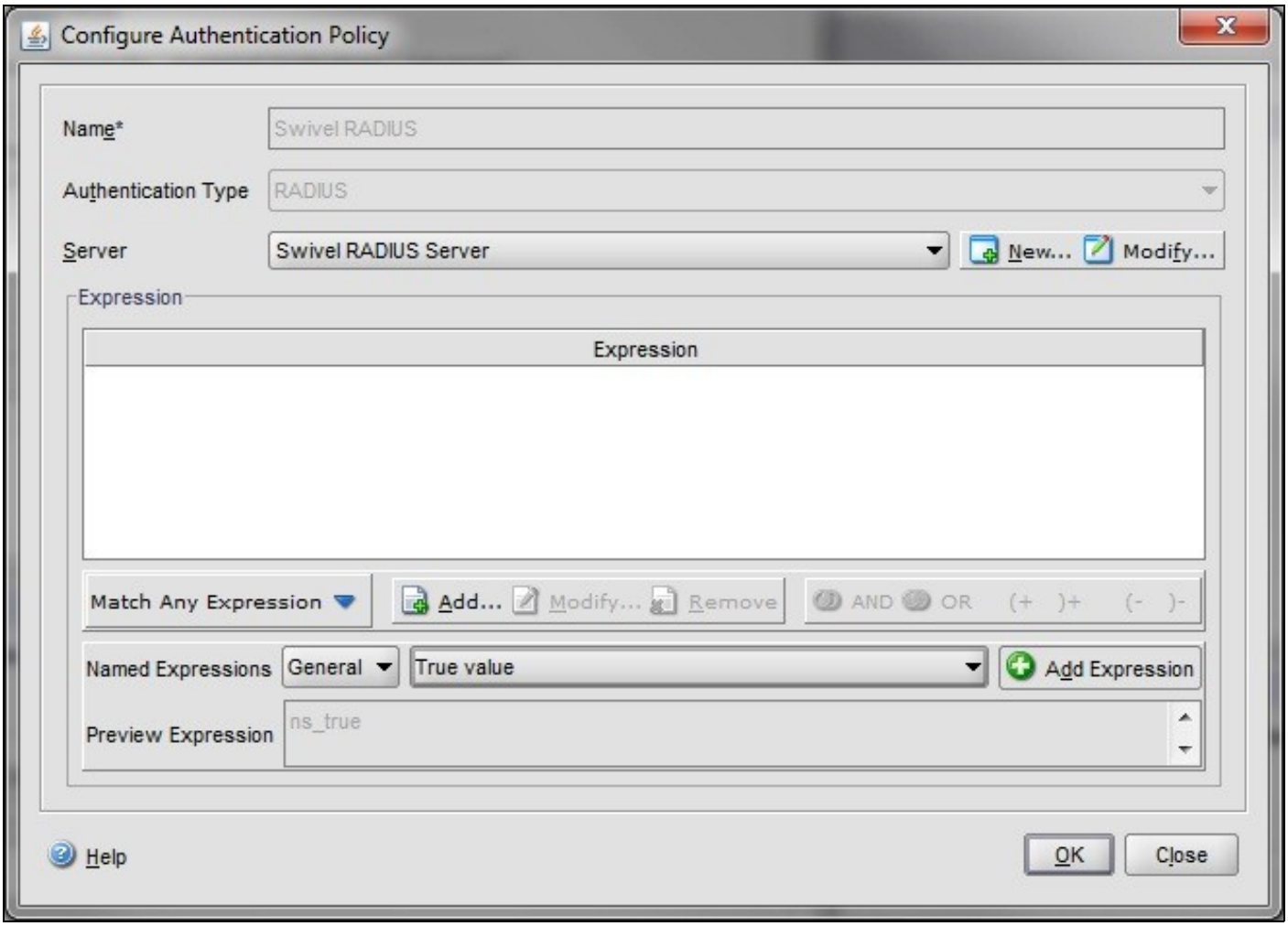
Name Swivel RADIUS Policy

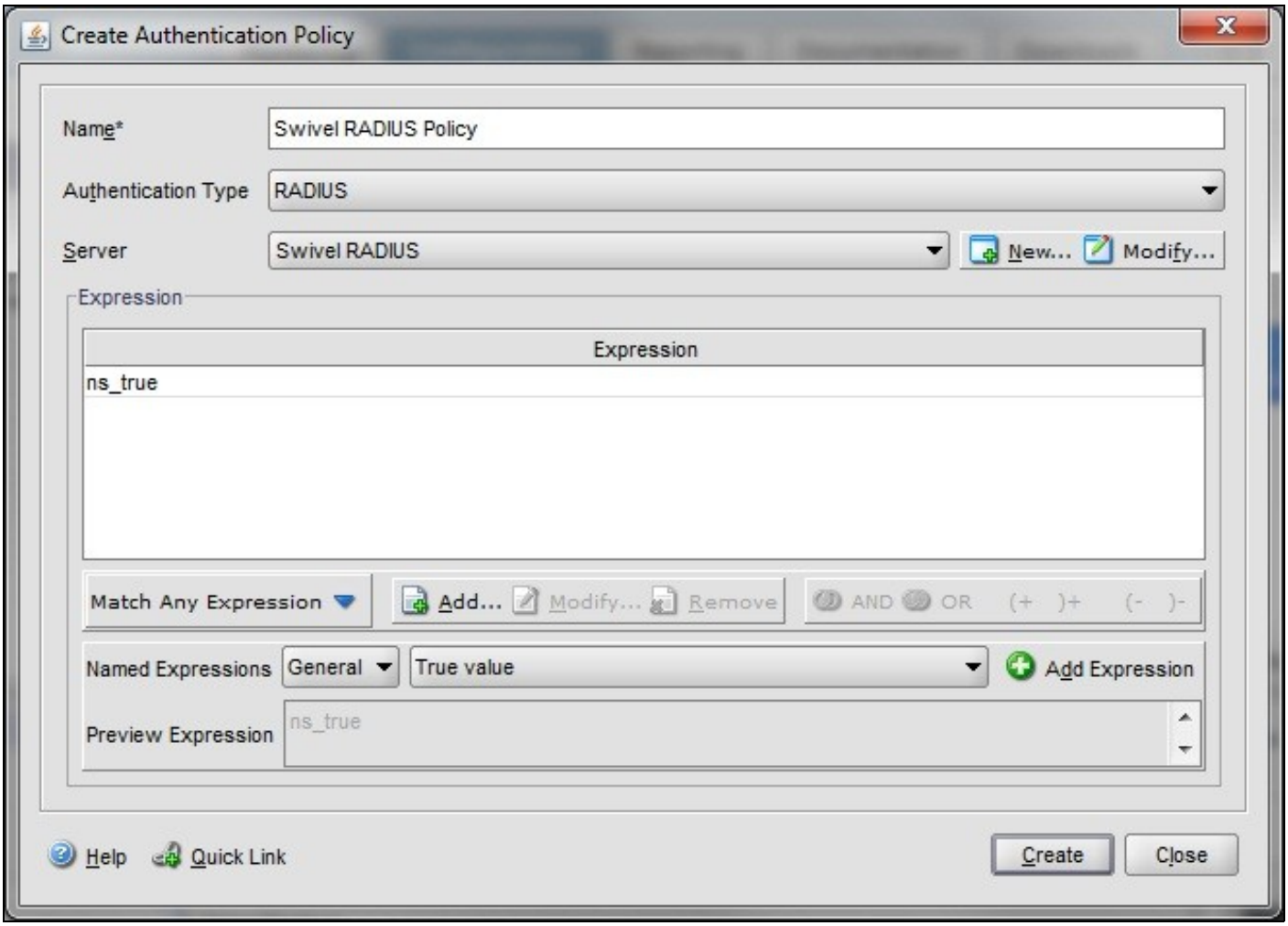
Authentication Type RADIUS

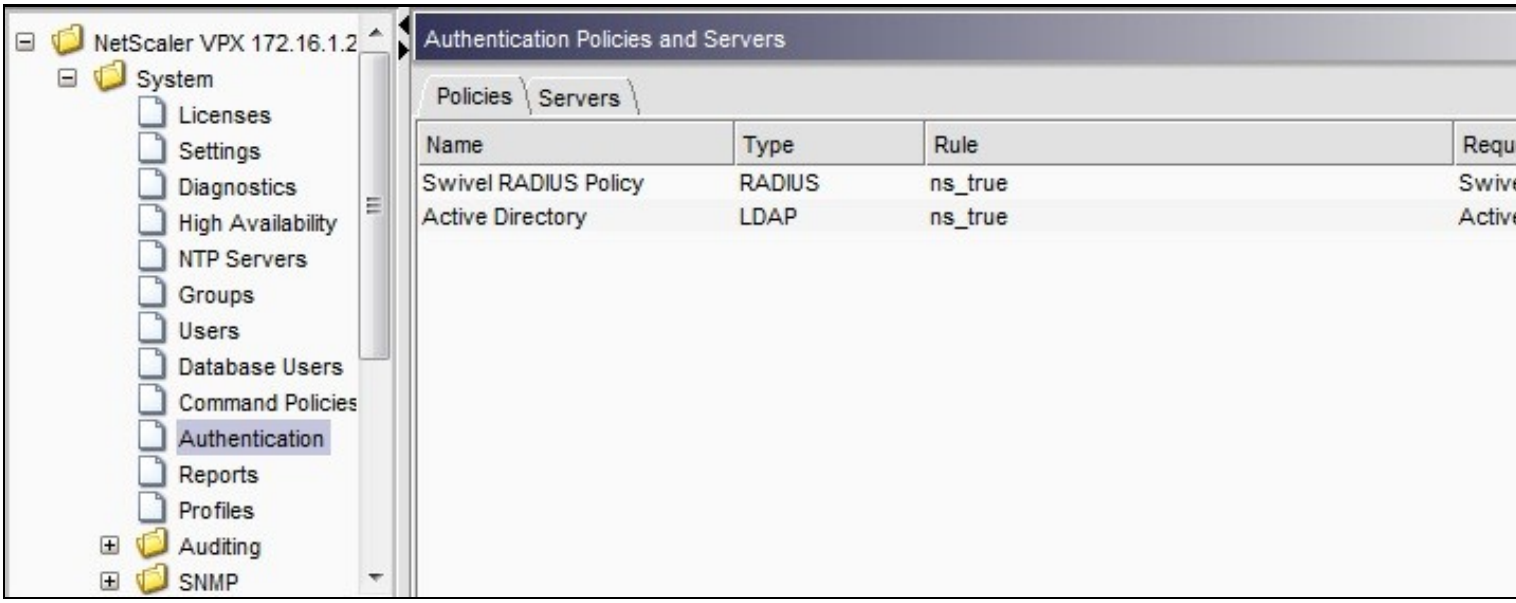
Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

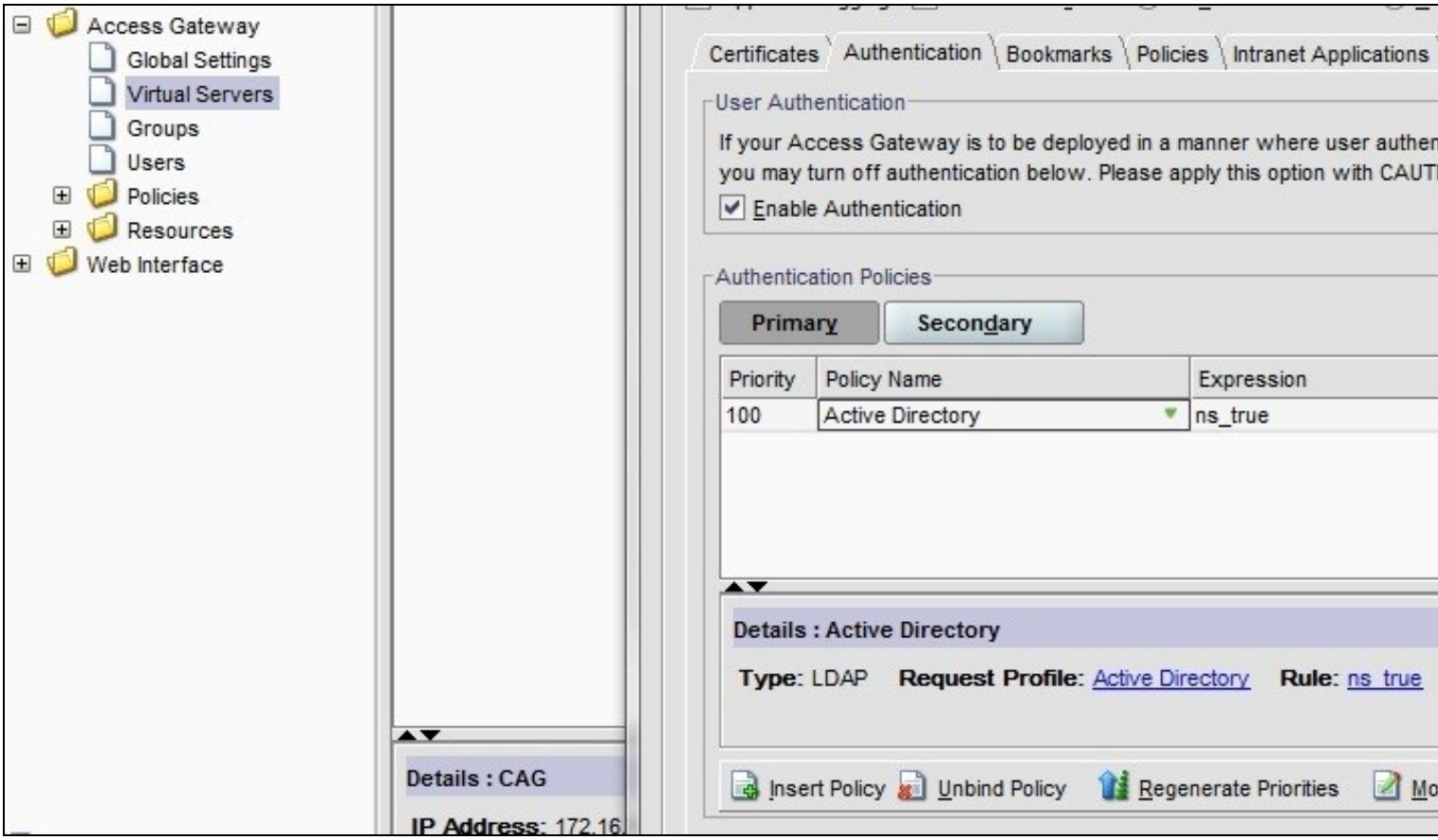


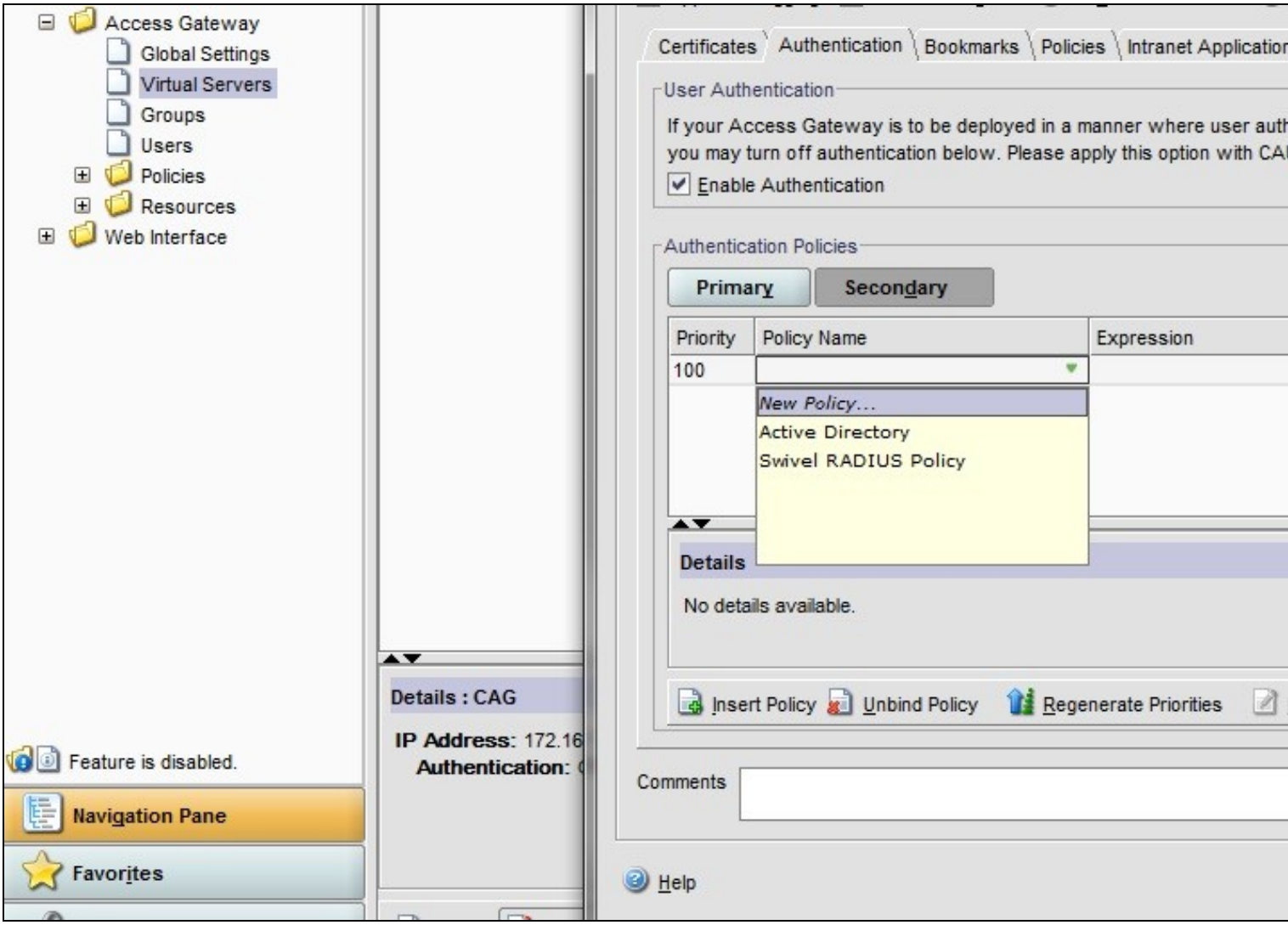

Configure Authentication Policy
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
Swivel RADIUS Server
New...
Modify...
Expression
Expression
Match Any Expression
Add...
Modify...
Remove
AND
OR
(+)+
(-)-
Named Expressions
General
True value
Add Expression
Preview Expression
ns_true
Help
OK
Close





The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.


Access Gateway
Global Settings
Virtual Servers
Groups
Users
Policies
Resources
Web Interface
Details : CAG
IP Address: 172.16
Certificates
Authentication
Bookmarks
Policies
Intranet Applications
User Authentication
If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUT
Enable Authentication
Authentication Policies
Primary
Secondary
Priority
Policy Name
Expression
100
Active Directory
ns_true
Details : Active Directory
Type: LDAP
Request Profile: Active Directory
Rule: ns_true
Insert Policy
Unbind Policy
Regenerate Priorities



160.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

161 Additional Configuration Options

161.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

161.2 Netscaler SSL Bridge

The Netscaler allows a SSL Bridge to be created that allows a Network Address Translation to allow access to the Swivel instance to provide single channel images or Mobile App security strings. On the Netscaler Gateway Administration Console Configuration tab select Traffic Management, Load balancing, Virtual Servers, then click on Add, to open a Create Virtual Server (Load Balancing) window.

The Netscaler requires an external NAT to the Swivel server, and the Netscaler Network bridge allows this to be done using the Netscaler. The Swivel appliance is usually use to provide the proxy port on 8443 or 443

Name Name of the SSL Bridge

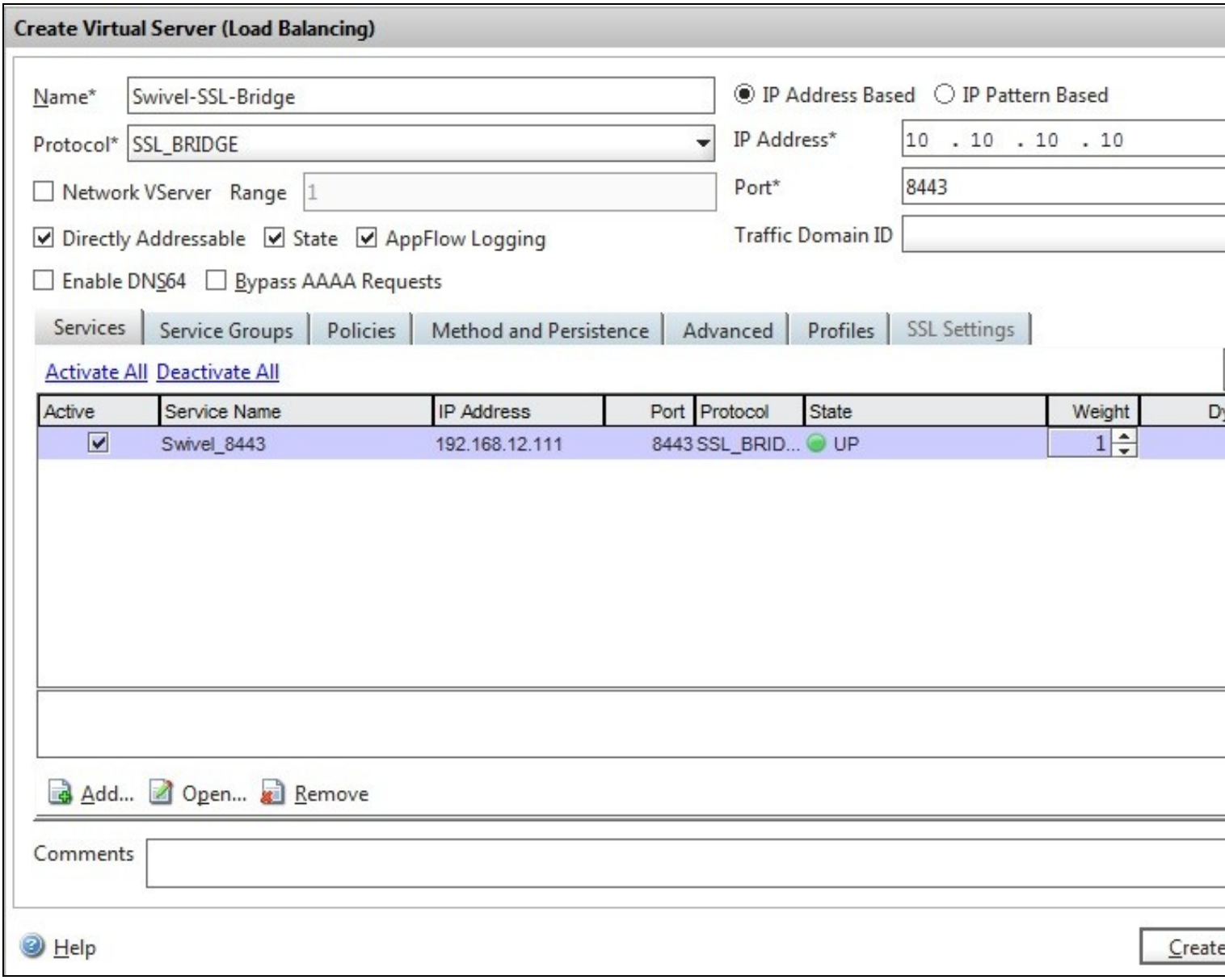
Select IP Adress Based

Protocol select SSL_Bridge

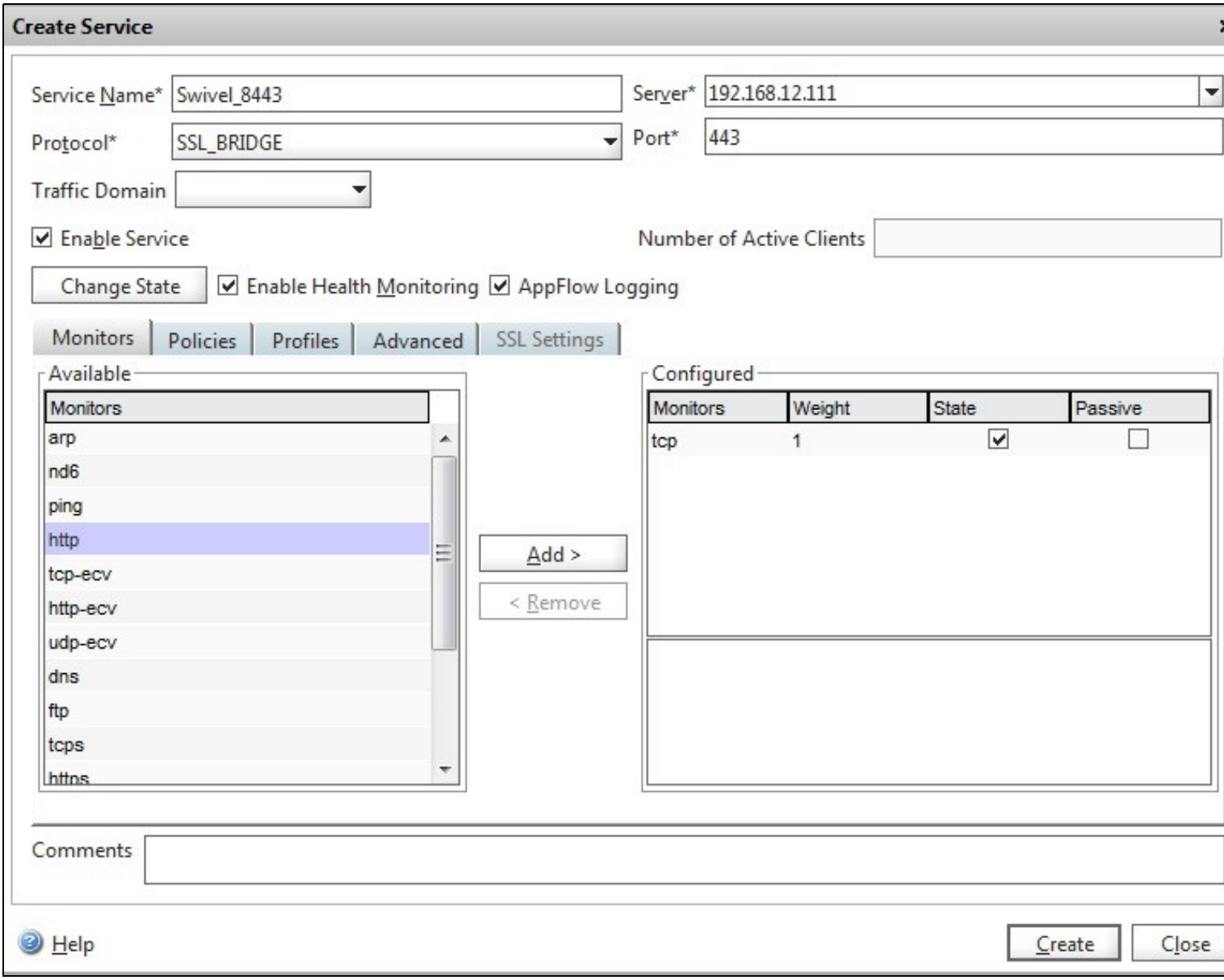
IP address Enter the public IP Address

Port Enter the Swivel instance port number, usually 8443

The following should be ticked *Directly Accessible'*, **State**, **AppFlow Logging**



Click Add and enter the required details.



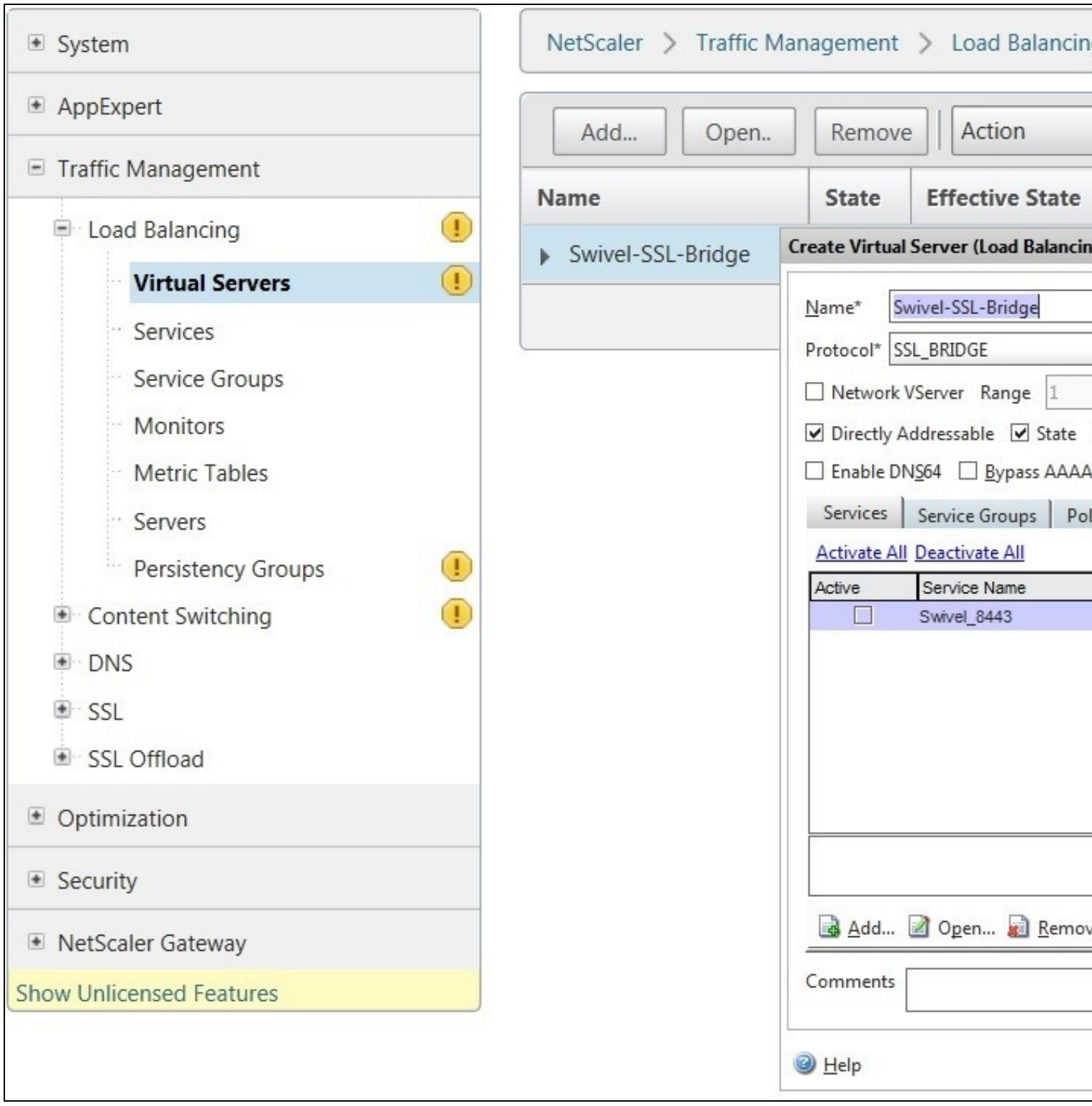
Service Name Name of the SSL Bridge

Server Swivel server address

Protocol select SSL_Bridge from the drop down menu

port select the port used to connect to the SSL bridge, usually 443

From the Monitors tab select TCP then Add it to the list of Configured so that it appears on the right hand side with the State box checked., then click on Create.



161.3 Login Page Customisation

This step only needs to be followed if login page customisation is required.

161.4 Upgrading Netscalers with Custom Pages

Citrix recommend when upgrading a Netscaler with custom pages, the custom pages should be set back to use default pages, upgrade and then the custom pages reapplied. When upgrading it is recommended to make a backup or snapshot of the existing system.

When upgrading a Netscaler 10.1 with custom pages to 10.5, backup the modified pages and scripts, then set the login page back to default. Upgrade, test the Administration console, then upload the modified pages as if carrying out a new Swivel install as given below, then recreate the custom tar file as below as this will then include the updated GUI.

161.5 Customisation Overview

One Touch

One touch is a different approach as the user is redirected to a separate page to authenticate and therefore does not actually see the Netscaler login page.

Refer to VPN_OneTouch_Integration

To customise the page for one touch you need to include the following in the header section of index.html where <swivelappliance> is the hostname of the associated Swivel Appliance

```
//-->
//-> Swivel elements
function redirect(){
window.location.replace("https://<swivelappliance>:8443/onetouch/onetouch?returnurl=" + 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];
      //   alert(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;
       //alert(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"];

if(typeof passwordPassedIn == 'undefined') {
 redirect();
} else {
$('[name=passwd]').val(passwordPassedIn);
$('[name=login]').val(usernamePassedIn);
 //alert("GO " + usernamePassedIn);
 document.getElementsByName("vpnForm")[0].submit();

 }
});
```

Before the closing </SCRIPT> tag

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Winsdows based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
- Display Security String Index
- Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, they are incorporated into the archive deployed at boot time.

161.5.1 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

161.5.2 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /netscaler/ns_gui/vpn
cp index.html index.html.bak
```

161.5.3 Customise the login script

The login page can be customised using the standard theme or the Green bubble theme, or possibly another theme. Download the required theme from the pre-requisites above. Note that to use the customised Green Bubble theme, you first have to select the standard Green Bubble theme, then apply the customisation.

161.5.3.1 Requesting a TURing image

These files can be modified before uploading

Modify pinsafe.js. The pinsafeUrl variable value in pinsafe.js needs to be changed to reflect the Hostname and port number of the relevant Swivel server.

For an virtual or hardware appliance this will normally be similar to:

```
pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/";
```

For a software only install see Software Only Installation

161.5.4 Customise the login prompt

Modify the language resource files in /netscaler/ns_gui/vpn/resources. If you are only using the English language, then edit en.xml and search for

```
<String id="Password2">
```

this should be around line 59.

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password" with a value of "AD Password". You should therefore have 2 lines as follows:

```
<String id="Password">AD Password</String>
<String id="Password2">OTC:</String>
```

(Note that Password1 has no colon at the end, whereas Password2 has a colon).

161.5.4.1 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.

Edit the file rc.netscaler to copy across any modified language pages, as for English which is included in the script.:

```
cp /var/mods/en.xml.mod /var/netscaler/gui/vpn/resources/en.xml
```

161.5.5 Upload files to Netscaler

On the Netscaler ensure that either the default or green bubbles theme is used. On the Netscaler Gateway, select **Netscaler Gateway**/**Global Settings**, then click on **Change Global Settings**, and under the **Client Experience** tab check the *UI Theme*. After modifying the pages, this will be set to custom.

Download the files under the prerequisites and modify as described above, then copy them to the following locations:

index.html to /var/netscaler/gui/vpn/index.html

pinsafe.js to /var/netscaler/gui/vpn/pinsafe.js

161.5.6 Create the boot archive file

```
mkdir /var/ns_gui_custom

cd /netscaler

tar -zcvf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*
```

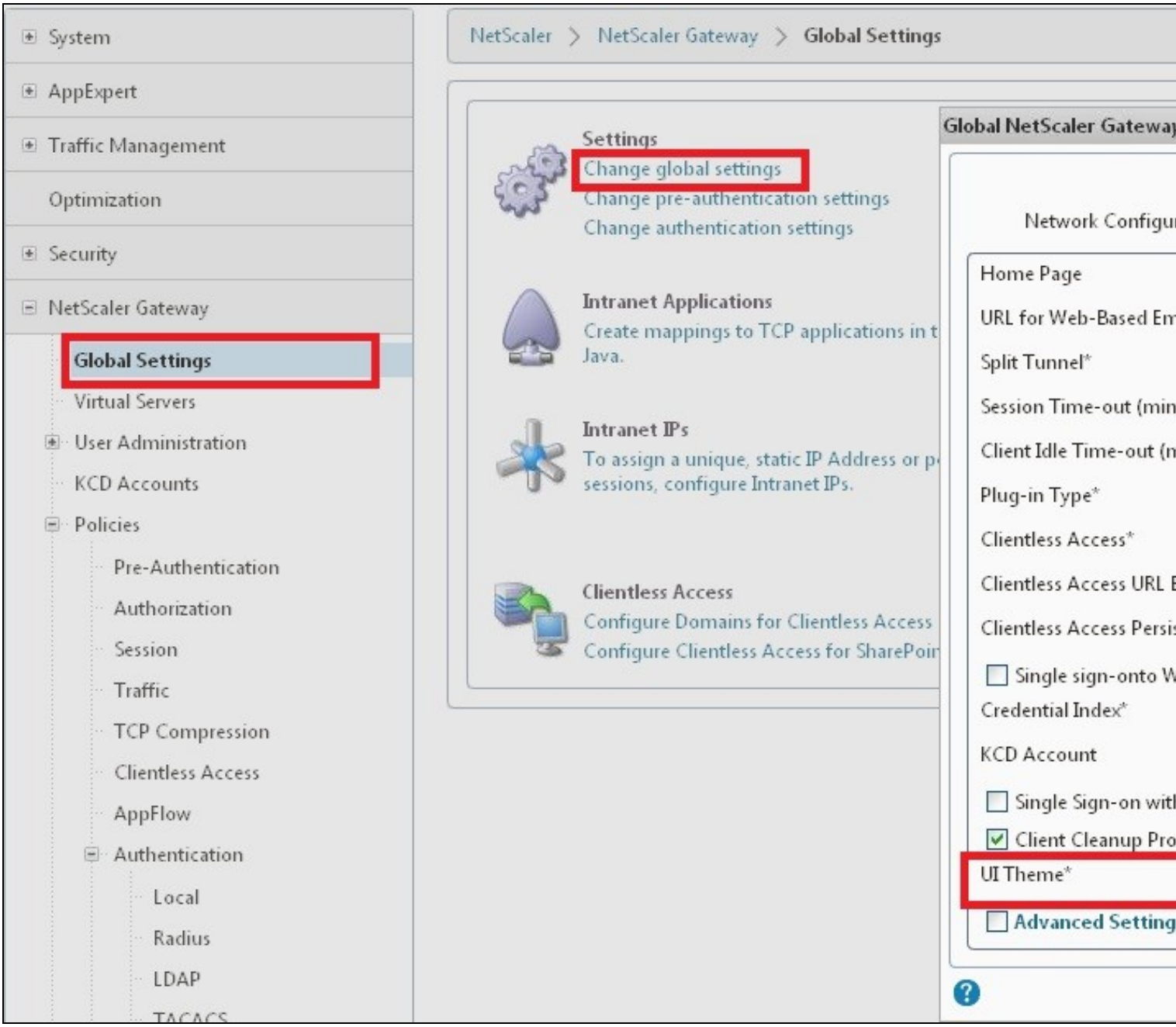
This should create the customtheme.tar.gz file used at boot time, and list all the files used.

161.5.7 Tell the Netscaler to use the customised login pages

/netscaler/ns_gui is a symbolic link that by default points to /var/netscaler/gui, by setting the custom login, this link changes to the custom pages i.e. /var/ns_gui_custom/ns_gui. Therefore it is important that the above boot archive be created before switching to custom. Also note that WinSCP may cache the symbolic link and give the wrong location, so may need to be refreshed in the /netscaler folder.

On the Netscaler Gateway, select **Netscaler Gateway**/**Global Settings**, then click on **Change Global Settings**, and under the **Client Experience** tab change the *UI Theme* to *Custom*, then click on OK

Note: If the Netscaler pages are changed back from Custom to Default, then the index.html is replaced with the defaault index.html, and if a new custom page is required, then the custom index.html will need to be copied back.



161.5.8 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time and that the login page has been modified as required.

161.6 Additional Login Customisation options

161.6.1 Automated TURing Display

With the automated TURing display, when the user leaves the username field, the TURing will be automatically displayed. A login using the TURing image is expected for that user.

Edit the index.html file

```
search for onFocus="loginFieldCheck()"
```

Add a new attribute after this, as follows:

```
onBlur="showTuring()"
```

Example:

```
onFocus="loginFieldCheck()" onBlur="showTuring()" style="width:100%;"
```

161.6.2 Changing the button labels

If you want to want to change the button text such for sending security strings to SMS or email on-demand, rather than showing a TURing image, or change the GET Image text you may want to change the label of the button. You can do this as follows:

Edit the index.html file and locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

```
id="btnTuring" value="Get Image"
```

Change the value attribute to an appropriate alternative, such as "Send Message".

161.6.3 Requesting the string Index

See also Multiple Security Strings How To Guide

Modify pinsafe.js. The pinsafeUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For a virtual or hardware appliance this will normally be similar to:

```
pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/DCIndexImage?username=";
```

For a software only install see Software Only Installation

161.6.4 PINpad

This is a version of the 9.3 customisation modified for Pinpad. Currently in beta testing. Note that in order to use PINpad you will need a Swivel virtual or hardware appliance with the latest proxy application installed. You can get this from here.

PINpad pre-req

161.6.5 Requesting an SMS

See also Challenge and Response below

Modify pinsafe.js. The pinsafeUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an virtual or hardware appliance this will normally be similar to:

```
pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

161.7 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. RADIUS Challenge and Response can be optionally configured to enter a username and Password, which will then ask for a One Time Code. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

If Single Channel is not being used at all, then a TURing image is not required. Therefore, if you configured a message Resend button (which would replace a Show Image button), then in the pinsafe.js, the parameter:

```
onclick= "showTuring();"
```

Must be changed to:

```
onclick= "sendMessage();"
```

Optionally, you can remove the showTuring function altogether. Which is in addition to the above step of changing onClick=.

Example fucnction code:

```
function showTuring() {showImage(pinsafeUrl + "SCImage");}
```

161.8 Image Request button displayed when needed

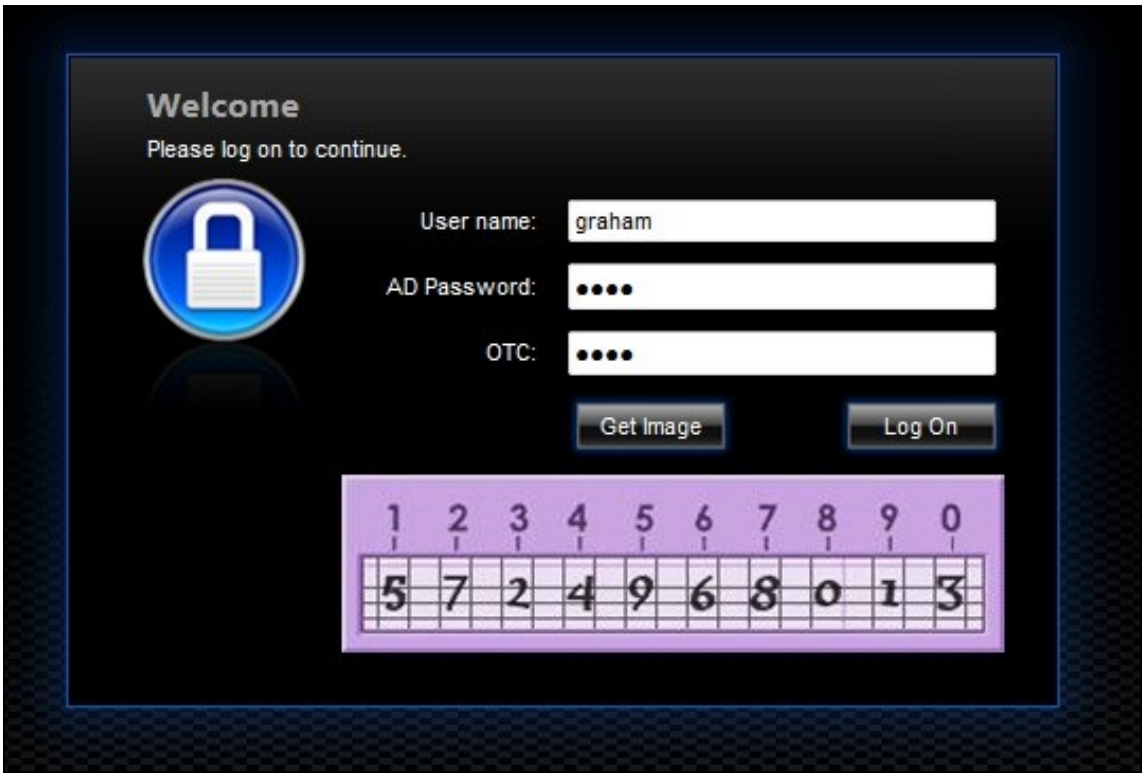
The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
```

```
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

162 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.



For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

If the incorrect credentials are used then the login should fail

Where the TURing image is not used, then the Get Image page modification can be omitted

163 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

164 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

164.1 Error Messages

Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

Username field length incorrect

If the username field is too short it can be increased. Edit the index.html file and locate the below section setting the size="40"

<td align="right" style="padding-right:10px;white-space:nowrap;"></td> <td colspan=2 style="padding-right:8px;"><input id="Enter user name" class="CTXMSAM_ContentFont" style="font-size: 8pt" type="text" title="" name="login" size="40" maxlength="127" onFocus="loginFieldCheck()" style="width:100%;" /></td>

login command failed over API. Reason: Response not of type text/xml: text:html

This error can be seen on the Netscaler Administration console when upgrading with a custom theme. This will preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

Look for the line containing -UITHEME CUSTOM and change it to DEFAULT as below:

```
set vpn parameter -localLanAccess ON -defaultAuthorizationAction ALLOW -proxy BROWSER -clientCleanupPrompt OFF -forceCleanup none -clientOp
```

After making the changes, reboot the system to login.

165 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

166 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

167 Citrix Netscaler Gateway 11

168 Introduction

- 
Netscaler TURing
- 
Netscaler PINpad

This document shows the steps required to integrate Swivel with the Citrix NetScaler 11.0. Swivel can provide Two Factor authentication with SMS, Token, and Mobile Phone Client and strong Single Channel Authentication with TURing or Pinpad, or in the Taskbar using RADIUS.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad.

There is an alternative solution using Rewrite/Responder policies, which is recommended in preference to the solution outlined below. It is described in the Netscaler 12 article, but it applies to version 11 as well. Please check Citrix Netscaler Gateway 12.

169 Prerequisites

NetScaler version 11.0. The single channel customisation was created using build 62, and there may be minor cosmetic issues with other versions.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

Netscaler pages to modify and/or Swivel files for version 11.0 default theme.

Netscaler pages to modify and/or Swivel files for version 11.0 Green Bubble theme.

If you would prefer to deploy ready-made themes, see the following:

- Default theme TURing image
- Default theme PINpad
- Green Bubble theme TURing image
- Green Bubble theme PINpad

See below for details on deploying these themes.

169.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used upgrading Netscalers with Custom Pages

170 Baseline

Tested with Swivel 3.10.4

Citrix Netscaler Gateway NS11.0 Build 62.0

171 Architecture

The Citrix NetScaler makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

172 Swivel Configuration

172.1 Configuring the RADIUS server

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

172.2 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.

172.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

173 Citrix Netscaler Gateway Configuration

The Swivel integration uses RADIUS authentication, and where the login page is modified it uses the Netscaler custom web pages which are configured and then copied into an archive file which is deployed at boot time.

173.1 Citrix NetScaler RADIUS Configuration

The NetScaler needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel virtual or hardware appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. **Note: for virtual or hardware appliances, the Swivel VIP should NOT be used as the RADIUS server IP address, see VIP on PINsafe Appliances**

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under System->Authentication->RADIUS, select the Servers Tab, click "Add" and enter the following information:

Name Swivel RADIUS

Server Name The name or IP address of the Swivel server

Port 1812

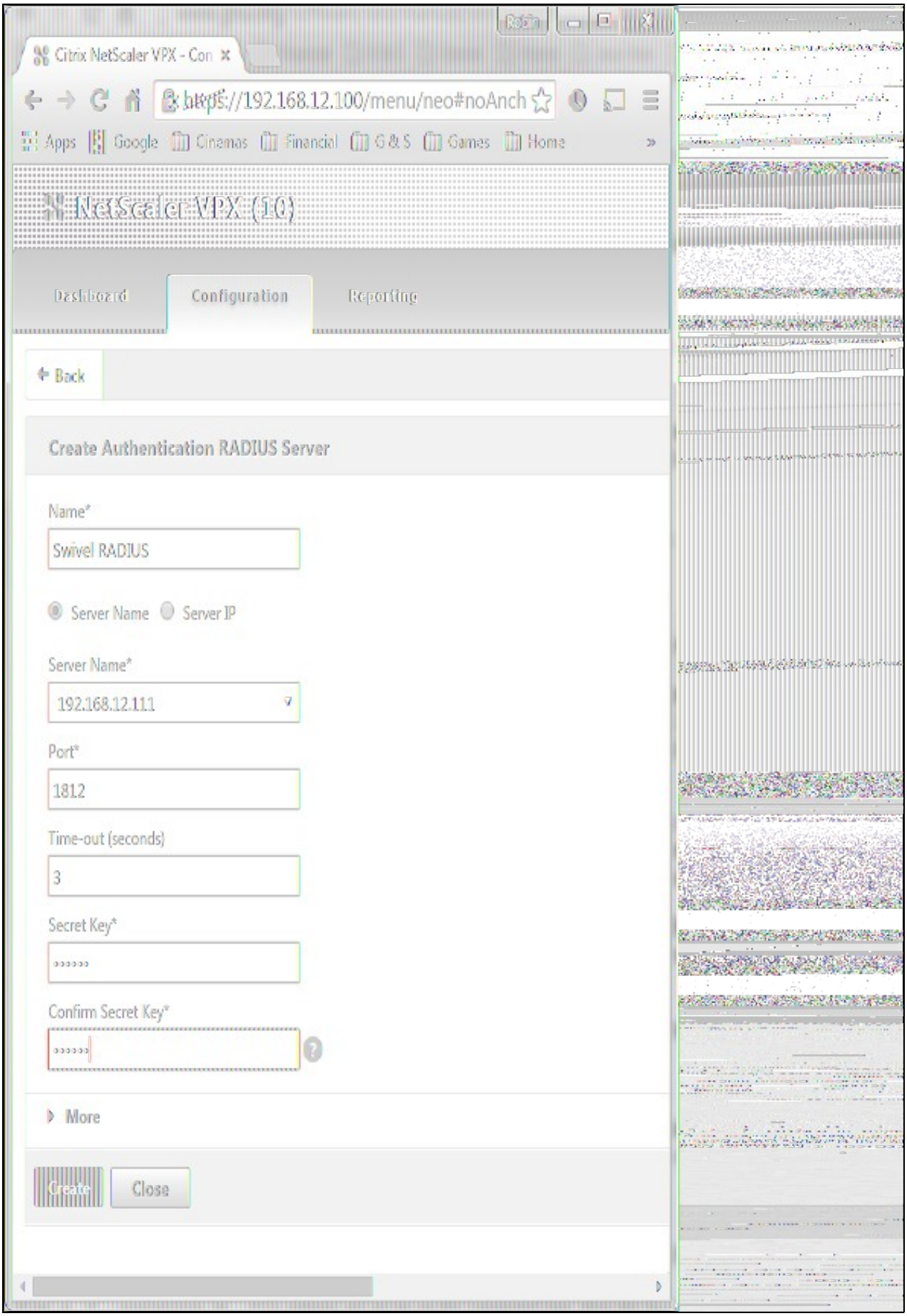
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

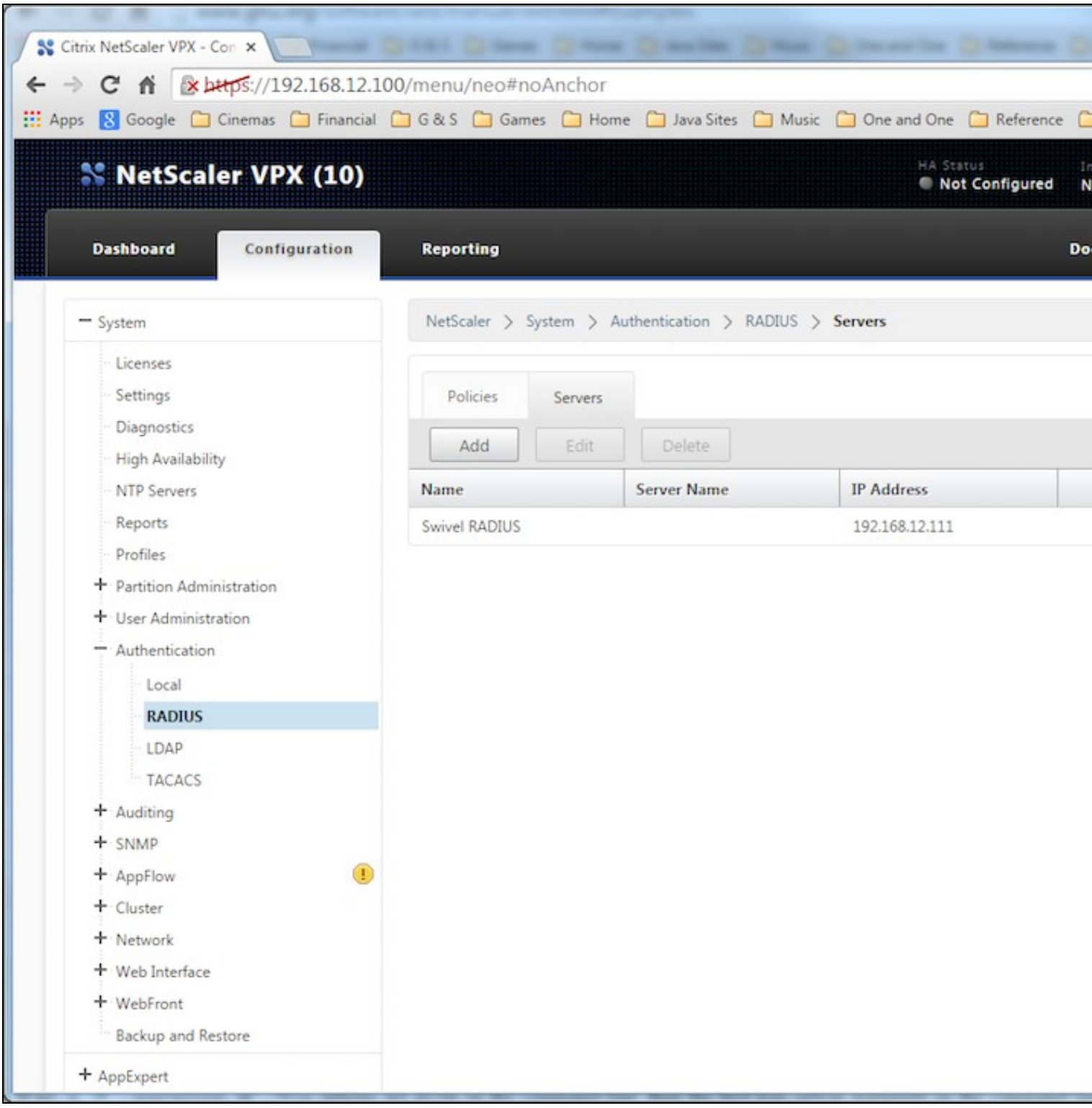
Group Prefix CTXSUserGroups=

Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.


Citrix NetScaler VPX - Con
https://192.168.12.100/menu/neo#noAnch
Apps
Google
Cinemas
Financial
G & S
Games
Home
NetScaler VPX (10)
Dashboard
Configuration
Reporting
Back
Create Authentication RADIUS Server
Name*
Swivel RADIUS
Server Name
Server IP
Server Name*
192.168.12.111
Port*
1812
Time-out (seconds)
3
Secret Key*
Confirm Secret Key*
More
Create
Close

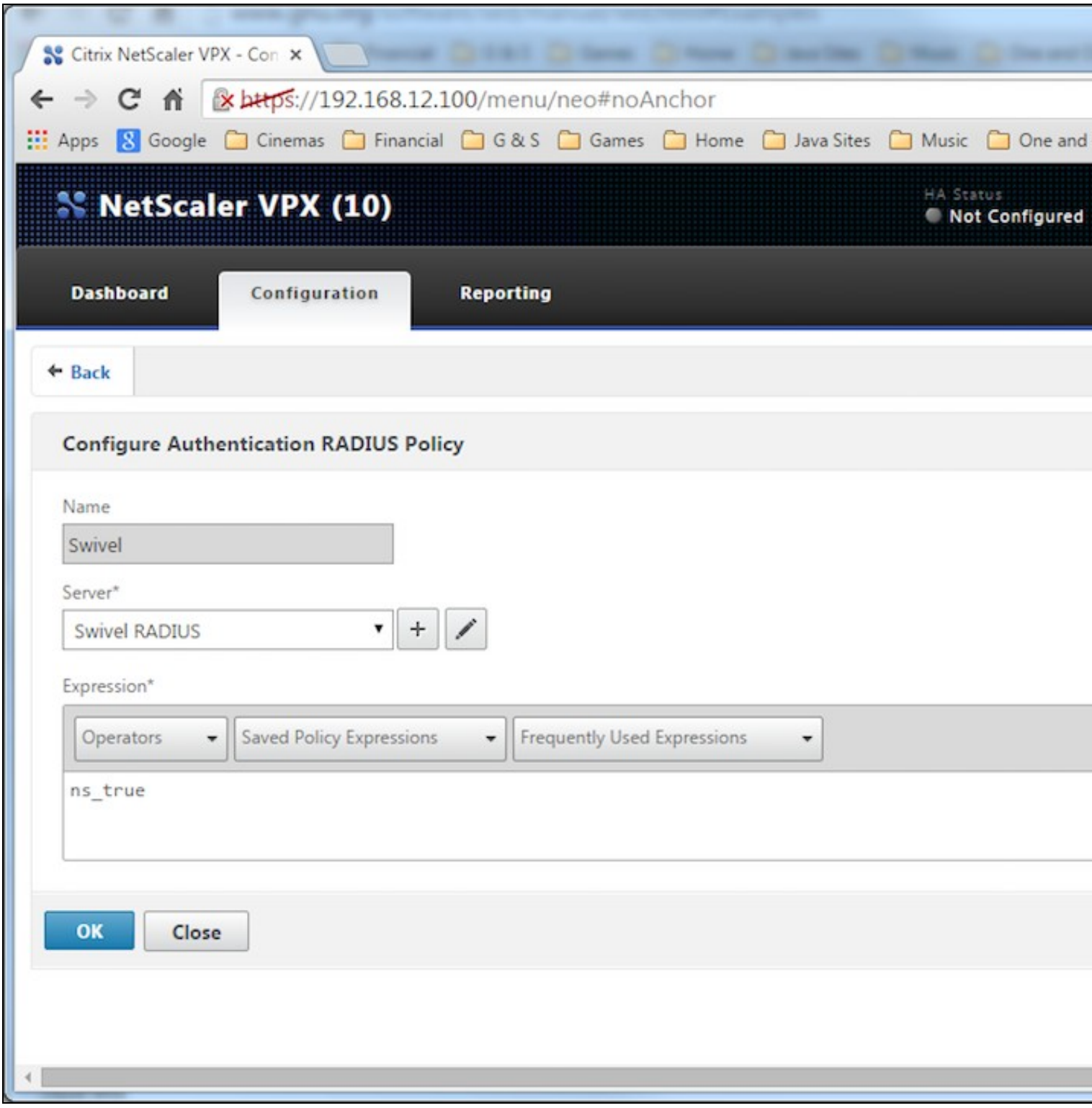


Now select the Policies Tab, click "Add" and enter the following information:

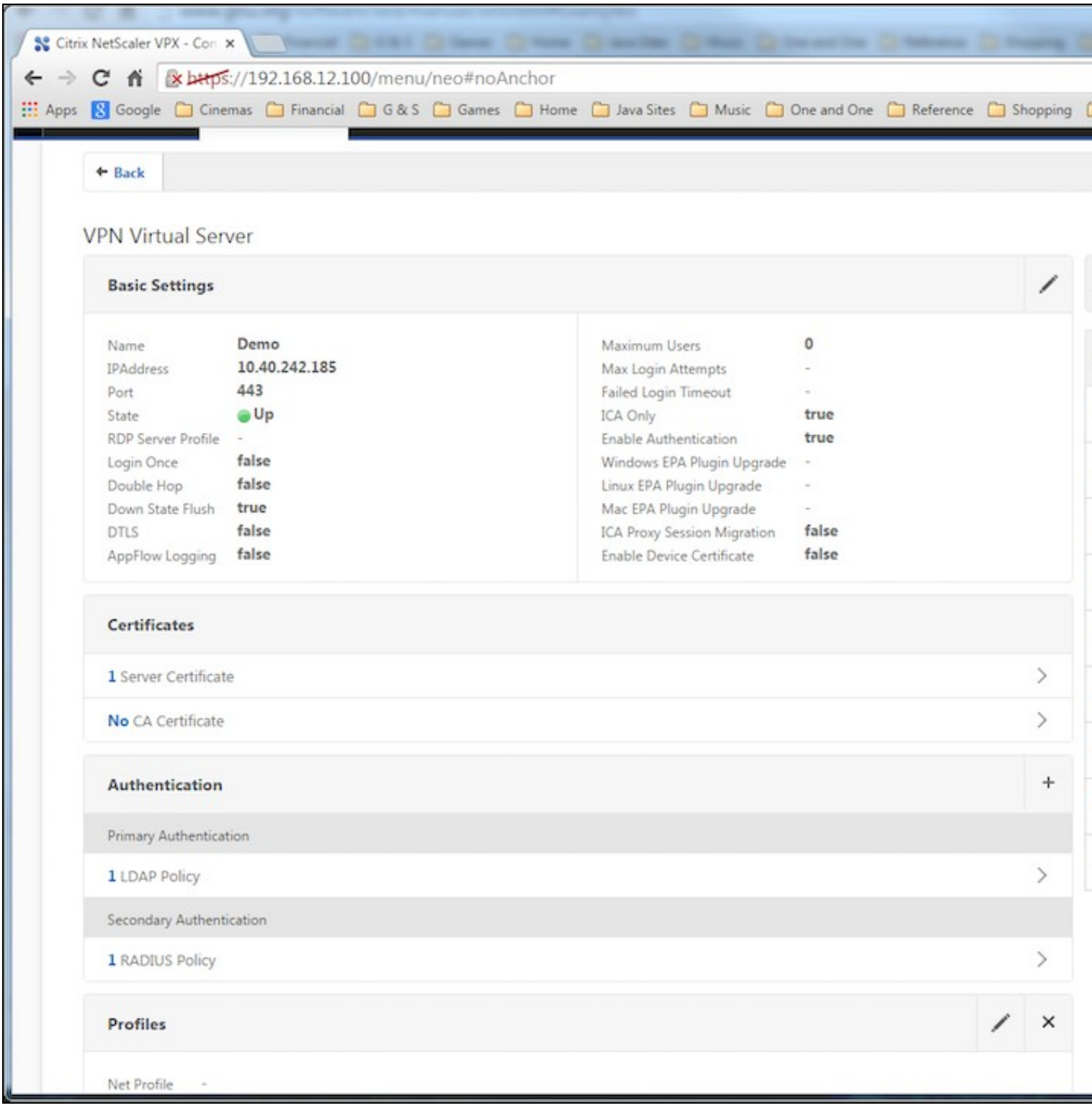
Name Swivel RADIUS Policy

Server Swivel RADIUS

Expression select "ns_true" under Saved Policy Expressions



The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.



173.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

174 Additional Configuration Options

174.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

174.2 Netscaler SSL Bridge

The Netscaler allows a SSL Bridge to be created that allows a Network Address Translation to allow access to the Swivel instance to provide single channel images or Mobile App security strings. On the Netscaler Gateway Administration Console Configuration tab select Traffic Management -> Load Balancing -> Virtual Servers, then click on Add, to open a Create Virtual Server (Load Balancing) window.

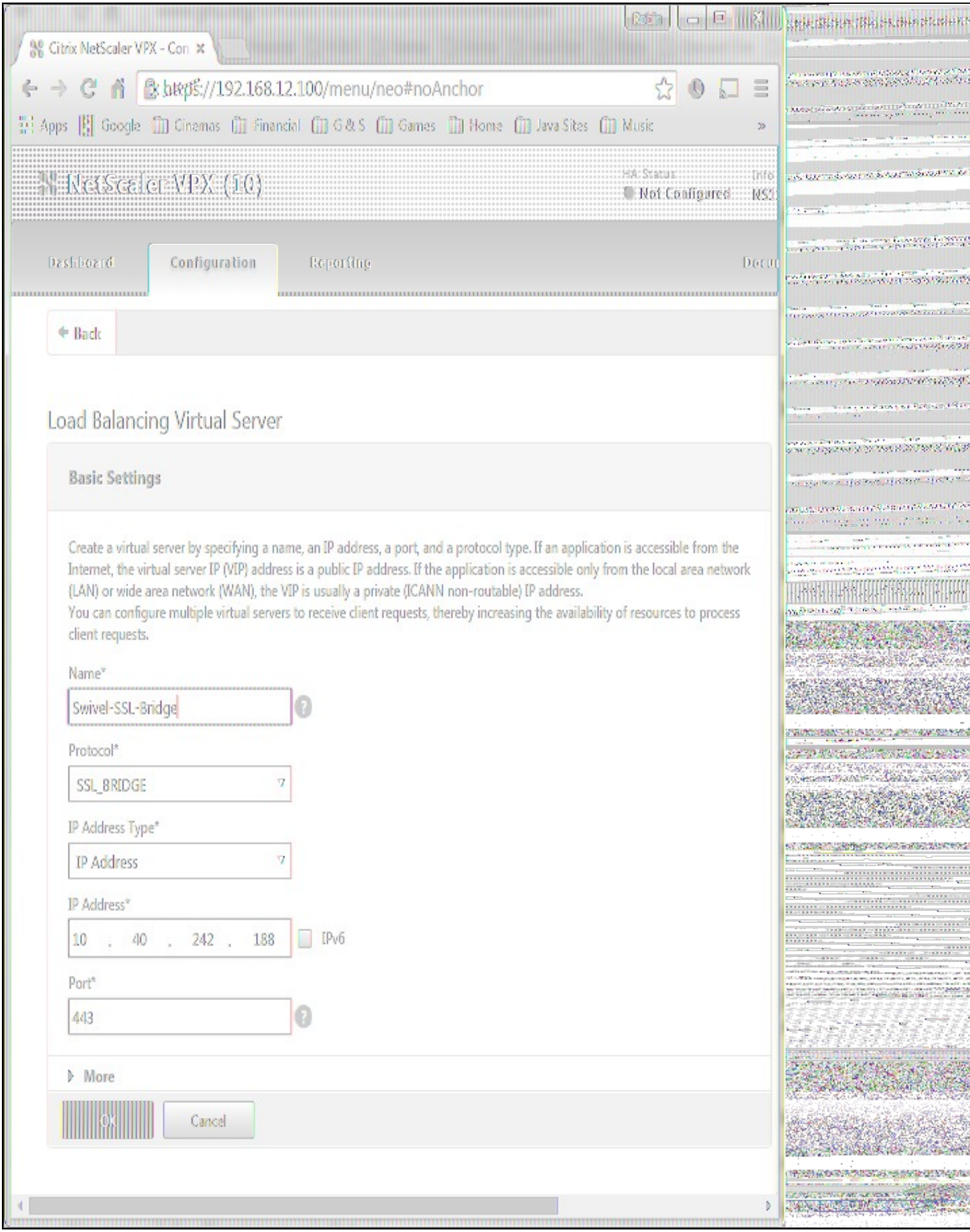
Name Name of the SSL Bridge

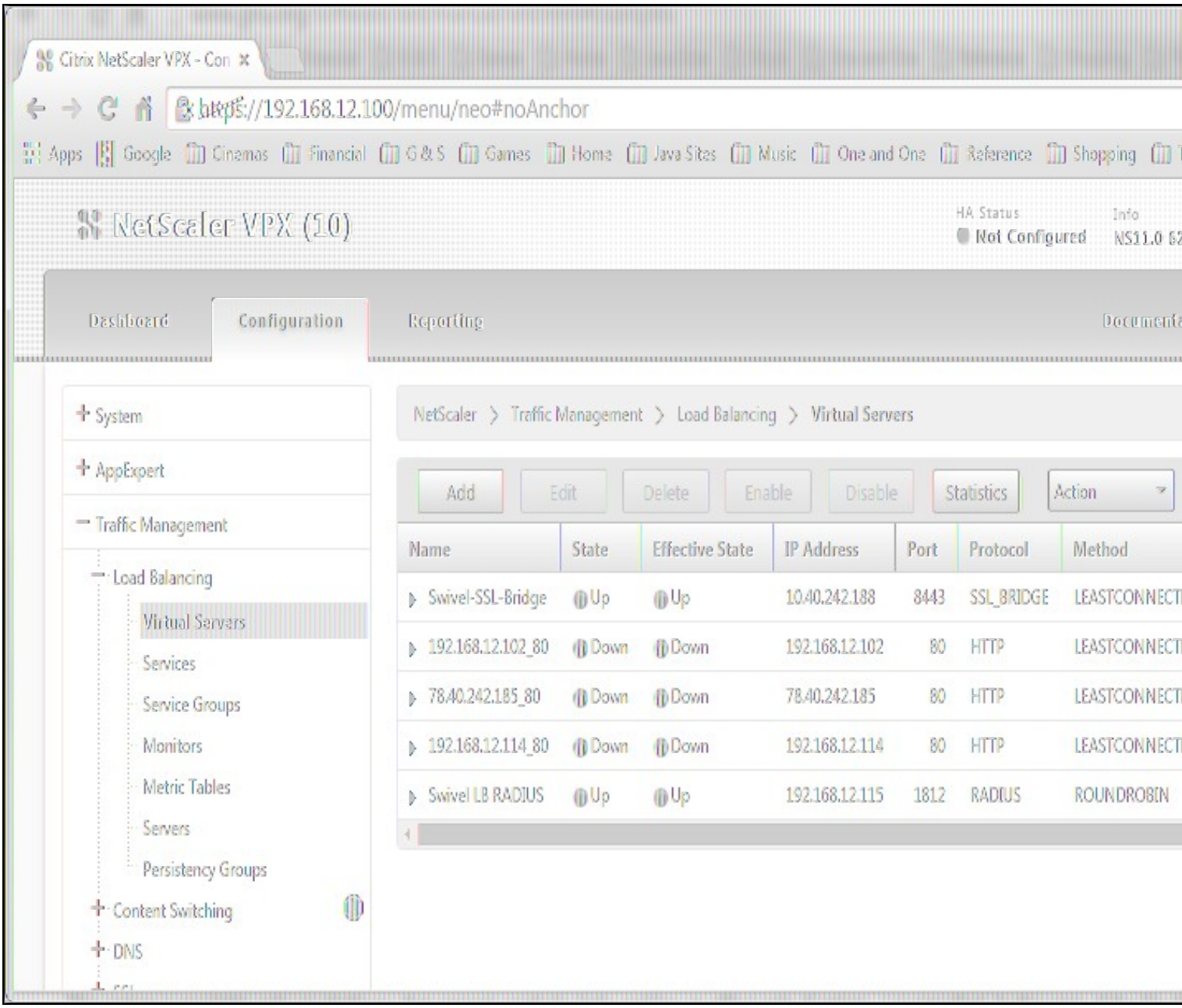
Protocol select SSL_Bridge

Select IP Adress Based

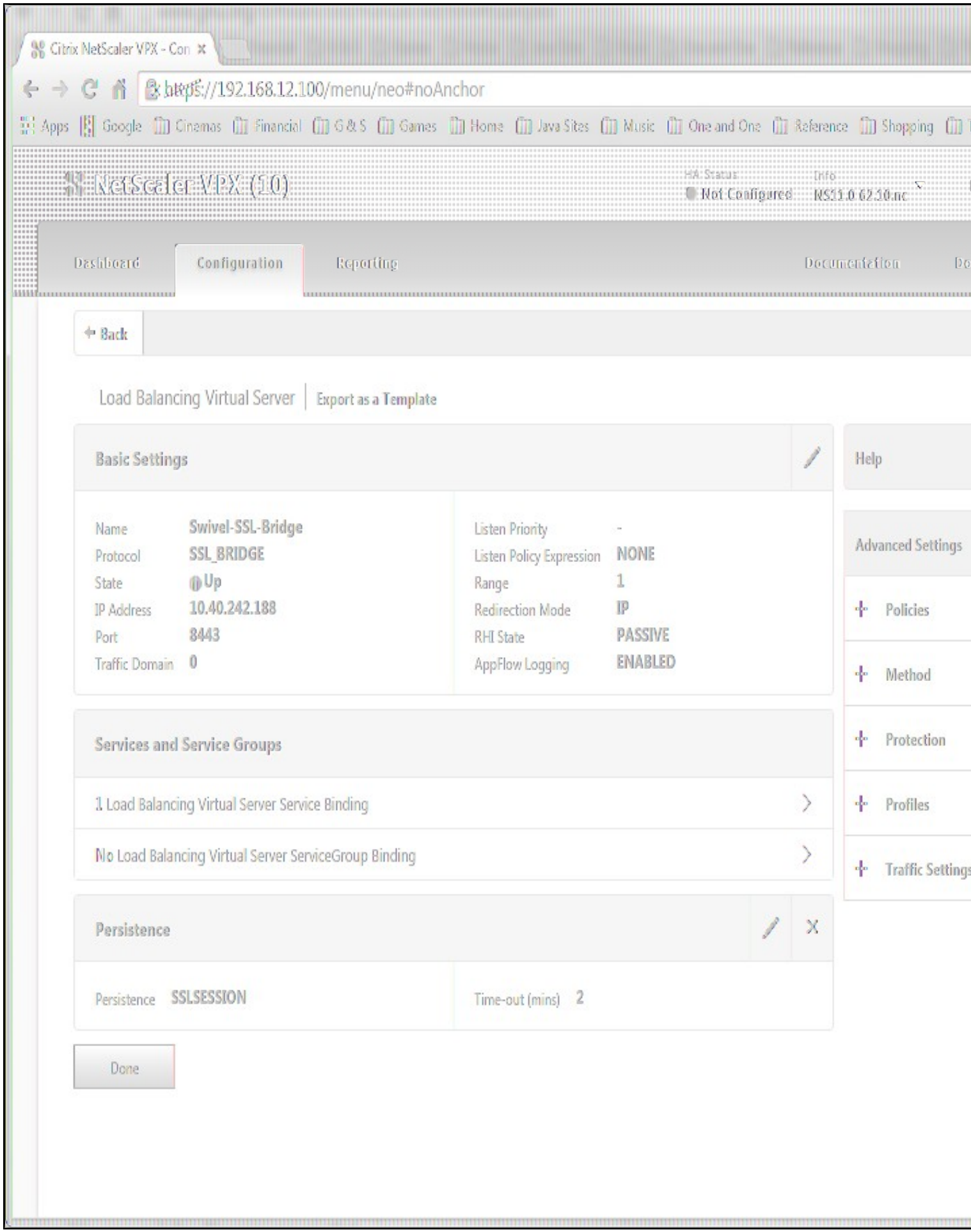
IP address Enter the public IP Address

Port Enter the internet-facing port number, usually 443

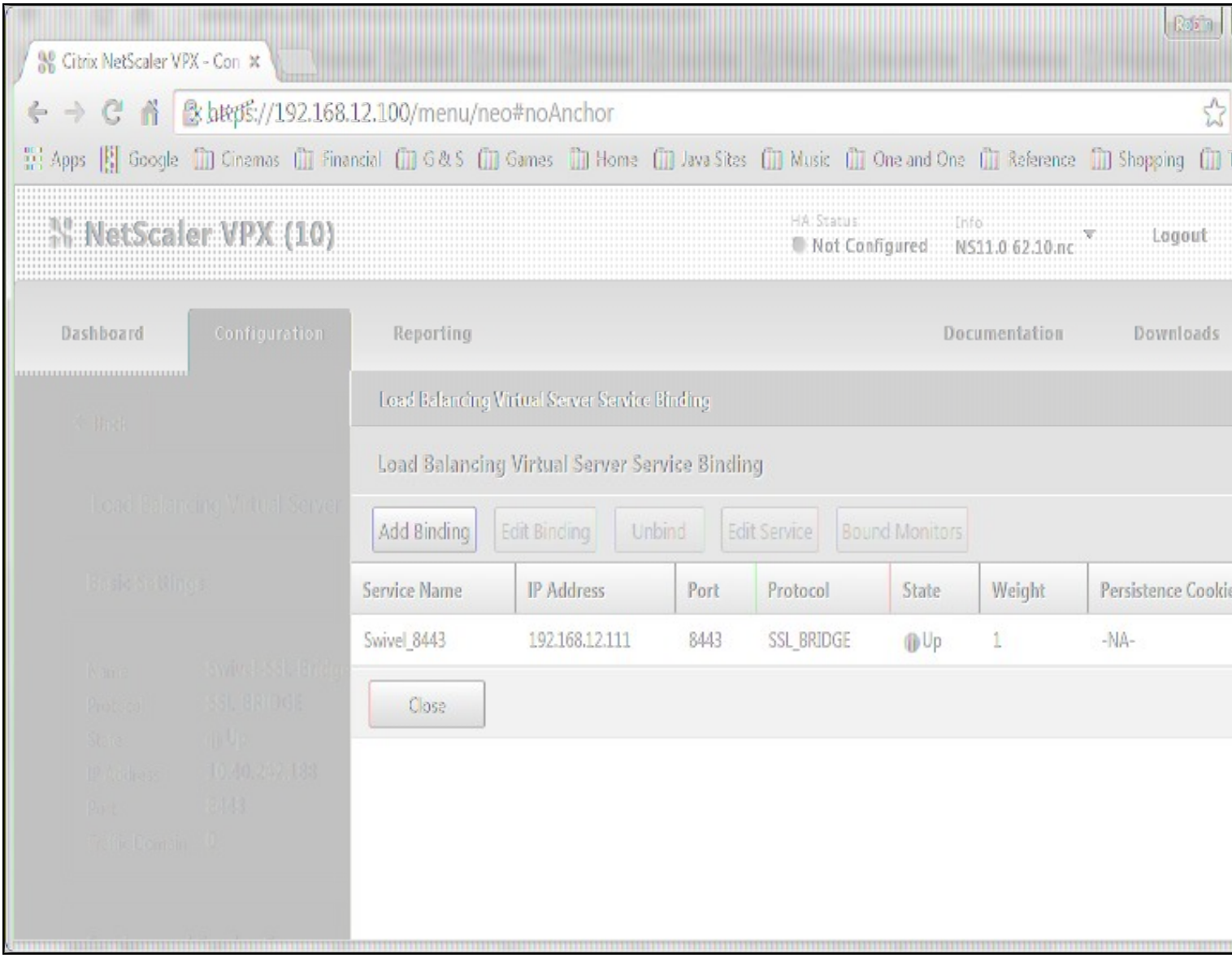

Citrix NetScaler VPX - Con
https://192.168.12.100/menu/neo#noAnchor
Apps
Google
Cinemas
Financial
G & S
Games
Home
Java Sites
Music
NetScaler VPX (10)
HA Status
Not Configured
Info
NS1
Dashboard
Configuration
Reporting
Back
Load Balancing Virtual Server
Basic Settings
Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.
Name*
Swivel-SSL-Bridge
Protocol*
SSL_BRIDGE
IP Address Type*
IP Address
IP Address*
10 . 40 . 242 . 188
IPv6
Port*
443
More
OK
Cancel



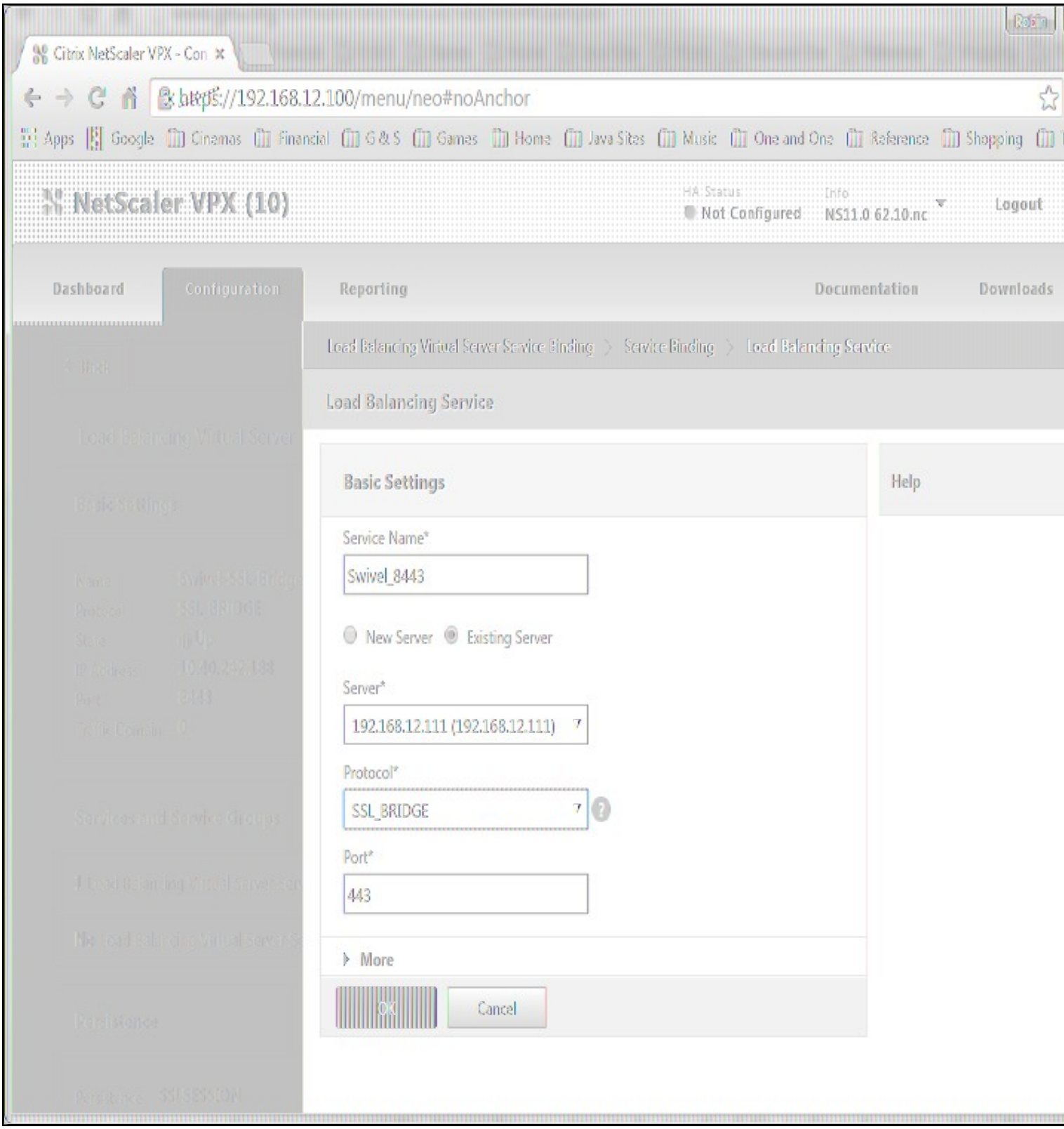
After creating the virtual server, select it and then Edit


Citrix NetScaler VPX - Con
https://192.168.12.100/menu/neo#noAnchor
Apps
Google
Cinemas
Financial
G & S
Games
Home
Java Sites
Music
One and One
Reference
Shopping
NetScaler VPX (10)
HA Status
Not Configured
Info
NS11.0 62.10.nc
Dashboard
Configuration
Reporting
Documentation
Back
Load Balancing Virtual Server
Export as a Template
Basic Settings
Name Swivel-SSL-Bridge
Protocol SSL_BRIDGE
State Up
IP Address 10.40.242.188
Port 8443
Traffic Domain 0
Listen Priority -
Listen Policy Expression NONE
Range 1
Redirection Mode IP
RHI State PASSIVE
AppFlow Logging ENABLED
Help
Advanced Settings
Policies
Method
Protection
Profiles
Traffic Settings
Services and Service Groups
1 Load Balancing Virtual Server Service Binding
No Load Balancing Virtual Server ServiceGroup Binding
Persistence
Persistence SSLSESSION
Time-out (mins) 2
Done

Select "Load Balancing Virtual Server Service Binding"



Now click "Add Binding", then under "Select Service", click "+"



Service Name Name of the SSL Bridge

Select "New Server" and enter the IP address of the Swivel server.

Protocol select SSL_Bridge from the drop down menu

port select the port used to connect to Swivel server, usually 8443 for the proxy application.

From the Monitors tab select TCP then Add it to the list of Configured so that it appears on the right hand side with the State box checked., then click on Create.

174.3 Login Page Customisation

This step only needs to be followed if login page customisation is required. Many of the steps described below are derived from the following articles:

This article describes creating a custom theme on NetScaler 10.x:

http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-connect-users-wrapper-con/ng-connect-users-cr-integration-con/ng-connect-custom-theme-page-tsk.html

This article describes the additional steps required for NetScaler 11:

http://discussions.citrix.com/topic/367268-netscaler-11-custom-theme/ - item #13.

Thanks to the originators of these articles.

Update: we recommend using rewrite / responder actions to customise the login page, as suggested by Stuart Carroll in the Additional Information section. We have adapted and updated his original solution, which is now available in the NetScaler 12 article. Despite the name, it will also work with NetScaler 11.

174.3.1 Using Existing Customisations

If you already have a customisation including Swivel TURing or PINpad, from version 10.x, it may still work with version 11. Results are mixed on this. However, the customisations described on these articles are based on the assumption that you are starting from the default or green bubble theme for version 11. They will not work if you are starting from a 10.x theme. In this case, you should start from one of the built-in themes for version 11 and customise those.

174.3.2 First Steps

Follow these steps whether you plan to use a pre-built theme or to customise your own theme.

Citrix recommend when upgrading a Netscaler with custom pages, the custom pages should be set back to use default pages, upgrade and then the custom pages reapplied. When upgrading it is recommended to make a backup or snapshot of the existing system.

When upgrading a Netscaler 10.1 or 10.5 with custom pages to 11.0, backup the modified pages and scripts, then set the login page back to default. Upgrade, test the Administration console, then upload the modified pages as if carrying out a new Swivel install as given below, then recreate the custom tar file as below as this will then include the updated GUI.

Similarly, we recommend that you select the Default theme initially, before starting the customisation.

Ensure that the folder for the custom theme exists:

- Log on to the NetScaler Gateway command line and enter the following commands:

```
shell
mkdir /var/ns_gui_custom
```

You may get the response "File exists".

Copy the theme files for either the Default or Green Bubble theme using the following commands:

```
cd /var/netscaler/logon/themes
cp -r Default Custom
```

or for the Green Bubble theme

```
cp -r Greenbubble Custom
```

If you are using one of the ready-made themes linked above, skip to the section Deploying a Ready-Made Theme. If you are customising an existing theme, continue to the next section.

174.3.3 Customising an Existing Theme

174.3.3.1 Preparing the Custom Theme

Assuming that you have copied the appropriate theme as described in First Steps, select the Custom theme in order to ensure it is deployed. The files you need to modify will now be in /var/netscaler/logon/themes/Custom. Prepare the new custom theme as follows:

```
tar -cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/*
```

Now use the NetScaler administration console to select the custom theme: select NetScaler Gateway -> Global Settings, then click on Change Global Settings, select the Client Experience tab, and at the bottom of the tab, switch the UI Theme to Custom.

174.3.3.2 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

174.3.3.3 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /var/ns_gui_custom/ns_gui/vpn
cp index.html index.html.bak
cd js
cp gateway_login_form_view.js gateway_login_form_view.js.bak
```

174.3.3.4 Customise the login script

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Windows-based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

It is assumed that your custom theme has already been deployed under /var/ns_gui_custom/ns_gui. As noted above, it is also assumed that the theme is based on one of the built-in version 11 themes. If you have a version 10.x customisation that you cannot get to work with version 11, please contact support@swivelsecure.com for further advice.

Download the customised files from the pre-requisites above. This contains 5 files, in the appropriate folders:

- /vpn/index.html - a replacement for the existing file, containing additional lines to insert the swivel files below
- /vpn/js/gateway_login_form_view.js - a replacement for the existing file, containing a single additional line, which calls a script from swivel.js to insert the customisation.
- /vpn/js/swivel.js - a new file, containing the JavaScript to insert the customisation
- /vpn/images/swivel.css - a new file, containing the stylesheet for the Swivel customisation
- /vpn/images/pinpadBlank.png - an optional blank image for the PINpad buttons.

Before you copy these files across, you will need to modify the first part of swivel.js as shown here:

```
// Set this to be the correct URL for the required image.
var swivelUrl = "https://citriximage.swivelsecure.com/proxy/";
// Set this to "turing" or "pinpad". Anything else will result in no image.
var swivelImageType = "pinpad";
// Set this to the ID of the password field to populate: "passwd" or "passwd1"
var pinpadField = "passwd1";
```

- swivelUrl should contain the public URL for your image. Do not add "SCImage" or "SCPinPad" - this will be done for you.
- swivelImageType should be "turing" or "pinpad" as described
- pinpadField defines which password field should be filled by the PINpad buttons. If Swivel is the primary authentication, use "passwd", or for secondary authentication use "passwd1".

174.3.3.5 Customise the OTC field and TURing image button text

This is an optional step.

Modify the language resource files in /netscaler/logon/themes/Default/resources. If you are only using the English language, then edit en.xml and search for

```
<Partition id="logon">
```

Just below this, look for

```
<String id="Password2">Password 2</String>
```

Replace "Password 2" with "OTC".

If you want to change the label on the TURing button, insert a new line just below this:

```
   <Property id="New_Turing" property="value">New Image</Property>
```

Replace "New Image" with the appropriate text.

If you want to change the label on the PINpad refresh button, insert the following line:

```
   <Property id="Refresh_Pinpad" property="value">Refresh</Property>
```

Replace "Refresh" with the appropriate text.

174.3.3.6 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, following the pattern above.

174.3.3.7 Upload files to Netscaler

Download the files under the prerequisites and modify as described above, then copy them to the appropriate locations under /var/ns_gui_custom/ns_gui.

174.3.3.8 Create the boot archive file

```
cd /var/ns_gui_custom
tar -zcvf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*
```

This should create the customtheme.tar.gz file used at boot time, and list all the files used.

174.3.3.9 Select the custom theme

- Log on to the NetScaler Administration Console and select the "Custom" theme.
- Save customisation changes.

174.3.3.10 Create Backup and Script to Deploy Files

Once you have a working configuration, you should back up the modified files to a suitable location off the NetScaler. It is recommended that the backup directory structure reflects the deployed structure - e.g. put the .js files in a js subdirectory, and the .css file(s) in a images subdirectory. This makes it easier to carry out the next step.

As NetScaler often replaces files after a reboot, you also need to take precautions to ensure the custom files are restored after a reboot. To do this, you need to copy the backups you just created into a folder on the NetScaler: the recommended location is to create a folder "custom" under /var/mods. As described above, the directory structure under custom should reflect the directory structure under vpn.

To restore these files on reboot, you need to edit the file /nsconfig/rc.netscaler. Insert the following line at the beginning of the file:

```
cp -r /var/mods/custom/* /var/netscaler/ns_gui/vpn/*
```

This assumes that your web directory is /var/netscaler/ns_gui - modify accordingly.

174.3.3.11 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time and that the login page has been modified as required.

The following section can be skipped if you are customising an existing theme.

174.3.4 Deploying a Ready-Made Theme

These instructions assume you are using one of the pre-built themes listed above.

- Copy the chosen theme to /var/ns_gui_custom. We recommend WinSCP to copy the files, but any suitable file transfer file will do.
- Go to /var/netscaler/logon/themes/Custom/resources and edit en.xml (again, you can use WinSCP for this):
  - ♦ Search for "Password2"
  - ♦ If required, change the text for <String id="Password2"> to "OTC":

```
<String id="Password2">OTC</String>
```

- ♦ Insert a new line below this:

```
<String id="SwivelUrl">https://swivel.mycompany.com/proxy/</String>
(Substitute the public URL for your Swivel images (TURing or Pinpad) in the above.)
```

- ♦ Save the file.
- ♦ If you need to support multiple languages, repeat this process for all supported language files.
- Log on to the NetScaler Administration Console and select the "Custom" theme.
- Save customisation changes.

If you prefer, as an alternative to inserting the Swivel URL in the resources file(s), you can manually modify swivel.js, as described below. However, if you do this, you will also need to rebuild the custom theme, again as described above.

174.4 Additional Login Customisation options

174.4.1 Requesting the String Index

See also Multiple Security Strings How To Guide

To request the string index, use the "turing" option.

Modify swivel.js. Search for the following line:

```
swivelUrl += "/SCImage?username=";
```

Replace "SCImage" with "DCIndexImage".

174.4.2 Requesting an SMS

See also Challenge and Response below

To request an SMS on demand, use the "turing" option.

Modify swivel.js. Search for the following line:

```
swivelUrl += "/SCImage?username=";
```

Replace "SCImage" with "DCMessage".

174.4.3 One Touch

DISCLAIMER: the following One Touch solution is based on NetScaler 10.5, and has not yet been tested on version 11.

One touch is a different approach as the user is redirected to a separate page to authenticate and therefore does not actually see the Netscaler login page.

Refer to VPN_OneTouch_Integration

To customise the page for one touch you need to include the following in the header section of index.html where <swivelappliance> is the hostname of the associated Swivel Appliance

```
//-->
//-> Swivel elements
function redirect(){
window.location.replace("https://<swivelappliance>:8443/onetouch/onetouch?returnurl=" + 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];
      //  alert(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;
        //alert(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"];

if(typeof passwordPassedIn == 'undefined') {
 redirect();
} else {
$('[name=passwd]').val(passwordPassedIn);
$('[name=login]').val(usernamePassedIn);
 //alert("GO " + usernamePassedIn);
 document.getElementsByName("vpnForm")[0].submit();

 }
});
```

Before the closing </SCRIPT> tag

174.5 Challenge and Response

To use two-stage authentication - also known as challenge and response - you will need these custom files. These files are for the Green Bubble theme: for different themes, see the detailed customisation section below. Also note that these files only support TURing in the second stage: for other options, see below.

See Challenge and Response How to Guide for details on setting up challenge/response on the Swivel server. In particular, note that the option "Send username with challenge" must be set to "Yes" to use single-channel challenge-response, so if your version of the Swivel software is too old to have that option, you will need to upgrade in order to use challenge-response with TURing.

174.5.1 Customisation

See above for details on where the custom files need to be put. Always take backups of the original files before making any changes. If you are using dual channel, you may not need to make any of these changes: see comments below.

You should always download the custom files linked above, even if you are not using the Green Bubble theme with TURing, as you will need the file swivel.js at least. This should be put in the js folder. The other files that need to be changed are index.html, nsshare.js and js/gateway_login_form_view.js.

The only change to index.html is to insert a single line:

```
<script type="text/javascript" src="/vpn/js/swivel.js"></script>
```

somewhere in the <head> section.

The only change required to gateway_login_form_view.js is as follows:

Locate the following line:

```
 changePage();           // Prefill names if cert auth
```

Insert before it the following line:

```
 customLoginPage(form);
```

This calls a function from swivel.js to add the Swivel customisation to the first login page. This hides the Swivel password field, and copies the first password field to it before submitting the page. This assumes that you are using the "Check repository password" option. If you don't want to use that, don't make this change.

The second login page is rendered by nsshare.js, so you need to make the following changes to it, only if you want to show TURing in the second page. In the custom files, these are inserted before the DialogInclude function, but they can go anywhere in the file:

```
 // Alter this URL as appropriate.
 var swivelUrl = "https://citriximage.swivelsecure.com/proxy/SCImage?username=";

 function showTuring(sUser) {
   if (sUser!="") {

     // Find the image field.
     var varImg = document.getElementById("imgTuring");

     // Set the image SRC and make it visible
     varImg.src = swivelUrl + sUser + "&random=" + Math.round(Math.random()*100000);
     varImg.style.display = "";

   }

 }

 function showTuringImageChallenge() {
   var challengeDiv = document.getElementById("dialogueStr");
   if (challengeDiv) {
     var challenge = challengeDiv.innerHTML;
     var colonPos = challenge.lastIndexOf(":");
     if (colonPos > 0) {
```

```
      var username = challenge.substr(0, colonPos).trim();
      challenge = challenge.substr(colonPos+1);
      challengeDiv.innerHTML = challenge;
      showTuring(username);
    }
  }
}
```

Then, in the function DialogueBodyII, look for

```
  ln += '<tr><td class="dialogueSubmitCell" style="float:left">';
```

and insert the following line before it:

```
  ln += '<tr><td><img id="imgTuring" style="display:none" /></td></tr>';
```

Then, at the end of DialogueBodyII, insert the following line:

```
  showTuringImageChallenge();
```

If you are unclear about any of these changes, they are clearly labelled in the custom files provided.

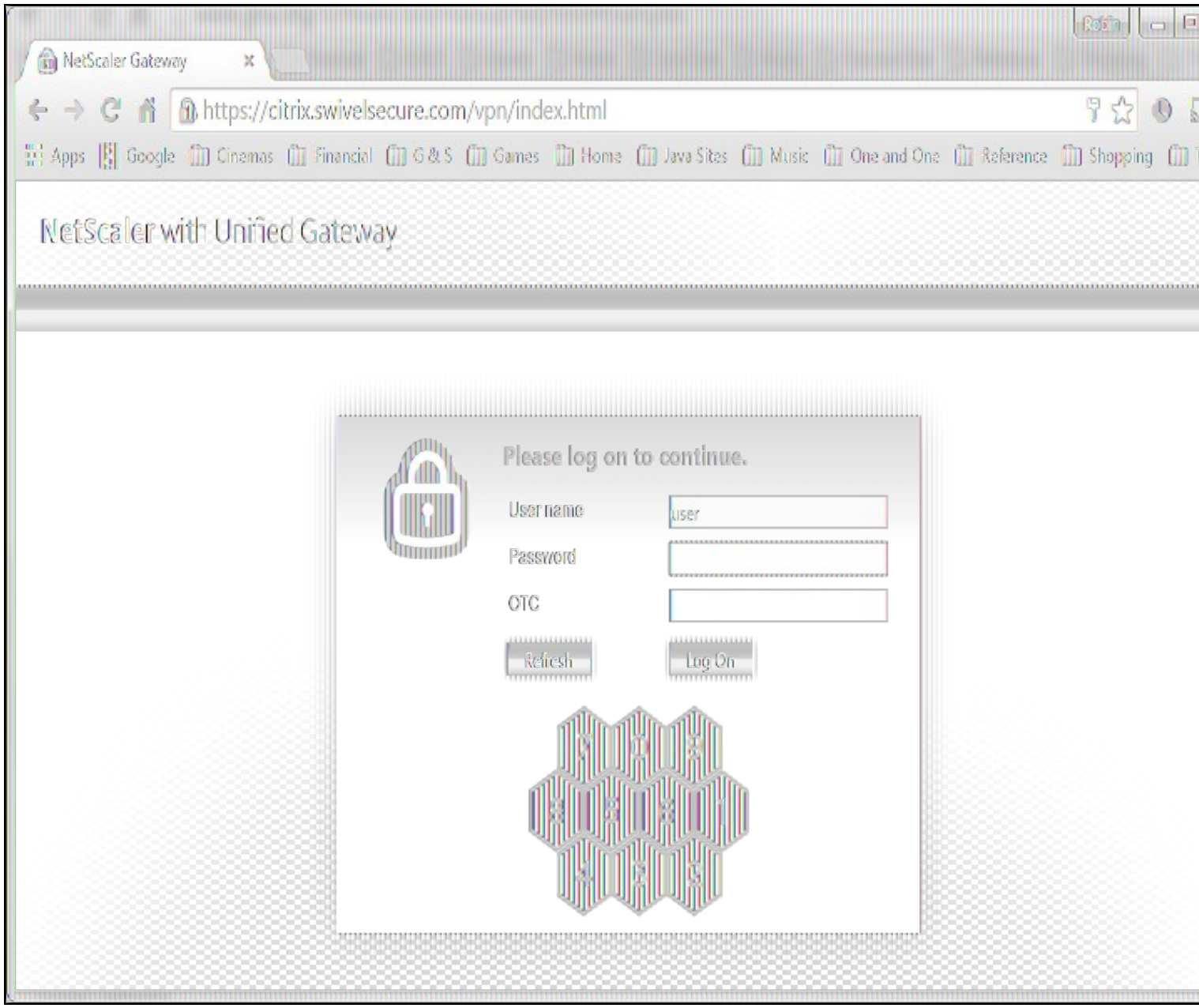
174.6 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

175 Testing

Browse to the login page and check that a TURing or PINpad image appears and the One time Code can be entered to login.



176 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

177 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

177.1 Error Messages

Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

Username field length incorrect

If the username field is too short it can be increased. Edit the index.html file and locate the below section setting the size="40"

<td align="right" style="padding-right:10px;white-space:nowrap;"></td> <td colspan=2 style="padding-right:8px;"><input id="Enter user name" class="CTXMSAM_ContentFont" style="font-size: 8pt" type="text" title="" name="login" size="40" maxlength="127" onFocus="loginFieldCheck()" style="width:100%;" /></td>

login command failed over API. Reason: Response not of type text/xml: text:html

This error can be seen on the Netscaler Administration console when upgrading with a custom theme. This will preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

Look for the line containing -UITHEME CUSTOM and change it to DEFAULT as below:

```
set vpn parameter -localLanAccess ON -defaultAuthorizationAction ALLOW -proxy BROWSER -clientCleanupPrompt OFF -forceCleanup none -clientOp
```

After making the changes, reboot the system to login.

178 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

Potential File Locations:

/netscaler/ns_gui/vpn

/var/ns_gui/vpn

/var/ns_gui_custom/vpn

/var/netscaler/gui/vpn

179 Additional Information

NOTE: there is an alternative solution to this that uses the NetScaler rewrite feature, and so doesn't require you to make changes to any files. It also has the advantage that it can be applied selectively. Many thanks to Stuart Carroll for finding this approach:

http://www.stuartc.net/blog/tech/netscaler-11-0-swivel-integration-using-netscaler-rewrite/

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

180 Citrix Netscaler Gateway 12

181 Introduction

This article covers how to adjust an integration between pinsafe protocol and Citrix Netscaler Gateway 12.

Swivel can provide Two Factor authentication with SMS, Token, and Mobile Phone Client and strong Single Channel Authentication with TURing or Pinpad, or in the Taskbar using RADIUS. For all the methods which do not require an image at the article Citrix_Netscaler_Gateway_11 covers them.

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad. Both the authentication methods need an image for which there are a set of rules to be applied. This document covers the application of those rules through the NS command line.

181.1 Integration Architecture

Swivel Secure ? Radius ? Nas ? Netscaler ? login page ? AD ? login customised page

182 Turing Image Integration

This solution uses the NetScaler Rewrite and Responder features: please make sure these features are enabled before proceeding. The custom actions and policies can be added through the web administration console, but we provide them below as NetScaler shell commands.

This solution will work with NetScaler 11 as well, and is recommended in preference to the previous article.

You can customise the labels from the web console. Under NetScaler Gateway, select Portal Themes, then the theme you are using, and Edit. On the right, click Logon Page, and the text can be edited there.

There is need to have a valid certificate for the turing image to appear. As a trial you can try a self signed certificate that is trusted by the host: cd /usr/local/share/ca-certificates/swivel.crt

It has been reported that the rewrite and responder actions used for version 11 do not work with the latest release of version 12. Below is an updated set of actions & policies that need to be installed. Before you install them, edit the responder action and change the URL following pinsafeUrl to the correct URL for your TURing. You don't need the "SCImage" part - that will be added automatically.

To install the rules, you need to open a command prompt on the NetScaler. You can just paste the entire file contents to the shell window. Once you have installed them, they have to be bound to a virtual server. There isn?t a script for that as it will be different for each installation. It's easiest to do this right at the netscaler?s web admin console.

182.1 Rewrite Rules

Copy the lines from the text below to a text editor: note that each action should be on a single line. Edit the URL as described above, then copy and paste the result into your NetScaler?s command line. Be sure to have complete lines without additional spaces or line breaks.

The action Act_Sentry_Username_Blur and the associated policy is optional, and shows the TURing image as soon as you tab away from the username. If you prefer users to click a button to get the image, then do not include this action/policy.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri

add rewrite action Act_Sentry_Mod insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=$('<div></div>').addClass('field').add

add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_

add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search

add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho

add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js

add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Mod

add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_Append

add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA

add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur

add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox

add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

182.1.1 Binding the applied rules

This is done at the netscaler GUI.

Select the virtual server you are going to use, and edit it. Scroll down to the Policies section and click "+". Select Responder policy, then click Continue. Click "Add Binding" and select the policy "ResPol_pinsafe.js". Click Bind. Click Close, then click + again. This time, select "Rewrite" as the policy, and "Response" as the type. Click "Add Binding" and then select the rewrite policies just added, one at a time. After each one, make sure the GOTO expression is "NEXT", to ensure that all policies are executed. This doesn?t apply to the responder policy. In the end there should be 5 rewrite policies in total (4 if you don't want automatic TURing), and one responder policy. It doesn't matter which order you add them.

The last thing you will need to do is to persuade NetScaler not to use the cached version of its JavaScript. Go back to the command prompt, and open a shell. The following have been tested successfully for Netscaler?s web files, and we recommend trying both to ensure the result:

cd /netscaler/ns_gui/vpn/js

cd /var/netscaler/gui/vpn/js

After getting to those locations apply touch as Netscaler seems to cache JavaScript files.

```
touch gateway_login_form_view.js
```

You should now get the TURing image embedded into the login page.

182.2 Green Bubble Theme

Use the following rules for the Green Bubble theme.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri

add rewrite action Act_Sentry_ModGB insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_image=$(\"<div></div>\").attr({'id':'divTur

add rewrite action Act_Sentry_AppendEULAGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_image)\"" -se

add rewrite action Act_Sentry_AppendGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_image)\"" -search "text(\"form

add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho

add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js
```

```
add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModGB
add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_AppendGB
add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULAGB
add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur
add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox
add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

The action names have been changed, so that you can have actions for multiple themes in the configuration and simply change the policies to point to the appropriate actions.

182.3 RfWebUI theme

Unfortunately, the RfWebUI theme doesn't support responder actions. Instead, you have to replace the file script.js with the one below, or if it is already modified, add the attached scripts to the existing file.

The file can be found under /var/netscaler/logon/themes/RFWebUI/. If you have copied the original RFWebUI theme, the last part of the path will be whatever the new theme is named as.

As with other customisations, you will need to modify the first line to set swivelUrl to the correct public URL for your system.

Customised script.js

182.4 X1

Here are the actions and policies for the X1 theme. Only one action needs to be changed here.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri
add rewrite action Act_Sentry_ModX1 insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=$(\"<div></div>\").addClass('field')
add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_
add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search
add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho
add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js
add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModX1
add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_Append
add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA
add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur
add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox
add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

183 Pinpad Integration

The following document provides the rules which need to be applied for Pinpad integration. Before applying the responder action you'll need to edit the url for the swivel server to match yours: swivel.mycompany.com:8443/proxy/SCPinPad.

Be sure you have 2 rewrite actions (one of which is big), 2 rewrite policies, 2 responder actions and 2 responder policies. Avoid adding extra spaces when copying the rules onto the netscaler's shell.

```
add rewrite action ReAct_pinpad_js insert_before_all "HTTP.RES.BODY(12000)" q{"\r\n<script type=\"text/javascript\" src=\"/vpn/pinpad.js\"></

add rewrite action ReAct_Insert_Pinpad replace_all "HTTP.RES.BODY(1000000)" q|"form.append(field_errormsg);\r\n\tvar refresh_button=$(\"<inpu

add rewrite policy RePol_pinpad_js "HTTP.REQ.URL.EQ(\"/vpn/index.html\")" ReAct_pinpad_js

add rewrite policy RePol_Insert_Pinpad "HTTP.REQ.URL.EQ(\"/vpn/js/gateway_login_form_view.js\")" ReAct_Insert_Pinpad

add responder action ResAct_pinpad.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinpadUrl=\\\"https://swivel.mycompany.com:8443/proxy/SC

add responder action ResAct_pinpad.css respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"div.pinpadHidden { display : none; }\r\n\"+\"div.pinpadVisi

add responder policy ResPol_pinpad.js "HTTP.REQ.URL.EQ(\"/vpn/pinpad.js\")" ResAct_pinpad.js

add responder policy ResPol_pinpad.css "HTTP.REQ.URL.EQ(\"/vpn/pinpad.css\")" ResAct_pinpad.css
```

184 Delete previous rules

The optimal option is to unbound all the rules through the NS GUI and after delete them. Also bear in mind the need to touch the .js files mentioned throughout the article as NS caches the previous versions - so changes might not be visible or immediately available.

185 Adjust Buttons at the login page

For further adjustments of the login page read the following section. Bear in mind X1 theme allows a quick editing of some features so the following might not apply. Normally the login page can be slightly edited, we are not going onto details regarding aesthetics and branding but only renaming of some sections which report to this integration.

185.1 Edit Password to OTC

The example below describes the use of the english language at the login interface.

> shell root@VLABSRV0# cd /var/netscaler/logon/themes/Default/resources root@VLABSRV0# chmod +w en.xml root@VLABSRV0# vi en.xml

```
[change word directly ? beginning of the word - cw ? write ? escape - :wq!]
```

ng> <String id="User_name">User name</String> <Property id="Enter user name" property="title">Enter user name</Property> <String id="Password">OTC</String> <String id="Password2">Password 2</String> <String id="Enter password">Enter password</String> <Property id="Log_On" property="value">Log On</Property> <String id="You need to enter login name">You need to enter login name</Stri ng> <String id="You need to enter passwd">You need to enter a password</String> * <String id="Enter_password2_Alert">You need to enter the second password </String> <String id="domain">Domain</String> <String id="eula_title">End User License Agreement</String> <String id="eula_agreement">I accept the </String> <String id="terms">Terms & Conditions</String> <String id="errorMessageLabelBase">errorMessageLabel</String> <String id="eulaback">Back</String> <String id="errorMessageLabel4001">Incorrect credentials. Try again.</String > <String id="errorMessageLabel4002">You do not have permission to log on at t his time.</String> <String id="errorMessageLabel4003">Cannot connect to server. Try connecting en.xml: 597 lines, 51853 characters. root@VLABSRV015# exit shell

- You can also change ?You need to enter a password? to ?You need to enter an OTC?. We recommend avoiding obvious naming, mainly as a security measure.

186 Troubleshooting

If the logging in is not working please check the certificate and if the netscaler as the same valid certificate. Also if there as been made any change to the ip?s check if there is a firewall blocking the content.

It has been reported that sometimes the JavaScript file gets cached. To resolved this you should touch gateway_login_form_view.js and try to log after. NetScaler tends to cache JavaScript files, and doesn't detect changes made by rewrite rules. You have to force it to refresh its cache.

If the pinsafe.js file is coming through OK it means that some of the rules are working.

For further assistance please write to supportdesk@swivelsecure.com

187 Netscaler Upgrade from 11 to 12

As recommended by CITRIX, for previous versions the upgrade should be made gradually, eg from NS 11.0 to NS 11.1 prior to get to NS 12. The upgrade should be easily done through the NS GUI but if you bump into trouble the CLI upgrade version is also easy.

Download the build file from Citrix page, Netscaler Gateway 12, upload it to /flash through Filezilla/WinSCP. Example below:

soc@support ~ $ ssh nsroot@10.10.10.21 > save config > shell root@VLABSRV0# cd /nsconfig root@VLABSRV0# cp ns.conf ns.conf11.ns root@VLABSRV0# cd /var/nsinstall

root@VLABSRV0# mkdir nsinstall12 root@VLABSRV0# cd nsinstall12 root@VLABSRV0# mv /flash/build-12.0-53.13_nc_32.tgz . root@VLABSRV0# tar -xvzf build-12.0-53.13_nc_32.tgz (...) root@VLABSRV0# ./installns installns: [36026]: VERSION ns-12.0-53.13.gz (...) installns: [36026]: installns version (12.0-53.13) kernel (ns-12.0-53.13.gz)

The Netscaler version 12.0-53.13 checksum file is located on http://www.mycitrix.com under Support > Downloads > Citrix NetScaler. Select the Release 12.0-53.13 link and expand the "Show Documentation" link to view the SHA2 checksum file for build 12.0-53.13.

There may be a pause of up to 3 minutes while data is written to the flash. Do not interrupt the installation process once it has begun.

Installation will proceed in 5 seconds, CTRL-C to abort Installation is starting ... installns: [36026]: Installation is starting ... installns: [36026]: detected Version >= NS6.0 installns: [36026]: Installation path for kernel is /flash (...) installns: [36026]: Installing Linux EPA and Linux EPA version file... (...) Installation has completed. Reboot NOW? [Y/N] Y Rebooting ? installns: [36026]: Rebooting ...

188 nFactor ? Customizing UI to Display Images

Please also check the following article at the Citrix website: https://support.citrix.com/article/CTX225938

189 Backup Configuration

We'd also recommend backing up the configuration in case after a reboot the configuration gets messed up:
https://ogris.de/howtos/netscaler-restore.html

190 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

191 Introduction

Citrix 10.5 allows the RADIUS to be monitored and load balanced in a number of ways. Earlier versions such as 10.1 also have this capability but have different configuration screens.

Where Swivel Single Channel Sessions (TURing, Pinpad), and SMS by On Demand Authentication and Mobile Provision Codes, it is expected that Appliance Synchronisation will also be used.

192 Prerequisites

Swivel HA solution

Netscaler 10.x

193 Baseline

Swivel 3.10.3

Netscaler 10.5

194 Swivel Configuration

The Swivel servers should be setup as indicated in the integration guide.

Configure a RADIUS NAS entry for the Netscaler SNIP interface, see RADIUS Configuration

Optionally set **Authenticate non-user with just password:** to Yes and configure a non Swivel user with a static password, see RADIUS Static Password.

195 Netscaler Configuration

The Netscaler Configuration should be setup and tested to be working before attempting these steps.

195.1 Create a Swivel Radius Monitor

On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/**Monitors**, then Add

Expand the Special Parameters and add **Response Codes** to 3 for Access Reject and add 2 for Access Accept

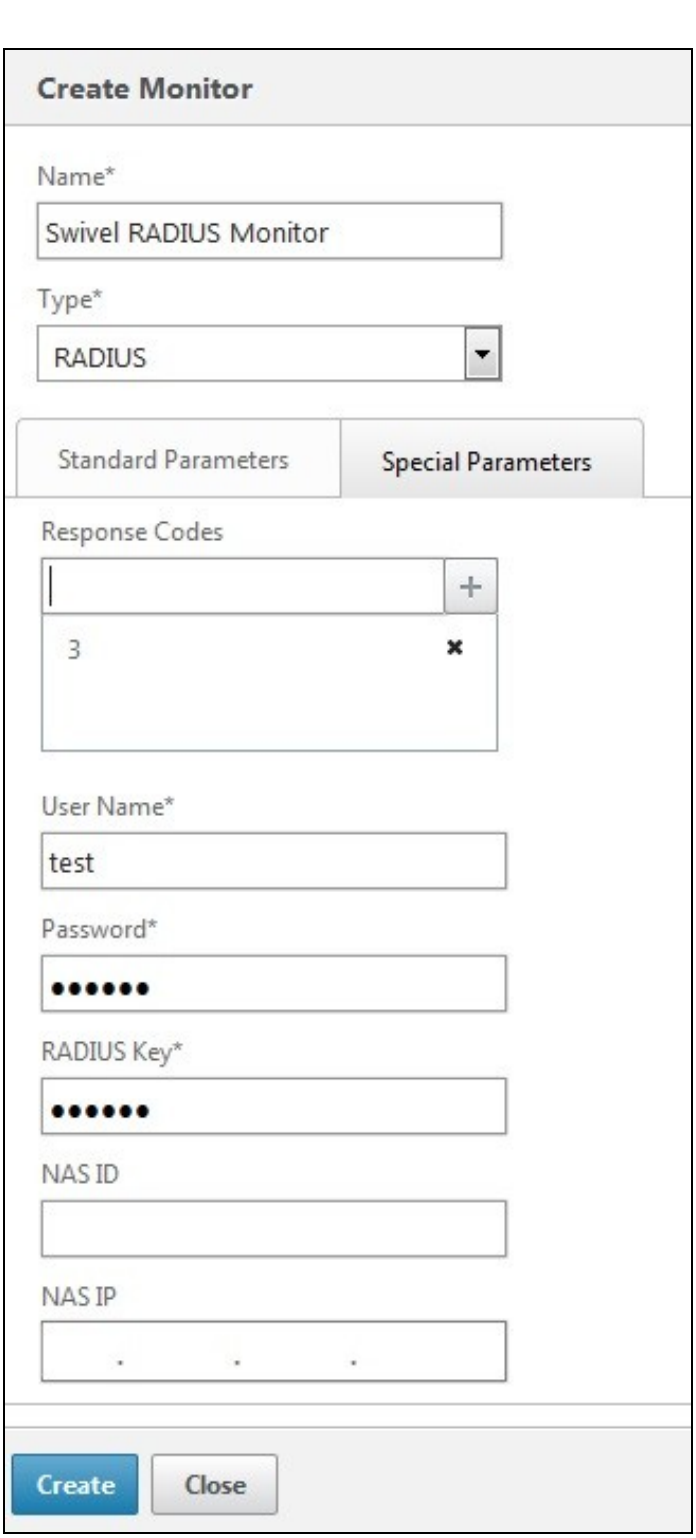
Set **Username** to an appropriate test user

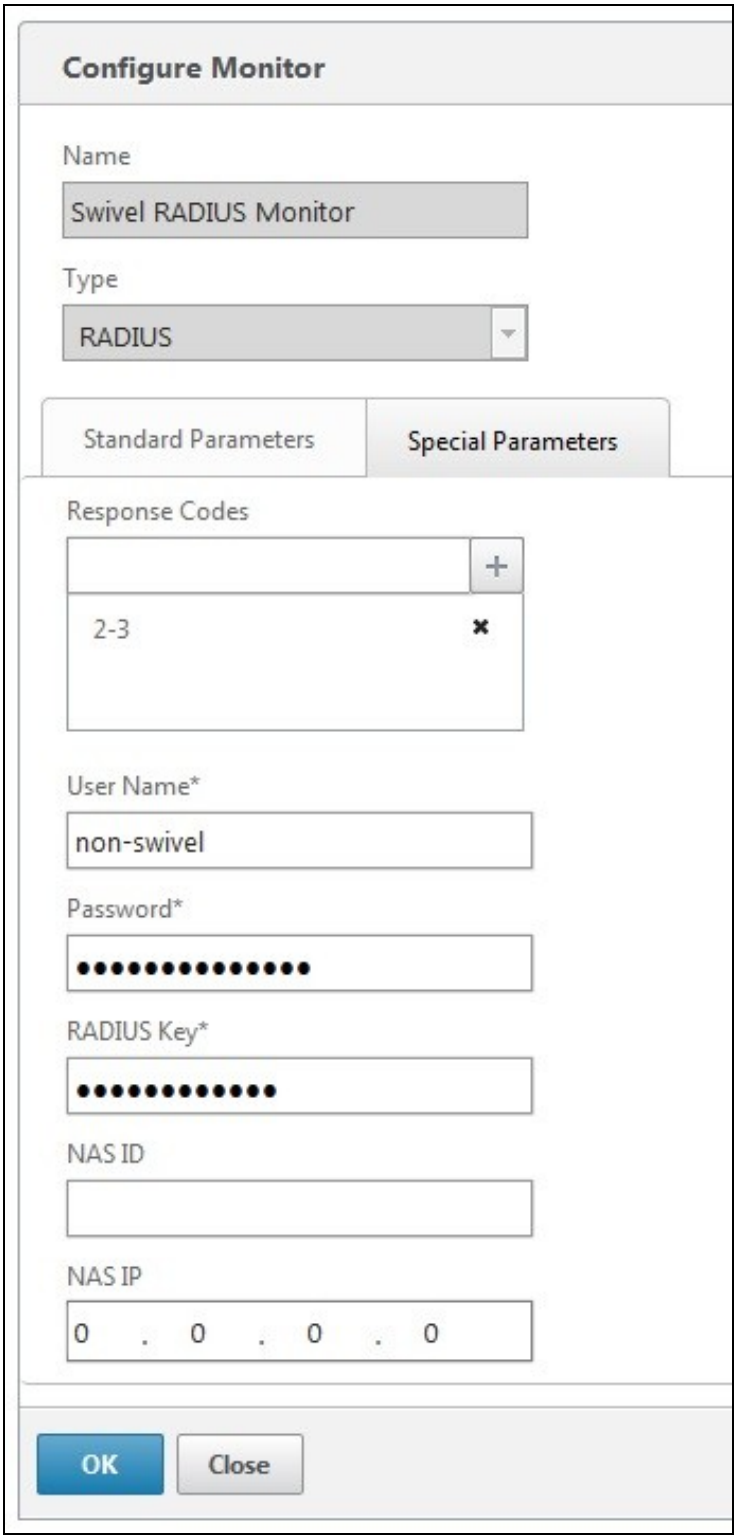
Set **Password** to the required value if Authenticate non-user with just password if authenticate non Swivel user is used (or random if not)

Set **RADIUS Key** to the value for the Swivel RADIUS NAS

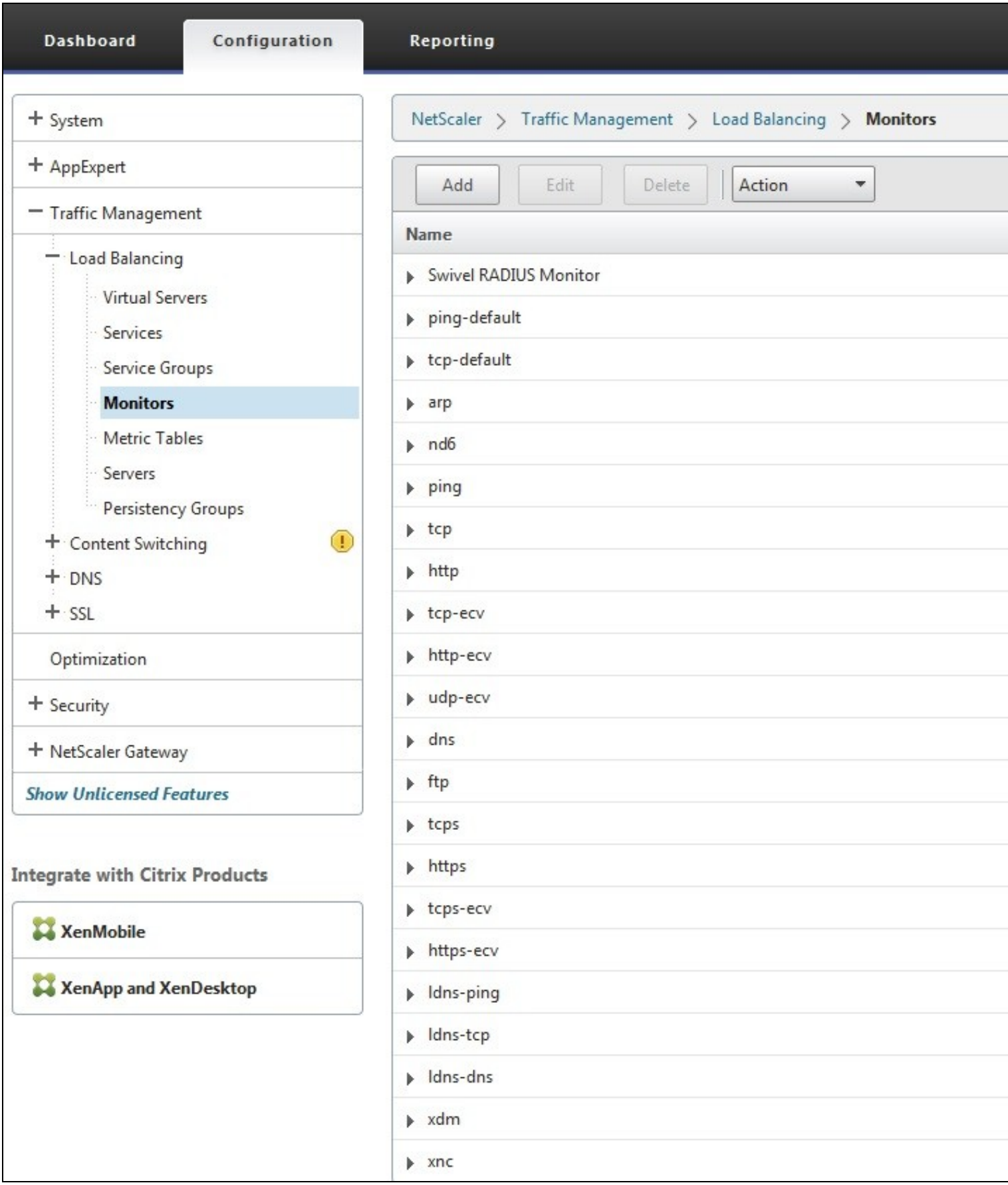
Leave other settings as default

Click Create to create the Monitor





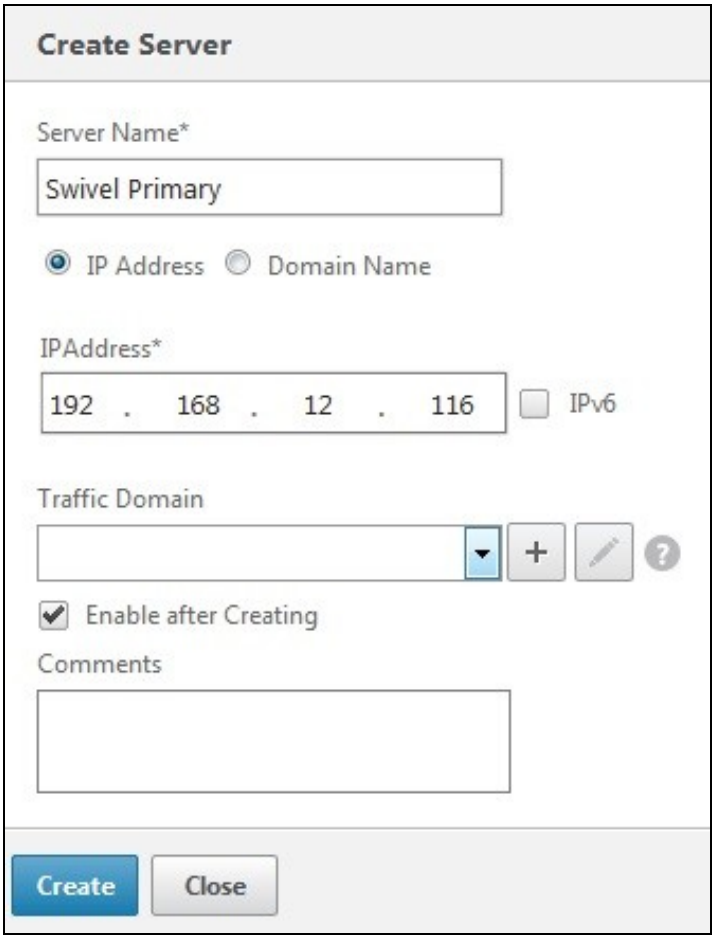
The Monitor should appear in the list.

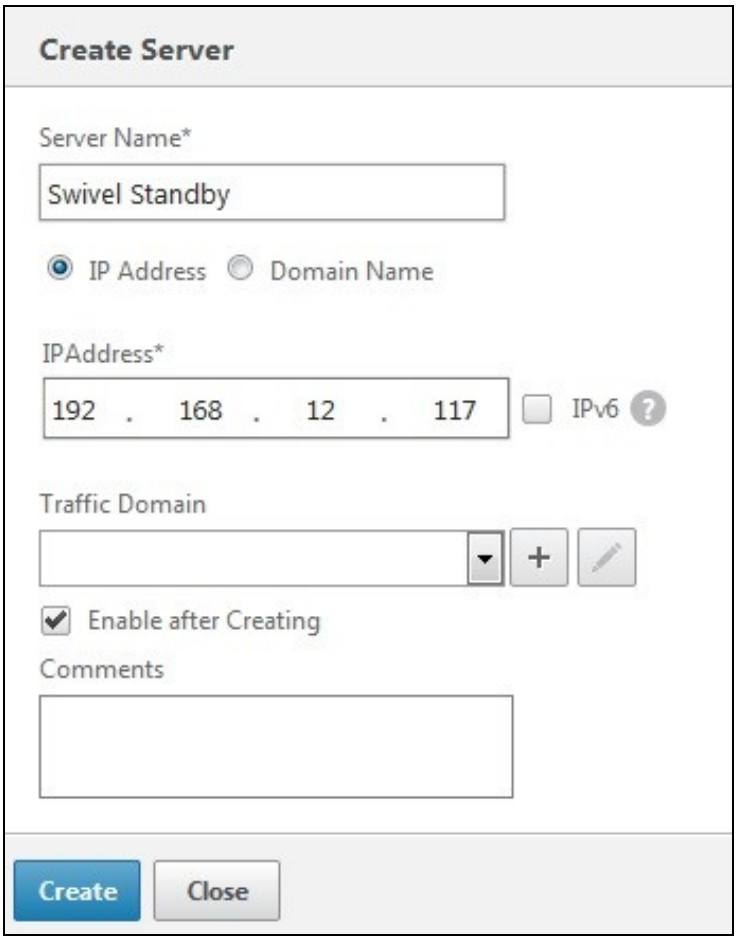

Dashboard
Configuration
Reporting
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Content Switching
DNS
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
Integrate with Citrix Products
XenMobile
XenApp and XenDesktop
NetScaler > Traffic Management > Load Balancing > Monitors
Add
Edit
Delete
Action
Name
Swivel RADIUS Monitor
ping-default
tcp-default
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
xdm
xnc

195.2 Create Entries for the Swivel RADIUS Servers

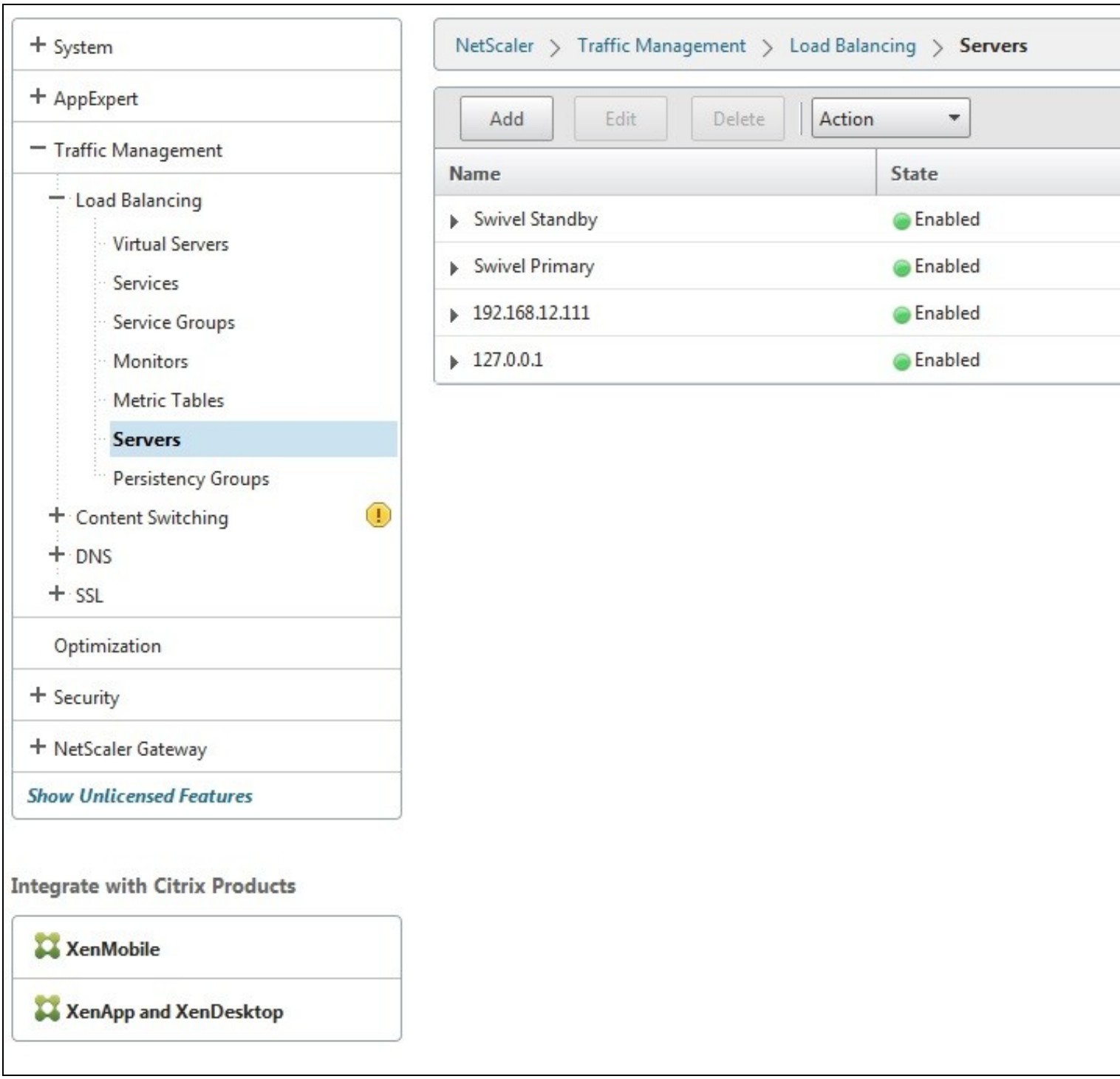
On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/**Servers**, then Add. Enter the details for each of the Swivel RADIUS servers. If the Swivel servers are already configured, then this step can be skipped over.

Enter **Server Name' *and* IP Address/Hostname**





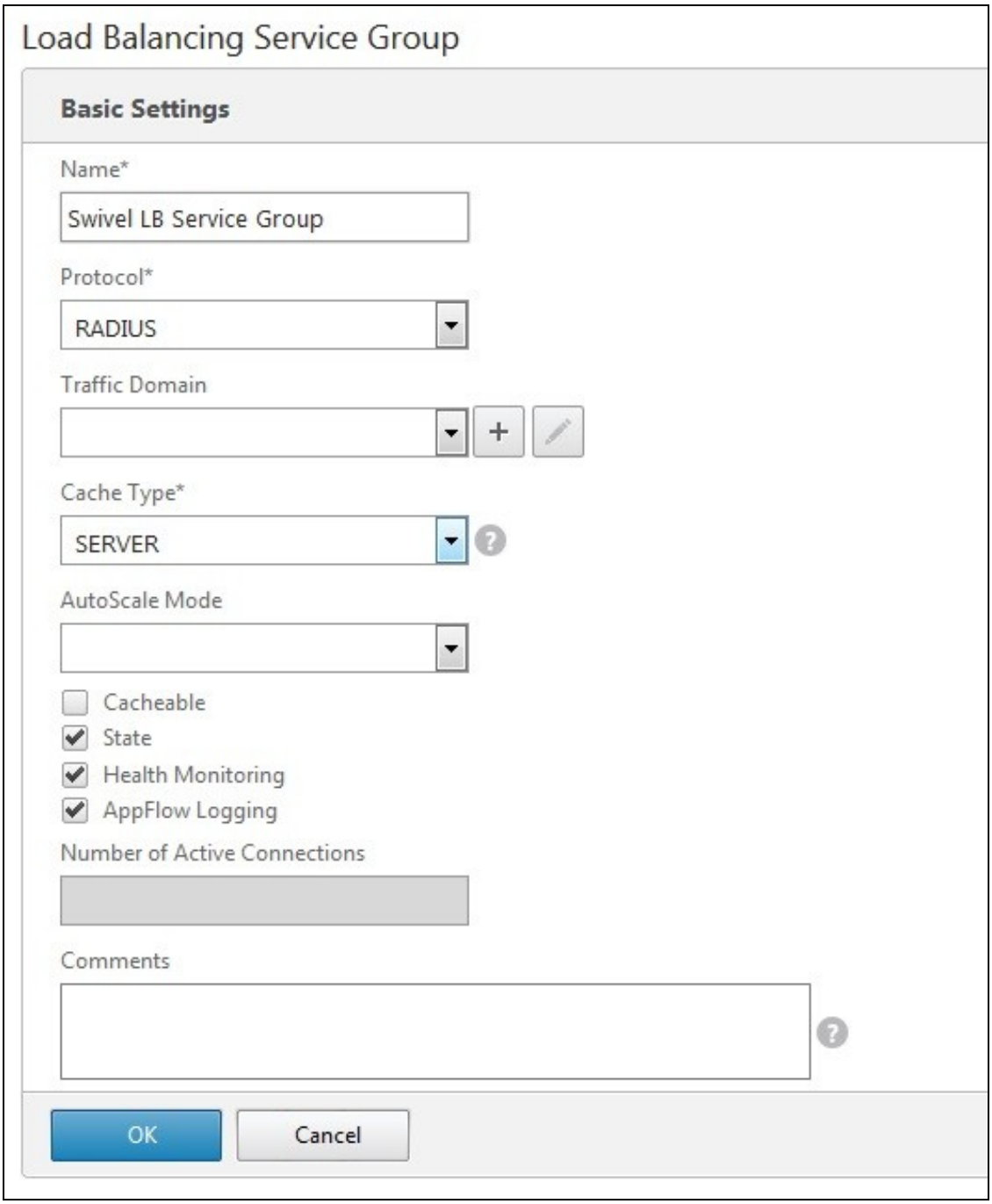
Click Create to create the Server



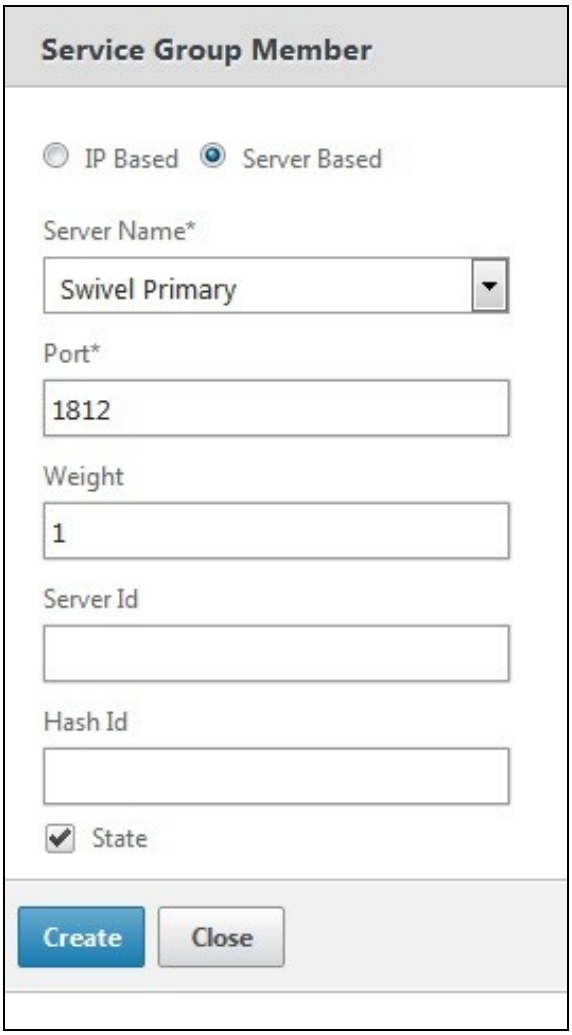
195.3 Create a Swivel Load Balance Service Group

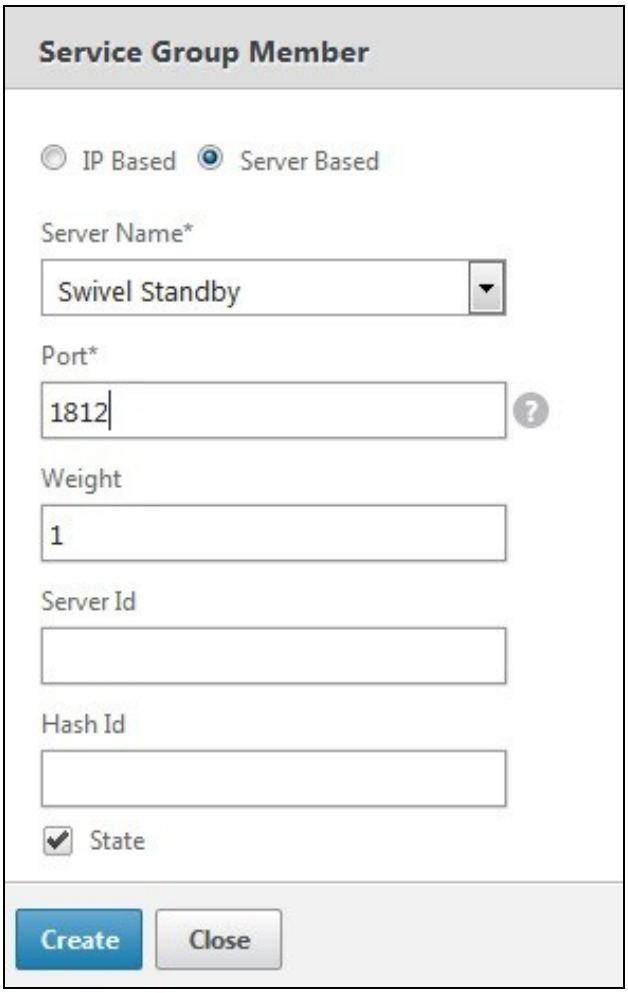
On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/**Service Group**, then Add.

Enter the **Name**, **Protocol** RADIUS, then click OK, and



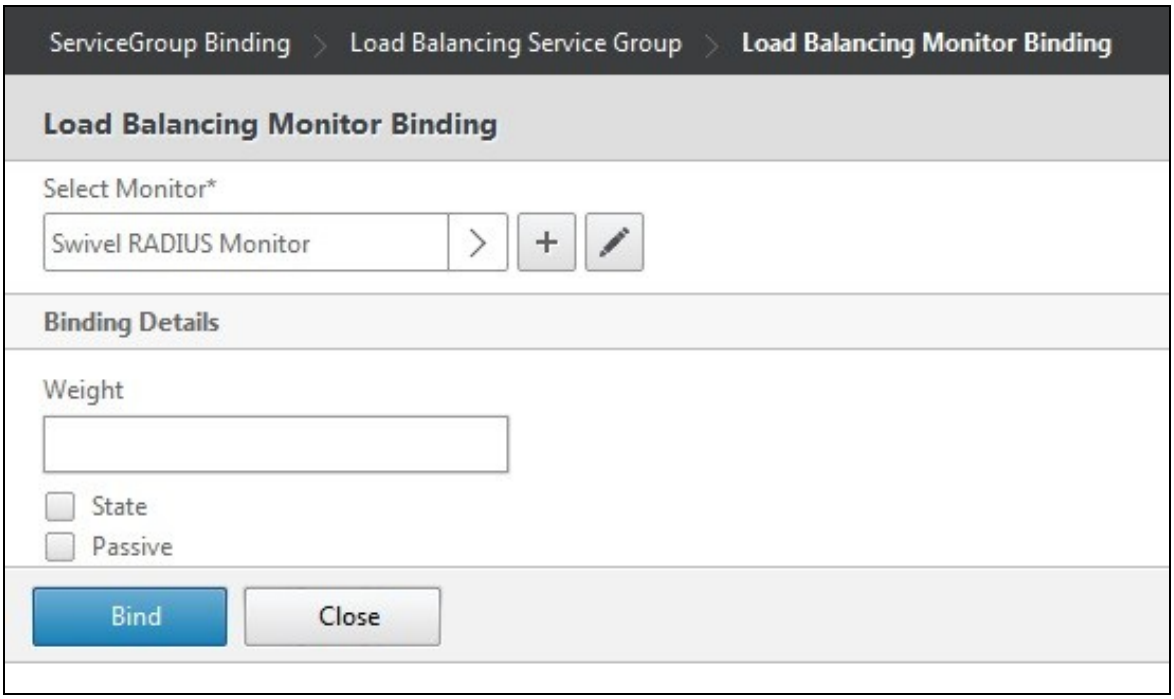
Click below the **Service Group members** to add members to the group, select the **Server Based** radio button to add in the Swivel RADIUS servers and enter **Port** 1812. Repeat for each Swivel server to be added.





195.3.1 Add the Monitor to the Load Balance Server Group

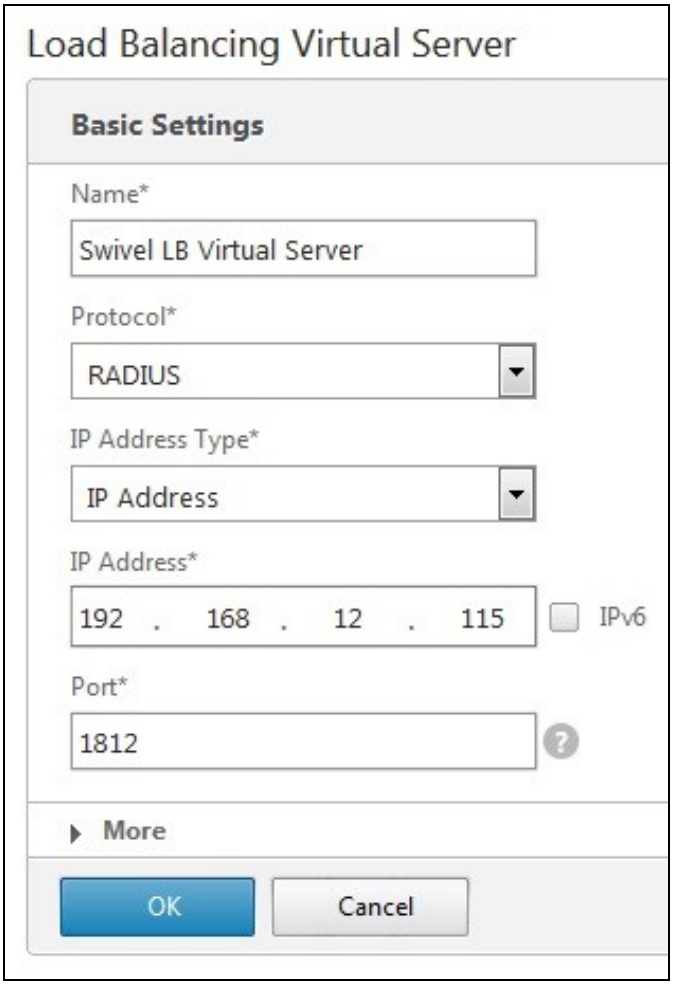
From the Right Handside select Monitor so it appears at the bottom then click it again to add the Swivel RADIUS Monitor.



Click **Bind** to add it, then Done.

195.4 Create A Virtual Server

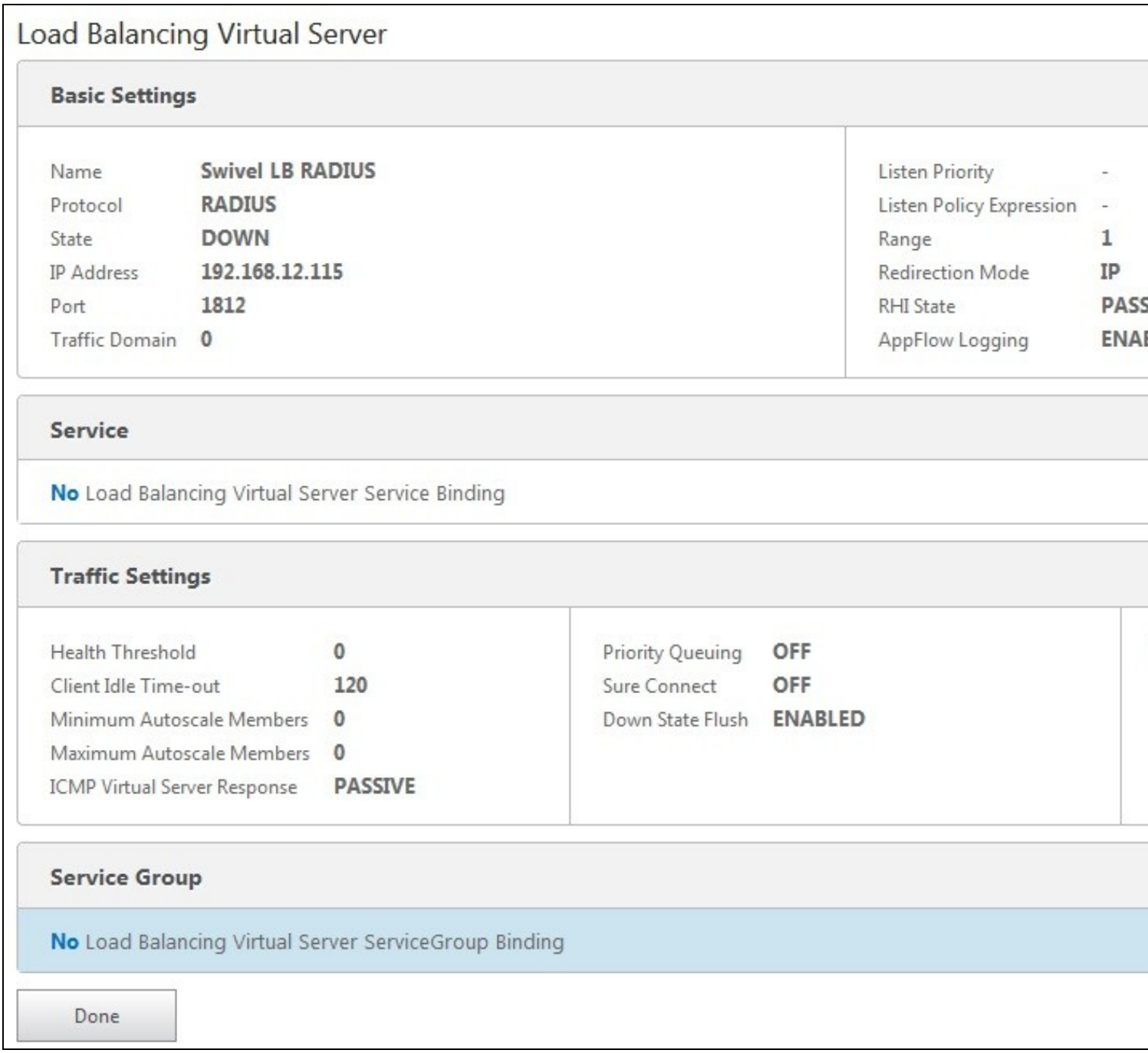
On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/**Virtual Servers**, then Add. Enter a **Name** for the Virtual Server **IP Address**, **Protocol** and **Port**.



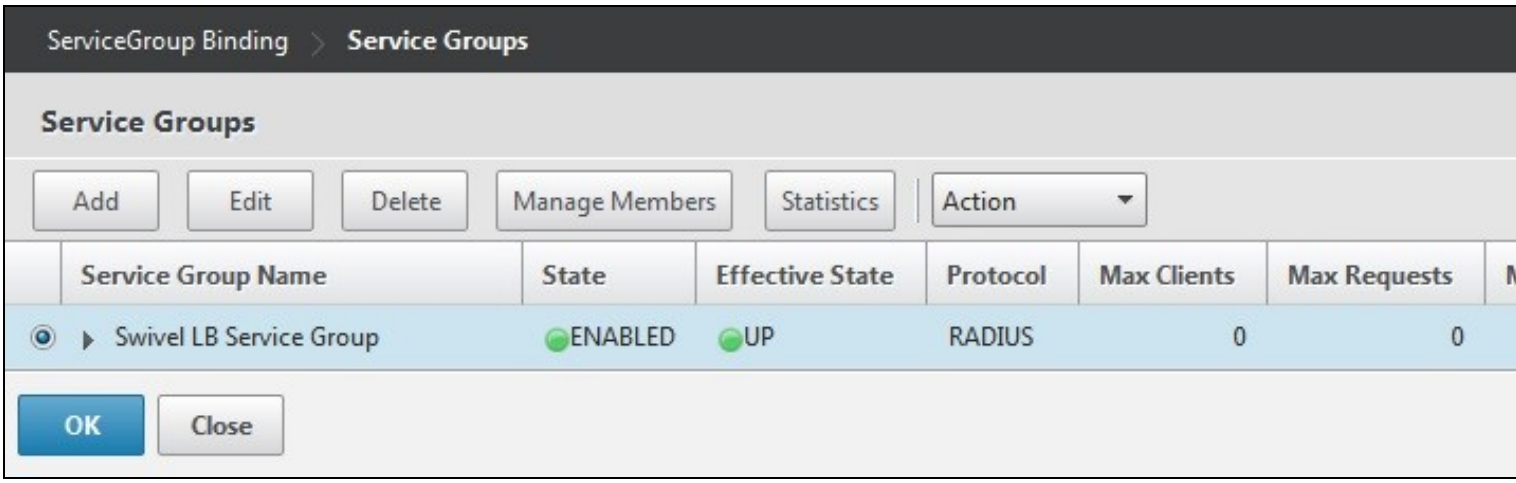
Click OK to create the entry

195.4.1 Add the Service Group to the Virtual Server

After configuring the Virtual Server, the Service section will appear, click on OK to bring up the **Service Group** on the right hand side.



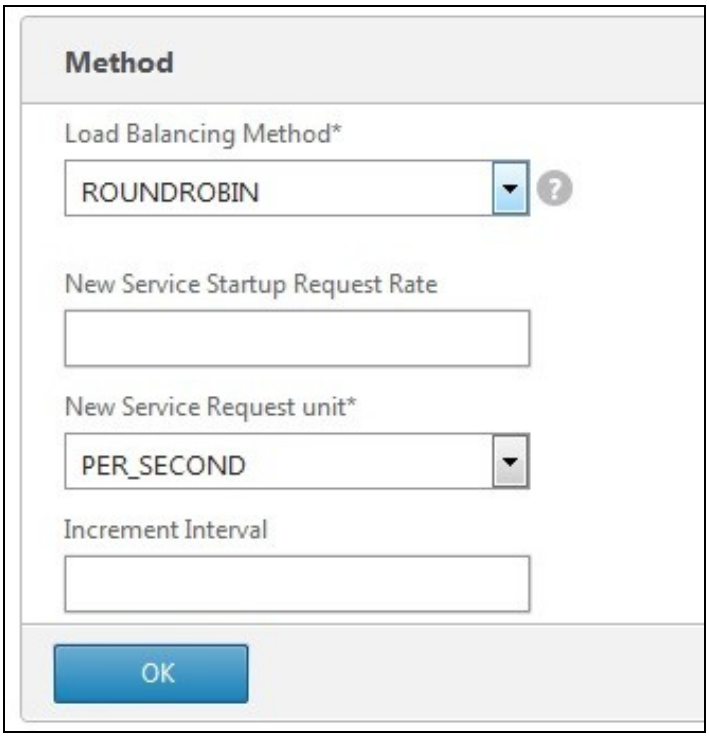
Click on the Service Group, it will appear at the bottom allowing it to be seleceted, and then click on **Select Service Group Name** to choose the required service group created earlier.



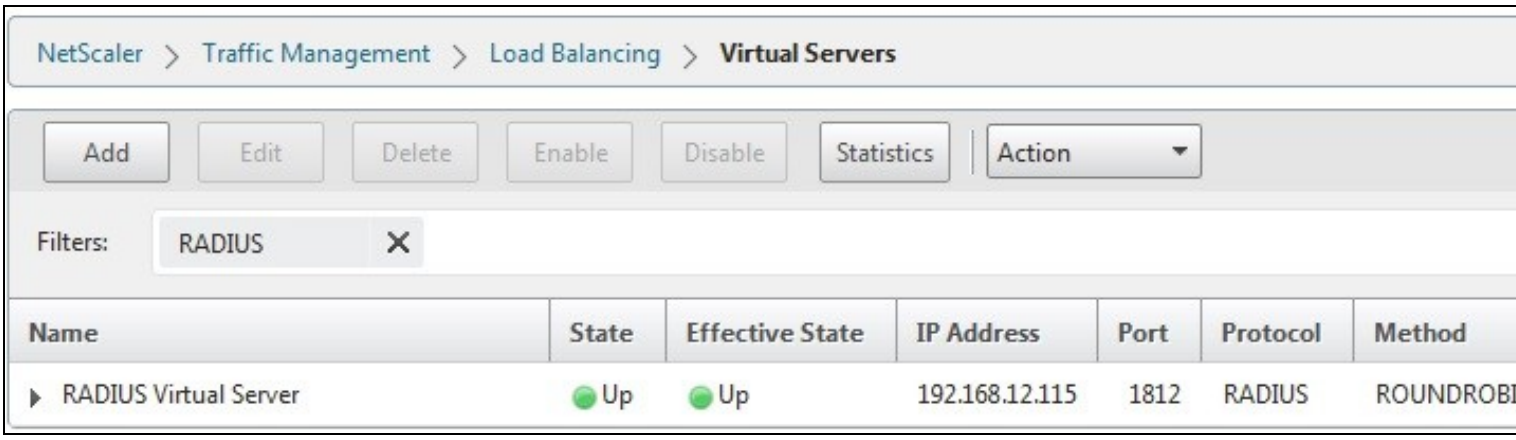
Then click **Bind**

195.4.2 Add the Method to the Virtual Server

Select Method and then from the **Load Balancing Method** drop down select **ROUNDROBIN** then click on OK.



Click Done and the Virtual server should be created.



195.5 Netscaler RADIUS configuration

The Netscaler can now be configured to use the new Virtual Server as its RADIUS servers following the original documentation.

196 Testing

When functioing RADIUS entries will be seen in the Swivel RADIUS logs for each test.

Try RADIUS authentications and see which Swivel server that recieves them. Stopping one RADIUS server should indicate on the Virtual Servers that health is degraded, i.e. 50% for two servers.

197 Known Issues

The load balancing can produce a large number of logs.

198 Troubleshooting

199 Citrix Products Integration Matrix

199.1 A guide to PINsafe and Citrix Product Integration

Product Integration

Product	SMS Text	Mobile Phone Client	Taskbar Utility	TURing Image	Index number display	Token
CAG Standard 4 or 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5 with WI authentication	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AAC 4.5	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AC	Yes	Yes	Yes	No	No	Yes
CAG Enterprise (Netscaler) 8 or 9 or 10 10.x	Yes	Yes	Yes	Yes	Yes	Yes
WI 4.5, 4.6, 5.0, 5.1, 5.2, 5.3, 5.4	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
PS 4 with WI	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Receiver	Yes	Yes	Yes	Yes*	Yes*	Yes

CAG = Citrix Access Gateway

AAC = Advanced Access Controller (AAC 4.x)

PS = Presentation Server

WI = Web Interface

Index Number Display is the ability to display the index number in the login page

Yes* When viewed in browser before receiver starts

200 Citrix Web Interface 4 with Presentation Server 4

200.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix Presentation Server 4 web interface. This also works with Citrix Secure Gateway v3.0. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

200.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 45083 of the Citrix web interface and have been tested with versions 4.0 and 4.2, for later versions please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.cs ? Customised login logic constants.
- login.cs ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here: File:Citrix_PS_4.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

200.3 Baseline

PINsafe 3.x

Citrix Web Interface build 3.x, 4.0, 4.2

200.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

200.5 PINsafe Configuration

200.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

200.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet.

On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

200.6 Citrix Web Interface Configuration

200.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.cs and login.cs to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

200.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

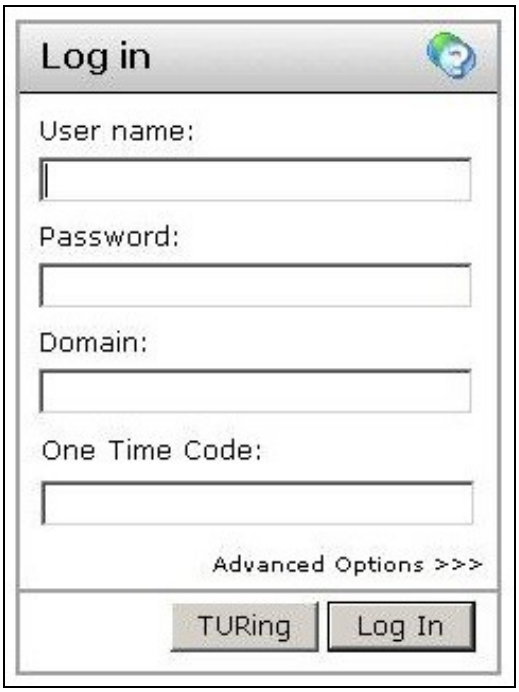
```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

200.7 Additional Configuration Options

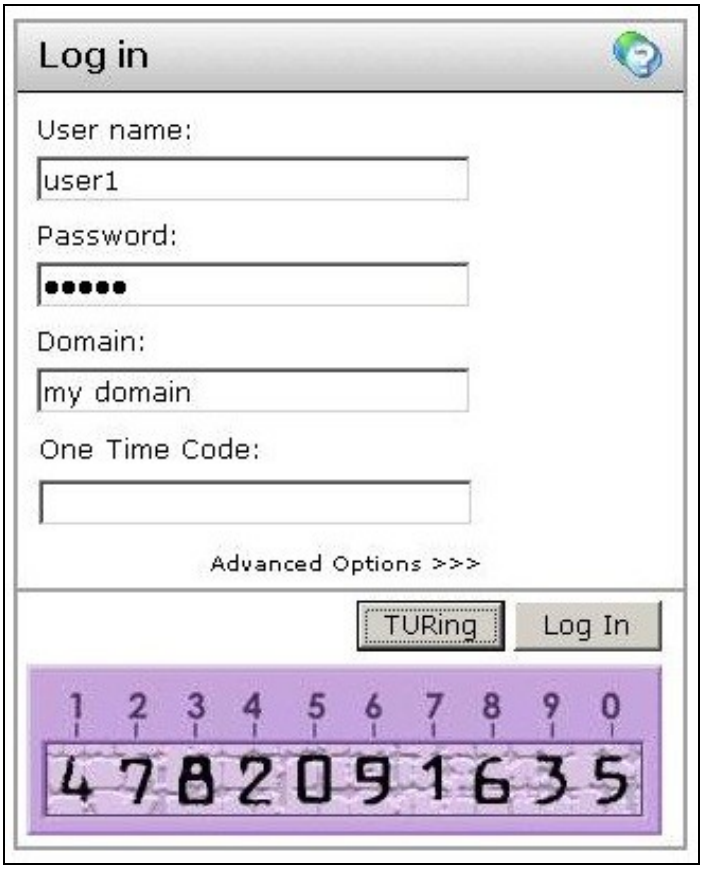
200.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface login with SMS (Do not click on the Turing Button)



Citrix Web Interface login with Turing



200.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

200.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

200.11 Known Issues and Limitations

Self signed certificates are not supported with this version of the integration, either use a valid certificate, or non SSL communications or upgrade the Web Interface version.

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

200.12 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

201 Citrix Web Interface 4.5 Integration

201.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.5 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

201.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.5.1.8215 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.aspxf ? Customised login logic constants.
- login.aspxf ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\MetaFrame

201.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.5.1.8215

201.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

201.5 PINsafe Configuration

201.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

201.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCIMage servlet.

On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

201.6 Citrix Web Interface Configuration

201.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

201.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

201.7 Additional Configuration Options

201.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

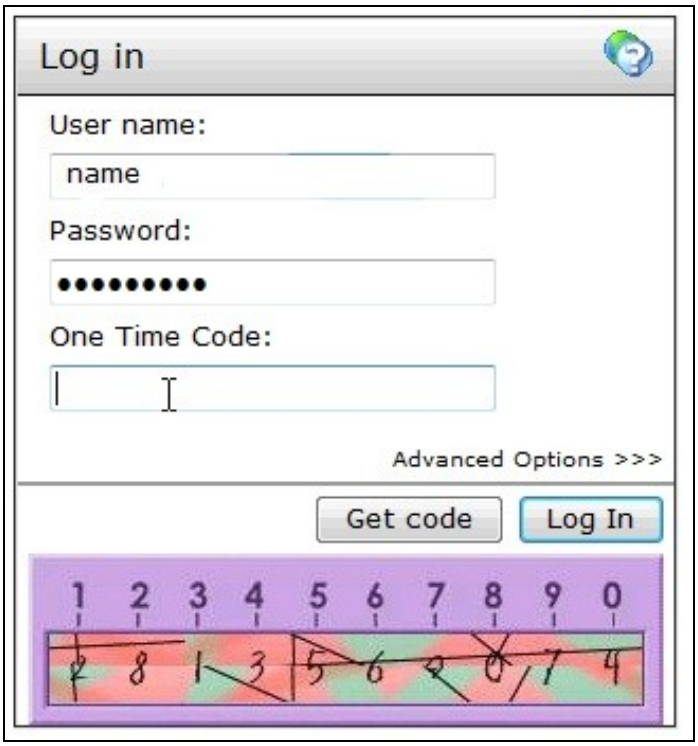
to

if (!pc.Login(user,password, otc))

201.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with TURing image (For SMS do not click on Get Code button)



201.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

201.9.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

201.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

201.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

201.12 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

202 Citrix Web Interface 4.6 Integration

202.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.6 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

202.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.6.0.18291 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.aspxf ? Customised login logic constants.
- login.aspxf ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

202.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.6.0.18291

202.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

202.5 PINsafe Configuration

202.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

202.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet.

On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

202.6 Citrix Web Interface Configuration

202.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

202.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

202.7 Additional Configuration Options

202.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

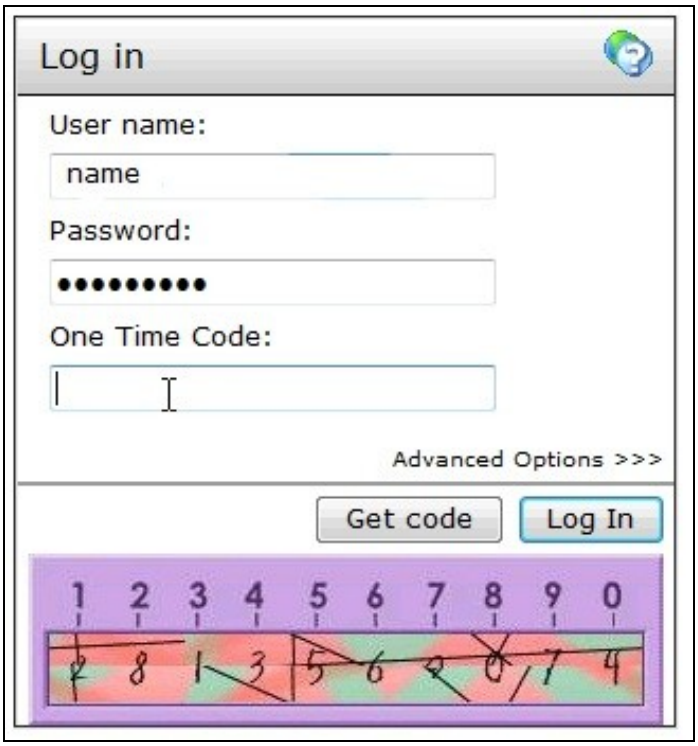
to

if (!pc.Login(user,password, otc))

202.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with Turing image (For SMS do not click on Get Code button)



202.9 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

202.10 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

202.10.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

202.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

202.12 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

203 Citrix Web Interface 5.0 Integration

203.1 Introduction

This document outlines the necessary steps to integrate Swivel authentication into the Citrix 5.0 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the Swivel server as the Image is proxied through the Web Interface server.

203.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.0.1.29110 of the Citrix web interface, if you have a later version please contact your Swivel reseller for an update. Your Swivel server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? Swivel authentication client library.
- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from Swivel to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for Swivel integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

203.3 Baseline

Swivel 3.5

Citrix Web Interface build 5.0.1.29110

203.4 Architecture

The Citrix Web Interface makes authentication requests against the Swivel server by RADIUS.

204 Swivel Configuration

204.1 Configuring the RADIUS server

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

204.2 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.

204.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

204.3 Citrix Web Interface Configuration

204.3.1 Copy accros the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

204.3.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the Swivel server.

204.3.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your Swivel installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />
```

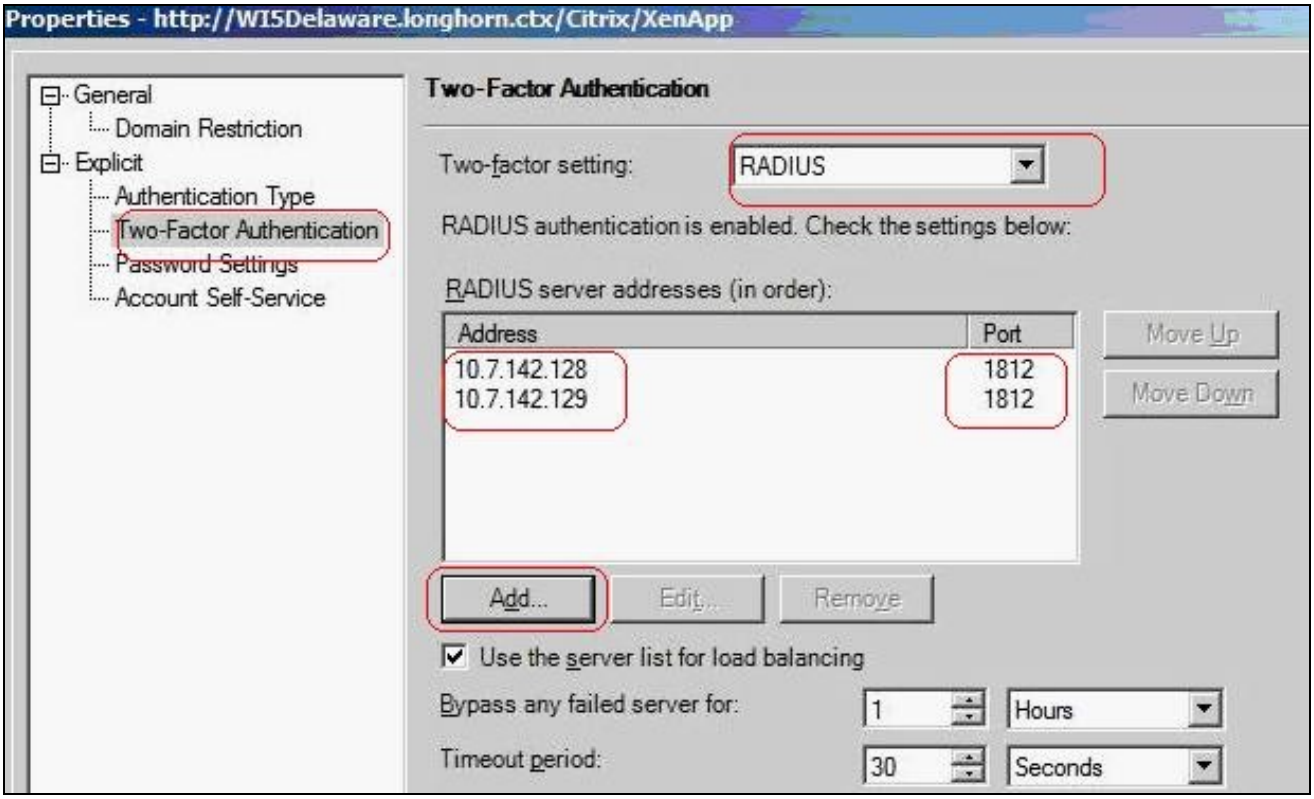
```
<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />
```

204.3.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, the select Radius from the dropdown list.



204.4 Additional Configuration Options

see Citrix Web Interface 5.X additional login page options

204.5 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Citrix credentials should the user be logged in.

204.6 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the Swivel RADIUS entries.

204.7 Troubleshooting

Check the Swivel logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the Swivel server or for testing the client can accept the certificate (load Image URL into browser)
- Swivel server not accessible, check networking and firewalls. Check the Swivel server logs for a session started message.
- Incorrect Swivel URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

204.7.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the Swivel NAS setting do not match.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

204.8 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the Swivel settings and files so the Swivel integration may need to be applied again.

204.9 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

205 Citrix Web Interface 5.1 Dual Channel button

205.1 Citrix Web Interface Dual Chanel Integration Notes

This outlines how to replace the Single Channel Image request button with a Dual Channel button. This is a supplement to the Citrix Web Interface 5.1 Integration guide.

205.2 Log-in page Customisation

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending , and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
       href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
       onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
       onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
       tabIndex="<%=Constants.TAB_INDEX_FORM%>"
       id="dcmessage"
       name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

205.3 Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

206 Citrix Web Interface 5.1 Integration

207 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.1 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

208 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.1.1 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.1_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

209 Baseline

PINsafe 3.5

Citrix Web Interface build 5.1.1

210 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

211 Swivel Configuration

211.1 Configuring the RADIUS server

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

211.2 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.

211.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

212 Citrix Web Interface Configuration

212.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

212.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

212.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />
```

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

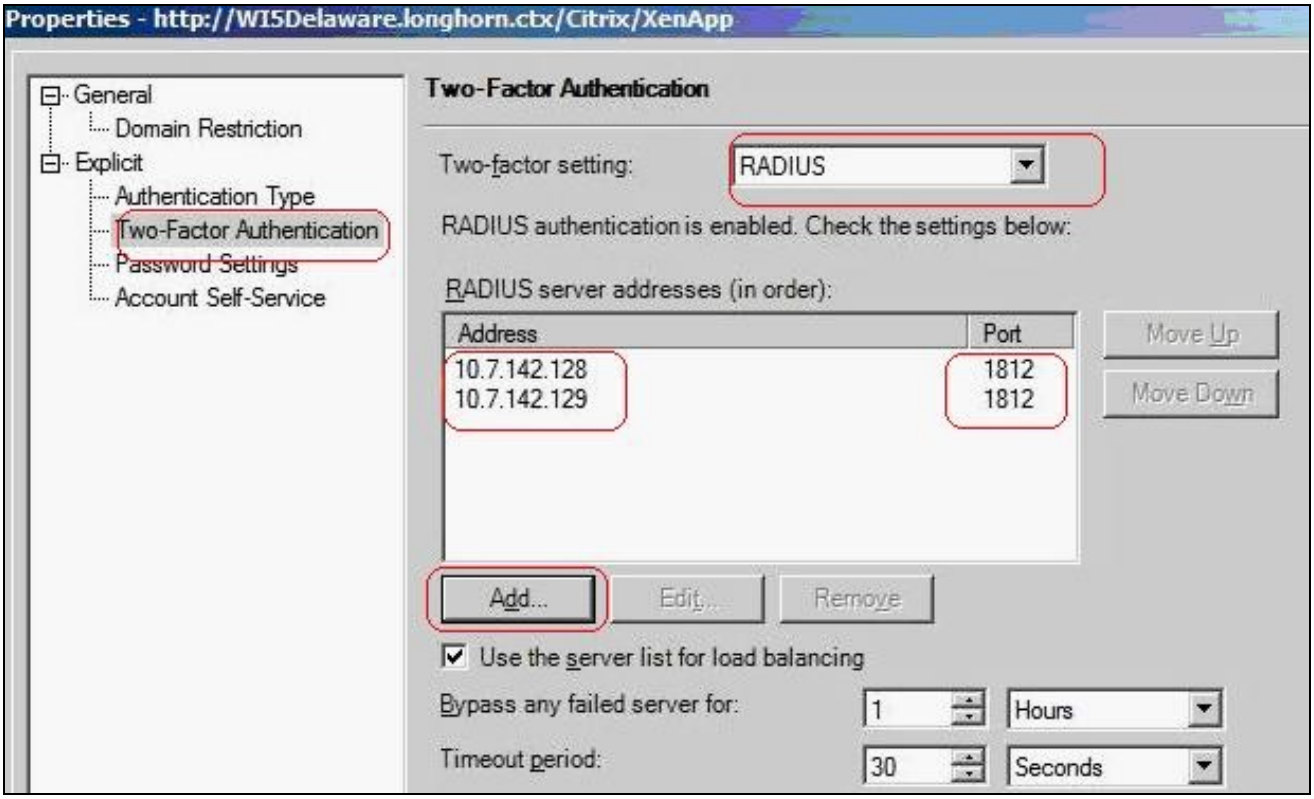
```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="true" />
```

212.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list.



213 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

213.1 Self Reset

This outlines how to add the self reset option to the Citrix Web Interface.

The Citrix Web Interface 5.1 self reset files can be downloaded here: File:Citrix_WI_5.1_SelfReset.zip

Download PINsafeClient.dll and copy to the bin folder overwriting the existing file installed above. Copy reset.aspx and reset.aspx.cs into the auth folder.

Add reset.aspx to the list of unprotected pages in web.config. Locate key="AUTH:UNPROTECTED_PAGES", and at the end of the value field, insert ",./reset.aspx".

Insert a link on the Citrix login page to open the reset page.

Edit app_data\include\loginMainForm.inc, and insert the following line after the login button row, immediately before the </table> tag.

<tr><td>Forgotten my PIN</td></tr>

214 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

215 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the PINsafe RADIUS entries.

216 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

216.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

217 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

218 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

219 Citrix Web Interface 5.2 Integration

220 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.2 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

221 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.2 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.2_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

222 Baseline

PINsafe 3.5

Citrix Web Interface build 5.2

223 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

224 Swivel Configuration

224.1 Configuring the RADIUS server

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

224.2 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.

224.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

225 Citrix Web Interface Configuration

225.1 Copy across the Web Interface Files

The The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

225.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

225.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />
```

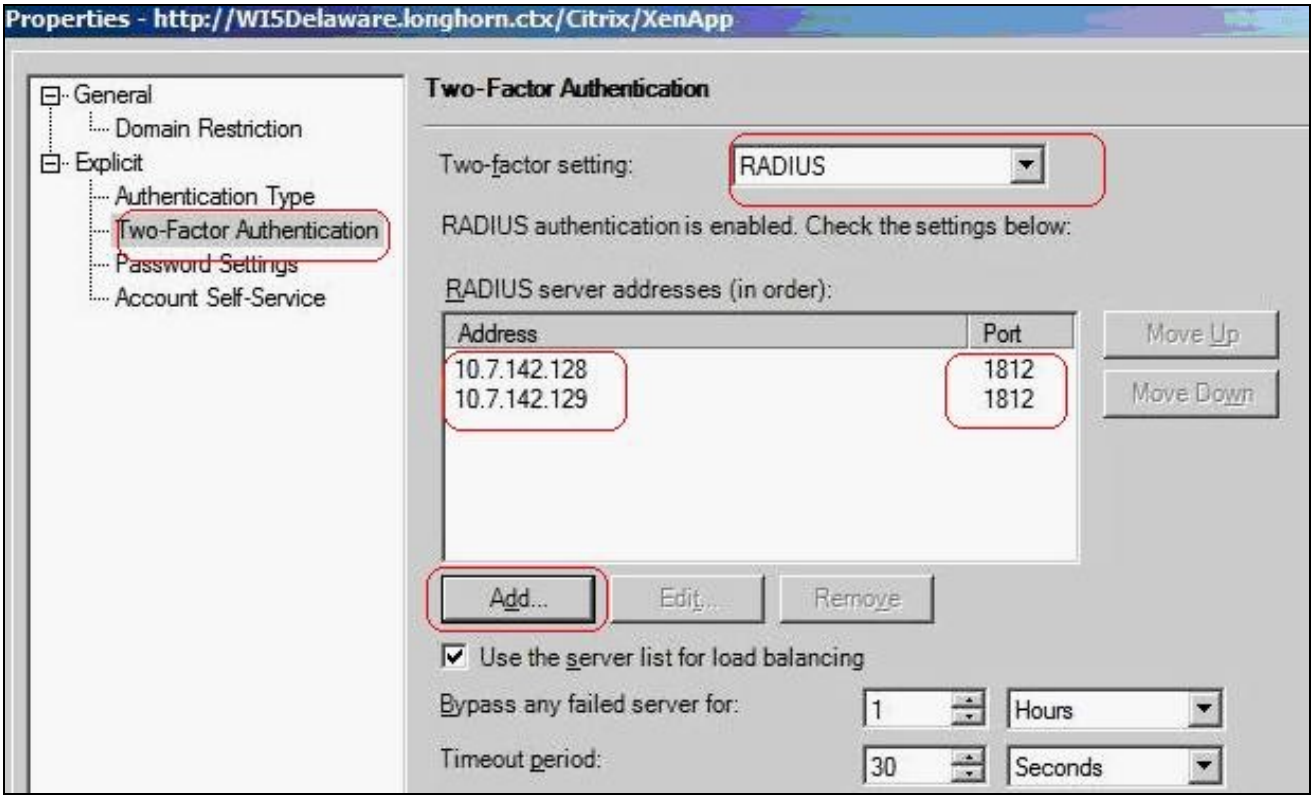
```
<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />
```

225.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Configure the PINsafe server as RADIUS server. If you have more than 1 PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

226 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

227 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

228 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

229 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

229.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

230 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

231 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

232 Citrix Web Interface 5.3 Integration

233 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.3 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

234 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.3 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependant on the OS being 32 bit or 64 bit.

235 Baseline

PINsafe 3.5

Citrix Web Interface build 5.3

236 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

237 Swivel Configuration

237.1 Configuring the RADIUS server

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

237.2 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.

237.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

238 Citrix Web Interface Configuration

238.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

238.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

238.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Note: The setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be set to <add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />
```

The settings for a software install of PINsafe are:

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />
```

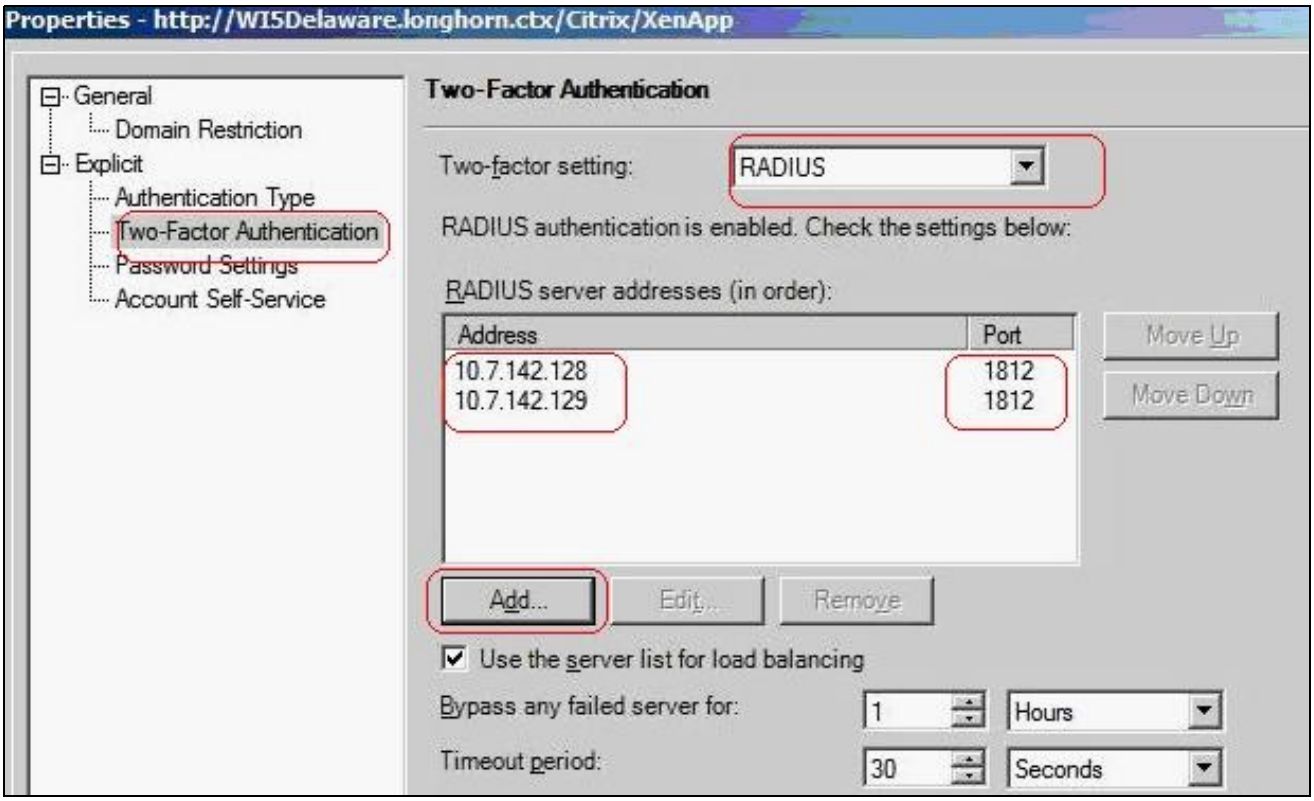
```
<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />
```

238.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

239 Additional Configuration Options

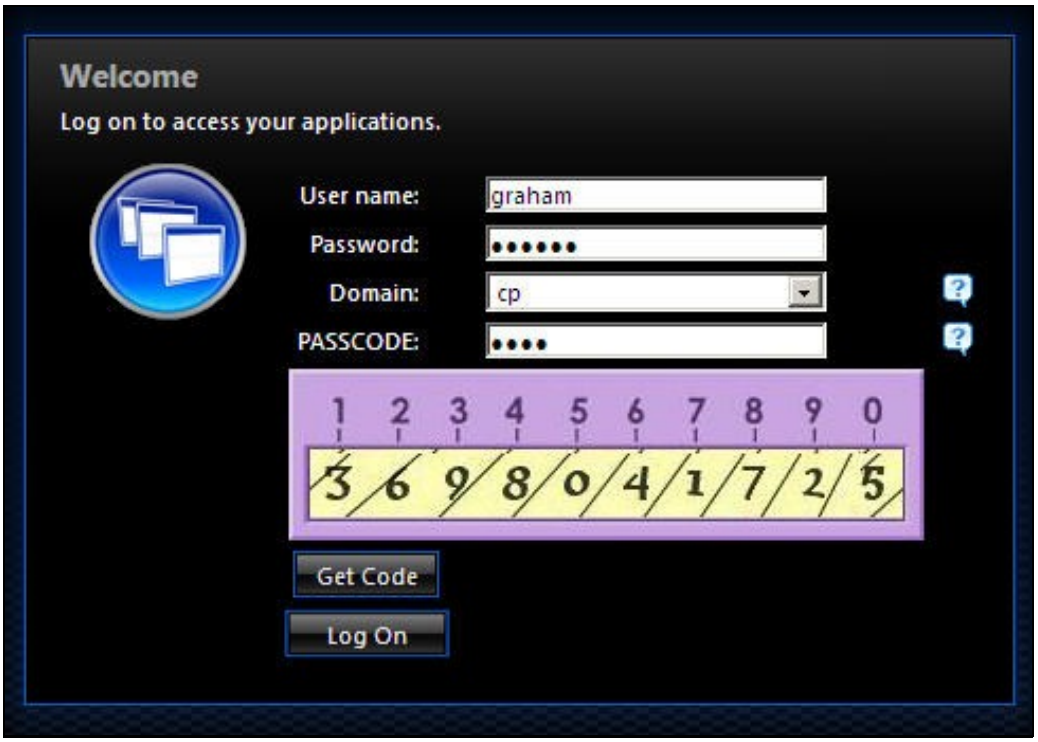
see Citrix Xen App 5.x additional login page options

240 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication

Login Using Single Channel Graphical Turing Image



241 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

242 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a PINsafe virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

242.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

243 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

244 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

245 Citrix Web Interface 5.4 Integration

246 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.4 web interface/Xen App. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

A statement from Citrix: *All 7.x versions of XenApp and XenDesktop now support the use of Web Interface 5.4. Citrix has extended support of Web Interface for XenApp 7.5, XenDesktop 7.5, XenDesktop 7.1 and XenDesktop 7.0 to allow more time for planning and transition to StoreFront. Note, no new features will be added to Web Interface and its end-of-life remains August 2016.*

247 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.4 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation and need to be edited as required (see below):

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js.add ? Customised login page client script.
- loginStyle.inc.add ? Customised login form style.
- loginMainForm.inc.add ? Customised login form.
- web.config.add ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here.

An alternative solution, which includes buttons for TURing image and message request, can be found here. This solution includes two additional files: pinsafe_message.aspx and pinsafe_ping.aspx.

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependent on the OS being 32 bit or 64 bit.

NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

NOTE: the files with the extension ".add" cannot simply be copied into the appropriate directories. They are text files containing notes as to how you should modify the corresponding files to implement PINsafe customisation. See the notes below for more details.

248 Baseline

PINsafe 3.7

Citrix Web Interface build 5.4

249 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

250 Swivel Configuration

250.1 Configuring the RADIUS server

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

250.2 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.

250.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

251 Citrix Web Interface Configuration

251.1 Edit the radius_secret.txt

On the Citrix Web Interface server

Edit the conf/radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server. A copy of this file is included in the zip archive.

251.2 Edit the web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Note: the setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be changed to

```
<add key="RADIUS_NAS_IDENTIFIER" value="citrix_wi" />
```

Note: It is recommended that you use the same value as the identifier in the NAS entry in the PINsafe admin console.

If the Web Interface server has multiple network interfaces, the value of RADIUS_NAS_IP_ADDRESS may need to be set to the IP address used by the NAS. This is the IP address of the Web Interface server, NOT the PINsafe server.

Make sure that the following entry is included, if it is not there already:

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />
```

To allow access to the TURing image from the login page, locate the following line:

```
<add key="AUTH:UNPROTECTED_PAGES" ...
```

The value attribute on this entry is a list of URLs that can be accessed without authentication. Add the following to the end of this list (before the closing quote):

```
,/auth/pinsafe_image.aspx
```

If you are using the alternative integration, you will need to include the other files:

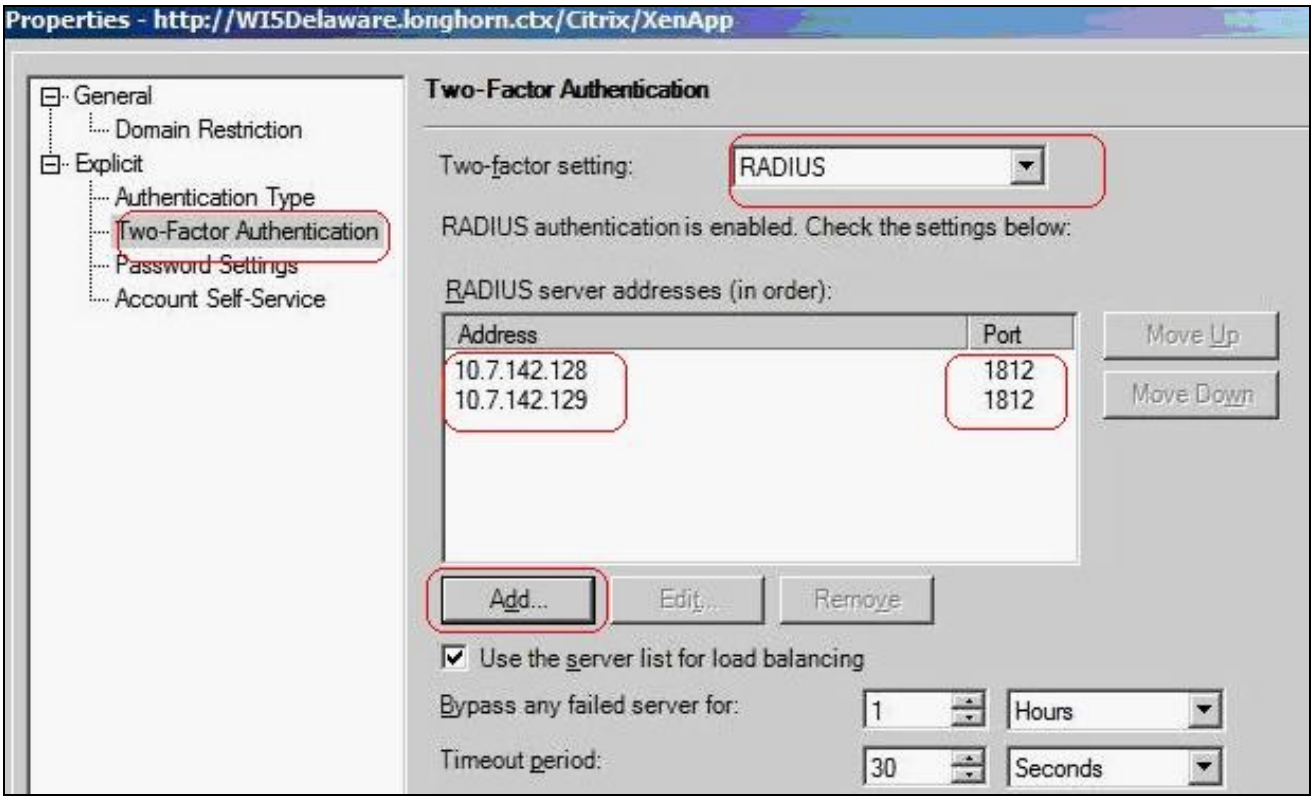
```
,/auth/pinsafe_image.aspx,/auth/pinsafe_message.aspx,/auth/pinsafe_ping.aspx
```

251.3 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

252 Additional Configuration Options

The above modifications will allow authentication to the Web Interface using some of the PINsafe authentication mechanisms such as SMS, mobile Phone applet, and Taskbar. Additional configuration options including the single channel TURing image are listed below.

see also Citrix Web Interface 5.X additional login page options

252.1 Changing the OTC label

To change the label for the PINsafe one-time code field from the default of ?PASSCODE:?, locate the file C:\Program Files\Citrix\Web Interface\5.4.0\Languages\accessplatform_strings.properties. (If the language is not English, locate the appropriate file for the appropriate language, if it exists). Edit this file, and locate the line containing ?Passcode=PASSCODE:?. Replace the second word PASSCODE with OTC, or an appropriate text.

252.2 Configuring Single Channel: Modifying the Web Interface Files

The required files (see prerequisites) are of two types: those NOT ending in ".add" need to be copied to the following locations below the root of the Citrix web interface site. Those ending in ".add" contain instructions describing how to modify the corresponding file without the ".add" extension. Where an existing file is being replaced or modified, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory. The below files contained within the zip file should extract to the relevant locations.

The majority of the files included in the integration are modifications to existing files. This are stored with the same name as the file they are intended to modify, but with the additional extension of .add. Each file contains instructions as to how the original files should be added. More details are given below:

1. Copy pinsafe_image.aspx to /auth. This is a new file, not a modification to an existing one.

2. Edit login.js in /auth/clientscripts. Insert the contents of login.js.add at the start of this file, below the header, as indicated in the file itself.

3. Edit loginMainForm.inc in /app_data/include. Insert the contents of loginMainForm.inc.add as indicated in this file: locate a particular section of the file and insert a line.

4. Edit loginstyle.inc in /app_data/include. Insert the contents of loginstyle.inc.add at the bottom of this file, before the footer text, as indicated in the file.

5. Ensure file permissions are set correctly on the copied files, Authenticated users need read permissions.

252.3 Configuring Single Channel: Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

The web.config.add file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />
```

The settings for a software install of PINsafe are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

```
<add key="PINsafe_AcceptSelfSigned" value="false" />
```

252.4 Challenge and Response Authentication with Count Down Timer

Citrix Web Interface can be configured to use Challenge and Response whereby a user enters a username and password, and if that is correct the user is sent an SMS message and will be prompted to enter an OTC. By default the OTC sent is valid for two minutes only, so a count down timer is provided to show how long the user has left.

For information on configuring the PINsafe RADIUS Challenge and response see Challenge and Response How to Guide.

The required files can be downloaded here: Challenge and Response with count down files

Extract the files ensuring their correct locations

challenge.inc is copied to app_data/include

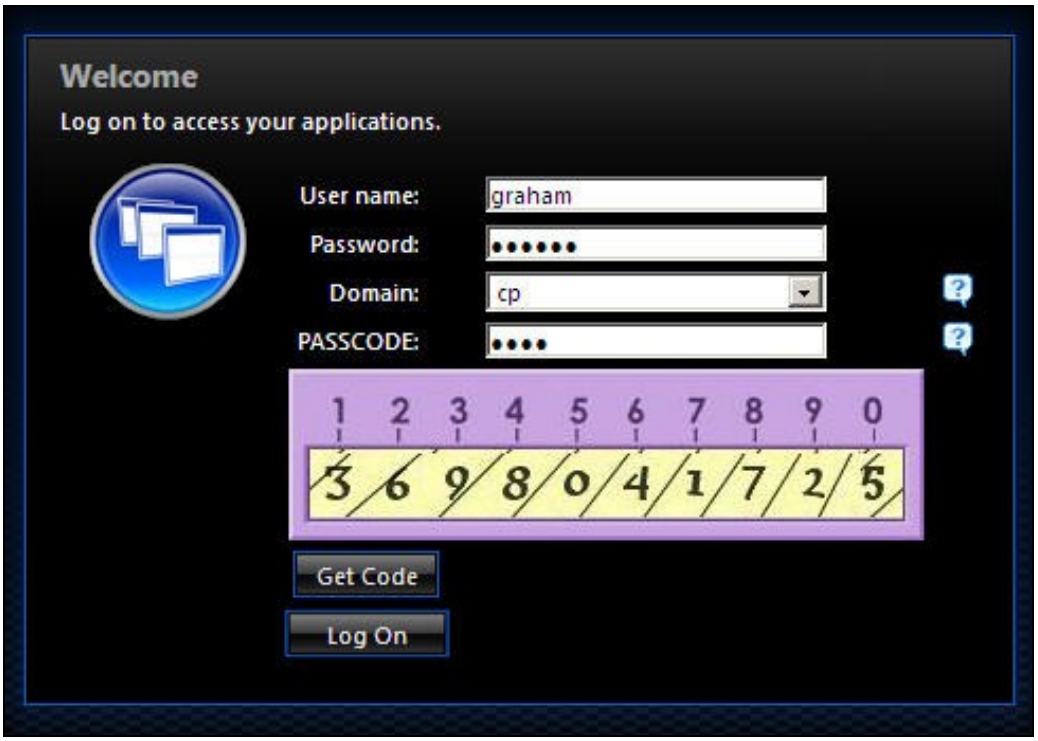
challenge.js to auth/clientscripts

253 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication

Login Using Single Channel Graphical Turing Image



254 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

255 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate, you need to add the following entry to web.config:

```
<add key="PINsafe_AcceptSelfSigned" value="true" />
```

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

255.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

256 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

If you need to use userPrincipalName to authenticate to Swivel, you may find that the domain name is removed before sending the username to Swivel. To avoid this, make the following changes:

Locate and edit the file app_code\PagesJava\com\citrix\wi\pageutils\TwoFactorAuth.java

Find the following method:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
  if (fullyQualified) {
    return token.getShortDomain() + "\\" + token.getShortUserName();
  } else {
    return token.getShortUserName();
  }
}
```

Replace it with the following:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
  return token.getUserIdentity();
}
```

257 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

258 Citrix Web Interface 5.X additional login page options

258.1 Citrix Web Interface 5.x additional login page options

This outlines how to further customise the Citrix login page. This is a supplement to the Citrix Web Interface 5.x Integration guides.

258.2 Removing the Single Channel Button

To remove the *refresh image*, delete the following text:

```
 "<a class='leftDoor' href='javascript:onTuringButtonClick();'>" +
                                "Refresh Image" +
                                "</a>
```

258.3 Replacing the Single Channel Button with a Dual Channel Button

258.3.1 Replacing TURing image with a Dual Channel (SMS) request

Edit the file pinsafe_image.aspx

find the following line:

```
       url.AppendFormat("{0}:{1}/{2}/SCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

Replace with:

```
       url.AppendFormat("{0}:{1}/{2}/DCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

258.3.2 Compatibility

This has been tested on Citrix Web Interface 5.1

258.3.3 Dual Channel Button modification

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending , and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
    <div class="otcButtonPane"><a
           href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
           onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
           onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
           tabIndex="<%=Constants.TAB_INDEX_FORM%>"
           id="dcmessage"
           name="dcmessage"
       ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

To change the Refresh Image button modify the file under auth\clientscripts\login.js.add and search for the line Refresh Image and change to the required text, such as Request Code or Request SMS.

```
          "<span class='rightDoor'>Refresh Image</span>" +"
```

258.3.4 Dual Channel Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

258.4 Single Channel Button with an automated Single Channel Image

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to automatically show the Turing image without the need for pressing the button when the user enters into the required field.

258.4.1 Compatibility

This has been tested on Citrix Web Interface 5.1 using the Single Channel Turing Image

258.4.2 Single Channel Button to automated Single Channel Image modification

Edit the loginMainForm.inc file on the Citrix server. Locate the username field - look for the following:

```
<input type='text' name='<%=Constants.ID_USER%>' ...
```

insert the following line after that one:

```
onblur='onTuringButtonClick()'
```

This causes the turing image JavaScript function to be called when the user leaves the username field.

258.4.3 Automated Single Channel Image Testing

Test the image from the login page. Check the Swivel logs for the single channel image requests.

258.5 Turing, Dual channel and Display Index buttons

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to add additional buttons of Show Turing Image, Send Dual Channel Security String and Display Index number. See also Multiple Security Strings How To Guide

258.5.1 Compatibility

This has been tested on Citrix Web Interface 5.3

258.5.2 Required Files

The following files are required and should be used for installation: [1]

258.5.3 Installation Instructions

Follow the installation instructions for the relevant Citrix version.

258.5.4 Testing

Verify that three buttons are displayed and that they show the expected results when selected.

The following screen shots show the different buttons in use

Single Channel TURing Image request

Multiple Security String Message index number telling user which security string to use for authentication

Securiy String On Demand Confirmation message of sending the user a Security String

259 Cyberoam UTM SSL VPN

260 Introduction

This document describes steps to configure a Cyberoam UTM firewall with integrated SSL VPN and PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility. It is not possible to embed the graphical single channel image directly into the login page.

260.1 Prerequisites

Cyberoam CRxxx (except CR15i and CR15wi as these do not have SSL VPN support)

Cyberoam Firmware 10.x

PINsafe 3.x

260.2 Baseline

Cyberoam CR25i firmware 10.01.0 build 739

PINsafe 3.8

260.3 Architecture

The Cyberoam CR25i makes authentication requests against the PINsafe server by RADIUS. PINsafe can also verify the AD or other supported repository password where required.

261 Swivel Configuration

261.1 Configuring the RADIUS server

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

If Tight Integration is to be used with RADIUS groups then ensure RADIUS Groups is set to YES.

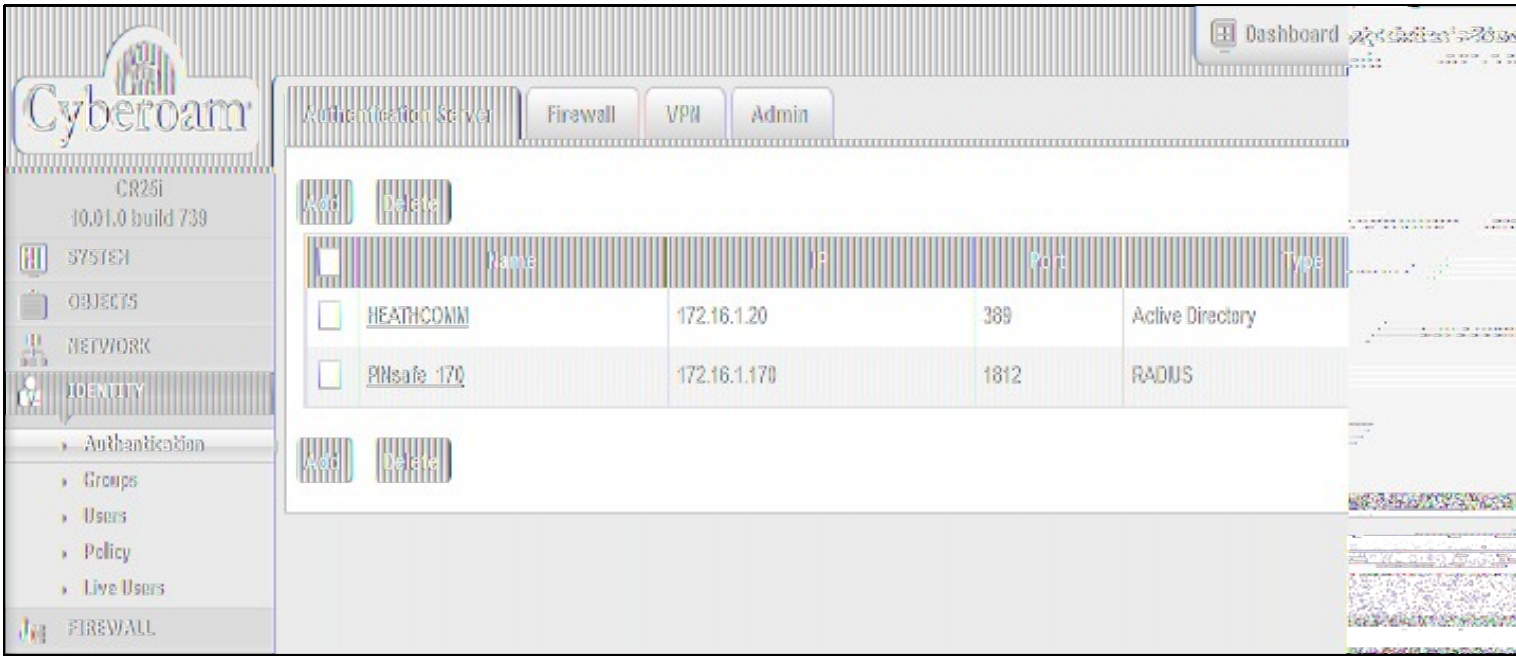
261.2 PINsafe Dual Channel Authentication

See Transport Configuration

262 Cyberoam CR25i Configuration

262.1 Define a RADIUS server on the Cyberoam

On the Cyberoam CR25i Administration console select Identity, then Authentication and the Authentication Server Tab, then click on Add.



Enter the PINsafe RADIUS server authentication details as follows:

- Server Type: RADIUS Server
- Server Name: Descriptive name for the PINsafe server
- Server IP: PINsafe server IP address
- Authentication Port: usually 1812
- Shared Secret: A secret password also entered on the PINsafe RADIUS NAS entry
- Integration Type: Loose Integration or Tight Integration as described below:

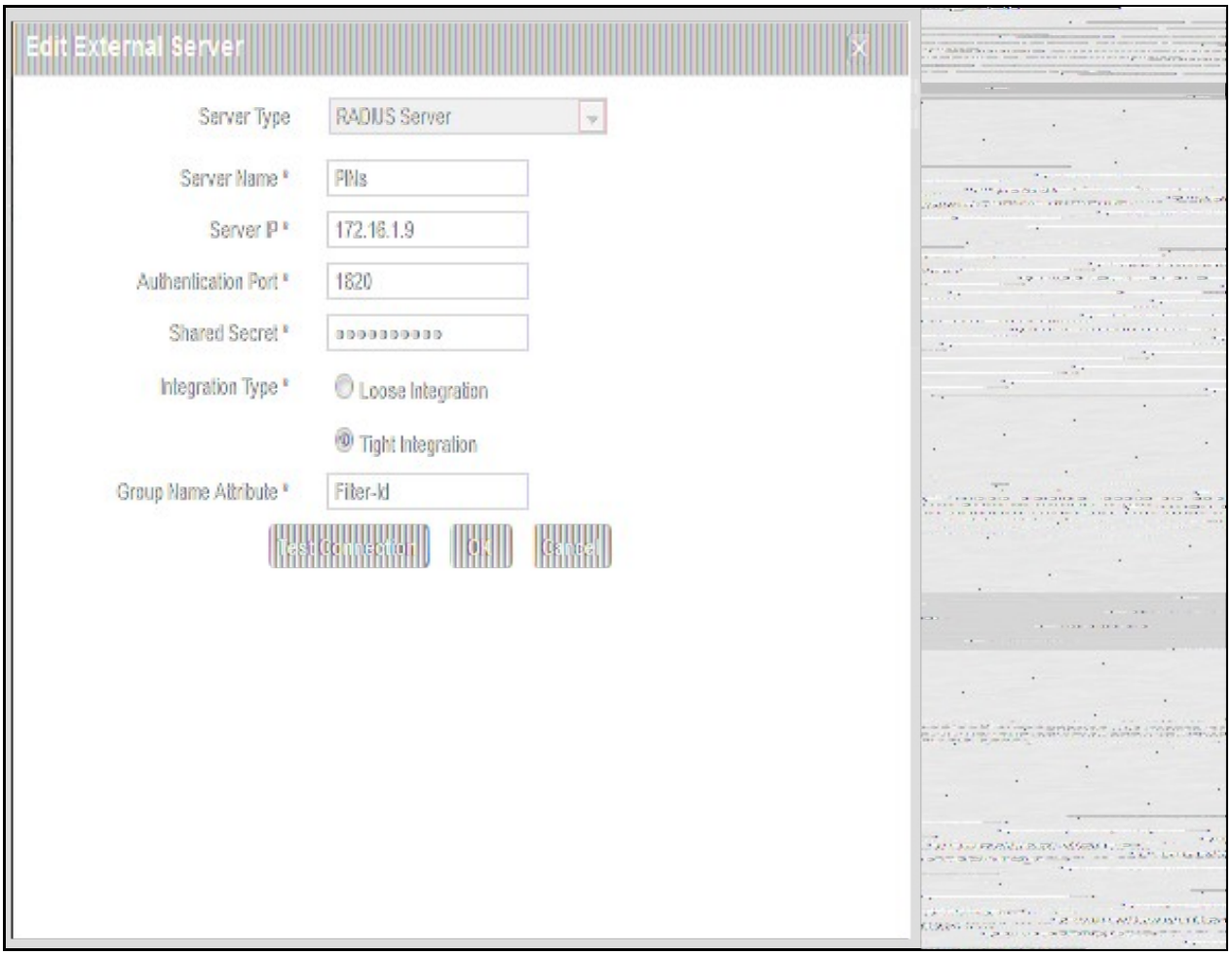
262.1.1 Loose Integration

With loose integration, Cyberoam does the Group management and does not synchronize groups with RADIUS server when user tries to logon. By default, users will be the member of Cyberoam default group irrespective of RADIUS Server group. Administrators can change the group membership. If Loose Integration is used, new users will be added to the default user group on the Cyberoam.

262.1.2 Tight Integration

With Tight integration, Cyberoam synchronizes groups with the PINsafe RADIUS Server every time the user tries to logon. Hence, even if the group of a user is changed in Cyberoam, on each subsequent login attempt, the user logs on as the member of the same group as configured on the PINsafe RADIUS Server. In this case group membership of each user is as defined in the RADIUS Server. The PINsafe RADIUS server needs to be configured to use RADIUS groups.

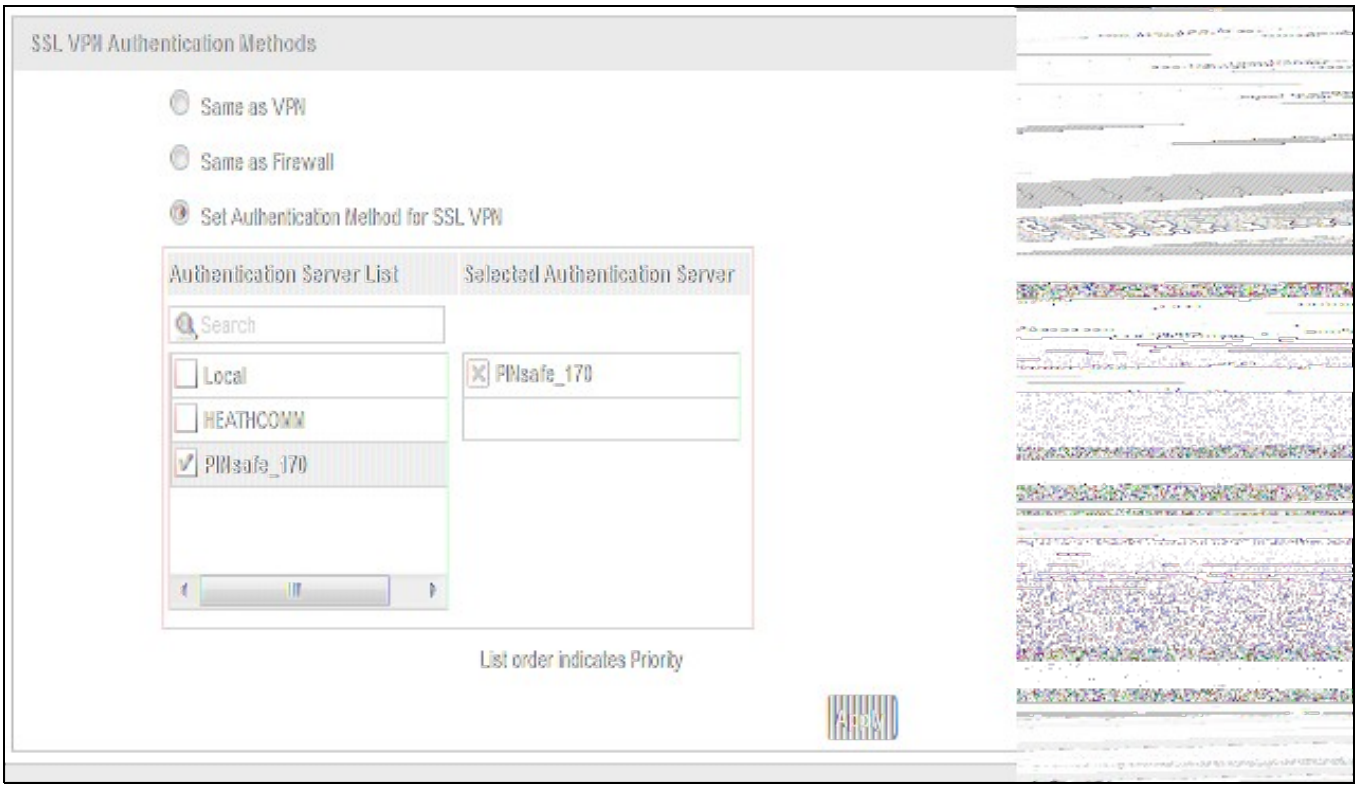
Note: when creating a SSL VPN policy, a user needs to login to the Captive Portal first, which creates the RADIUS user on the Cyberroam. They can then login to the SSL VPN portal



262.2 Cyberoam SSL VPN Authentication Methods

On the Cyberoam Administration console select Menu Identity, then Authentication then the VPN tab and select the Set Authentication Method for SSL VPN. All authentication servers that have been configured on the unit is shown on the left side. So the PINsafe RADIUS server added in the previous step should show up here. Tick the server to select it. It will then be shown in the list on the right side. It is possible to select more than one server if you have an active/active PINsafe configuration.

Note is is not possible to check authentication against multiple authentication types, the first authentication method that matches the user will be used. To configure authentication with multiple authentication servers see Additional Cyberoam Configuration Options below.



262.3 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.

262.4 Additional Cyberoam Configuration Options

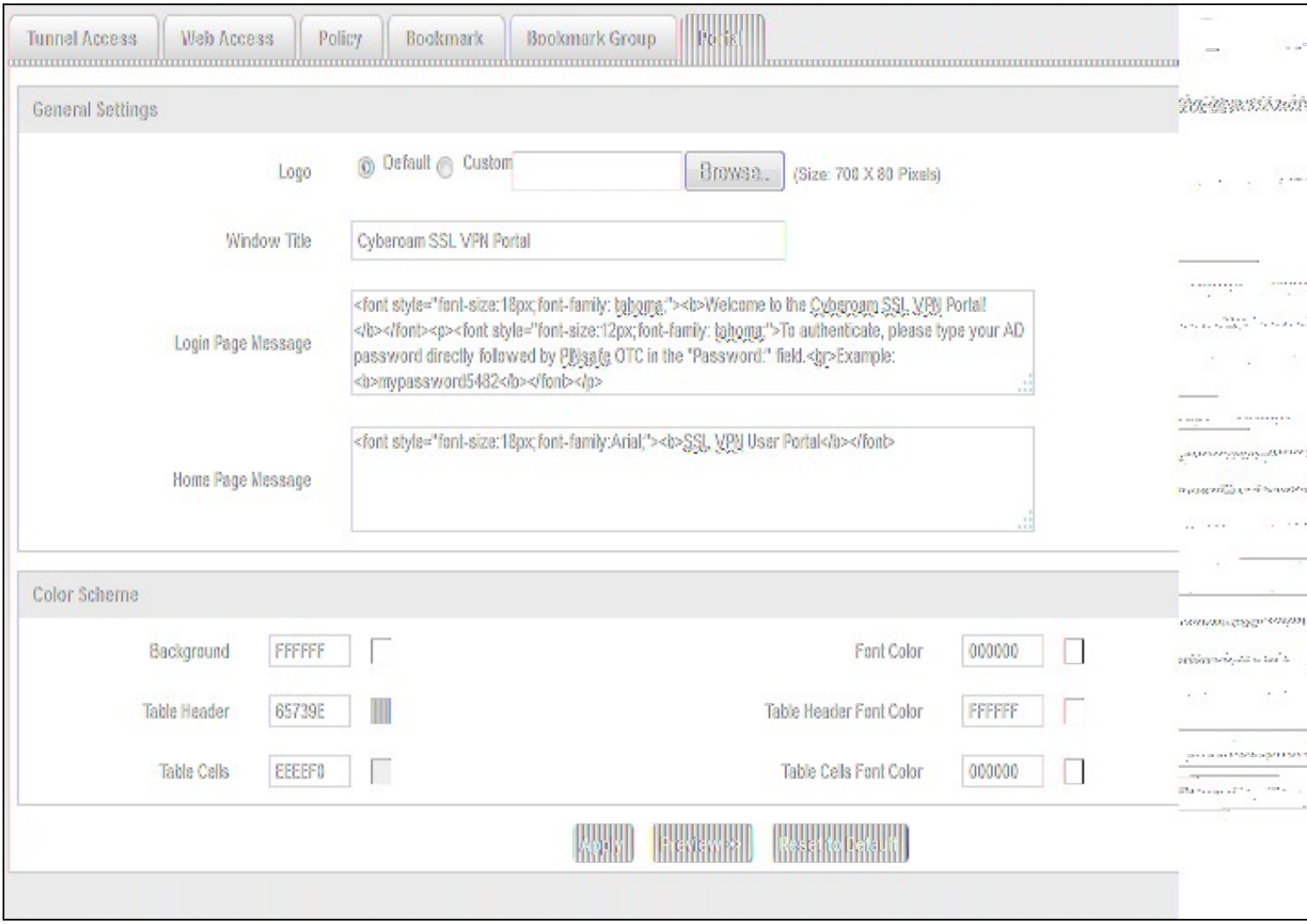
262.4.1 Configuring Authentication with AD Password and OTC

PINsafe can be configured to Check the password of supported repositories such as Active Directory. To do this the Check Password with repository must be enabled on the PINsafe server. PINsafe 3.7 and earlier have this as a global setting affecting all users, to select this option on the PINsafe Administration Console select Policy then Password, for PINsafe 3.8 onwards, it is defined by each NAS, under RADIUS then NAS. For more information see the Password How to Guide

The Password must be entered followed directly by the OTC on the login page by the user, e.g. passwordnnnn

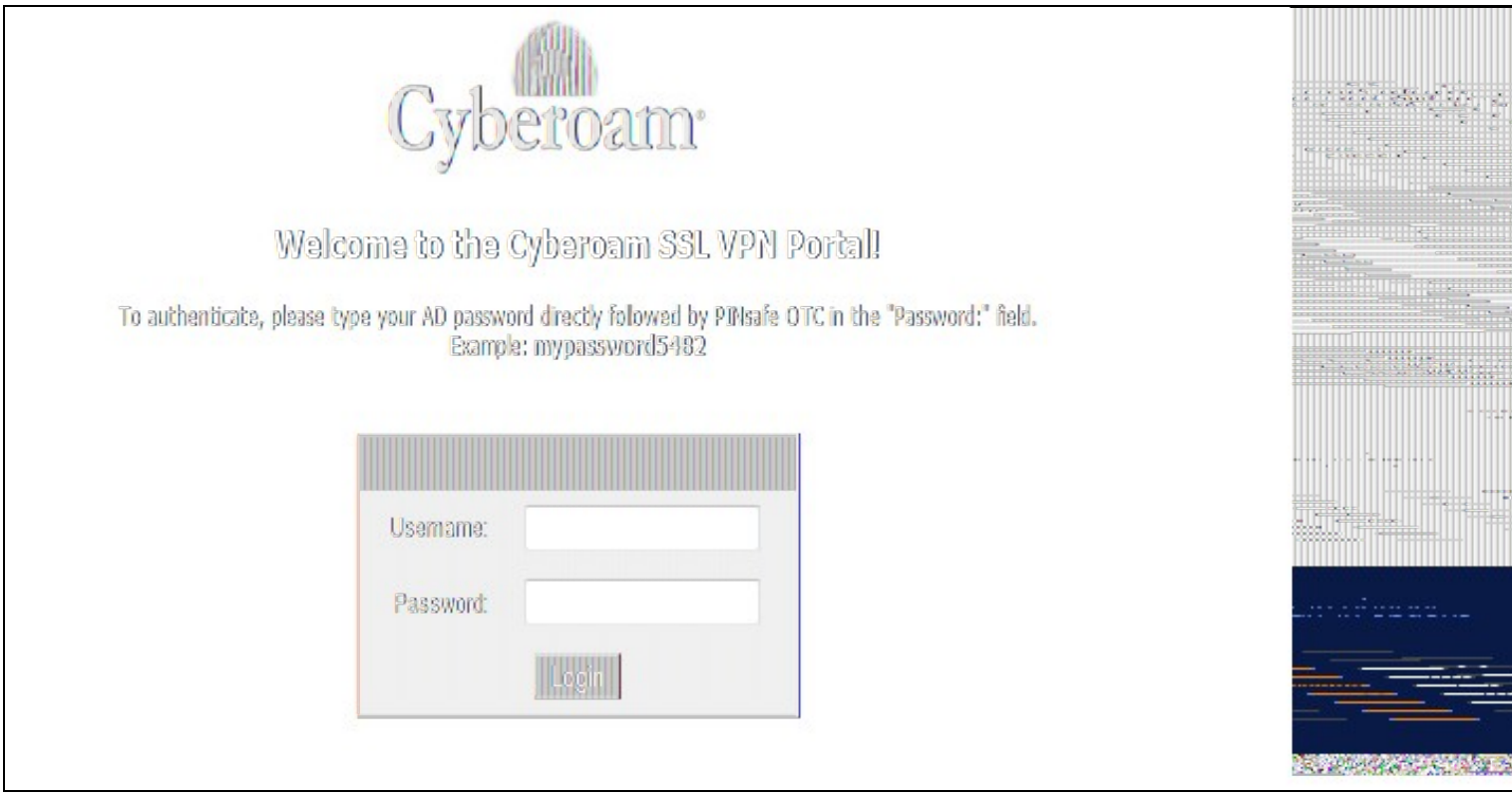
262.4.2 Modifying the Cyberoam login page

The Cyberoam login page can be modified to display different text and colours. To do this, on the Cyberoam Administration console select VPN, then SSL then select the Portal Tab. The below example shows modification for explianing how to add AD password and One Time Code.



262.5 Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. The below example shows the combination of AD password with OTC for authentication.



262.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

262.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

262.8 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

263 Deploy ACD using MS group policies

264 Introduction

These are the instructions to use the windows group policies to "deploy" the AuthControl Desktop (Credential Provider).

265 Steps

1 - Install the Credential Provider on a single machine. Configure it as required, then use File, Export Settings from the configuration program to create a settings file named acd.xml. Alternatively, if you have a pre-configured build, there is no need for this step.

2 - Create a network share that can be accessed by all computers. Copy both the credential provider MSI and acd.xml (if required) to that folder.

3 - From the domain controller, in Server Manager, select the Tools menu, then "Group Policy Management".

4 - Select the domain node on the left-hand window. Right-click and choose "Create a GPO in this domain and link it here".

5 - Give the GPO a name, such as "AuthControl Credential Provider", and click OK.

6 - Under Group Policy Objects, find the GPO you just created, right-click on it and click Edit.

7 - Choose Computer Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

8 - From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Leave deployment method as "Assigned".

9 - Choose User Configuration, Policies, Software Settings, Software installation and repeat the last 2 steps, except this time, the deployment method should be "Published".

10 - Close the editor and left-click on the GPO. Under Scope you should see the domain name in the Links section. Right-click on it and check "Enforced". Note that this will install the CP on every computer in the domain. It should be possible to restrict the policy to a single Organisational Unit, by applying the GPO link to that OU. You can only apply policies to domains or OUs, not ordinary containers. You can also restrict the policy by creating a group of computers and adding that group to Security Filtering.

9a) Choose User Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

9b) From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Set deployment method to "Published".

266 Notes

Our understanding is that steps 7 and 8 make the software available for network installation. This step installs the software automatically if it is not yet installed, the next time each user connects to the domain.

The notes on the final step suggest how you can restrict which computers have the WCP installed.

Check the link below for more details:

https://support.microsoft.com/en-gb/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server

267 Changing Settings

If you want to change the settings for computers that already have AuthControl Desktop installed, for example, to enable or disable test mode, currently the only way to do this is to change the registry settings directly.

All the settings are in the following registry key:

\\HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\AuthControl Desktop

You will need to know the names of the settings in the registry: please contact Swivel Secure support for specific requests. We will give an example below of enabling or disabling Test Mode, for which the setting name is "TestMode".

1. Open "Group Policy Management" from a Domain Controller.
2. Right-click on the domain, or an OU if you only want to apply the policy to a subset
3. Select "Create a GPO in this domain and link it here". Give the GPO a name.
4. Right-click on the GPO and select "Edit"
5. Expand the tree for "Computer Configuration" -> "Preferences" -> "Windows Settings" -> "Registry"
6. Right-click on "Registry" and select New -> Registry Item
7. Make sure that action is "Update" and Hive is "HKEY_LOCAL_MACHINE"
8. Enter Key Path as "SOFTWARE\Swivel Secure\AuthControl Desktop". Make sure you type this correctly, including the correct spacing
9. Enter the Value name as "TestMode". To change a different value, enter the name as given by Swivel Secure
10. Set the value type to REG_DWORD (this is for numeric or on/off settings - for text settings use REG_SZ)
11. Set the value data to 1 to enable TestMode, or 0 to disable it.
12. Click OK

Note two points:

- The settings are only applied when a computer is restarted
- The settings are not applied immediately, so it is possible that the first login after restart will still use the old settings.

268 Ericom PowerTerm WebConnect

269 Introduction

This article describes how to integrate Swivel with the PowerTerm WebConnect by Ericom using SMS, Mobile Client and the Taskbar utility. It is not possible to embed the Single Channel within the login page.

270 Prerequisites

Swivel 3.3

PowerTerm WebConnect

271 Baseline

Swivel 3.9

272 Architecture

Ericom PowerTerm WebConnect authenticates users by using RADIUS authentication against Swivel.

273 Installation

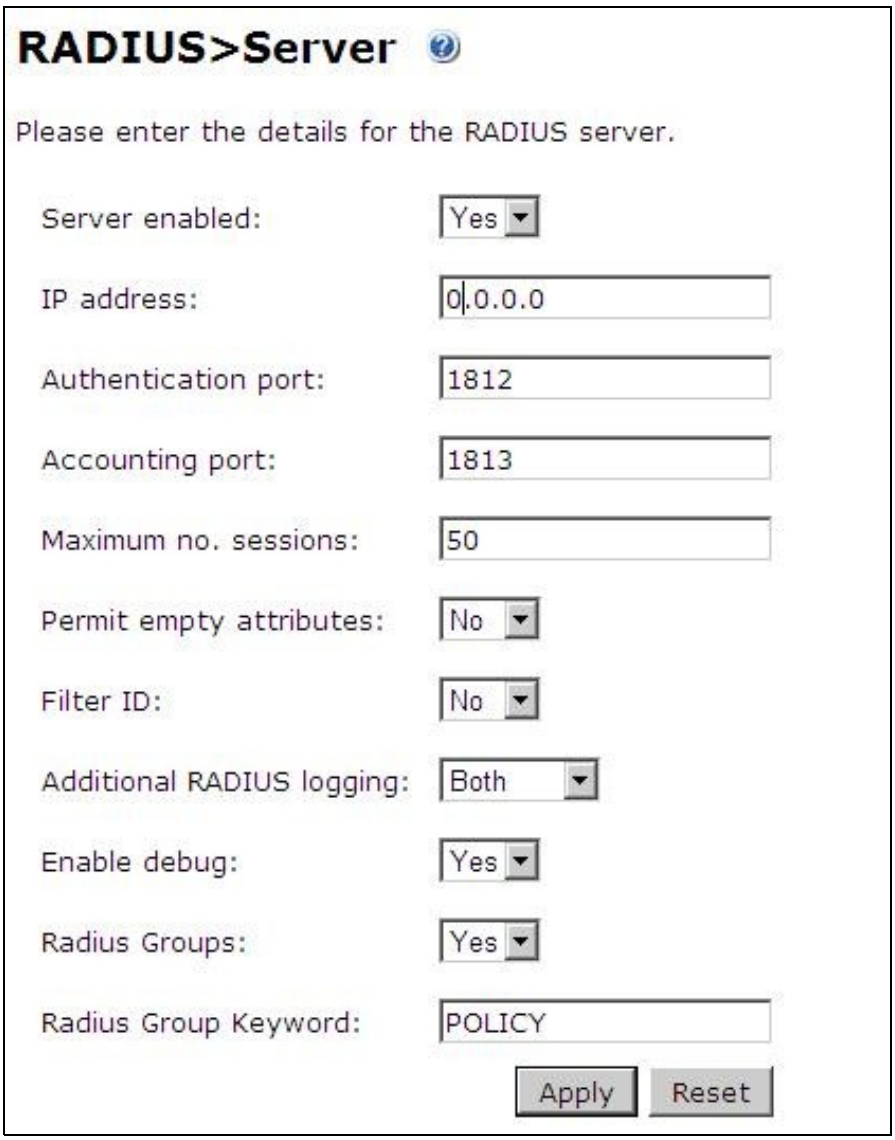
273.1 Swivel Integration Configuration

273.1.1 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.

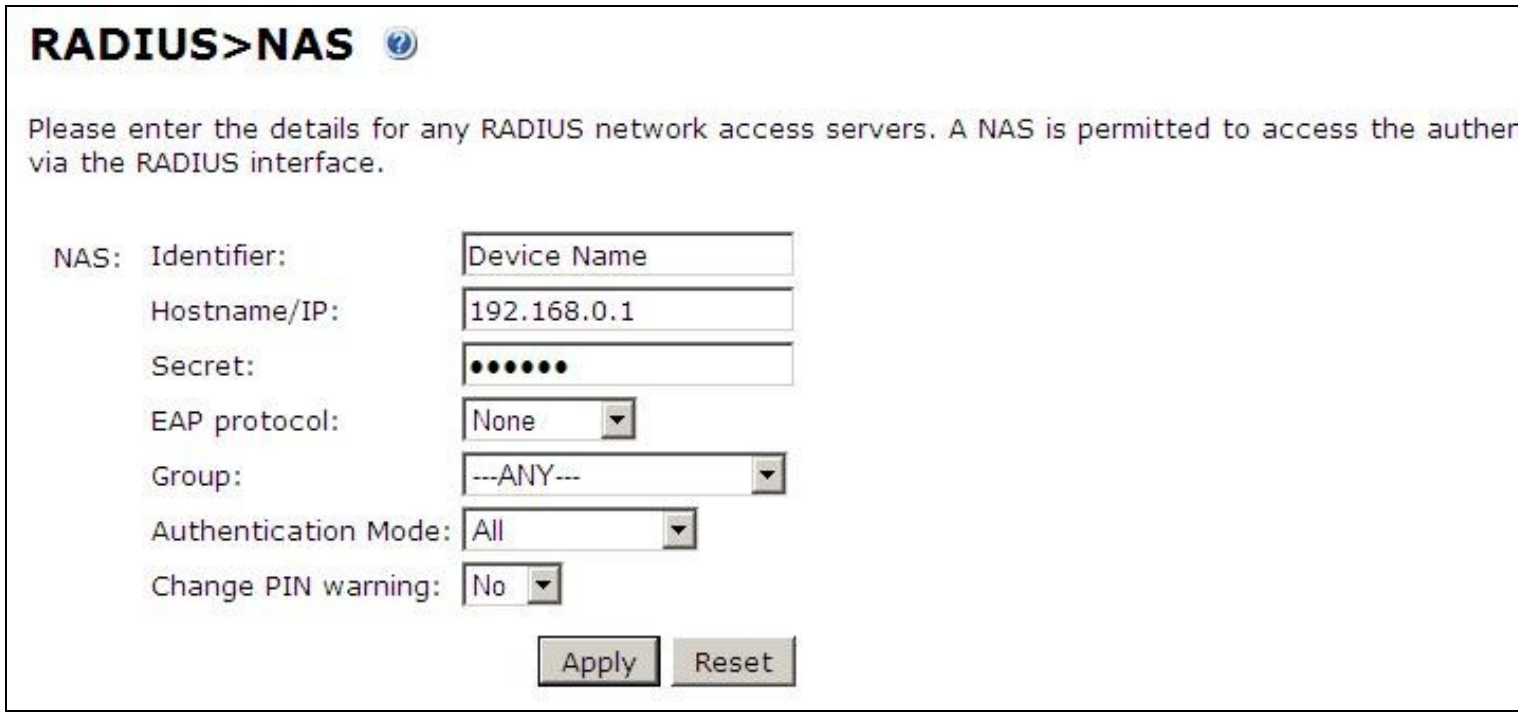
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

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



273.1.2 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.



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.

273.2 Ericom PowerTerm WebConnect Integration

273.2.1 RADIUS Server Configuration

Launch the PowerTerm WebConnect Administration Console and go to the Main Configuration (Files | Configuration | Main).

In the [ConnectionPoint=Internet] section set the option AuthenticationMethod=Radius.

This setting specifies that connections to this Connection Point will be authenticated with RADIUS.

Configure settings for the RADIUS connection

Radius_server Address of the Swivel RADIUS server

Radius_port (UDP) port that the Radius server is listening on. Default: 1812

Radius_sec_timeout timeout to wait for response from the Radius server. Default: 2

Radius_retries number of times to retry sending of the authentication request if a timeout occur. Default: 3

Radius_secret RADIUS server?s secret password as entered in the NAS section of Swivel.

Restart the PowerTerm WebConnect Server service.

273.2.2 Configuring Applications

Go to applicable published application?s Advanced section (applicable applications are those that will be used by users authenticating with RADIUS). Uncheck the option Use WebConnect User Credentials. Place %u in the Username field, and %X?Network Password? in the Password field.

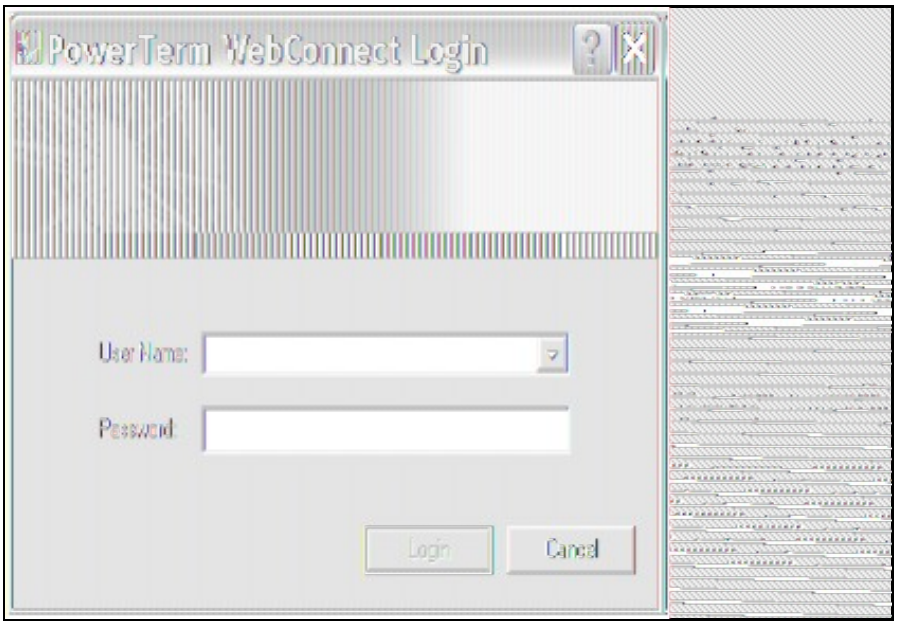
Uncheck the option ?Use Default Domain?

NOTE: Network Password should be entered exactly as is, do not replace the text with a user?s password. There needs to be a space between - ?Network? and ?Password?

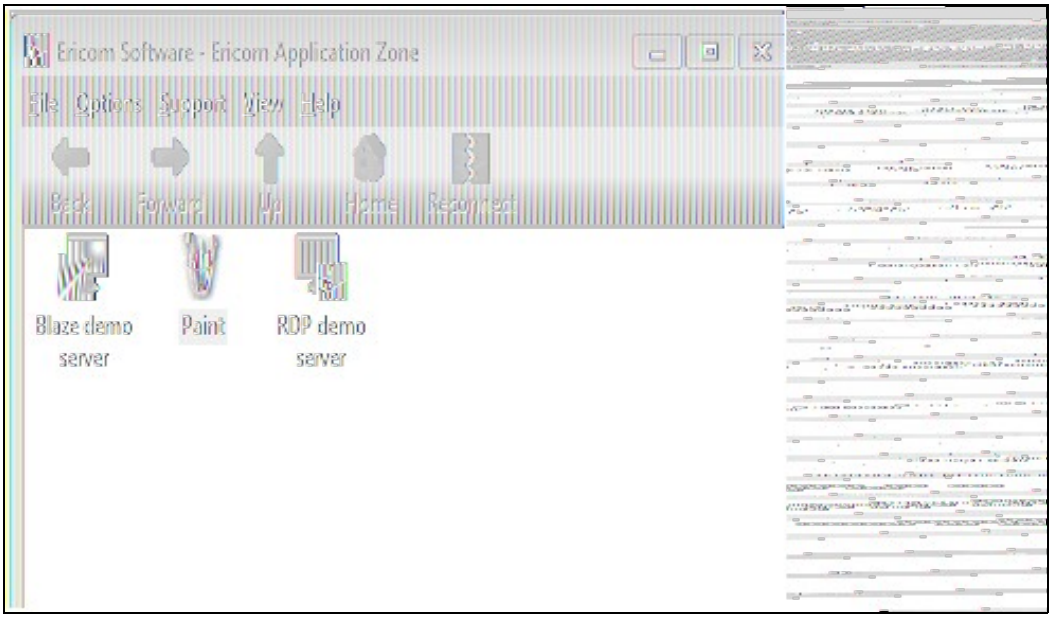
273.3 Additional Installation Options

274 Verifying the Installation

When users launch the Application Zone they will see the following screen, should log in with their username and Swivel One Time Code.



If the authentication is successful, the Application Zone will open displaying the users applications.



The first time the user launched an application, they will be prompted for their network password, as shown below.

The application will then open.

275 Uninstalling the Swivel Integration

Remove the RADIUS authentication for applications, check the option Use WebConnect User Credentials and remove the RADIUS server settings.

276 Troubleshooting

277 Known Issues and Limitations

278 Additional Information

279 F5 APM Integration

280 F5 Big-IP Access Policy Manager (APM) Integration Notes

This article describes how to integrate the F5 Big-IP Access Policy Manager with Swivel. The article covers two aspects:

- the integration of the two servers so that the F5 uses Swivel as its RADIUS server
- the modification of the F5 login page to include the TURing image or other Swivel elements as required.

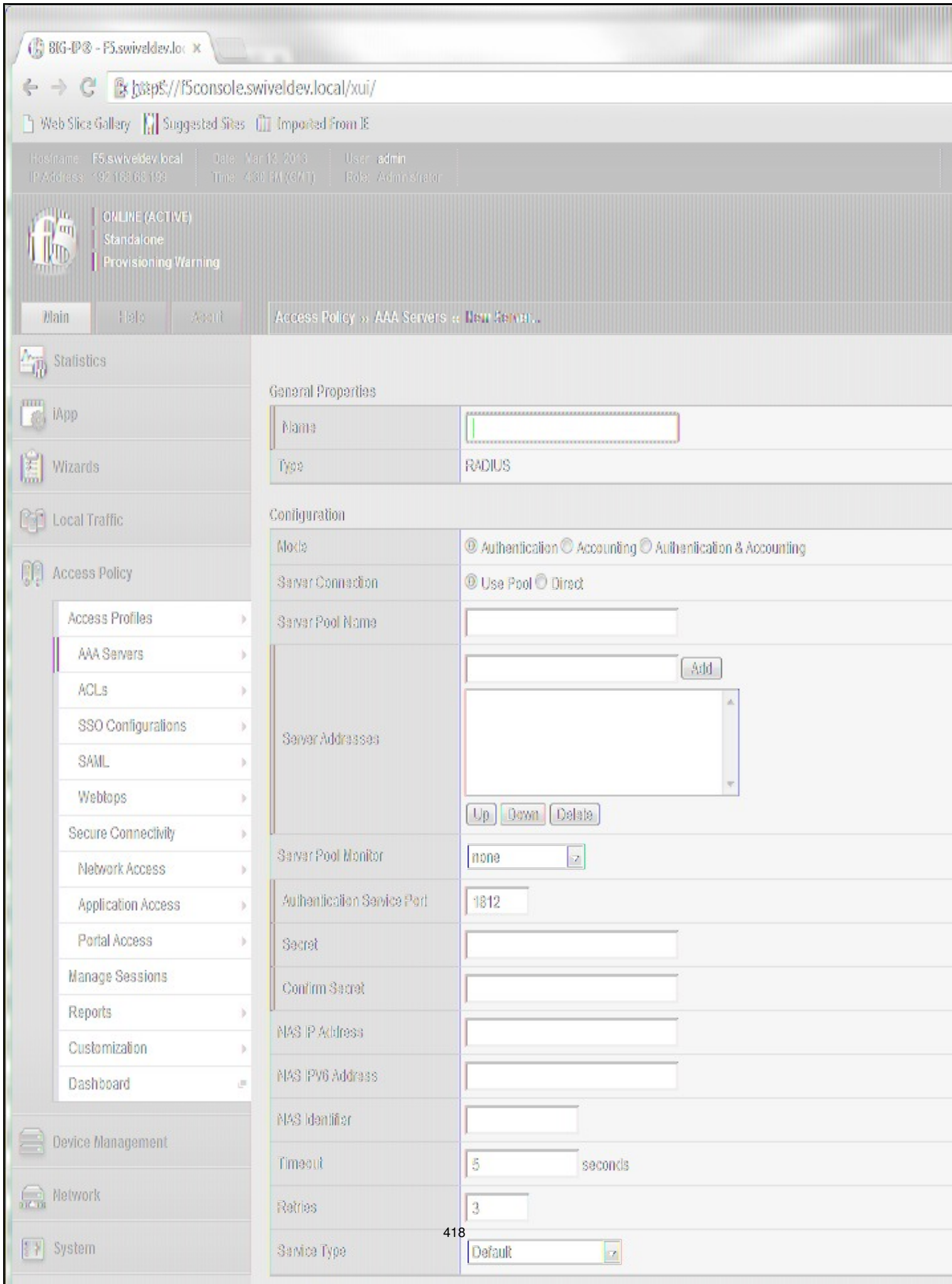
281 RADIUS Integration

To use Swivel with F5 Big-IP you need to enable the Radius Server on Swivel. (On the RADIUS->Server page)

A NAS Entry then need to be created that includes the F5 server IP address/hostname and a shared secret.

The associated configuration then needs to be created on the F5 server.

This is done on the Access-Policy->AAA-Servers screen.


BIG-IP® - F5.swiveldev.loc
https://f5console.swiveldev.local/xui/
Web Slice Gallery
Suggested Sites
Imported From IE
Hostname: F5.swiveldev.local
IP Address: 192.168.66.199
Date: Mar 13, 2013
Time: 4:30 PM (GMT)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Provisioning Warning
Main
Help
Acout
Access Policy » AAA Servers « New Server...
Statistics
iApp
Wizards
Local Traffic
Access Policy
Access Profiles
AAA Servers
ACLs
SSO Configurations
SAML
Webtops
Secure Connectivity
Network Access
Application Access
Portal Access
Manage Sessions
Reports
Customization
Dashboard
Device Management
Network
System
General Properties
Name
Type
RADIUS
Configuration
Mode
Authentication
Accounting
Authentication & Accounting
Server Connection
Use Pool
Direct
Server Pool Name
Server Addresses
Add
Up
Down
Delete
Server Pool Monitor
none
Authentication Service Port
1812
Secret
Confirm Secret
NAS IP Address
NAS IPV6 Address
NAS Identifier
Timeout
5
seconds
Retries
3
Service Type
Default

Once this entry has been created it can be used when defining Access Profiles.

It is important to remember the name of the profile created as this will be required for the customisation.

281.1 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.

282 Logon page Customisation

Once you have configured your access policy, you need to modify the logon page. You can edit it from the management console as follows:

From the Main menu, select Access Policy, then Customization. From the View dropdown, select Advanced Customization. From the folder tree, select Customization Settings -> Access Profiles -> [Your access profile] -> Access Policy -> Logon Pages -> Logon Page -> logon.inc.

Search for the line

```
function OnLoad()
```

Insert the following immediately before it:

For TURing image:

```
// **** PINsafe Customisation Start ****

// Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCImage?username=";

function ShowTuring() {
  var usernameField = document.getElementById("input_1");
  if (usernameField && usernameField.value && usernameField.value != "") {
    var img = document.getElementById("turing_img");
    if (img) {
      img.style.display = "";
      img.src = imageUrl + usernameField.value + "&random=" + Math.floor(Math.random()*10000);
    }
  }
}
// **** PINsafe Customisation End ****
```

Or for PinPad:

```
// **** PINsafe Customisation Start ****

// Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCPinPad?username=";

function ShowPinPad() {
  var usernameField = document.getElementById("input_1");
  if (usernameField && usernameField.value && usernameField.value != "") {
    var padno = Math.floor(Math.random() * 100000);
    for (var i=0; i<10; i++) {
      var img = document.getElementById("pinpad" + i);
      if (img) {
        var url = imageUrl + usernameField.value + "&padno=" + padno + ":" + i;
        img.src = url;
      }
    }
  }
}

function InsertPinPad() {
  var footerCell = document.getElementById("credentials_table_footer");
  if (footerCell) {
    var footerRow = footerCell.parentNode;
    var formTable = footerRow.parentNode;
    var pinpadRow = document.createElement("tr");
    pinpadRow.setAttribute("id", "turing_row");
    var pinpadCell = document.createElement("td");
    pinpadCell.setAttribute("colspan", "2");
    pinpadCell.setAttribute("align", "center");
    var pinpadTable = document.createElement("table");
    pinpadTable.style.height = "225px";
    pinpadTable.style.width = "150px";
    var row, cell, img;
    for (var r=1; r<=9; r+=3) {
      row = document.createElement("tr");
      for (var c=r; c<r+3; c++) {
        cell = document.createElement("td");
        cell.setAttribute("align", "center");
        img = document.createElement("img");
        img.src = "images/blank.png";
        img.setAttribute("id", "pinpad" + c);
        img.setAttribute("onclick", "AddDigit(" + c + ")");
        cell.appendChild(img);
        row.appendChild(cell);
      }
      pinpadTable.appendChild(row);
    }
    row = document.createElement("tr");
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
    img.src = "images/refresh.png";
    img.setAttribute("onclick", "ShowPinPad()");
    cell.appendChild(img);
    row.appendChild(cell);
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
    img.src = "images/blank.png";
    img.setAttribute("id", "pinpad0");
    img.setAttribute("onclick", "AddDigit(0)");
    cell.appendChild(img);
    row.appendChild(cell);
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
    img.src = "images/clear.png";
    img.setAttribute("onclick", "ClearOtc()");
    cell.appendChild(img);
```

```
    row.appendChild(cell);
    pinpadTable.appendChild(row);
    pinpadCell.appendChild(pinpadTable);
    pinpadRow.appendChild(pinpadCell);
    formTable.insertBefore(pinpadRow, footerRow);
  }
}

// Check that the following field is correct. If PINsafe is the ONLY form of authentication,
// or is the first authentication, it will be "input_2".
// If it is the second authentication, it will be "input_3".
var otcFieldId = "input_2";

function AddDigit(digit) {
  var otcField = document.getElementById(otcFieldId);
  if (otcField) {
    otcField.value += digit;
  }
}

function ClearOtc() {
  var otcField = document.getElementById(otcFieldId);
  if (otcField) {
    otcField.value = "";
  }
}

// **** PINsafe Customisation End ****
```

A few lines below this are the following lines:

```
if( form == null ){
  return;
}
```

Below this, insert the following for TURing:

```
// **** PINsafe Customisation Start ****
var footerCell = document.getElementById("credentials_table_footer");
if (footerCell) {
  var footerRow = footerCell.parentNode;
  var formTable = footerRow.parentNode;
  var turingRow = document.createElement("tr");
  turingRow.setAttribute("id", "turing_row");
  var turingCell = document.createElement("td");
  turingCell.setAttribute("colspan", "2");
  turingCell.setAttribute("align", "center");
  var turingImg = document.createElement("img");
  turingImg.setAttribute("id", "turing_img");
  turingImg.style.display = "none";
  turingCell.appendChild(turingImg);
  var turingBrk = document.createElement("br");
  turingCell.appendChild(turingBrk);
  var turingBtn = document.createElement("input");
  turingBtn.setAttribute("type", "button");
  turingBtn.setAttribute("value", "New Image");
  turingBtn.onclick = ShowTuring;
  turingCell.appendChild(turingBtn);
  turingRow.appendChild(turingCell);
  formTable.insertBefore(turingRow, footerRow);
}
// Optional: to automatically show the TURing after entering the username, include the following lines.
var usernameField = document.getElementById("input_1");
if (usernameField) {
  usernameField.onblur = ShowTuring;
}
// Optional: if the username is pre-populated, use the following line to display the TURing image immediately
ShowTuring();
// **** PINsafe Customisation End ****
```

or this for Pinpad:

```
  // **** PINsafe Customisation Start ****
  InsertPinPad();
  // The next section is optional - use this if you want to show the TURing automatically when the username changes.
  var usernameField = document.getElementById("input_1");
  if (usernameField) {
    usernameField.onblur = ShowPinPad;
  }
  // **** PINsafe Customisation End ****
```

282.1 Removing the Automatic TURing image

Remove or comment out the following lines with // at the front

```
// Optional: to automatically show the TURing after entering the username, include the following lines.
var usernameField = document.getElementById("input_1");
if (usernameField) {
  usernameField.onblur = ShowTuring;
}
```

For Pinpad, the penultimate line above will be

```
  usernameField.onblur = ShowPinPad;
```

The final step here is to set the image URL. There are a number of options:

- The simplest option is to use the Swivel Server directly. However, this requires that the Swivel Server is directly accessible from the internet, which is not a recommended solution, as it is a security risk. Also, you will need a commercial SSL certificate on the Swivel server to avoid problems with certificate errors. In this case, simply replace *<your_swivel_server>* above with the external URL of your Swivel Server.
- The second option is to create a virtual server on the F5 Big-IP to act as an anonymous proxy to the Swivel Server. This is suitable if the F5 is your only Swivel integration, as it requires that the F5 is set as the default gateway for your Swivel appliance. Details for this are not provided, as it should be clear from the F5 documentation how to do this. You might also want to create an iRule to restrict access only to the TURing image, as suggested below. In this case, you should replace *<your_swivel_server>* with the external URL of your F5. If you have set up the virtual server with a different service port, you might need to change this as well.

```
when HTTP_REQUEST {
  if { [HTTP::uri] starts_with "/pinsafe/SCImage?" } {
    pool PINsafe_8080
  } else { HTTP::respond 403 }
}
```

- The third option is suitable if you have other Swivel integrations. In this case, you can use the URL of the TURing image on the other integration to deliver the TURing image. For example, if you have an integration with Outlook Web Access, use the following:

```
var imageUrl = "https://<your_swivel_server>/owa/auth/SCImage.aspx?username=";
```

Here, replace *<your_swivel_server>* with the URL of your OWA server.

Another example: if you have a UAG integration, use the following:

```
var imageUrl = "https://<your_swivel_server>/InternalSite/images/customupdate/images.asp?username=";
```

NOTE: If you are using Pinpad, substitute **SCPinPad** for **SCImage** above.

283 Testing

Now when the F5 server is accessed via the **pinsafe** access policy the user should see a modified login page with the option to request a TURing image.

The user should enter their username and see a TURing image when the click the TURing button. At this point a Session Start message for the user should show in the PINsafe logs.

If no image shows, check that the URL is correct and ensure that there is no firewalls blocking the request.

Also check that Session Create by Username is enabled on the Swivel server.

The user should then enter their one-time code. The login.

If the log-in fails, check the Swivel log files to see if a RADIUS request was logged. If not then check the settings for the RADIUS on F5 and Swivel to ensure IP Addresses, port numbers and shared secrets all match. Also check that no firewalls are blocking the RADIUS requests.

If RADIUS attempts are being logged but authentication is failing, check that the session was started correctly and that there is no password associated with the account etc.

284 F5 Firepass Integration

284.1 Introduction

This document outlines the steps required to integrate the F5 Networks FirePass SSL VPN with the Swivel PINsafe authentication server.

FirePass VPN appliances are able to use external RADIUS servers for providing authentication. The PINsafe server provides RADIUS authentication, thus the FirePass VPN can be configured to use the PINsafe server for authentication via RADIUS.

PINsafe users can use either PINsafe?s Single Channel (TURing, PATtern) or Dual Channel (SMS, Swivlet applet) methods to retrieve Security Strings, which are applied against the user?s PIN to extract a One-Time Code (OTC) which represents the password for an authentication request.

With Dual Channel methods, the user already holds one or more Security Strings on their mobile device (and can request more at any time) so with the FirePass VPN configured to use the matching PINsafe server for RADIUS authentication, no further integration is required.

However with Single Channel methods, the user must be presented with a TURing or PATTern image upon login (representing a single time-limited Security String), so they can extract their OTC. The Authentication configuration section below describes how to achieve the RADIUS configuration. Single Channel requires access to the PINsafe server by a Public IP address.

284.2 Prerequisites

284.2.1 Baseline

The FirePass VPN appliance tested was FirePass 600. (http://www.f5.com/products/FirePass/FP600.html)

The PINsafe server used was PINsafe v3.1. However, no changes have been made to PINsafe since then which would render the integration invalid.

The primary web browser used for testing was Internet Explorer 6.0.2900.2180.xpsp_sp2_gdr.050301-1519.

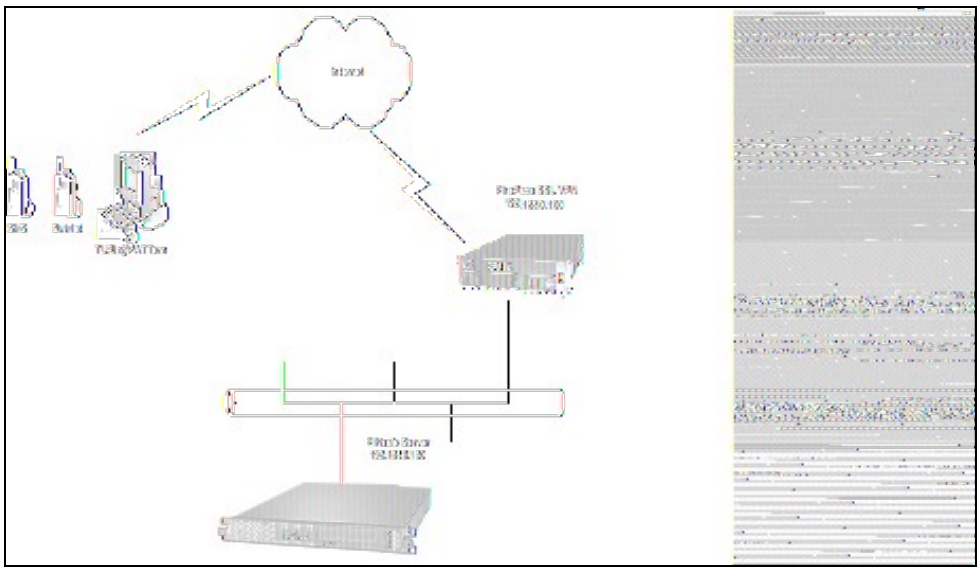
284.3 Architecture

The user connects to the FirePass VPN using a web browser, pointing to the appropriate login URL for the VPN in question.

The FirePass VPN is configured to use a PINsafe server for RADIUS authentication.

Users are stored and maintained in the PINsafe server.

Figure 1. The following diagram shows the configuration used and is typical. This example is used throughout this document:



284.4 Installation

284.4.1 PINsafe Configuration

Configuration of the PINsafe server for RADIUS authentication with the FirePass VPN consists of three steps:

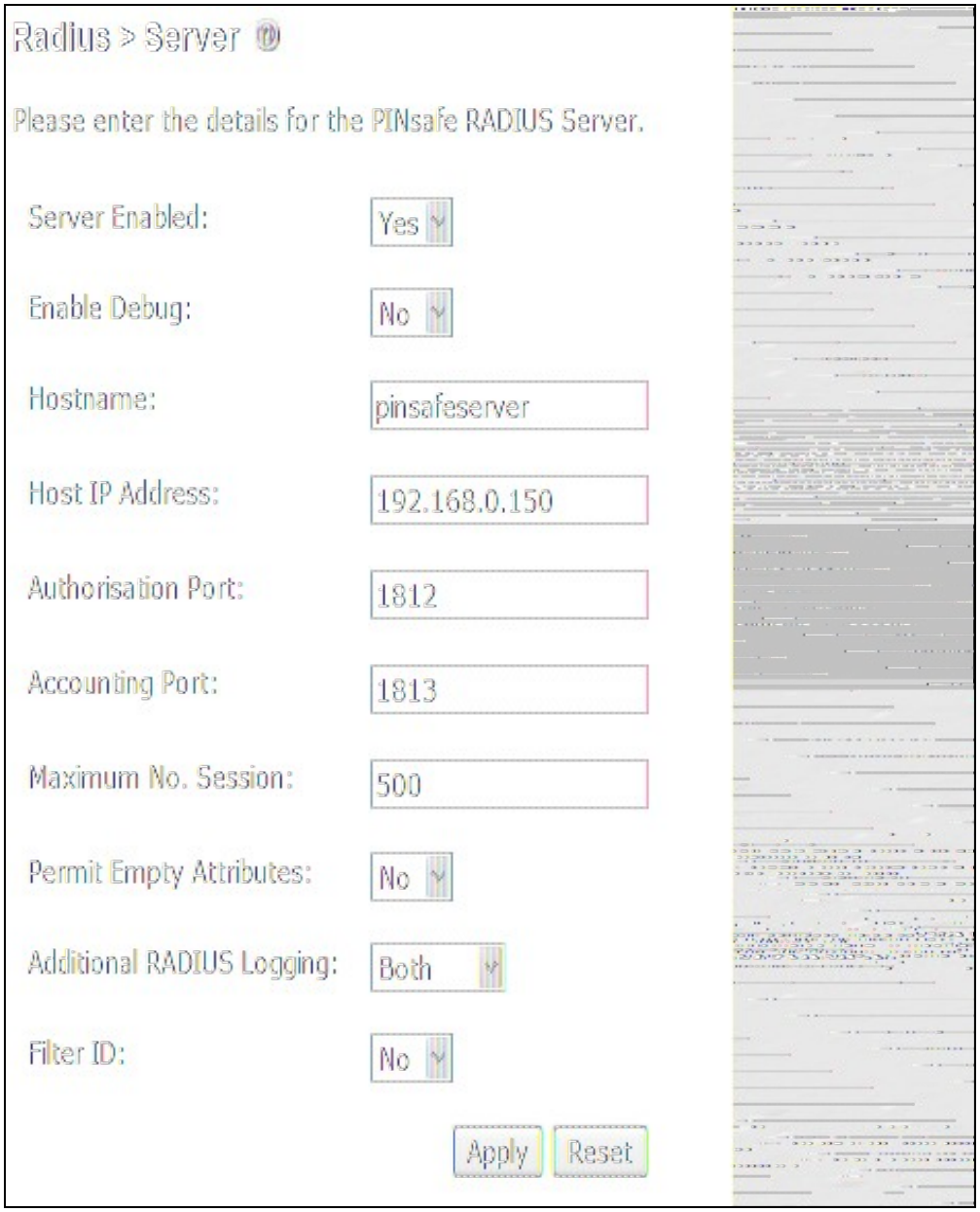
1. Configure PINsafe RADIUS settings.
2. Set up the NAS (Network Access Server), which in this case is the FirePass VPN.
3. Configure the PINsafe server to allow TURing/PATTern session creation with a username.

NOTE ? This document assumes that the PINsafe server has been configured to use a specific user repository and populated with users. Please refer to the PINsafe Administration Guide for detailed instructions.

1. Configuring PINsafe RADIUS settings

Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In our example (see diagram above) the RADIUS Mode is set to ?RADIUS Server? and the HOST IP (the PINsafe server) is set to 192.168.0.150.

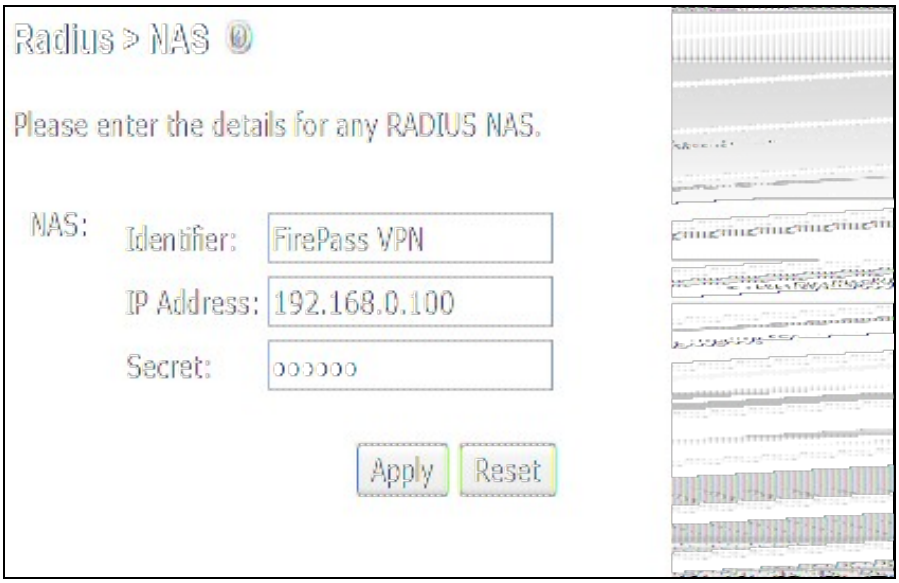
Figure 2. PINsafe RADIUS configuration page.



2. Setting up the NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. In our example (see Figure 3), the meaningful name ?FirePass VPN? has been assigned so it can be identified if you have more that one NAS configured. The IP address has been set to the IP of the VPN appliance, and the NAS secret assigned that will be used on both the PINsafe server and VPN RADIUS configuration.

 Figure 3. Extract from PINsafe NAS setup page



3. Configure the PINsafe server to allow TURing/PATTern session creation with a username.

The PINsafe server must be configured to allow a Single Channel session to be created by accessing a specific URL on the PINsafe server. The following URL would create a start a session and return the image for the user ?test?:

For a Swivel hardware or virtual appliance http://Swivel_IP:8443/proxy/SCImage?username=test

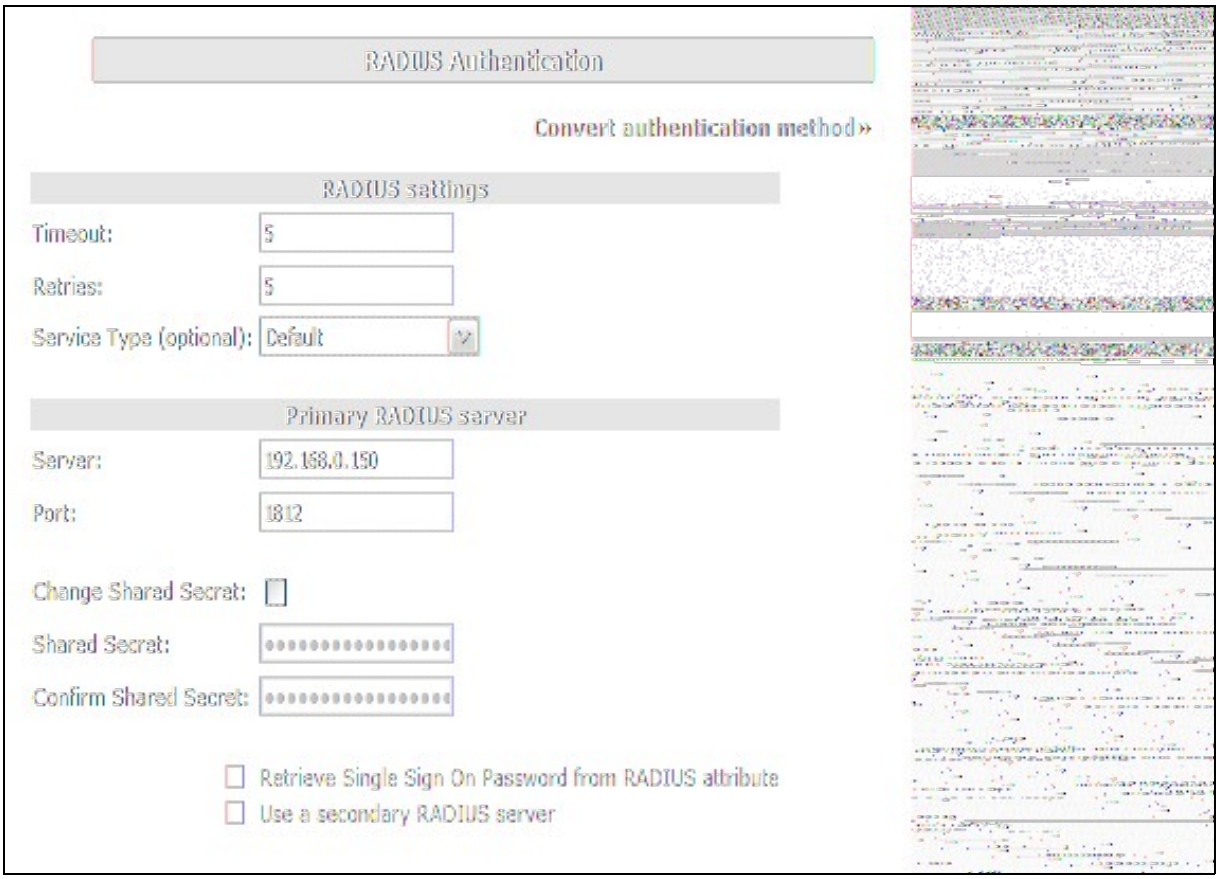
For a software only install see Software Only Installation

284.5 F5 Networks FirePass VPN Configuration

The RADIUS FirePass configuration is found under Users, Groups, Master Groups, Radius_Users, and then the Authentication tab. The Primary RADIUS server was set to the IP address of the PINsafe server followed by the authorization port (see Figure 5). The shared secret entered was the same secret entered in the PINsafe NAS entry (see Figure 3).

If you want to configure a secondary PINsafe RADIUS server for failover you would add the details of the server in the ?Secondary RADIUS server? section on this page. If you are utilizing the High Availability PINsafe solution, failover/redundancy is managed by that solution, thus you would only enter the Primary RADIUS server address.

Figure 4. Extract from FirePass RADIUS Authentication setup page



284.6 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.

284.7 Modifying the FirePass login page for PINsafe TURing image

The PINsafe sends Security Strings to users via SMS, Swivlet applet (Dual Channel) or through a TURing image (Single Channel) accessed by public IP address from the PINsafe server. The user extracts their One Time Code (OTC) from the Security String and enters it into the VPN sign-in. If the user has been assigned a PINsafe server static password, they must enter the password plus their OTC. For example, if the user?s PINsafe static password was ?foobar? and their OTC were 7452, they would enter ?foobar7452? at the login prompt.

If the PINsafe user were configured to use Dual Channel (SMS or applet), they should have a security string ready on their mobile device. No modification to the FirePass login page would be required. For Single Channel users, we need some way of presenting a TURing image on the FirePass VPN?s login page. This can be achieved through configuration of the FirePass login screen via WebDAV.

To enable WebDAV based customization

1. Create an HTTP web service on the Device Management : Configuration : Network Configuration : Web Services screen.
2. Select the **Allow insecure access** option on the Device Management : Security : User Access Security screen.
3. Check **Allow WebDAV sandbox customization** on the Device Management : Customization screen and enter a WebDAV password in the text box that appears.

The WebDAV sandbox is accessed via HTTP at the URI /**sandbox** as the user **webdav**. So, for example, if the FirePass controller has been configured using the steps above with a HTTP web service at 192.168.0.99, you would use the URL **http://192.168.0.99/sandbox/**.

Any content can be placed in the sandbox directory. The FirePass controller uses specific files to override or supplement stock system behavior. To add the TURing image to the right of the logon prompt, the **right.inc** file was created and added to the sandbox, with the following content:

```
<script language="JavaScript">


</script>

<input name="btnTuring" type="button" value="OTC Image" class="submitbutton" onclick="ShowTuring()" />

<img id="imgTuring" style="visibility:hidden;" alt="Turing image" />
```

Edit the following line with the correct IP address

sUrl="http://192.168.0.150:8443/proxy/SCImage?UserName=";

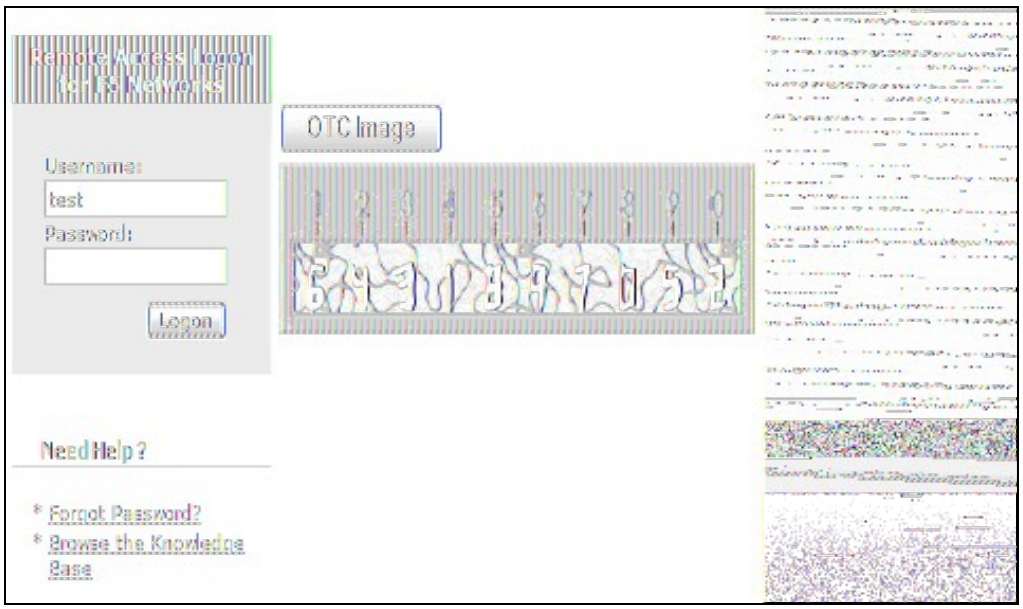
For PINsafe 3.1.3a and later the following line needs to be edited:

sUrl="http://192.168.0.150:8443/proxy/SCImage?username=";

To upload the WebDAV pages browse to the sandbox with a web browser using http (not https) and enter the WebDAV username and password.

Once loaded into the sandbox, the login page should contain a new button and the ability to display the TURing image.

Figure 6. Example of a modified FirePass login page



284.8 Verifying Installation

Navigate to the F5 interface login page. The customisation is visible in the addition of a **One Time Code Image** button. Only when a correct PINsafe one time code is entered should the user be logged in. This can be done either by entering the OTC for a dual channel login, or selecting OTC Image and entering the OTC for a single channel login.

284.9 Troubleshooting

Check the PINsafe logs for any failure information.

284.10 Additional Information

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

285 F5 SAM Integration

286 F5 Secure Access Manager (SAM) Integration Notes

This article describes how to integrate the F5 Secure Access Manager with Swivel. The article covers two aspects:

- The integration of the two servers so that the F5 uses Swivel as its RADIUS server
- The modification of the F5 login page to include the TURing image or other Swivel elements as required.

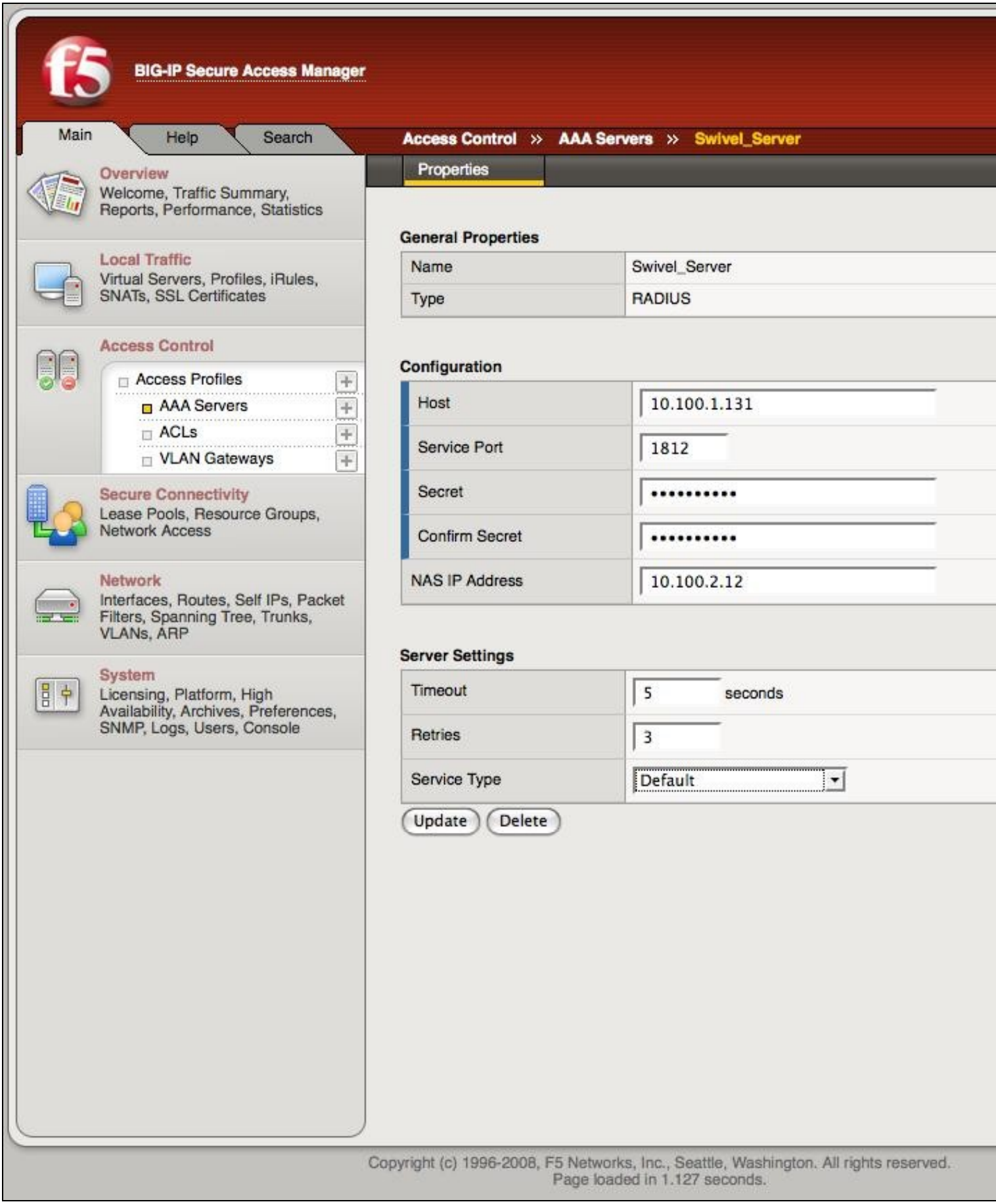
287 RADIUS Integration

To use Swivel with F5 SAM you need to enable the Radius Server on PINsafe. (On the RADIUS->Server page)

A NAS Entry then need to be created that includes the F5 server ip address/hostname and a shared secret.

The associated configuration then needs to be created on the F5 server.

This is done on the Access-Control->AAA-Servers screen.



Once this entry has been created it can be used when defining Access Profiles.

It is important to remember the name of the profile created as this will be required for the customisation.

287.1 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.

288 Log-in page Customisation

To modify the log-on page to include a TURing image you need secure-shell access (SSH) to the server.

Assuming that the Access Profile is called **pinsafe** the modifications are implemented by editing the file

/config/customization/advanced/logon/**pinsafe**_act_logon_page_ag/logon_en.inc

The steps are as follows.

1. Change directory to the required location

```
cd /config/customization/advanced/logon/pinsafe_act_logon_page_ag
```

2. Take a back-up of the existing file. Note that this example assumes that the Access Policy uses English. If another language is specified then you need to edit the corresponding file, eg log_fr.inc for French.

```
cp log_en.inc tmp_logon_en.inc
```

3. Edit the login file or copy a modified version of the file onto the server.

An example modified script is shown here. The required modifications are between the lines of asterisks. The setting of the sUrl variable needs to correspond to the PINsafe server being used.

4. To register the changes the following commands must be executed.

```
b customization group pinsafe_act_logon_page_ag action update
b profile access pinsafe generation action increment
```

289 Testing

Now when the F5 server is accessed via the **pinsafe** access policy the user should see a modified login page with the option to request a TURing image.

The user should enter their username and see a TURing image when the clcik the TURing button. At this point a Session Start message for the user should show in the PINsafe logs.

If no image shows, check that the URL is correct and ensure that there is no firewalls blocking the request.

Also check that Session Create by Username is enabled on the PINsafe server.

The user should then enter their one-time code. The login.

If the log-in fails, check the Swivel log files to see if a RADIUS request was logged. If not then check the settings for the RADIUS on F5 and Swivel to ensure the IP Addresses, port numbers and shared secrets all match. Also check that no firewalls are blocking the RADIUS requests.

If RADIUS attempts are being logged but authentication is failing, check that the session was started correctly and that there is no password associated with the account etc.

290 Fortinet Fortigate Integration

291 Introduction

This document describes steps to configure a Fortinet Fortigate with Swivel as the authentication server.

292 Prerequisites

Fortinet 3.x appliance and Fortinet 3.x integration script

or

Fortinet 4.x appliance and Fortinet 4.x integration script

Swivel 3.x

NAT/Public IP address if the Single Channel TURing image or other Dual channel images are to be displayed in the login page.

293 Baseline

Fortinet 3.x

Fortinet 4.x

Fortinet 6.x

Swivel 3.x

Swivel 4.x

294 Architecture

Fortinet authenticates users through RADIUS, and uses Swivel as a RADIUS server.

295 Swivel Configuration

295.1 Configuring the RADIUS server

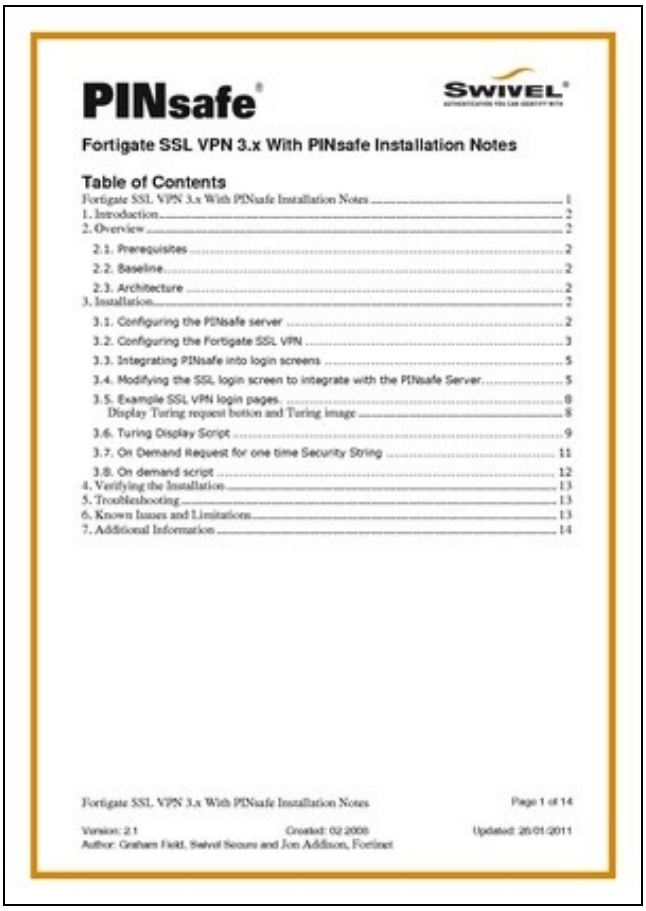
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

295.2 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.

296 Fortinet Fortigate Configuration

296.1 Fortinet FortigateVersion 3.x Integration guide



PINsafe®

SWIVEL®

Fortigate SSL VPN 3.x With PINsafe Installation Notes

Table of Contents

Version: 2.1 Created: 02 2008 Updated: 26/01/2011

Author: Graham Field, Swivel Secure and Jon Addison, Fortinet

296.2 Fortinet Fortigate Version 4.x Integration guide

On the Fortigate Administration console select User/Remote/RADIUS, then click on Create New and enter the following information:

Name A descriptive name for the Swivel RADIUS servers

Primary Server Name/IP The IP or hostname of the Swivel server (Do not use a Swivel VIP in this field)

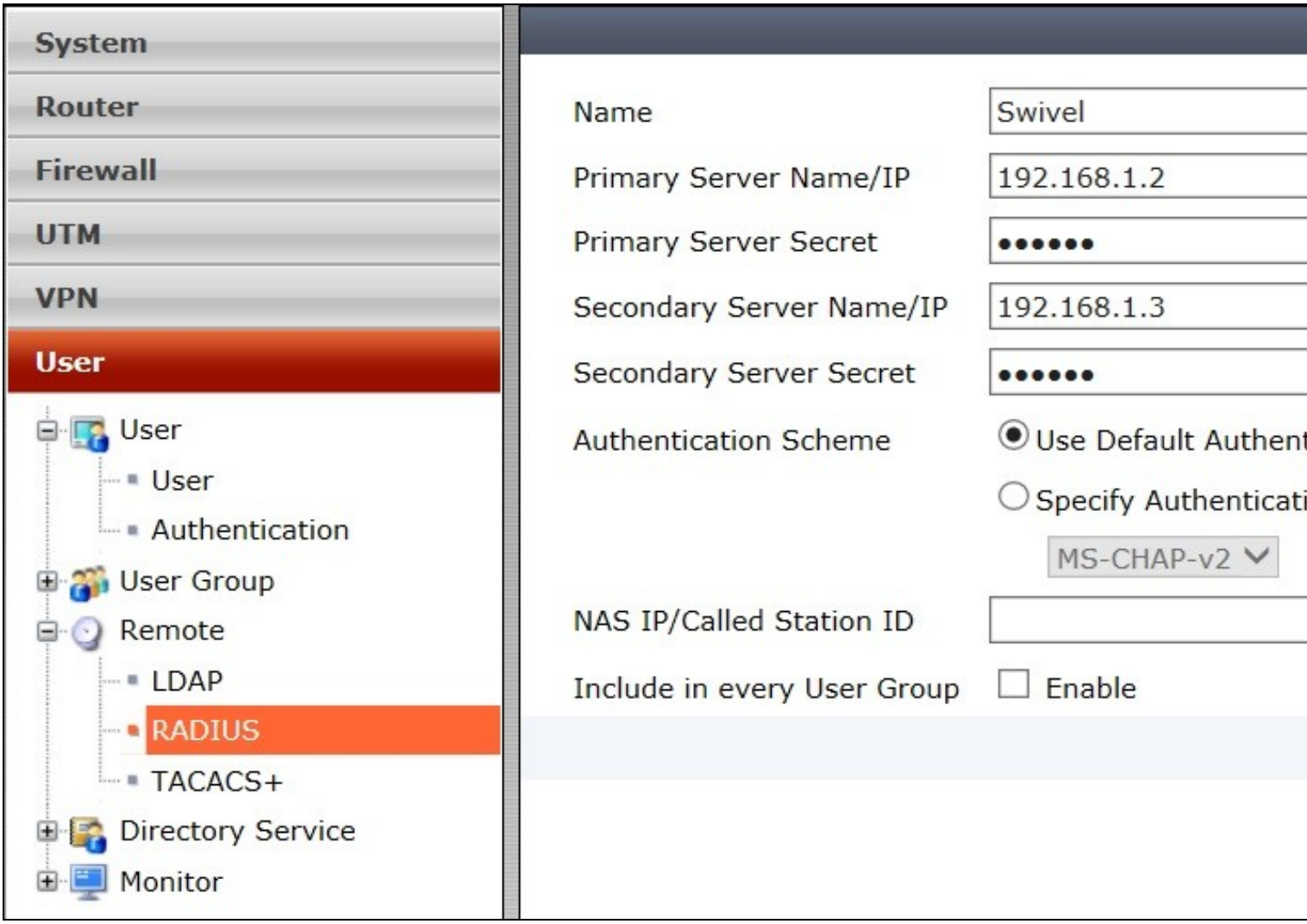
Primary Server Secret The shared secret entered on the Swivel RADIUS NAS

Standby Server Name/IP The IP or hostname of a standby Swivel server (Do not use a Swivel VIP in this field)

Standby Server Secret The shared secret entered on the standby Swivel RADIUS NAS

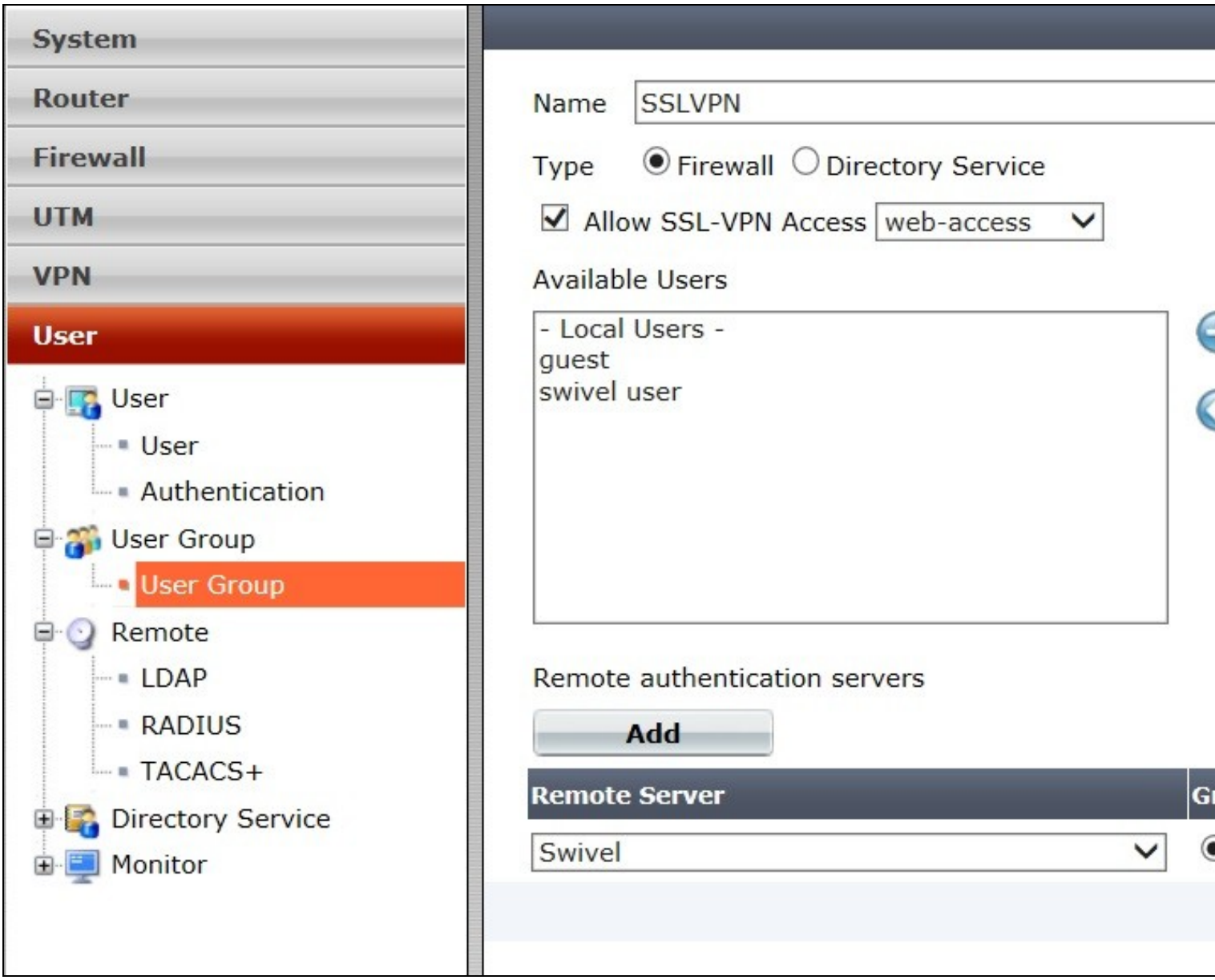
Authentication Scheme leave as Use Default Authentication Scheme unless Mobile App authentication or Check Password With Repository is used, in which case this should be set to use PAP.

By default the Fortigate and Swivel use port 1812 for RADIUS authentication.



On the Fortigate Administration console select User/User Group then select the required group, or create a new one, for Swivel Authentication then and under Remote authentication servers click on Add and select the Swivel Authentication server configured above. If not configured already the SSL-VPN access and any local user authentication can also be configured.

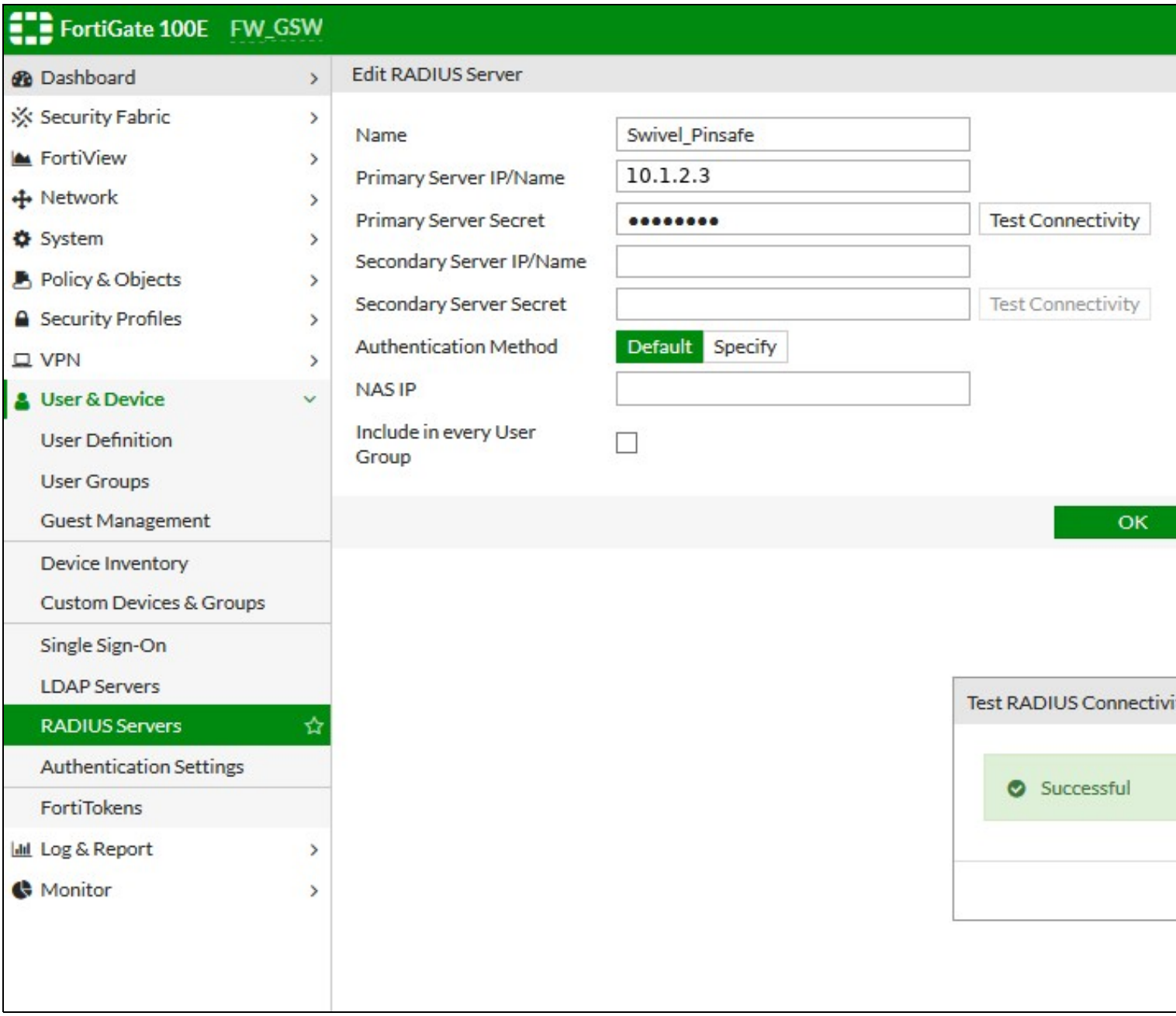
When multiple authentication servers are used, the Fortigate will use the username and password or One Time Code against each starting with local, until a successful authentication is made.



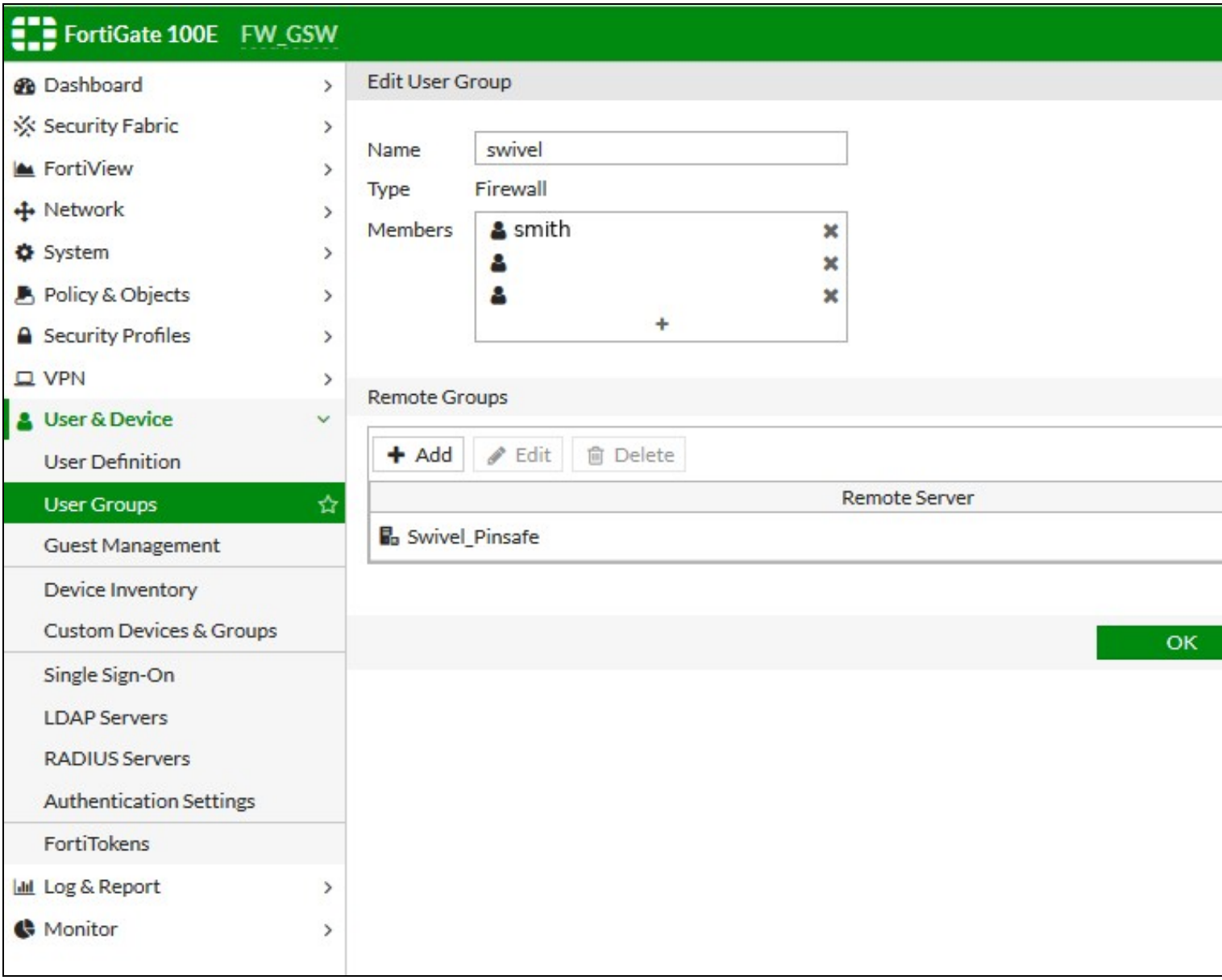
296.3 Fortinet Fortigate Version 6.x Integration guide

The images below show the steps to follow for a successful integration between swivel and fortinet products running version 6. Make sure to follow the first steps for integration with v4 products.

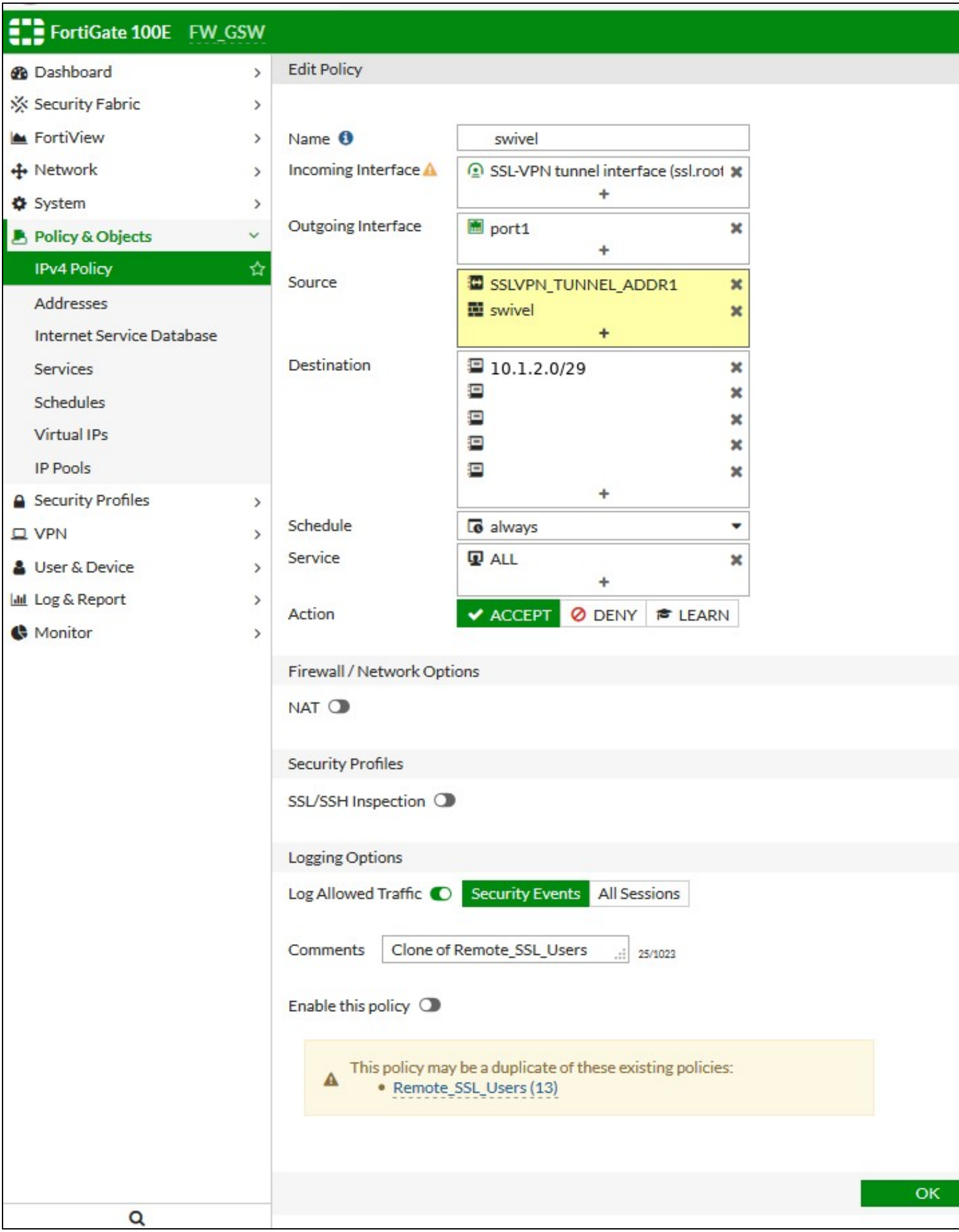
For further information regarding Fortinet FortiOS 6: https://docs.fortinet.com/uploaded/files/4328/fortios-v6.0.0-release-notes.pdf



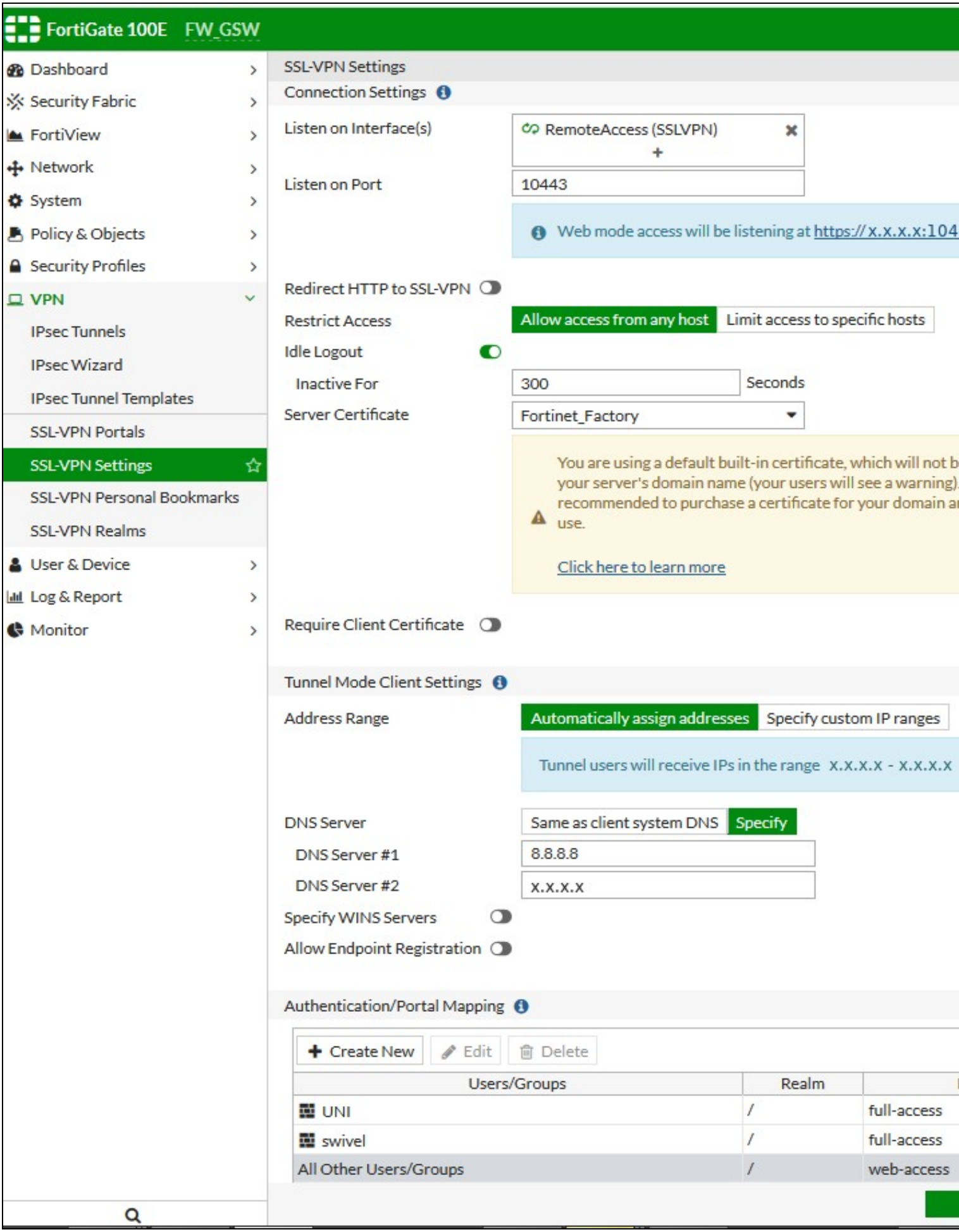
Select Radius Servers, create a Swivel Radius Server to bind to the the Appliance and test the connection. After create a user group for Swivel.



Edit Policy and fill all the entries. Destination might have more entries for different network and sub nets ranges.


FortiGate 100E FW_GSW
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Security Profiles
VPN
User & Device
Log & Report
Monitor
Edit Policy
Name
swivel
Incoming Interface
SSL-VPN tunnel interface (ssl.root
Outgoing Interface
port1
Source
SSLVPN_TUNNEL_ADDR1
swivel
Destination
10.1.2.0/29
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
Firewall / Network Options
NAT
Security Profiles
SSL/SSH Inspection
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Comments
Clone of Remote_SSL_Users
25/1023
Enable this policy
This policy may be a duplicate of these existing policies:
Remote_SSL_Users (13)
OK

Go to SSL VPN settings and check the settings. Default for listening will be port 10443. The DNS #2 can also have a resolution DNS specific for the customer's environment.


FortiGate 100E FW_GSW
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Personal Bookmarks
SSL-VPN Realms
User & Device
Log & Report
Monitor
SSL-VPN Settings
Connection Settings
Listen on Interface(s)
RemoteAccess (SSLVPN)
Listen on Port
10443
Web mode access will be listening at https://x.x.x.x:104
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not b
your server's domain name (your users will see a warning).
recommended to purchase a certificate for your domain a
use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range x.x.x.x - x.x.x.x
DNS Server
Same as client system DNS
Specify
DNS Server #1
8.8.8.8
DNS Server #2
x.x.x.x
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
UNI
/
full-access
swivel
/
full-access
All Other Users/Groups
/
web-access

296.4 Test the RADIUS authentication

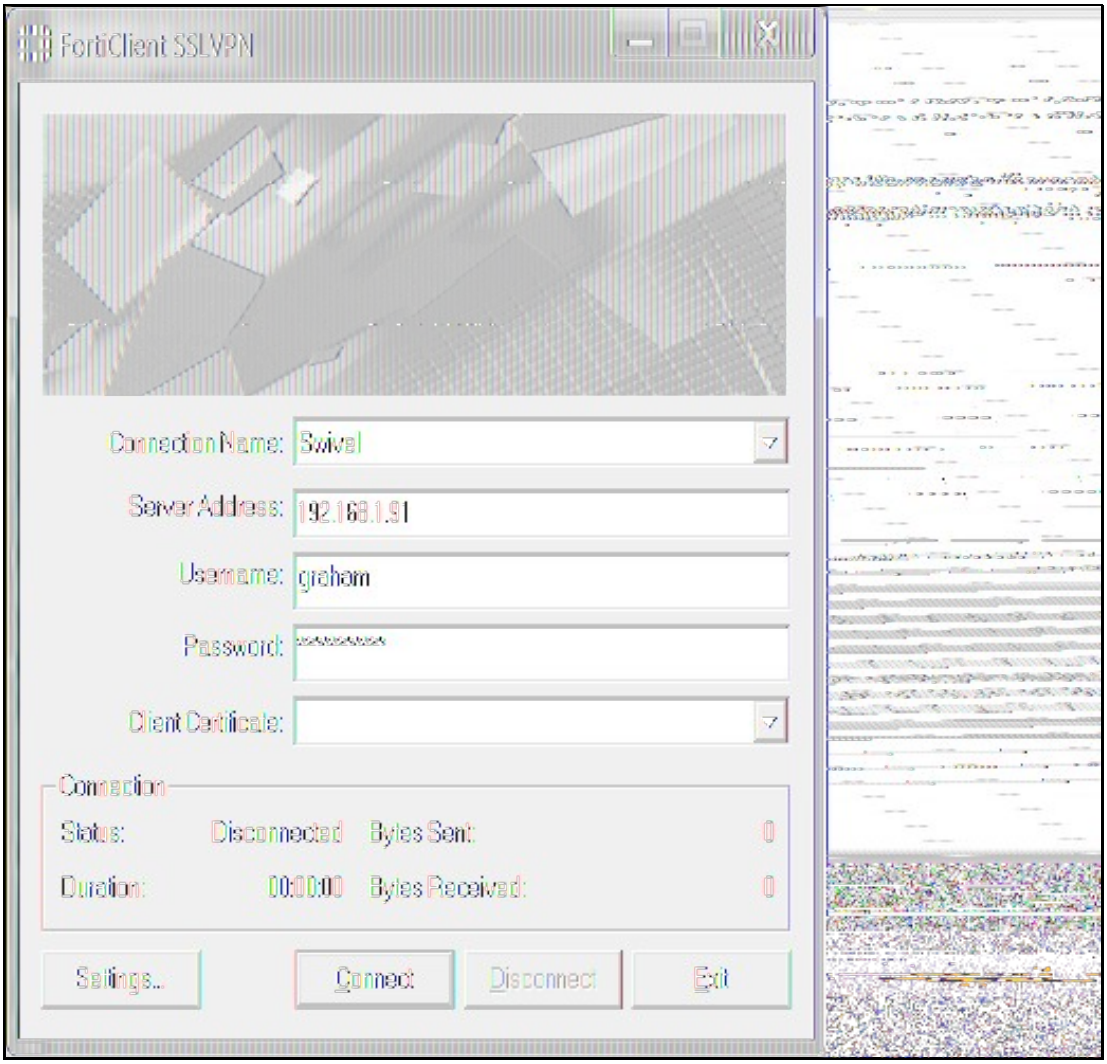
At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select 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.

297 Additional Configuration Options

Swivel can also check a password in addition to the One Time Code using Check Password with repository, see Password How to Guide

297.1 Forticlient

The above authentication integration will also work with the Fortinet Fortigate Fortclient for Client VPN access.



297.2 Login Page Customisation

The above configuration will allow authentication to be made by SMS, Mobile App, Hardware Token, and the Swivel Taskbar utility. To allow single channel authentication such as TURing or Pinpad, or images for other forms of authentication such the the security string index, then the login page can be modified. It may also be possible to modify other pages such as the Login Challenge Page.

On the Fortigate Administration console select System/Config/Replacement Messages, then click on SSL VPN to reveal the SSL VPN login message, then click on the edit icon. Paste in the required login page modifications.

Note Single channel images usually require a NAT to be used to the Swivel server.

Modify the script to use the Swivel server details:

```
//URL of radiusTuring page on the PINsafe server....
var sUrl="https://192.168.1.3:8443/proxy/SCImage?username=";
```

For a Swivel appliance the following should be used with the Swivel server IP/DNS name for the NAT entry:

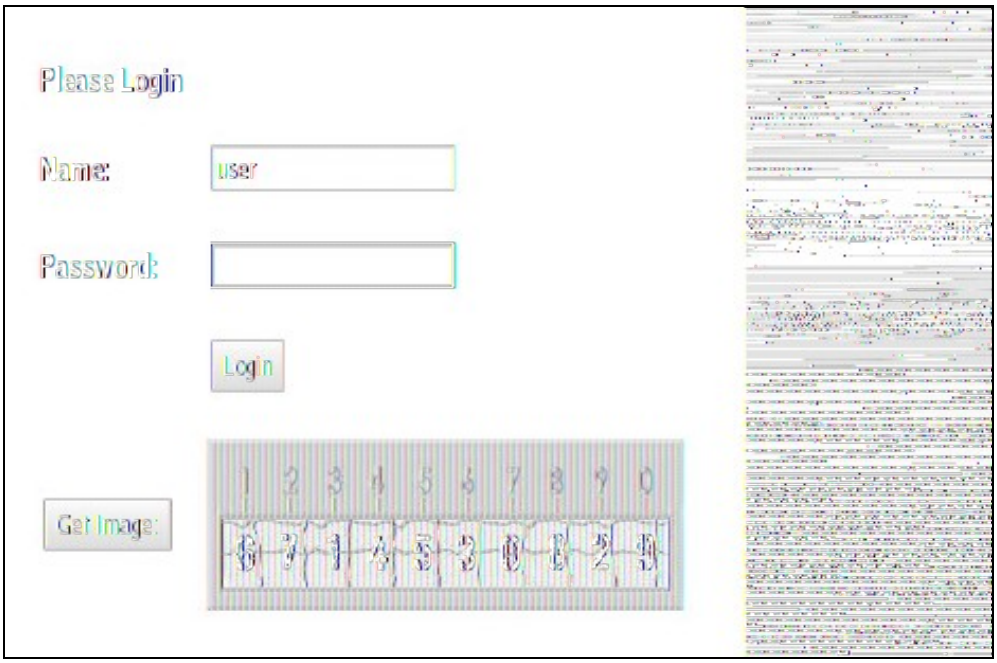
var sUrl="https://192.168.1.3:8443/proxy/SCImage?username=";

For a software only install see Software Only Installation

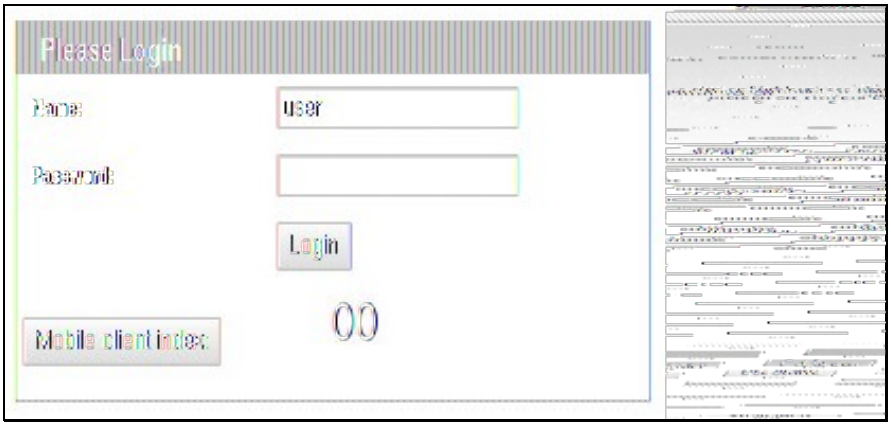
298 Testing

Browse to the VPN login page and test a Swivel authentication.

Example TURing login page



Example security string index login for Mobile or for SMS



299 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

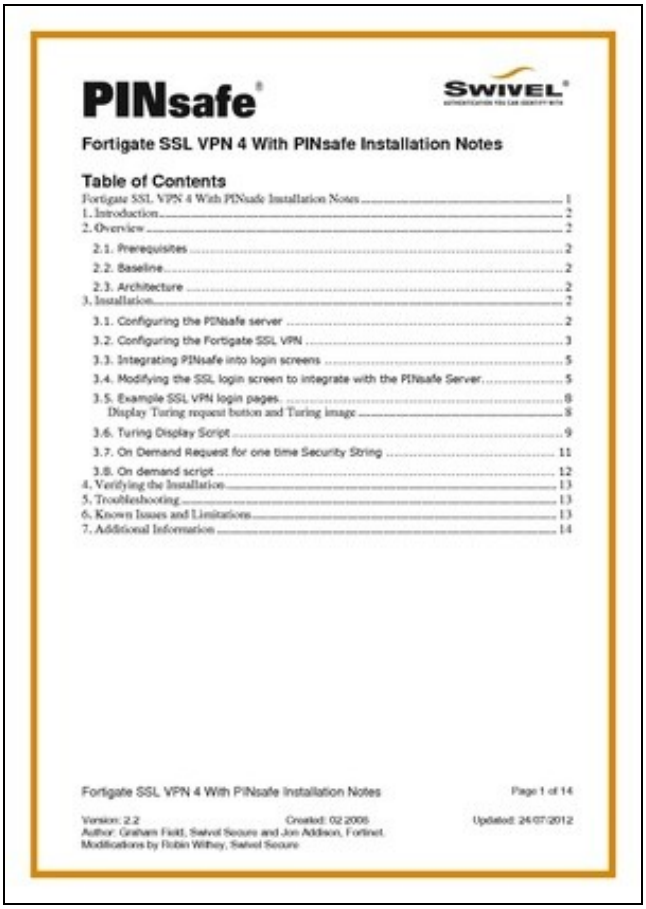
Login page modifications absent

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.

300 Known Issues and Limitations

None

301 Additional Information



PINsafe®

SWIVEL®

Fortigate SSL VPN 4 With PINsafe Installation Notes

Table of Contents

Fortigate SSL VPN 4 With PINsafe Installation Notes Page 1 of 14

Version: 2.2 Created: 02 2008 Updated: 24/07/2012

Author: Graham Field, Swivel Secure and Jon Addison, Fortinet.
Modifications by Robin Withey, Swivel Secure

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

302 HOB Remote Desktop VPN

303 Introduction

This document outlines the integration of PINsafe with the HOB Remote Desktop VPN.

304 Prerequisites

PINsafe 3.x

HOB RD VPN WebSecureProxy

If the graphical single Channel image is to be used, then the image must be accessible by the client from the internet, this is usually done by a NAT to the PINsafe server.

HOB RD VPN WebSecureProxy PINsafe Integration files

305 Baseline

PINsafe 3.7

HOB RD VPN WebSecureProxy 2.2 0108

306 Architecture

Users connect to the HOB RD VPN WebSecureProxy login page and enter their username and One Time Code. The authentication information is sent to the PINsafe server by RADIUS. RADIUS ChangePIN and Two Stage Challenge and Response authentication are also supported through RADIUS.

307 Swivel Configuration

307.1 Configuring the RADIUS server

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

307.2 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.

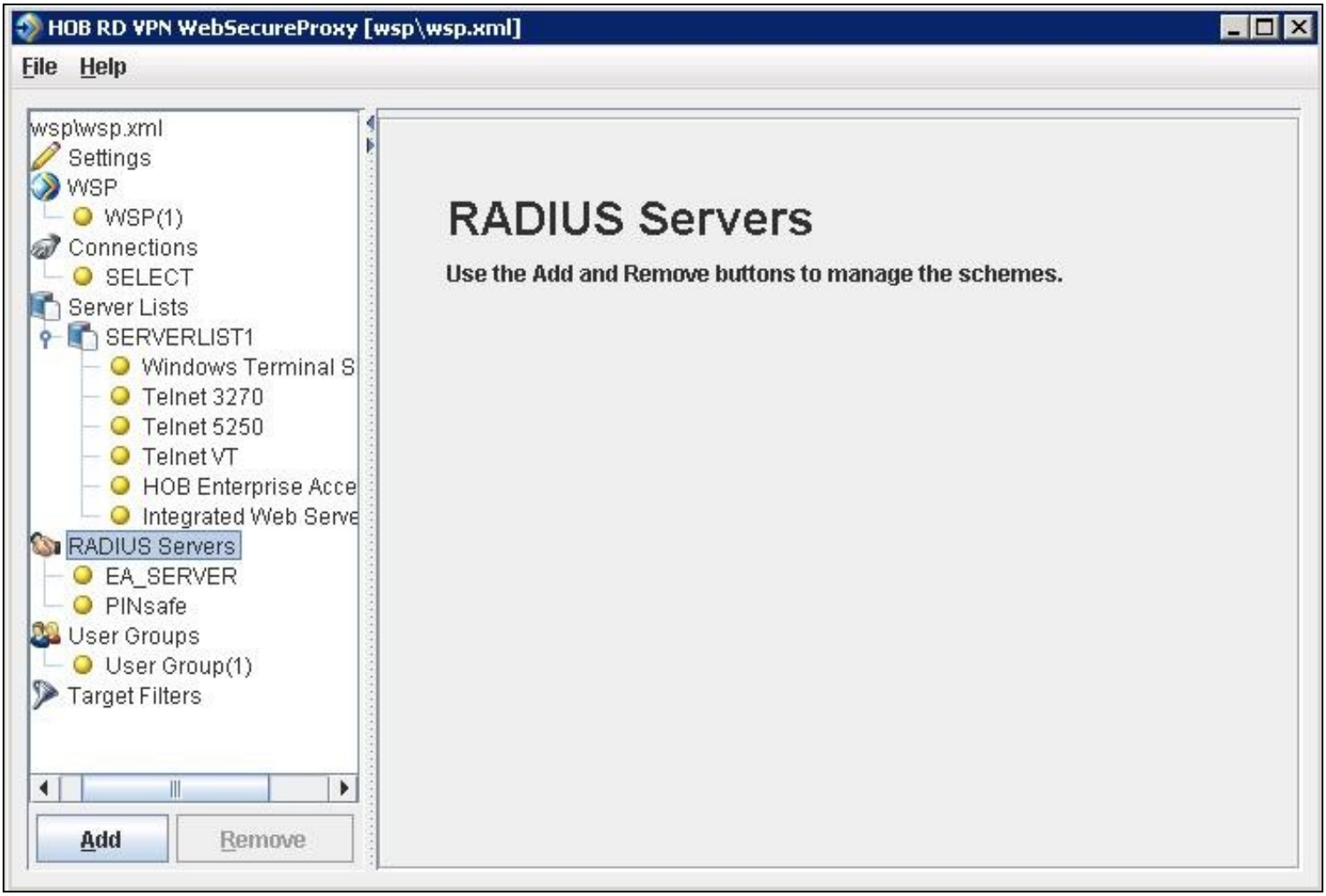
307.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

308 HOB RD VPN WebSecureProxy Integration

308.1 Create a RADIUS Server

On the HOB RD VPN WebSecureProxy Administration Configuration select RADIUS Servers then Add.



Enter the details for the PINsafe RADIUS server, the following information is required:

Name: A descriptive name such as PINsafe

Host IP Address: The hostname or IP address of the PINsafe server

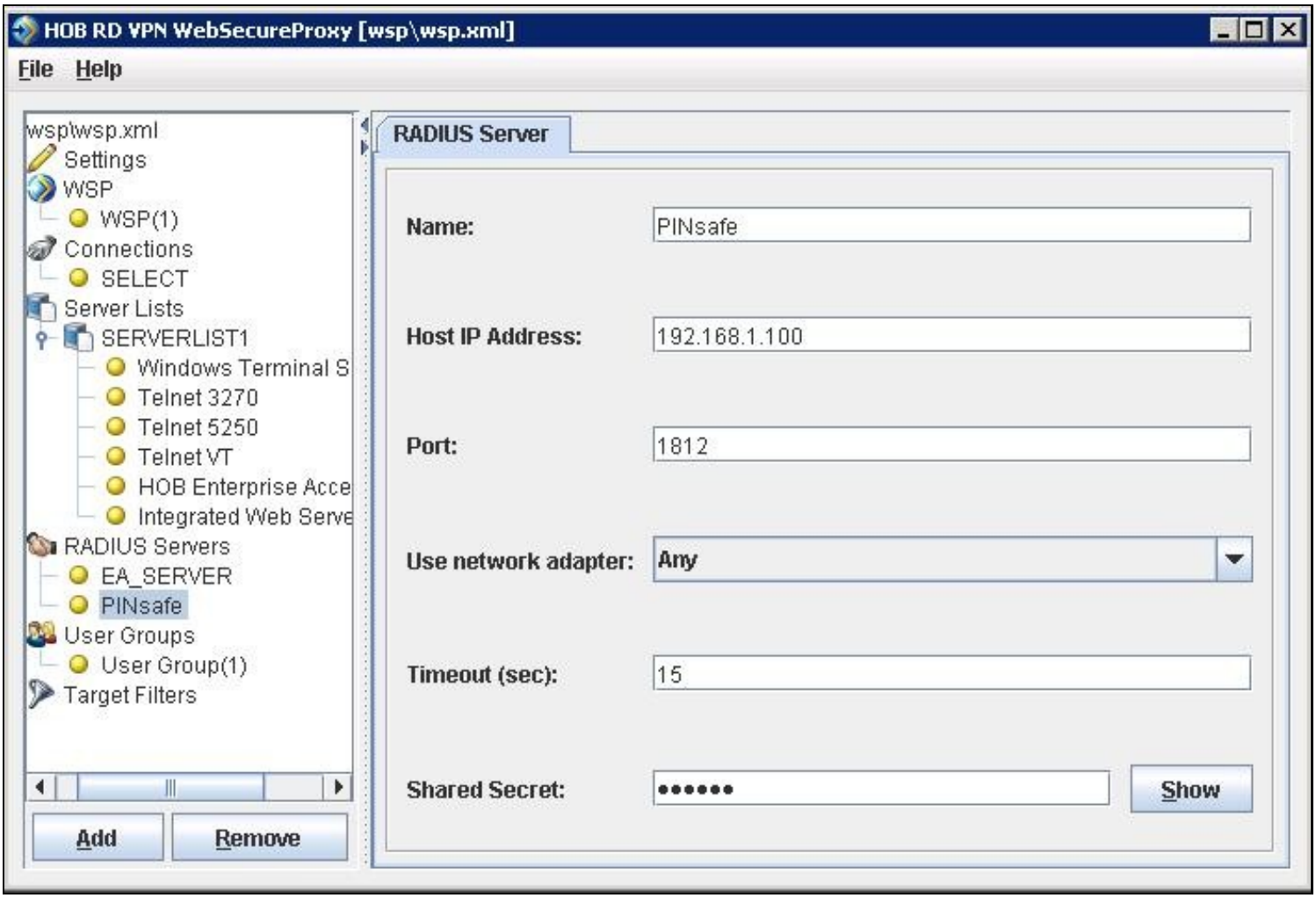
Port The port used for RADIUS authentication on the PINsafe server, usually 1812

Use network adapter: The network adapter from which authentication requests are sent from.

Timeout (sec): The length of time to wait for a RADIUS authentication attempt fails.

Shared Secret: A value that is also entered and must match on the PINsafe RADIUS NAS.

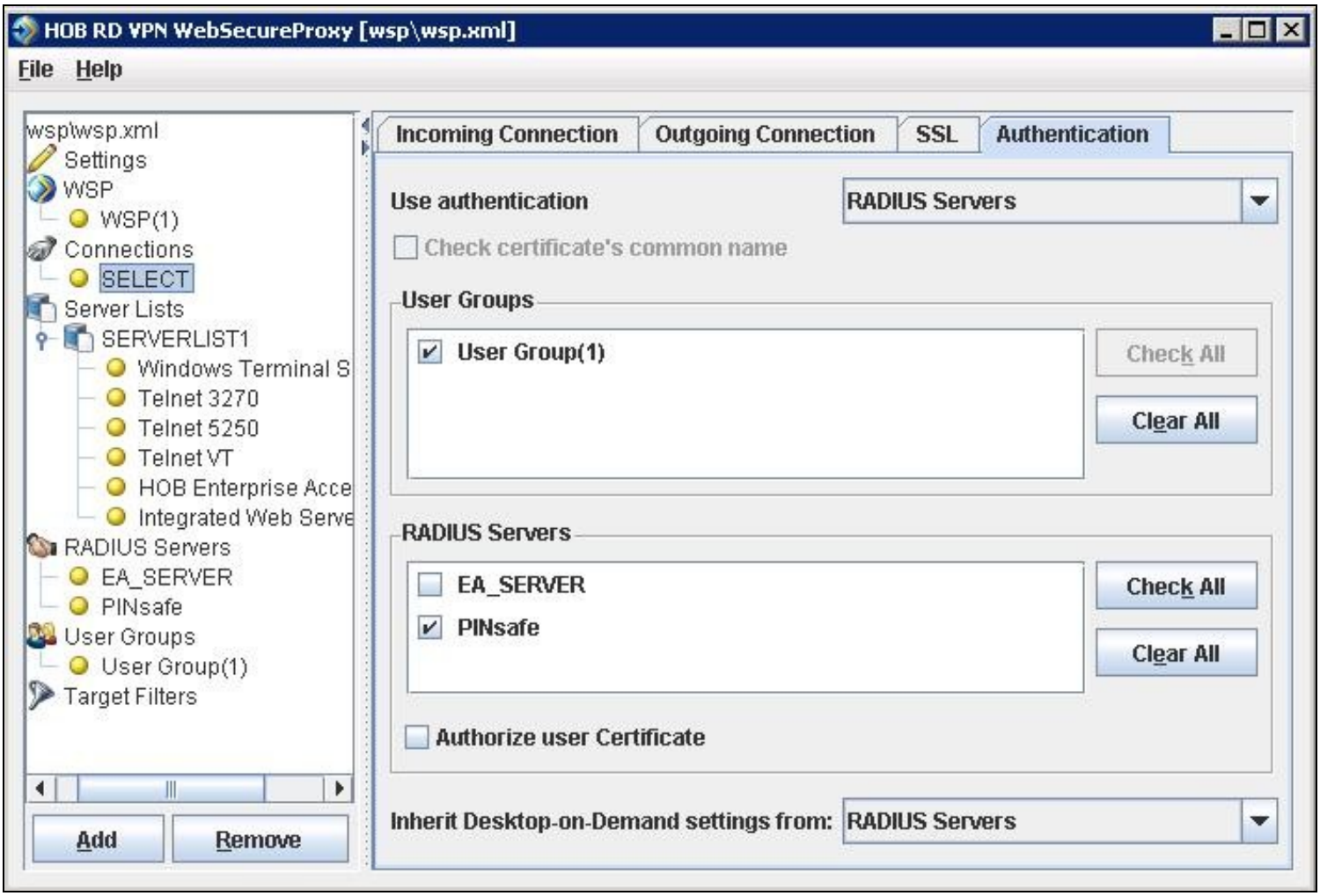
When complete click on File, then Save. For settings to take affect the HOB WebSecureProxy may need to be restarted.



308.2 Assign the PINsafe RADIUS server to a Connection

On the HOB RD VPN WebSecureProxy Administration Configuration select Connections, then the name of the required connection, then select the Authentication tab. Set the Use authentication to RADIUS and ensure that the PINsafe RADIUS server is selected.

When complete click on File, then Save. For settings to take affect the HOB WebSecureProxy may need to be restarted.



308.3 Additional Installation Options

308.3.1 Single Channel, Index and Message request

The HOB RD VPN WebSecureProxy will now be configured to allow authentication for Dual channel such as SMS and mobile phone applet. To configure additional options such as the graphical single channel image, and the security string index the login page must be modified. See also Multiple Security Strings How To Guide

Edit the pinsafe.js file and change the IP address of the PINsafe server to be that of the public NAT address of the PINsafe server.

```
pinsafeUrl = "http://192.168.1.100:8443/proxy/";
```

For a Swivel virtual or hardware appliance this will usually need to be: pinsafeUrl = "https://192.168.1.100:8443/proxy/";

For a software only install see Software Only Installation

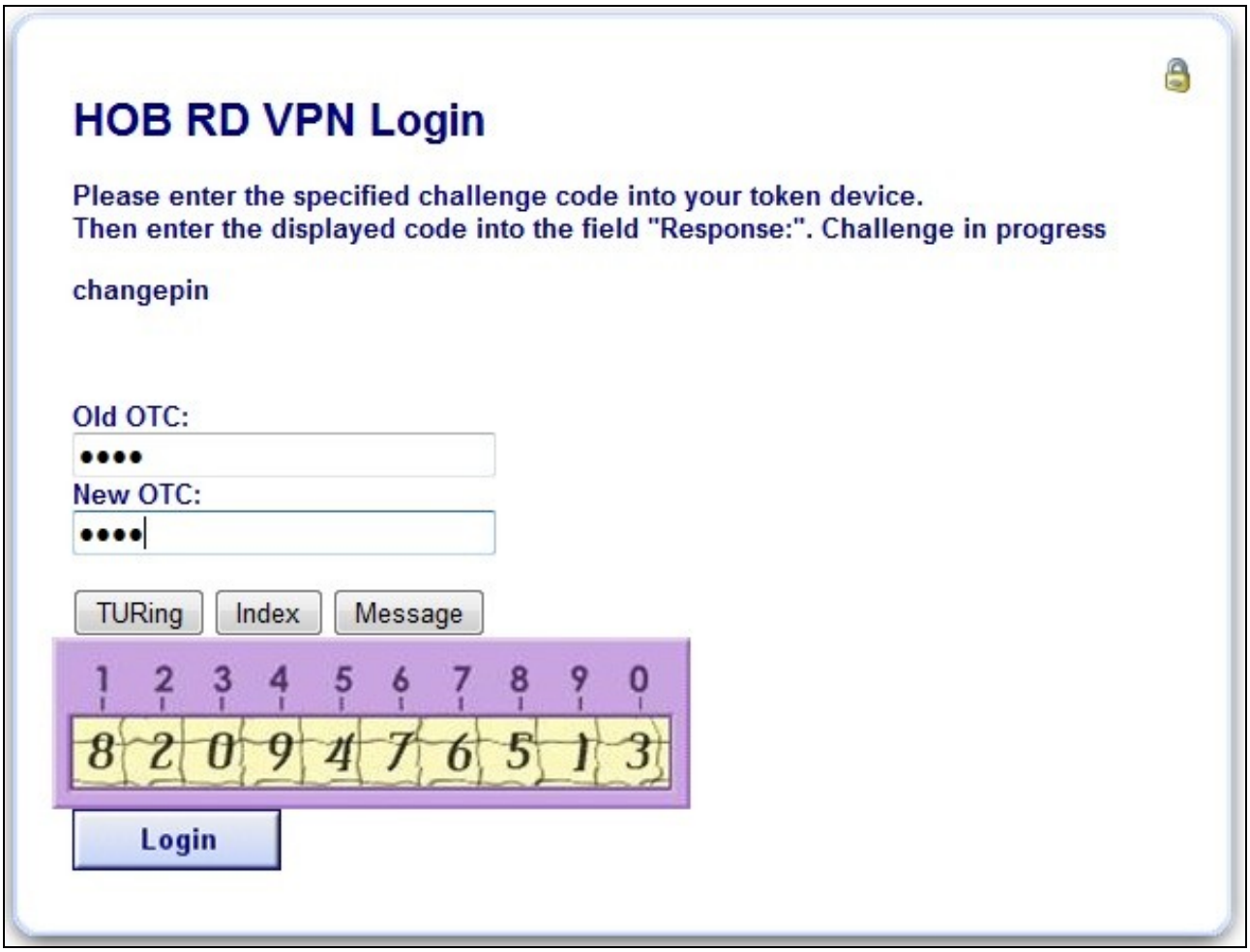
Backup the original files and then upload the modified files and login pages to the Hob RD VPN server, <path to install>\HOB\rdvpn\www\login

The default installation path is: c:\Program Files\HOB\rdvpn\www\login

For changes to the login page to take effect the HOB WebSecureProxy may need to be restarted.

308.3.2 Change PIN

To enable ChangePIN, on the PINsafe administration console select RADIUS/NAS then set ChangePIN Warining to Yes. Upload the modified login pages as detailed above. When a user is required to change their PIN they are automatically redirected to the ChangePIN page. Remember that the PIN number is never entered during the changePIN process, instead old and new one time codes are entered. A user may use SMS or tthe mobile phone to change their PIN. If a PINsafe password is being used, they must use <password><OTC>.



308.3.3 Challenge and Response and Two Stage Authentication

To enable Challenge and Response and Two Stage Authentication:

1. Upload the modified login pages as detailed above.

2. On the PINsafe administration console select RADIUS/NAS then set Two Stage Auth to Yes.

3. On the PINsafe administration console select RADIUS/Server and set Use Challenge/Response to Yes.

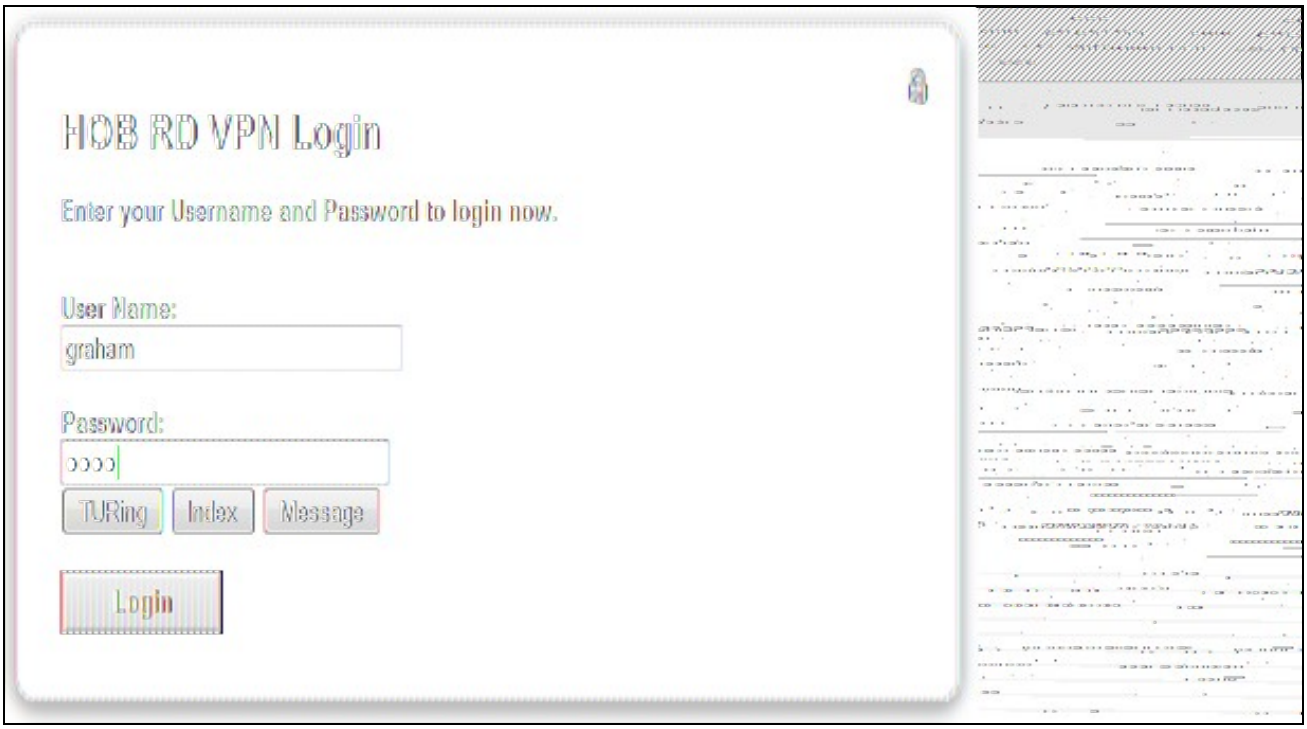
4. On the PINsafe administration console select Policy/Password and set Require Password to Yes, and Check Password with Repository to Yes. In PINsafe 3.8 this option is located under RADIUS/NAS.

When a user logs in they will be prompted to enter their password, and if correct will be redirected to another page where they can enter their one time code. The Challenge and Response option allows the user to be sent an SMS message on a correct password being entered.

309 Verifying the Installation

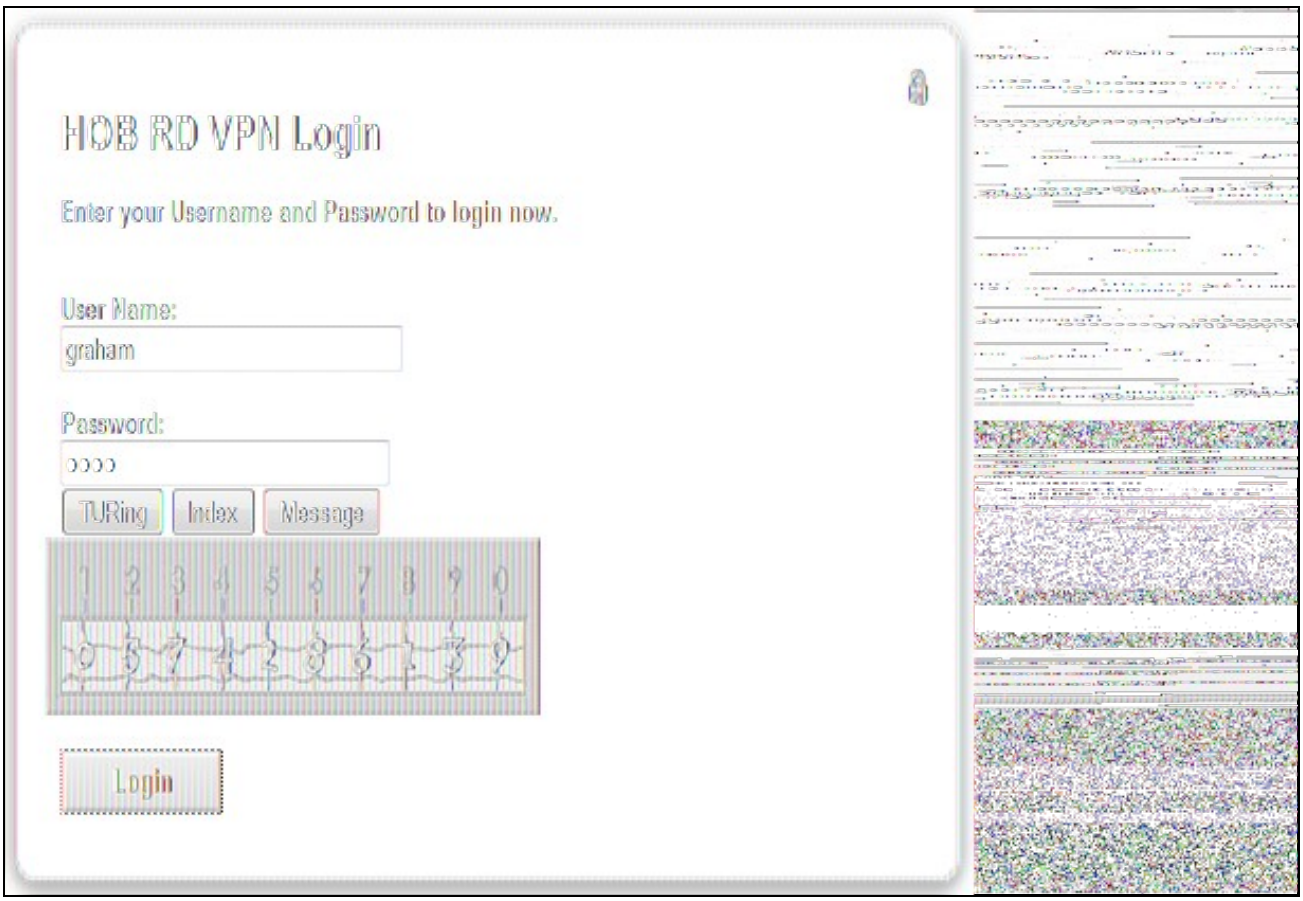
Attempt a login using the username and One Time Code.

For the dual channel login using SMS or mobile phone applet, enter the username, and then the One Time Code. Do not click on the TURing button. If the Message button has been added, then this can be used to request a new SMS message after the username has been entered.

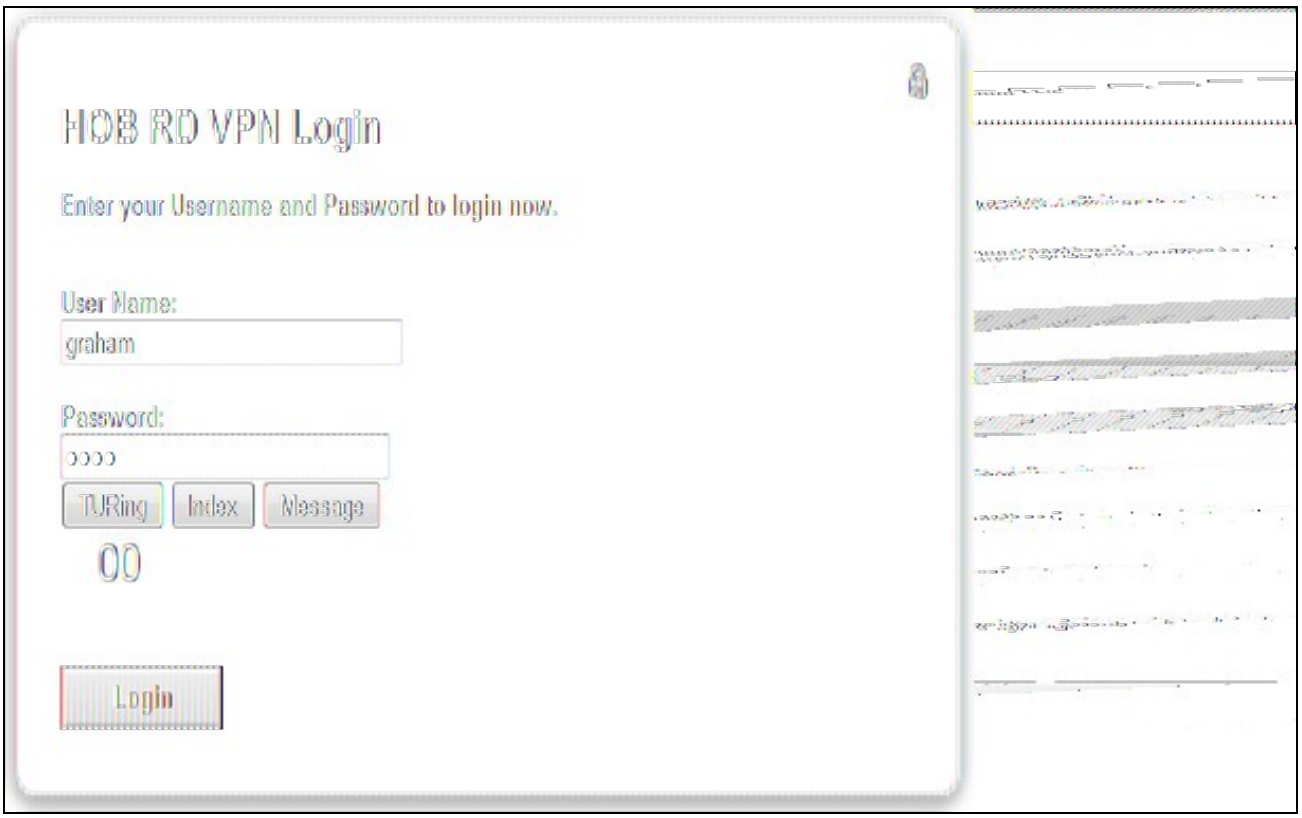


For the Single Channel authentication enter username and click on TURing.

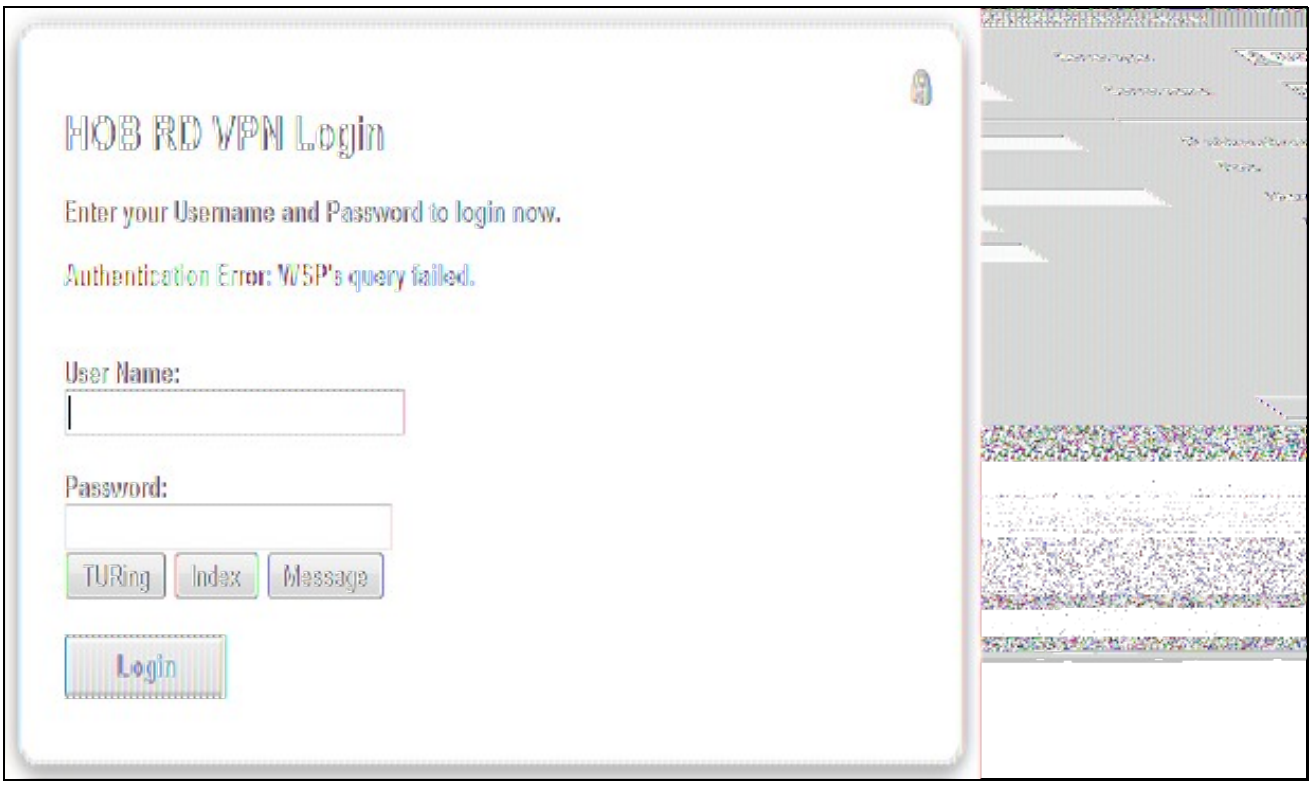
Enter the One Time Code then click on login.



If multiple Security Strings are being sent by SMS, then the string index can be requested to tell the user which security string should be used. Enter the username then click on Index. Enter the one time code associated with that number.



Verify that entering an incorrect one time code fails an authentication.



310 Uninstalling the PINsafe Integration

Copy the original files back on the HOB RD VPN server, and remove the PINsafe RADIUS server from the HOB RD VPN WebSecureProxy. Remove the PINsafe RADIUS server entry under RADIUS Servers.

311 Troubleshooting

Check the PINsafe logs for error messages. Specifically look for RADIUS requests to see if they are reaching the PINsafe server and Session Started messages to verify Single Channel images are being requested where used.

312 Known Issues and Limitations

313 Additional Information

314 Juniper ChangePIN

315 Introduction

This document outlines how to integrate the Swivel ChangePIN with Juniper. See also RADIUS ChangePIN and ChangePIN How to Guide

316 Prerequisites

Swivel Server

Juniper SSL VPN version 6 or 7 OS.

Modified Changepin page for version 6

Modified Changepin page for version 7

317 Baseline

Juniper SA 2000 JunOS 6 or 7.

Swivel 3.8

318 Architecture

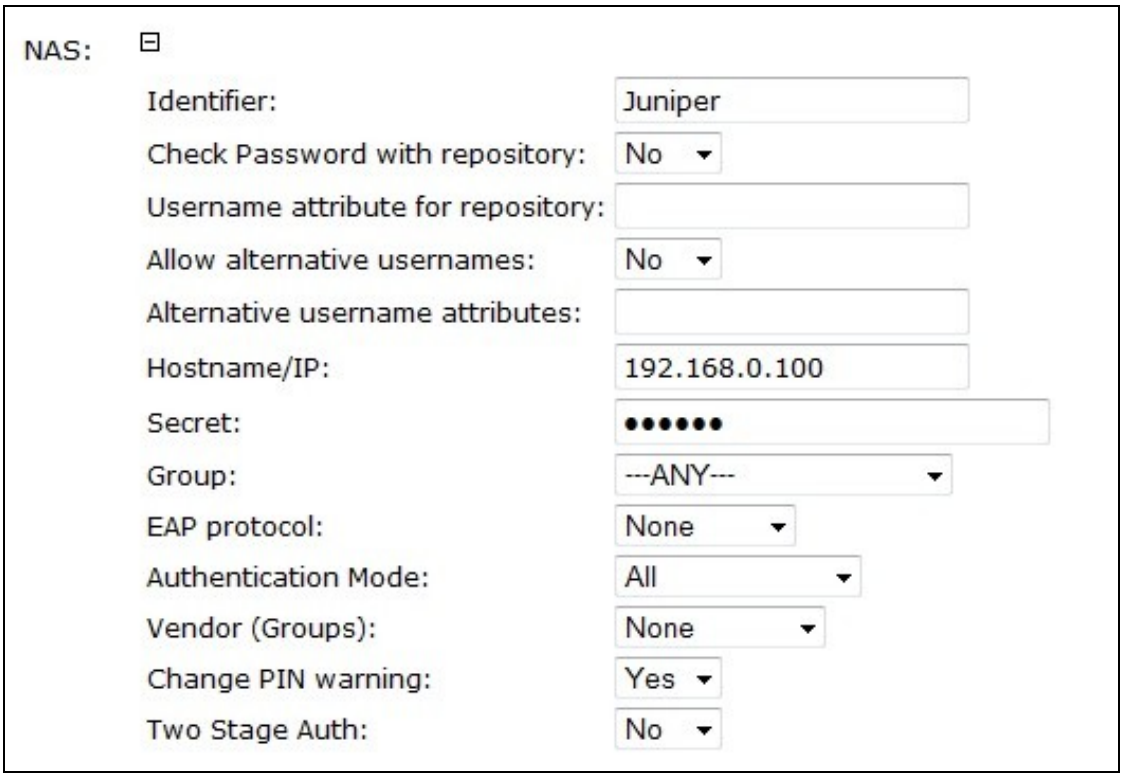
A user authenticates against the Juniper server, which passes the RADIUS authentication to the Swivel server. If the user is required to Change their PIN the Swivel server responds with a RADIUS Challenge, and the user is redirected to a change PIN page.

319 Installation

Configure the Swivel and Juniper so that they are fully working together, see Juniper SA 6.x Integration or Juniper SA 7.x Integration or Juniper SA 8.x Integration

319.1 Swivel Integration Configuration

On the Swivel Administration Console select RADIUS then NAS and edit the required Juniper NAS entry Change PIN Warning to Yes, then apply the settings.



319.2 Juniper ChangePIN Integration

Download the login page and add the modified ChangePIN page given above under prerequisites, rename and edit as appropriate, add to the zip file and upload to the Juniper server.

319.2.1 Juniper ChangePIN page options

Edit the following options:

```
var OTC_OPTION = "image"; // button, image, disable
```

image When the user tabs down from the username field, the TURing will automatically show, used for Single Channel access

button The login page will present a TURing button. Click the button to display the TURing, used for Single or Dual Channel access

disable The TURing image will not be shown, used for Dual Channel access.

TURingImage: Is the URL used to generate a TURing image. This should point to the internal IP address of the appliance

var TURingImage = "https://turing.swivelsecure.com/proxy/SCImage?username=";

319.2.2 Juniper RADIUS Custom rules

On the Juniper Administration console select the Swivel RADIUS server and create a Custom RADIUS rule with the following settings:

Name: ChangePIN

Response Packet Type: Access Challenge

Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand Matches the expression

Value: changepin

Action: use the appropriately modified page; *Show Next Token page* or *show New Pin Page*

	Name	Response Packet Type	Attribute criteria
	ChangePIN	**Access Challenge**	(Reply-Message matches the expression "change

319.3 Additional Installation Options

319.3.1 Combining Swivel and RSA RADIUS changePIN

Where Swivel is acting as a proxy RADIUS server for RSA authentication, Swivel can proxy the RADIUS request.

Configure the Swivel RADIUS proxy so that it will authenticate RSA users, see RADIUS Proxy How to guide.

On the Juniper edit the Swivel RADIUS authentication setting to add an additional custom rule with the following settings:

Name: RSAChangePIN

Response Packet Type: Access Challenge

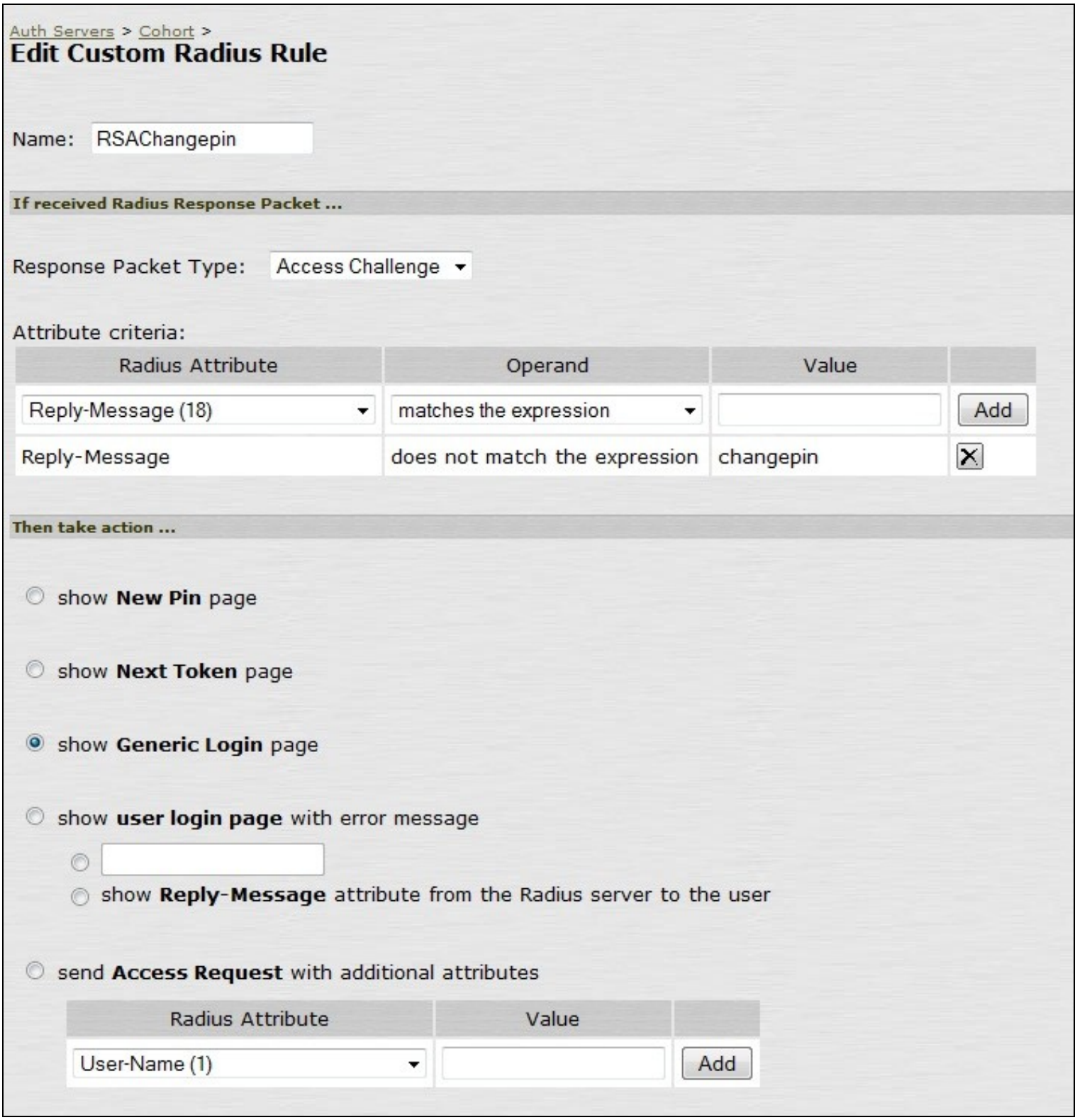
Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand does not match the expression

Value: changepin

Action: show Generic Login page

Apply the settings



Note: The Juniper displays the Generic login page as *show **Defender** page*

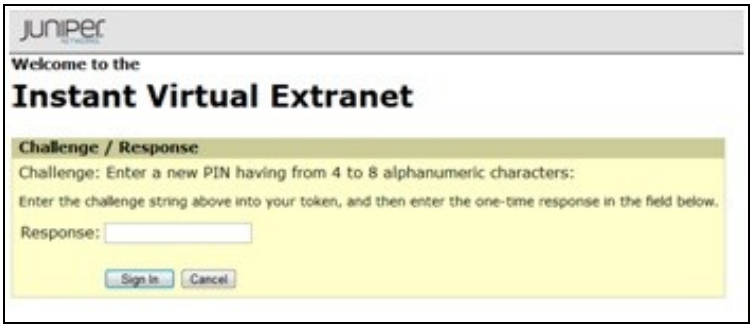
	Name	Response Packet Type	Attribute criteria
☐	ChangePIN	**Access Challenge**	(Reply-Message matches the expression "change
☐	RSAChangepin	**Access Challenge**	(Reply-Message does not match the expression "

320 Verifying the Installation

Login as a Swivel user.

Set the user to be required to change their PIN, the user should be redirected to the ChangePIN page. The user will be required to enter their old OTC, and a new OTC based on what they want their PIN to be. This OTC could be from the TURing, SMS message or mobile app. Remember to never enter the Swivel PIN.

Where RSA authentication is being used, require the user to change their PIN, and they should be redirected to a RSA Change PIN page. The the first time a user accesses the system with a new token the user will be required to enter a new PIN. If the user wanted a PIN of 1234 the would enter 1234 in the box.



The RSA server then send a challenge asking for the PIN to be re-entered to confirm the user has not miss-typed it. The user would again enter 1234.

Once the user has successfully changed their PIN the RSA server asks them to login again with their new PIN plus token code. The user would enter 1234XXXXXX where XXXXXX is the code displayed on the token.

If the RSA server sees the token go out of sync it will ask the user to enter their next token code. The user would now enter XXXXXX where XXXXXX is the next code displayed on the token after the code the user used to authenticate. They do not type their PIN at this stage.

321 Uninstalling the Swivel Integration

Remove the modified login pages and RADIUS customisation.

322 Troubleshooting

Check the Swivel logs for authentication, proxy and ChangePIN requests.

323 Known Issues and Limitations

Where Swivel and RSA change PIN is being used and the user is a Swivel and a RSA user, and dual channel authentication is being used, then the Change PIN will fail for RSA users. for single channel users not using dual channel authentication, the proxy server can be used to detect the presence of a single channel session being started.

324 Additional Information

325 Juniper OneTouch

326 Overview

This document is intended to supplement the the OneTouch Mobile guide and the OneTouch Voice guide for using the Swivel Juniper OneTouch Demo application.

327 Prerequisites

Swivel 3.10.4

Juniper 7.x or 8.x

Nexmo Account (or other Telephony provider) for OneTouch Voice telephone-based solution

Latest version of the Swivel Appliance Proxy available from Downloads

Swivel OneTouch Application demo available from Downloads

Juniper Custom login pages OneStage.zip or TwoStages.zip

328 Baseline

(The version tested with)

Swivel 3.10.4

Juniper 7.x

329 Architecture

See OneTouch Voice and OneTouch Mobile

330 Installation

330.1 One Touch Demo Application Installation

Install the Swivel OneTouch Demo Application

330.2 Swivel Integration Configuration

Configure the Swivel server and users as detailed in this guide OneTouch Voice or OneTouch Mobile.

330.3 Juniper One Touch Integration

330.4 Modifying the Custom login Pages

Modify the Juniper login pages either for OneStage or TwoStage authentication.

330.4.1 For Single Stage authentication

Open the OneTouchOneStage.zip file

Modify the LoginPage.thtml file

edit the 2 URLs to access to your OneTouch demo app:

e.g.: http://localhost:8081/onetouchdemo/onetouch?returnurl=

Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

330.4.2 For Two Stage Authentication

Open the OneTouch2Stages.zip file

Modify the Defender.thtml file

edit the URLs to access to your OneTouch demo app:

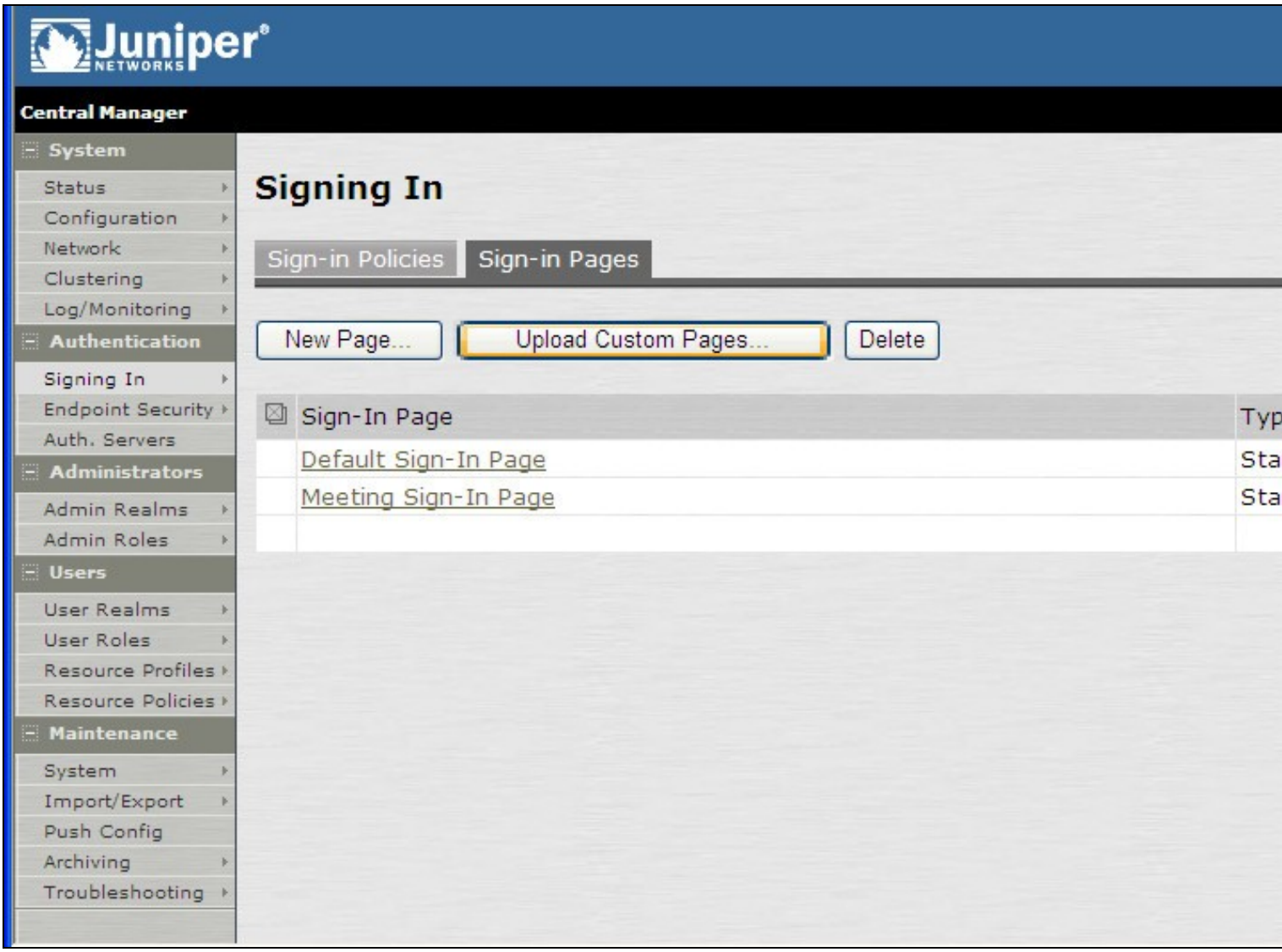
e.g.: http://localhost:8081/onetouchdemo/onetouch?returnurl=

Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

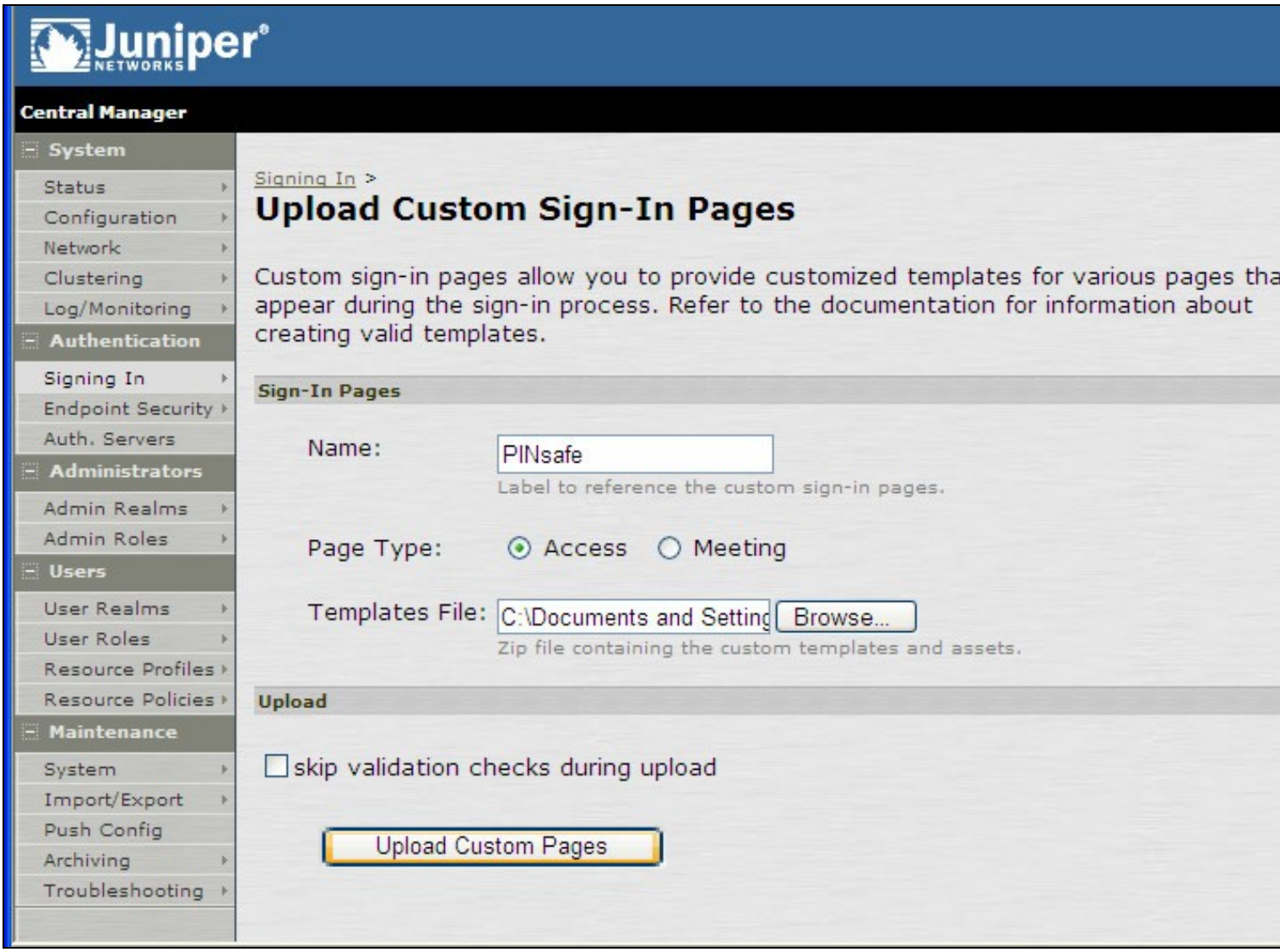
330.5 Uploading the Custom Sign in pages

As with the Swivel Juniper integration, the custom pages need to be uploaded and assigned to a signing-in policy and realm.

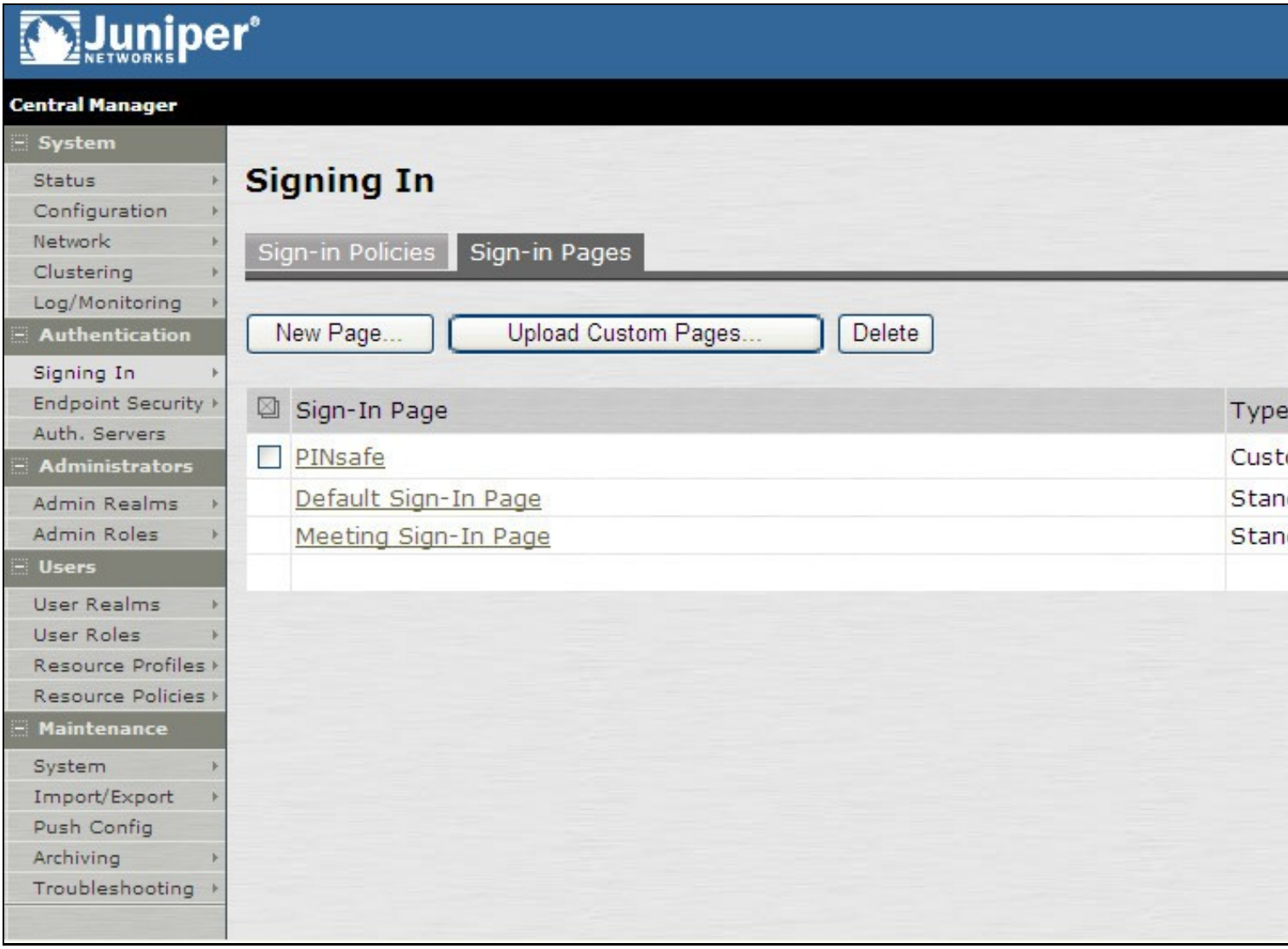
Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.



Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.

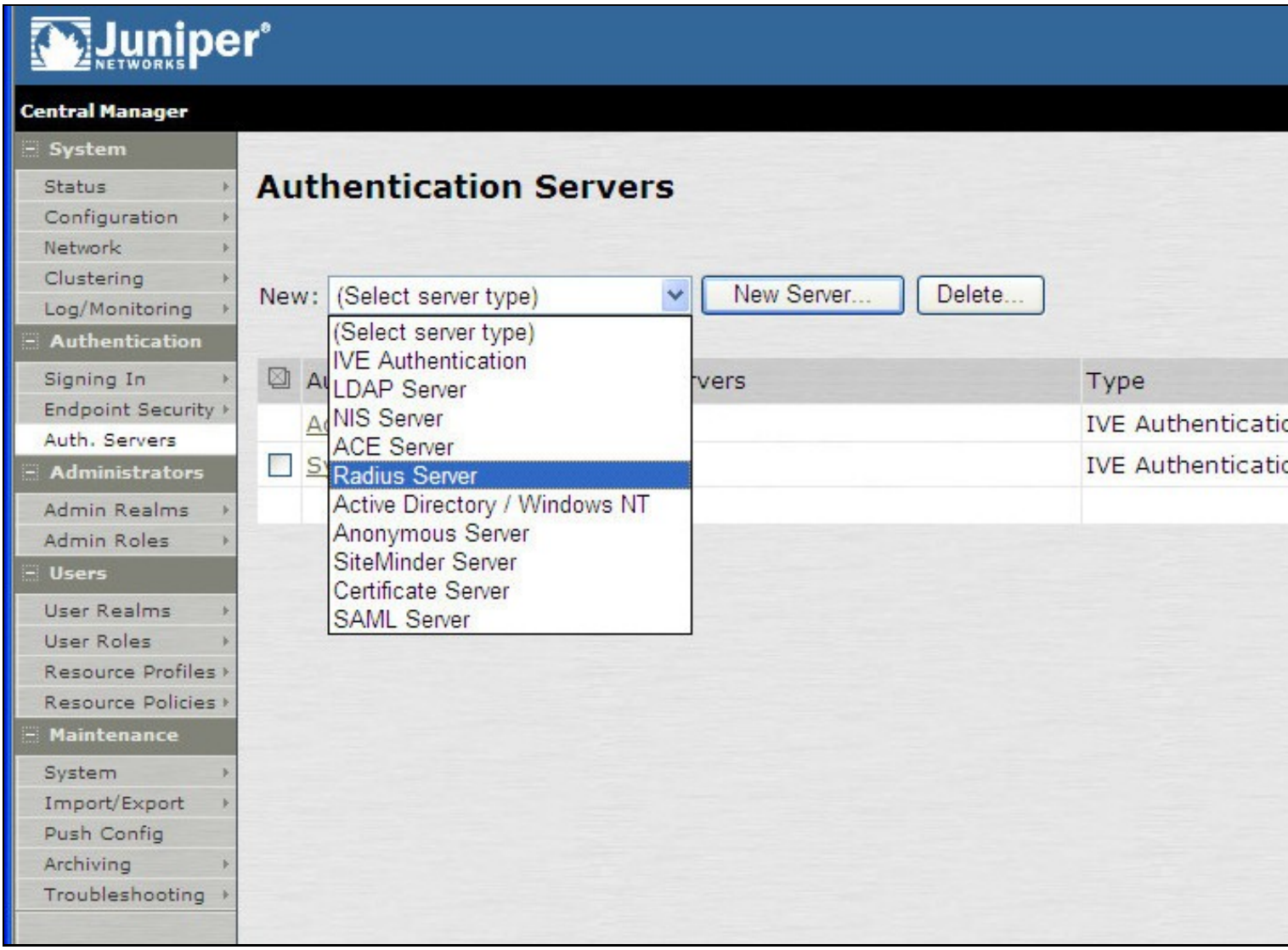


The new signing in page should be listed.



330.6 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.



The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

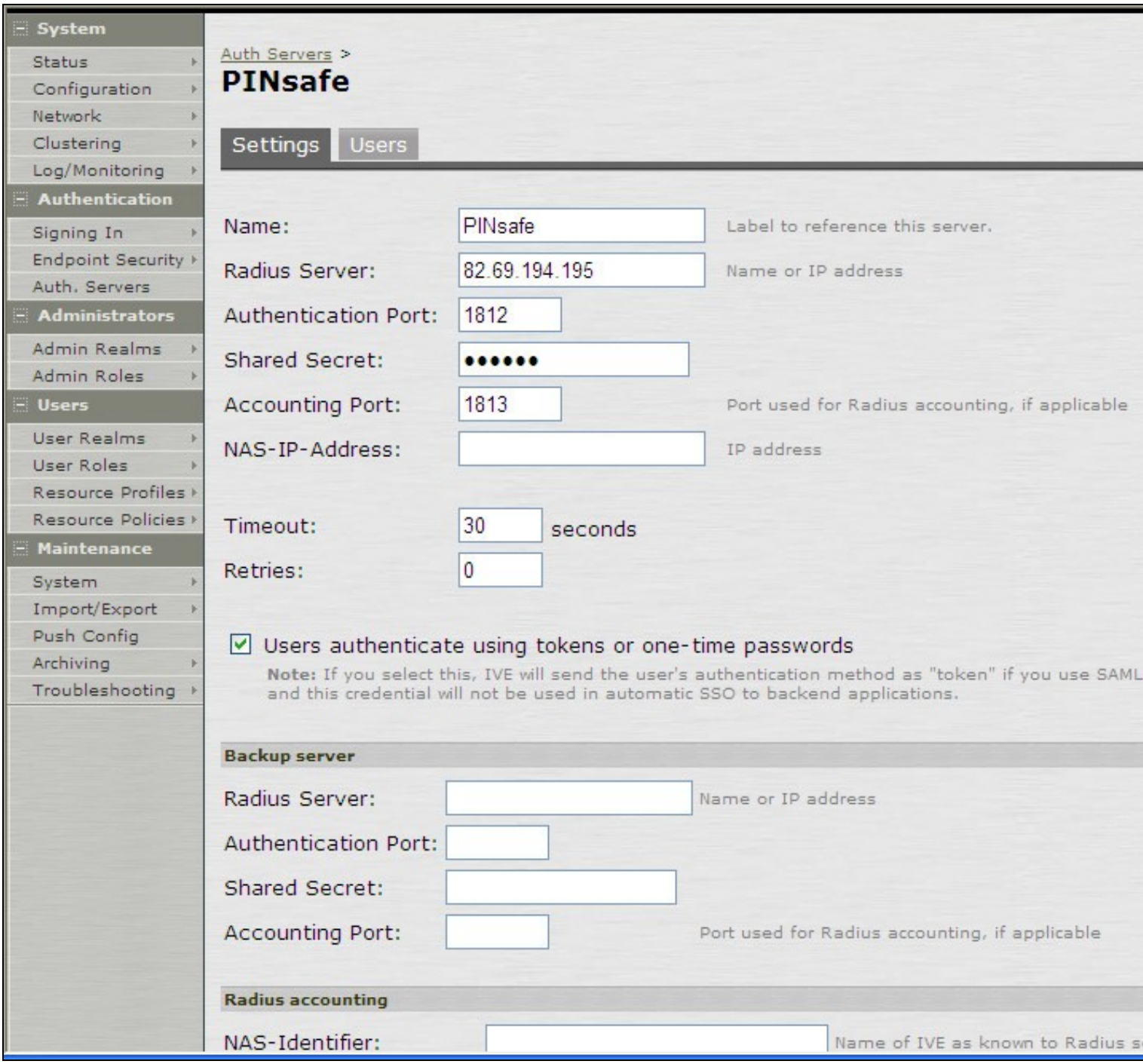
Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.



For Two Stage Authentication Go to the auth, select the server used for one touch and add a new challenge rule. The value has to be the same as configured on Defender.thtml and radius_challenges.txt on the Swivel core.

Example Rule:

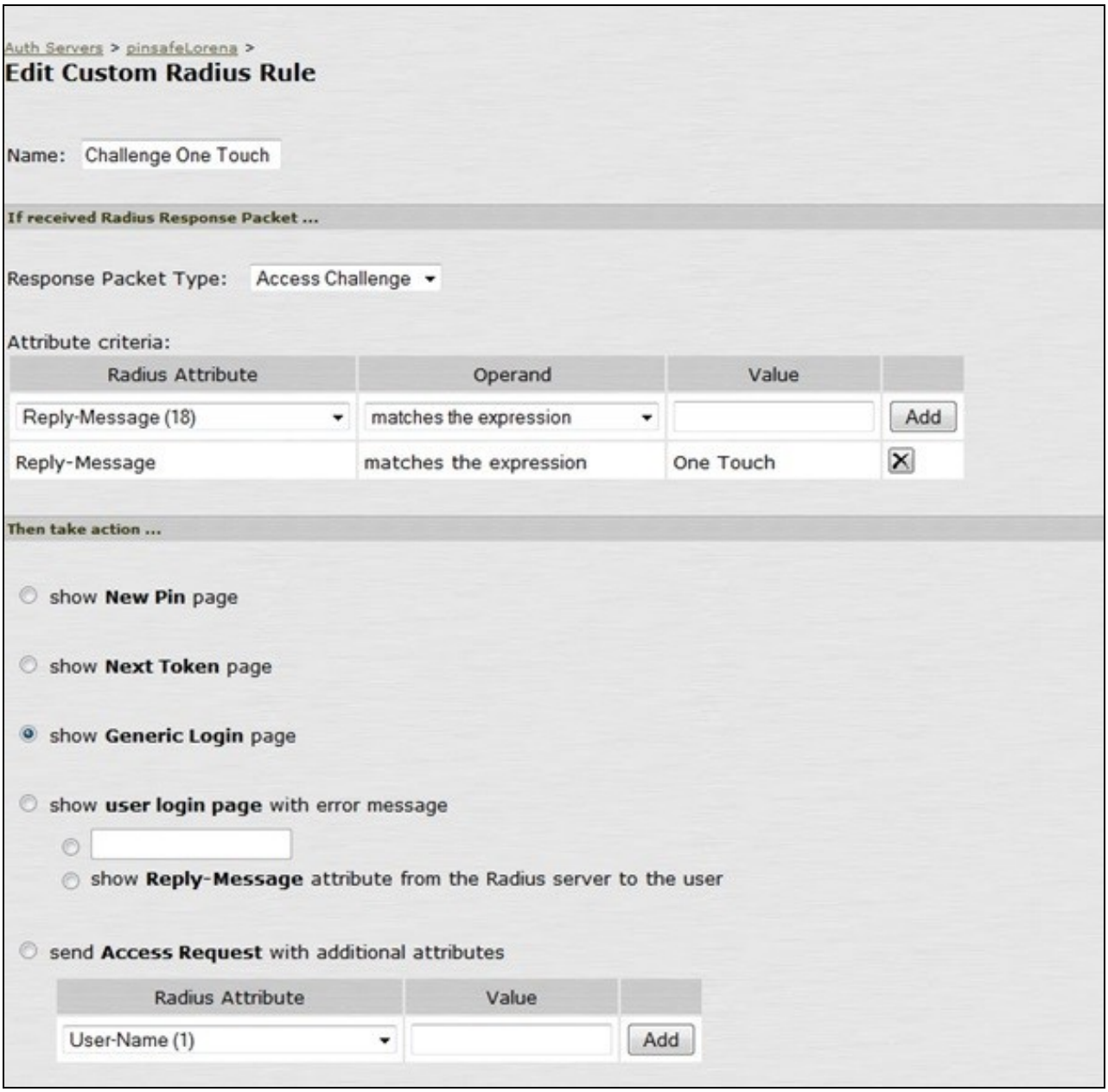
Name: Challenge One Touch

Response Packet Type: Access Challenge

RADIUS Attribute: Reply-Message

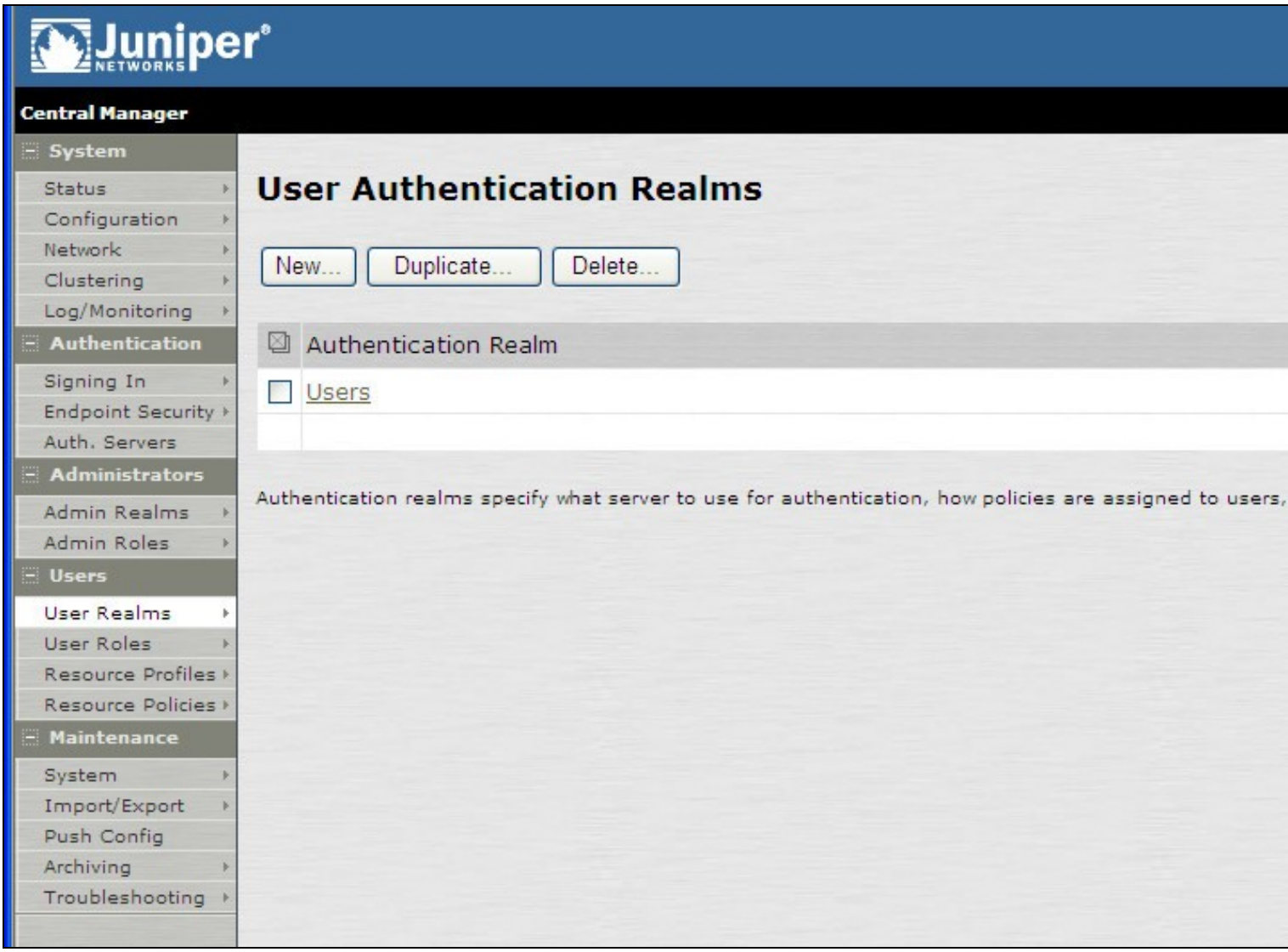
Operand: matches the expression

Value: One Touch



330.6.1 Authentication Realm Configuration

Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.



330.7 Additional Installation Options

331 Verifying the Installation

332 Uninstalling the Swivel Integration

333 Troubleshooting

334 Known Issues and Limitations

335 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.

336 Juniper SA 5.x Integration

336.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 5.x Basic Integration Guide

Juniper SA 5.x files for modified login page

Juniper SA 5.x Enhanced Integration Guide

337 Juniper SA 6.x Integration

337.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 6.x Integration Guide

337.2 Troubleshooting

INFO RADIUS: <69> Access-Request(1) LEN=147 192.168.1.1:13145 Access-Request by ADMIN\graham Failed: AccessRejectException: AGENT_ERROR_NO_USER_DATA

INFO 192.168.1.1 Juniper:Login failed for user: ADMIN\graham, error: No data for the user was found.

Authentication has failed as the User Ream has been configured with <USER> instead of <USERNAME>

338 Juniper SA 7.x Integration

339 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 8.x integration guide see Juniper SA 8.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

340 Prerequisites

Juniper 7.x

Swivel 3.x

Modified login pages can be downloaded from here: PINsafe modified pages also requires sample pages from Juniper appliance.

It is possible to access Juniper SSL VPN from mobile devices such as iPhone, Blackberry, Windows Mobile and Andriod devices.

To support this, additional pages needs to be modified to support Swivel.

Mobile login pages can be downloaded from here: Swivel Mobile login pages, and should be included if the Single channel images are required on mobile devices.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. A valid certificate is required on the Swivel server.

341 Baseline

Juniper 7.2

Swivel 3.7

342 Architecture

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

343 Installation

343.1 Swivel Configuration

343.1.1 Configuring the RADIUS server

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

343.1.2 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.

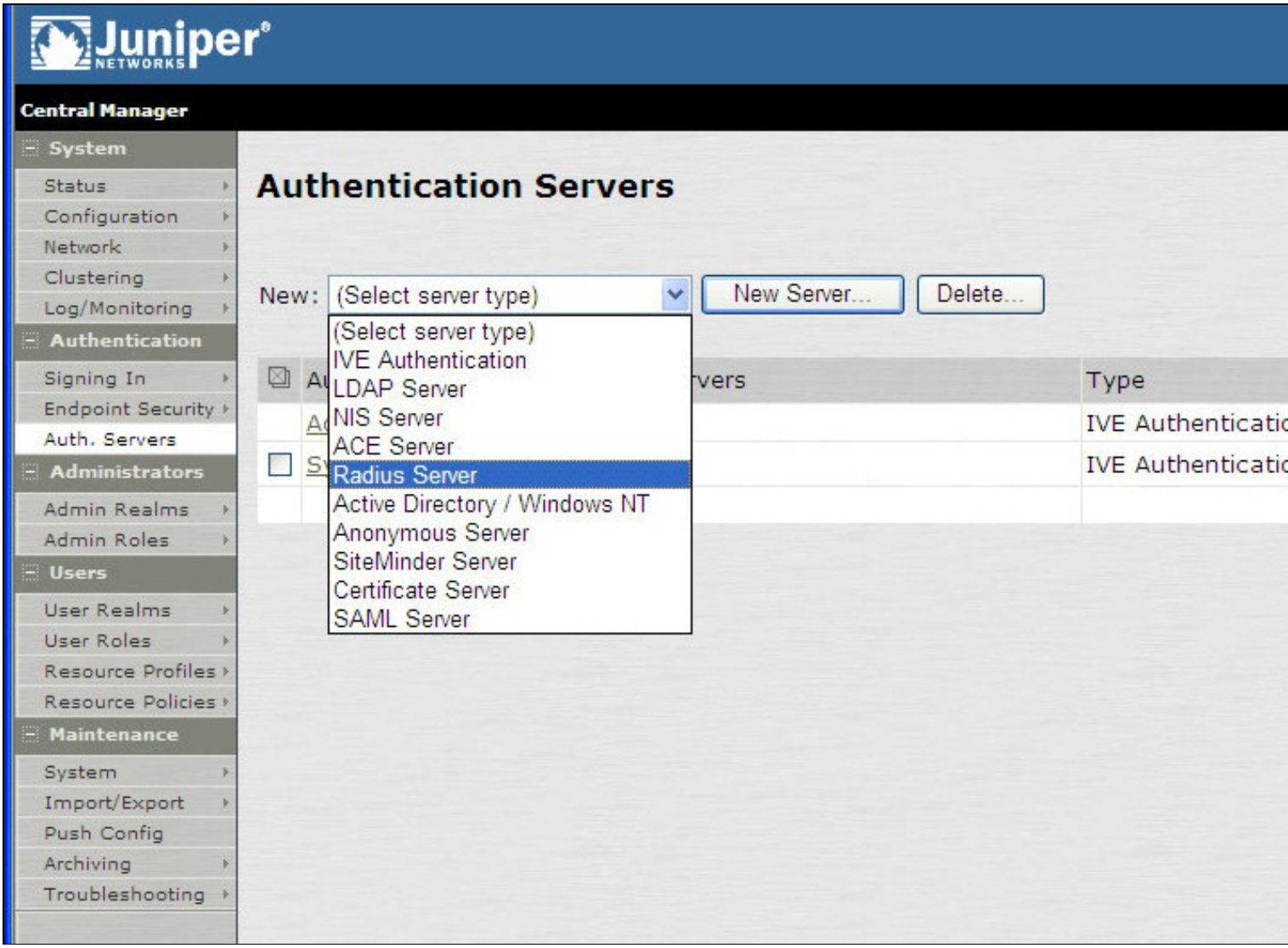
343.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

343.3 Juniper Integration

343.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.



The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

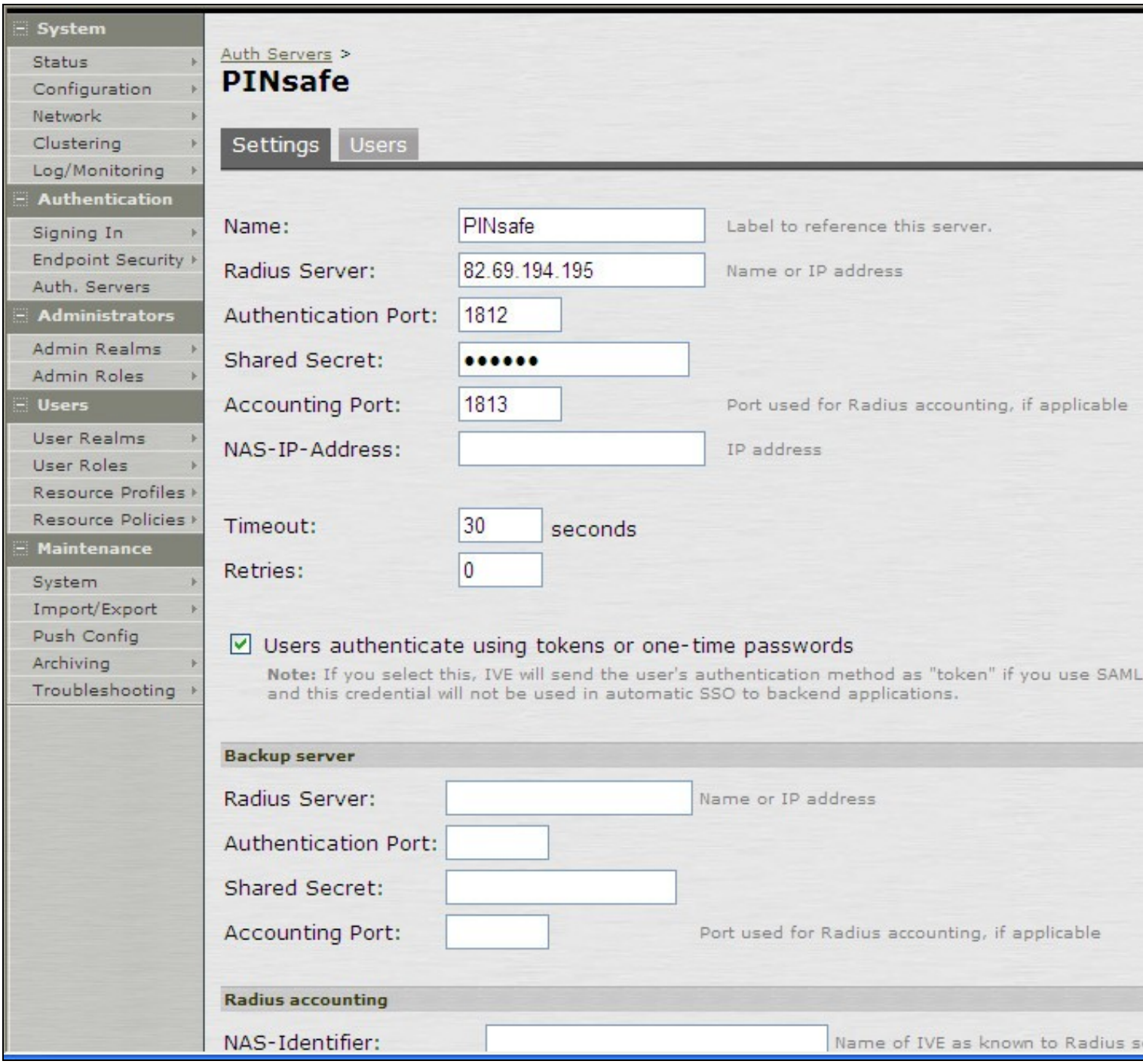
Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

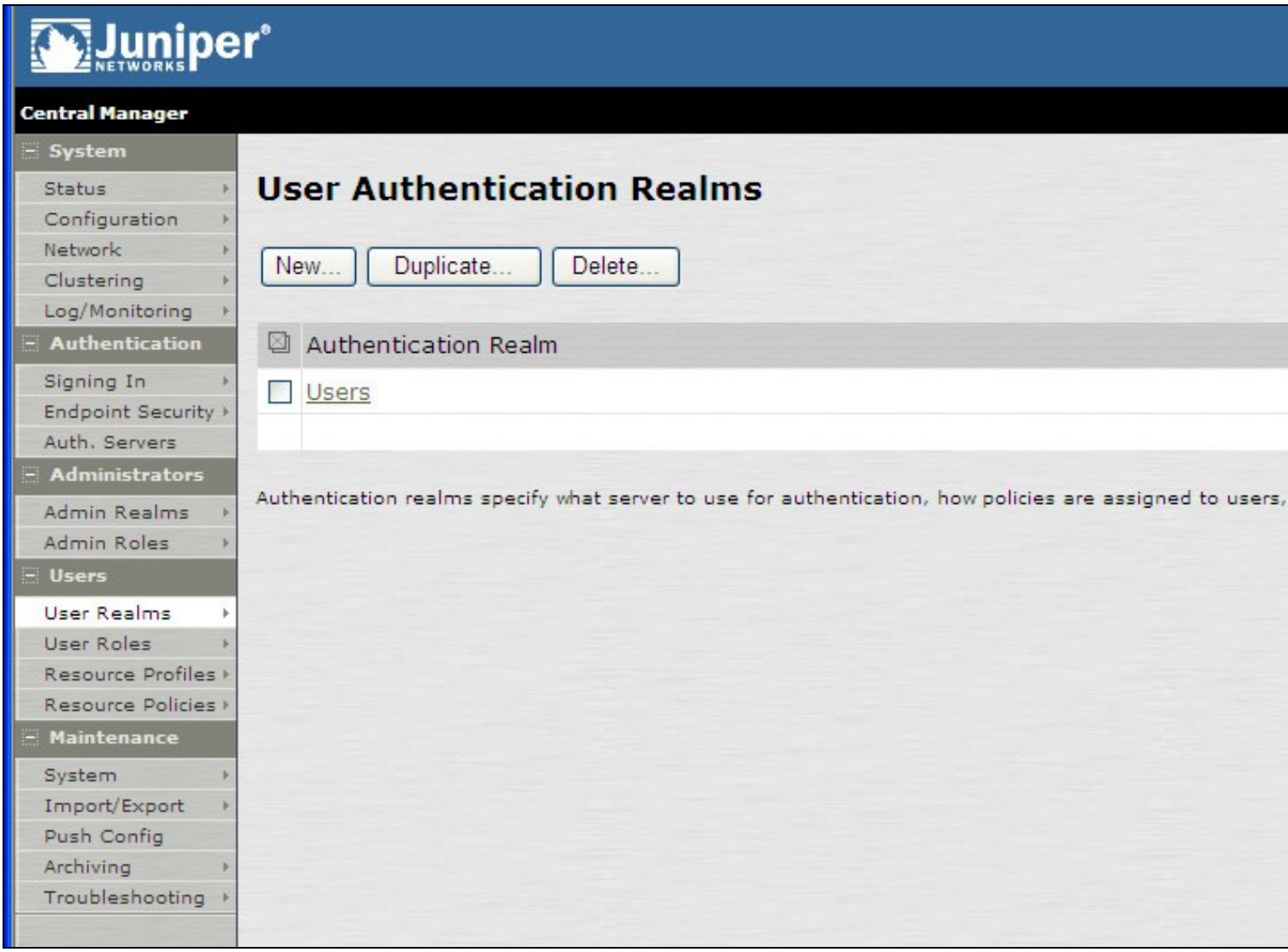
Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.



343.3.2 Authentication Realm Configuration

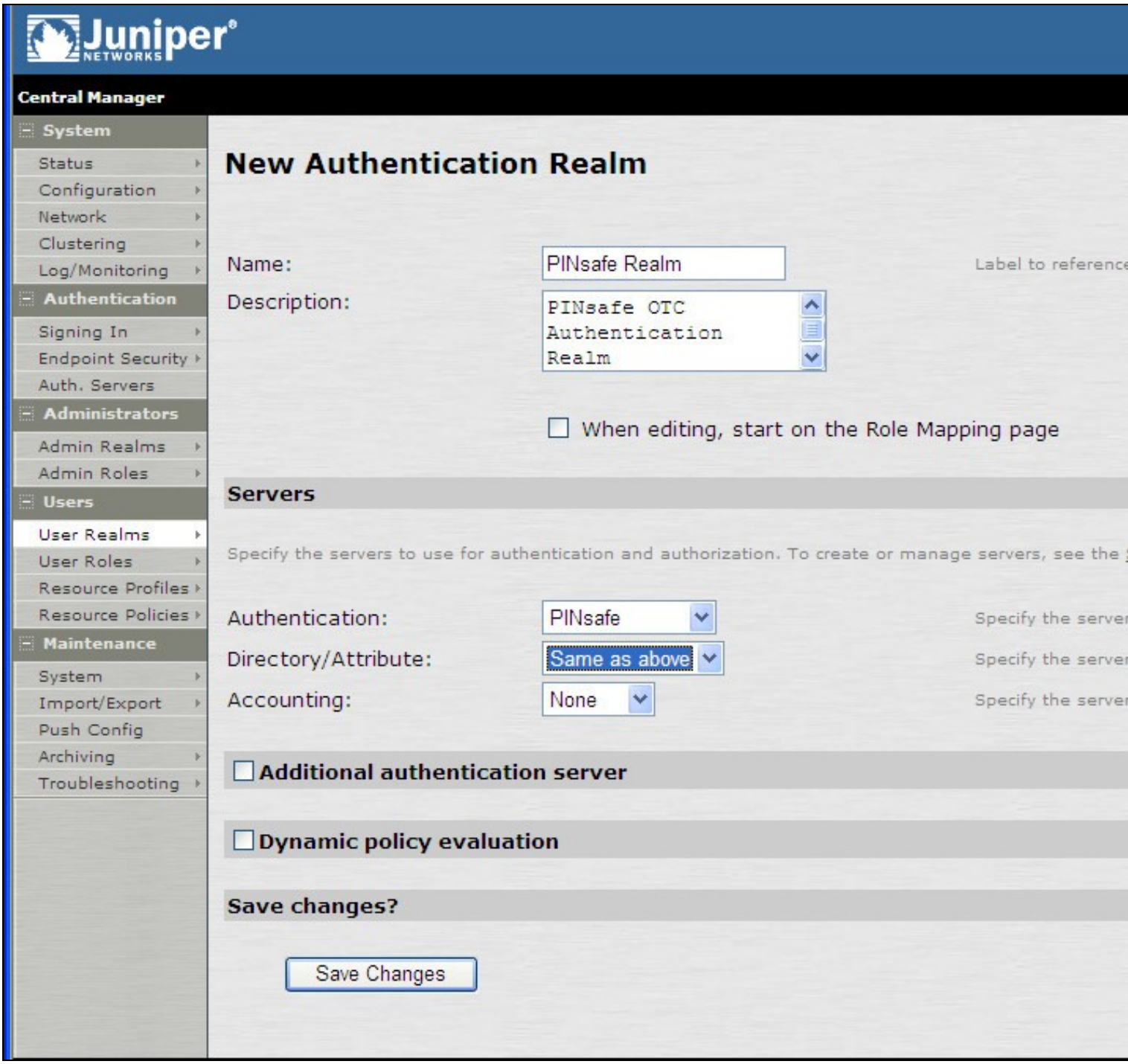
Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.



343.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

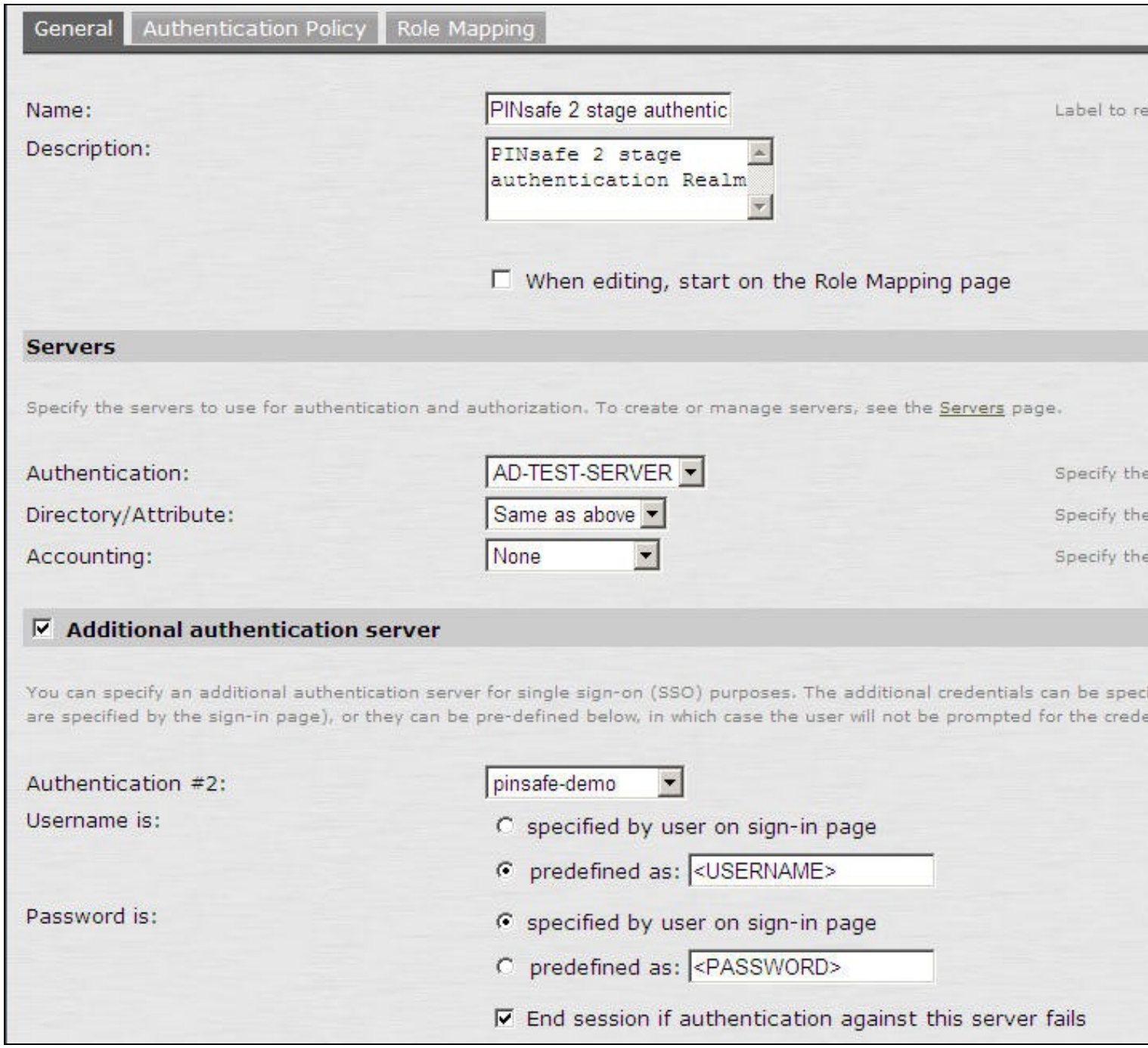
To configure Swivel as the server select the Swivel server as the first listed Authentication Server.



343.3.4 Swivel as the Secondary Authentication Server

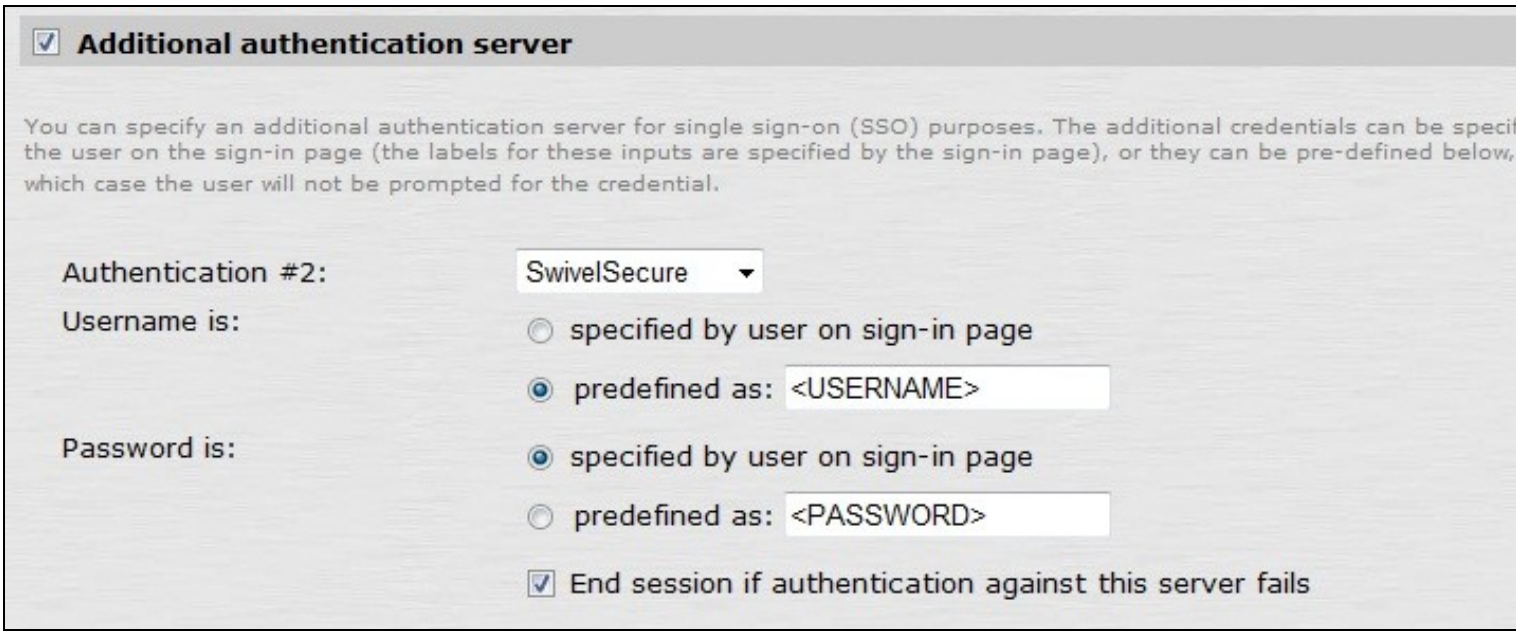
Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box **Additional authentication server**

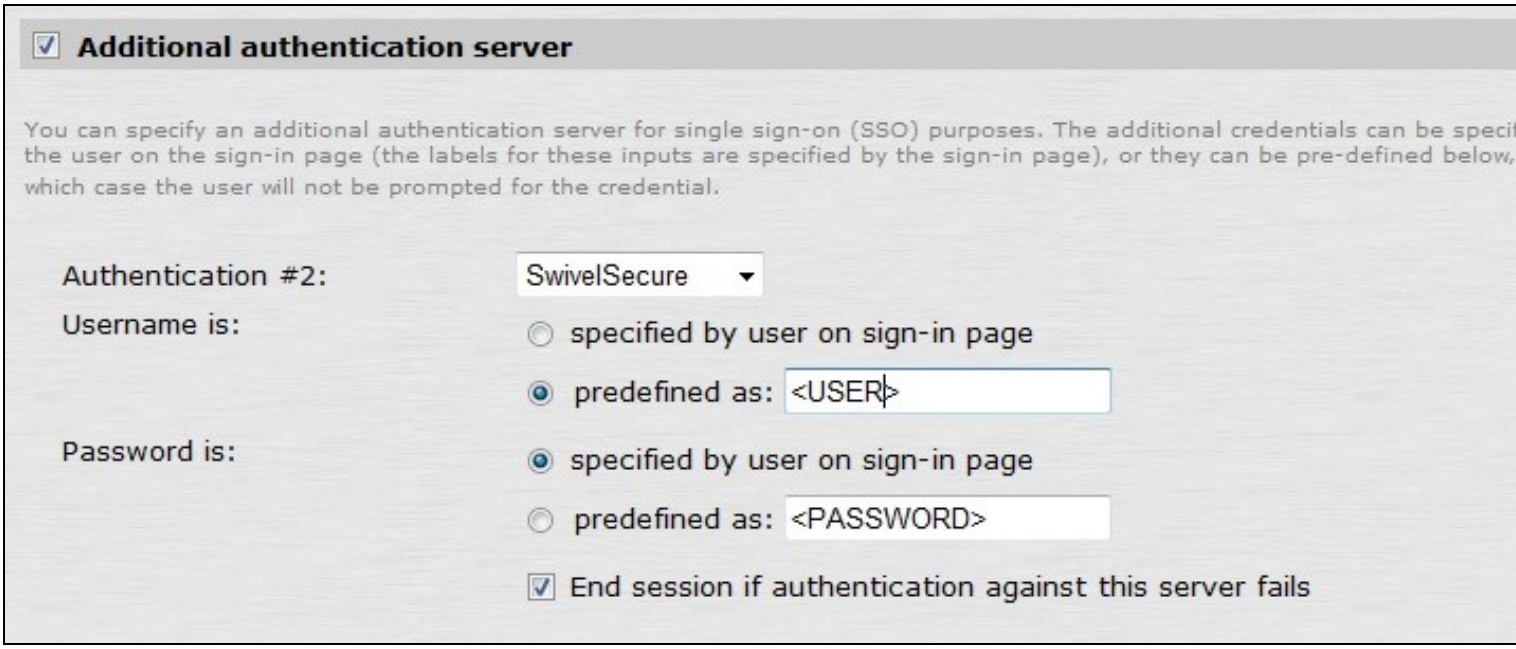


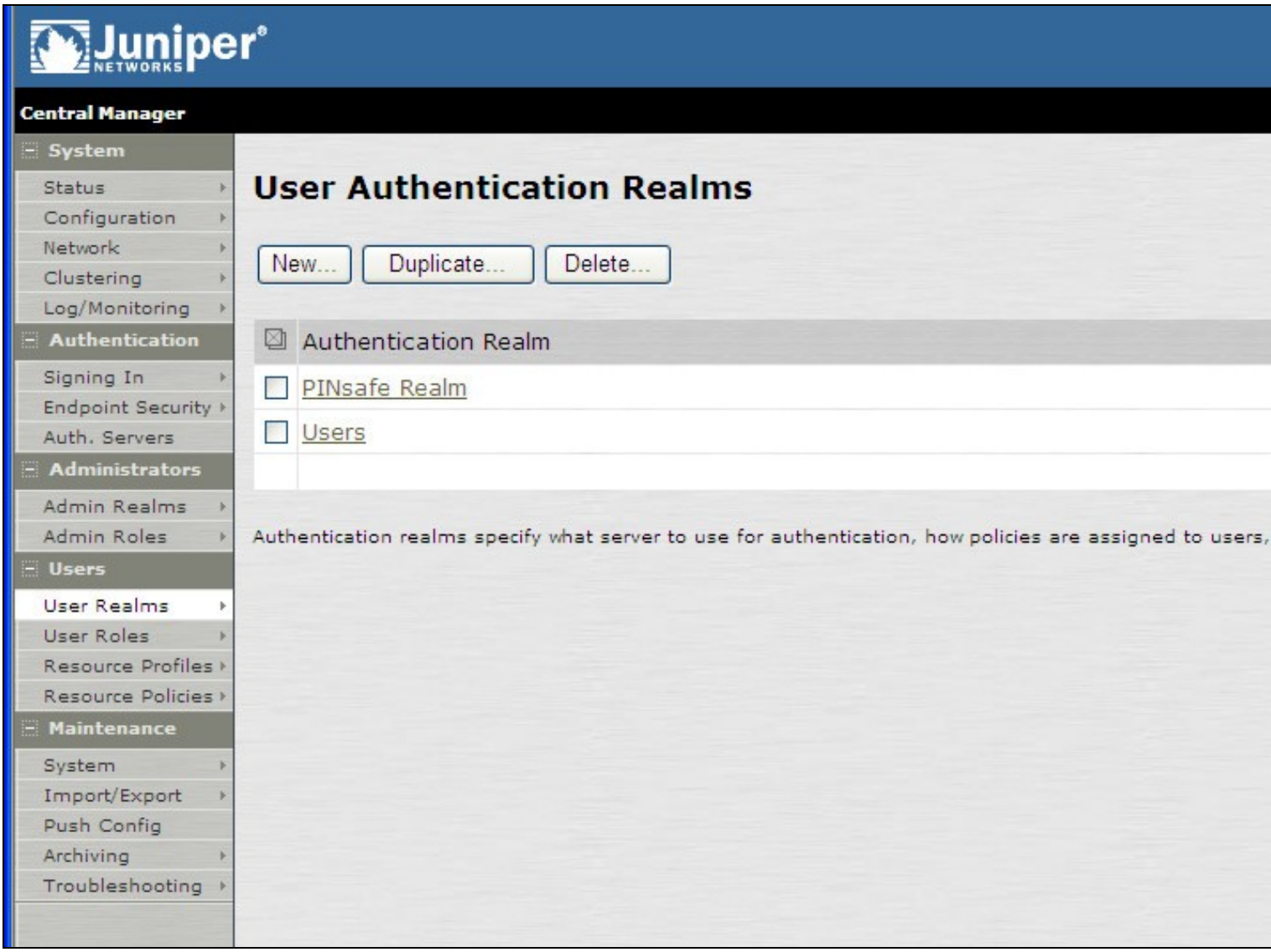
NOTE: when <USERNAME> is used then just the Username is sent to the Juniper, without a Domain prefix/suffix. When <USER> is used then the Domain Name may be added in the authentication request to the Swivel instance in the form domain\username.

USERNAME


Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USERNAME>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails

USER

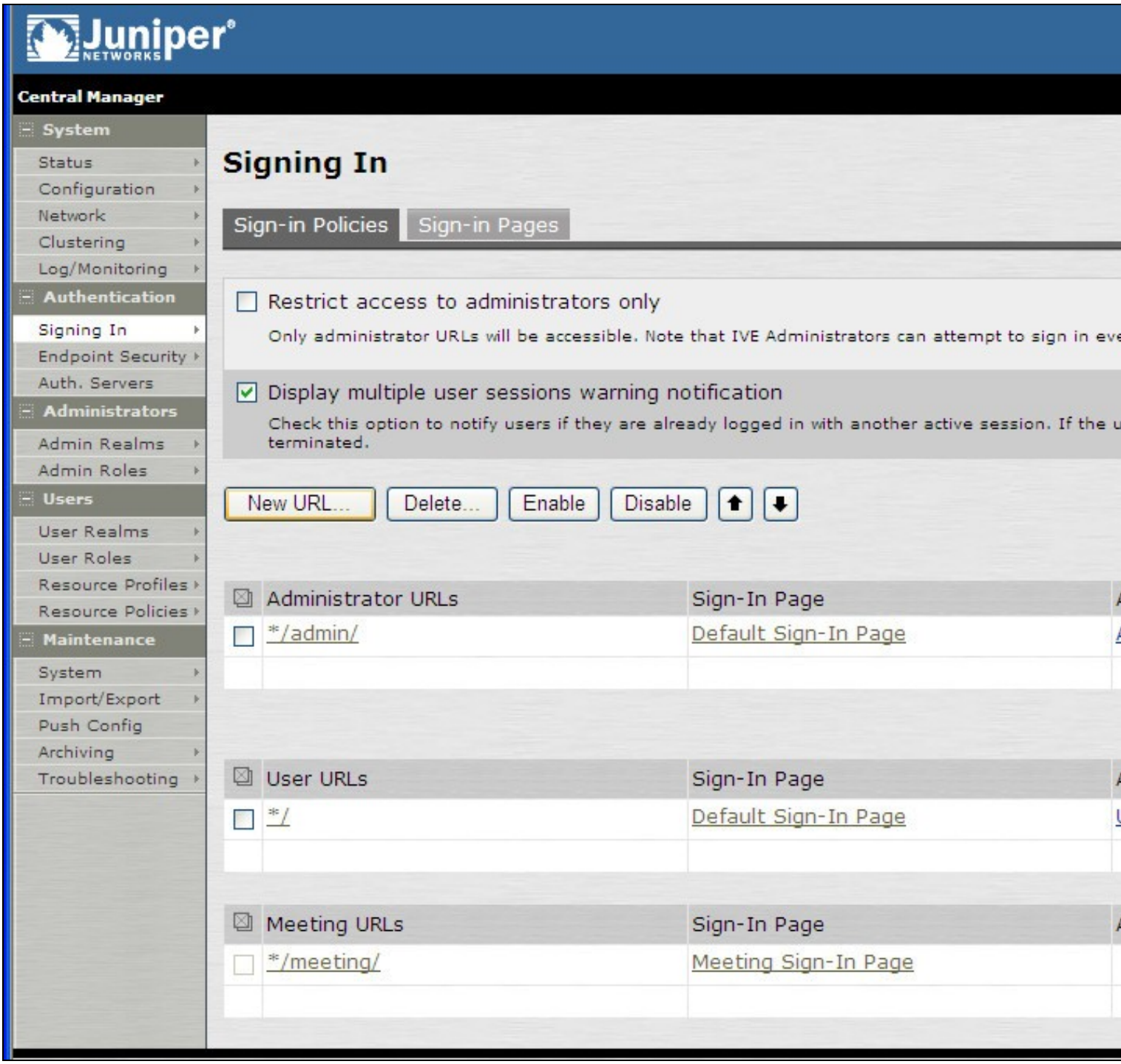

Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USER>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails



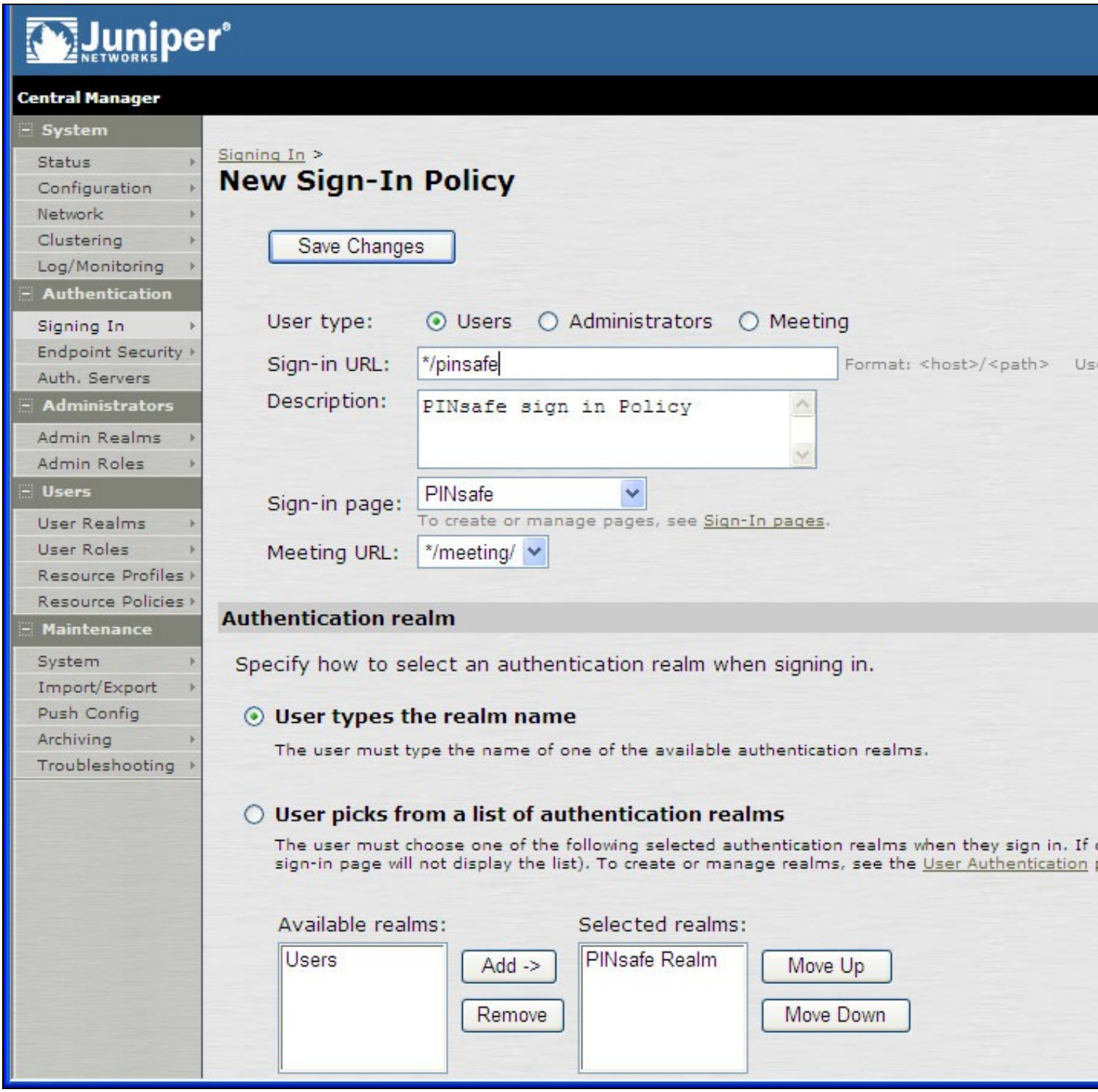
343.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.



Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.



When complete the new Swivel policy should be listed.


Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
Restrict access to administrators only
Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve
Display multiple user sessions warning notification
Check this option to notify users if they are already logged in with another active session. If the u
terminated.
New URL...
Delete...
Enable
Disable
Administrator URLs
Sign-In Page
*/admin/
Default Sign-In Page
User URLs
Sign-In Page
*/
Default Sign-In Page
*/pinsafe/
PINsafe
Meeting URLs
Sign-In Page
*/meeting/
Meeting Sign-In Page

344 Additional Installation Options

Swivel can provide additional authentication options including:

Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

344.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

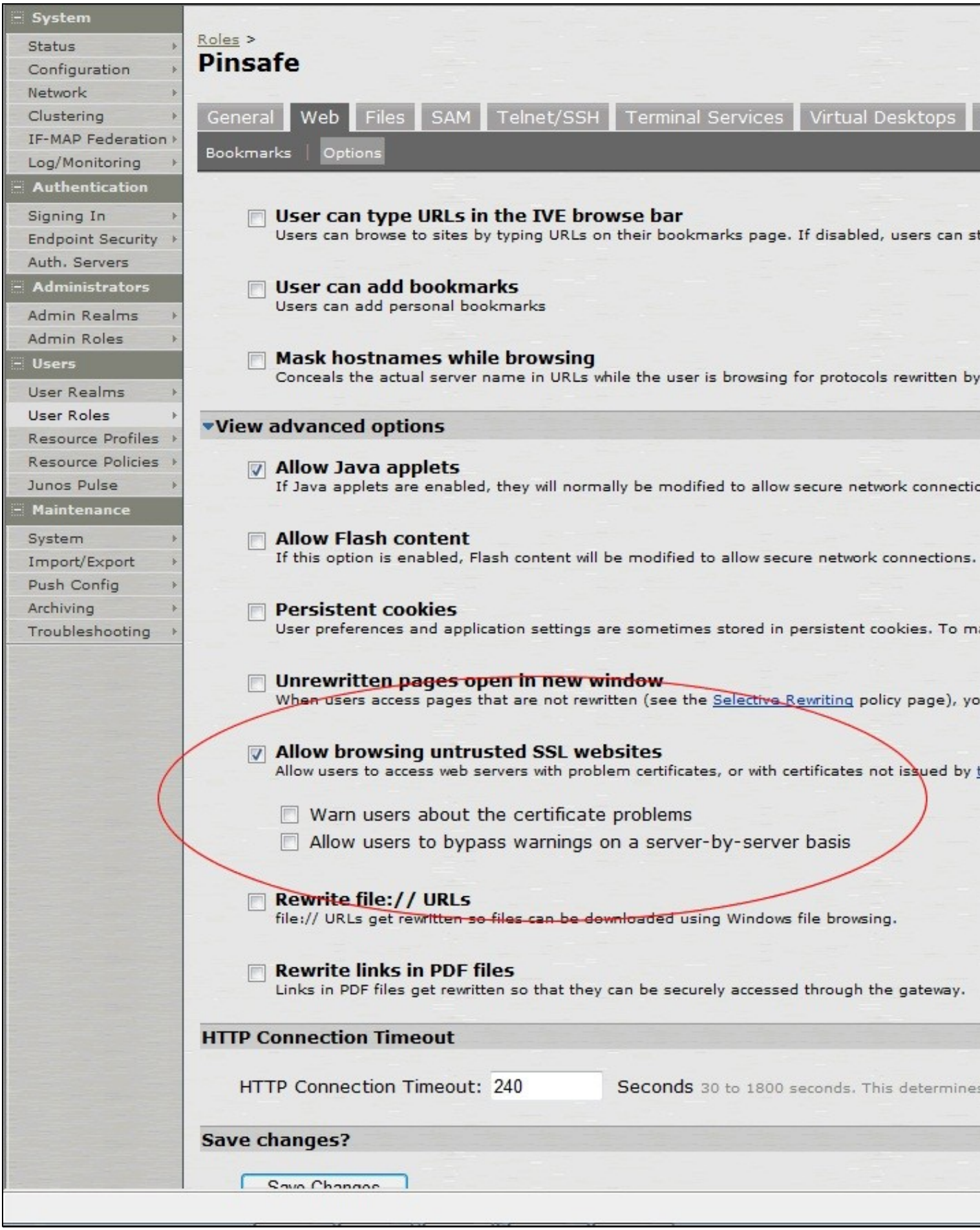
Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

344.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.


System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
Pinsafe
General
Web
Files
SAM
Telnet/SSH
Terminal Services
Virtual Desktops
Bookmarks
Options
User can type URLs in the IVE browse bar
Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can st
User can add bookmarks
Users can add personal bookmarks
Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
View advanced options
Allow Java applets
If Java applets are enabled, they will normally be modified to allow secure network connectio
Allow Flash content
If this option is enabled, Flash content will be modified to allow secure network connections.
Persistent cookies
User preferences and application settings are sometimes stored in persistent cookies. To ma
Unrewritten pages open in new window
When users access pages that are not rewritten (see the Selective Rewriting policy page), yo
Allow browsing untrusted SSL websites
Allow users to access web servers with problem certificates, or with certificates not issued by
Warn users about the certificate problems
Allow users to bypass warnings on a server-by-server basis
Rewrite file:// URLs
file:// URLs get rewritten so files can be downloaded using Windows file browsing.
Rewrite links in PDF files
Links in PDF files get rewritten so that they can be securely accessed through the gateway.
HTTP Connection Timeout
HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determines
Save changes?
Save Changes

344.1.2 Creating an ACL for the Virtual hostname role

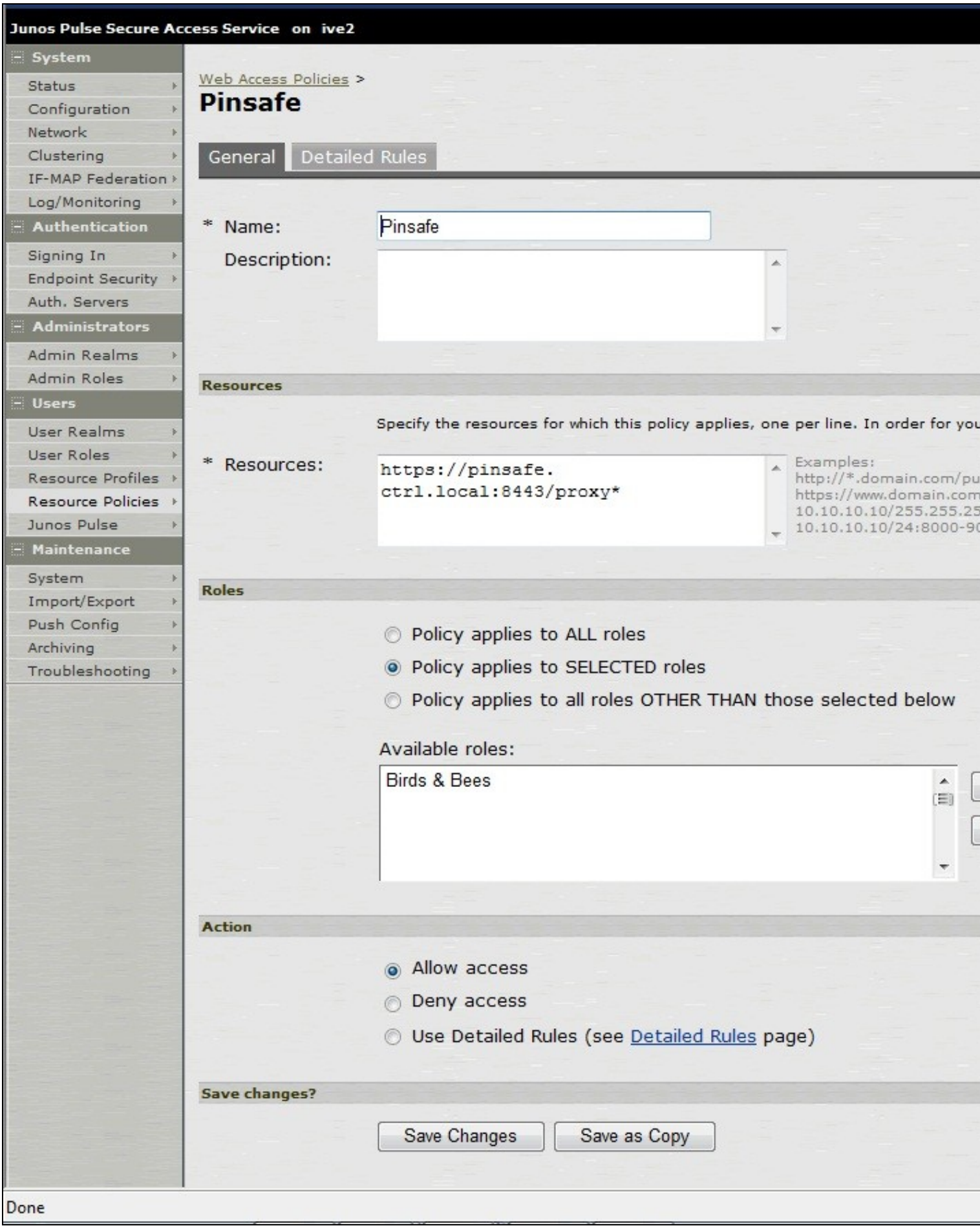
An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.


Junos Pulse Secure Access Service on ive2
System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Web Access Policies >
Pinsafe
General
Detailed Rules
* Name:
Pinsafe
Description:
Resources
Specify the resources for which this policy applies, one per line. In order for you
* Resources:
https://pinsafe.
ctrl.local:8443/proxy*
Examples:
http://*.domain.com/pu
https://www.domain.com
10.10.10.10/255.255.25
10.10.10.10/24:8000-90
Roles
Policy applies to ALL roles
Policy applies to SELECTED roles
Policy applies to all roles OTHER THAN those selected below
Available roles:
Birds & Bees
Action
Allow access
Deny access
Use Detailed Rules (see Detailed Rules page)
Save changes?
Save Changes
Save as Copy
Done

344.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New Page. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

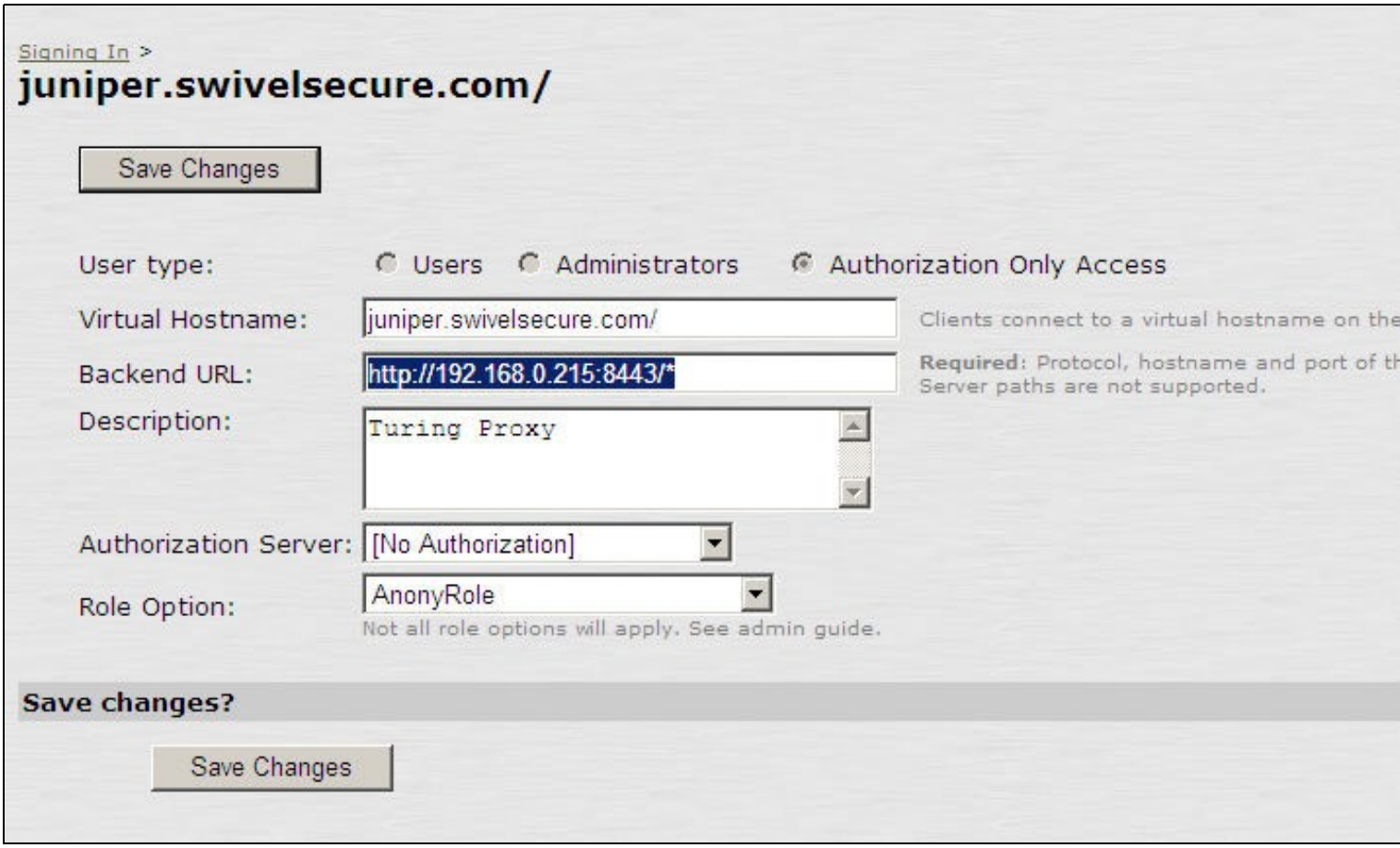
Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

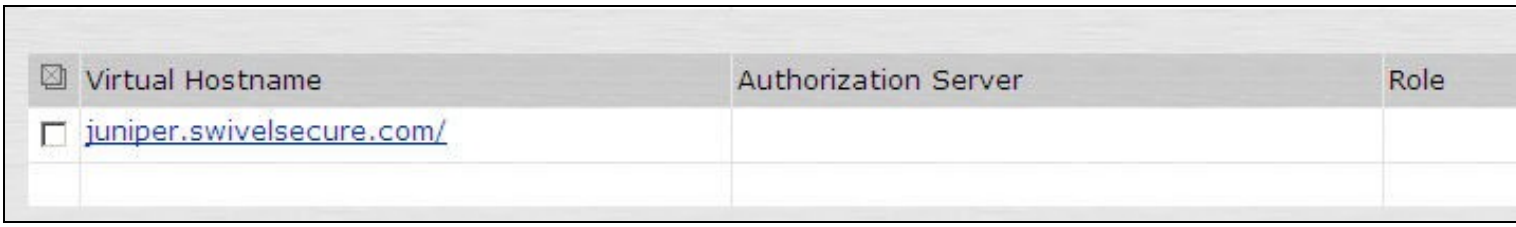
For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes





344.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

https://<turing.mycompany.com>/proxy/SCImage?username=test

Software Install

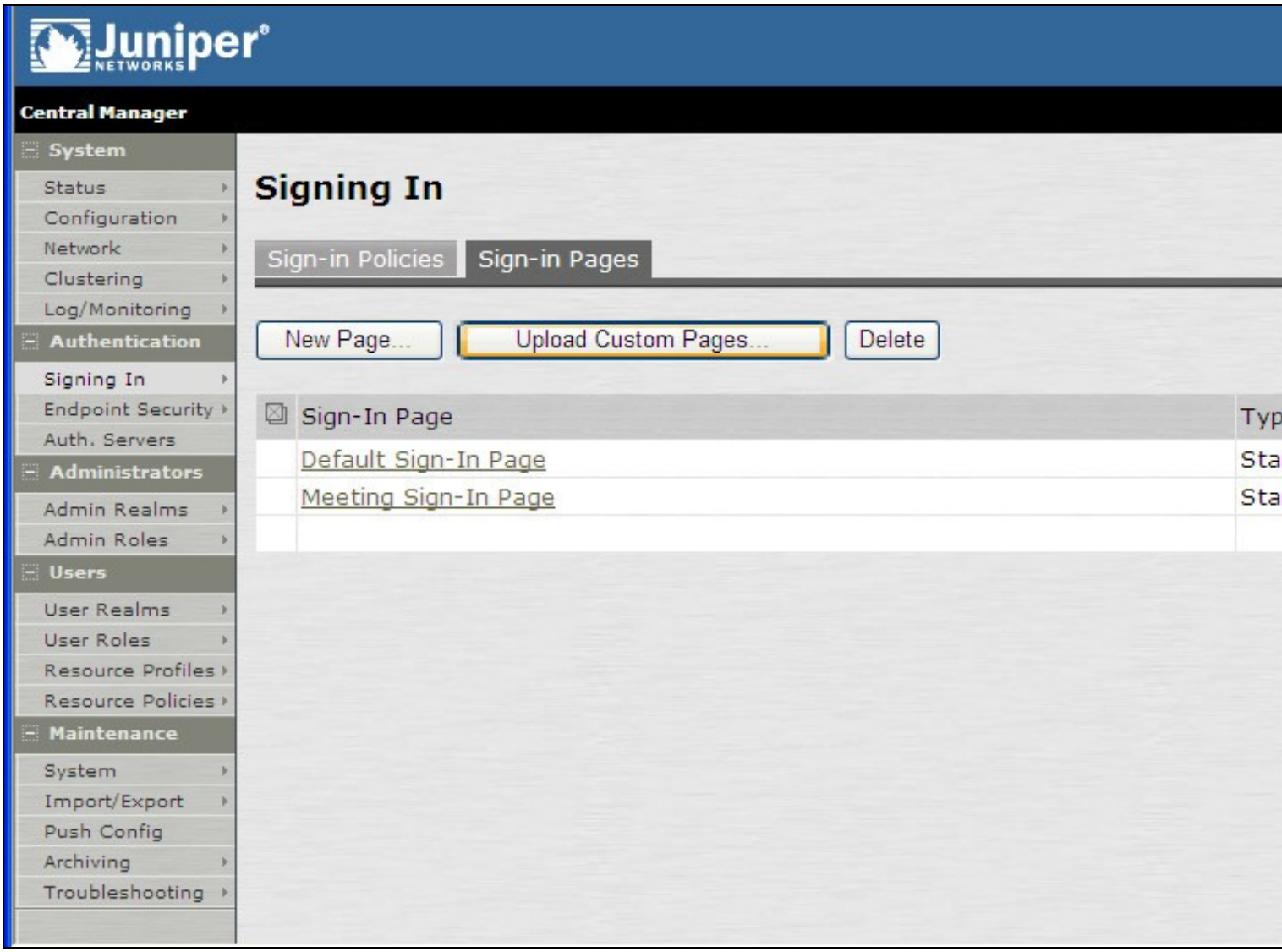
For a software only install see Software Only Installation

Then verify the external access using

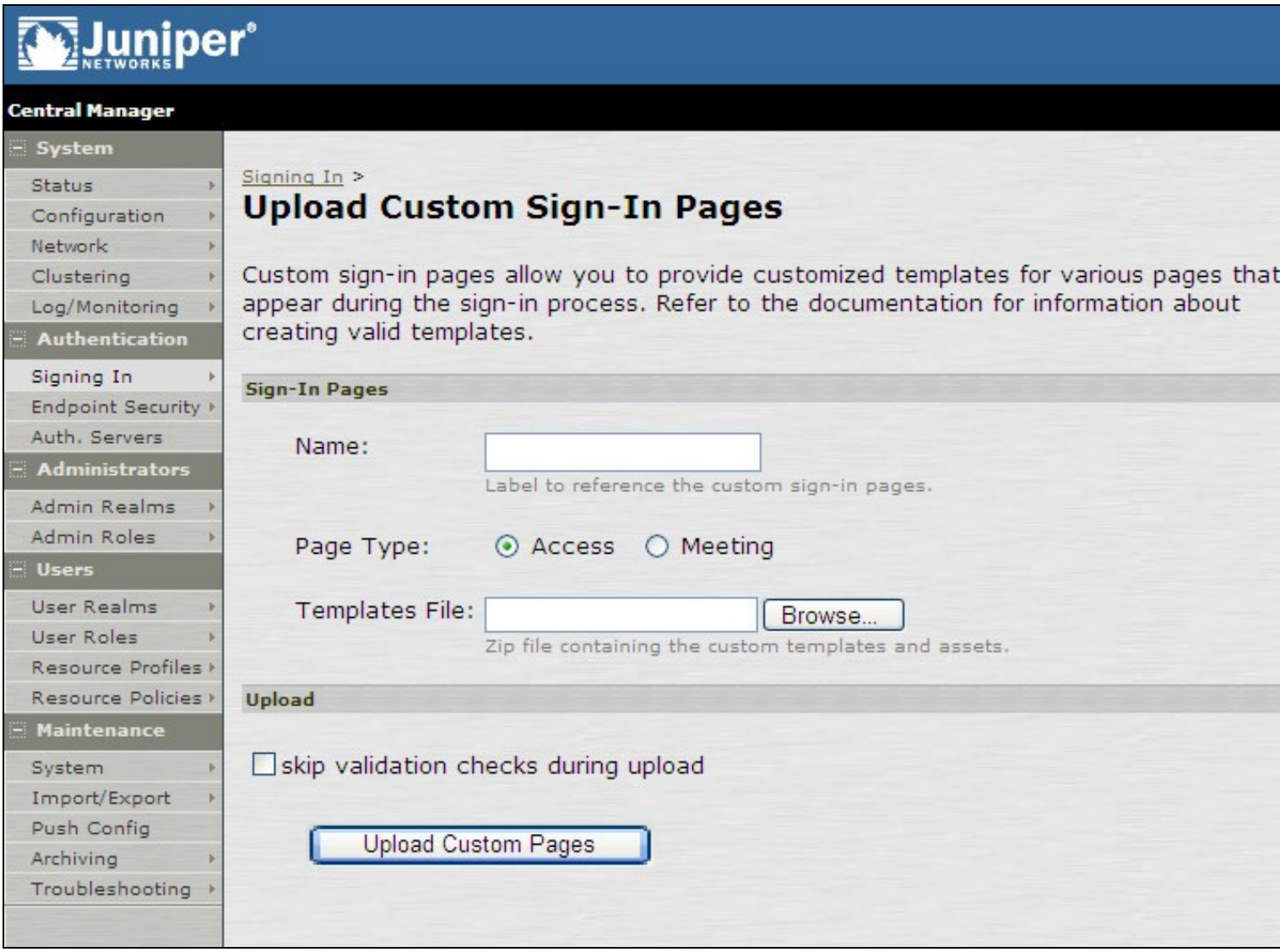
https://<turing.mycompany.com>/pinsafe/SCImage?username=test

344.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.



Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.



Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within **LoginPage.thtml** should be edited to suit your environment as the below modifications.

344.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/SCImage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/SCImage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/SCImage?username=";
```

Software install

```
http://hostname:8080/pinsafe/SCImage?username=";
```

344.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

344.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/DCMessage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/DCMessage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

344.2.4 Modifying the login button text

The login page button and link to *Get Another Image* may be modified.

To modify the login button text locate the text *value='Turing'* and replace the Turing with the required text.

To modify the *Get another image?* URL, locate the two instances of *Get another image?* and change the text as required.

344.2.5 Modifying the login for PINpad

The custom page for Pinpad, is available from here.

Follow the same instructions as above, but note the following:

- The zip file contains 3 additional images that need to go into the *imgs* folder of the Juniper custom login.
- **OTC_OPTION** needs to be set to **"pinpad"**, which it already is in the attached file.

- You need to set the value for *PinpadImage*, rather than *TURingImage* to match your own Swivel instance.

Example

```
var PinpadImage = "https://hostname:8443/pinsafe/SCImage?username=";
```

to

```
var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";
```

344.2.6 Modifying the Login pages for Mobile Devices

Download the mobile modified pages that can be uploaded with any other modified pages to add Swivel authentication to the login.

Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above.

var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

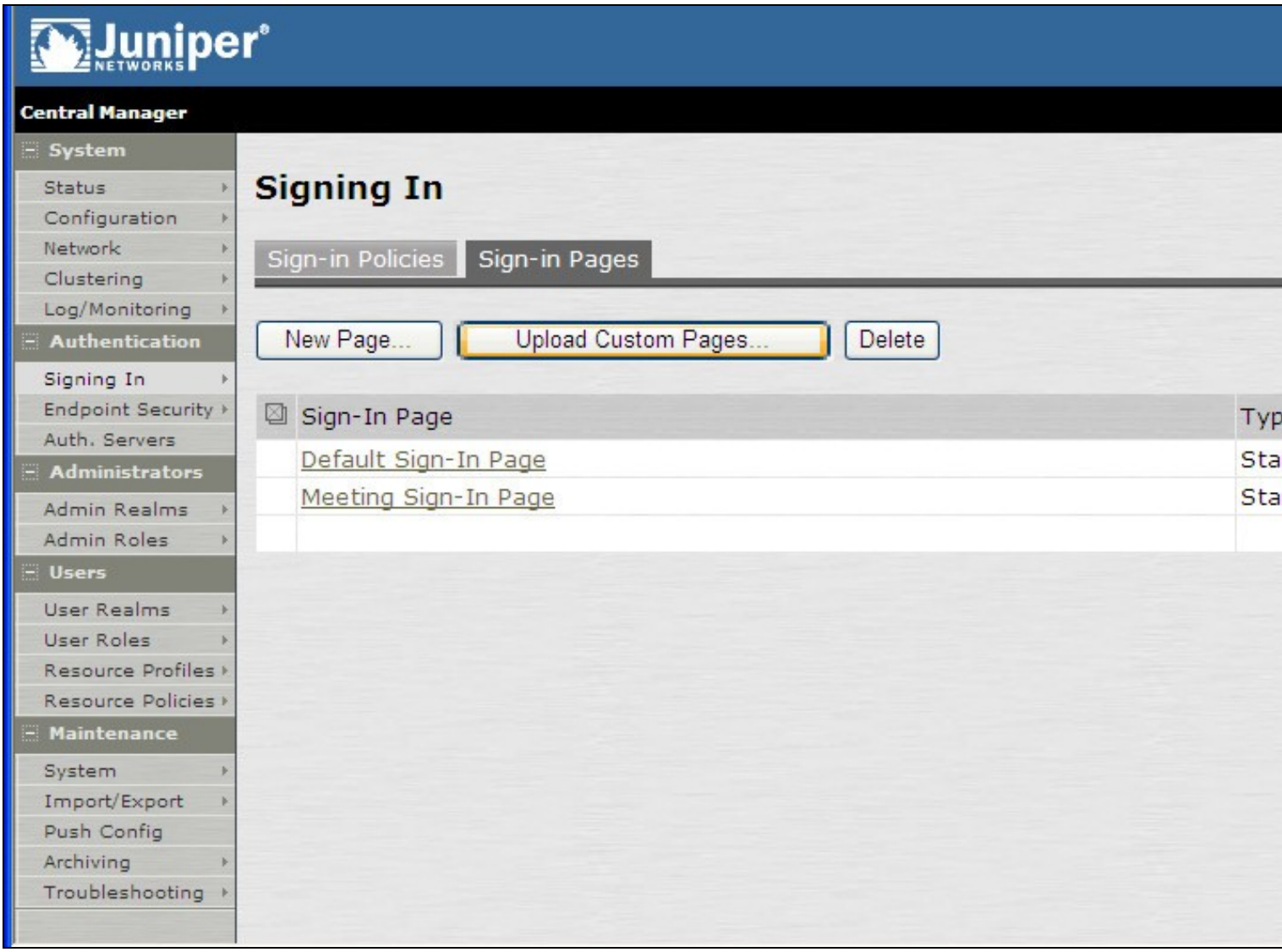
344.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

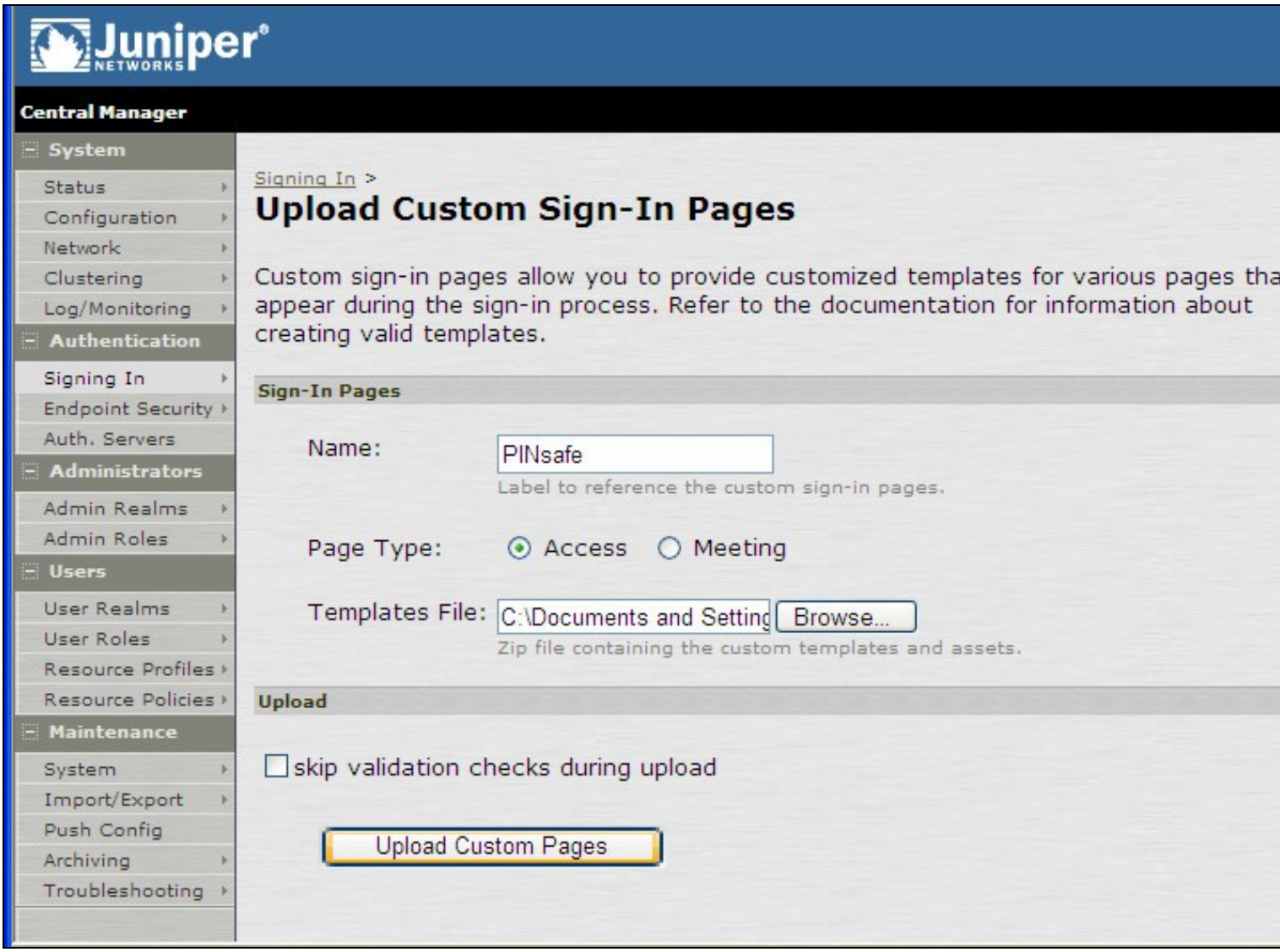
Juniper Network Connect with TURing

344.2.8 Uploading the Modified Page

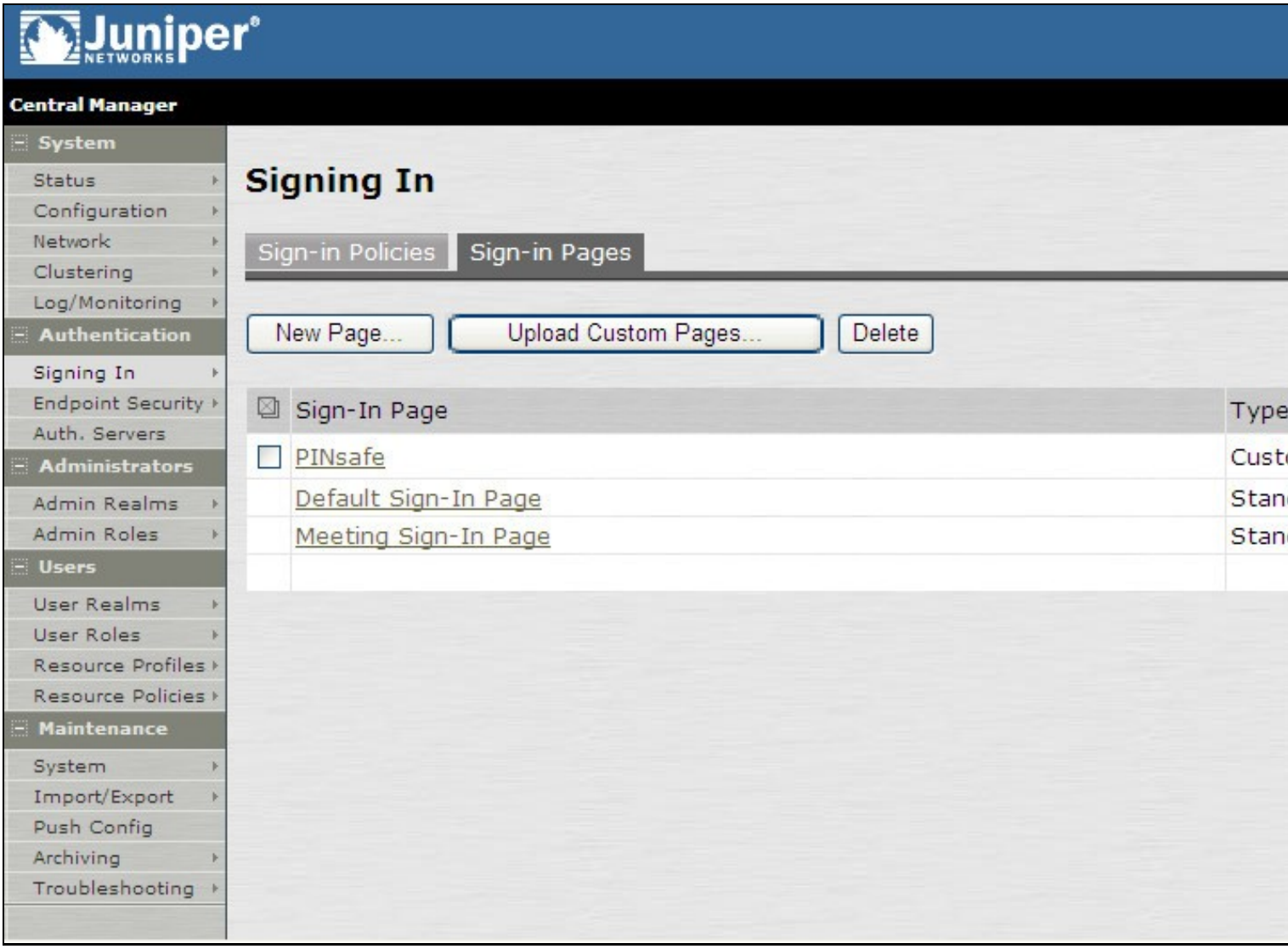
Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.



Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.



The new signing in page should be listed.

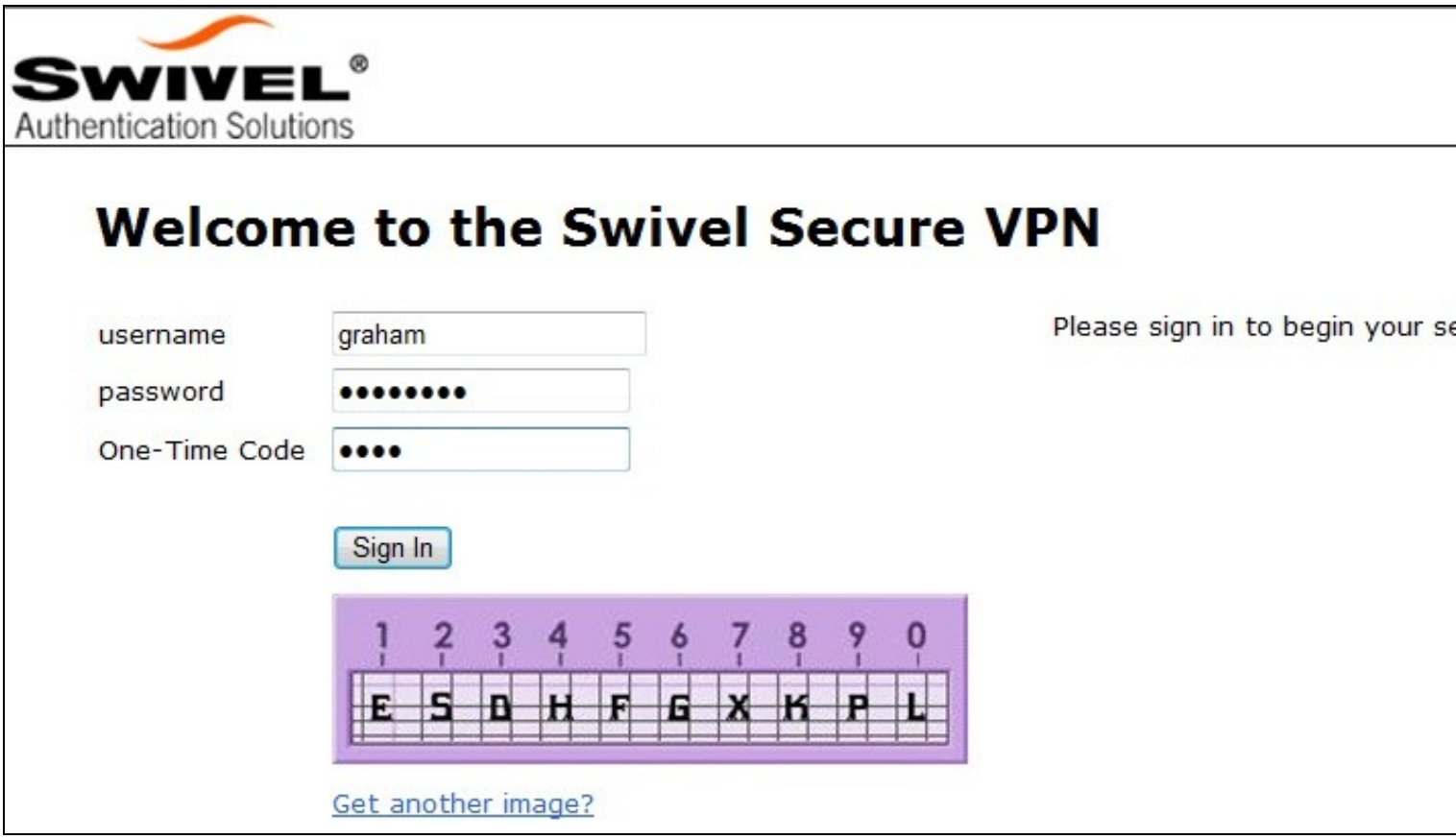

Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
New Page...
Upload Custom Pages...
Delete
Sign-In Page
Type
PINsafe
Default Sign-In Page
Meeting Sign-In Page

345 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

Dual Channel Authentication

Single Channel Authentication



346 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

347 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Internal Certificate Authorities

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username. When USERNAME is used then just the username is sent to the Juniper.

348 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

348.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

```
<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si
```

A modified login page is available here: iPad modified login page

348.2 Junos Pulse usability issue

Junos Pulse for SSL VPN: How to resolve usability issue (very small fonts and field size) with the VPN login screen on iPhone running iOS 7

348.3 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

349 Additional Information

Custom sign-in pages for Pinpad can be found here.

350 Juniper SA 8.x Integration

351 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 7.x integration guide see Juniper SA 7.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

352 Prerequisites

Juniper 8.x

Swivel 3.x

Modified login pages can be downloaded below. Note that you don't need the included image files unless you are using Pinpad.

It is possible to access Juniper SSL VPN from all mobile devices, however additional pages need to be modified to support Swivel integration.

Mobile login pages can be downloaded below, and should be included if the Single channel images are required on mobile devices. NOTE: These have not been tested on version 8.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. Since the Juniper will be supporting at least two different host names, the SSL certificate on the Juniper must either be a wildcard certificate, or must include SANs (Subject Alternative Names) for all host names used.

353 File Downloads

PINsafe modified pages

Swivel Mobile login pages

Modified pages for both PC and tablets. These files have been tested internally only, and do not currently work with PINpad on tablets. The main advantage is that you only need edit one file - swivel-header.thtml - to set the image URL for all devices.

354 Baseline

Juniper 8

Swivel 3.9.7

355 Architecture

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

356 Installation

356.1 Swivel Configuration

356.1.1 Configuring the RADIUS server

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

356.1.2 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.

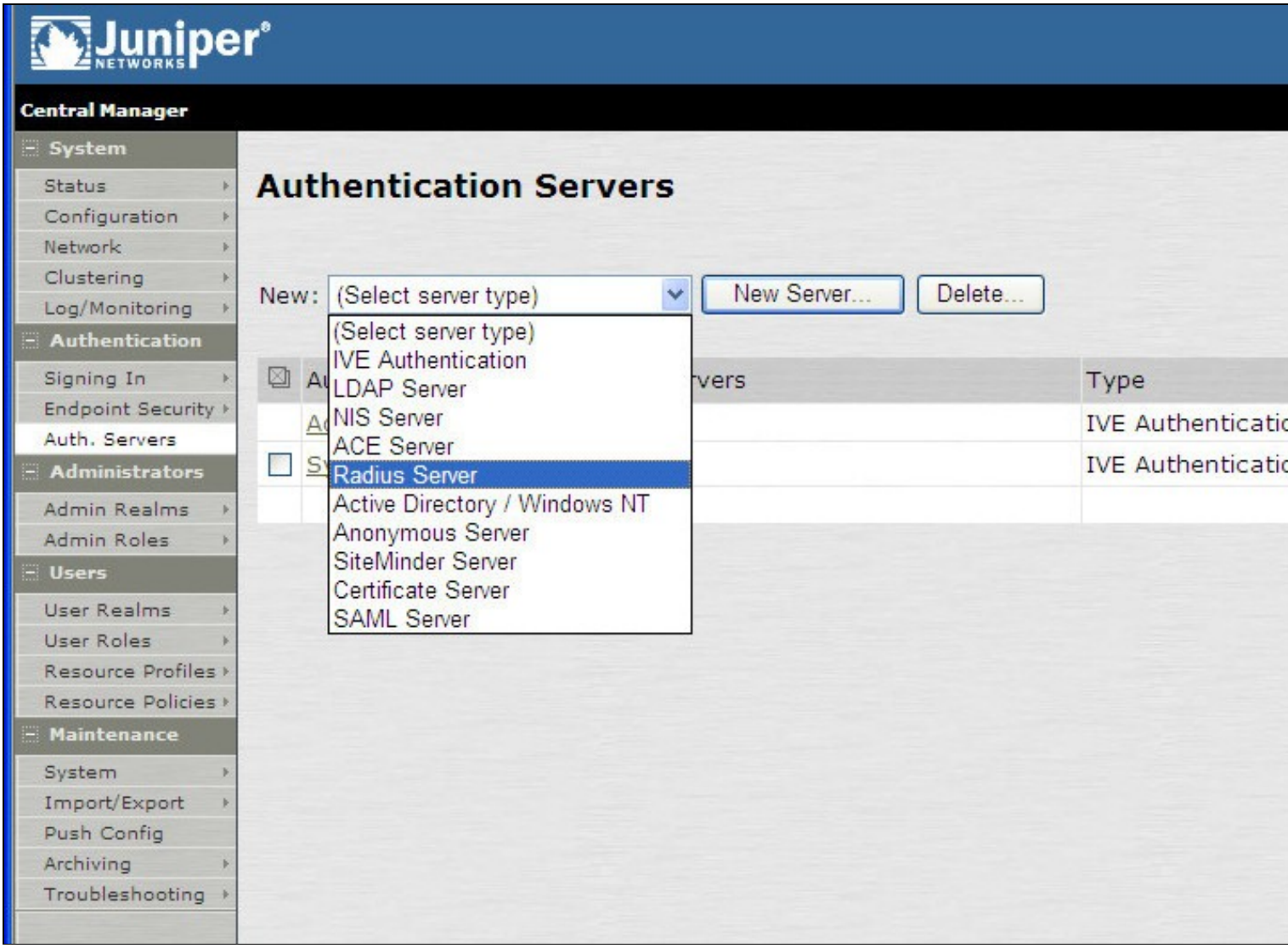
356.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

356.3 Juniper Integration

356.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.



The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

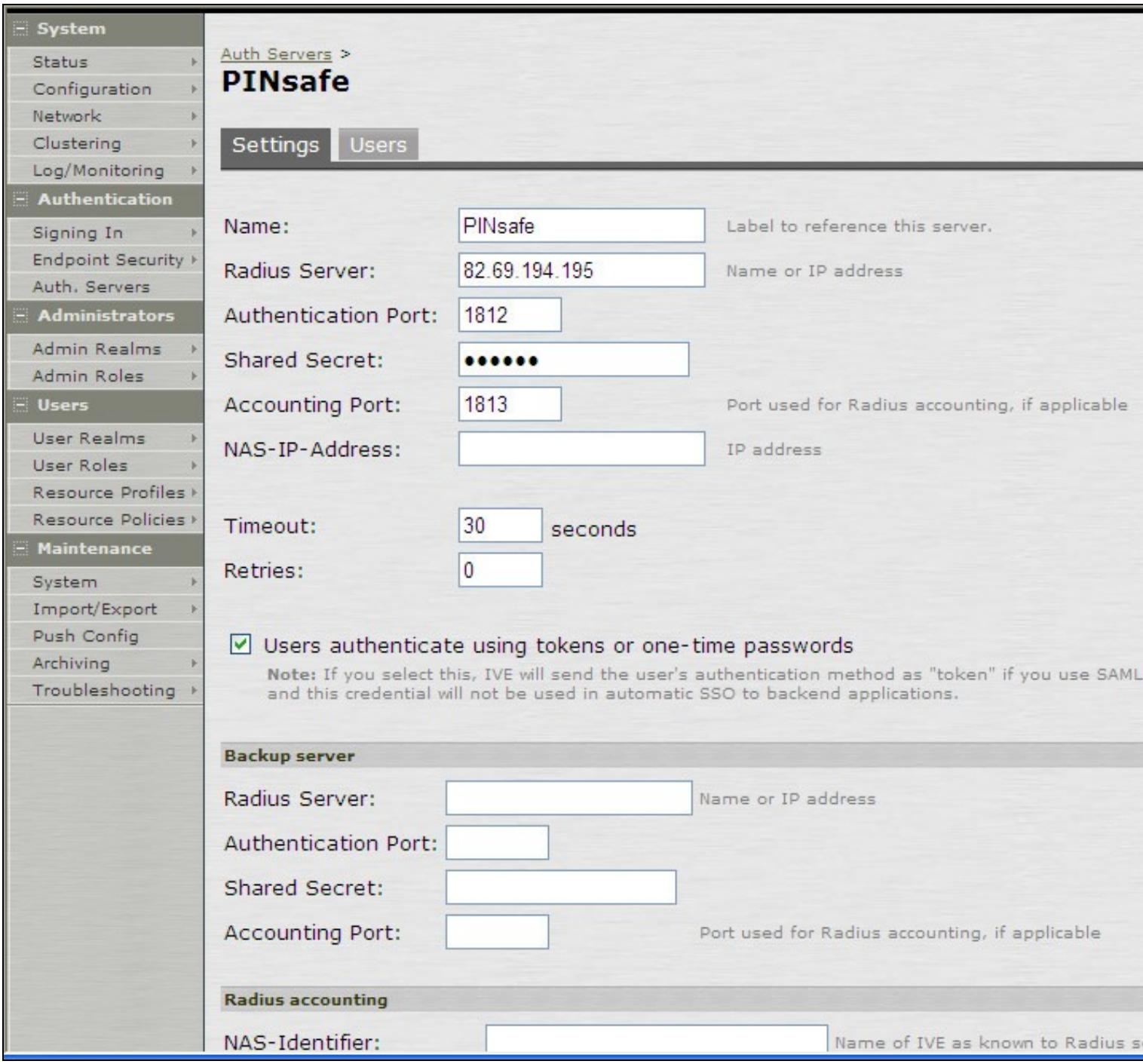
Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

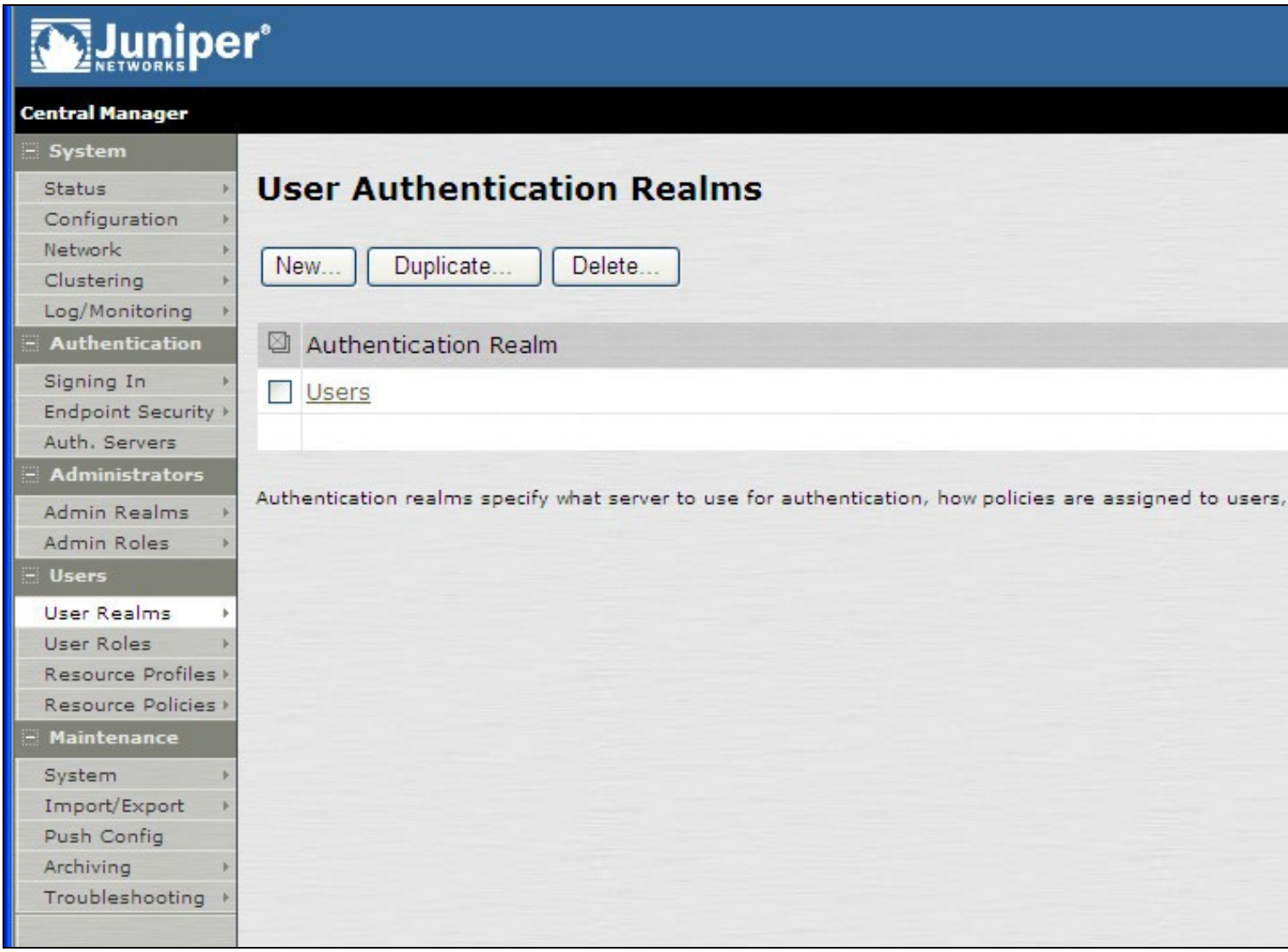
Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.



356.3.2 Authentication Realm Configuration

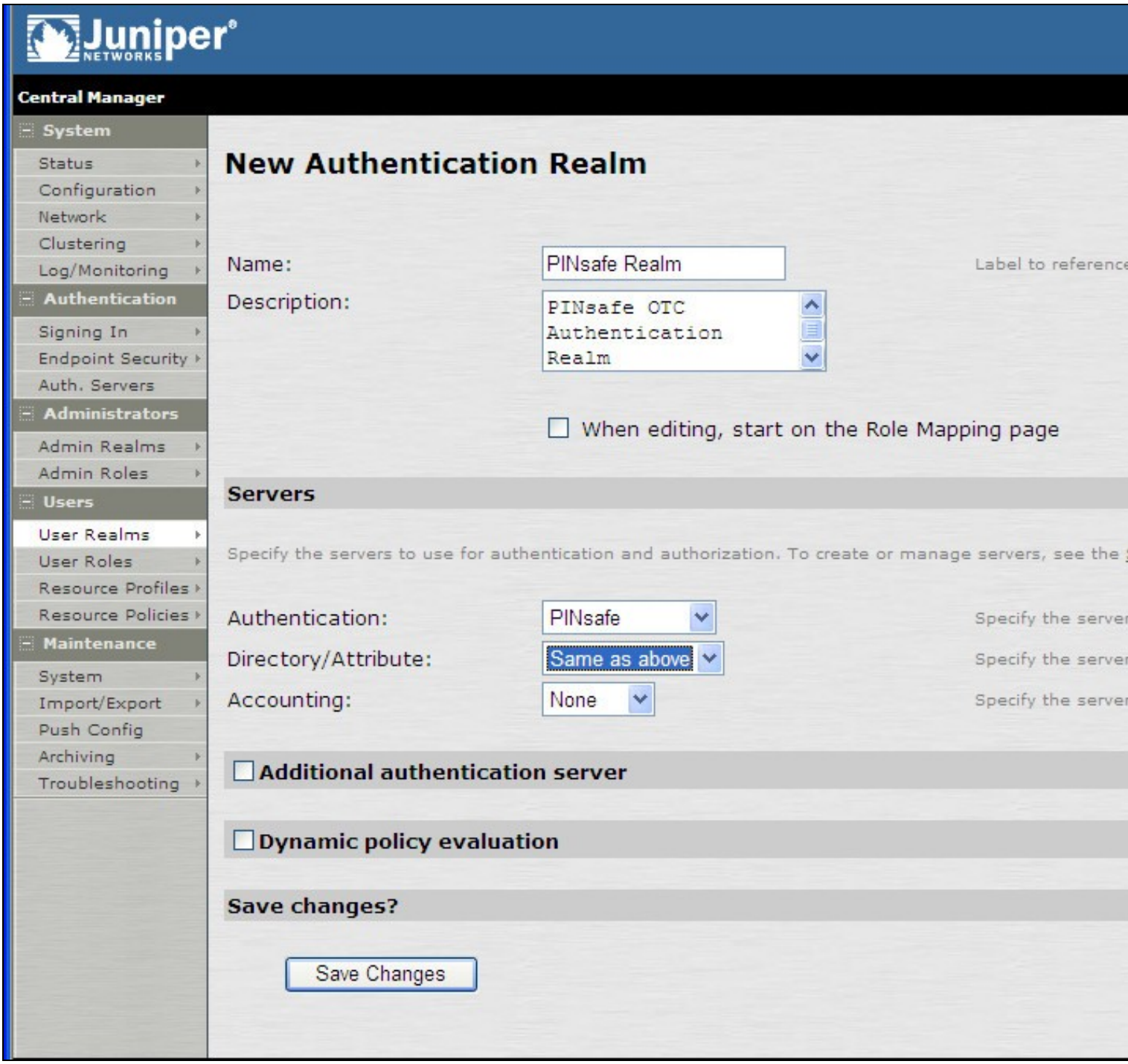
Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.



356.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

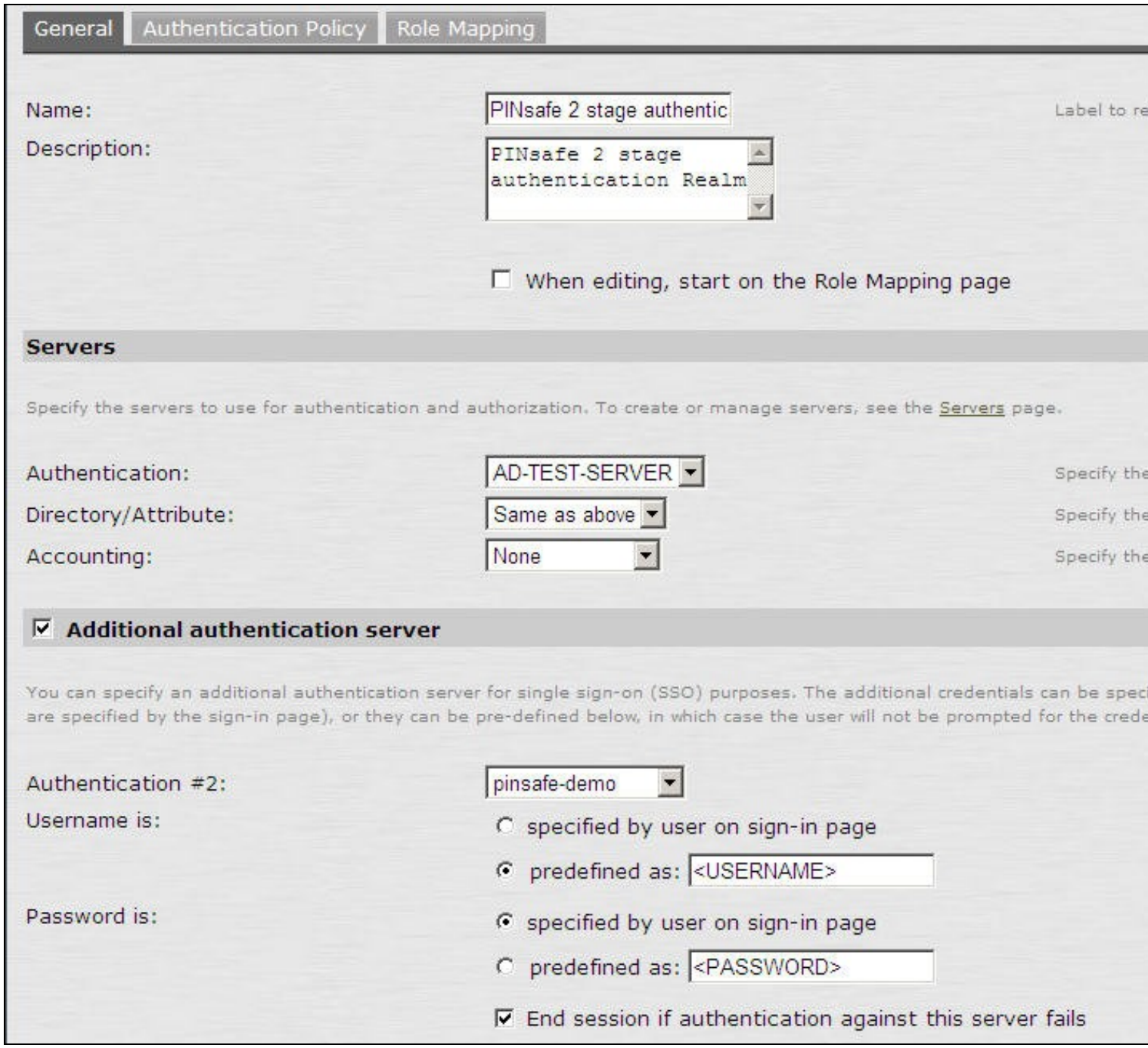
To configure Swivel as the server select the Swivel server as the first listed Authentication Server.



356.3.4 Swivel as the Secondary Authentication Server

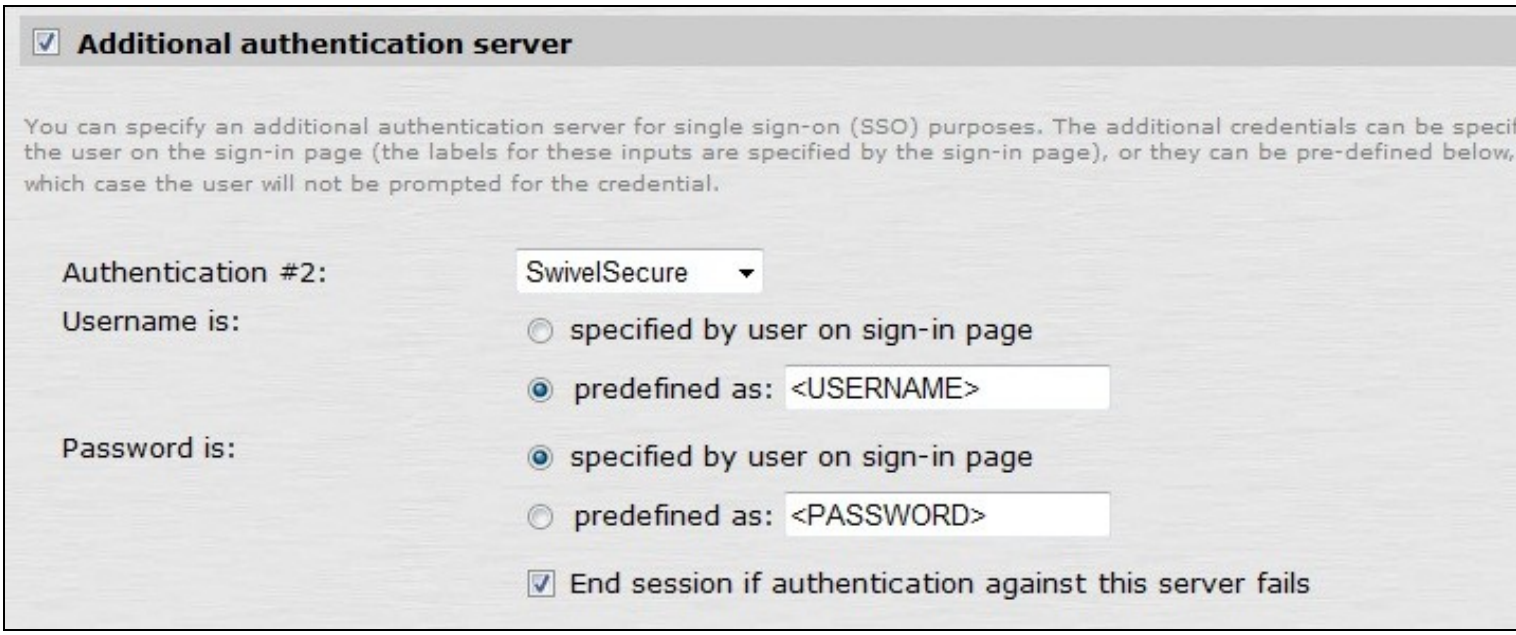
Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box **Additional authentication server**

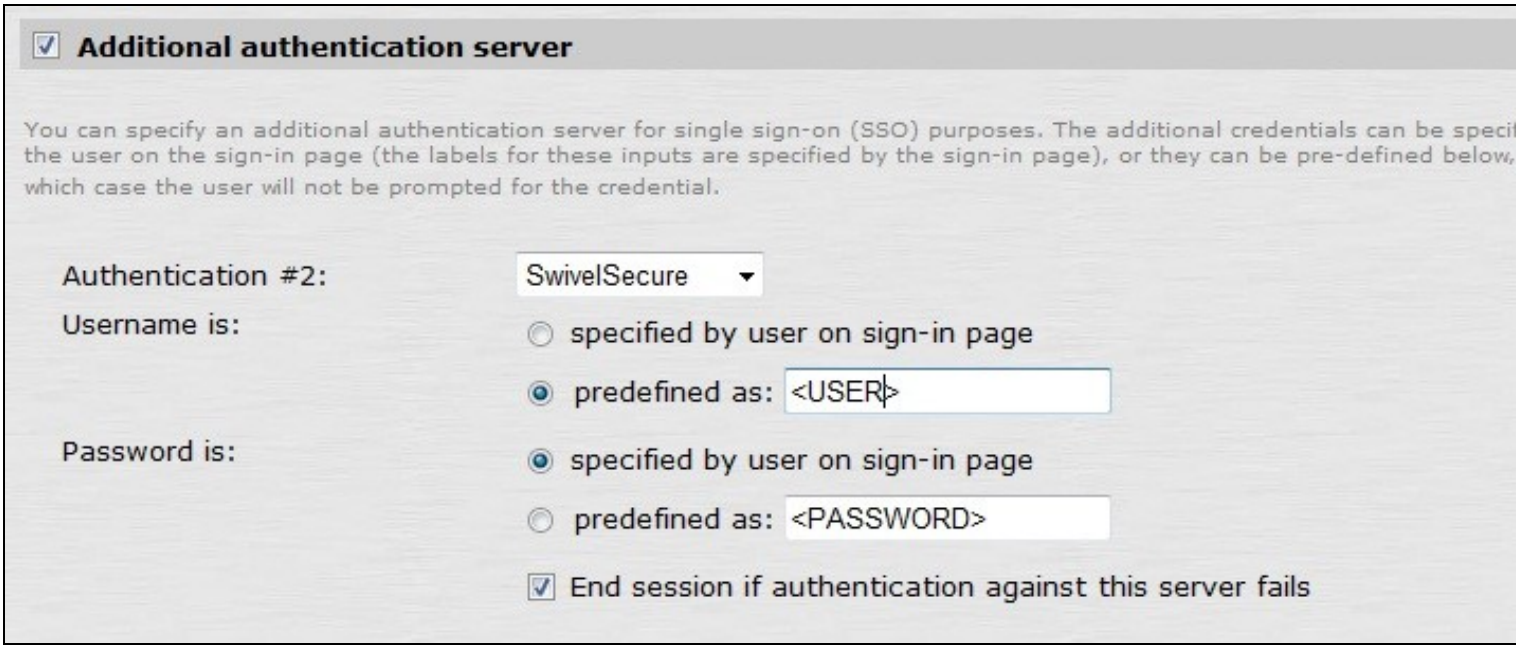


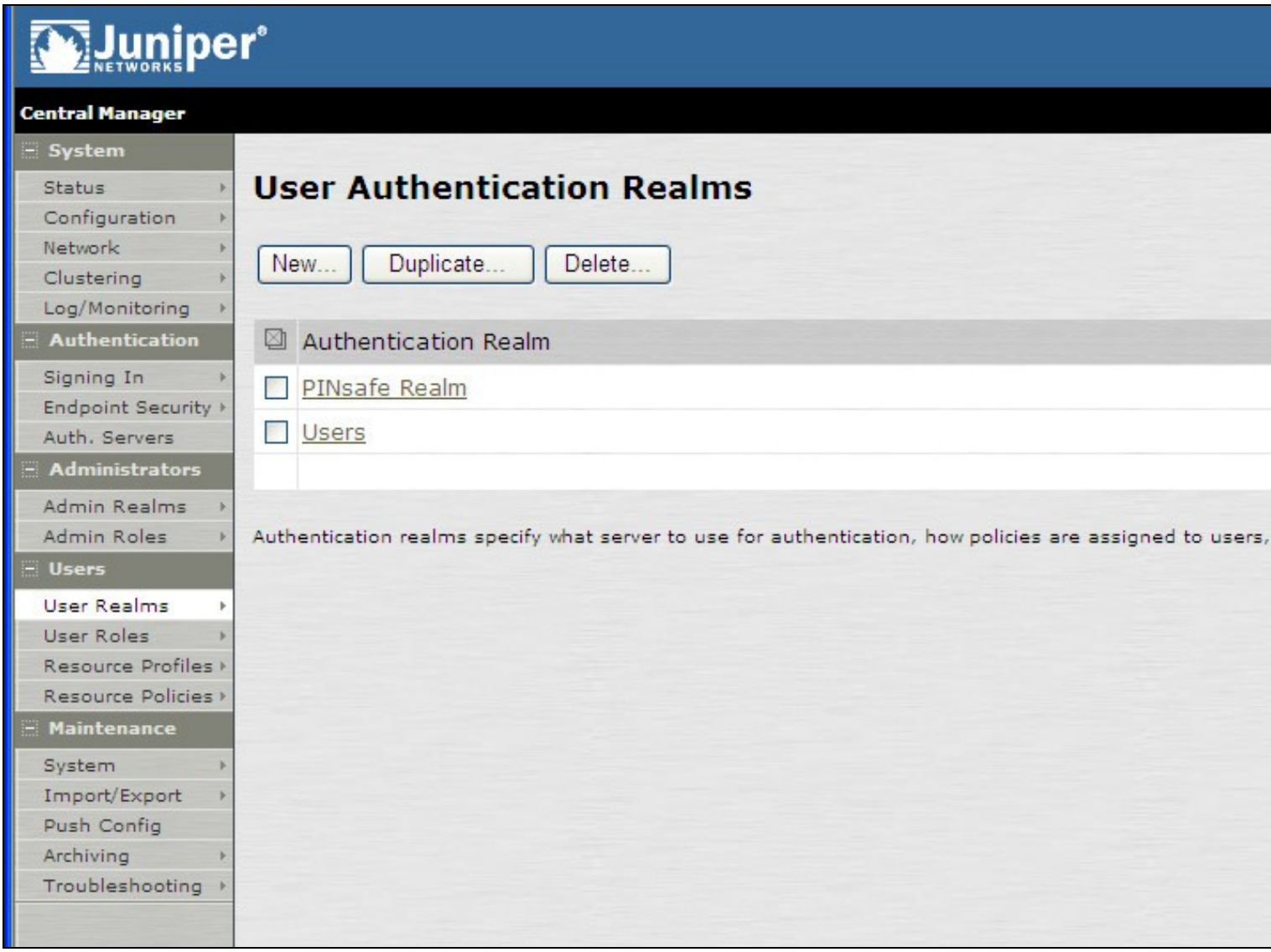
Note when USERNAME is used then just the username is sent to the Juniper. When USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username.

USERNAME


Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USERNAME>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails

USER

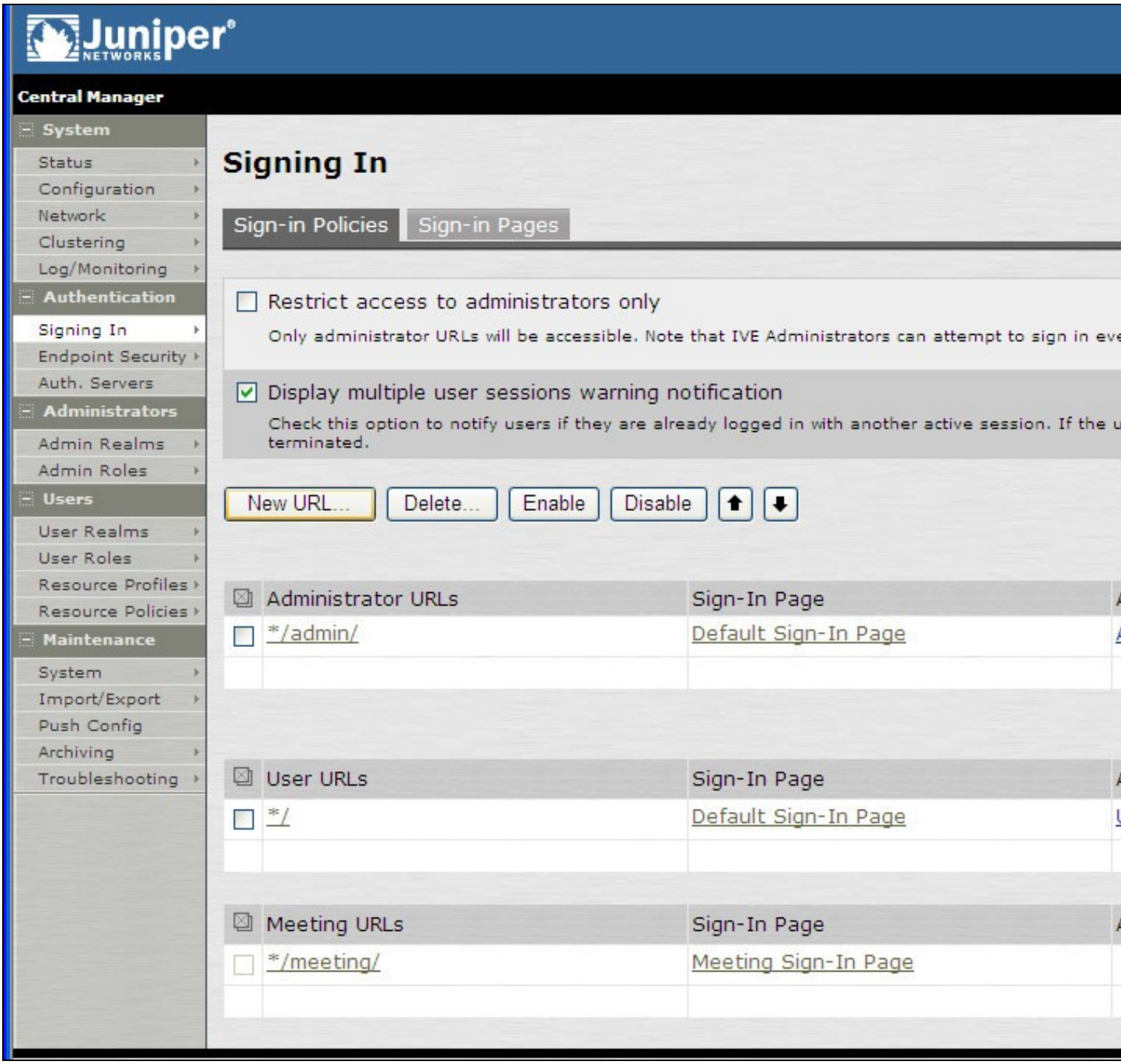

Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USER>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails



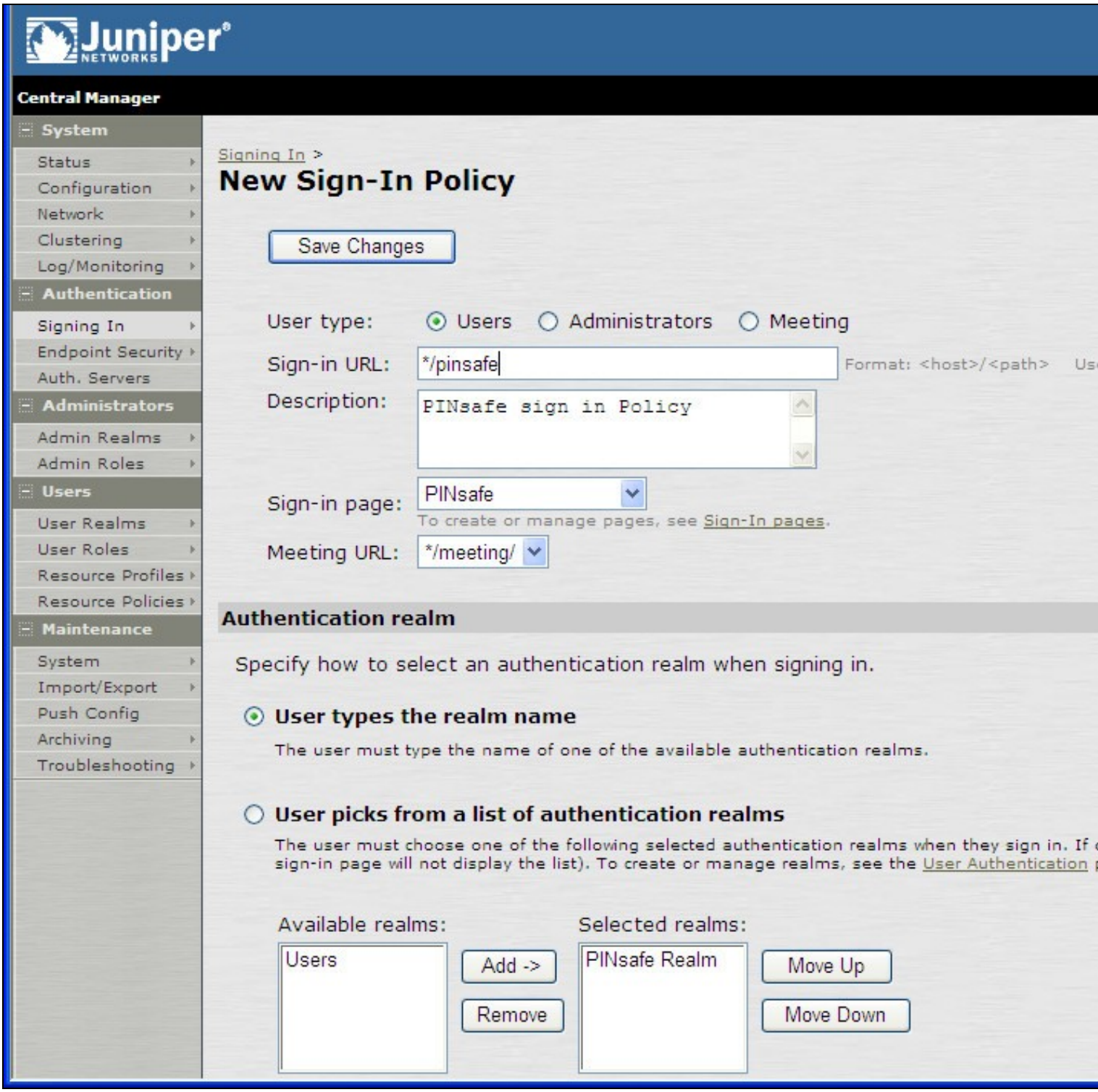
356.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.



Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.



When complete the new Swivel policy should be listed.


Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
Restrict access to administrators only
Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve
Display multiple user sessions warning notification
Check this option to notify users if they are already logged in with another active session. If the u
terminated.
New URL...
Delete...
Enable
Disable
Administrator URLs
Sign-In Page
*/admin/
Default Sign-In Page
User URLs
Sign-In Page
*/
Default Sign-In Page
*/pinsafe/
PINsafe
Meeting URLs
Sign-In Page
*/meeting/
Meeting Sign-In Page

357 Additional Installation Options

Swivel can provide additional authentication options including:

Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

357.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

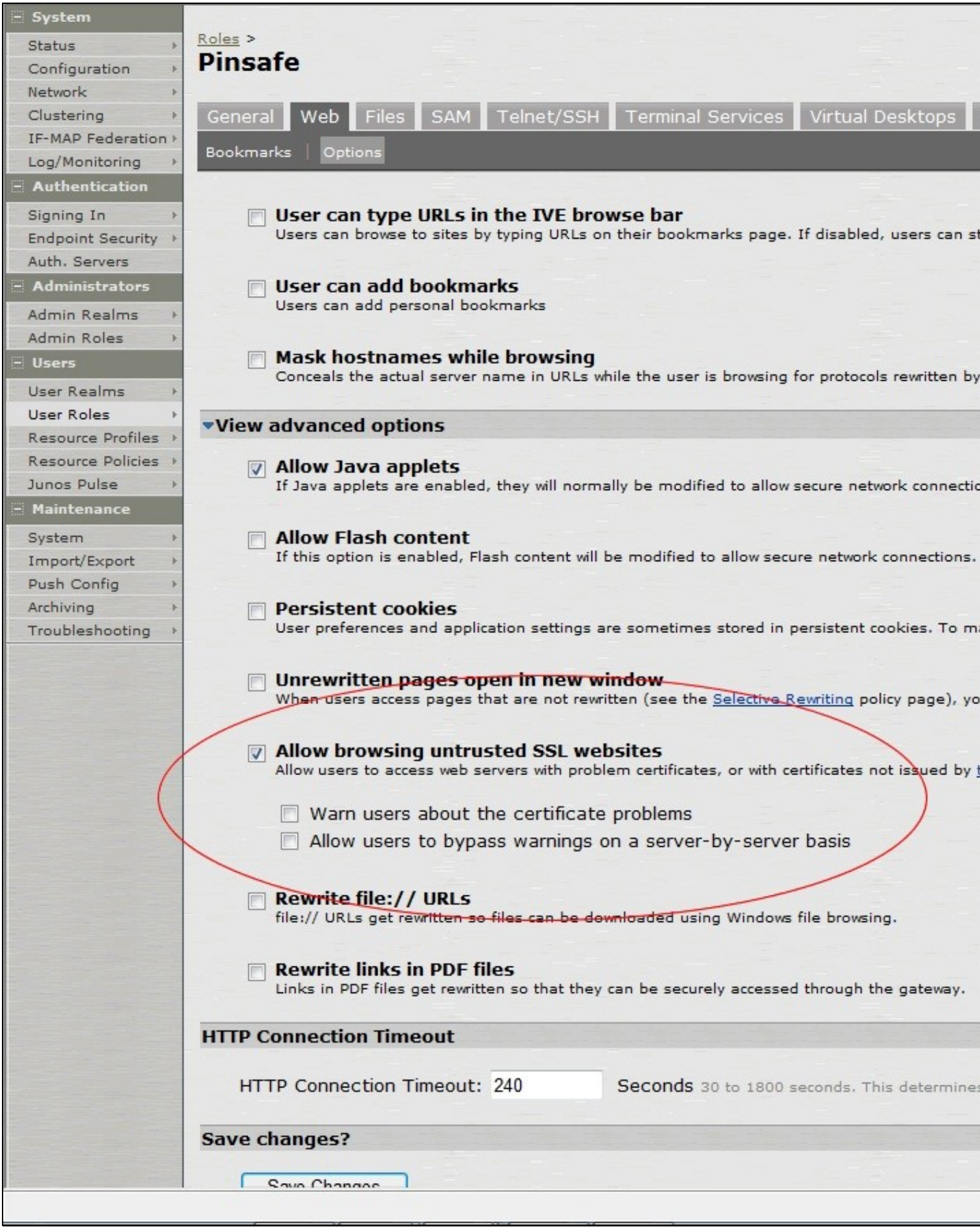
Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

357.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.


System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
Pinsafe
General
Web
Files
SAM
Telnet/SSH
Terminal Services
Virtual Desktops
Bookmarks
Options
User can type URLs in the IVE browse bar
Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can st
User can add bookmarks
Users can add personal bookmarks
Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
View advanced options
Allow Java applets
If Java applets are enabled, they will normally be modified to allow secure network connectio
Allow Flash content
If this option is enabled, Flash content will be modified to allow secure network connections.
Persistent cookies
User preferences and application settings are sometimes stored in persistent cookies. To ma
Unrewritten pages open in new window
When users access pages that are not rewritten (see the Selective Rewriting policy page), yo
Allow browsing untrusted SSL websites
Allow users to access web servers with problem certificates, or with certificates not issued by
Warn users about the certificate problems
Allow users to bypass warnings on a server-by-server basis
Rewrite file:// URLs
file:// URLs get rewritten so files can be downloaded using Windows file browsing.
Rewrite links in PDF files
Links in PDF files get rewritten so that they can be securely accessed through the gateway.
HTTP Connection Timeout
HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determines
Save changes?
Save Changes

357.1.2 Creating an ACL for the Virtual hostname role

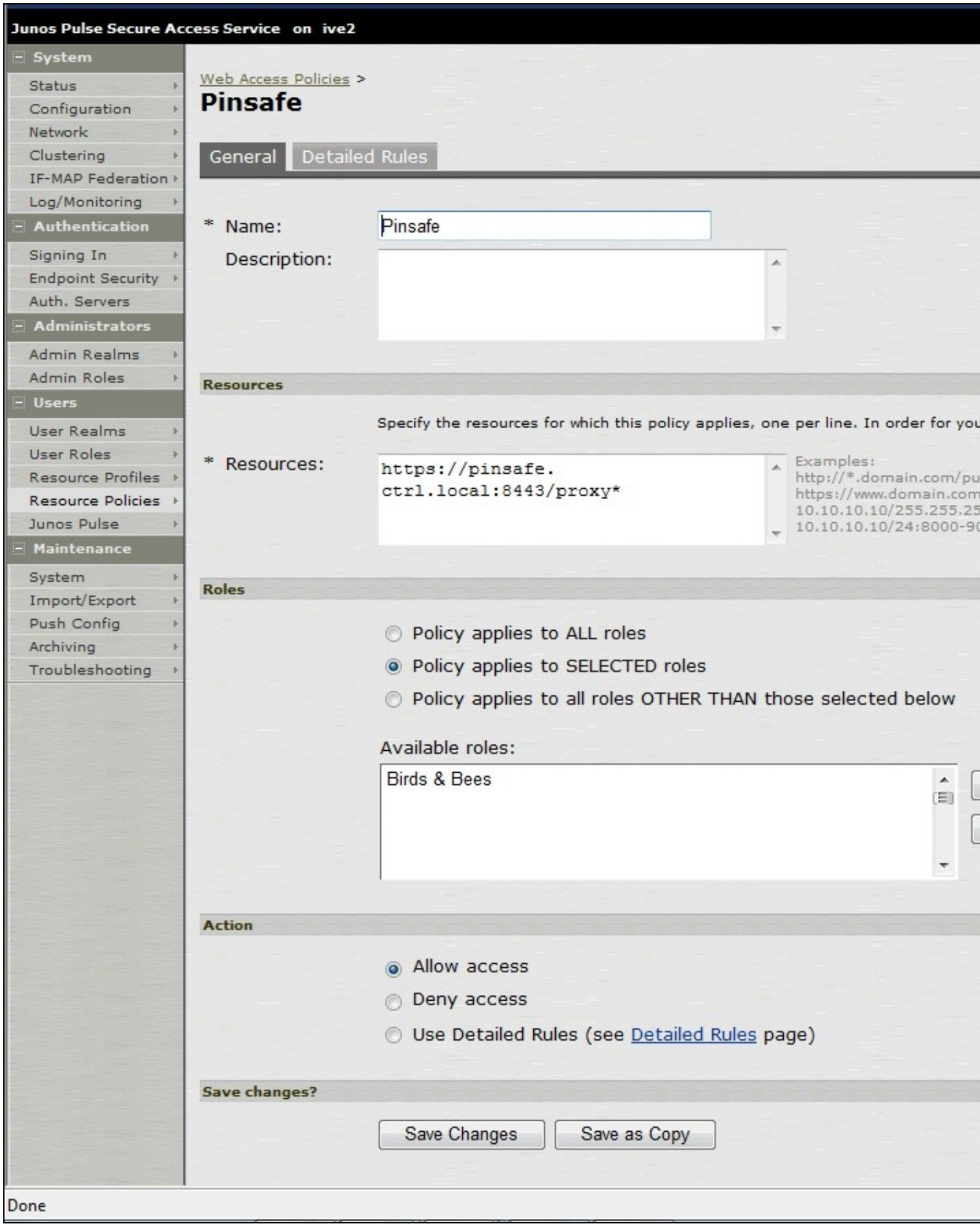
An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.


Junos Pulse Secure Access Service on ive2
System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Web Access Policies >
Pinsafe
General
Detailed Rules
* Name:
Pinsafe
Description:
Resources
Specify the resources for which this policy applies, one per line. In order for you
* Resources:
https://pinsafe.
ctrl.local:8443/proxy*
Examples:
http://*.domain.com/pu
https://www.domain.com
10.10.10.10/255.255.25
10.10.10.10/24:8000-90
Roles
Policy applies to ALL roles
Policy applies to SELECTED roles
Policy applies to all roles OTHER THAN those selected below
Available roles:
Birds & Bees
Action
Allow access
Deny access
Use Detailed Rules (see Detailed Rules page)
Save changes?
Save Changes
Save as Copy
Done

357.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New URL. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

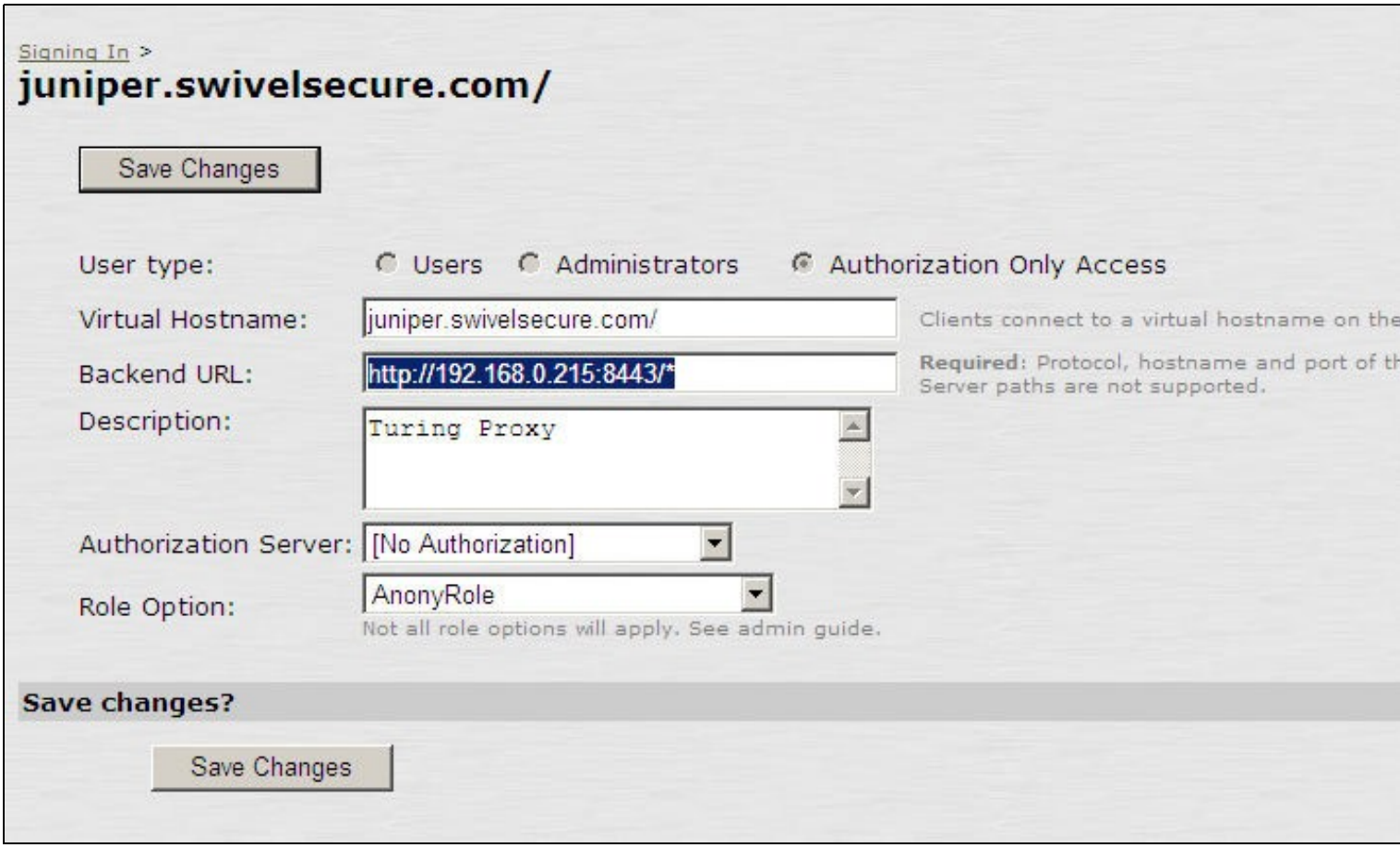
Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

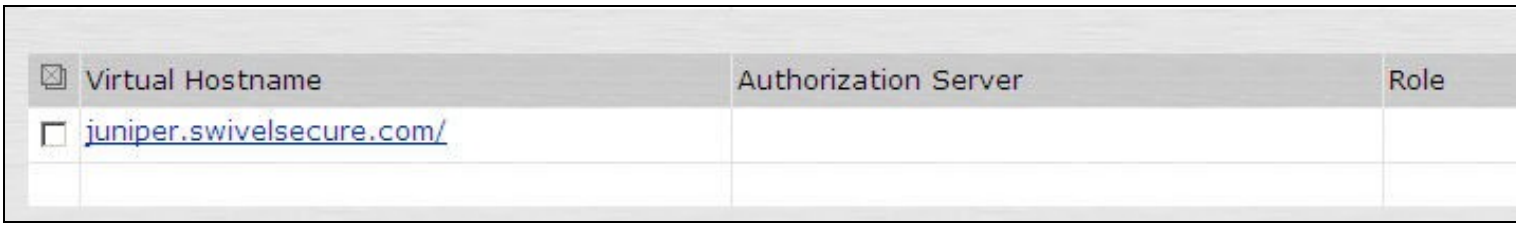
For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes





357.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

https://<turing.mycompany.com>/proxy/SCImage?username=test

Software Install

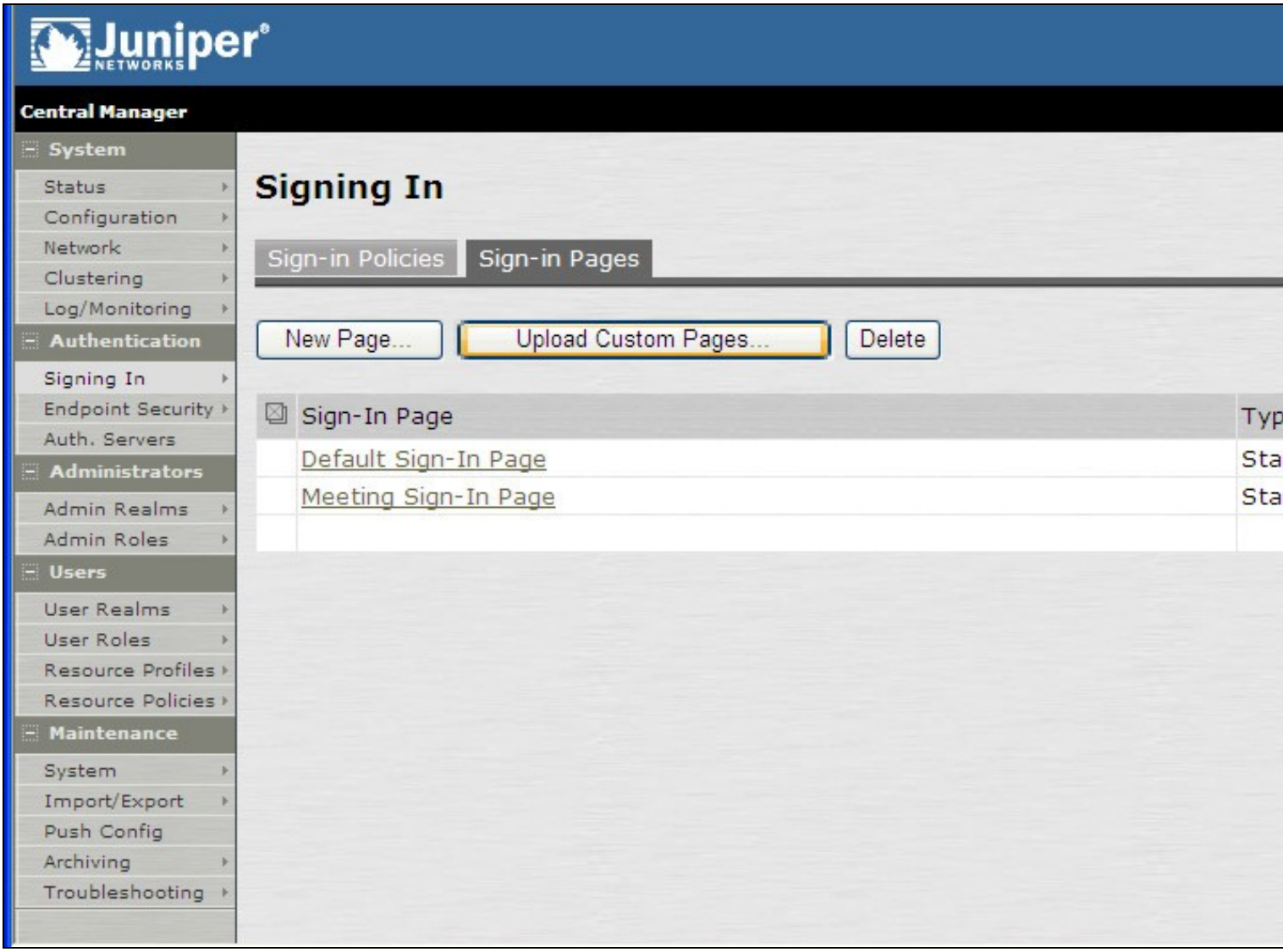
For a software only install see Software Only Installation

Then verify the external access using

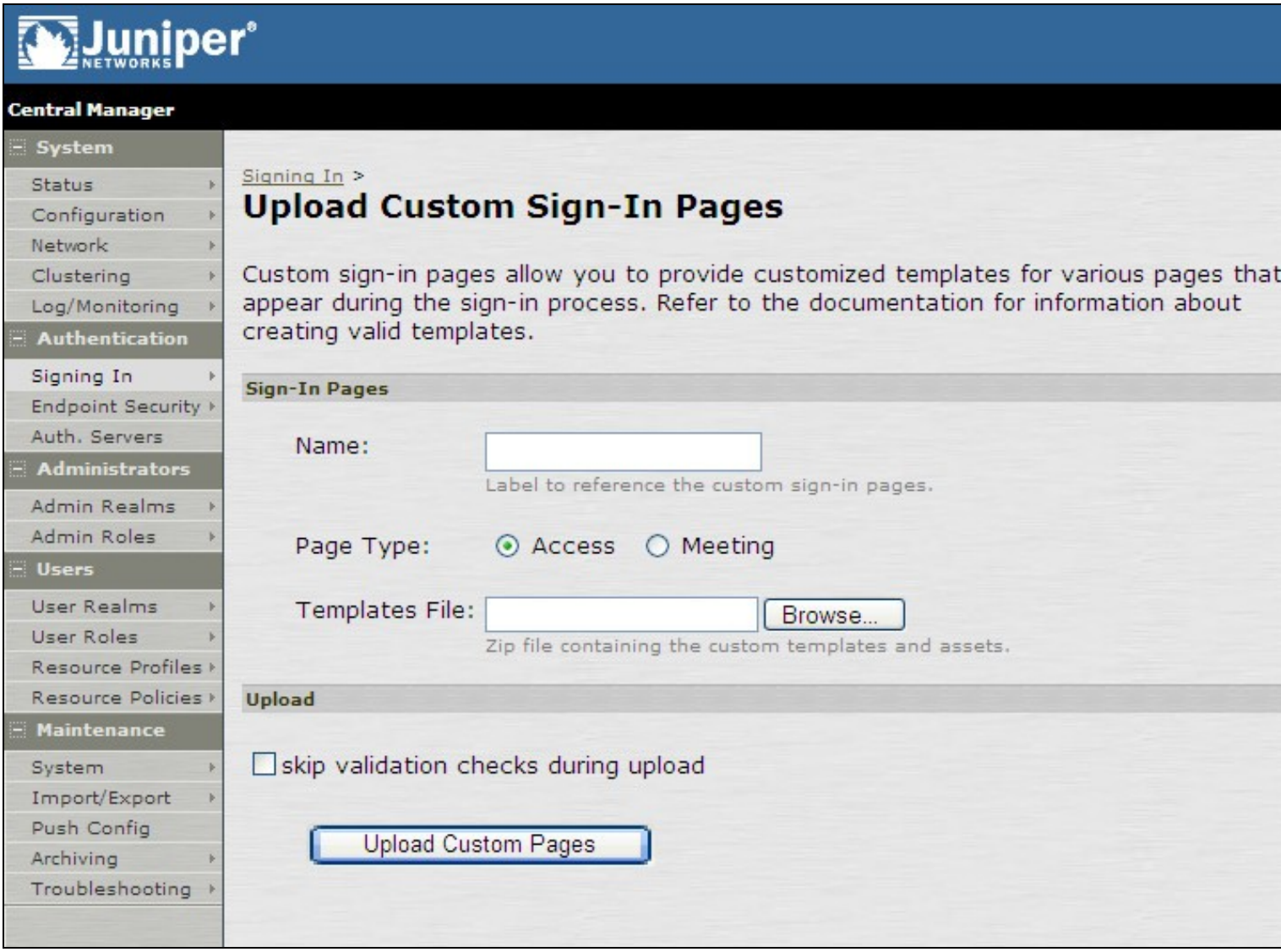
https://<turing.mycompany.com>/pinsafe/SCImage?username=test

357.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.



Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.



Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within **LoginPage.thtml** should be edited to suit your environment as the below modifications.

If you are using the combined PC and tablet version, you should make these changes to swivel-header.thtml.

357.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/SCImage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/SCImage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

357.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

357.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/DCMessage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/DCMessage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

357.2.4 Modifying the login button text

The login page button and link to *Get Another Image* may be modified.

To modify the login button text locate the text *value='Turing'* and replace the Turing with the required text.

To modify the *Get another image?* URL, locate the two instances of *Get another image?* and change the text as required.

357.2.5 Modifying the login for PINpad

Customising for Pinpad can be done using the same custom pages as above. Follow the same instructions as above, except the following:

- The zip file contains 3 additional images that need to go into the *imgs* folder of the Juniper custom login.
- **OTC_OPTION** needs to be set to **"pinpad"**.
- You need to set the value for *PinpadImage*, rather than *TURingImage* to match your own Swivel instance.

Example

```
var PinpadImage = "https://hostname:8443/pinsafe/SCImage?username=";
```

to

```
var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";
```

357.2.6 Modifying the Login pages for Mobile Devices

The prerequisites section contains the mobile modified pages that can be uploaded with any other modified pages to ad wivel authentication to the login.

Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above.

var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

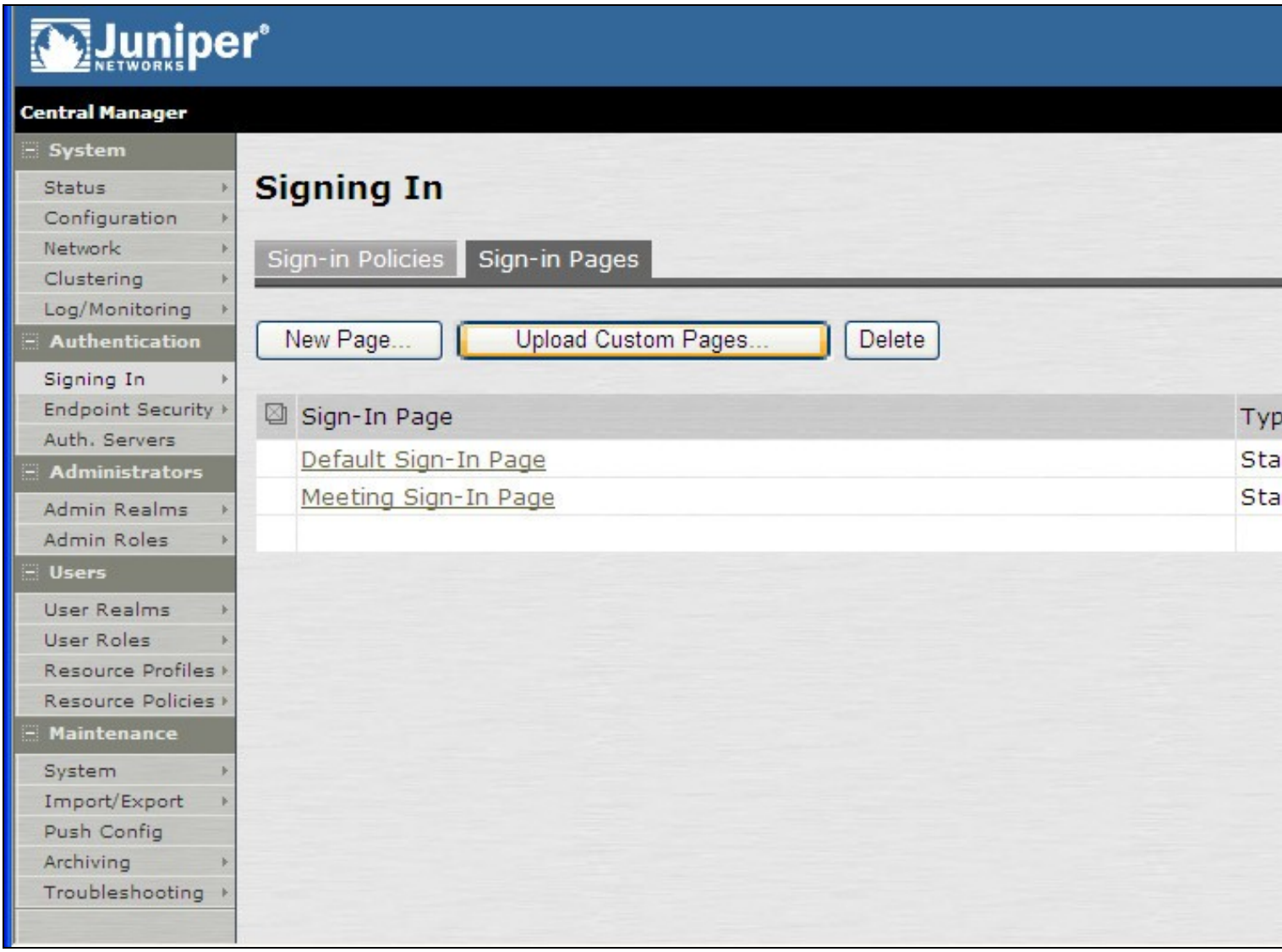
357.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

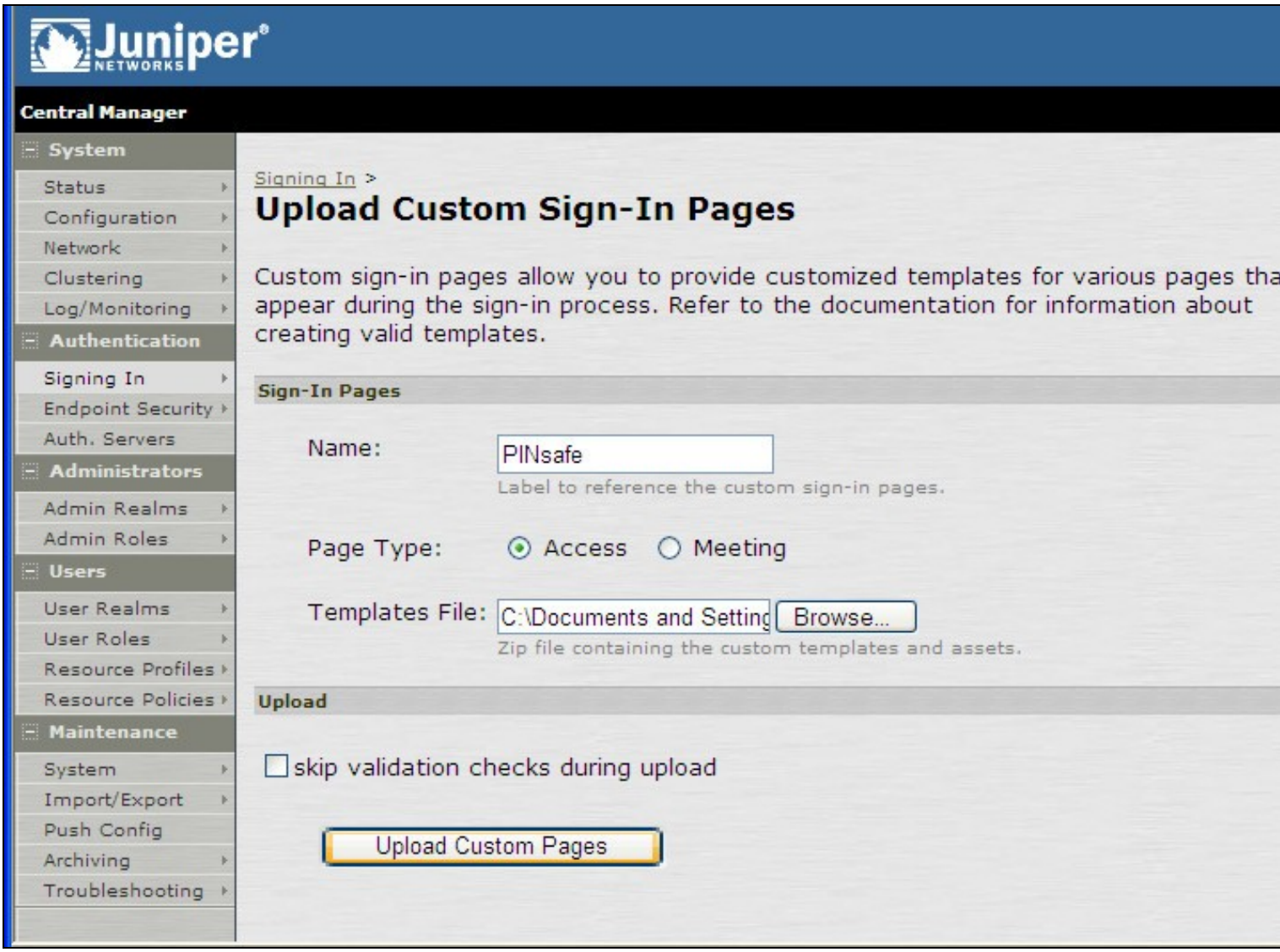
Juniper Network Connect with TURing

357.2.8 Uploading the Modified Page

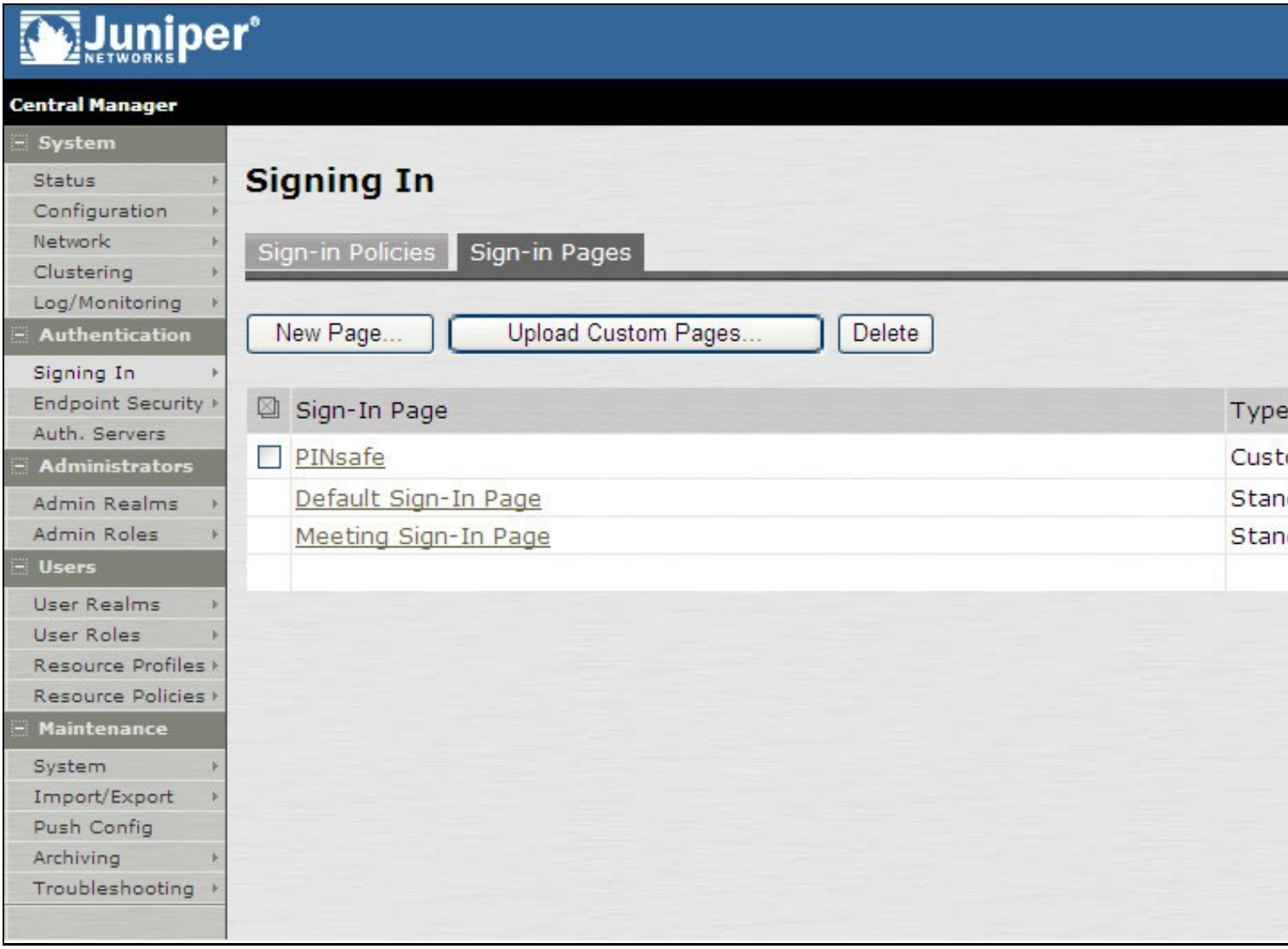
Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.



Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.



The new signing in page should be listed.

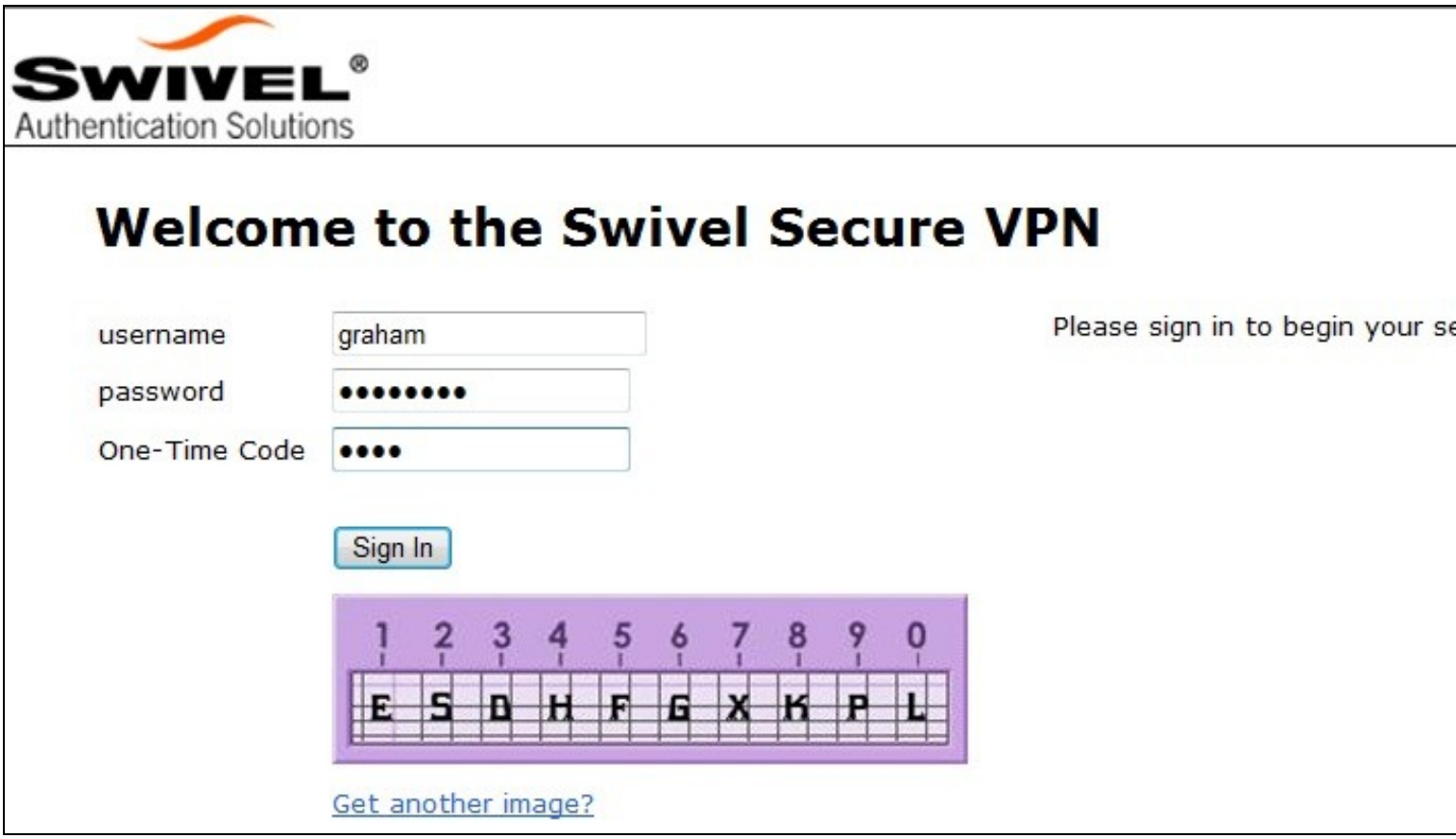

Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
New Page...
Upload Custom Pages...
Delete
Sign-In Page
Type
PINsafe
Default Sign-In Page
Meeting Sign-In Page

358 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

Dual Channel Authentication

Single Channel Authentication



359 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

360 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Internal Certificate Authorities

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username. When USERNAME is used then just the username is sent to the Juniper.

361 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

361.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

```
<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si
```

A modified login page is available here: iPad modified login page

361.2 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

362 Additional Information

Custom sign-in pages for Pinpad can be found here.

363 Juniper Two Stage Challenge and Response

363.1 Juniper Two Stage and Challenge and Response Authentication

363.2 Introduction

Juniper supports the use of a challenge and response whereby a password is used prior to entering a One Time Code. In addition the Challenge and Response mechanism allows an SMS to be sent upon successful entry of a password.

363.3 Prerequisites

PINsafe 3.7

Juniper 6.x

Dual Channel authentication

Two stage authentication requires the use of either a PINsafe password, or that Check password with repository is enabled.

363.4 Baseline

PINsafe 3.7

Juniper 6.4

363.5 Architecture

Juniper using RADIUS authentication to the PINsafe server, with security strings sent to the user using an SMS gateway.

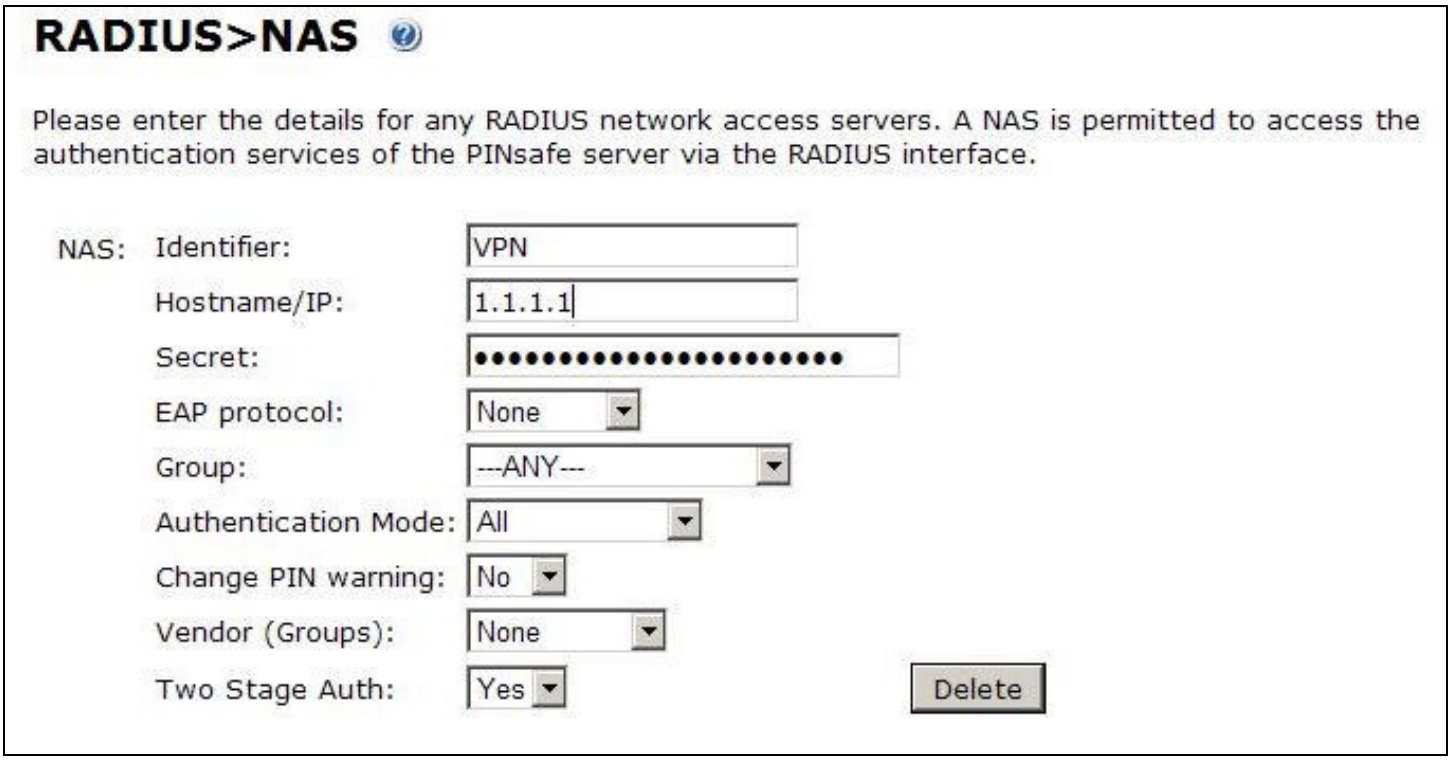
363.6 Installation

Configure the PINsafe server and Juniper appliance for Dual Channel Authentication. Ensure either the user has a PINsafe password, or that Check password with repository is enabled.

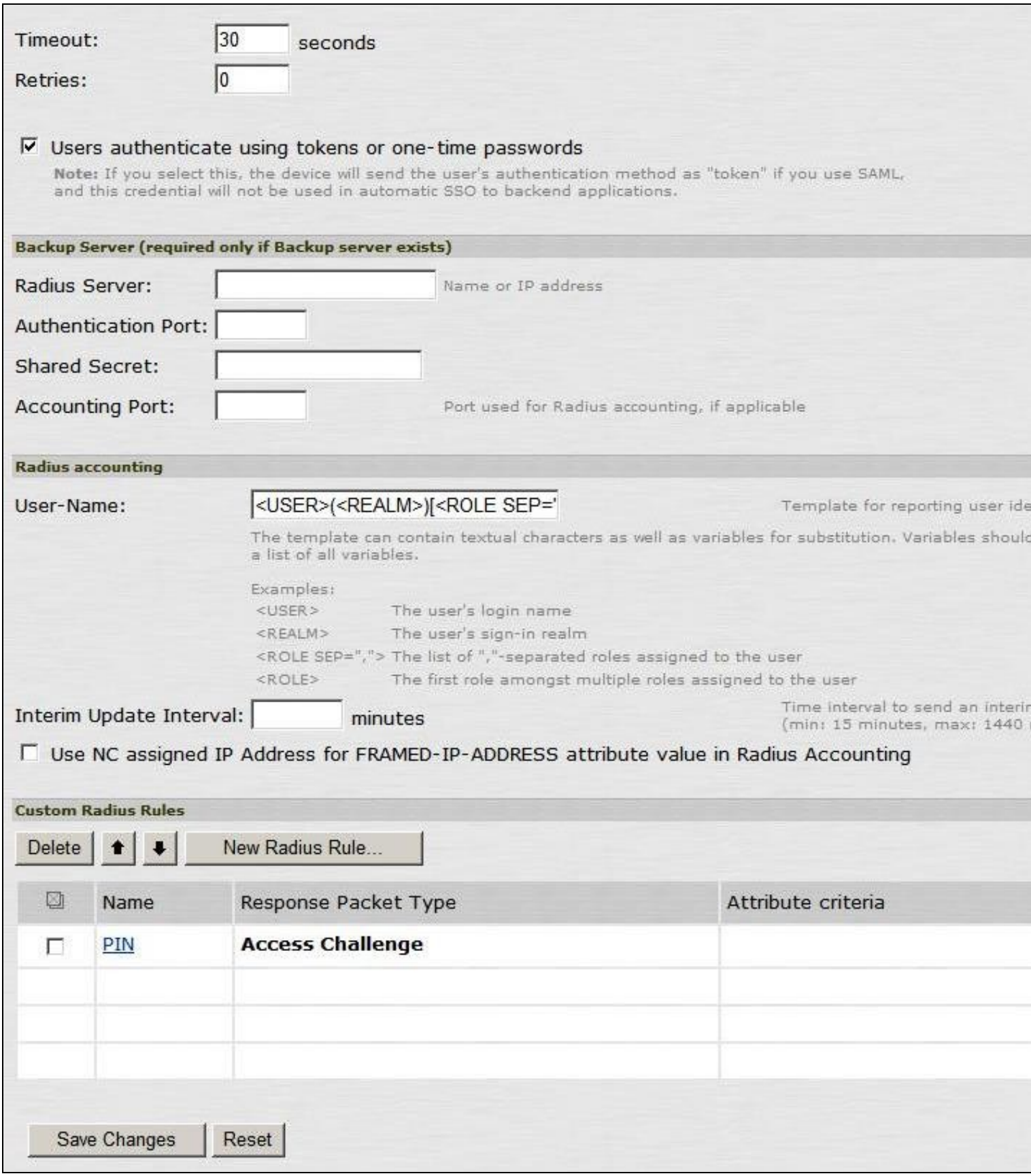
363.7 Adding Two Stage Authentication

See also: Two Stage Authentication How to Guide

On the PINsafe Administration Console server select RADIUS/NAS and the Access device which two stage authentication is required. Set the Two stage Auth to Yes and Apply.



On the Juniper Administration Console, browse to the Authentication/Auth Servers menu, and select the PINsafe RADIUS authentication server. Under Custom RADIUS Rules click on the New RADIUS Rule button.

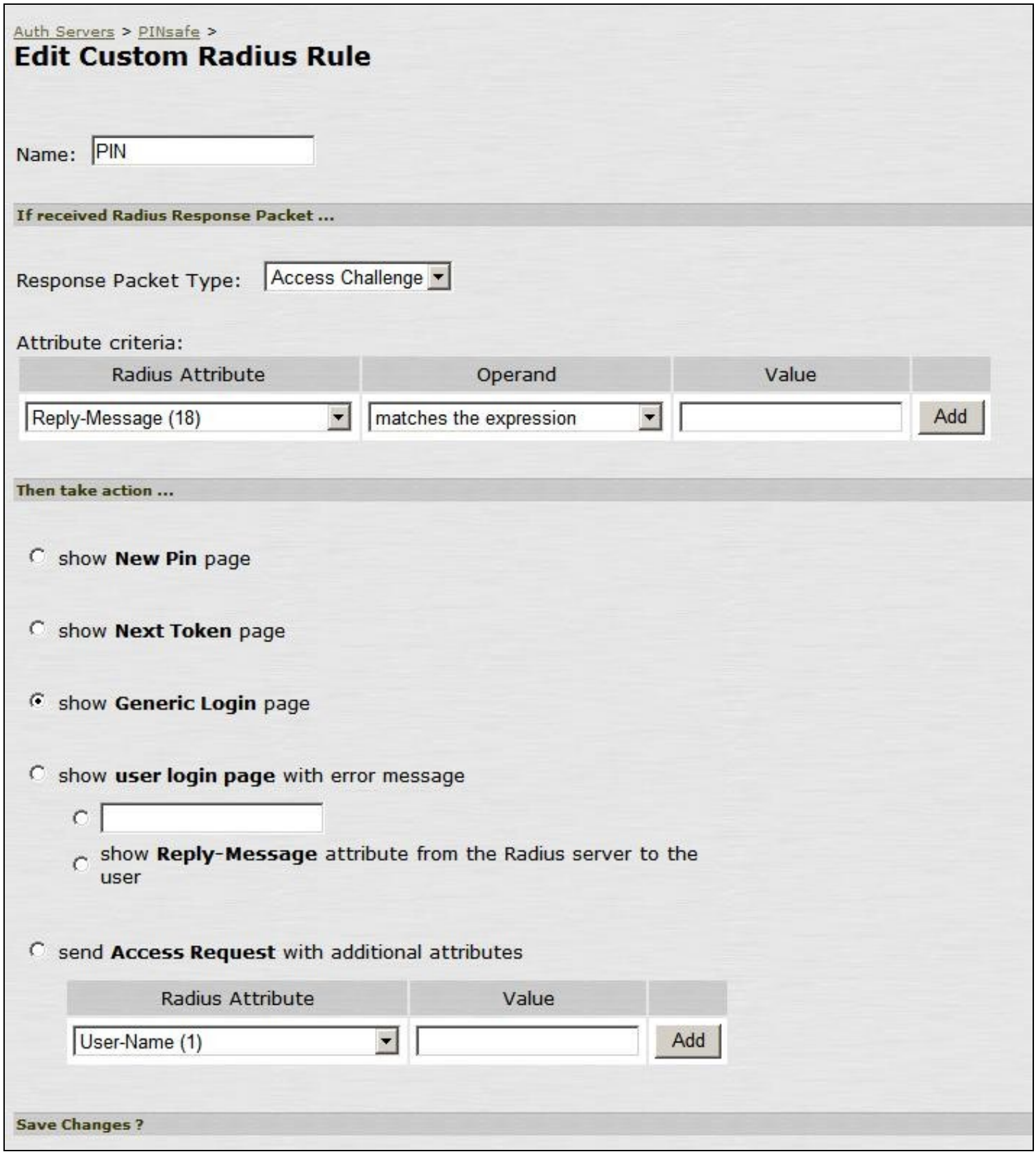


Enter a name for the Rule and ensure Response Packet Type is set to Access Challenge.

Under Attribute Criteria ensure RADIUS Attribute is set to Reply Message (18), with the Operand matches the expression, leave the value setting blank.

Ensure that the radio button for ?Show Generic Login Page? is selected.

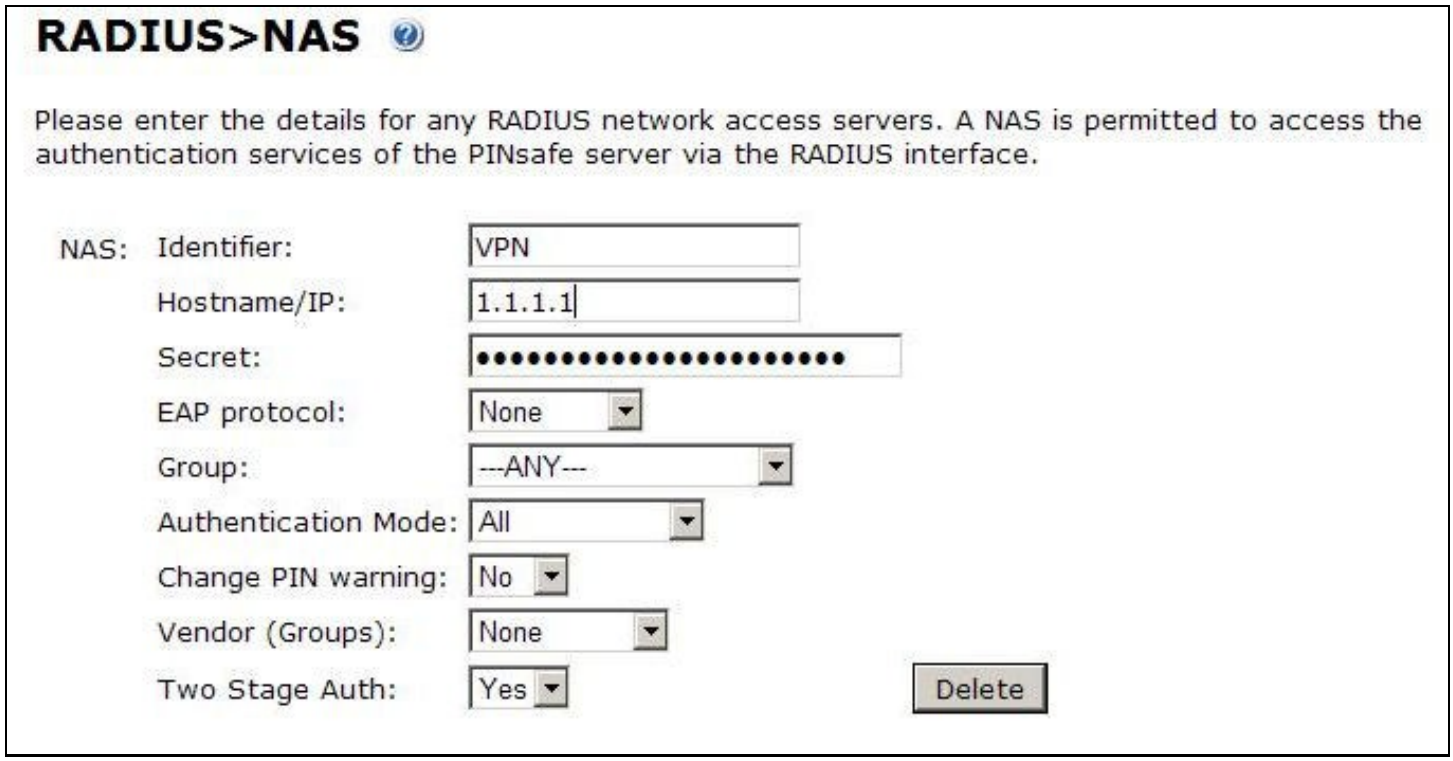
Click on Save Changes.



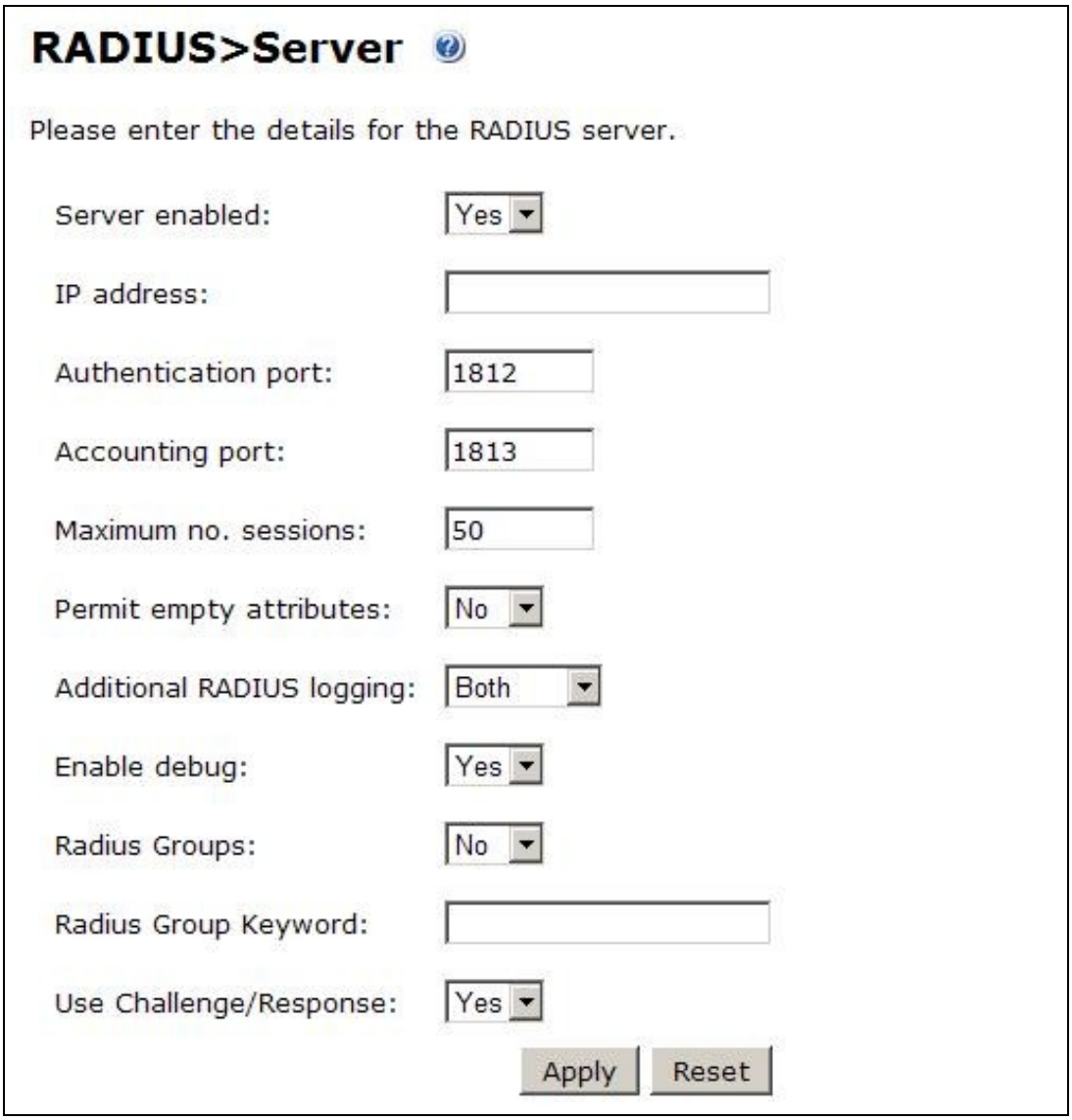
363.8 Adding Challenge and response Authentication

See also: Challenge and Response How to Guide

For PINsafe 3.7 and later, on the PINsafe Administration Console server select RADIUS/NAS and ensure the Two Stage Auth is set to Yes, then click on Apply.



For PINsafe 3.6 and earlier, on the PINsafe Administration Console server select RADIUS/Server and ensure the Use Challenge/Response is set to Yes, then click on Apply.



On the PINsafe Administration Console server select Server/Dual Channel. For delivery of a new security string upon entering a correct password, ensure On-Demand Authentication is set to Yes, then click on Apply.

363.9 Combining Juniper and PINsafe Two Stage Authentication

Using the Juniper AD authentication is useful for single Sign On (SSO) features, so it may be of use to combine the Juniper Two Stage login with that of the PINsafe Two Stage authentication in order to send the user a security string or OTC when the AD password is entered. To configure this:

Enable Two Stage Authentication on the Juniper

Enable two Stage Authentication on the PINsafe Administration Console

Enable Check Password with Repository on the PINsafe Administration Console, See Check Password With Repository

On the Juniper select the User Realm relating to the required Authentication Realm and change the **set Password is:** to the value **Predefined as <PASSWORD>**

When an authentication is made, the AD password is used for the Juniper and the PINsafe Two Stage Authentication so it does not need to be entered twice.

363.10 Verifying the Installation

Check the PINsafe logs

Check the Juniper logs

363.11 Troubleshooting

View the users security string to ensure the correct security string is being used.

Ensure authentication is working with standard authentication.

363.12 Known Issues and Limitations

PINsafe 3.7 Beta required the use of Multiple Authentications per string to be enabled for dual/single channel located on the PINsafe Administration console under Server/Single Channel or Server/Dual Channel.

363.13 Additional Information

Juniper can also be configured for Constrained Delegation where a PINsafe One Time Code is entered and this signs the user into their AD applications without the use of an AD password in the login process. See the following documentation: http://www.juniper.net/techpubs/software/ive/6.x/6.4/

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

364 Microsoft Direct Access Integration

365 Introduction

Microsoft Direct Access allows a VPN connection to be brought up when a user requires access to an organisations internal resources. PINsafe can authenticate a user accessing those internal resources using Dual channel authentication such as SMS, Mobile Phone Client and the Taskbar utility Taskbar How to Guide and Token.

366 Prerequisites

Microsoft Direct Access fully configured

Microsoft CA server for OTP authentication

PINsafe 3.x

367 Baseline

Microsoft UAG SP1 with Direct access configured

PINsafe 3.8

368 Architecture

When a Direct Access connection is made, a pop up appears for the user prompting them to enter their One Time Code. This is then checked by the UAG against PINsafe using RADIUS authentication.

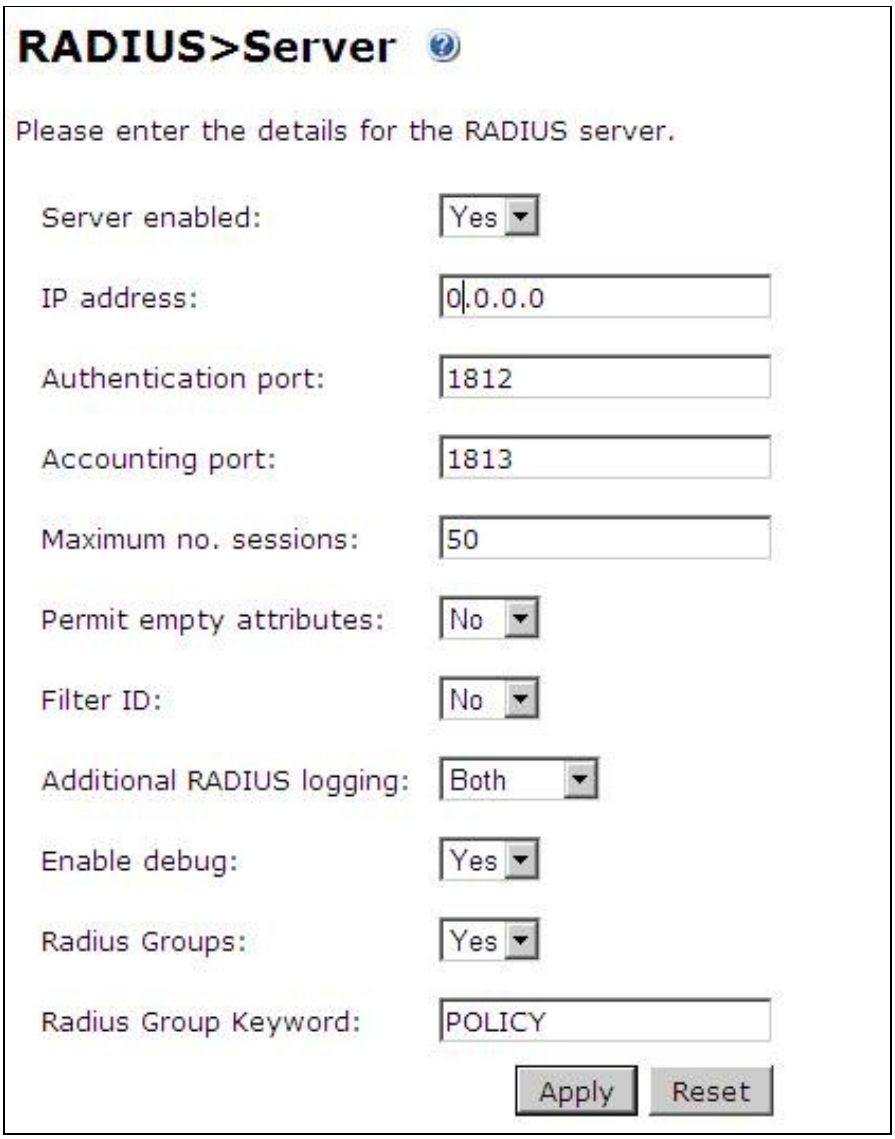
369 Installation

369.1 PINsafe Configuration

369.1.1 Configuring the RADIUS server

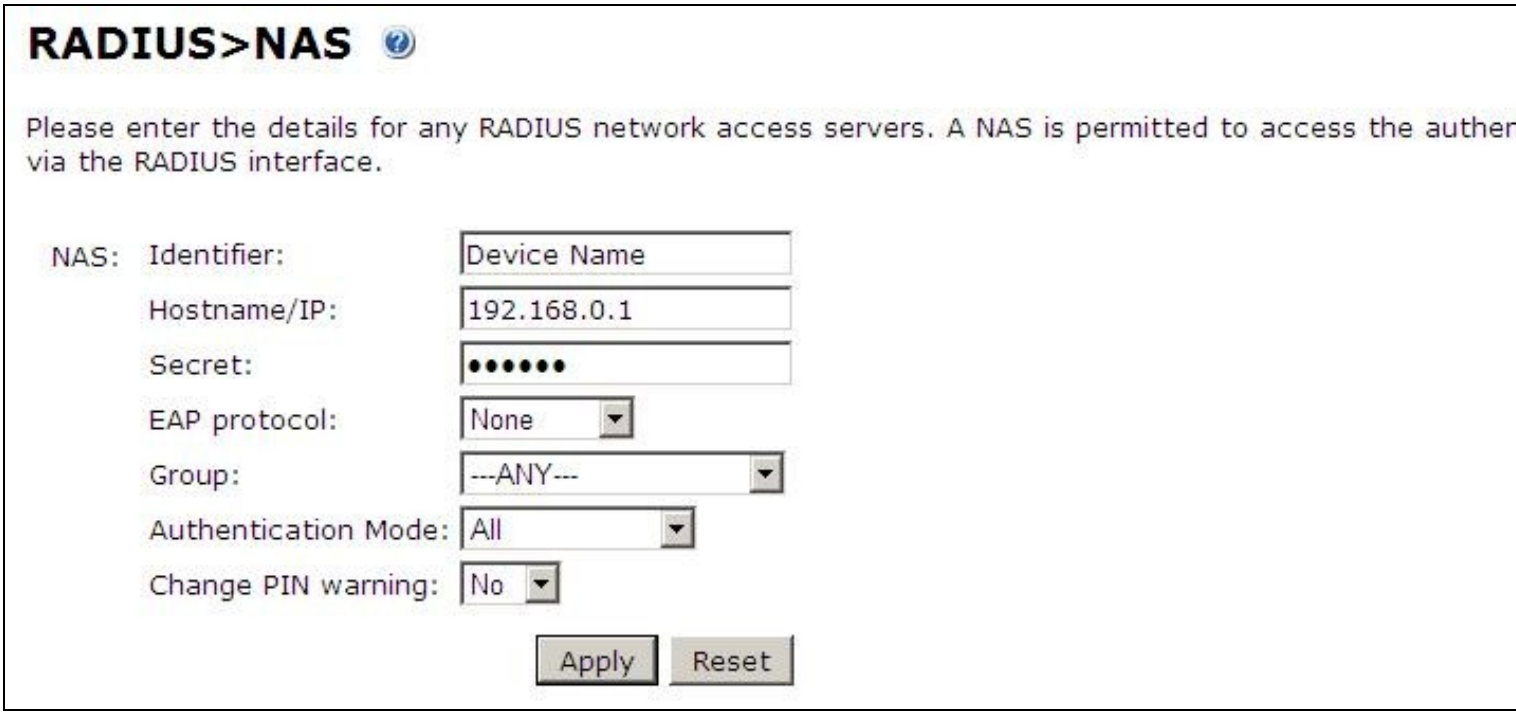
Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

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



369.1.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe 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 PINsafe server and VPN RADIUS configuration.



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

369.1.3 Enabling Session creation with username

PINsafe can be configured to use the Taskbar to present a TURing image to users when prompted for authentication by Direct Access. See Taskbar How to Guide

To allow Single Channel authentication on PINsafe follow the below steps.

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 PINsafe username:

Appliance

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

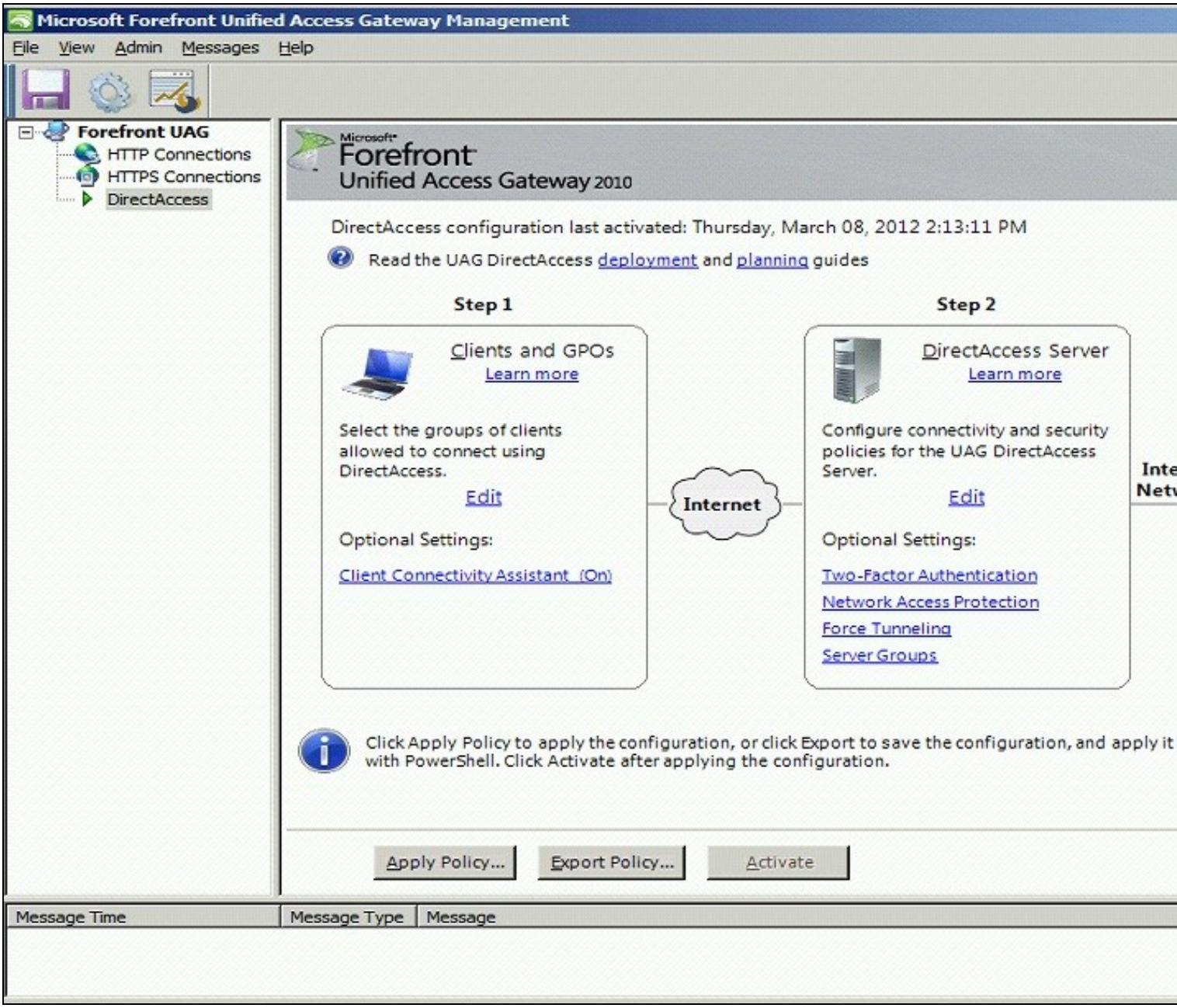
For a software only install see Software Only Installation

369.2 Microsoft Direct Access Integration

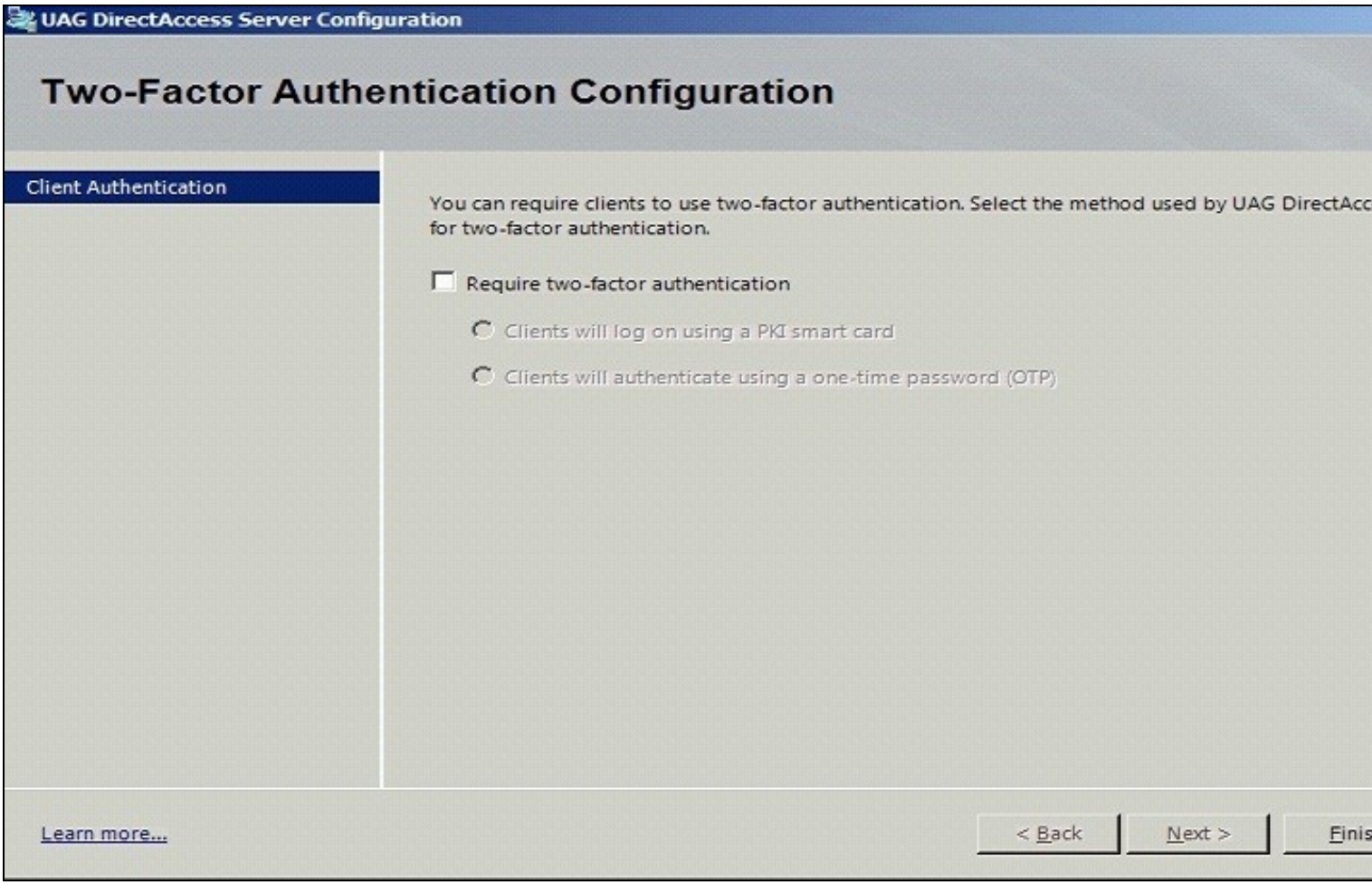
Ensure that the Microsoft Direct Access is fully working and tested before startigng the PINsafe integration.

369.2.1 Enable Two Factor Authentication

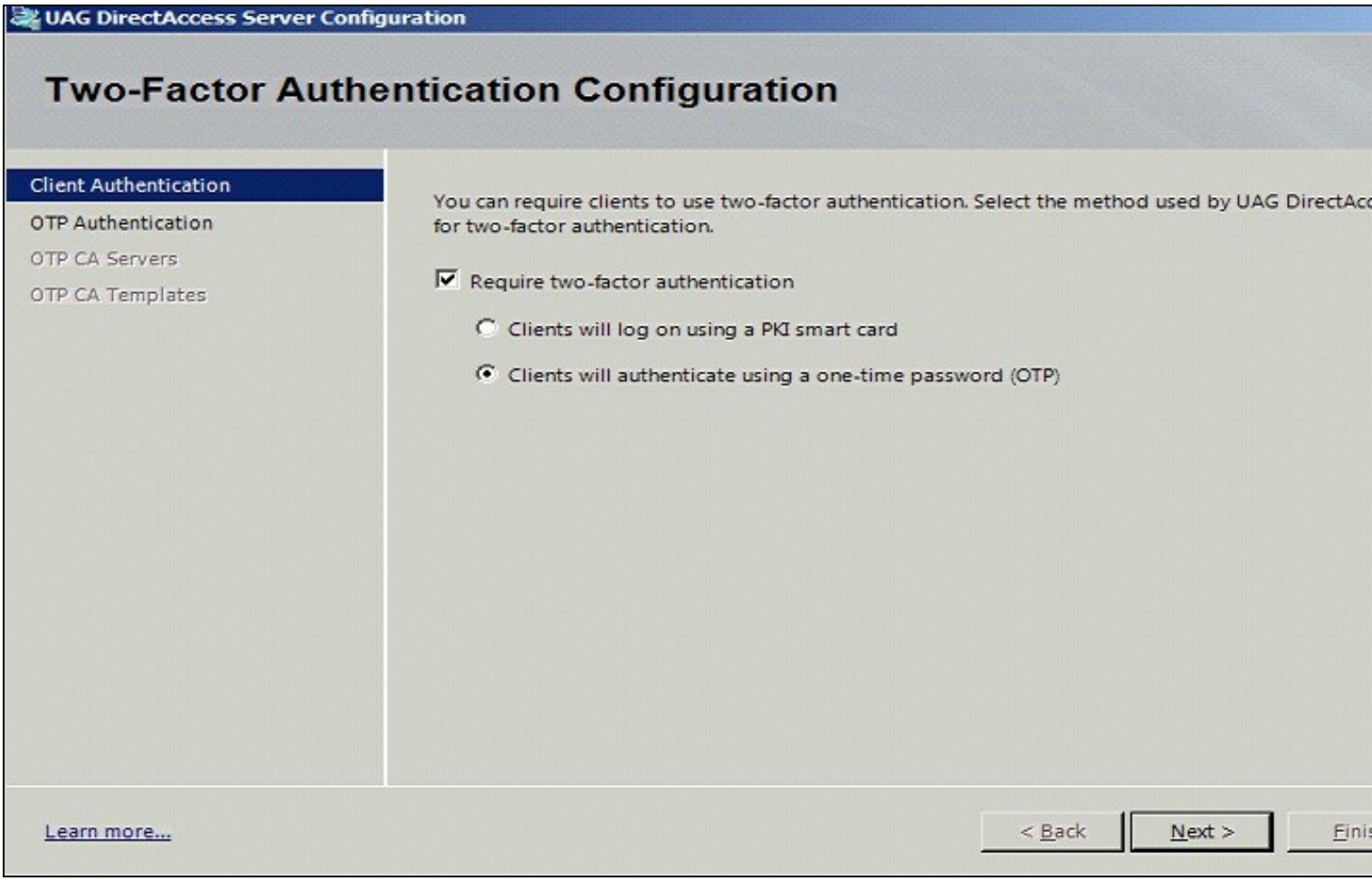
On the Forefront UAG Direct Access configuration page select under Step 2 Optional Settings the link for *Two-Factor Authentication*



Click on *Require two-factor authentication*

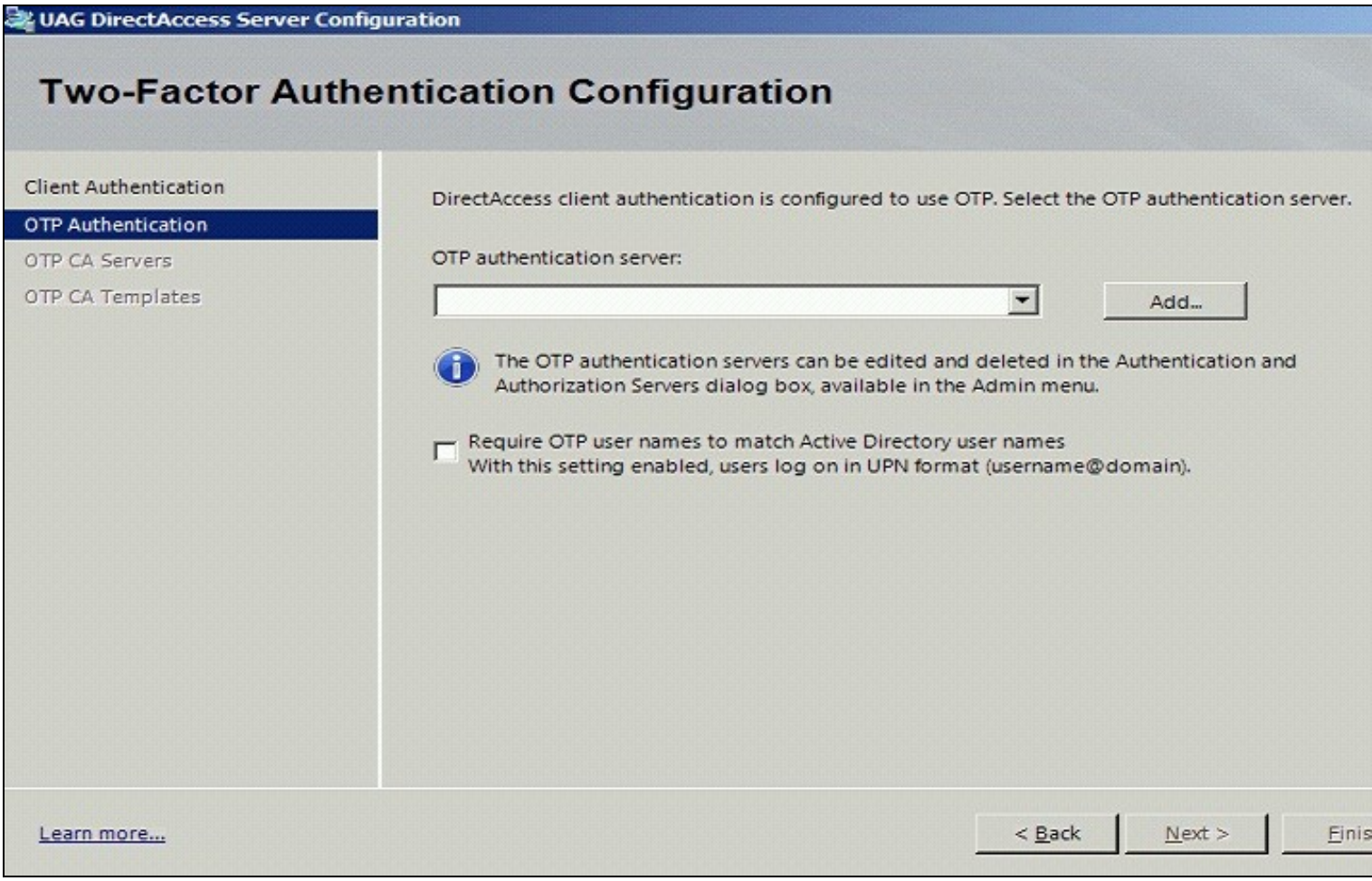


Click on *Clients will authenticate using a one-time password (OTP)*



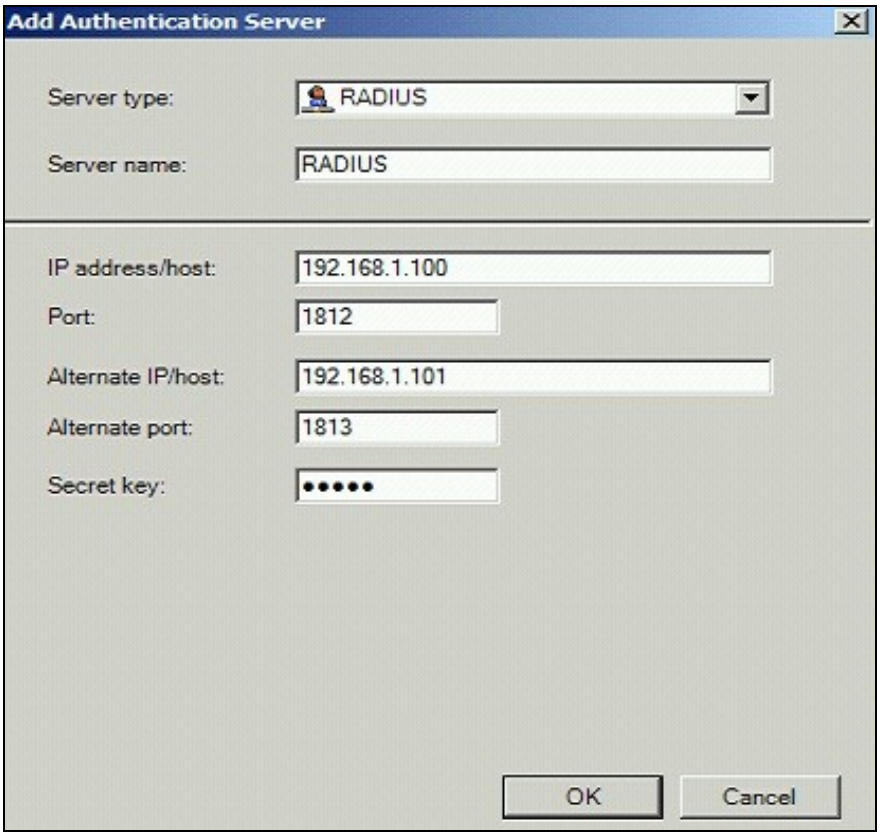
369.2.2 Configure OTP Authentication Server

On the OTP Authentication tab click Add

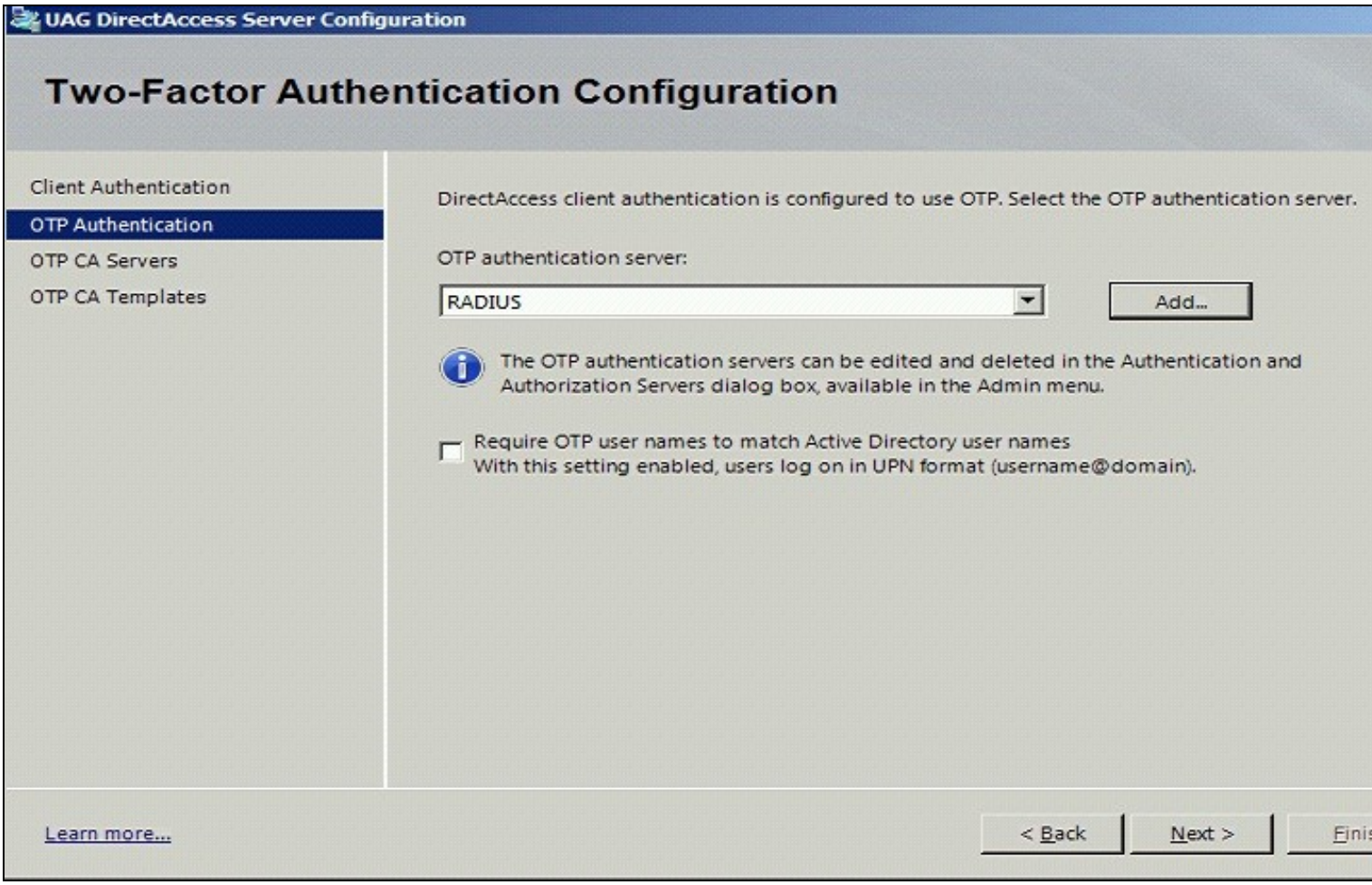


Select Server Type RADIUS and enter the following information:

- Server Name: A descriptive name for the RADIUS server
- Port: RADIUS port used by the Swivel server, usually 1812
- IP address/host: The Swivel RADIUS server
- Alternate IP/host: A secondary Swivel RADIUS server
- Alternate port: The port used by the secondary Swivel server, usually 1812
- Secret Key: A shared secret entered on the Swivel servers.

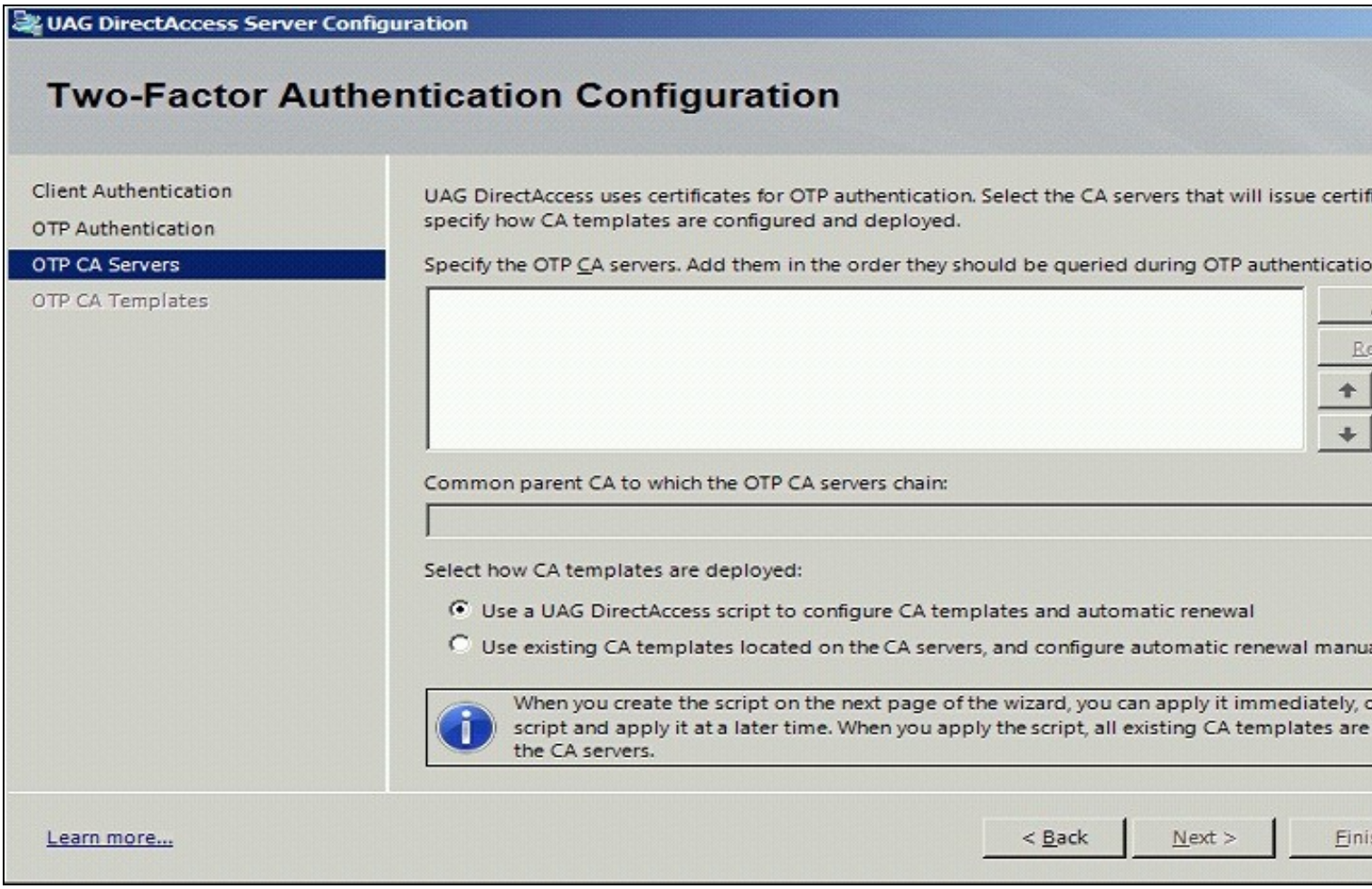


Ensure that the new Swivel server is selected. Optionally select *Require OTP user names to match Active Directory user names with this setting enabled, users log on in UPN format (username@domain).* then the user name will be automatically populated at the direct access login.

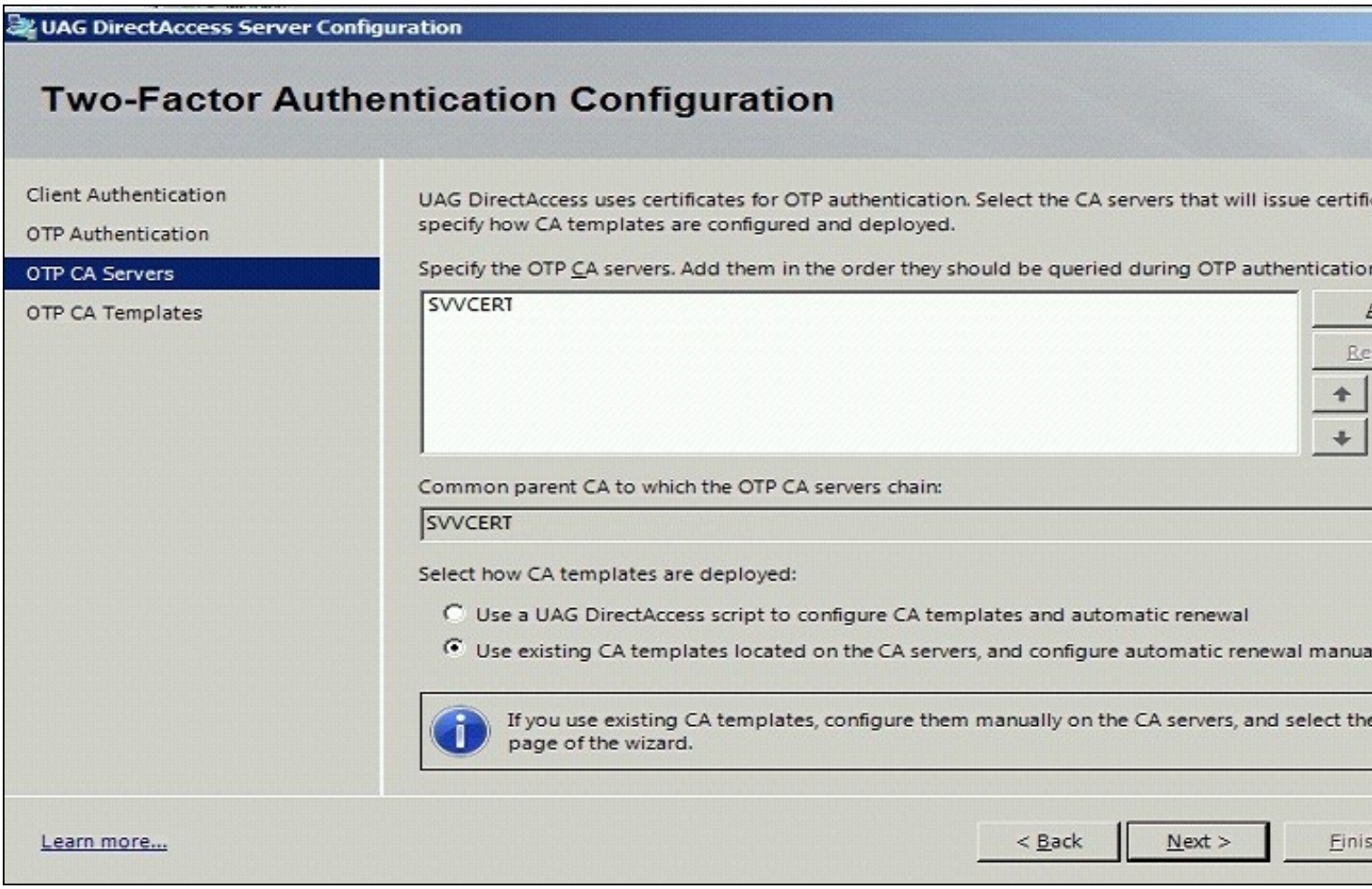


369.2.3 CA Server Configuration

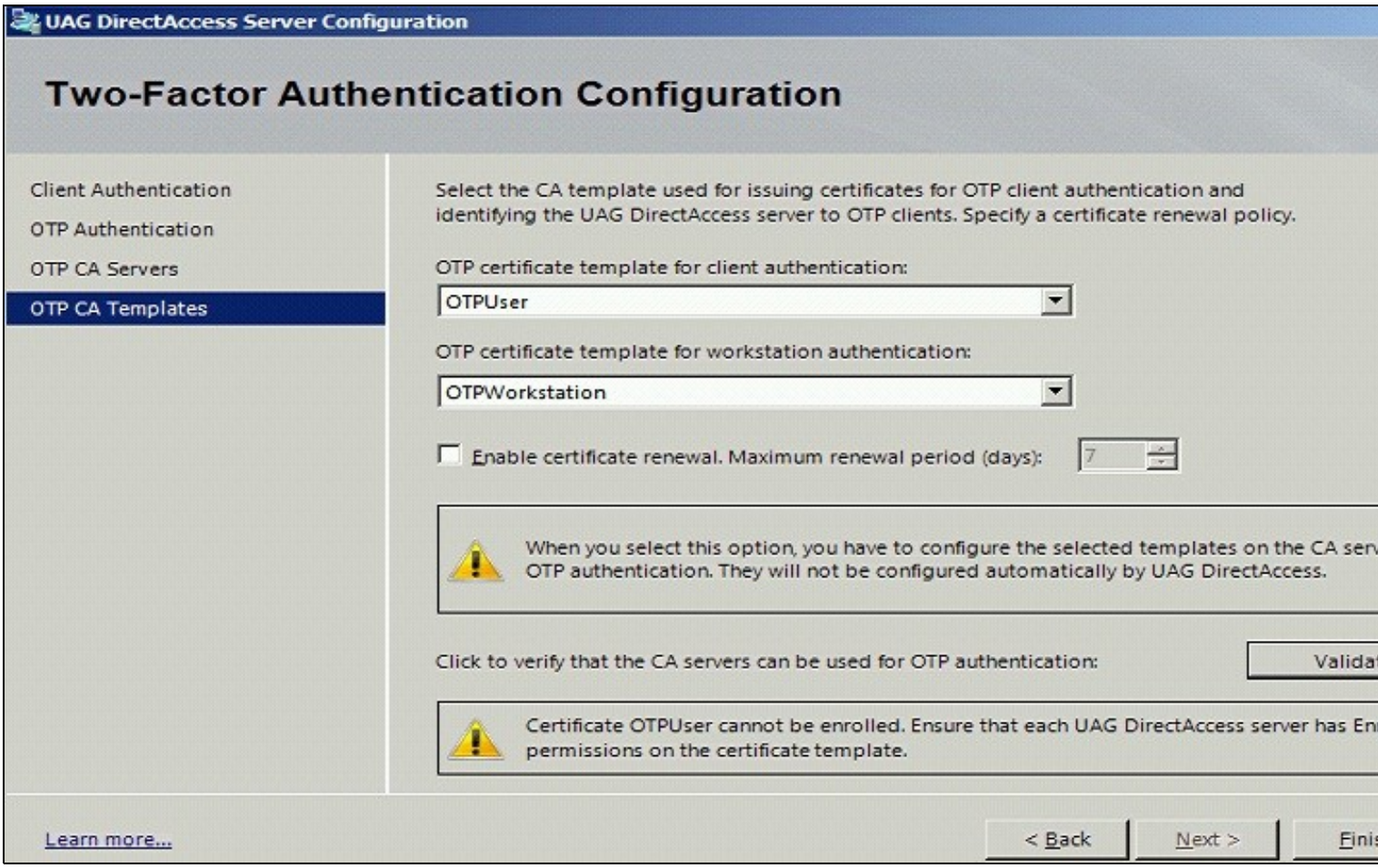
Under OTP CA Servers click on Add and select the OTP CA Server.



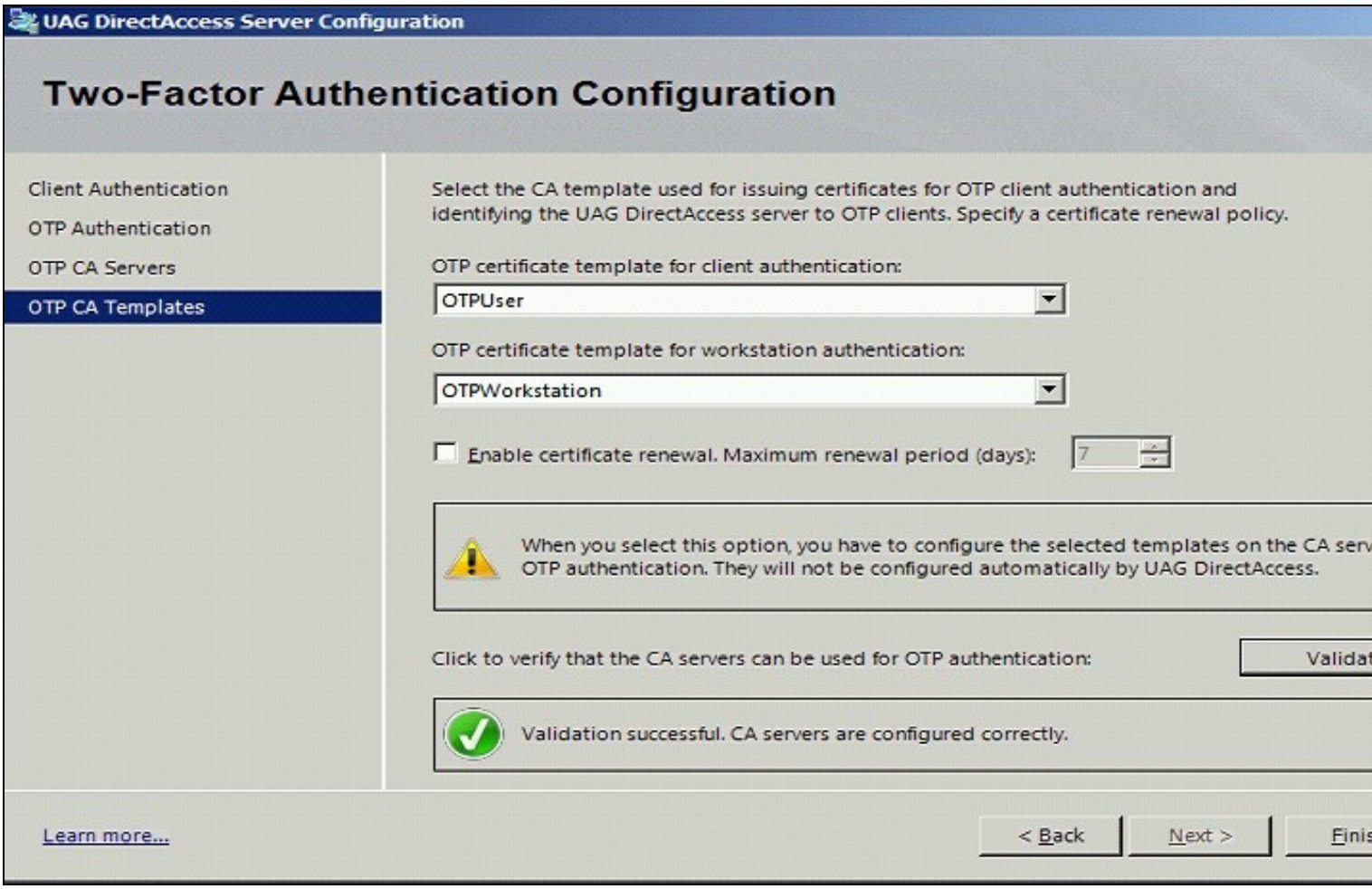
This example is configured to use existing CA templates.



Select the required templates



Validate the CA templates



369.3 Additional Installation Options

370 Verifying the Installation

Access with the Direct Access client entering username, AD password and One Time Code. If the option to *Require OTP user names to match Active Directory user names* then the user name will be automatically populated.

Check the UAG and PINsafe logs for authentication messages.

371 Uninstalling the PINsafe Integration

372 Troubleshooting

373 Known Issues and Limitations

374 Additional Information

Microsoft DirectAccess

375 Microsoft IAG Integration

375.1 Introduction

This document covers the integration of PINsafe with the Microsoft Intelligent Application Gateway.

375.2 Prerequisites

PINsafe 3.x

Microsoft IAG

The IAG integration guide can be found here: IAG SP1 Integration Guide and here SP2 Integration Guide

375.3 Baseline

375.4 Architecture

375.5 Installation

375.5.1 PINsafe Integration Configuration

375.5.2 Access Device or Application Integration

375.5.3 Additional Installation Options

375.6 Verifying the Installation

375.7 Uninstalling the PINsafe Integration

375.8 Troubleshooting

375.9 Known Issues and Limitations

375.10 Additional Information

376 Microsoft IAG Multiple Authentication

376.1 PINsafe and IAG/UAG Integration using multiple repositories

This article explains how to use PINsafe with Microsoft IAG/UAG so that different applications are available to users depending on how they authenticated.

These notes are based on IAG Version 3.7 and PINsafe Version 3.6

This article shows the approach required to add this functionality to a standard IAG/UAG and PINsafe integration. Standard integration notes are available from the Microsoft IAG Integration guide and should also be referred to.

376.2 Approach

The approach is to create two different repositories on the IAG. One repository will use Agent-XML for authentication the other will use RADIUS.

One repository will be associated with single channel authentication, the other with dual channel authentication.

The login page will determine which repository the user is authenticating based on whether the user has requested a single channel (TURing) image or not.

The IAG will be configured to allow access to specific applications based on the repository a user has authenticated to.\

On the PINsafe server the NAS or Agent associated with the IAG Dual channel repository will be set to accept dual channel authentication only.

376.3 Implementation

The names used for repositories etc are just examples, but sometimes names are important, eg the repository of type "other" needs to have the same name as the associated .inc file and needs to reflected in the checkradio() function in PinsafeLogin.asp

376.3.1 PINsafe Configuration

In this example radius will be used for dual channel authentications only so on the PINsafe server

Enable RADIUS server

Create a NAS entry for the IAG

Set ip address and shared secret as required

Set mode to dual channel only for the NAS

Create an Agent entry for the IAG

Set ip address and shared secret as required

376.3.2 IAG Repository Configuration

Copy images.asp to von\IntnernalSite\Images\CustomUpdate

Ensure that it is the version that can also handle index images and ensure that the IP addresses etc match the PINsafe server

```
if request.querystring("index") <> "" then
  Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
  objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/DCIndexImage?username="&request.querystring("username"), false
else
  Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
  objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/SCImage?username="&request.querystring("username"), false
end if
```

Create a new Repository called pinsafe of type other.

Copy the pinsafe.inc file to von\InternalSite\inc\CustomUpdate

Edit pinsafe.inc so that the secret (m_secret), ip address and port matches that of the PINsafe server

```
function checkswivelpwd (userName, password)
LIGHT_TRACE "checkswivelpwd entered for " & userName
LIGHT_TRACE "SWIVEL - lets check if the password is right"
Dim strHTML
m_secret = "secret"
Dim objWinHttp
m_request = "<?xml version=""1.0"" ?><SASRequest><Version>1.0</Version><Action>login</Action><Username>" & username & "</Username><OTC>" & pa
& m_secret & "</Secret></SASRequest>"
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
objWinHttp.Open "GET", "http://<ipaddress>:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Create a new Repository called pinsaferadius or type RADIUS.

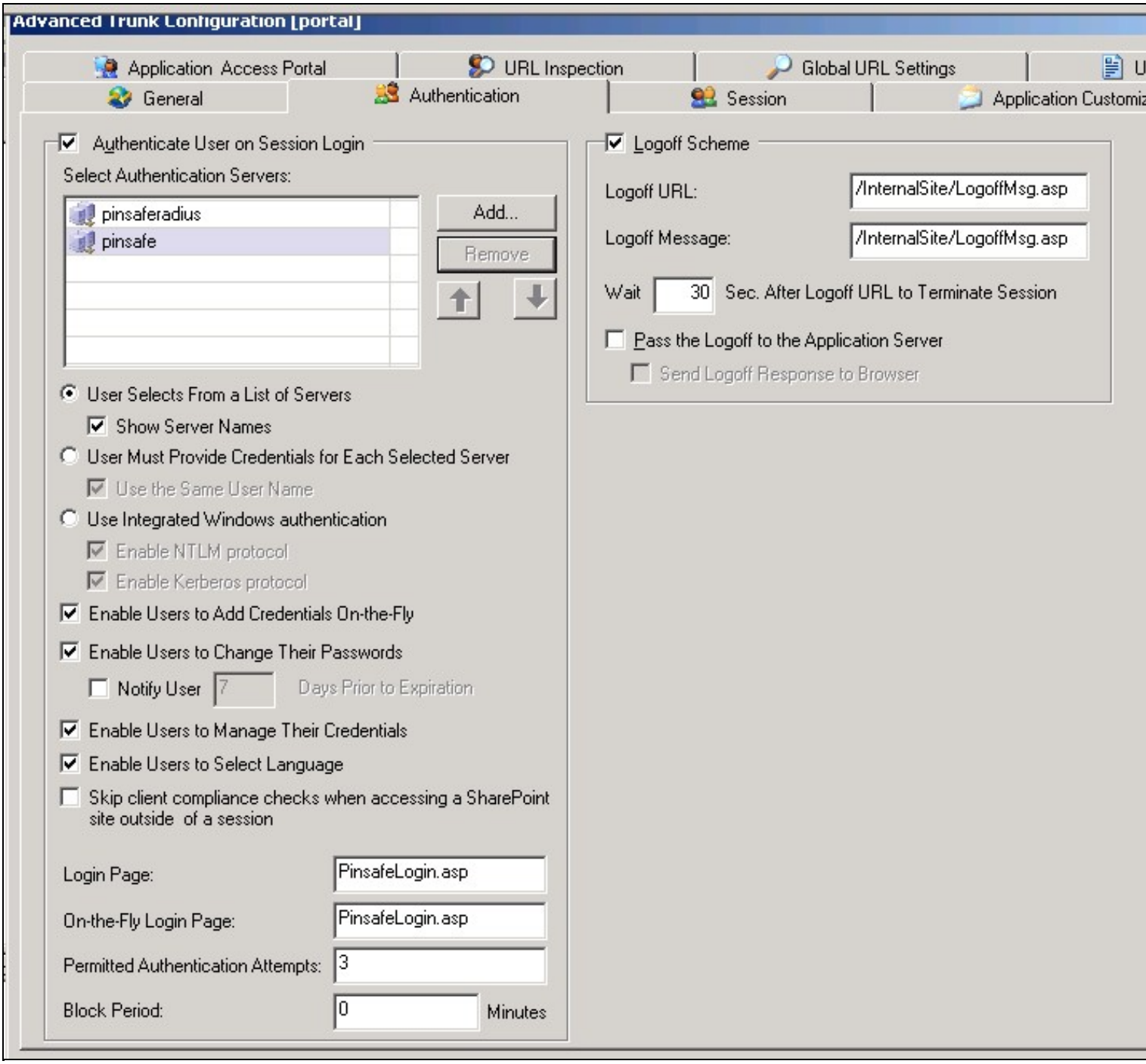
Enter the details of the PINsafe RADIUS server on the config screen.

376.3.3 Trunk Configuration

For the trunk you are using eg portal, ensure that both pinsafe and pinsaferadius repositories are associatd with the page

Also ensure that the option User Selects from A List of Servers is set

Set the login pages to be PINsafeLogin.jsp



Now copy the PINsafeLogin.jsp to von\InternalSite

Edit the PINsafeLogin.jsp to ensure that the repository names match those that you are using and that the dual channel and single channel authentication are matched to the correct repository.

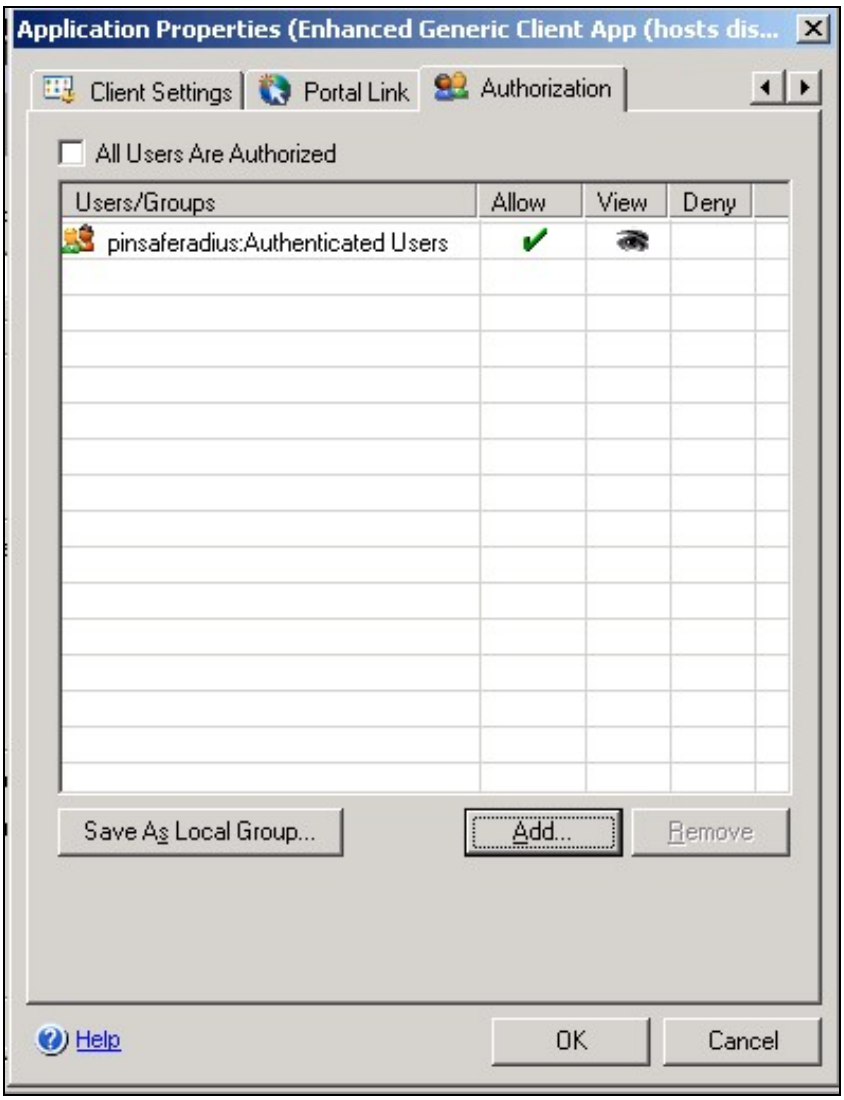
```
function checkradio()
{
  var radiovalue = eval(document.form1.swivel[1].checked);
  var r = document.getElementById("repository");
  if (radiovalue == true)
  {
  //alert("turing");
  //TURing selected, therefore refresh TURing image
  updateotp();
  //repository for TURing is pinsafe
  r.value = "pinsafe"
  } else{
 //alert("sms");
 updateindex(); //if we are using multi-sms update index will display required index
 r.value = "pinsaferadius"
 //repository for TURing is pinsaferadius
 }
```

}

376.3.4 Application Authorization

With different repositories aligned to different authentication methods, it is possible then to make some applications only accessible when a user has authenticated using the dual channel method.

To do this restrict access to applications to the pinsaferadius group on the Trunk->Applications-.Authorization tab

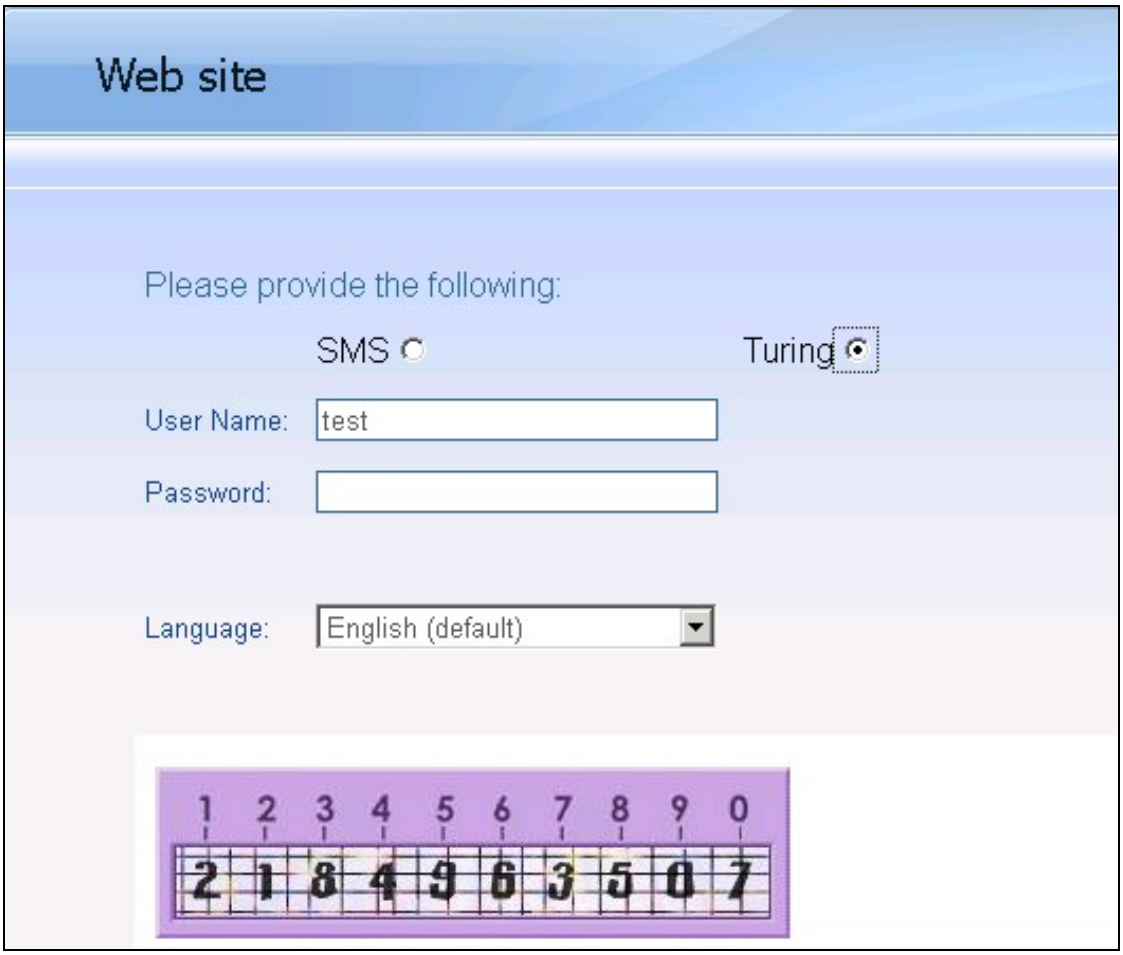


376.4 User Experience

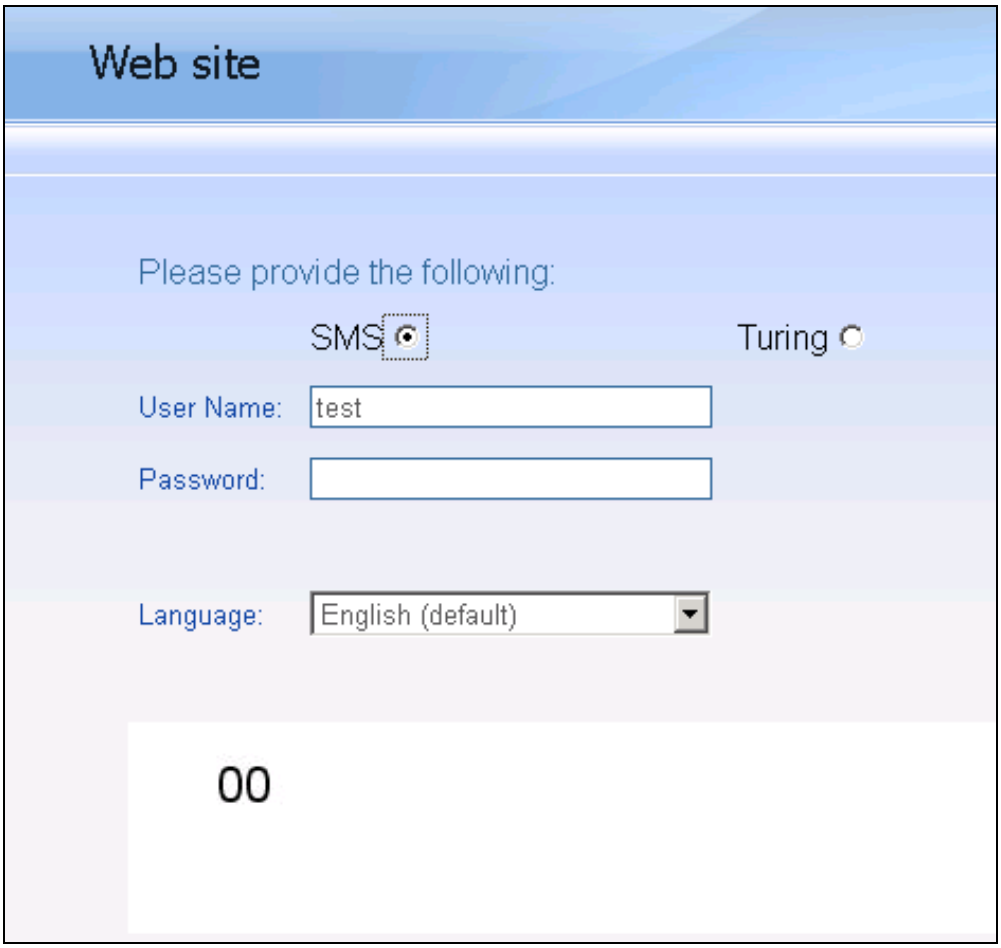
The user is presented with the option of authenticating via SMS or TURing.

To authenticate the user enters their username and then clicks on the authentication method they wish to use.

If they select TURing and TURing image is displayed.



If they select SMS (and multi-SMS is being used) the index of the security string that they need to use is displayed.



(If they have no valid SMS strings, -1 is shown)

When they make their selection the login page automatically associates them with the correct repository.

After authentication they will only have access to applications appropriate to their method of authentication.

377 Microsoft IAG SMS login video

377.1 Microsoft IAG SMS login Video

PINsafe_IAG_SMS_login.swf

378 Microsoft IAG Turing login video

378.1 Microsoft IAG TURing login Video

PINsafe_IAG_Turing_login.swf?

379 Microsoft ISA 2006 Cluster Integration

379.1 ISA 2006 Cluster Integration

379.2 Overview

In an ISA cluster, the Swivel filter needs to be registered with the cluster on the storage server and on each member of the cluster.

If all the ISA Servers are installed on 32-bit operating systems, then you can use version 1.2 of the PINsafe ISA filter, which manages filter registration as part of the login process. You must install on the configuration storage server first, and then on each member server. See the standard ISA filter integration guide (link below) for further instructions.

If you are running ISA Server on a 64-bit operating system, the reference above will not work. Instead, you will have to use the older 64-bit version together with installation scripts.

Refer to the ISA 2006 integration guide for additional steps, for both versions of the filter. Microsoft_ISA_2006_Integration

379.3 Prerequisites

These are required in addition to the ISA 2006 Integration prerequisites

- RegisterFilter.vbs
- RegisterFilterMember.vbs

These files can be downloaded from here: File:PINsafe_ISA_2006_Cluster_Registration.zip

379.4 ISA 2006 Cluster Installation Steps

379.4.1 Install the PINsafe filter

Run the setup.exe file on each of the ISA servers ignoring errors relating to registration of the PINsafeISAFIlter

379.4.2 Ensure the PINsafe Filter is on each ISA server

Ensure that the PINsafeISAFilter.dll is installed on C:\Program Files\Microsoft ISA Server on all ISA servers.

379.4.3 ISA Cluster Storage Server Filter Registration

On the configuration storage server copy RegisterFilter.vbs to C:\Program Files\Microsoft ISA Server and run it.

You may have to run it from the command prompt, specifying the fully-qualified name of the configuration storage server, if that is not the server you are running it from.

379.4.4 ISA Cluster Member Filter Registration

Copy RegisterFilterMember.vbs to C:\Program Files\Microsoft ISA Server on each member server, and run. Once you have done this, check that it appears in the list of web filters for the server.

when manually registering a web filter .dll, from the command prompt you need to be in the SAME directory as the .DLL, otherwise you will get an error:

Error: The Web Filter referenced by Server xxxxxx does not exist The error occurred on object ?xxxxxx? of class ?Server? in the scope of array ?Learning-ISA?

379.4.5 Configure the ISA Filter

Configure the ISA filter using the configuration tool provided. Each ISA server in the cluster will need to be configured. To start is select Start/Programs/PINsafe ISA Filter/Configuration.

380 Microsoft ISA 2006 Integration

381 Microsoft Internet Security and Acceleration Server (ISA) Integration Notes

382 Introduction

This document outlines the necessary steps to integrate Swivel authentication into either Outlook Web Access (OWA) 2003 or Sharepoint Forms-based Authentication (FBA) provided with Microsoft ISA Server 2006. Additionally the login page can be further customised, for further information see: Microsoft ISA 2006 web page customisation How to Guide. If the ISA server is part of a cluster then the filter needs to be installed on each cluster, the 32 bit installer handles cluster registration, for further information and manual registration see Microsoft ISA 2006 Cluster Integration

Note that with the release of version 1.2 of the Swivel ISA filter, filter registration is part of the configuration process. See below for more information. This also means that the same installer can be used for Enterprise and Standard ISA Server. Unfortunately, version 1.2 supports 32-bit operating systems only. However, there is a 64-bit version for Microsoft Forefront Threat Management Gateway. The documentation for this is now available from a separate page here.

383 Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in ISA Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required.

If the option to check a user is a Swivel user and issue a OTC field is to be used, this requires Swivel 3.4 or later.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The ISA server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per ISA server for the integration, and the integration will require a restart of the ISA Firewall Services.

383.1 ISA 2006 Filter

The installer can be downloaded from here.

383.2 TMG Filter

The TMG version can be found here. NOTE: this is version 1.4.0 of the TMG filter, released 23/8/12, which includes a number of enhancements over previous versions. See the included documentation.

384 Baseline

Swivel 3.4 or later (3.6 or later preferred)

Microsoft ISA Server 2006 or Microsoft Forefront TMG

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

385 Architecture

The ISA server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

The default install path for the standard OWA login page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\Exchange\HTML

The standard install path for PINsafe OWA authentication page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML

386 Swivel Configuration

386.1 Configure a Swivel Agent For XML Authentication

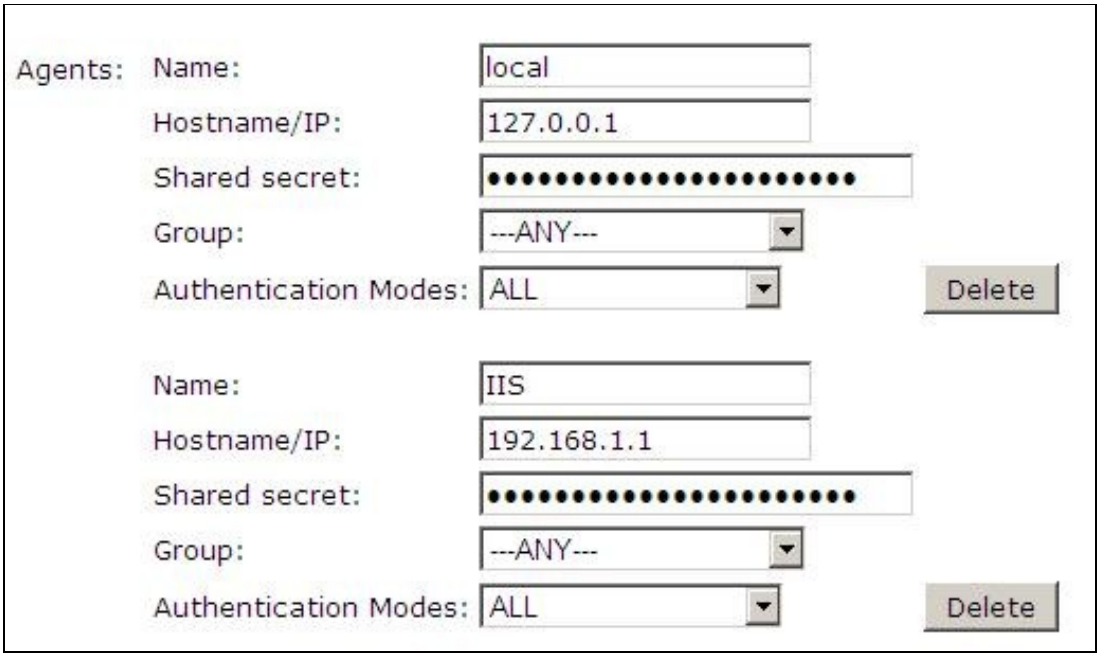
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the ISA internal IP address

4. Enter the shared secret

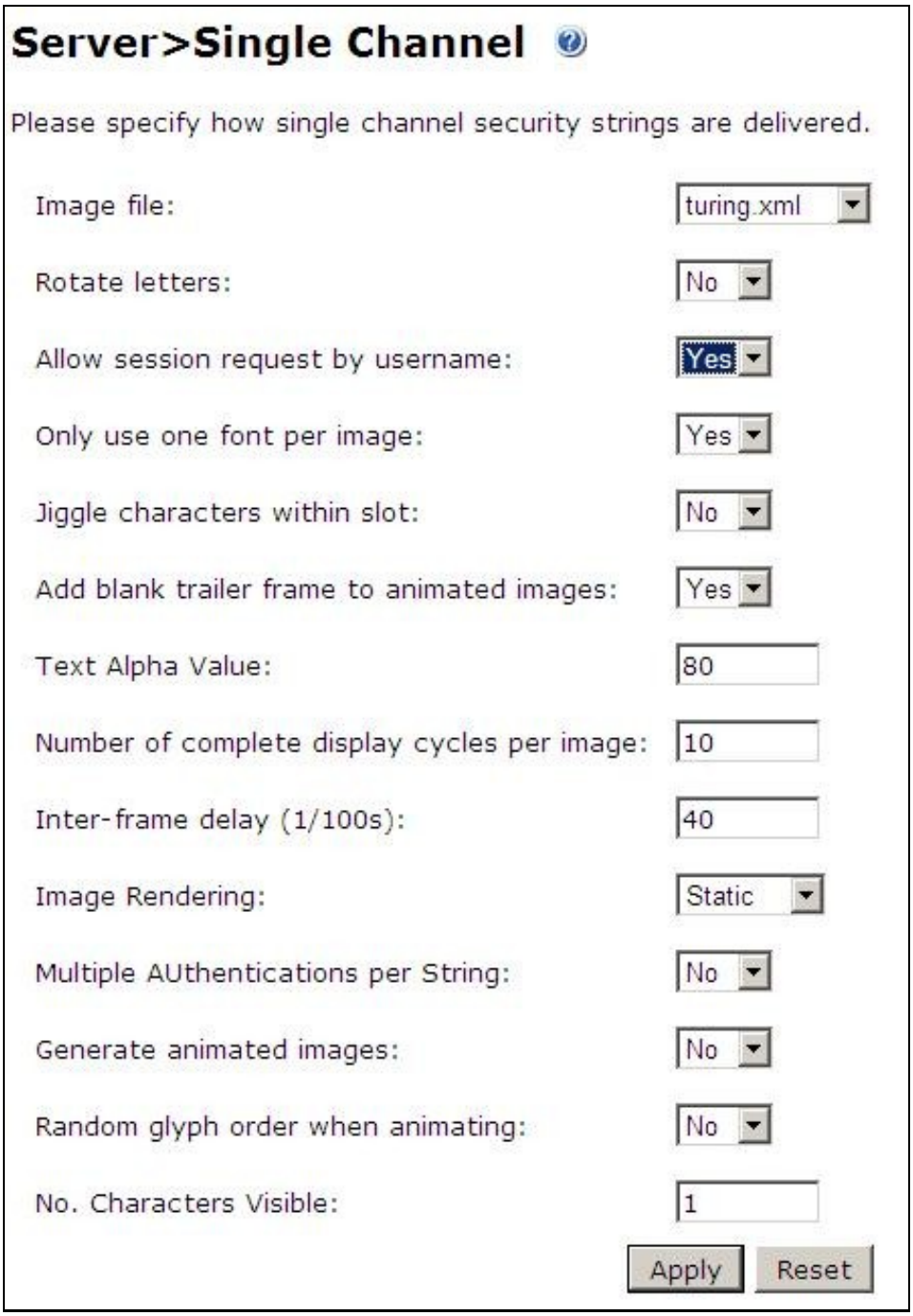
5. Click on Apply to save changes



386.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



386.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

1. Ensure the RADIUS server is running on Swivel
2. On the Swivel Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the ISA internal IP address
5. Enter the shared secret
6. Click on Apply to save changes

387 ISA Installation

The following steps should be carried out on the ISA server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below.

387.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the ISA Server documentation, if you have not already done so. Ensure that they are working as expected.

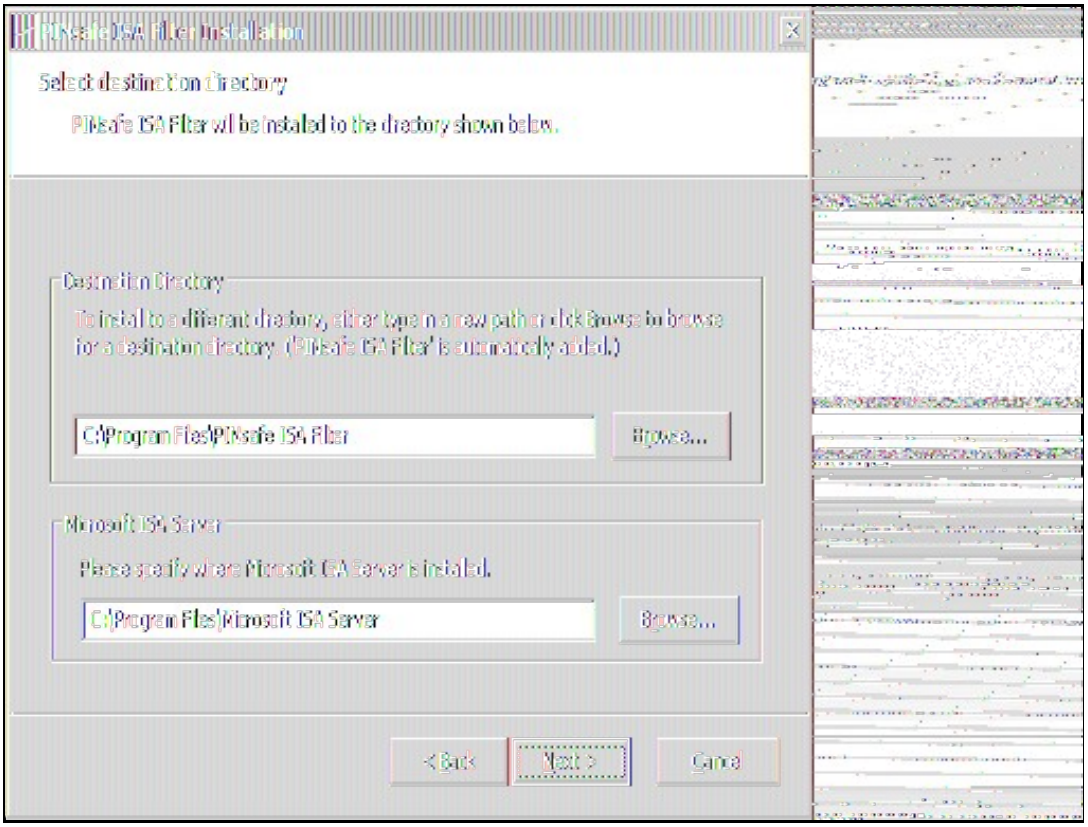
387.1.1 Configure ISA firewall rules

Create an access rule permitting HTTP access from the ISA Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

387.1.2 Install the ISA server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeISAFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft ISA Server, usually C:\Program Files\Microsoft ISA Server.



Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

387.2 Register the ISA Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with Swivel. You have a choice of registration types:

[[Image: Register_Filter.PNG]]

Select the right option for your requirements. The last option is required if you are installing on the Configuration Storage server and the same server is also a member of the ISA server array.

387.2.1 Configure the ISA server

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/PINsafe ISA Filter/Configuration.

PINsafe configuration tab:

Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. PINsafe virtual or hardware appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with ISA. (Hint: Use port 8080)

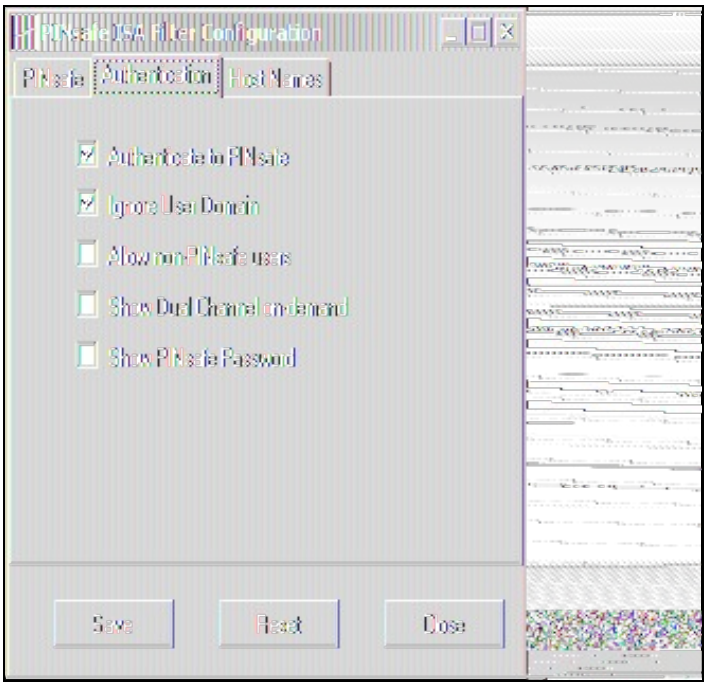
Context: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel virtual or hardware appliance where the proxy port is available, the path pinsafe using port 8080 should still be used, the ISA proxy provides security.

SSL: will, if checked, send requests to the Swivel server using https, rather than http.

Allow self-signed: when checked, causes SSL certificate errors from the PINsafe server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. After you enter this value, you will be prompted to enter it again, to confirm that it is correct.

Authentication configuration tab:



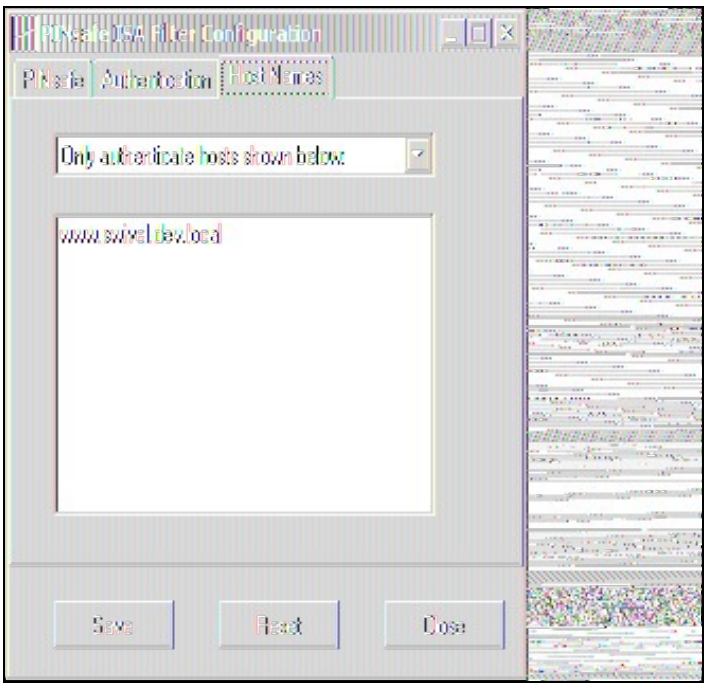
Authenticate to PINsafe: should be checked to use standard Swivel authentication. You should uncheck this if you are using the ISA filter to protect a Sharepoint website, as described in the ?Special Considerations for Sharepoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain: This will remove the AD domain of users, and when Swivel is using the SAM account name it should normally be checked, in this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the full name will be sent to Active Directory and should be used when Swivel uses the User Principle Name.

Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

The last two options on this tab should not be used - they do not work, and are there for future enhancement.

Hosts configuration tab:



This feature is new to version 1.2. Previously, when installed, the PINsafe ISA filter would affect all authentication requests through the ISA Server. This option allows you to apply PINsafe authentication per host name. It can either be configured to authenticate all host names except those specified, or to authenticate only those hosts specified, and to ignore all others.

387.3 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors. The 32 bit installer handles cluster registration, for further information and manual registration see Microsoft_ISA_2006_Cluster_Integration

387.4 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeOWA? for Outlook Web Access

and ?PINsafeWeb? or ?PINsafeRadius? for Sharepoint or other websites (?PINsafeISA? for TMG).

You should always use PINsafeRadius for Sharepoint, for reasons described below. You may use either set of forms for standard websites. Note that the TMG filter does not require a different set of custom pages for RADIUS.

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the ISA server. It can take a long time to restart this service, and if you are connecting to the ISA Server via remote desktop, you may be temporarily disconnected from it.

388 SSL Certificate Considerations

There would appear to be an issue with a recent security update for ISA Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the PINsafe ISA Server integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the ISA Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your PINsafe server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the ISA Server, if it is not already. The third option is simply to generate a self-signed certificate on the Swivel server, with the correct host name, and to install that directly into the ISA Server trusted root store (see below).

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel virtual or hardware appliance. Otherwise, refer to the relevant documentation for your operating system.

388.1 Installing a Self Signed Certificate into the ISA trusted root store

If you want to do is to trust the Swivel server certificate the following steps may be carried out:

1. Copy /home/swivel/.keystore to a suitable machine (it doesn?t have to be the ISA server).

2. Open the file in Keystore Explorer.

3. Right-click on the certificate (if there is more than one, it will probably be called ?swivel?). Select ?Export?, then ?Export key pair?.

4. Enter a password for the exported certificate. I recommend using ?lockbox?, but anything will do.

5. Select the export path. It doesn?t actually matter what the extension is.

6. Copy the exported certificate to the ISA Server. The remaining commands are done on the ISA Server.

7. Open ?mmc? from the Run dialog.

8. Select File -> Add/Remove Snap-in.

9. From the dialog, select ?Certificates? and click ?Add?.

10. Select ?Computer account?, then ?Local computer?.

11. Click OK.

12. Go to Certificates -> -> Trusted Root Certificate Authorities.

13. Right-click, then ?All Tasks?, ?Import?.

14. Select the exported certificate. You will need to enter the password. We recommend marking the key as exportable. Make sure the certificate is imported into the -> Trusted Root Certificate Authorities.

15. If you look under Certificates -> Personal -> Certificates, you should see the new certificate.

16. You may need to restart the Microsoft Firewall service before it shows the new certificate.

389 Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

Once you have configured everything, reboot the ISA server.

390 Verifying Installation

390.1 Outlook Web Access

Navigate to the URL on which ISA Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

Note that if a username is entered in the form Domain\username, the Domain\ portion of the username will be stripped before being passed to the Swivel server. This permits the use of sAMAccountName as the username attribute for synchronisation between Swivel and Active Directory.

Dual Channel Login

Single Channel Login

390.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain\user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

391 Additional Options

391.1 RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. PINsafeRADIUS custom login pages provided with the filter can be used.

391.2 Turning off Automated Security Strings

When a user enters their username and then their AD password, they will usually generate a single channel TURing image or for Dual channel On Demand authentication, automatically send an SMS message. This option is for the the integration using the OWA filter and will stop the automated display of single channel TURing images and the automated sending of SMS security strings.

The automation can be disabled by disabled by editing C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafe\OWA\HTML\usr_pwd.htm (Exact path may vary depending upon installation).

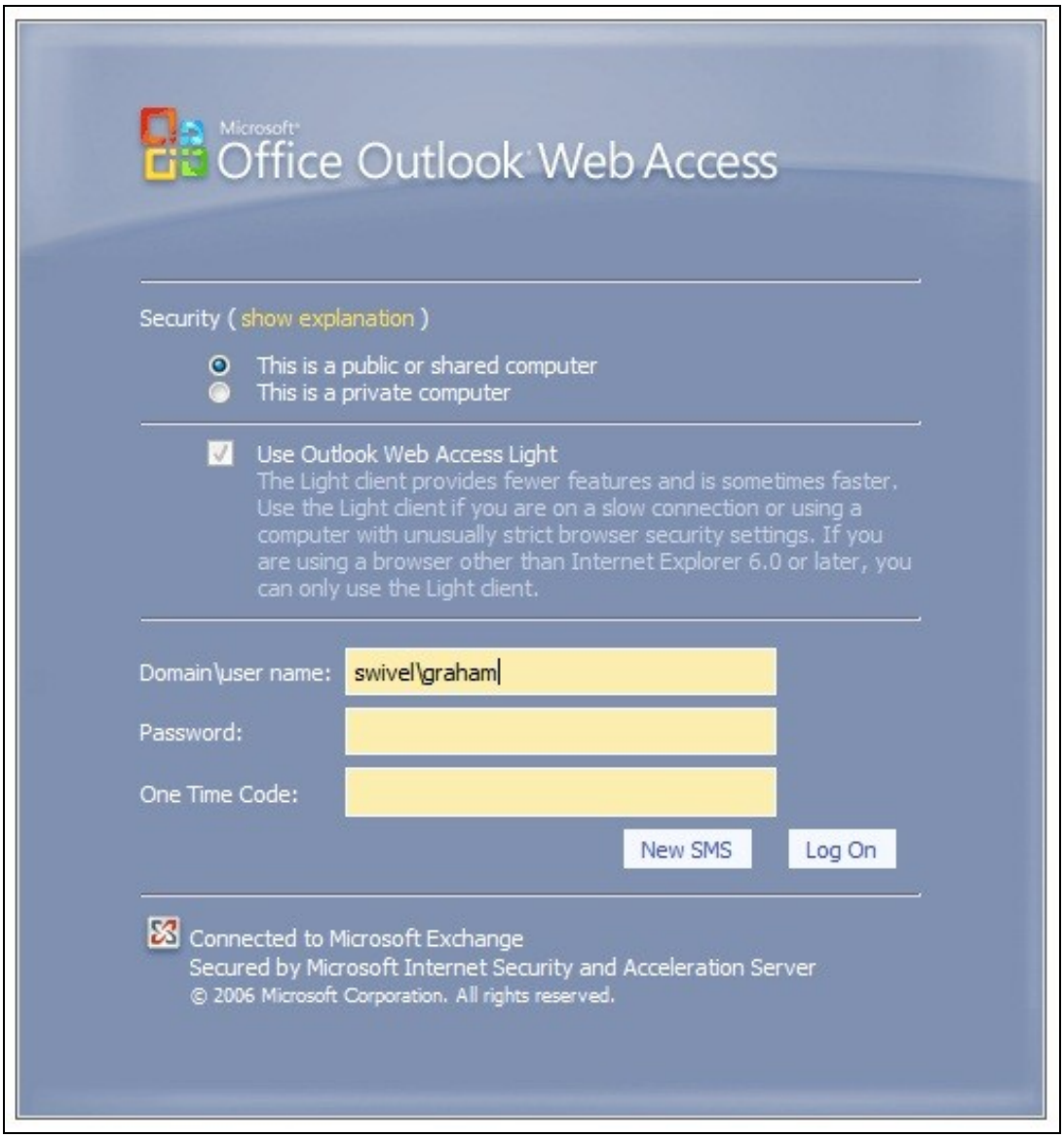
First Make a backup copy of the file

Edit the file in a text editor

Locate the setUserExists function

below this locate and remove the entire line ShowTuring();

Modified login page showing SMS on request



391.3 Editing the Security String Request Buttons

The message request buttons can be edited to display different messages.

The default International English language version is located in the the following file:

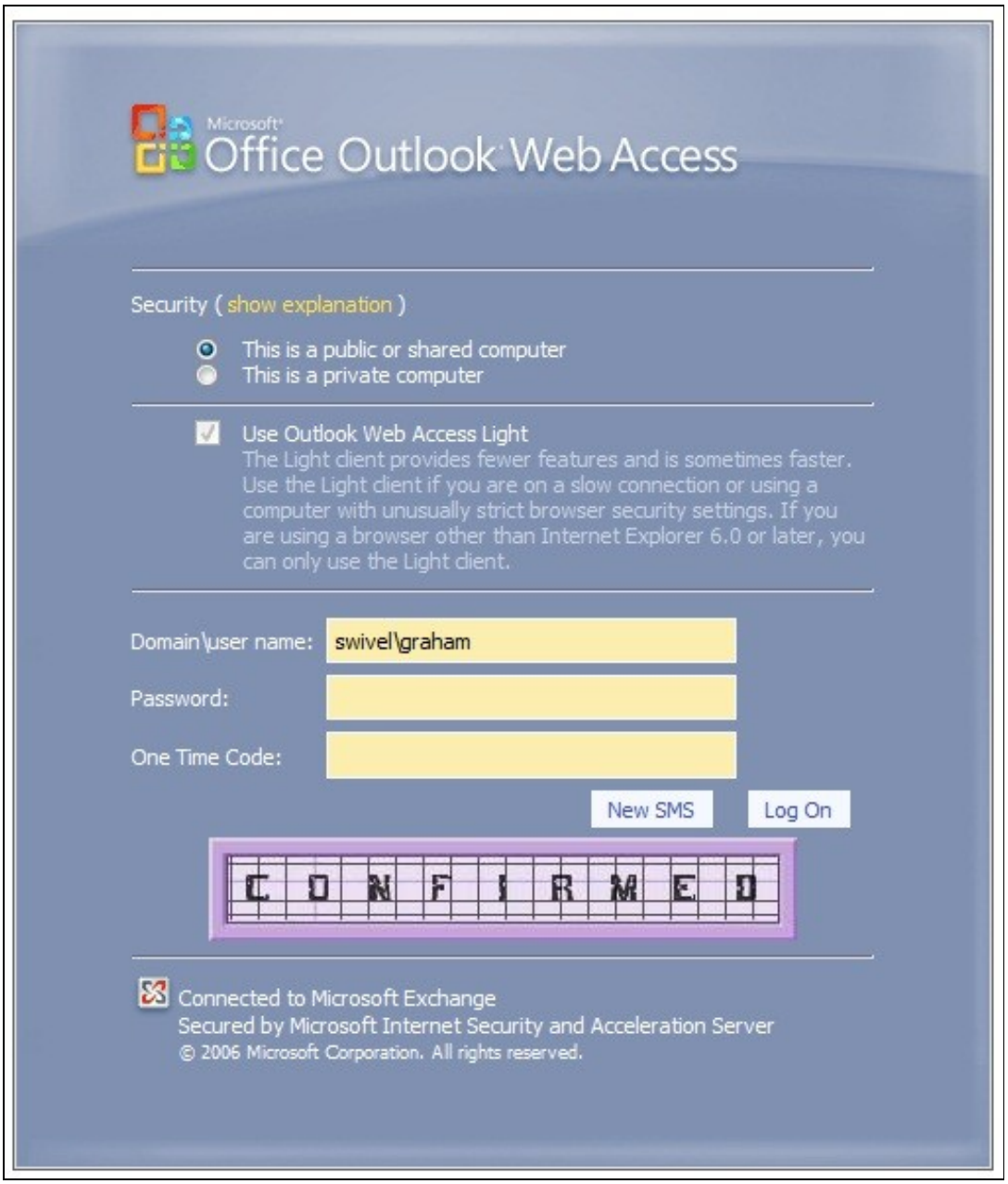
C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML\nls\en\strings.txt (Path may vary with installation, and different language files may also be edited)

First Make a backup copy of the file

Edit the file in a text editor

Find the line L_StartSession_Text="Get Image" (May also be L_StartSession_Text="Start Session" or L_StartSession_Text="Refresh Image")

Modified login page



392 Uninstalling

392.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

393 Known Issues

394 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

The Swivel authentication filter logs its activity to the standard Windows debug log. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

With regard to the Single Channel TURing image, the ISA server login page does not use SCImage, the image request comes through the filter, so that the the Swivel server noes not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

Single Channel image does not appear:

- Check Swivel ISA filter settings
- Check the Firewall service is started
- Check the ISA server logs for any error messages
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Check the Swivel ISA filter is correctly installed. On the ISA Server Management: under Configuration, Add-ins for the server, "PINsafe Authentication Filter" should be enabled
- From the ISA server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel virtual or hardware appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

- If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the ISA filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

The following error can be seen when trying to install the Swivel ISA Filter on an ISA cluster:

```
Error 1904. Module C:\Program Files\Microsoft ISA Server\PINsafeISAFIlter.dll failed to register. HRESULT -2147024891. Contact your support
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.
The "PINSafe Authentication Filter" then does not appear in the Web Filters tab.
```

See Microsoft ISA 2006 Cluster Integration

The ISA 2006 filter will not work with ISA 2004.

See also: troubleshooting OWA 2007 publishing rules on ISA Server 2006

395 Additional Information

395.1 Note on Activesync and RADIUS authentication

If you are using the same listener for ActiveSync etc, then don't use the RADIUS (or RADIUS OTP) option, as this will affect authentication for the other types as well. Since using the AgentXML approach only affects forms authentication, it shouldn't affect ActiveSync, which doesn't use FBA.

395.2 ISA and OWA

Information regarding the configuration of ISA Server to publish OWA or Sharepoint may be found in the ISA Server help under Firewall policy.

396 Microsoft ISA 2006 web page customisation How to Guide

396.1 Microsoft ISA 2006 web page customisation How to Guide

NOTE: if you need to be able to support pass-through support for non-PINsafe users, the following article is insufficient. The current recommendation is to start with the files provided with the PINsafe ISA filter, and to customise them as required. Please contact support@swivelsecure.com for more details. Use the following article only if you do not need support for non-PINsafe users.

396.2 Overview

This is a brief outline of how to go about customising your forms-based authentication web pages in ISA server to support PINsafe authentication. It is assumed that you are reasonably familiar with modifying HTML pages.

396.3 Web Page Customisation

396.3.1 Install the ISA filter

First of all, you should install the latest version of the PINsafe ISA filter for ISA Server 2006, see Microsoft_ISA_2006_Integration. This includes customised pages for Outlook Web Access (OWA) and for general web access (the documentation specifically references Sharepoint, but it will work for other web applications).

You should only need to use this document if you wish to customise these pages further, or if you already have customised authentication pages to which you wish to add PINsafe functionality.

396.3.2 Obtain the ISA login pages

If you have not already got a customised set of ISA login pages, the simplest way is to make a copy of the entire contents of C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\ISA. This folder contains 3 sub-folders: HTML, cHTML and xHTML. The latter two are for mobile standards, which PINsafe does not currently support, principally because those standards do not support JPEG images, which is the format that TURing images are generated in, so only the HTML folder is of interest. The copy should be made into a folder under C:\Program Files\Microsoft ISA Server\CookieAuthTemplates. The name of the folder should correspond to the name you enter in the custom form name in the listener properties. Within this folder, 4 files potentially need to be modified: strings.txt, usr_pcode.htm, usr_pwd.htm and usr_pwd_pcode.htm. Additionally, if international support is required, other strings.txt files will need to be modified. These files are under the nls sub-folder, one for each language. Note that, for international characters to be displayed correctly, the strings.txt file must contain Unicode characters, so you will need to use a text editor that supports reading and saving Unicode files (e.g. NOT Notepad).

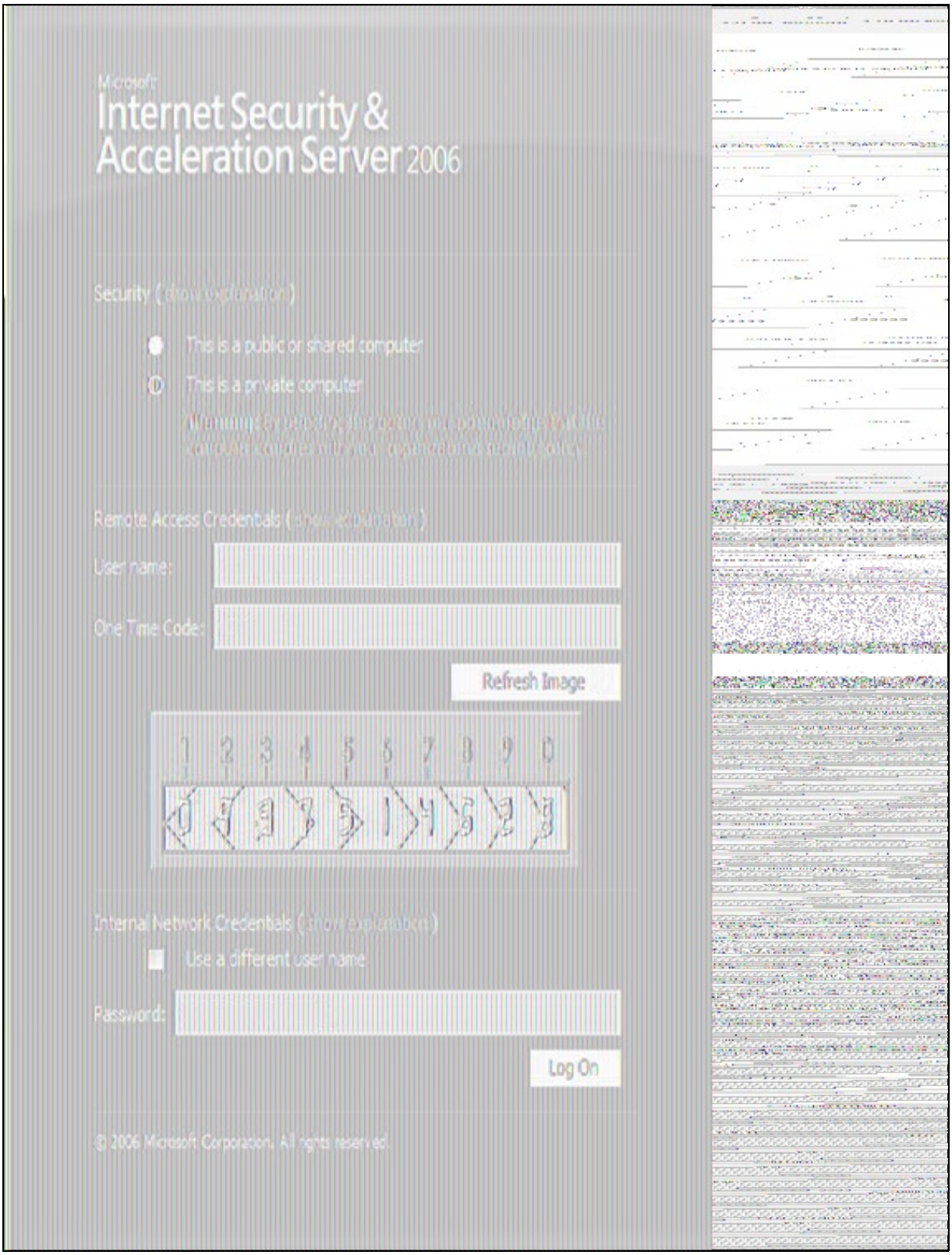
The strings.txt file supplied in the pinsafeWeb (or pinsafeOWA) folder of the PINsafe ISA filter installation should be sufficient for your needs, unless you have added other customised strings to your web pages.

Note also that if you have added custom images and/or stylesheets, you will need to include them in the new custom folder.

396.3.3 Customising the web pages

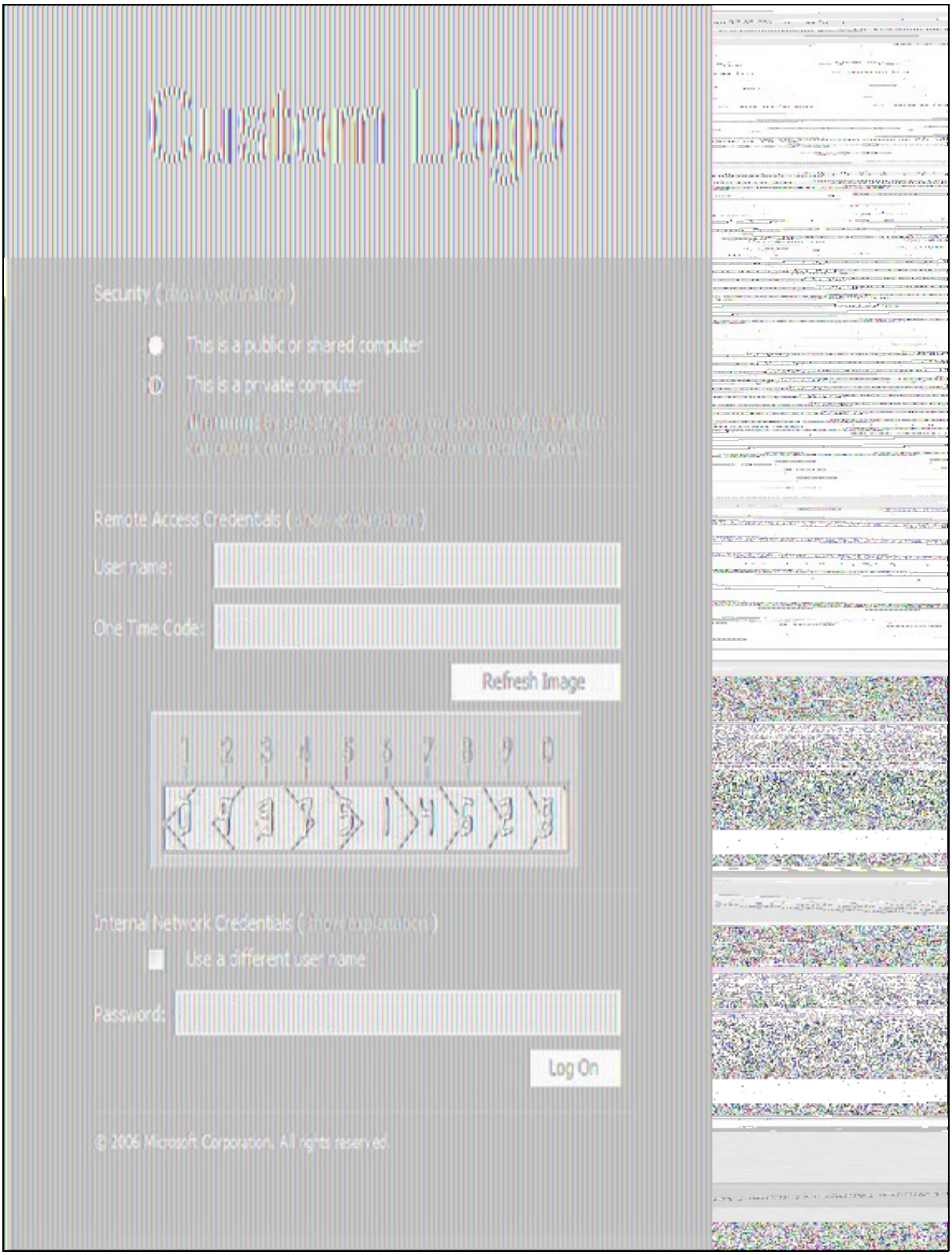
396.3.3.1 Change the Banner Logo

It is possible to change the logo displayed at the top of the login page. The page may look like this:



The image shown here at the top is in GIF format and is 500x115 pixels. On a 32-bit machine the picture can be found in "C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINSafeOWA\HTML" - if the ISA server was installed to a non-standard location then this will not be the location. The file name of the logo is lgnTop.gif.

In order to update the picture for display you can simply substitute a new logo of exactly the same format and size then restart the ISA service to complete the installation of the new logo. This should then display the next time the page is accessed. The end result should look like this:



396.3.3.1.1 Troubleshooting

If the page is requested by a refresh it is possible that the browser will display a cached version of the site. Clearing the cache within your browser may fix this.

If the logo is not of the same format (GIF) or of the same size (500x115pixels) then it may fail to display correctly.

If the name of the new image differs in case to the original then it may fail to load correctly.

When swapping the images it is recommended that you rename the old picture file and add the extension ".old". This will allow you to easily revert the image should the need arise.

396.3.3.2 Edit the strings.txt file

The entries added for PINsafe are:

L_OTC_Text = ?One Time Code:?

L_StartSession_Text = ?Start Session?

These are respectively the labels used for the one-time code text box and the TURing image request button. You can change these values (to the right of the = sign) to match your requirements, but ensure that the labels (to the left of the = sign) are as shown.

If you need to customise your pages for other languages, look in the nls sub-folder and find the sub-folder matching the language you need to use. Add strings with the same names as those shown above to the strings section. As noted above, please ensure that the files are saved as Unicode text.

Depending on what authentication method you are using, you may not need to modify all three of the login pages, as explained here:

- usr_pwd.htm is used for Active Directory plus PINsafe AgentXML authentication.
- usr_pcode.htm is used for RADIUS authentication as the ONLY form of authentication (i.e. when no Active Directory authentication is required).
- usr_pwd_pcode.htm is used when Active Directory authentication is used in conjunction with PINsafe RADIUS authentication.

The other 3 pages all need very similar modifications: they need a text box for the one-time code, a button to display the TURing image, a place to display the TURing image and the JavaScript necessary to display the image.

Starting with the last item, the following JavaScript should be sufficient:

```
function onClickStartSession()
{
    img = document.getElementById("PINsafeImage");
    username = document.getElementById("username");

    if ((img != null) && (username != null) && (username.value != ""))
    {
        var usernameValue;

        psn = username.value.indexOf("\\");
        if (psn != -1)
            usernameValue = username.value.slice(psn + 1);
        else
            usernameValue = username.value;

        img.src = "/PINsafeISAFilter.dll?username=" + usernameValue +
                  "&random=" + Math.round(Math.random()*1000000);
        img.style.display = "block";
    }
}
```

Note that, for usr_pwd_pcode.htm only, the fourth line should read

```
    username = document.getElementById("userid");
```

For the one-time code text box, both the id and the name attributes of the input field should be set to ?otc?:

```
<input id="otc" type="password" name="otc" />
```

For its label, use the value @@L_OTC_Text as the label text. This will be replaced by the label you defined in strings.txt:

```
<label for="otc">@@L_OTC_Text</label>
```

The button to display a TURing image should have an onclick event of ?onClickStartSession();?, and a value (label) of ?@@L_StartSession_Text?:

```
<input id="StartSession" type="button" value="@@L_StartSession_Text" name="StartSession" onclick="onClickStartSession();"/>
```

Finally, the placeholder for the TURing image should have an id of ?PINsafeImage?, and initially set to be invisible:

```
<img id="PINsafeImage" style="display:none;" />
```

397 Microsoft OWA 2003 IIS Integration

397.1 Introduction

PINsafe allows users to authenticate users of Outlook Web Access (OWA) on Microsoft Exchange Server 2003. An ISAPI filter installed on the Exchange server allows access to protected resources through the PINsafe authentication. NOTE: This document refers to the version of the filter numbered 1.2.0.0, and the configuration application with the same version number.

397.2 Prerequisites

Microsoft Exchange 2003 with OWA. It should be configured as a front-end server for MS Exchange, with forms-based authentication enabled.

Microsoft 2003 Server

PINsafe server: Requires PINsafe 3.x. PINsafe does not need to be installed on the same machine, but the target server must be able to connect to a PINsafe server without any authentication except that provided by PINsafe.

Users are able to login using standard OWA

IIS Filter for OWA 2003

397.3 Baseline

Microsoft Exchange 2003 with OWA using IIS 6.0

Microsoft 2003 Server

PINsafe 3.7

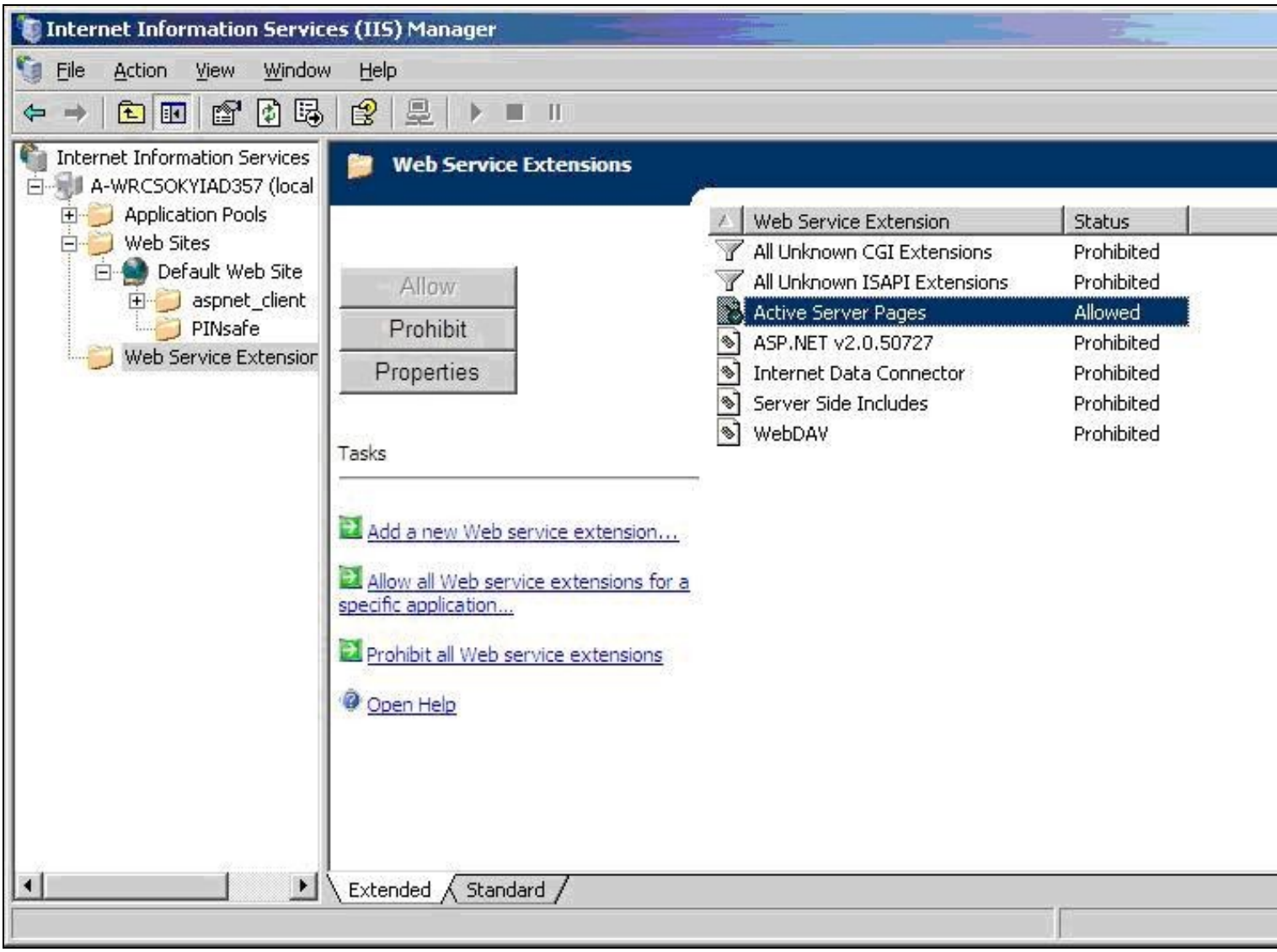
397.4 Architecture

The Exchange server makes authentication requests against the PINsafe server by XML authentication

397.5 Installation

397.5.1 Ensure Active Server Pages are Allowed

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



397.5.2 Software Installation

On the Exchange server run the PINsafeIISFilter.exe. The filter must be installed in the Exchange Server authentication web folder, which by default is C:\Program Files\Exchsrvr\exchweb\bin\auth. If this is not correct, change the target folder before installation. Select Start Menu Folder. When details are correct click on Install. If the error ?Incorrect Command Line Parameters? is seen click on OK.

397.5.3 Configuration of the IIS Filter

The Filter Configuration should start after installation or can be started through the Start Menu.

- PINsafe Server tab contains settings which define the PINsafe server which will be used to authenticate users.

Hostname/IP: The name or IP address of the PINsafe server.

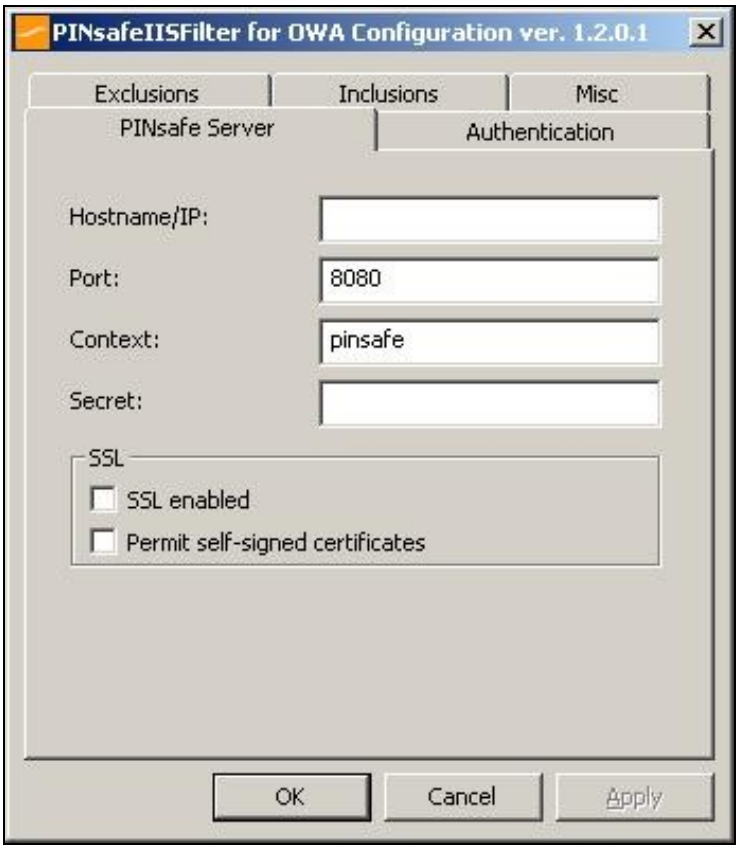
Port: The port number used by the PINsafe server, 8080 for a software install or PINsafe virtual or hardware appliance (do not use 8443)

Context: The PINsafe install name usually pinsafe, or for a PINsafe virtual or hardware appliance proxy.

Secret: The common secret used to communicate with the PINsafe server. This value must be the same as the secret defined for the PINsafe agent.

SSL enabled Tick this box to require SSL (HTTPS) communication with the PINsafe server, for a PINsafe virtual or hardware appliance ensure the box is ticked.

Permit self-signed certificates Tick this box to allow SSL certificates to be self-signed. This also ignores other certificate errors, such as site names not matching. For a PINsafe virtual or hardware appliance tick this box until a valid certificate is applied.



- The Authentication tab contains the following settings:

Idle time (s): The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Username header: The name of a cookie which will pass the username of the authenticated PINsafe user. If this value is blank, no cookie will be provided.

Single Indicates that single channel security strings (i.e. TURing image) are permitted.

Dual Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

On-demand dual Indicates that the login page should display a button to request dual-channel security strings.

Display password fields Indicates that the login page should show a field for PINsafe password as well as OTC.

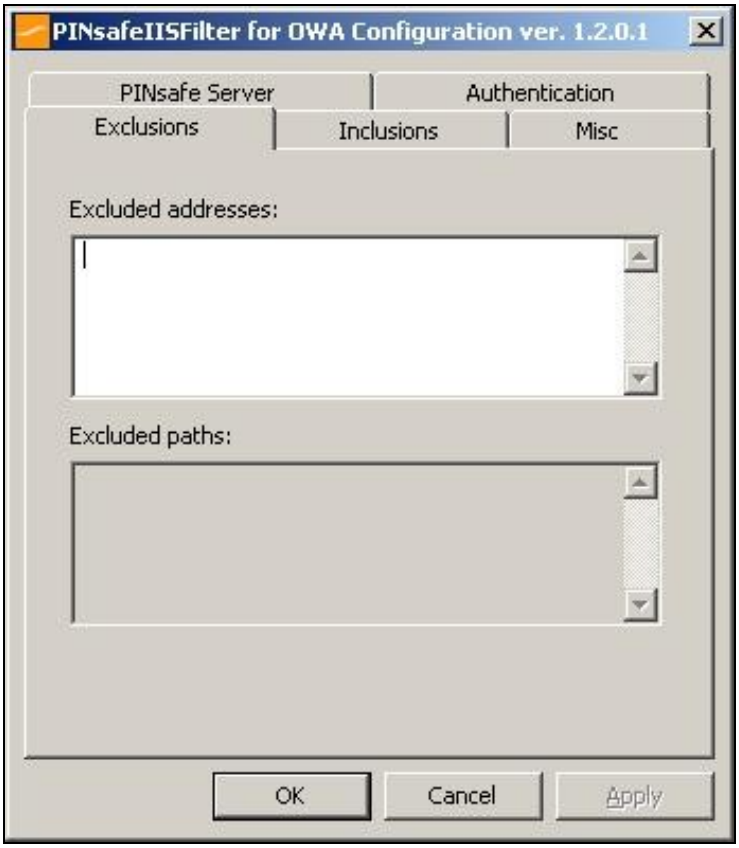
Permit self-reset Indicates that the user self-reset page should be enabled.

Standard auth. for non-PINsafe Users If enabled, users that PINsafe does not recognise will be allowed to authenticate using standard Active Directory methods. Note that this option requires PINsafe 3.5 or later. The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

- Exclusions

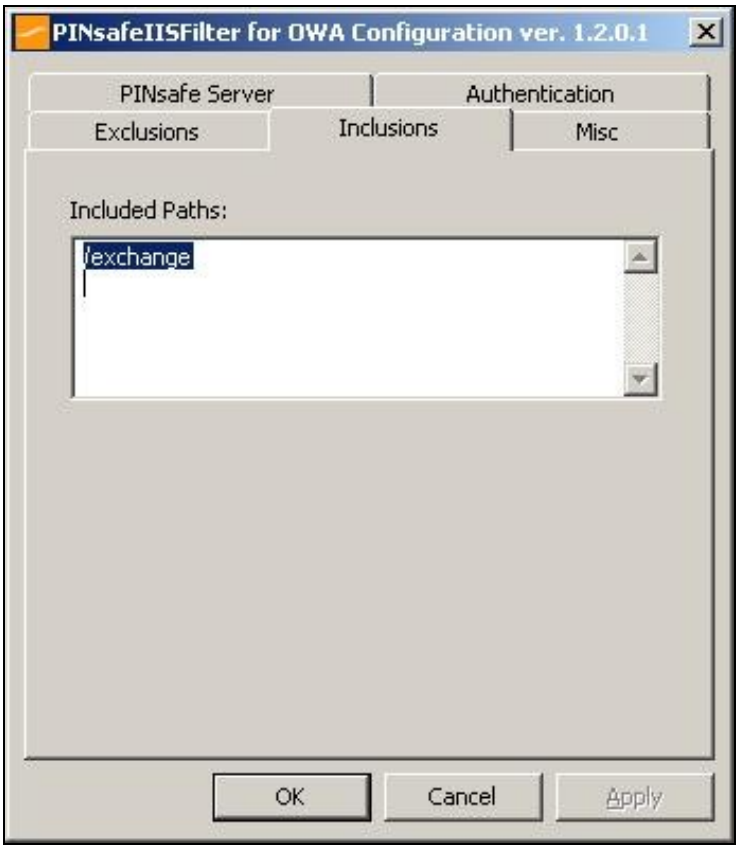
Excluded Paths: This is a list of paths within the current website which should be exempt from PINsafe authentication. This is only relevant if the included paths list is empty, in which case all paths not on this list will be protected by PINsafe.

Excluded addresses: This is a list of IP addresses which are exempt from PINsafe authentication. All requests from these addresses are passed through without authentication.



- Inclusions

Included Paths This is a list of paths within the current website which require PINsafe authentication. If this list is empty, the entire website will be protected except as indicated by the Exclusions tab. Paths should be one per line. You should at least ensure that the virtual folder ?/exchange? is listed.



- Misc Tab

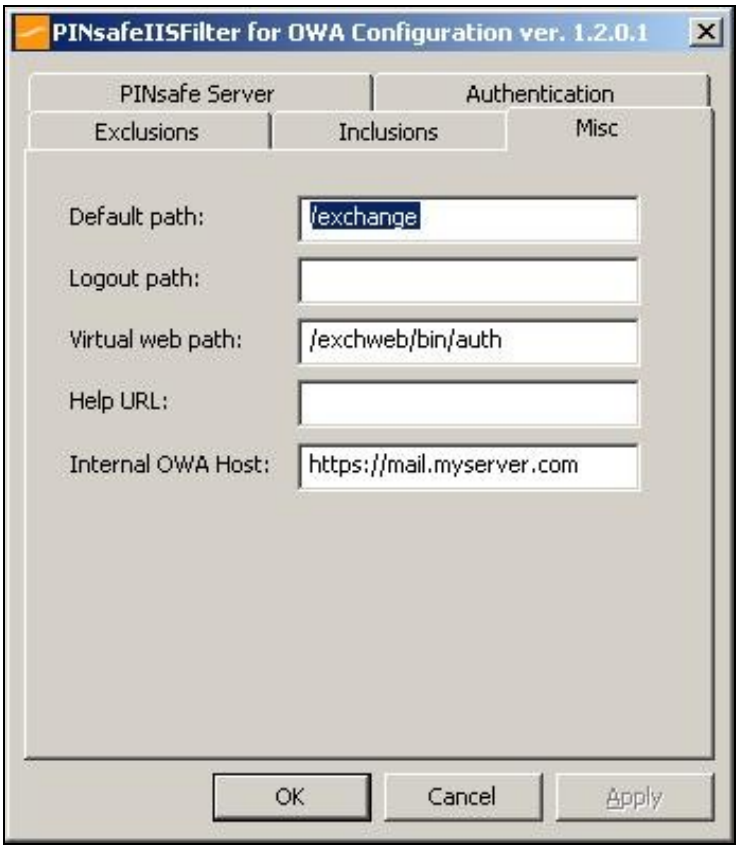
Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. For this particular version of the filter, it should be ?/exchange?. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the page she was trying to access. If the user requests the login page directly, she will be redirected to this location after authentication.

Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out.

Virtual web path: This is the path to the PINsafe authentication pages. The default for this version of the filter is ?/exchweb/bin/auth?. You should only change this if your Exchange server has an unusual configuration.

Help URL: The URL for PINsafe IIS filter help. The filter does not come with help pages as standard, so this should only be filled in if help pages have been provided by the reseller or end user.

Internal OWA Host: This should be set to the URL of the OWA Exchange server, for example https://mail.myserver.com. Since this URL is called from the server itself, you could use https://localhost, but if you do that, make sure that you check the option to accept self-signed certificates, as the server certificate will not match the name ?localhost?.



397.5.4 Modifying the OWA Authentication Pages

The installation process replaces the existing owalogon.asp file with one customised for PINsafe. The existing file is renamed to owalogon.asp.old. Note that if you have customised the OWA logon page, other than simply replacing images or text messages, then you will not be able to use the customised pages as they are. You will need to combine your own customisations with those necessary for PINsafe authentication. For help with this, please contact your reseller, or Swivel Secure.

397.5.5 Modifying the login Page to stop the Single Channel Image automatically appearing

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

397.5.6 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

397.5.7 International OWA login Pages

If you want to use an internationalized version of the logon page, you will need to modify the installed files by hand, as follows:

1. Open an Explorer window on the OWA authentication folder (by default C:\Program Files\Exchsrvr\exchweb\bin\auth).

2. Copy all of the files in the authentication folder except owalogon.asp.old and owaauth.dll to the language-specific folder you intend to use (if you need to support multiple languages, you will need to copy all of them to each folder).

3. Rename owalogon.asp.old back to owalogon.asp.

4. In each folder, make a backup copy of logon.asp (which was in the folder before), and copy all the lines beginning ?CONST? from the beginning of the original logon.asp file to the copy of owalogon.asp you have just created, replacing similar lines in that file. You will also need to change the strings labelled ?CONST L_OTC_Text? and ?CONST L_StartSession_Text? with appropriate translations of the English strings ?OTC? and ?Show TURing?. Finally, rename owalogon.asp to logon.asp.

NOTE: Unlike previous versions of the PINsafe ISAPI filter (both standard and OWA), the PINsafe customisation is not visible immediately. Once you enter a username, the OTC field will appear, as will a TURing image. This means that it is no longer necessary to click a button to get a TURing image.

However, a button is provided should you wish to refresh the image (if the first one is too difficult to read, for example). Note that if you enable the option to allow standard authentication for non-PINsafe users, and the user is not recognised, no OTC field or TURing image will be displayed. Note also in this case there may be a small delay while the user is checked.

397.5.8 Applying Settings

After the changes have been made click apply and from the Services application, usually found from the Control Panel Administrative Tools, restart the World Wide Web Publishing Services.

397.5.9 Activating the ISAPI filter

1. On the Internet Information Services Manager Select the Properties for the website

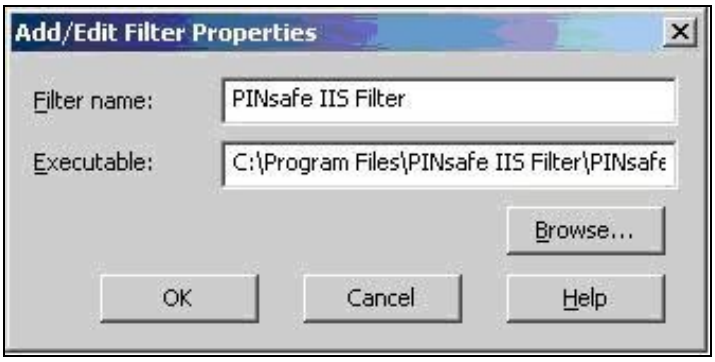
2. Select ISAPI filters

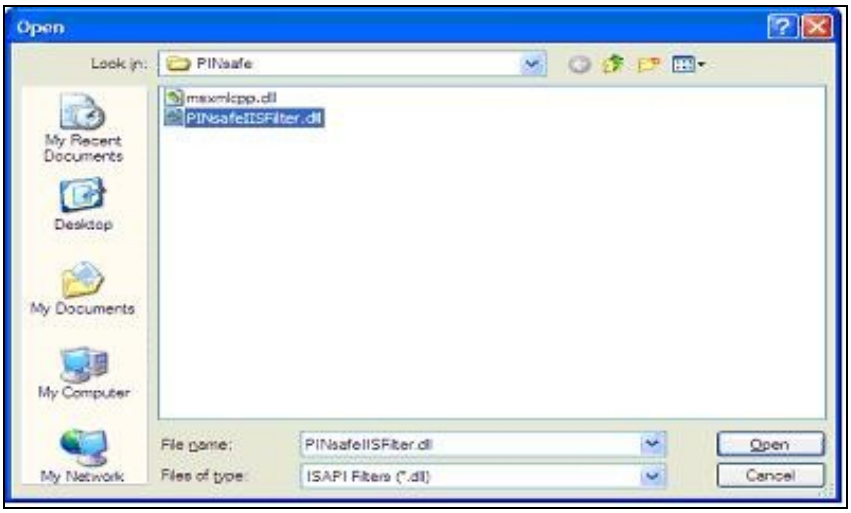
3. Select Add ISAPI filter

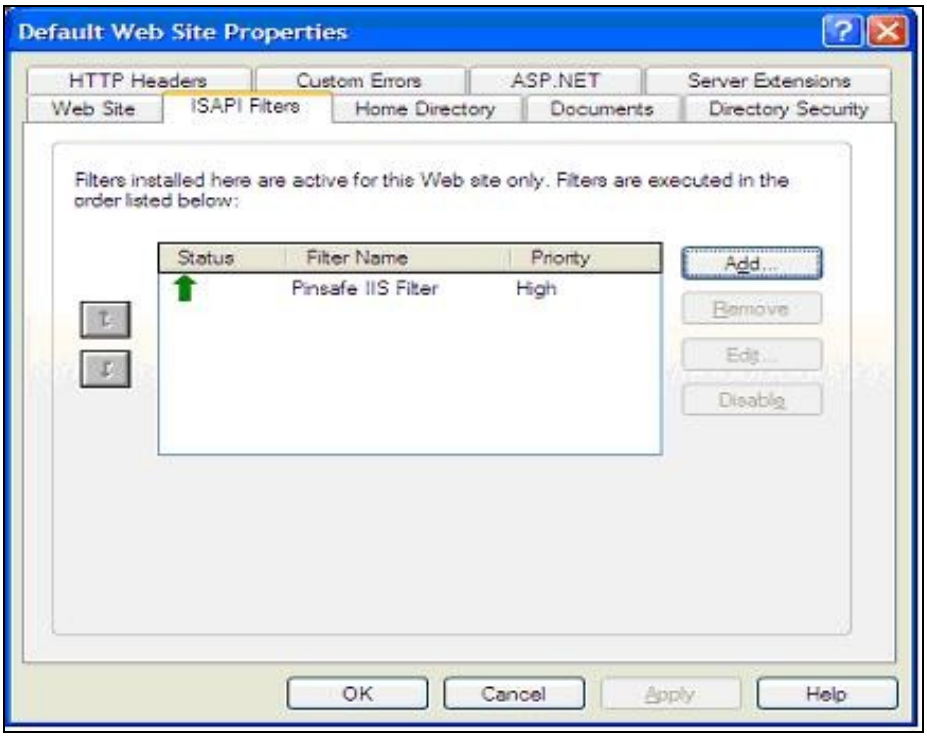
4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder bin of the installation folder.

Default: c:\Program Files\Exchsrvr\exchweb\bin\auth\bin\

5. Ensure PINsafe ISAPI filter is top filter then click on OK







397.5.10 Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

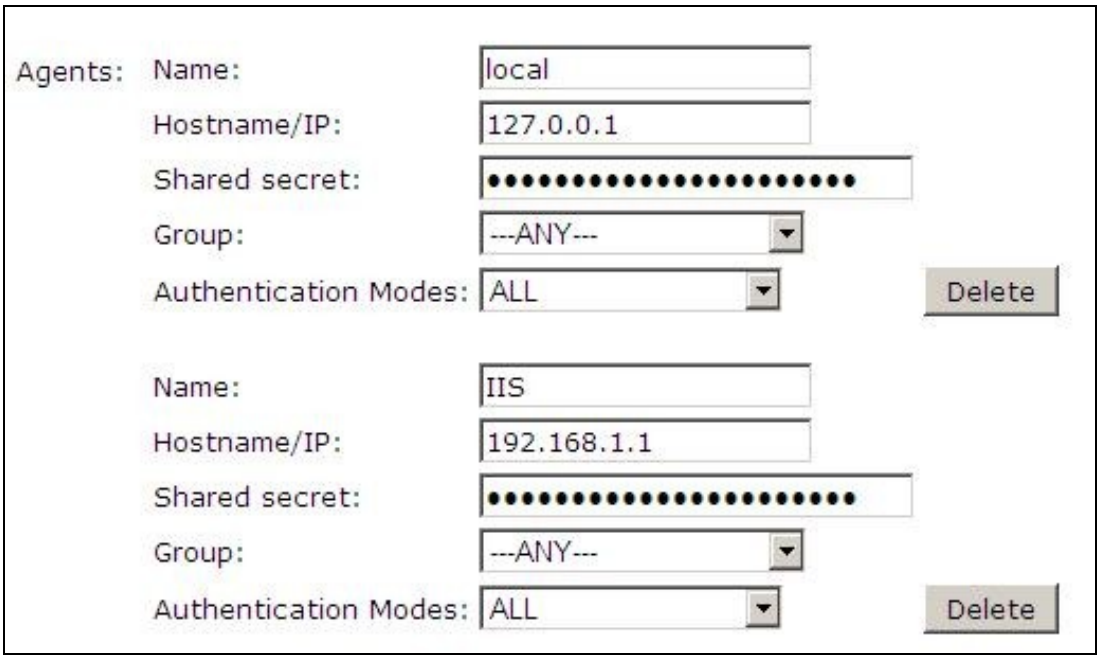
1. On the PINsafe Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the Exchange Filter

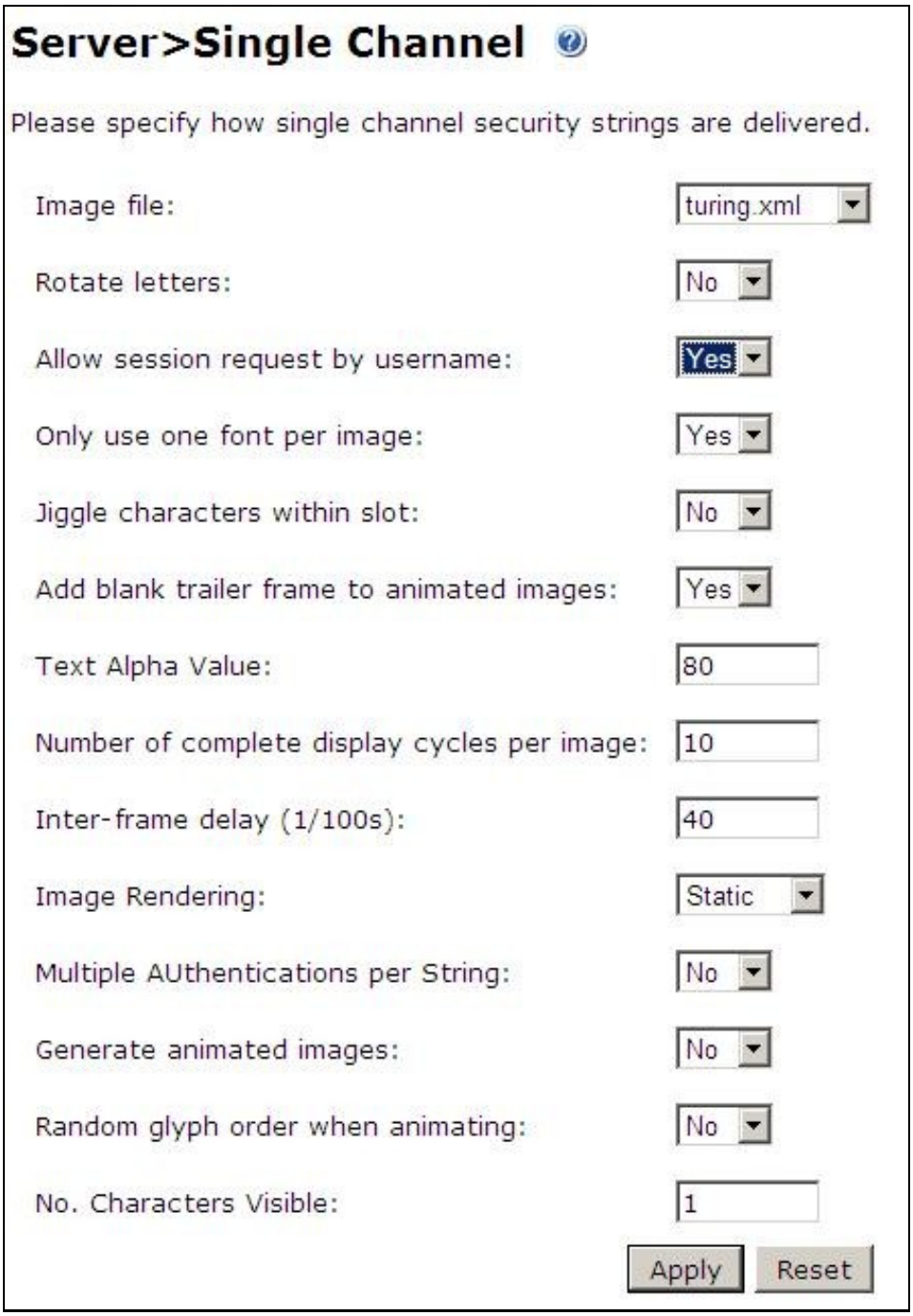
5. Click on Apply to save changes



Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



397.6 Verifying the Installation

To test the modifications, simply attempt to connect to Outlook Web Access. You should see the usual OWA authentication page, with two additions. Firstly, a third text box, for you to enter your PINsafe one-time code, and secondly, a new button labelled ?Show TURing? (or the equivalent if you have changed the language). To log on, enter your username (including domain if required) and click the ?Show TURing? button, if you are using TURing images. Enter your domain password and one-time code. Note that you should NOT use PINsafe passwords in this case. The authentication mechanism assumes that you have no PINsafe password, so will fail if you have. Now click ?Log On?, and if your credentials are correct, you should see the OWA interface as before.

397.7 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in /owa/auth, and renames the original to Logon.asp.old. To complete uninstallation this file must be copied back again.

397.8 Troubleshooting

397.8.1 General Errors

Check the PINsafe and Windows server logs, and the IIS log C:\Windows\System32\LogFiles\W3SVC1 (the last directory may be different if you have more than one website on the same server).

Add an entry to the hosts file on the OWA server (C:\Windows\System32\drivers\etc\hosts). Add a new line to the file containing the following:

127.0.0.1 <owaserver.domain>

Replace <owaserver.domain> with the full external host name used to access the OWA server (not including https://). Then change the internal OWA host name on the PINsafe configuration to https://owaserver.domain (replacing owaserver.domain as before).

Reboot the Exchange server if it has not been started

Check the AD User is not required to Change their Password

Check the AD User account is not locked

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

Turing image appears but user cannot authenticate.

Verify that the OWA is configured to use port 8080 and context pinsafe. port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed.

397.8.2 No Login Page Errors

No login page, check the Exchange version

Check to see if an International version of OWA is being used

397.8.3 Single Channel (Turing) Image issues

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For PINsafe software and virtual or hardware appliance installs:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

397.8.4 Active Server Pages Errors

If the web page is redirected to the owalogon.asp page but an error message appears, then ensure that the Active Server Pages are allowed. To verify this select the Internet Information Services Manager, expand the required server then click on Web Service Extensions.

397.8.5 ISAPI Filter Issues

NOTE: after the first time you authenticate to OWA, you should check that the ISAPI filter is loaded and running properly. Go to the web site properties dialog and locate the ISAPI filters tab. If the PINsafe filter doesn?t have a green arrow next to it, or the priority shows as ?Unknown?, then it is not working properly. You will still get redirected to the login page, and the built-in OWA security will handle that, but without the filter, it is possible for a knowledgeable person to authenticate with just the username and password, and bypass PINsafe.

The following procedure should ensure that the filter is loaded correctly:

1. Check which application pool your web application is running as, then go to the properties page for that application pool.

2. On the Identity tab, change the user to ?Local System?. You will be warned that this is a potential security risk, but don?t worry ? it won?t be left like this.

3. Restart IIS.

4. Authenticate to OWA. This should ensure that the filter is loaded: go back and check it.

5. You can now go back to the application pool and change the identity back to what it was originally: it would appear that it is only necessary to run as an administrator to get the filter to register initially.

397.8.6 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1.

397.9 Known Issues and Limitations

PINsafe requires Forms Based Authentication (FBA), whereas iPhone and other Smart Phones (plus Outlook Anywhere) will require Non Forms Based Authentication (NFBA). You cannot have FBA and NFBA running on the same front end Exchange server. You would have to create a new Exchange server as a front end to the existing Exchange server and put the PINsafe OWA filter on that. You should be able to maintain services to the existing Exchange server whilst creating a new Exchange front end. Eventually you should be able to disable access to the old OWA, but maintain NFBA authentication to your other services.

To check if FBA is enabled, in the exchange manager, go to the server, select protocols, http and choose properties.

Microsoft have published a workaround for this issue, see Microsoft OWA with OMA on Exchange 2003

397.10 Useful Links

HTTP to HTTPS Redirect [1]

397.11 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

398 Microsoft OWA 2007 IIS Integration

399 Introduction

PINsafe allows users to authenticate users of Outlook Web Access (OWA) using Microsoft Exchange Server 2007.

Active Sync users are able to receive email without PINsafe authentication as this uses a separate URL.

400 Prerequisites

Microsoft Exchange 2007 with OWA

Microsoft 2003/8 server

Microsoft .Net Framework version 3.5

PINsafe 3.x

Users are able to login using standard OWA

IIS Filter for OWA 2007 version 2.7. This uses a different authentication mechanism from 2.6, which resolves problems reported by some users. Also some cosmetic fixes: in particular, Pinpad images are correctly sent as PNG format, rather than JPG.

Older versions:

IIS Filter for OWA 2007 version 2.6, including support for Pinpad and Change PIN

IIS Filter for OWA 2007 version 2.3

IIS Filter for OWA 2007 version 2.0

Login page for OWA 2007 8.2.301 (not necessary for version 2.6).

401 Baseline

For version 2.3 or later:

- Microsoft Exchange 2007 service Pack 3 with OWA using IIS
- Microsoft 2008 server
- PINsafe 3.7 or later

For version 2.0

- Microsoft Exchange 2007 service Pack 1 with OWA using IIS
- Microsoft 2003 server
- PINsafe 3.7 or later

402 Architecture

The Exchange server makes authentication requests against the PINsafe server by XML authentication

403 Installation

403.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be <ExchangeServerRoot>\ClientAccess\OWA

403.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

403.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use **8080** (**not 8443**)

Context: Swivel install name, for a Swivel virtual or hardware appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

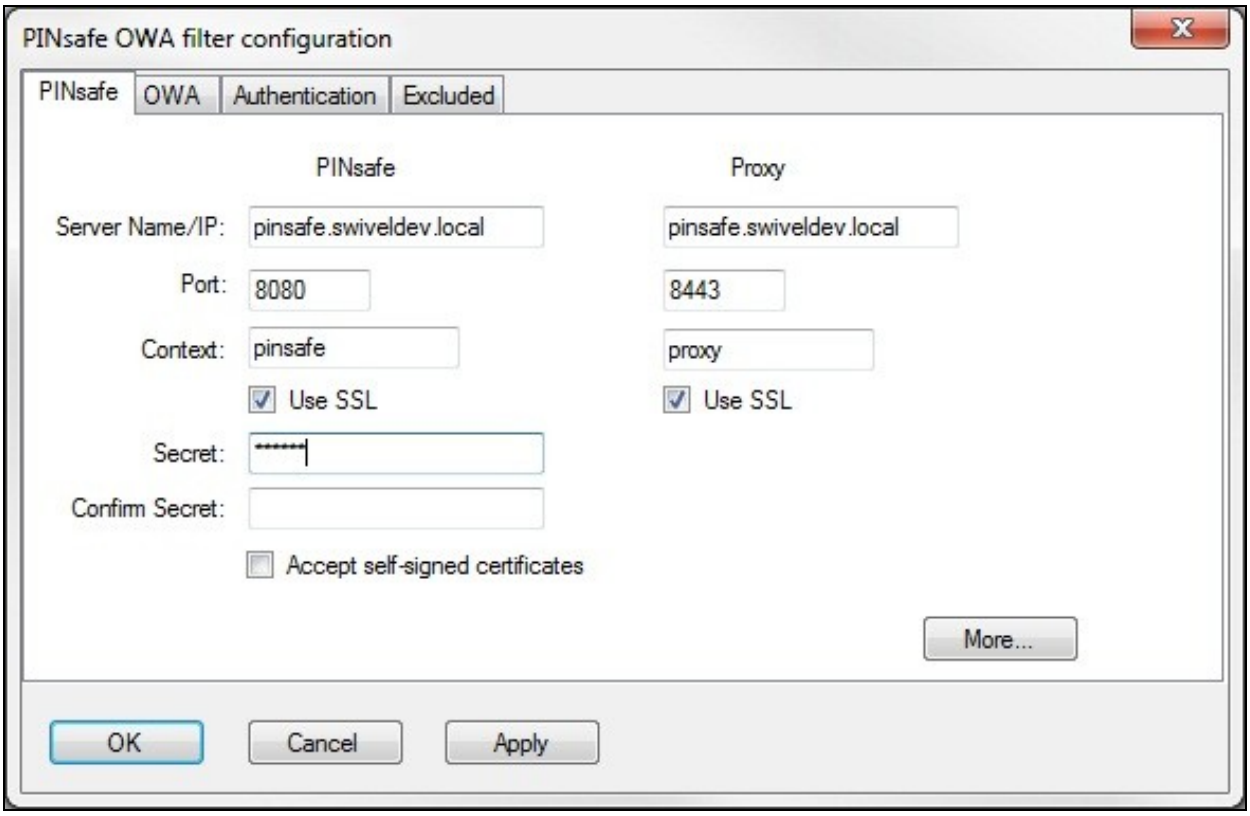
Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

Proxy Server These are used to retrieve TURing or PINpad images. If you are using a version of Swivel that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an virtual or hardware appliance, you MUST set them to be the same.

Proxy Port: Swivel server port, for a Swivel virtual or hardware appliance use **8443**

Proxy Context: Swivel install name, for a Swivel virtual or hardware appliance use proxy

Proxy Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.



403.2.2 OWA Settings

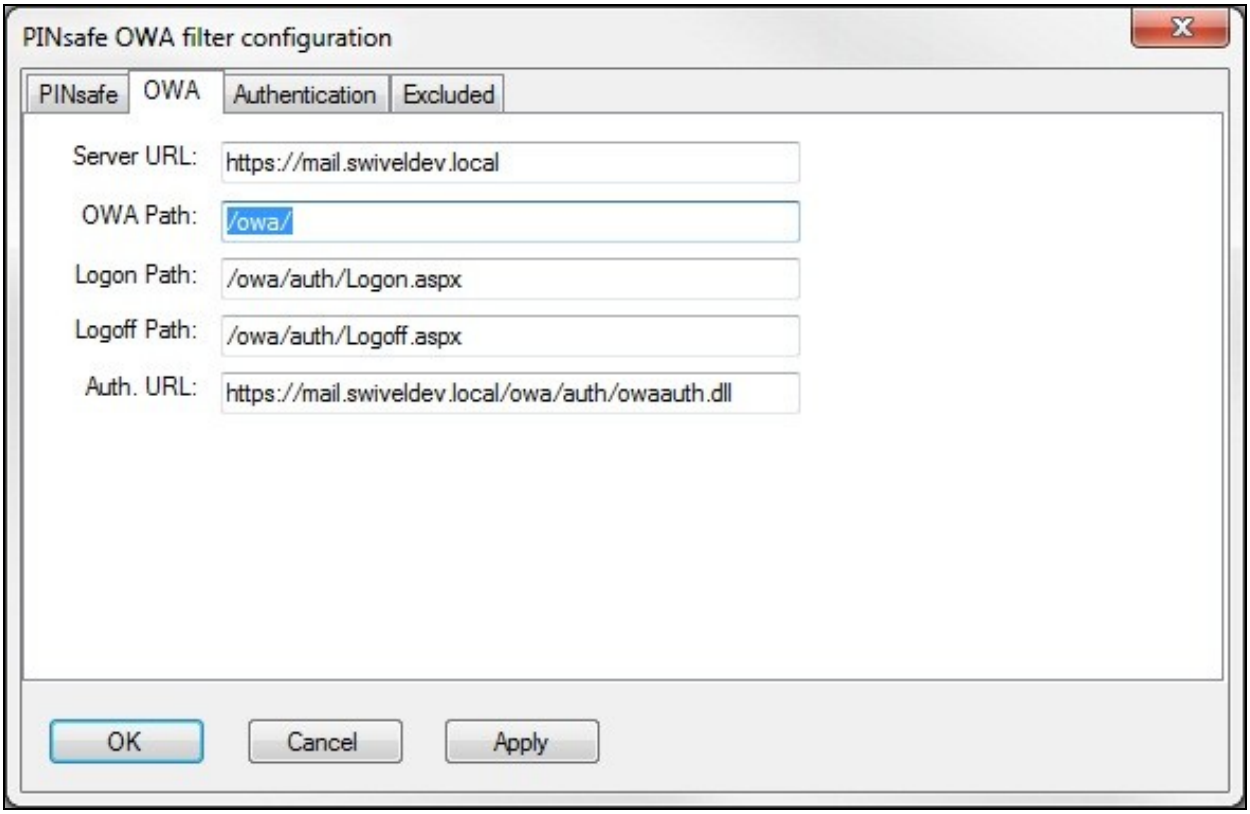
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/Logon.aspx

Logoff Path: Logoff path /owa/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll



403.2.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

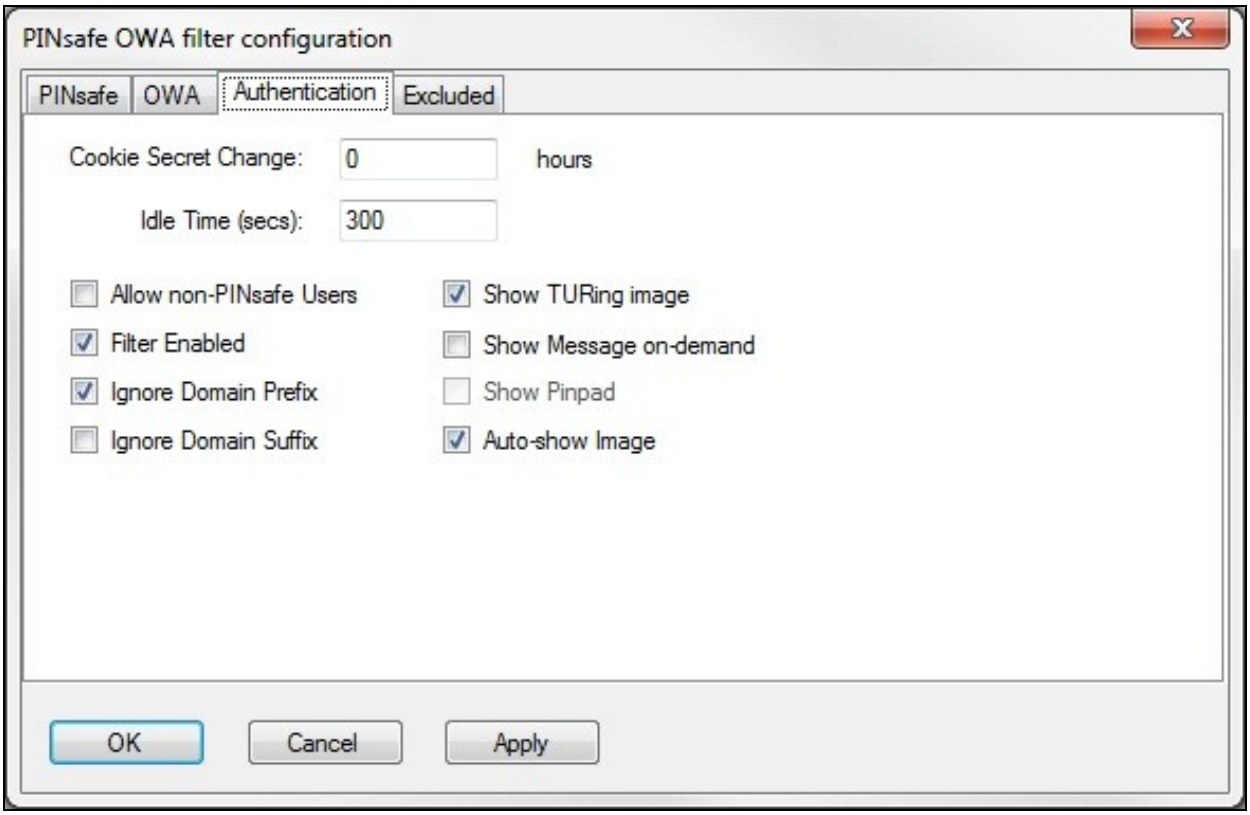
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

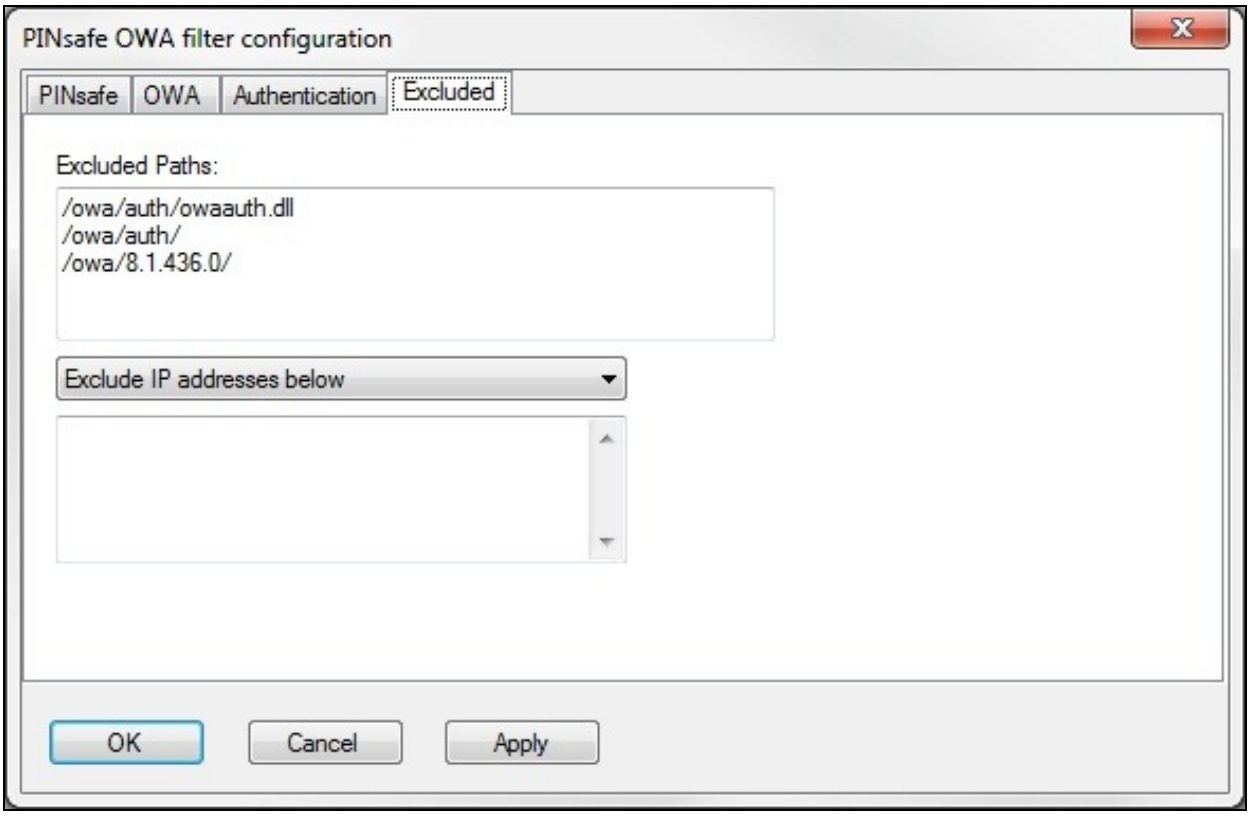
Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



403.2.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.



403.3 Configure The PINsafe Server

403.3.1 Configure a PINsafe Agent (For standard XML Authentication)

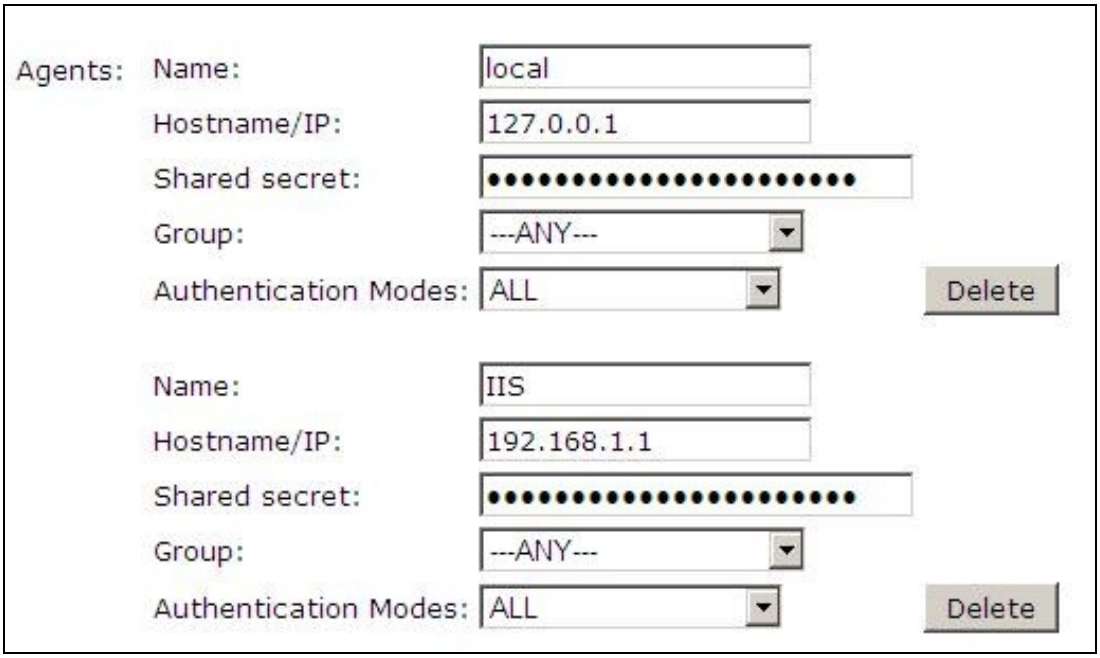
1. On the PINsafe Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the Exchange Filter

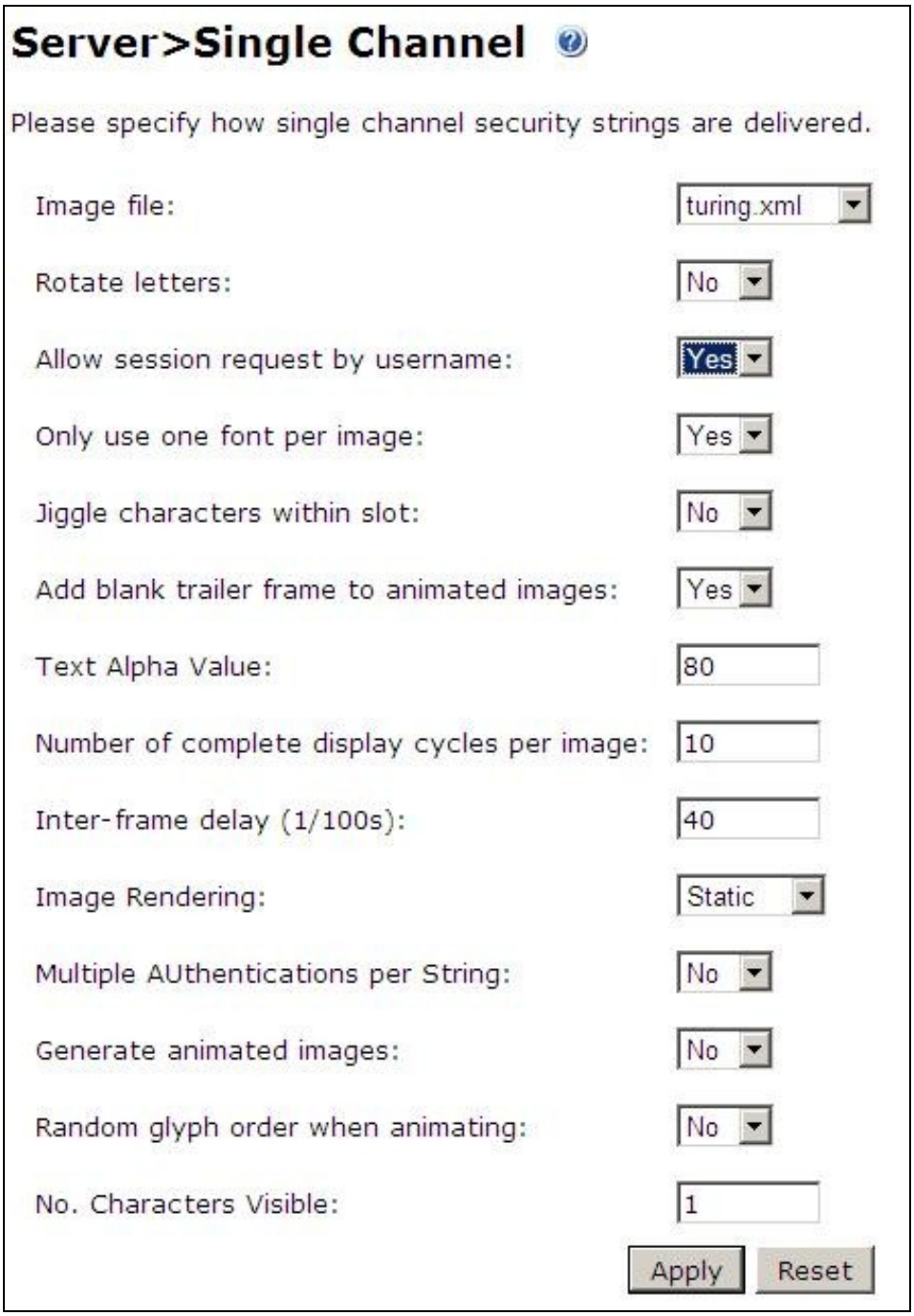
5. Click on Apply to save changes



403.3.2 Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



404 Additional Installation Options

404.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this section refers to earlier versions of the filter. In version 2.6 or later, this can be set using the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

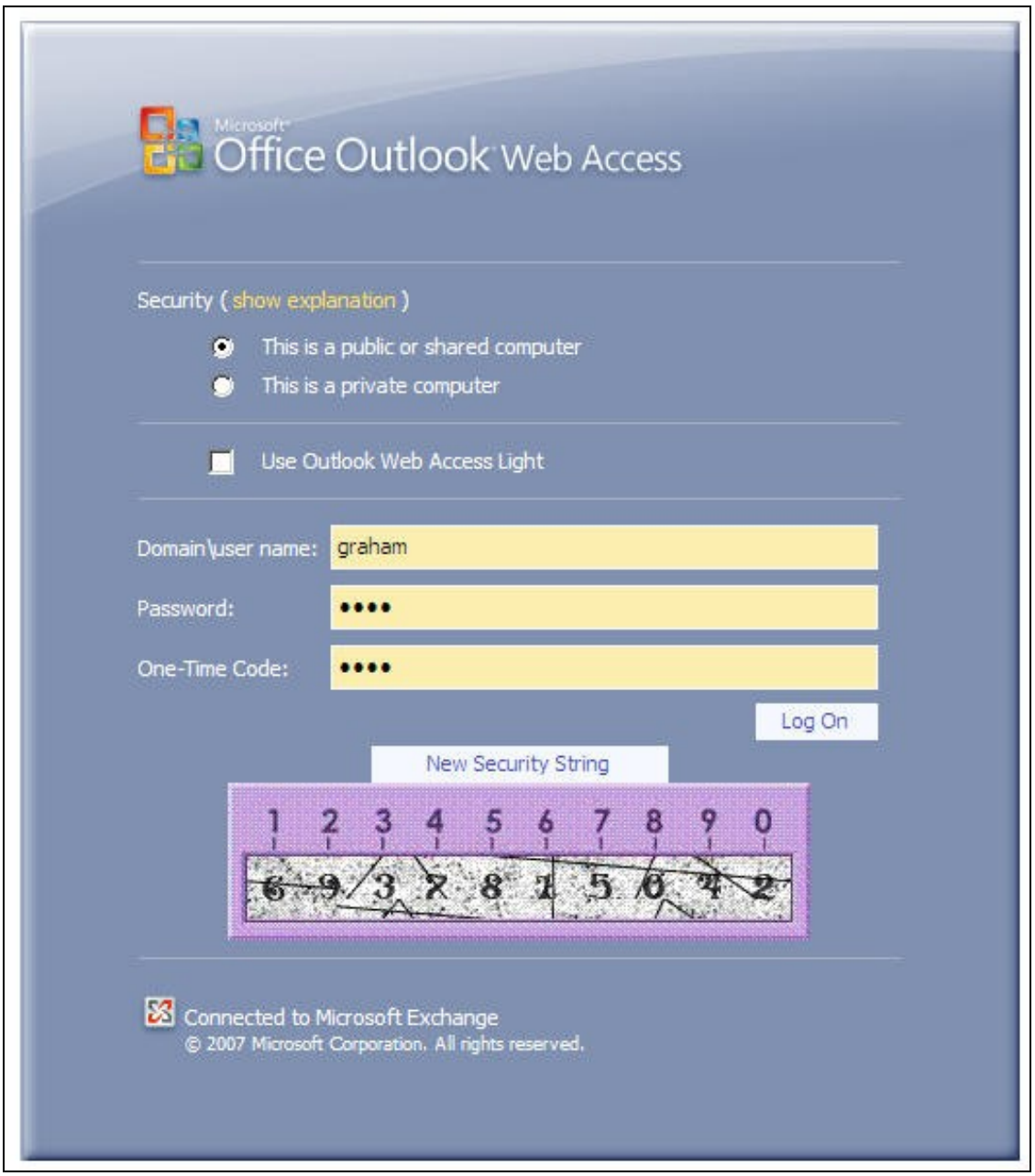
404.2 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

405 Verifying the Installation

Enter a username and AD password then the PINsafe OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

NOTE: if you have checked the option to allow non-PINsafe users, the OTC field and TURing button/image will not be displayed until you enter a username. If the username is not known to PINsafe, these elements will not appear. Similarly, if you have restricted the IP addresses to which PINsafe applies, the additional fields will not be displayed if PINsafe authentication is not required.



406 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in ClientAccess\owa\auth\, and renames the original to login.aspx.sav. To complete uninstallation this file must be copied back again.

407 Troubleshooting

Check the PINsafe and 2007 server logs

Logon page takes a long time to load. The first time the OWA modification is started, the PINsafe page may take a while to load.

No login page, check the Exchange version in <path to Exchange>\ClientAccess\Owa

Look for folders consisting of 4 numbers separated by dots, for example "8.3.213.0". The first number will always be "8" for OWA 2007. You will need to ensure that the highest such folder is included in the list of excluded paths. In version 2.6 or higher, this should be handled automatically.

In version 2.0 of the filter, the file login.aspx needs to be modified so that it references the correct exchange install version. A program to automatically modify the login page is here. In versions 2.3 and higher, logon page modification is automatic.

1. Unzip and copy to <path to Exchange>\ClientAccess\Owa\auth.

2. Rename logon.aspx logon.aspx.current, rename logon.aspx.bk logon.aspx.

3. Open a command prompt and change directory to <path to Exchange>\ClientAccess\Owa\auth and run the OWAModifyLogonfor IIS program from in command line specifying logon.aspx i.e. *OWAModifylogonforIIS.exe logon.aspx*. If the option to allow authentication for non PINsafe users is being used then use the option switch *true*, e.g. *OWAModifylogonforIIS.exe logon.aspx true*. Using the option switch *false* will stop non PINsafe user authentication.

4. Check the file has been modified by the datestamp which should have changed for logon.aspx.

5. On the PINsafe IIS Filter Update the PINsafe filter under the Excluded path using the highest OWA version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Blank page after an authentication. A login page may be displayed on the Exchange server. Verify the settings on the PINsafe filter point to the DNS name:

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

Auth. URL: This is the URL for OWA authentication and the is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

407.1 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Note that because of security restrictions in OWA, the OWA server must be referred to by name, not by IP address, and the SSL certificate must be valid, and must be for the named host.

408 Known Issues and Limitations

Updates to the OWA 2007 server may require changes to the Excluded paths. You will also probably need to reapply the logon page changes.

If you wish to use the PINsafe filter with dual channel authentication, on demand or in advance, the logon page will need to be manually modified. Please contact Swivel support (support@swivelsecure.com) for more information.

409 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

410 Microsoft OWA 2010 IIS Integration

411 Introduction

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2010 with Microsoft Exchange Server running on Microsoft 2008 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2010.

412 Compatibility

Microsoft Exchange Version and update release	Build Version	Compatibility Status
Exchange Server 2010	14.0.639.21	Compatible (old release only)
Exchange Server 2010 SP1	14.1.218.15	Compatible
Update Rollup 1 for Exchange Server 2010 SP1	14.1.255.2	Compatible
Update Rollup 2 for Exchange Server 2010 SP1	14.1.270.1	Compatible
Update Rollup 3 for Exchange Server 2010 SP1	14.1.289.7	Compatible
Update Rollup 4 for Exchange Server 2010 SP1	14.1.323.6	Compatible
Update Rollup 5 for Exchange Server 2010 SP1	14.1.339.1	TBC
Update Rollup 6 for Exchange Server 2010 SP1	14.1.355.2	Compatible
Update Rollup 7 for Exchange Server 2010 SP1	14.1.421.2	Compatible
Exchange Server 2010 SP2	14.2.247.5	Compatible
Update Rollup 1 for Exchange Server 2010 SP2	14.2.283.3	TBC
Update Rollup 2 for Exchange Server 2010 SP2	14.2.298.4	TBC
Update Rollup 3 for Exchange Server 2010 SP2	14.2.309.2	TBC
Update Rollup 4 for Exchange Server 2010 SP2	14.2.318.4	TBC
Update Rollup 5 for Exchange Server 2010 SP2	14.2.328.5	Compatible
Update Rollup 5-v2 for Exchange Server 2010 SP2	14.2.328.10	Compatible
Update Rollup 6 for Exchange Server 2010 SP2	14.2.342.3	Compatible
Exchange Server 2010 SP3	14.3.123.3	Compatible
Update Rollup 7 for Exchange Server 2010 SP3	14.3.210.2	Compatible
Update Rollup 8 (v2) for Exchange Server 2010 SP3	14.3.224.2	Compatible

Note: Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2010 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues and Limitations** sections before updating.

413 Prerequisites

- Microsoft Exchange 2010 with OWA using IIS7
- Microsoft 2008 Server
- Swivel version 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

The following is the latest release. Use this unless you have no Exchange service packs installed, in which case you need to use the older version, below. If you need a copy of an intermediate release for any reason, please contact support@swivelsecure.com.

413.1 Additional Prerequisites for Version 2.9

- Swivel Appliance version 3
- Microsoft .Net Framework 4.5 or later

NOTE: See notes below for additional installation requirements. Because of these additional requirements, it is recommended that you only upgrade to version 2.9 if you have a version 3 Swivel appliance.

414 File Downloads

Download links:

- Version 2.8
- Version 2.9

414.1 OWA Filter Change History

Recent changes:

- 2.9.0
  - Support for TLS 1.1 and 1.2. See notes below for additional requirements.
- 2.8.6
  - "Reapply Logon Page Changes" also updates default exclusions.
- 2.8.5
  - Fixed so that "/" is treated as a domain delimiter.
- 2.8.4
  - Change PIN page modified to show one field at a time.
- 2.8.3
  - Added hidden option to use previous authentication method.
  - Prevent Pinpad sessions being cached.
- 2.8.2
  - Fixed problem with names containing apostrophes.
- 2.8.1
  - Now supports direct upgrading - no need to uninstall a previous version before installing the new one. This only applies to upgrading from version 2.7 or later.
  - Change PIN Pinpad page selection of OTC field made more intuitive
  - Fix for bug introduced by changes in 2.7.7 when not using alternative usernames
- 2.7.7
  - Allow alternative usernames to work with versions of Swivel prior to 3.10 - see below.
  - Fixed some issues with Change PIN using Pinpad
- 2.7.6
  - Fixed problems with public/private flag
  - Changed Pinpad login to use session ID rather than username
- 2.7.1
  - Uses a slightly different authentication mechanism, since some users have reported problems with version 2.6.

Version 2.6 - if the new authentication mechanism causes problems with earlier service packs.

(Older release for OWA 2010 no service pack)

415 Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

416 Installation

NOTE: it is only necessary (or indeed possible) to install on Microsoft Exchange Client Access Servers. No installation is required on back end servers.

416.1 Preparation for Installing Version 2.9

As noted above, you should only upgrade to version 2.9 if your Swivel appliance requires TLS 1.1 or 1.2, i.e. you have appliance version 3 or higher. Note that it is possible to enable support for TLS 1.0 on version 3 appliances, in order to support legacy applications, but for security reasons it is recommended that you do not do this.

Support for TLS protocol versions 1.1 and 1.2 require Microsoft.Net Framework version 4.5 or later and ASP.Net version 4.0. If your Microsoft Exchange server is running on Windows Server 2012 or later, you may already have this, but Server 2008 does not have the requsite .Net Framework installed by default.

Note that the following procedure will require that the Exchange web server is restarted, so a small amount of down time is expected.

Download and install the requisite framework from the Microsoft website, ensuring that ASP.Net support is enabled.

Open IIS manager, and go to Application Pools. Select each MSExchange... application pool, click Basic Settings and change the .Net Framework version to v4.0.30319 (the last number may be different).

Once you have updated all the MSExchange application pools to ASP.Net version 4, restart IIS.

416.2 Upgrading to Version 2.9

Version 2.9 uses a different installation mechanism from previous versions. For this reason, it is not possible to upgrade to 2.9 without uninstalling previous versions first. However, it is possible to keep the settings from the previous version as follows:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa\PINsafeConfig, locate and run ForceUninstall.exe as Administrator. If this program does not exist, you will need to use the alternative mechanism below. Type "yes" to confirm removal, then "n" to prevent the settings being removed. Note that this technique does not remove the program from Programs and Features. You should attempt to remove it from here also, and when you get a warning that the program cannot be removed, accept the option to remove it from the list.

If the ForceUninstall program does not exist, you can use the following manual method:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa, edit web.config. Search for "PINsafe settings". Copy everything from this line down to "End of PINsafe settings" into a new file and save it. Now uninstall as normal. After installing version 2.9, the configuration program will appear, with blank settings. Cancel this program, then edit web.config as before. You should have default settings for the Swivel filter installed. Remove these and replace with the saved settings. Now run the configuration program again and make any changes as necessary.

416.3 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be the root Exchange path.

NOTE: it is not necessary to uninstall the previous filter before installing version 2.7.x or 2.8.x, as long as the previous filter is version 2.7 or later.

416.4 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

416.4.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use 8080 (not 8443)

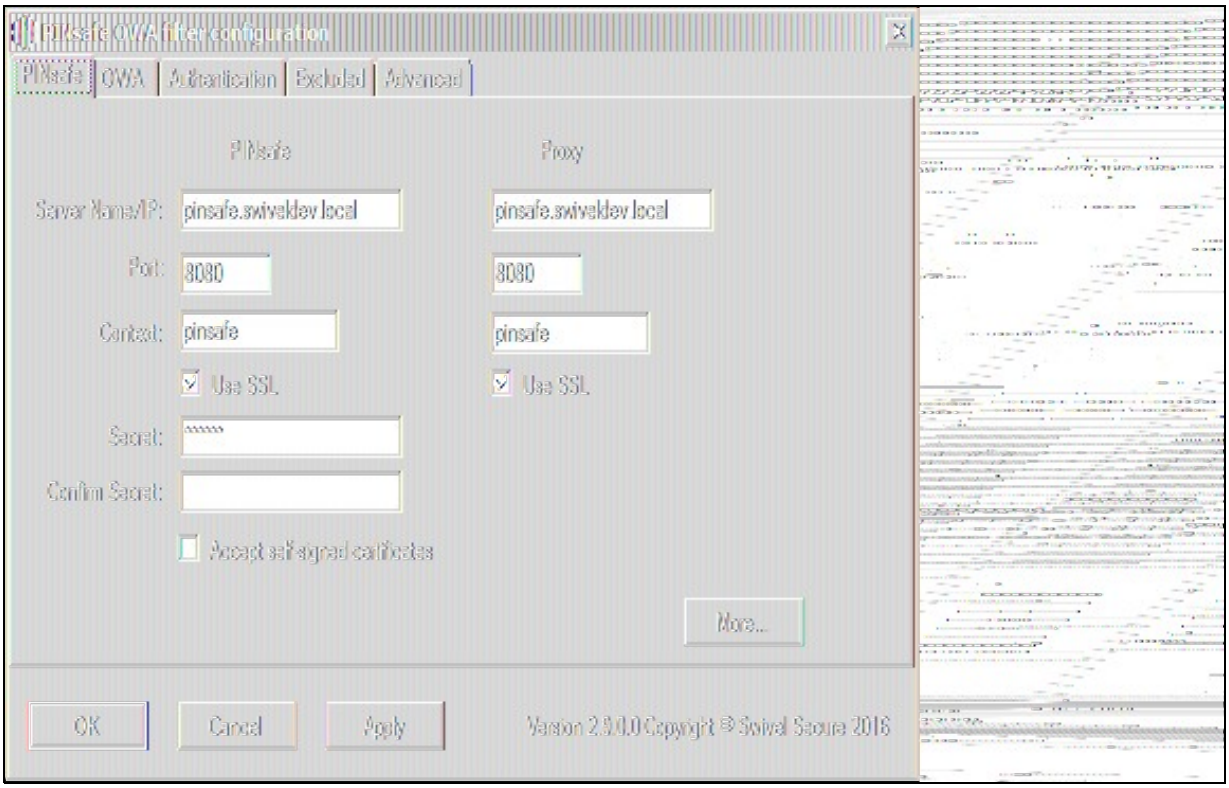
Context: Swivel install name, for a Swivel virtual or hardware appliance use pinsafe (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

Proxy Server, Port, Context, Use SSL These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using a virtual or hardware appliance, you MUST set them to be the same.



416.4.2 OWA Settings

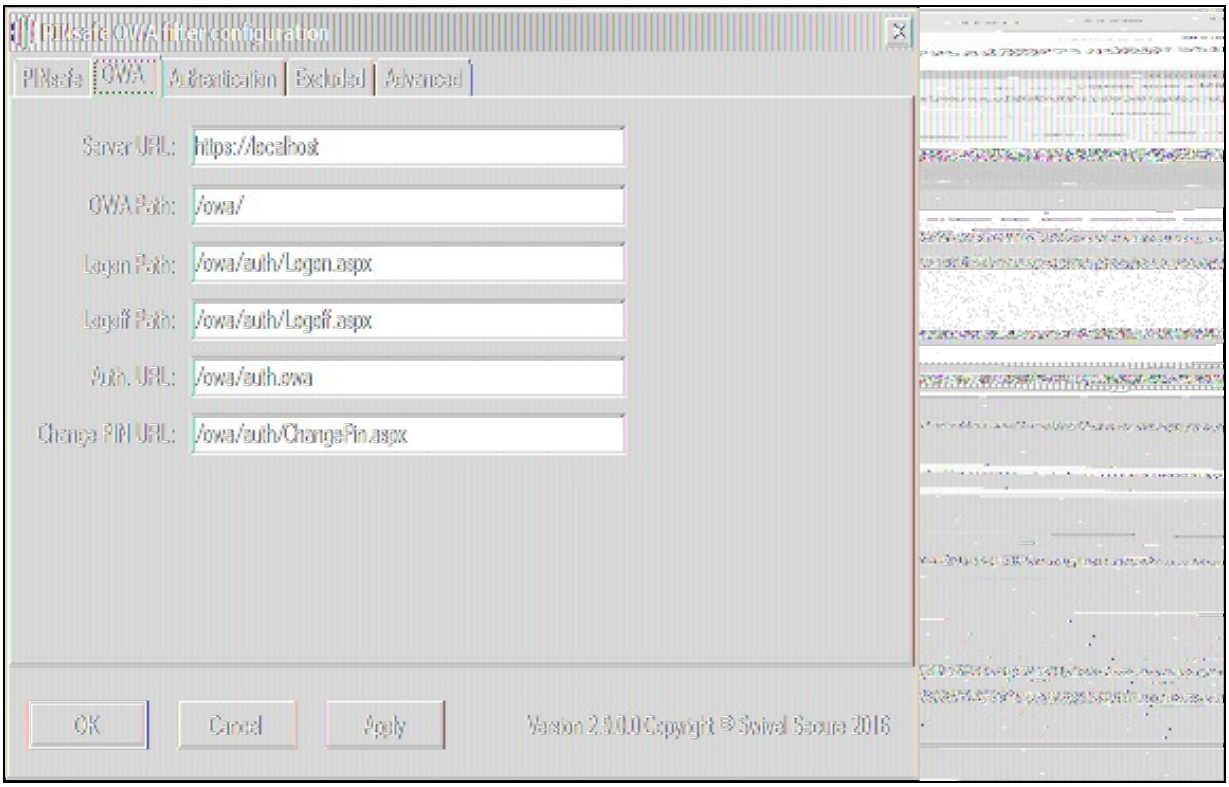
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/auth.owa



416.4.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

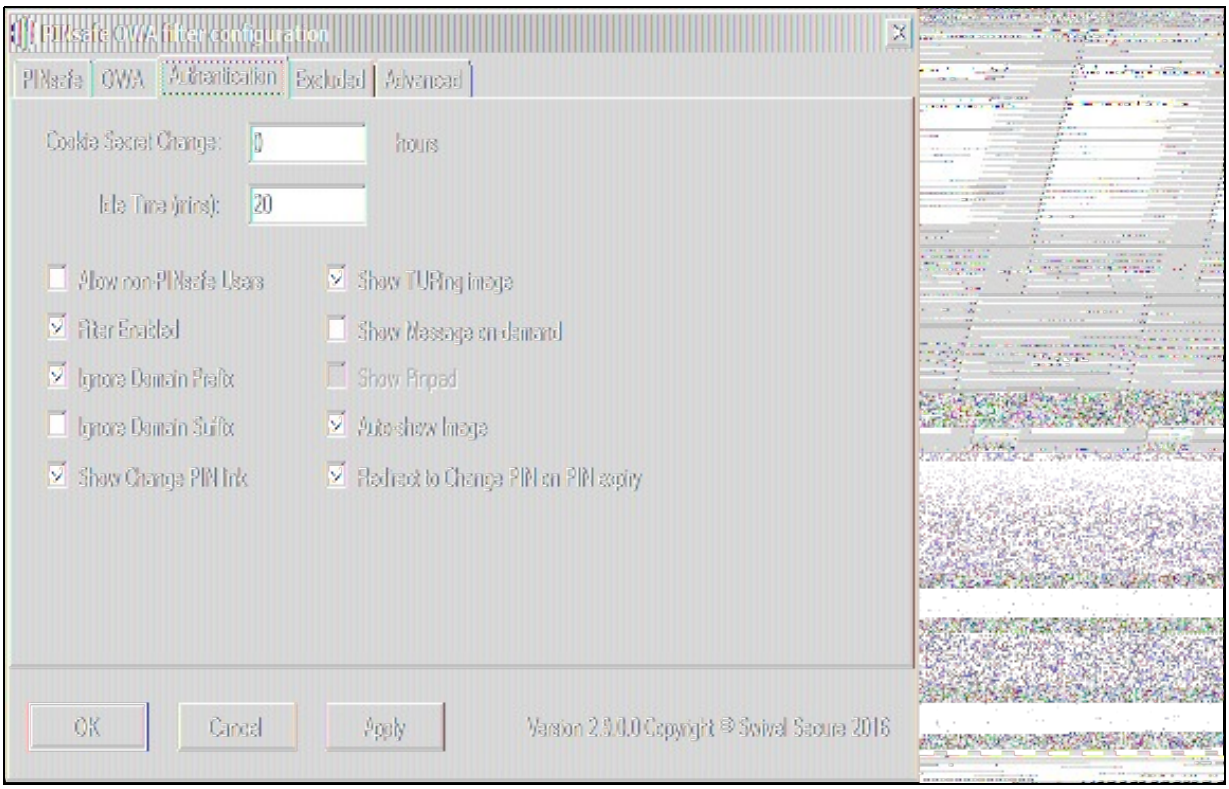
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

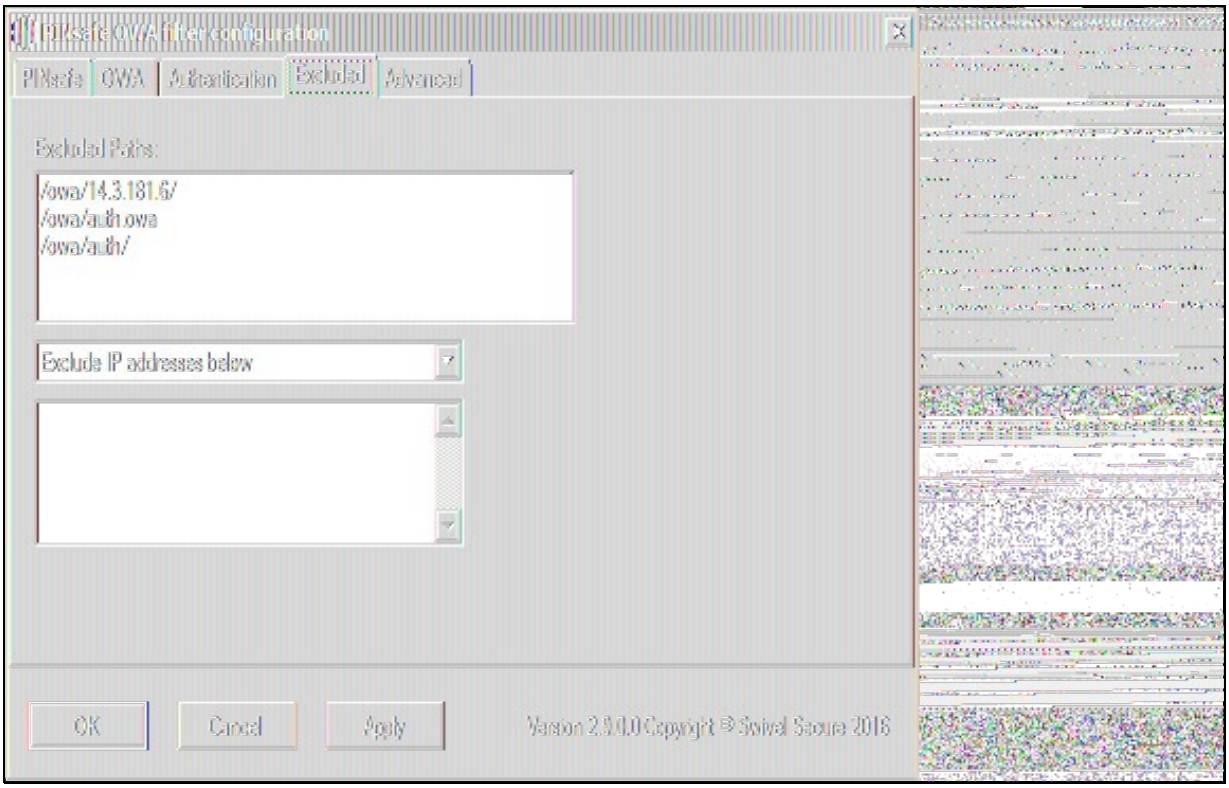
Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



416.4.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.



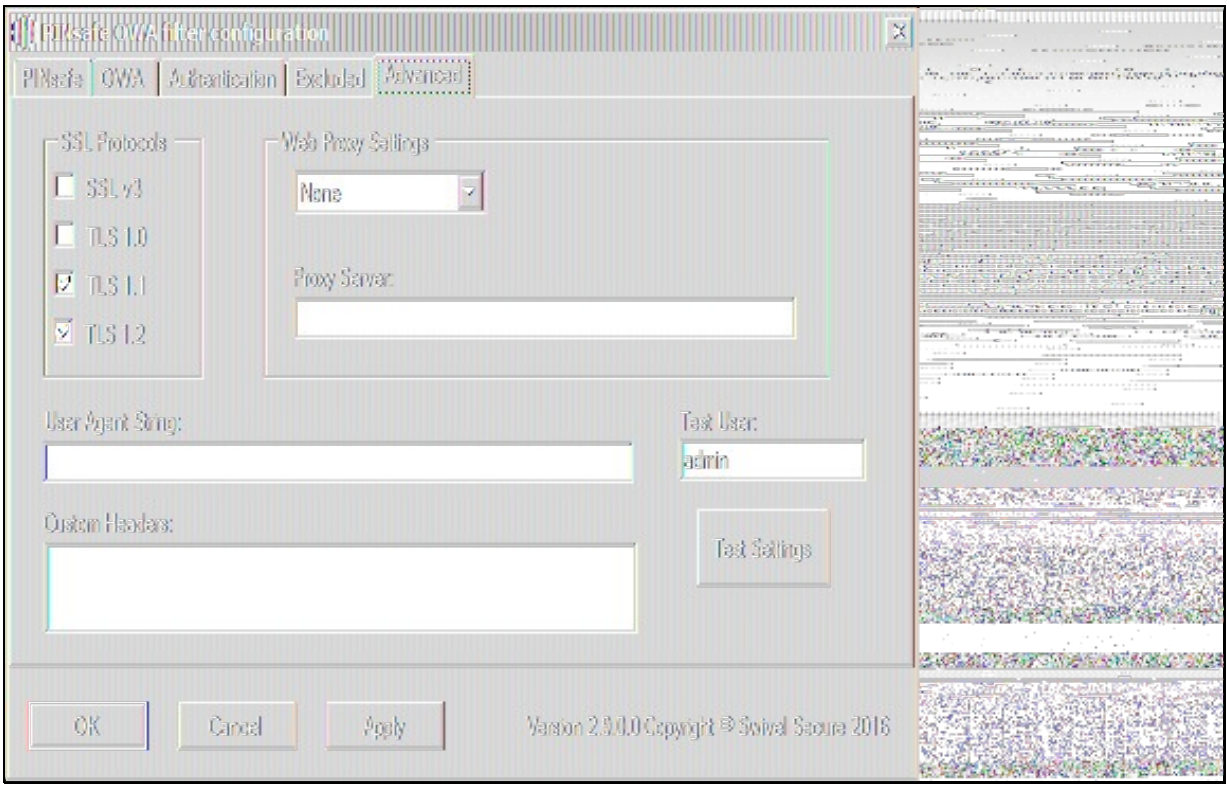
416.4.5 Advanced Settings

SSL Protocols: This indicates which protocols can be used for https communication with the Swivel server. The default allows SSLv3 and TLSv1, but the recommended setting for appliance version 3 is TLSv1.1 and TLSv1.2.

Web Proxy Settings: If the Exchange server needs to connect to a proxy server to access the Swivel server, you should specify the details here. Unless you are aware of such details, leave these as "None".

User Agent string: and **Custom headers:** These settings modify the http request sent to the Swivel server. Typically, you will not need to use these, but you may be aware of firewall rules between the servers which require such settings.

Test User: and **Test Settings** In order to test the settings, the configuration program will send a session start request on behalf of a user. You should enter a username that exists in the Swivel database (the default is 'admin'), then click Test Settings to confirm that the connection between the OWA Server and the Swivel server is correctly configured.



416.5 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

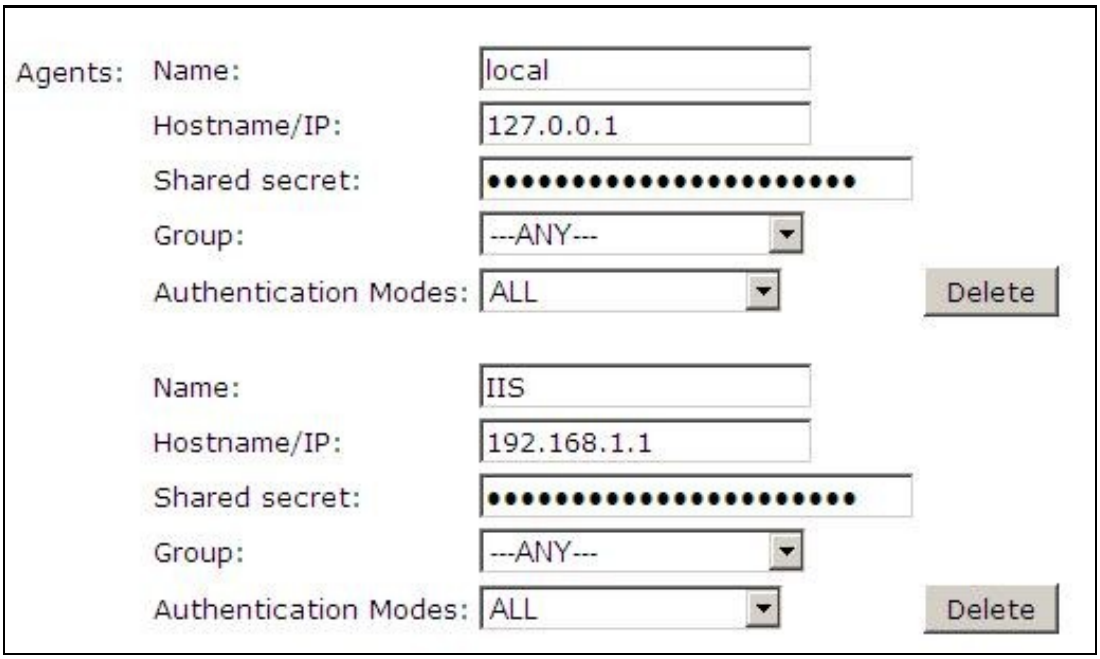
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the Exchange Filter

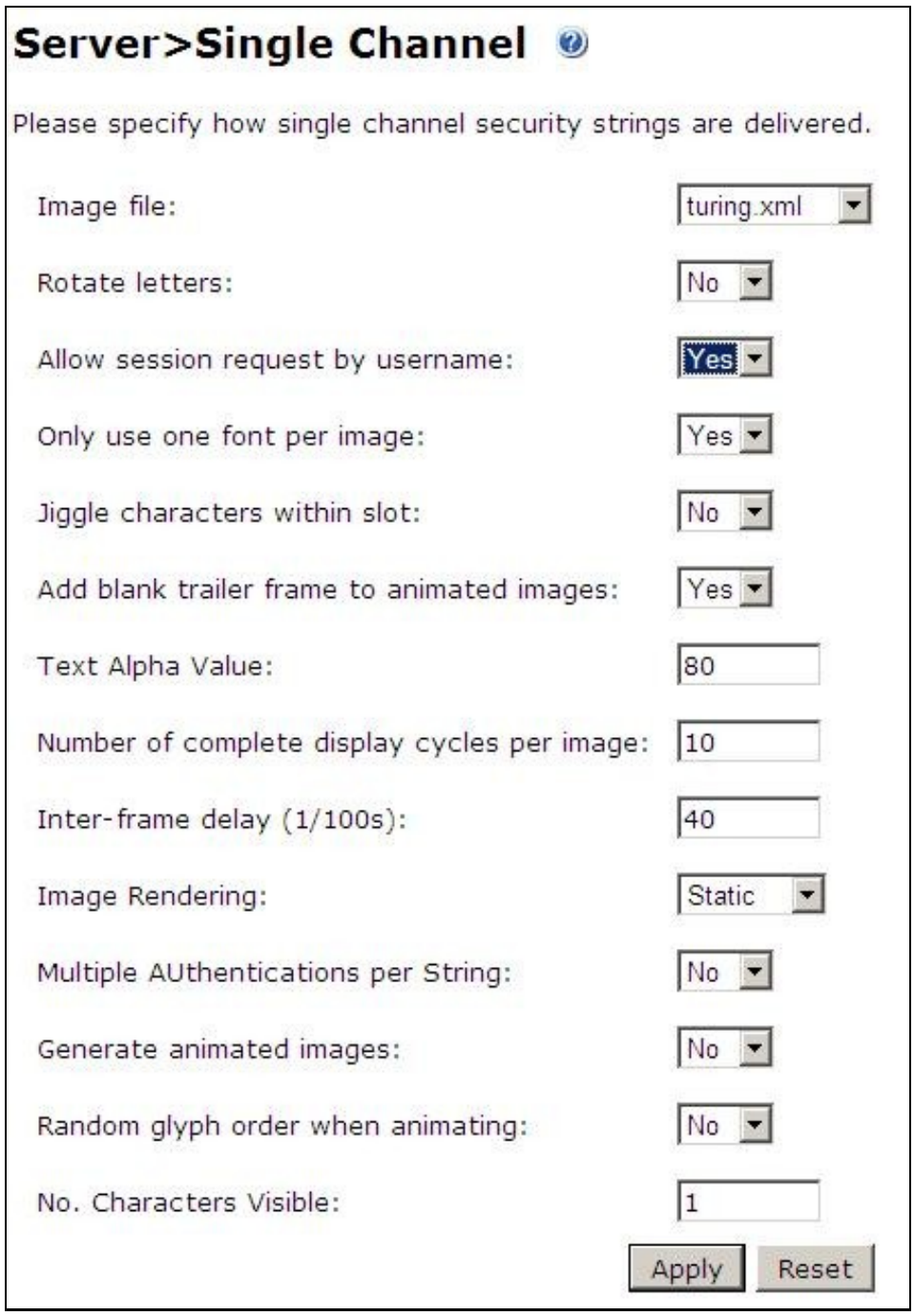
5. Click on Apply to save changes



Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



416.6 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

417 Additional Installation Options

417.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the Swivel server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

417.2 Modifying the login Page to allow Dual Channel On Demand Delivery

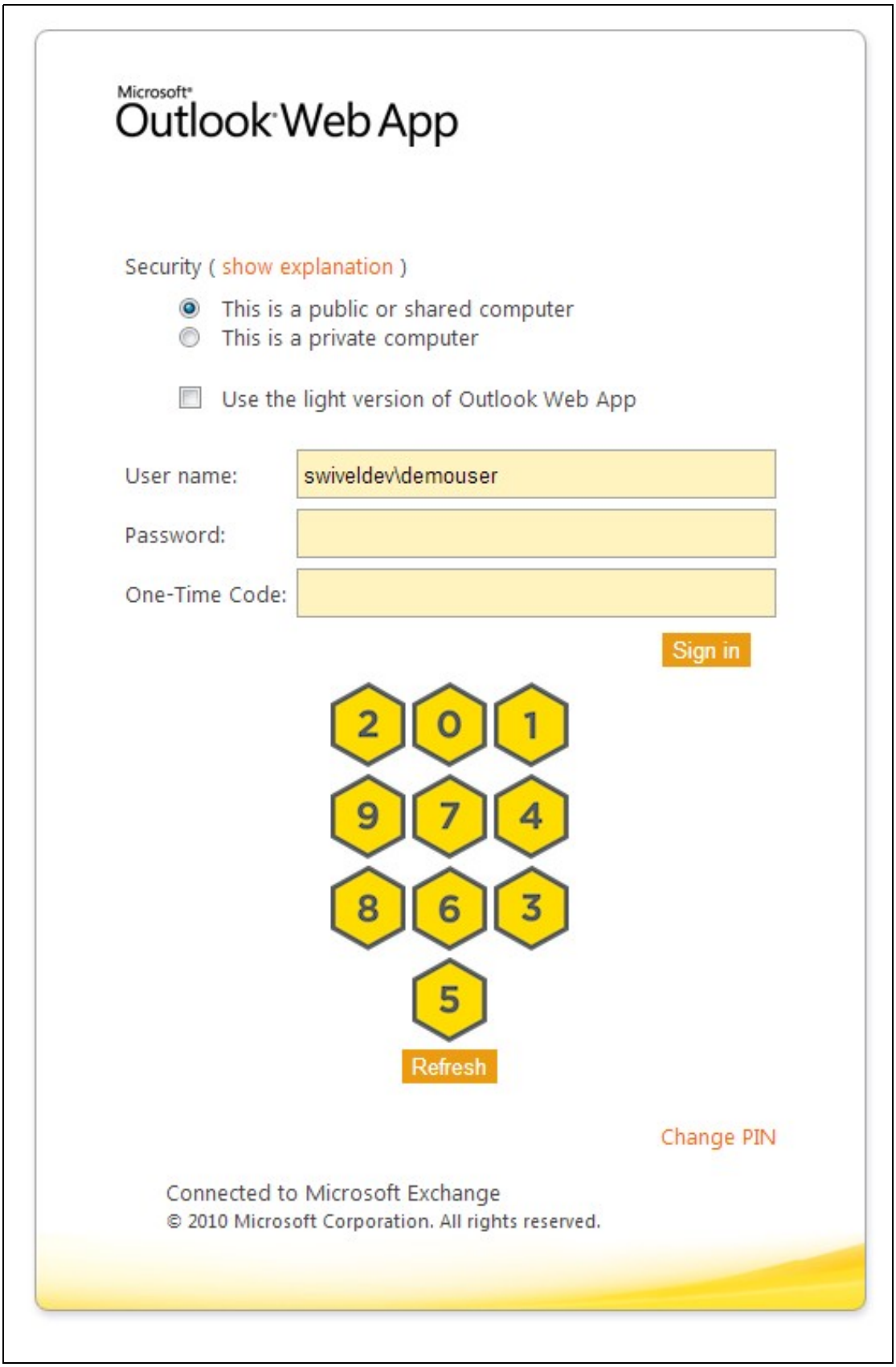
NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the Swivel Administration console under Server/Dual Channel.

418 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.



419 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in ClientAccess\owa\auth\ which can be restored to the original Login.aspx.

WARNING: In versions of the filter earlier than 2.5, the login page customisation program did not check if the customisation was already done. This could cause the file Logon.aspx.sav to be overwritten with a customised page. In this case, you will need to locate another copy of the original file, or contact support@swivelsecure.com for assistance.

419.1 Uninstalling Manually

NOTE: This procedure should only be undertaken if uninstalling using the menu option (or Programs and Features) fails. For safety, you are advised to make copies of all modified or removed files to a safe location outside the Exchange Server installation.

Firstly, locate the OWA folder. The default location for this is C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa.

Edit web.config in this folder: note that you may need to open your editor as Administrator in order to be able to change it. Search for the <modules> section. Within this, there should be a line such as the following:

```
<add type="com.swivelsecure.owafilter.PINsafeOWAFilter, PINsafeOWAFilter, Version=2.8.5.1, Culture=neutral, PublicKeyToken=xxxx" name="PINsa
```

The Version number and PublicKeyToken may vary. Remove this line, making sure not to remove anything else.

Locate the section beginning with

and ending with

Remove everything within this section. If you intend to reinstall the filter later, you might want to copy these settings somewhere for later reference. Alternatively, make a backup of the entire web.config.

Save the modified web.config.

Restart IIS to release the Swivel filter.

Delete the folder "PINsafeConfig" and all its contents.

Go into the "Bin" subfolder and delete the 3 DLLs beginning with "PINsafe": PINsafeClient.dll, PINsafeLogin.dll and PINsafeOWAFilter.dll.

Go into the "auth" subfolder and delete the following files:

- ChangePIN.aspx
- CheckClient.aspx
- CheckUser.aspx
- pinpadBlank.png
- pinpadClear.png
- pinpadNext.png
- pinpadPrev.png
- pinpadRefresh.png
- pinsafe.js
- pinsafe_cp.js
- PINsafeLogon.aspx
- SCImage.aspx
- SCPinpad.aspx
- SessionStart.aspx
- turingBlank.jpg
- Logon.aspx.old

Depending on which version of the filter you have, you may not have all of these files.

The final step is to restore the original logon page. You should have a file named Logon.aspx.sav. If this file does not exist, please contact support@swivelsecure.com for help. Delete the file Logon.aspx, and rename Logon.aspx.sav to Logon.aspx.

Now test that your OWA logon works without Swivel. Some older versions of the filter would apply the logon page modification multiple times, which means that Logon.aspx.sav also had the Swivel modifications. If you find that the Logon page still has Swivel modifications, then please contact support@swivelsecure.com to request advice on restoring the original Logon page.

420 Change PIN

The OWA filter includes a page for the user to change their PIN. It can be configured to redirect to the change PIN page automatically if the user's PIN has expired, and you can also include a link to the Change PIN page on the login page.

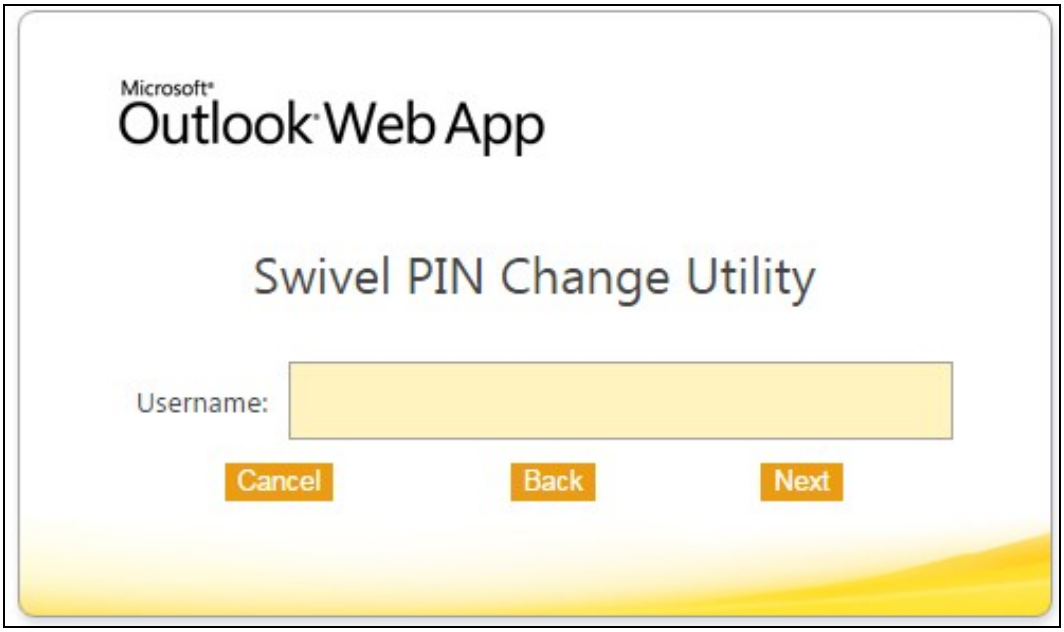
If you selected the Change PIN page in error, and want to return to the login page, then click the "Cancel" button ("Skip" button before 2.8.4) to return without changing your PIN.

NOTE: from version 2.8.4 onwards, the fields are shown one at a time. Click "Next" or press Tab to show the next field, or "Back" to go back and correct a field. See the Pinpad section below for example screen shots.

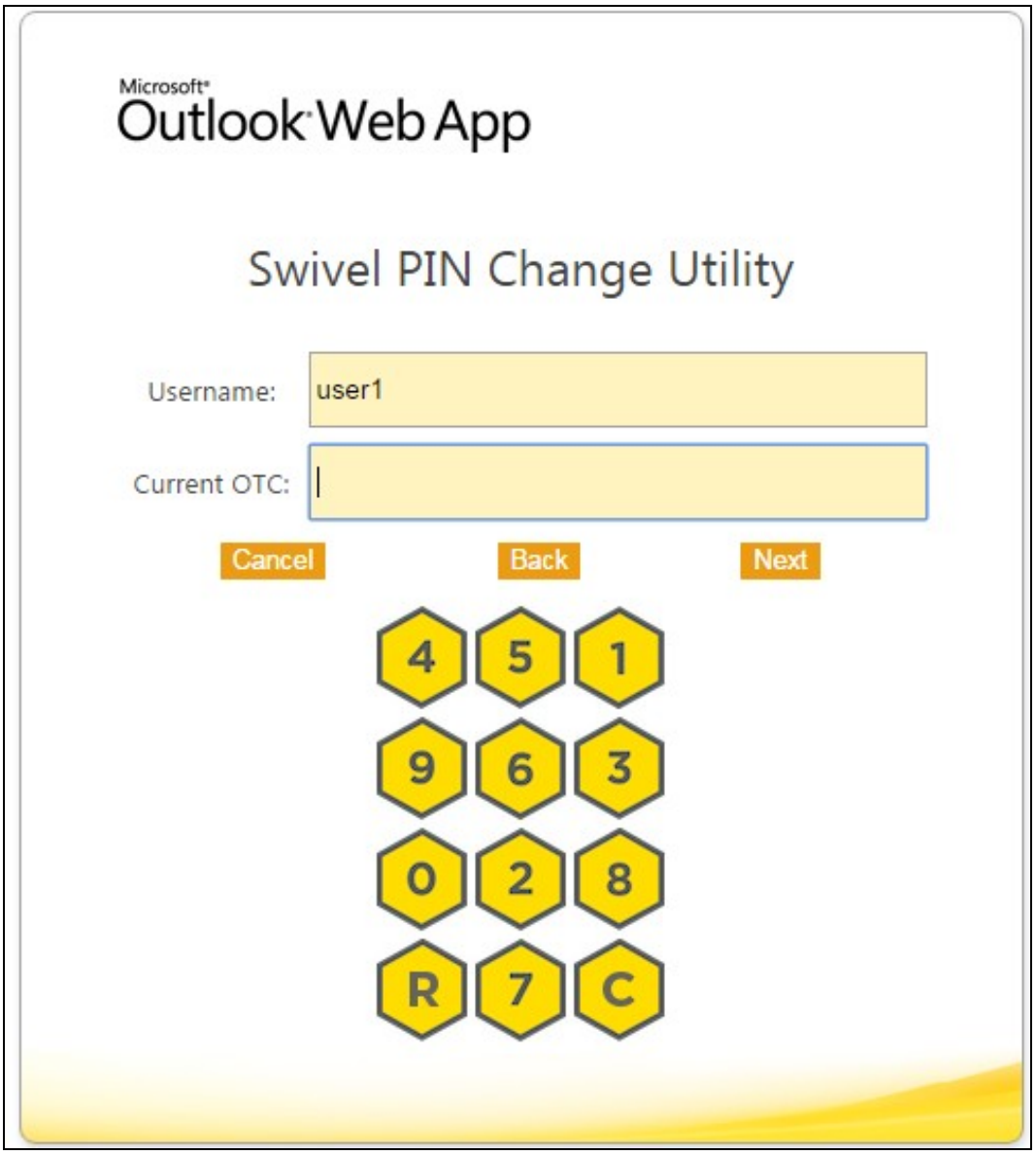
420.1 Change PIN with PinPad

The following instructions refer to the Change PIN page from version 2.8.4 onwards. See the following section for older versions.

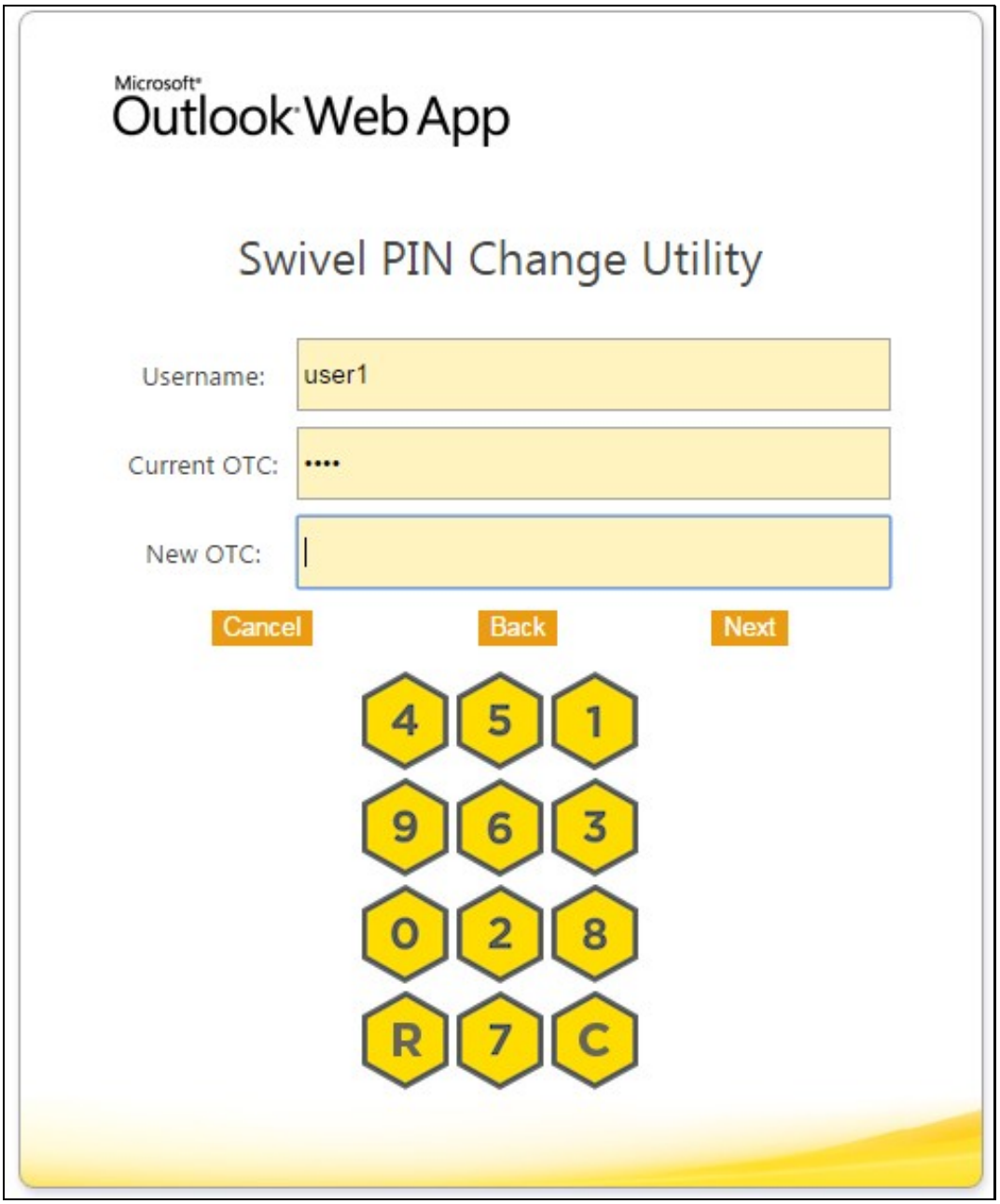
The initial screen (with or without Pinpad) looks like this:



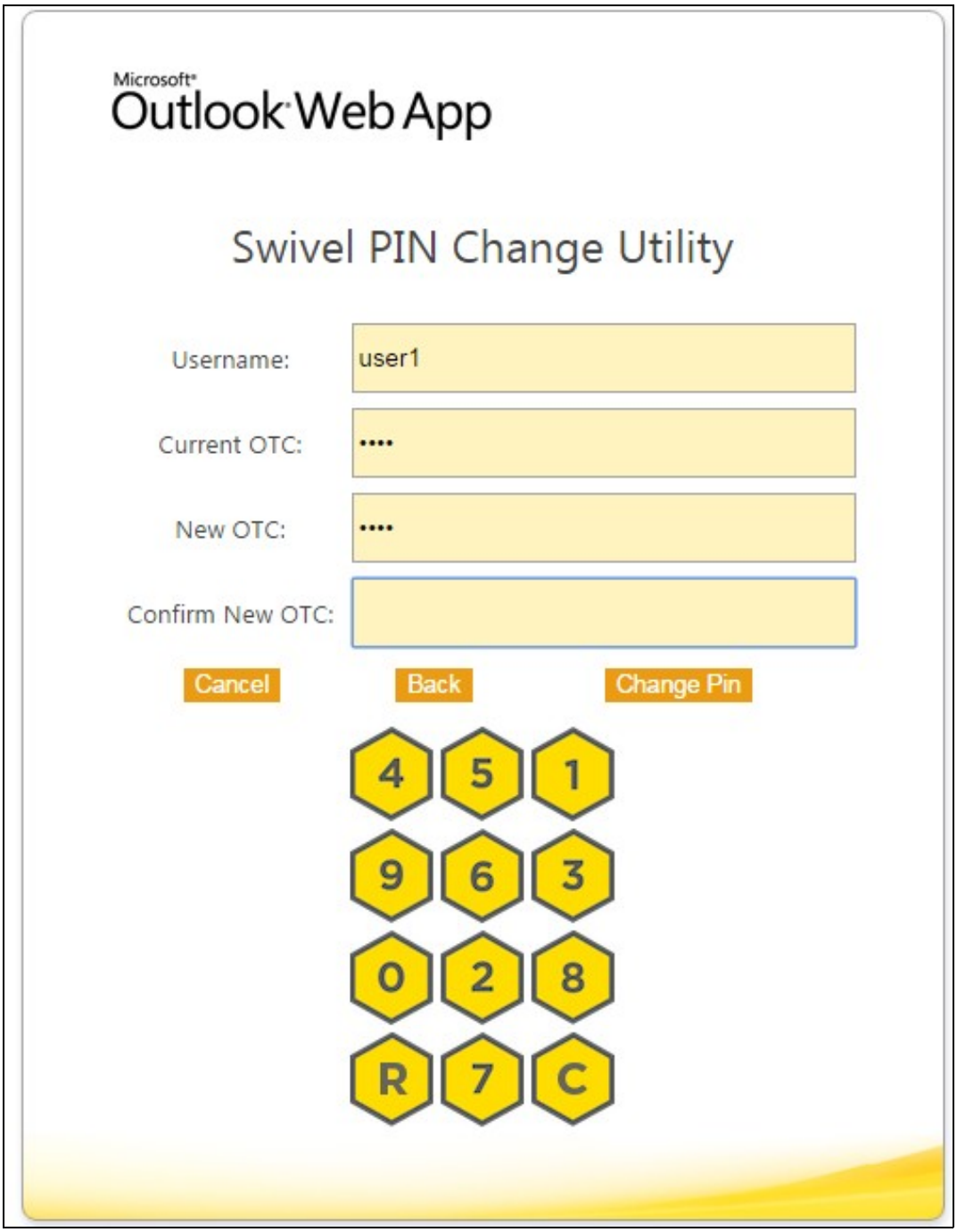
Enter your username and click "Next" or press Tab to show the next field and the Pinpad:



Click the buttons corresponding to the digits of your current PIN and then "Next":



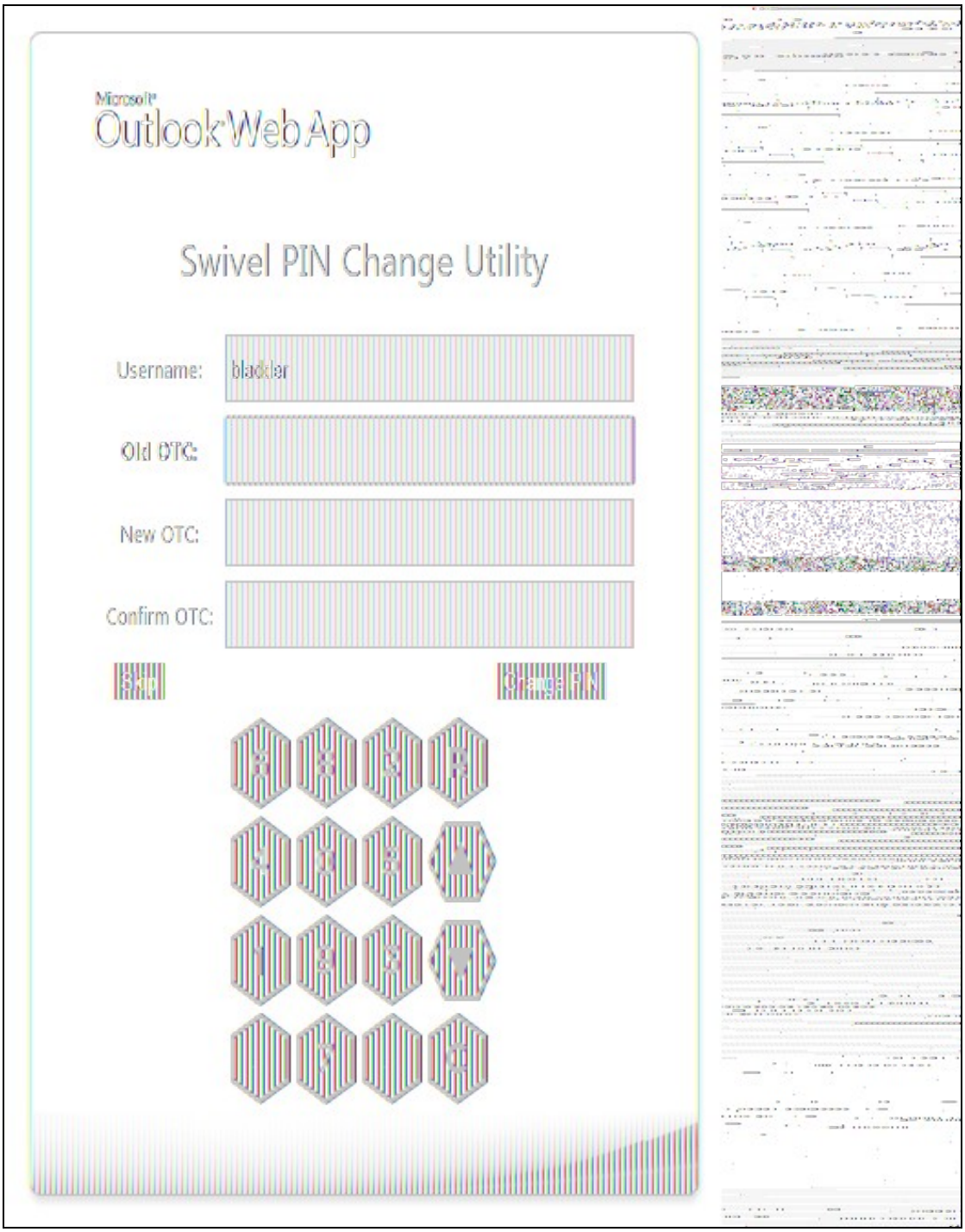
Click the buttons corresponding to the digits of your new PIN and then "Next":



Enter your new PIN again, to confirm, and then click "Change Pin".

420.1.1 PinPad prior to Version 2.8.4

When PinPad is enabled, there are 3 OTC fields, all of which can potentially use the Pinpad. For this reason, additional buttons are provided to select the field which is the target of the Pinpad:



You will notice that the current OTC field is highlighted in green. To select the next field, click on the down arrow button, or to go back to the previous field, click the up arrow button. You can also select an OTC field simply by clicking on it, or its label.

The "R" button will refresh the Pinpad (i.e. show a new pad), and the "C" button will clear the selected OTC field.

421 Troubleshooting

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

421.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v14\ClientAccess\OWA\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

421.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

421.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

421.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

NOTE: Version 2.7 or later of the filter should eliminate most of these problems. If you are still having problems of this nature with 2.7, please contact support@swivelsecure.com.

421.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

Again, this problem is no longer relevant in version 2.7 onwards.

422 Known Issues and Limitations

422.1 Known Issues with Version 2.9

It has been observed that the first time the website is accessed after installing the 2.9 filter, an error page is seen. This disappears after refreshing the page, and does not appear to recur.

422.1.1 Problems With Connection Settings

We have experienced problems with installations of the filter when Exchange 2010 is installed on Windows Server 2012, or when certain security updates are installed in Windows Server 2008. While the exact cause is not yet known, it seems to be related to SSL connection settings. We have found success in making adjustments to the SSL settings and User Agent string.

There is a beta release of version 2.8.7 available from here which allows you to adjust these settings.

422.1.2 Default Exclusions Not Applied

There is a known issue with versions up to 2.8.5 that if you apply an update to Exchange that causes the Exchange version number to change, the folder containing the latest version of images etc. is not automatically added to the list of exclusions. Even though it is shown in the configuration program, it isn't saved.

The recommended solution is to update to 2.8.6. Here, if you reapply the logon changes after an update, it will also update the version-specific inclusions.

The workaround for this is to alter another configuration item, then save the configuration. You can subsequently change the other item back again, but making another change will force the exclusions to be updated.

422.1.3 One-time Code Not Shown

There is a known issue if you are using the option to allow unknown users to log on without Swivel credentials. With certain versions of the core, users are not recognised, even though they are known to exist in the Swivel database.

Another problem, Swivel may not recognise email addresses if the Swivel username is not the email address.

Both of these problems can be resolved by the same solution: you need to use a hidden option:

Edit the OWA web.config file (by default in C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa). Note that you will probably need to open your text editor as Administrator in order to save changes.

Locate the following line:

<add key="PINsafeMultiUsername" value="False" />

If the above line is found, change value to "True".

If you cannot find the above line, search for

Insert the following line before the above line:

<add key="PINsafeMultiUsername" value="True" />

Note that this option will not work with versions of PINsafe earlier than 3.8.

422.1.4 Private Computer Option Doesn't Stay Selected

If your login page always defaults to Public computer and you have to select Private every time you log in, please upgrade to the latest version of the filter.

422.1.5 Swivel Customisation Lost

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. IMPORTANT: in versions earlier than 2.5, make sure you do not use this option on a page that has already been customised. This will cause the page to become corrupted, and will also overwrite the backed up, unmodified file.

Updates to the 2010 server may also require changes to the Excluded paths. In version 2.8.6 or later, running "Reapply Logon Page Changes" fixes this too. In version 2.5 or later, the updates are handled by the configuration program, but if you do not change any other settings, the update will not be applied.

422.1.6 Later Versions of the Filter Not Working With Service Pack 1

We have had reports of the latest filter not working with Exchange Server Service Pack 1. The recommended solution is to upgrade to the latest service pack, but you might like to try the following (version 2.8.3 or later):

Insert the following line in web.config (see description above):

<add key="PINsafeUseOldAuthentication" value="True" />

This option reverts to the authentication mechanism used in version 2.6 and earlier. It is not known whether this is the cause of the problems seen, but it has been shown to work in some installations.

422.1.7 Logging

By default, the filter does not record any audit information, but it may be useful to do so for monitoring and debugging purposes. You can enable logging by adding the following line in web.config:

<add key="PINsafeEnableDebug" value="True" />

This writes logs to C:\Users\Public\Documents\PINsafeOWAFilter.log. You can change the file location with the following option:

<add key="PINsafeDebugLocation" value="FullFilePath" />

Replace *FullFilePath* above with the full path of the file to write to. Make sure that the account that OWA is running as has write permissions to that file/folder. </nowiki>

423 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

424 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.

425 Microsoft OWA 2013 IIS Integration

426 Introduction

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2013 with Microsoft Exchange Server running on Microsoft 2012 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2013.

So far as the Swivel integration is concerned, there are no significant differences between OWA 2013 and 2016 or 2019. Therefore, the OWA 2013 filter should work with OWA 2016 and 2019 as well.

427 Compatibility

Microsoft Exchange Version and update release	Build Version	Compatibility Status
Exchange Server 2013	15.0.516.32	Compatible
Exchange Server 2013 CU 3	15.0.775.38	Compatible
Exchange Server 2016	15.1.225.42	Compatible
Exchange Server 2019	15.2.858.5	Compatible

Note: Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2013 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues and Limitations** sections before updating.

428 Prerequisites

- Microsoft Exchange 2013 or 2016 with OWA
- Microsoft 2012 Server R2
- Microsoft.Net Framework version 4.5
- Swivel 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- * As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

NOTE: above is the test environment used for the filter. It will probably work with earlier versions of the Operating System (e.g. 2008), as long as version 4.5 of the .Net framework is installed.

429 File Downloads

- Version 2.12. Changes:
  - Settings are retained on upgrade of this product or of OWA: the settings are now saved to a location outside the OWA folder (C:\ProgramData\Swivel Secure\OWA Filter). Note that this doesn't apply to upgrade from a version earlier than 2.12.
  - Support for logging within the configuration program. Logs are written to C:\ProgramData\Swivel Secure\OWA Filter.
  - Version 2.12.3 ensure that data folder exists before trying to read from it.
  - Version 2.12.2: Bug in program to re-apply logon page changes after OWA upgrade now fixed.
  - Version 2.12.2: control over which attributes are checked for unknown users
  - Version 2.12.2: more control over logging
  - Version 2.12.2: fixed issue with Cookie encryption
- Version 2.11. The main change here is support for Push authentication. Due to technical issues, this version is available from a server that does not have https support. For this reason, you cannot simply click on the link in most browsers. Instead, you must right-click on it, copy the link address and open it in a new tab.
- Version 2.10. This is largely a rebranding of version 2.9. It also uses default settings that are more relevant for newer versions of Sentry, and references OWA 2016 and 2019. One notable change is that the reference to proxy server has been removed, as it is no longer necessary.

NOTE: We apologise that the original installer for version 2.10 was missing a file. This has now been corrected, but if you installed the original version and don't want to reinstall, you can simply unzip ChangePIN.aspx and place it in the swivel folder of the OWA web site. The usual location for this is C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\swivel.

- Version 2.9. This version includes support for TLS version 1.1 and 1.2. It is only necessary to upgrade to this version if you have a Swivel appliance version 3. Version 2 appliances work fine with version 2.8, and no other new features have been added.
- Version 2.8.7. Some minor updates copied from OWA 2010 filter, plus bug fix for images not displaying in certain circumstances. Now supports upgrading without uninstalling.

430 Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

431 Installation

431.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V15), you will need to modify the installation path. The installation path should be the root Exchange path.

431.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

431.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel appliance use 8080 (not 8443)

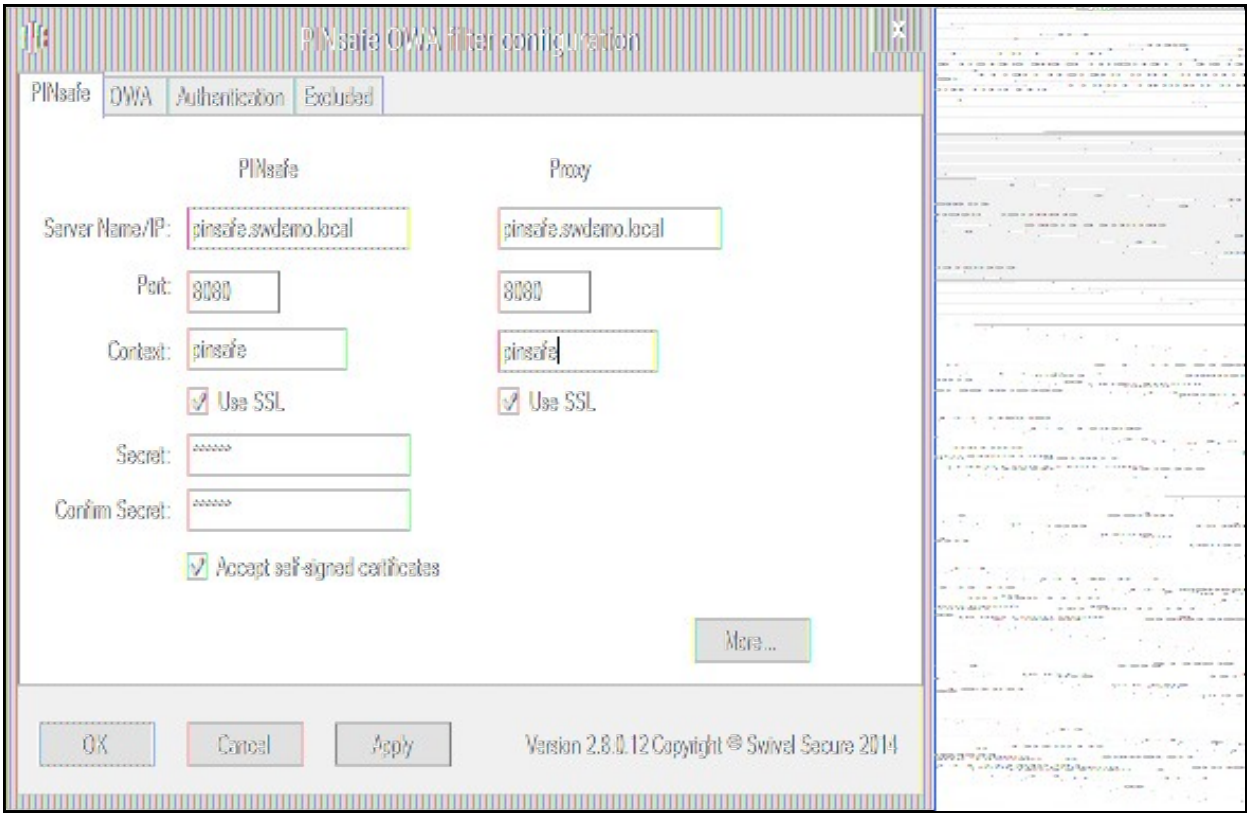
Context: Swivel install name, for a Swivel appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel appliance tick this box until a valid certificate is installed.

Proxy Server, Port, Context, Use SSL These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an appliance, you MUST set them to be the same. Version 2.10 removes the proxy settings altogether.



431.2.2 OWA Settings

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

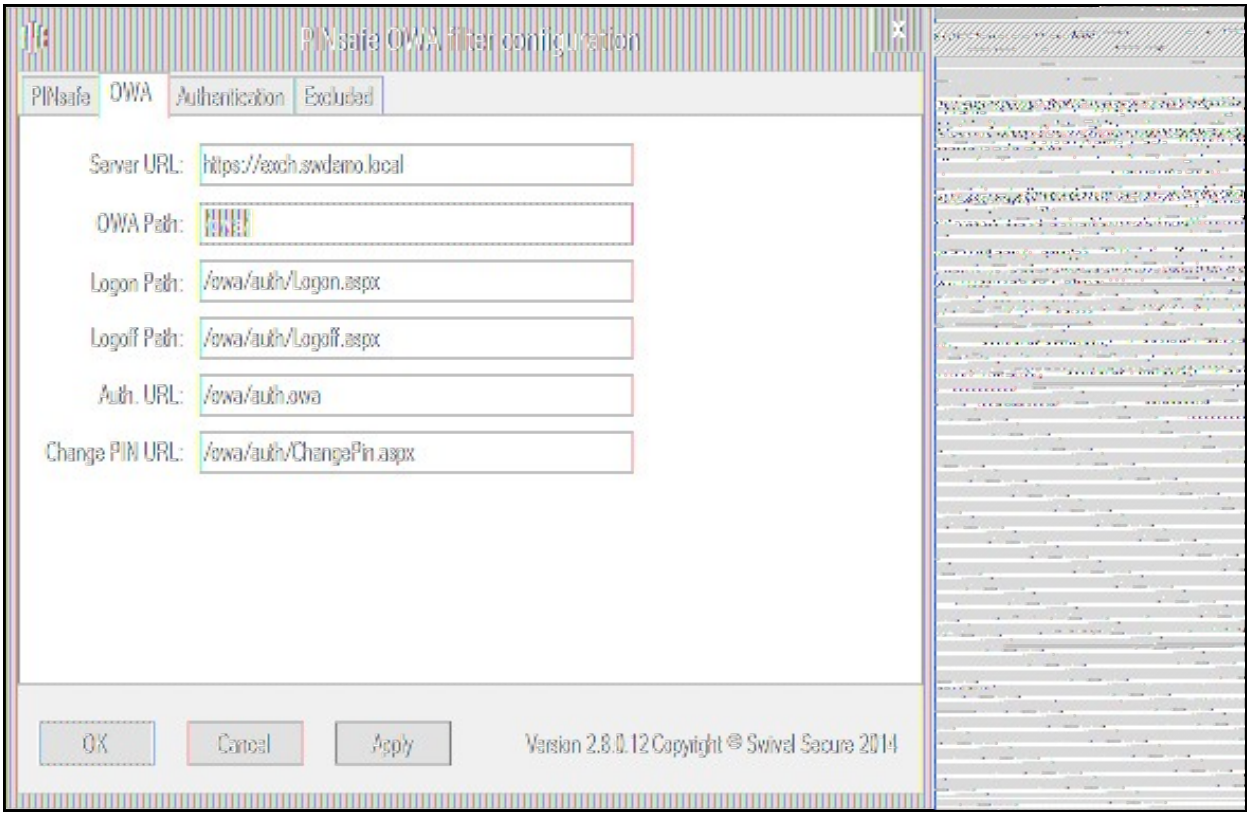
OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually /owa/auth/auth.owa

Change PIN URL: This is the URL for the Change PIN page. Note that the default URL is actually incorrect, but this value is currently ignored anyway.



431.2.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased. The idle time on the Swivel OWA filter is in addition to the session timeout built into OWA. The Swivel timeout will never increase the OWA timeout, only reduce it. Therefore, it will not compromise the security of the public computer settings.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

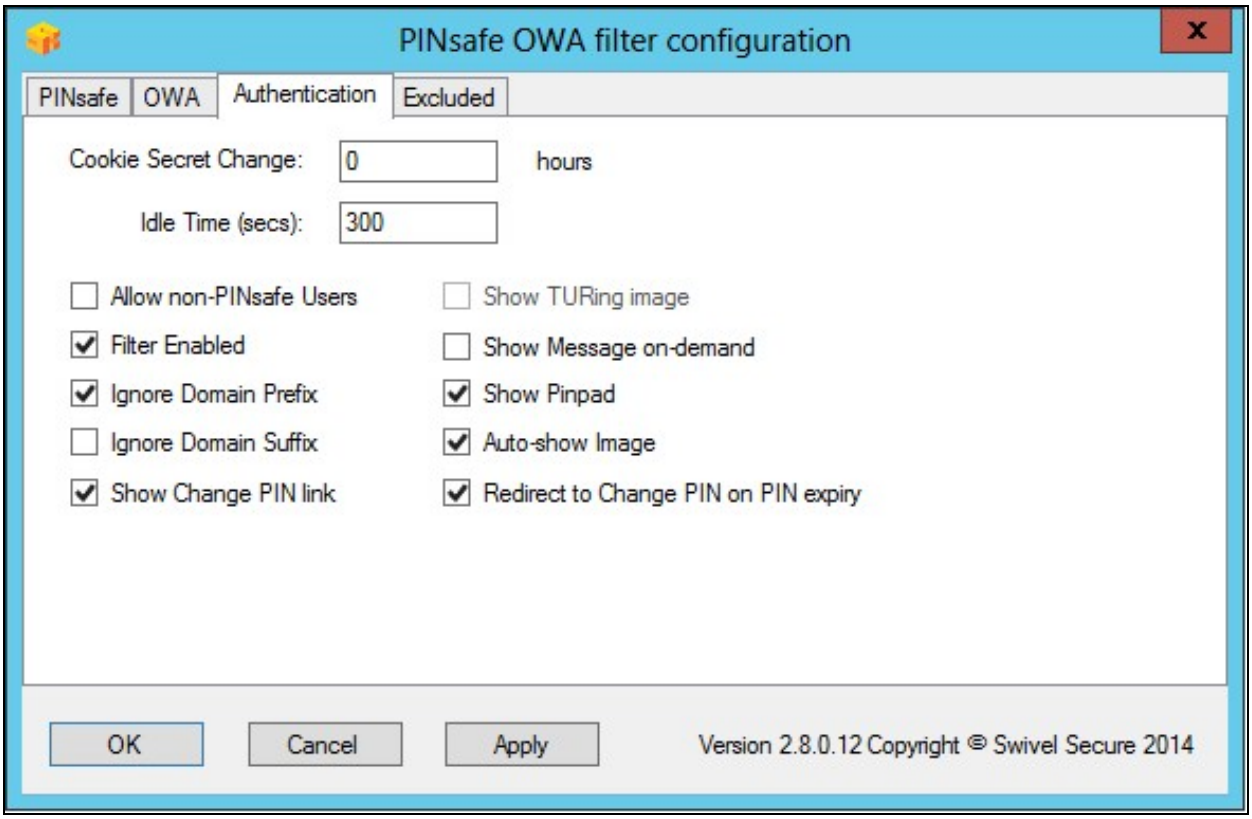
Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.

Show Change PIN link If this option is ticked, a link to the Change PIN page will be shown on the login page.

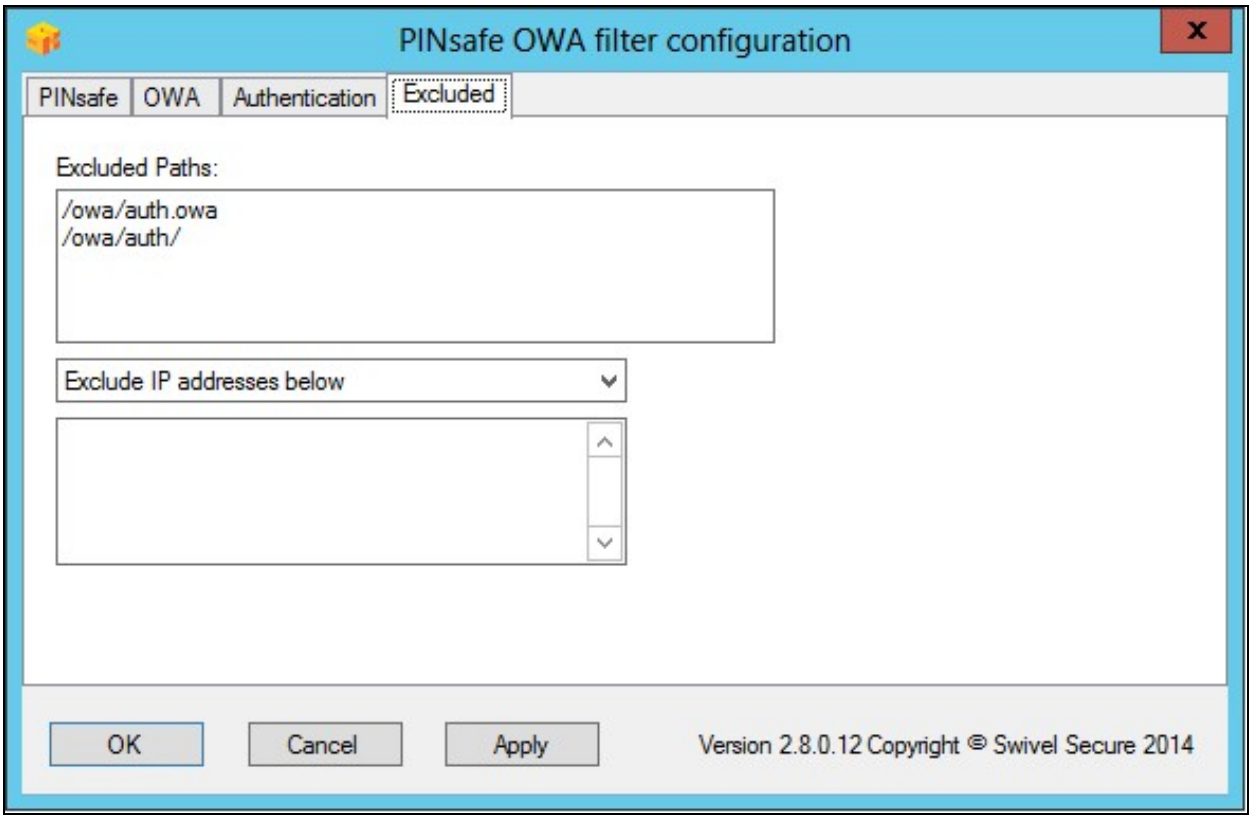
Redirect to Change PIN on PIN expiry If this option is ticked, users are automatically redirected after successful login to the Change PIN page, if their PIN has expired.



431.2.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported. To add multiple addresses, enter them into a text editor, one per line then copy and paste all entries, into the excluded field.



431.2.4.1 External/Internal User Authentication

Using the above excluded IP addresses it is possible to configure a range of IP addresses for users, such as internal users, that will not be required to use Swivel authentication.

431.3 Configure The Swivel Server

431.3.1 Configuring Swivel for Agent XML Authentication

To allow communication from the OWA server to the Swivel server we need to configure an agent, see Agents How to Guide

431.3.2 Configuring Swivel for Single Channel Images

If Swivel Single Channel images are to be used for authentication, then the following guide can be used.

Single Channel How To Guide

431.3.3 Configuring Swivel for Dual Channel Authentication

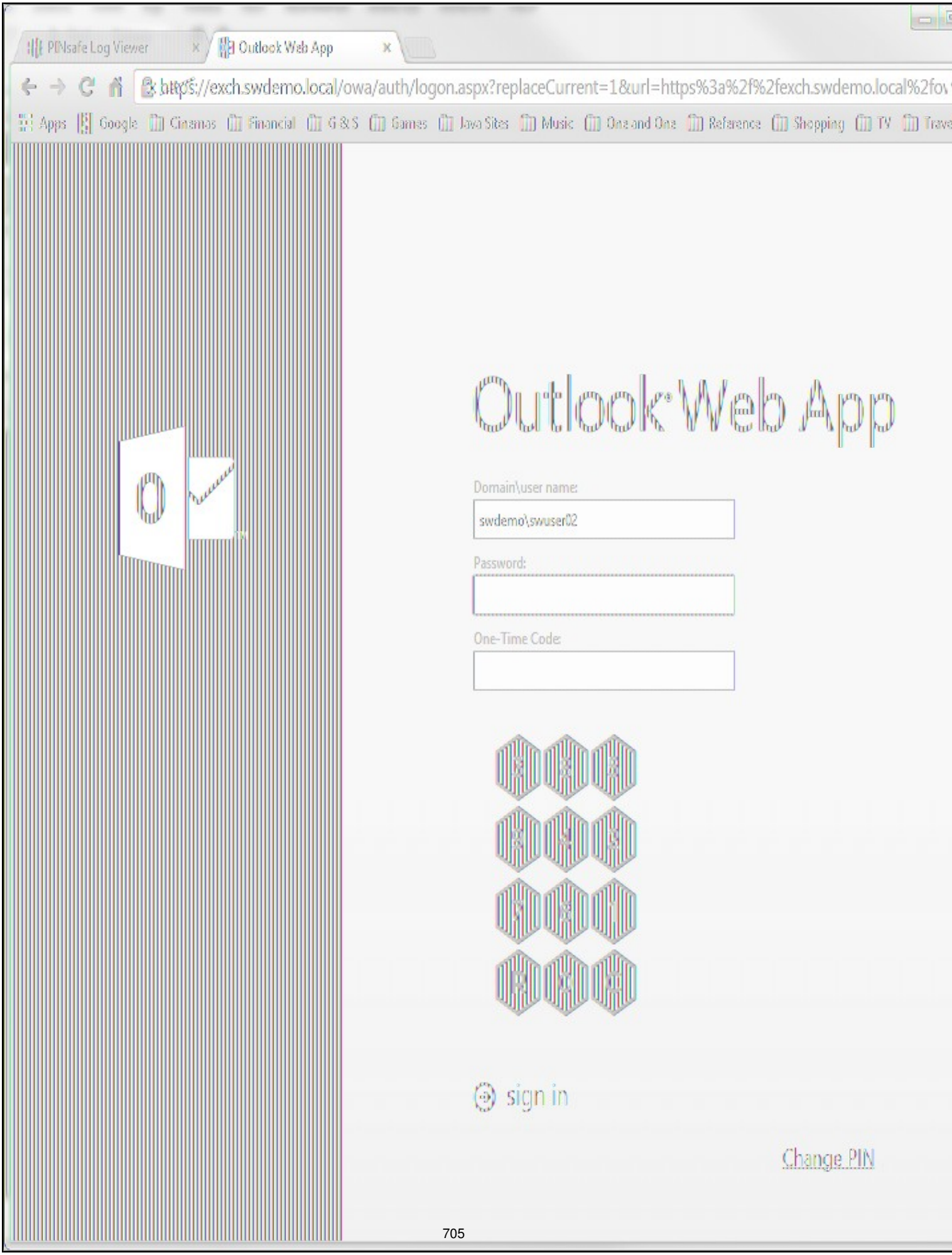
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

Transport Configuration

432 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.

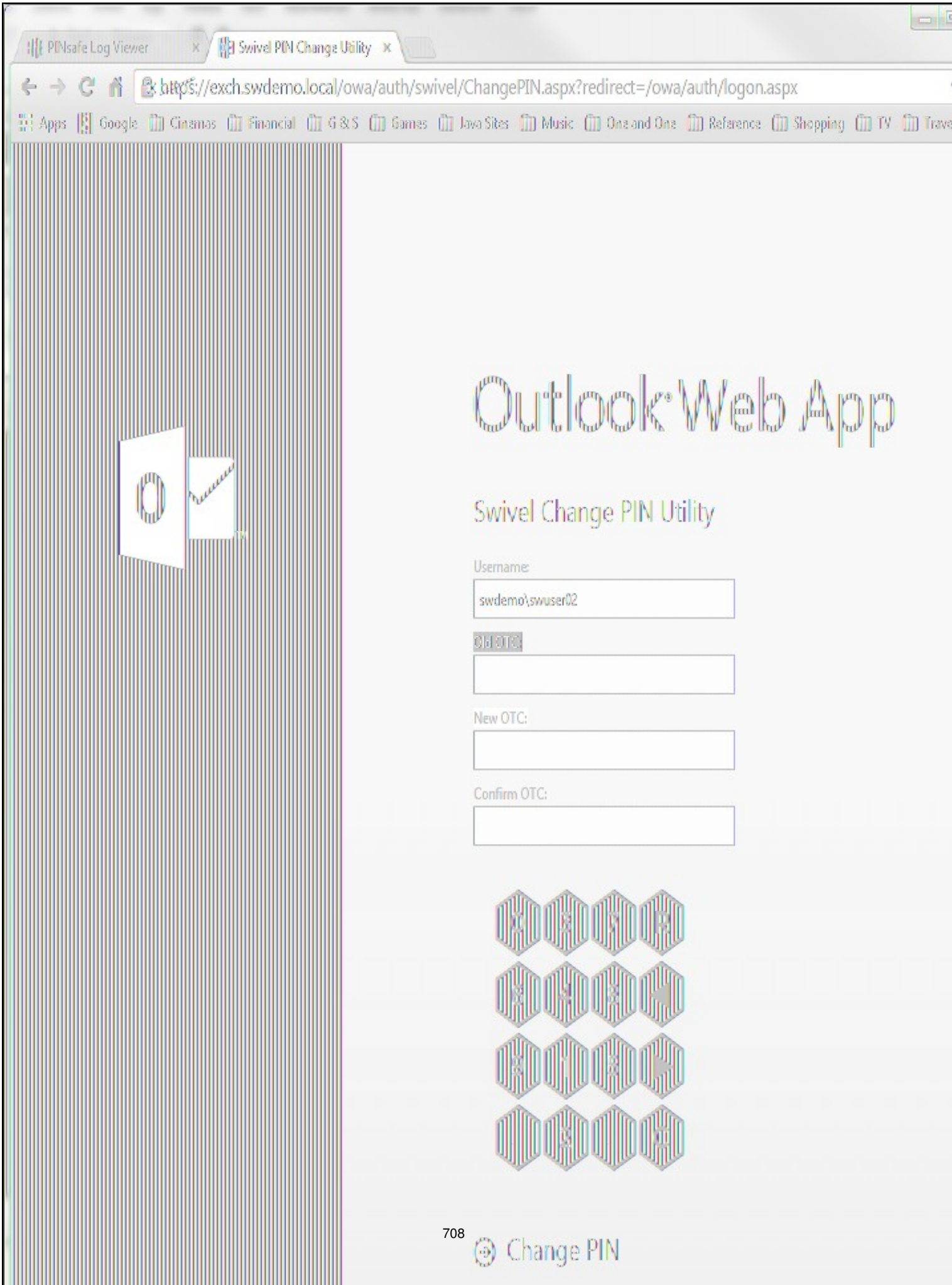

PINsafe Log Viewer
Outlook Web App
https://exch.swdemo.local/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fexch.swdemo.local%2fo
Apps
Google
Cinemas
Financial
G & S
Games
Java Sites
Music
One and One
Reference
Shopping
TV
Outlook Web App
Domain\user name:
swdemo\swuser02
Password:
One-Time Code:
sign in
Change PIN

433 Change PIN

The Change PIN page is reasonably self-explanatory, but using Pinpad with change PIN may need some clarification.

You will notice on the screen shot that "Old OTC:" is highlighted. This means that clicking on the Pinpad digits will enter the corresponding digit into that field. To change the active field, either click on the field itself, or click the arrow keys in the Pinpad display.

The **R** key will refresh the Pinpad display (i.e. display a new security string), and the **C** key will clear the currently-active field.


PINsafe Log Viewer
Swivel PIN Change Utility
https://exch.swdemo.local/owa/auth/swivel/ChangePIN.aspx?redirect=/owa/auth/logon.aspx
Apps
Google
Cinemas
Financial
G & S
Games
Java Sites
Music
One and One
Reference
Shopping
TV
Outlook Web App
Swivel Change PIN Utility
Username:
swdemo\swuser02
Old OTC:
New OTC:
Confirm OTC:
Change PIN

434 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in the Exchange Server folder (default is C:\Program Files\Microsoft\Exchange Server\V15) under the sub-folder FrontEnd\HttpProxy\owa\auth\. Rename this to restore the original Login.aspx.

435 Troubleshooting

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

435.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v15\FrontEnd\HttpProxy\owa\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

435.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

435.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

435.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

435.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

436 Known Issues and Limitations

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu.

There appears to be a problem locating the correct folder for OWA in some cases. We are investigating the cause of this, but meanwhile, if you are prompted to select the OWA folder, you should use the following:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HTTPProxy\owa

If Exchange Server is installed in a non-standard location, adjust the path accordingly, but the last part (FrontEnd\HTTPProxy\owa) should be the same.

436.1 TLS 1.2 Support

We have observed problems recently with the filter not working if TLS 1.2 only is enabled. We believe the problem is that the TLS 1.2 ciphers supported by Windows Server and the version of Java on our appliances do not overlap. If you are unable to connect the OWA filter to your Sentry appliance, it may be necessary to re-enable TLS 1.1 support on both the OWA filter and the appliance, and to enable the following cipher suite on the appliance: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA. In order to add this cipher suite, you will need command line access, so you will need assistance from Swivel Secure support.

436.2 Themes Support

The filter has been written and tested using the default theme (as seen in the screen shots). The screens may not look right (although they should still work) if the theme is changed. However, it should only be necessary to change the stylesheet in order to correct this. Please contact support@swivelsecure.com if you have difficulties getting the display looking right. In particular, the Change PIN page will only work with the default theme, and with the OWA 2013 versions listed above.

437 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

438 Additional Information

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

439 Microsoft OWA with OMA on Exchange 2003

439.1 OWA and OMA on Exchange 2003 Integration Notes

the following Microsoft knowledge base article might be of interest:

http://support.microsoft.com/kb/817379

439.2 Article Summary

When you try to access a Microsoft Exchange Server 2003 computer by using Microsoft Office Outlook Mobile Access or Exchange ActiveSync, you may experience connection or synchronization problems. These issues can occur if either of the following conditions is true:

The Exchange virtual directory on an Exchange back-end server is configured to require SSL.

Forms-based authentication is enabled.

However, these issues do not occur if these same conditions are true on the Exchange virtual directory on a front-end server.

440 Microsoft Terminal Services Integration

440.1 Overview

PINsafe integrates with the Microsoft Windows GINA to allow authentication through Terminal Services. For further information see Microsoft Windows GINA login

441 Microsoft TMG 2010 Integration

441.1 Microsoft Forefront Threat Management Gateway (TMG) Integration Notes

441.2 Introduction

This document outlines the necessary steps to integrate Swivel authentication into Microsoft TMG Server 2010 for use with Swivel for Dual Channel authentication using SMS, Mobile Phone Clients and Single Channel using TURing, PINpad and the Taskbar. If the TMG server is part of a cluster then the filter needs to be installed on each server in the cluster.

441.3 Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in TMG Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required. Certain features of the filter require later versions of Swivel:

- If the option to allow unknown users is required, this requires Swivel 3.4 or later.
- If the option to use Pinpad is required, the Swivel version must be 3.9.2 or higher, or a version of the appliance proxy from 2012.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The TMG server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per TMG server for the integration, and the integration will require a restart of the TMG Firewall Services. If you are replacing an older version of the Swivel filter, you must uninstall that version first. The filter configuration will not be lost. You will need to stop the TMG firewall service before uninstalling the old filter, or else you will be prompted to restart the server to complete uninstallation.

441.3.1 Swivel TMG 2010 Filter

The filter can be downloaded from here. NOTE: this is version 1.4.4 of the TMG filter, released 1/11/13. Version 1.4.4 fixes a bug found by some customers, whereby the login page was not detected in some circumstances, allowing authentication by password only. The same bug could also cause other failures, such as occasionally failing to show a TURing image. This version also adds better control over logging. See the included documentation for more details.

Version 1.4.3 was never released, but made detection of the required URLs case-insensitive.

Version 1.4.2 includes some bug fixes and enhancements, in particular:

- Redirecting to the login page after an incorrect one-time code now works correctly. This means that an error message is displayed if the one-time code is incorrect. It is also expected that this will resolve issues experienced by some customers whereby, having logged in once, users do not always have to re-enter their one-time code.
- The firewall service is restarted automatically after making configuration changes and before uninstalling the filter.

Version 1.4.1 fixes some bugs present in version 1.4.0. Version 1.4 includes a number of enhancements over previous versions. See the included documentation.

NOTE: if you are using this filter with RADIUS authentication, be aware that there are some errors in the file usr_pwd_pcode.htm. These need to be fixed manually - contact support@swivelsecure.com for details. An update with the correct script will be released shortly.

441.4 Baseline

Swivel 3.1 or later (3.6 or later preferred)

Microsoft Forefront TMG 2010

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

441.5 Architecture

The TMG server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

441.6 Swivel Configuration

441.6.1 Configure a Swivel Agent For XML Authentication

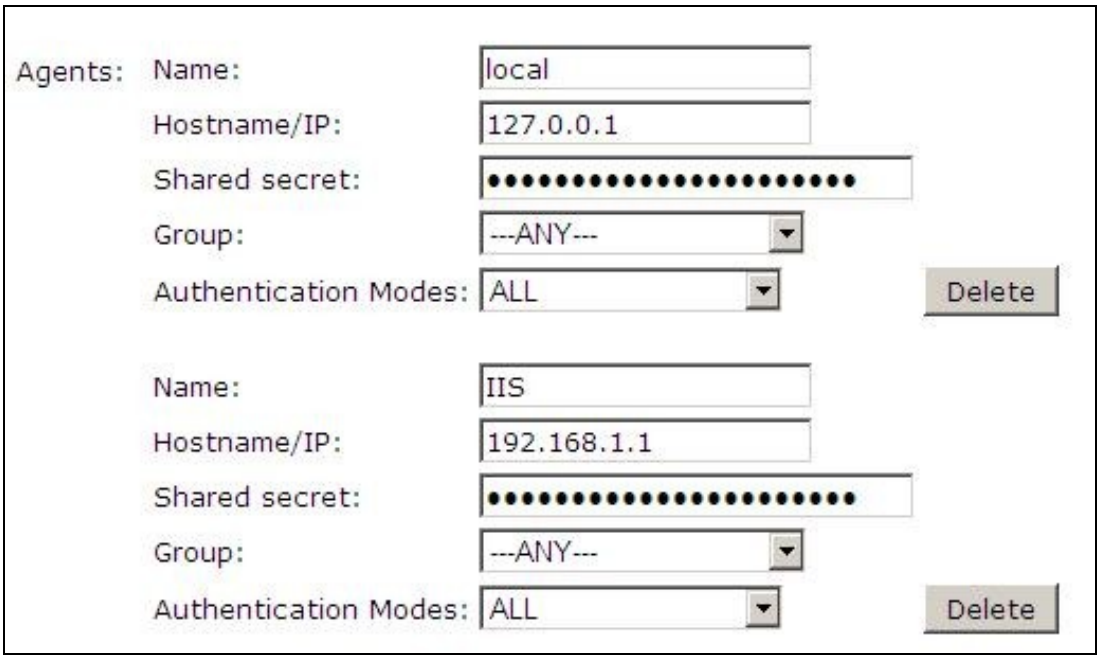
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the TMG internal IP address

4. Enter the shared secret

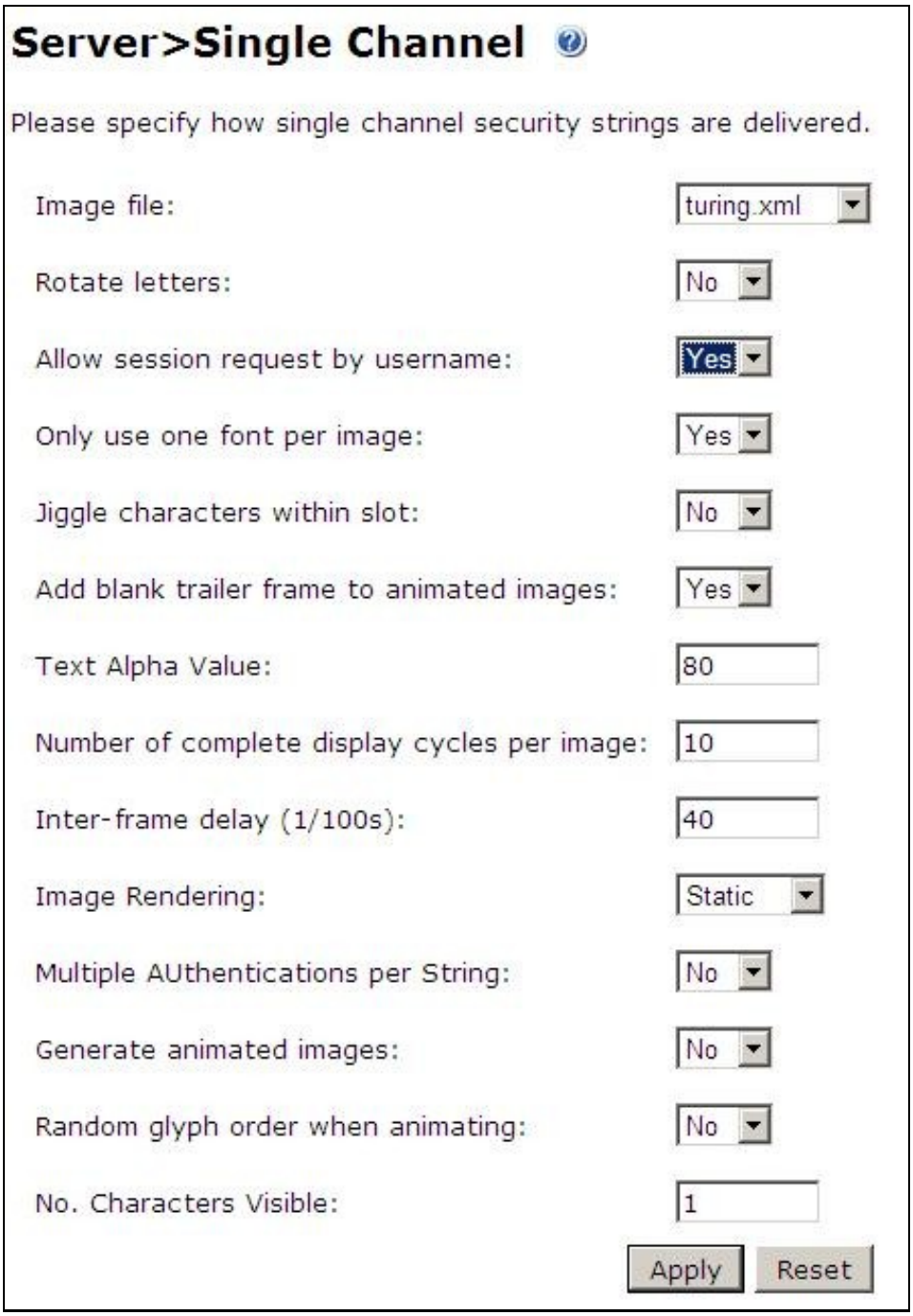
5. Click on Apply to save changes



441.6.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



441.6.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

1. Ensure the RADIUS server is running on Swivel
2. On the Swivel Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the TMG internal IP address
5. Enter the shared secret
6. Click on Apply to save changes

441.7 Swivel TMG Filter Upgrade

If an existing filter is installed then installing the new filter will first uninstall the existing filter.

441.8 Swivel TMG Filter Installation

The following steps should be carried out on the TMG server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below. To upgrade or reinstall the filter, first remove the existing Swivel TMG filter.

441.8.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the TMG Server documentation, if you have not already done so. Ensure that they are working as expected without Swivel authentication before attempting to install the Swivel filter.

For OWA, TMG should be configured to redirect to /owa automatically, otherwise a failure in the Swivel authentication will redirect to the root path, which will give an error. This external link shows how to configure this: Setting up an OWA redirect in Forefront TMG 2010 the easy way

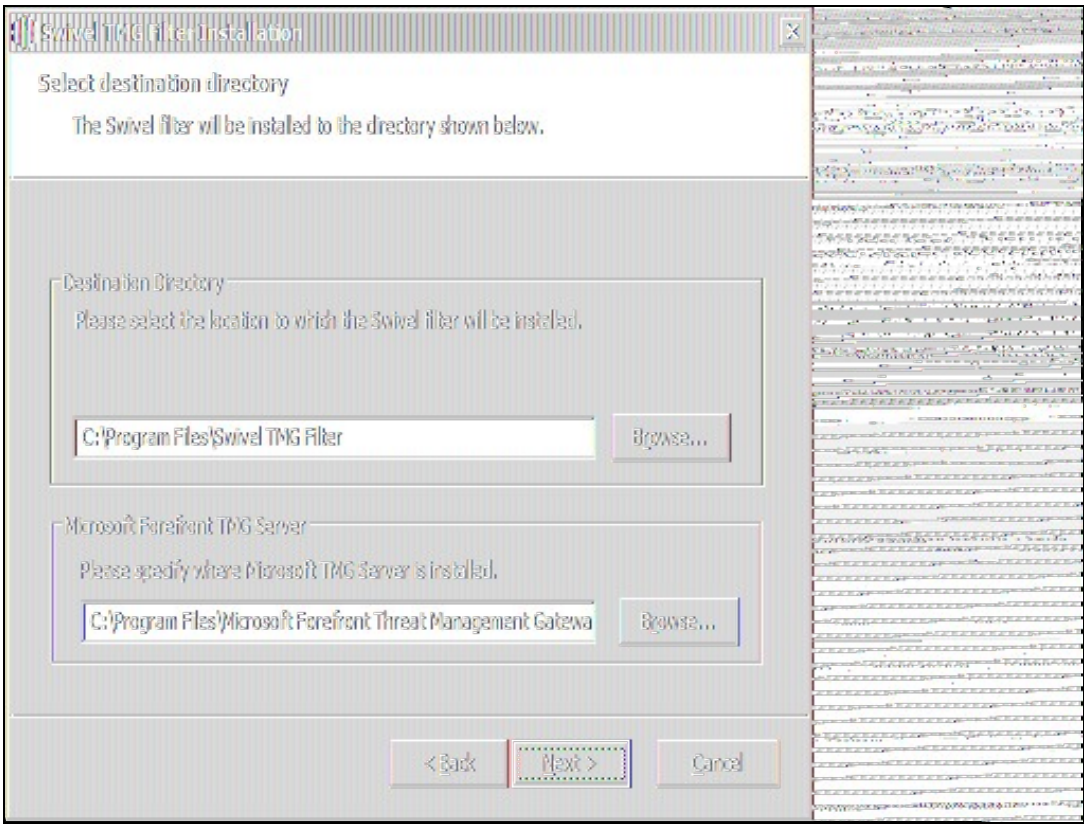
441.8.2 Configure TMG firewall rules

Create an access rule permitting HTTP access from the TMG Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

441.8.3 Install the TMG server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

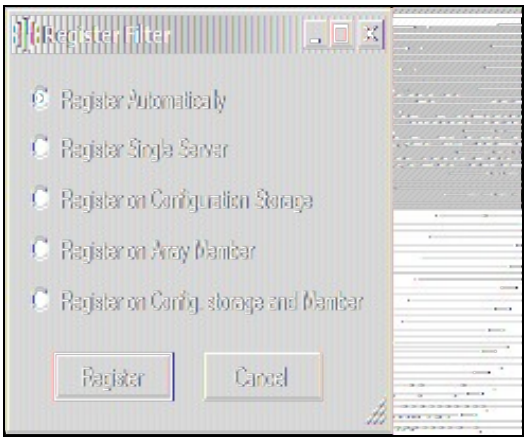
Run PINsafeTMGFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft TMG Server, usually C:\Program Files\Microsoft Forefront Threat Management Gateway.



Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

441.8.4 Register the Swivel TMG Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with TMG. You have a choice of registration types:

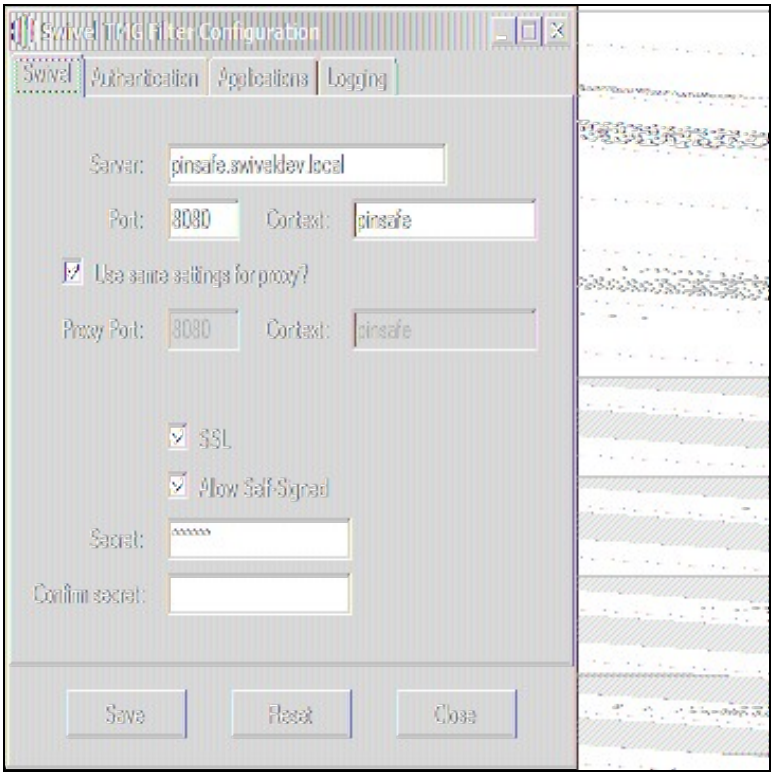


The Automatic registration option should work in most situations. Only try the other options if automatic registration fails.

441.8.5 Configure the TMG filter

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/Swivel TMG Filter/Configuration.

441.8.5.1 Swivel configuration tab



Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. Swivel appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with TMG. (Hint: Use port 8080)

Context: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel appliance where the proxy port is available, the path Swivel using port 8080 should still be used, the TMG proxy provides security.

Proxy port and **Proxy context** may be required if you are using Pinpad together with an appliance that has the a proxy application that supports Pinpad, but does not have a version of Swivel that supports it directly. In this case, you should use proxy port 8443 and proxy context "proxy". You can still use these values if you are not using Pinpad, but you are using a Swivel appliance.

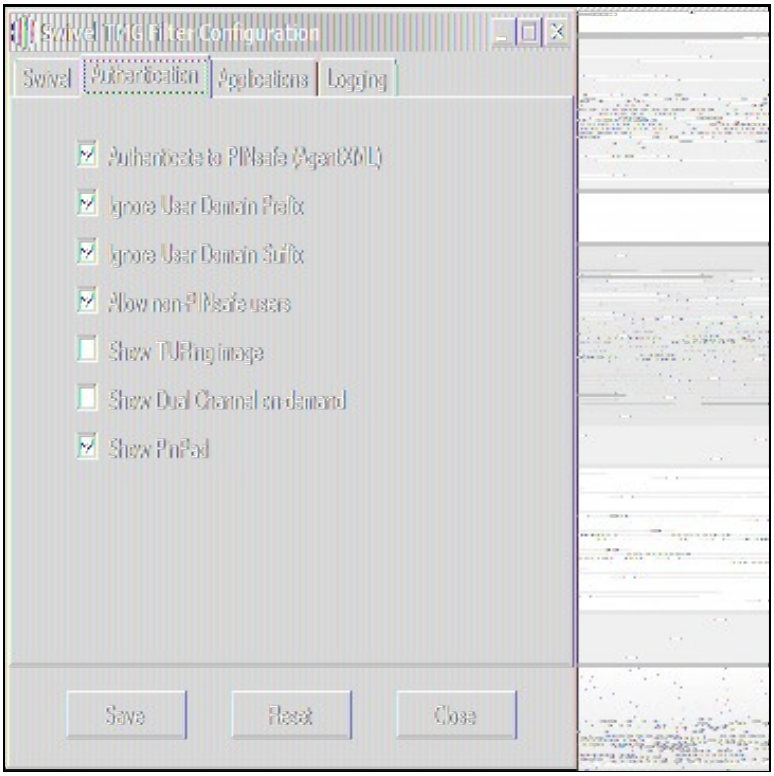
To clarify: the filter will use the proxy port and proxy context to retrieve TURing and Pinpad images (and message on-demand), but will use port and context to authenticate the user.

SSL: will, if checked, send requests to the Swivel server using https, rather than http. This applies to proxy as well: the current filter does not support connecting to one port on HTTP and the other on HTTPS.

Allow self-signed: when checked, causes SSL certificate errors from the Swivel server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. If you change this value, you must enter it twice to confirm the change.

441.8.5.2 Authentication configuration tab



Authenticate to PINsafe (AgentXML): should be checked to use standard Swivel authentication. You should uncheck this if you are using the filter to protect a SharePoint website, as described in the ?Special Considerations for SharePoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain prefix: This will remove the AD domain prefix for users (anything before the '\' symbol), and when Swivel is using the SAM account name it should normally be checked. In this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the prefix will be sent as part of the name to Swivel. If you use the domain prefix option in Swivel, you should uncheck this option.

Ignore user domain suffix: This will remove the AD domain suffix for users (anything after the '@' symbol). You should normally check this if you use sAMAccountName as the username for Swivel, but uncheck if you use userPrincipalName.

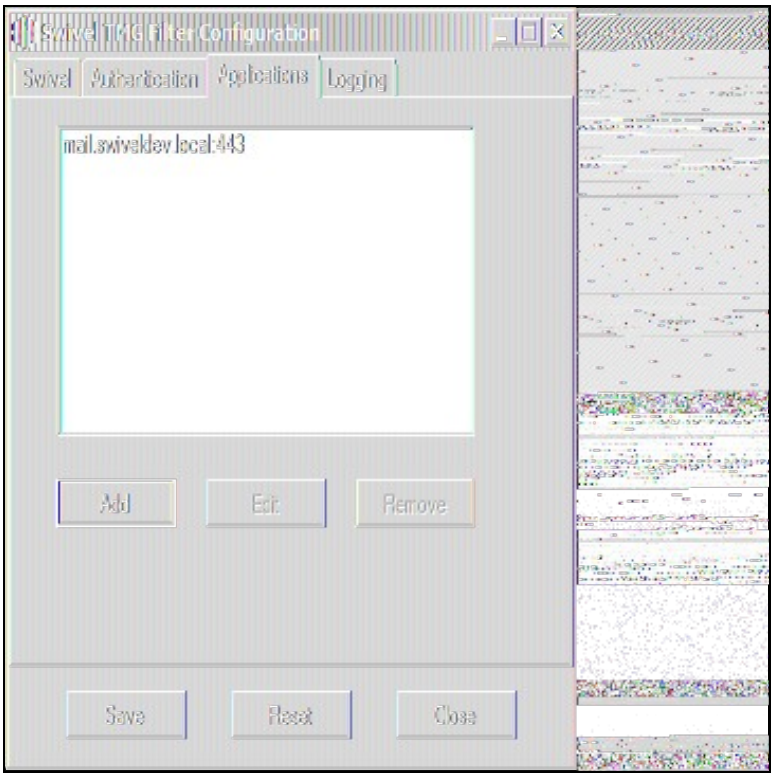
Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

Show TURing image: when checked, entering a username or clicking the Start Session button on the login screen will display a TURing image for that user. It is not possible to prevent automatic display of the TURing image (i.e. only display when the button is clicked) from the configuration program, but this can be managed with a simple modification of the login page. Please contact Swivel for more information.

Show Dual Channel on-demand: when checked, a button is displayed allowing the user to request a security string via SMS or email (depending on how the strings transport is configured in Swivel). This option can be used together with the TURing or Pinpad option if required.

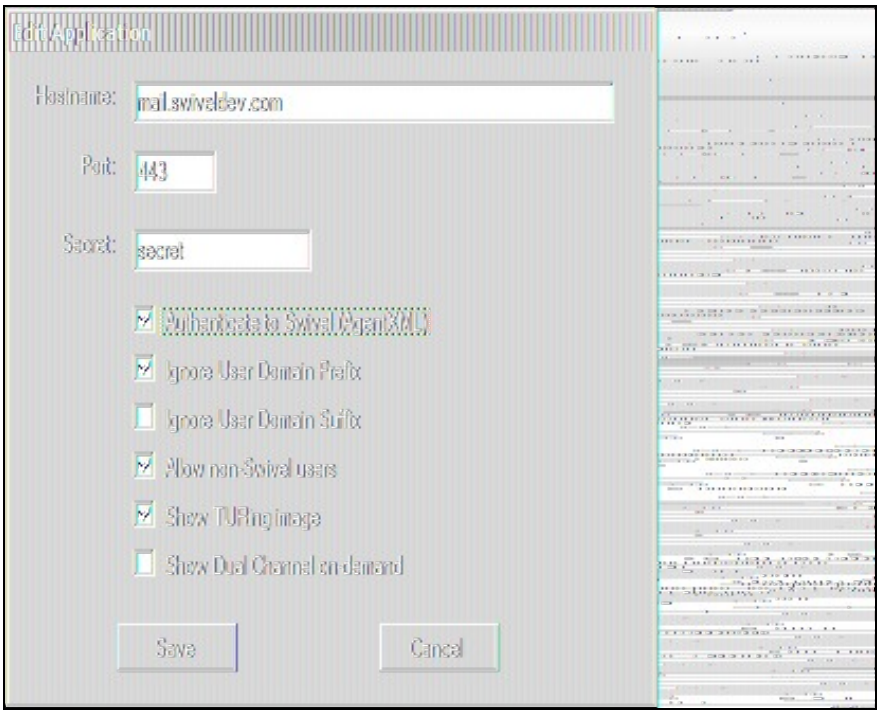
Show Pinpad: when checked, a Pinpad display is used to enter the one-time code. This option cannot be used with the TURing option, and requires that you have a version of Swivel or the appliance proxy that supports it.

441.8.5.3 Hosts configuration tab



This feature allows you to configure the filter to behave differently for different host names or ports on the TMG. It is only relevant if you are using the TMG to protect multiple websites.

If you add a new host, you will see the following form:



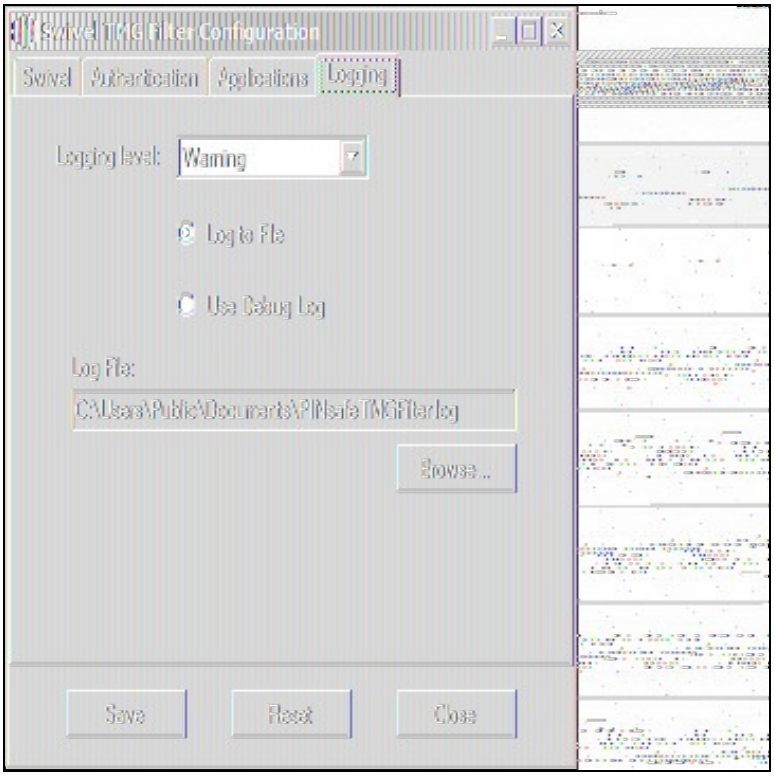
Specify the host name and port that this configuration should apply to. If you leave either one blank, it will apply to all host names on a given port, or all ports for a given host name.

You can specify a different secret from the default here. This allows you to use different Agents in Swivel, so for example, restrict authentication by groups. Swivel supports multiple agents for the same server, provided that the secret is different.

The remaining options override the default options for those particular settings. In particular, if you uncheck "Authenticate to Swivel", you can specify that certain host names do not require Swivel authentication.

If a request comes in that does not match any host name/port combination in this list, the default settings will apply.

441.8.5.4 Logging Configuration tab



Logging level controls how much data is logged: the levels are Debug, Info, Warning, Errors and None. The last option disables logging entirely. The most verbose level is Debug, and logs every single request received by the filter. It should only be used for troubleshooting.

You can choose to log to a file, or to a debug logger. The latter is provided for backward compatibility only ? you will need to have a debug logger installed to make use of it.

If you choose to log to a file, the default name is C:\Users\Public\Documents\PINsafeTMGFilter.log. Note that the log file does not roll over, but continues to fill up, so depending on what level of logging you use, you will need to back up or delete the log file regularly.

441.8.6 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors.

441.8.7 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeExchange? for Outlook Web Access

and ?PINsafeISA? for Sharepoint or other websites.

Modify the properties for the relevant policy rule, then select Apply, and click OK. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the TMG Server (not just activating TMG). It can take a long time to restart this service, and if you are connecting to the TMG Server via remote desktop, you may be temporarily disconnected from it.

441.9 SSL Certificate Considerations

There would appear to be an issue with certain security updates for TMG Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the Swivel TMG Filter integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the TMG Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your Swivel server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the TMG Server, if it is not already. The third option is simply to generate a self-signed

certificate on the Swivel server, with the correct host name, and to install that directly into the TMG Server trusted root store.

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel appliance. Otherwise, refer to the relevant documentation for your operating system.

441.10 Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

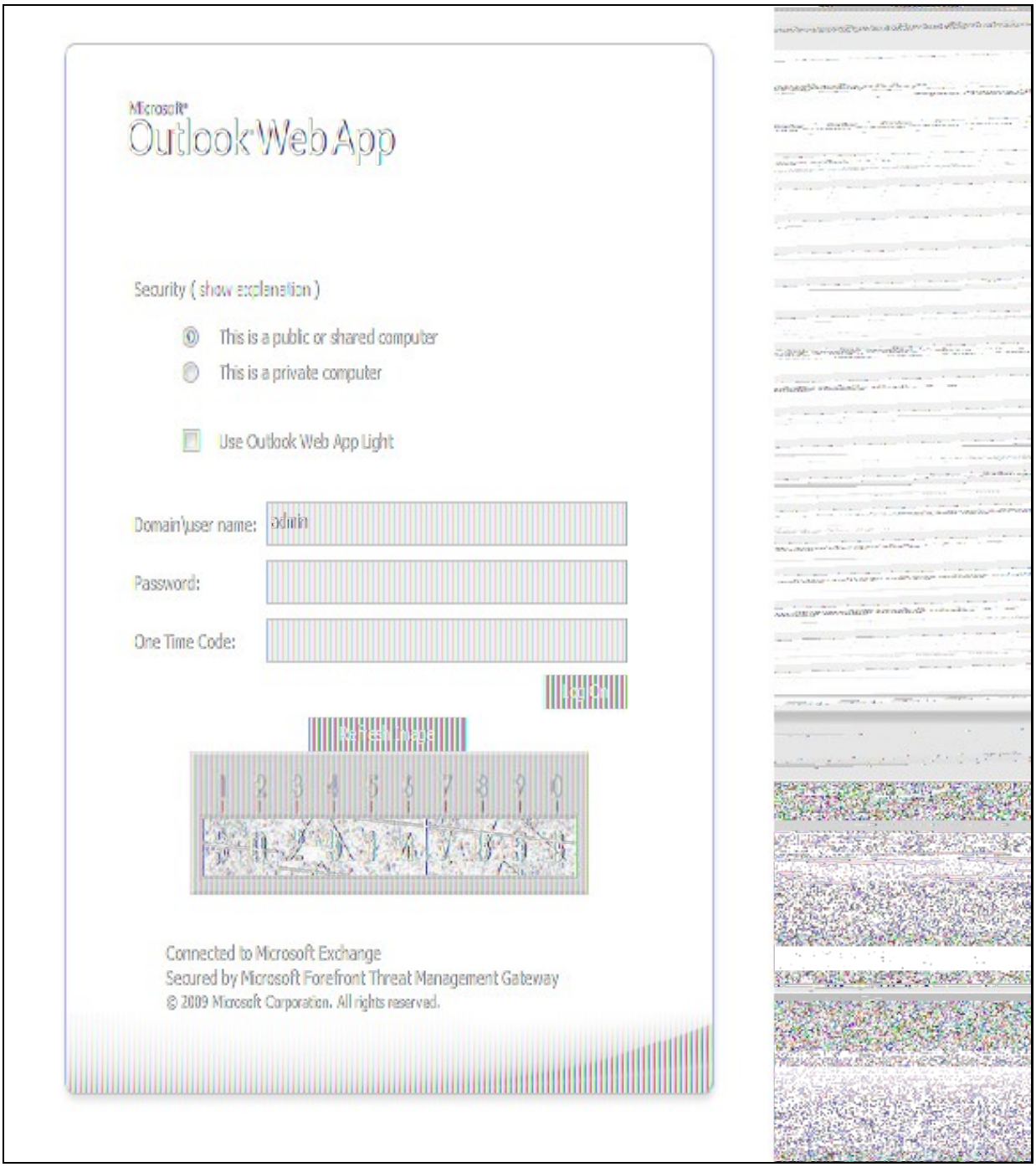
Once you have configured everything, reboot the ISA server.

441.11 Verifying Installation

441.11.1 Outlook Web Access

Navigate to the URL on which TMG Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

If you have enabled the option to allow non-Swivel users, then no Swivel customisation will be evident until after you enter the username and move to a different screen. The Swivel additional fields will then appear:



441.11.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain\user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

441.12 Additional Options

441.12.1 RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. Swivel RADIUS custom login pages provided with the filter can be used.

441.12.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

441.12.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

441.12.4 Disabling the Auto TURing feature

When a TURing image is generated it expects the user to authenticate with that image for the length of the Session Cleanup.

When using the XML authentication the automatic display of the TURing image can be prevented by editing the file: "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Delete the line *ShowTuring();* within the function *setUserExists(attribute)*.

441.13 Uninstalling

441.13.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

441.14 Known Issues

441.15 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

With regard to the Single Channel TURing image, the TMG server login page does not use SCImage directly: the image request comes through the filter, so that the the Swivel server does not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

441.15.1 Filter status Check

This should be made in a web browser against the TMG login.

https://<path_to_TMG server>/PINsafeTMGFilter.dll?usepinsafe

This should return a series of 0s and 1s, Example: 10100110, the order can show the status as below:

1 - Show one-time code field

2 ? Allow unknown users

3 ? Show TURing image

4 ? Show Message on demand

5 - Show Pinpad

6 ? Ignore domain prefix

7 ? Ignore domain suffix

If it cannot contact the Swivel server, or if the filter is disabled, the first digit will be 0. NOTE: for versions of the TMG earlier than 1.4, the PINpad flag is not present.

441.15.2 Enabling Swivel logging

The Swivel authentication filter can optionally log its activity to a file. By default, no logging takes place, but you can enable logging by editing the filter registry key directly, using Regedit. The key to edit is

\\HKEY_LOCAL_MACHINE\Software\Swivel Secure\PINsafeTMGFilter

Create a DWORD value named "LogOptions". Set it to 2 to enable logging to a file. Set it to 1 to enable logging to the Windows debug log (see below), or 3 to enable both. Setting it to 0, or omitting it entirely, results in no logging.

The default log file is

C:\Users\Public\Documents\PINsafeTMGFilter.log

If you want to log to a different file, create a String registry value in the filter key named "LogFile", and set the value to the full path of the log file.

Older versions of the filter always log activity to the standard Windows debug log. Newer versions can optionally do this as well. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

441.15.3 Single Channel image does not appear

- Check Swivel TMG filter settings
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Is the certificate using the internal hostname or the external hostname? The hostname used by Swivel must match the certificate hostname.
- Check the Swivel TMG filter is correctly installed. On the TMG Server Management: under System, on the Web Filters tab, "Swivel Authentication Filter" should be enabled
- From the TMG server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

or

https://<PINsafe server IP>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

- If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the TMG filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

441.15.4 Page fails to display after failed login

An **Access Forbidden message** is displayed. After a login failure, the user is redirected to https://hostname/, rather than https://hostname/owa. You can configure the TMG firewall rule to automatically redirect to /owa. This external link shows how to configure this redirect: Setting up an OWA redirect in Forefront TMG 2010 the easy way

441.15.5 Adding Swivel authentication stops other pages appearing

You can specify that PINsafe authentication only applies to certain host names, in which case the others are ignored. On the Swivel TMG filter disable Swivel authentication in the default configuration, then add an application with the host name that DOES require authentication, and set Swivel authentication ON for that one only, or if you want to be explicit, add all three host names, and disable Swivel authentication for the ones you don't want.

441.16 Additional Information

Information regarding the configuration of TMG Server to publish OWA or Sharepoint may be found in the TMG Server help under Firewall policy.

For assistance in Swivel installation and configuration please contact your reseller.

442 Microsoft UAG Integration

442.1 Introduction

This configuration document outlines how to integrate Swivel with Microsoft Forefront Unified Access Gateway using Active Directory authentication in addition to the Swivel authentication.

If installing Swivel on the UAG appliance it may be required to install Swivel to use a different port than the default 8080.

442.2 Prerequisites

Microsoft Forefront Unified Access Gateway

UAG and URL rewriting documentation

Swivel 3.x server with ChangePIN

ChangePIN configuration document

The following files are required to be uploaded to the UAG

images.asp

login.asp (Rename loginturingsms.asp as login.asp)

Portalname1postpostvalidate.inc

Token.inc

The files can be downloaded from here: UAG Files

UAG Update 1 requires a modified login page, this additional file can be downloaded here: UAG Update 1 Files

UAG SP1 through to SP4 requires modified login pages, the complete set of files can be downloaded here: UAG SP1 Files

UAG SP1 through to SP4 SMS only request button login also UAG SP1 through to SP4 TURing only request button login

RADIUS ChangePIN for UAG, backup then replace the file LoginContinue.asp

442.3 Baseline

Microsoft Forefront Unified Access Gateway 1.0.1101.0

Swivel 3.5

442.4 Architecture

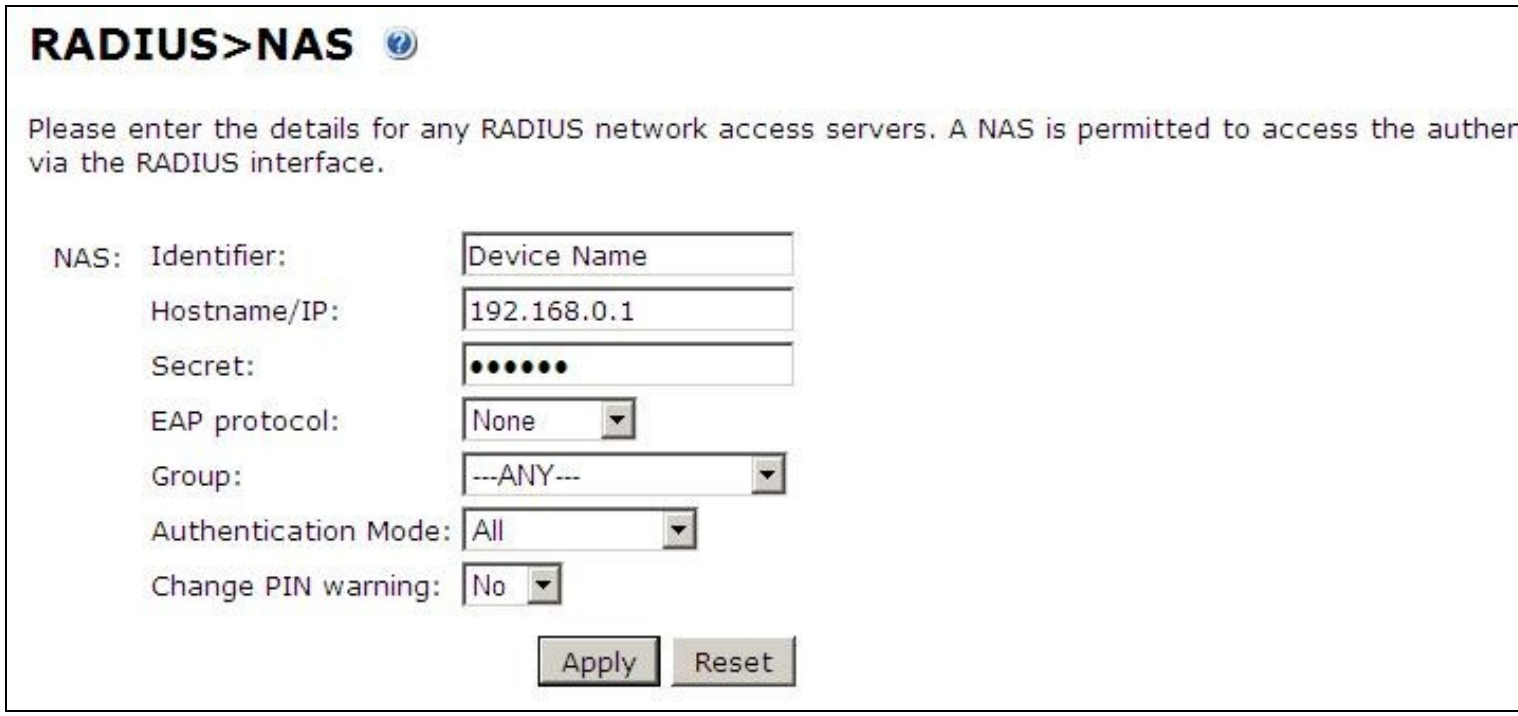
The UAG makes authentication requests against the Swivel server by RADIUS or XML.

442.5 Installation

442.5.1 Configure The Swivel Server

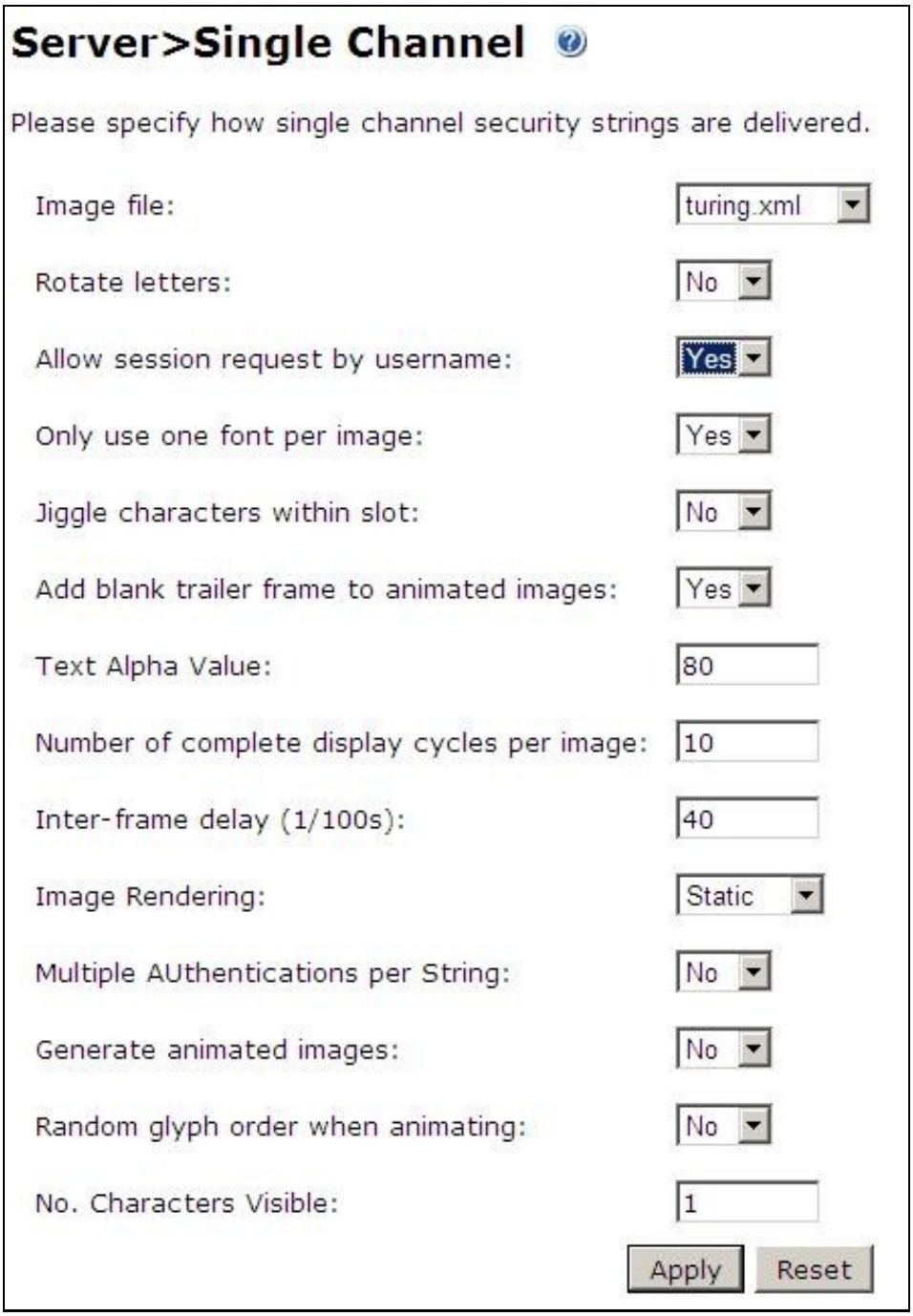
442.5.1.1 Configure a RADIUS NAS entry

1. Ensure the RADIUS server is running on Swivel
2. On the Swivel administration Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the UAG internal IP address
5. Enter the shared secret
6. Click on Apply to save changes



442.5.1.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel
2. Ensure ?Allow session request by username? is set to YES



442.5.2 Configure the UAG

442.5.2.1 Edit the UAG Configuration Files

Edit the file images.asp with the below URL to represent the Swivel server IP address and Swivel install name:

```
objWinHttp.Open "GET", "https://<hostname_of_pinsafe>:8443/proxy/SCImage?username=" & request.querystring("username"),false
```

Where <hostname_of_pinsafe> is your Swivel server hostname.

Then edit Token.inc with the required shared secret:

```
m_secret = "<secret>"
```

Where <secret> is your secret (do not enter the angle brackets).

442.5.2.2 Copy the Configuration files

Note: Ensure any existing files are backed up first.

1. Copy Token.inc and Portalname1postpostvalidate.inc to: <path to UAG install>\von\InternalSite\inc\CustomUpdate

2. Copy login.asp file to: <path to UAG install>\von\InternalSite\CustomUpdate

3. Copy images.asp to: <path to UAG install>\von\InternalSite\Images\CustomUpdate

442.5.2.3 Configure the TMG

Create a Threat Management Gateway rule to allow access from the UAG to the Swivel server

On the TMG configuration select New Access Rule and create a rule to allow traffic from the UAG to the Swivel server.

Port 8443 (or port 8080 for software installs, older virtual or hardware appliances and when using XML authentication)

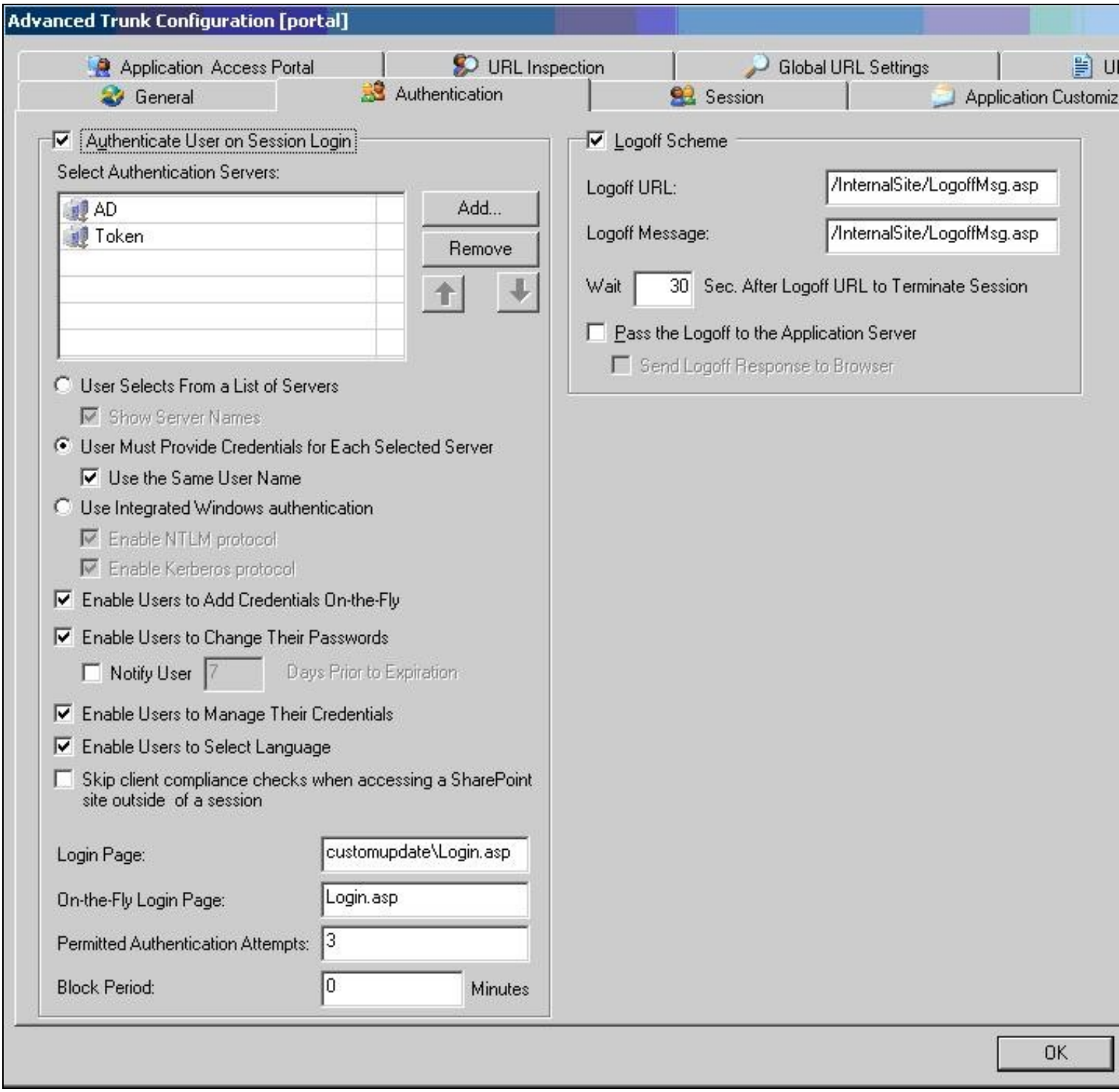
From Local Host (i.e. the UAG)

To Swivel Server (or Internal Network)

Outbound Traffic

442.5.2.4 Configure Login Page

Select the UAG Configuration GUI, From the Advanced Trunk Configuration select Authentication and set the Login Page to customupdate\Login.asp. This can be changed to reflect a different install location or trunk.



442.5.2.5 RADIUS authentication Configuration

Swivel can be configured as the Primary authentication server or more usually is configured as a secondary authentication server. When using Swivel as a secondary authentication such as with Active Directory, ensure that the options for secondary authentication are selected.

To enable RADIUS authentication create a repository of type ?RADIUS? on the UAG configuration.

To use RADIUS do the following-

1. Access the UAG configuration GUI.

2. Click on Admin Authentication Users/Group repository

3. Select New to create a new repository

4. In the drop down menu, select ?RADIUS? and in the Name field enter Swivel RADIUS

5. Enter the IP of the Swivel server. Note, when using a Swivel HA pair, do not use the VIP address for RADIUS authentication, but use the real IP address.

6. Enter port 1812

7. If required enter a second IP/port

8. Enter a shared secret key of the same value as the Swivel server

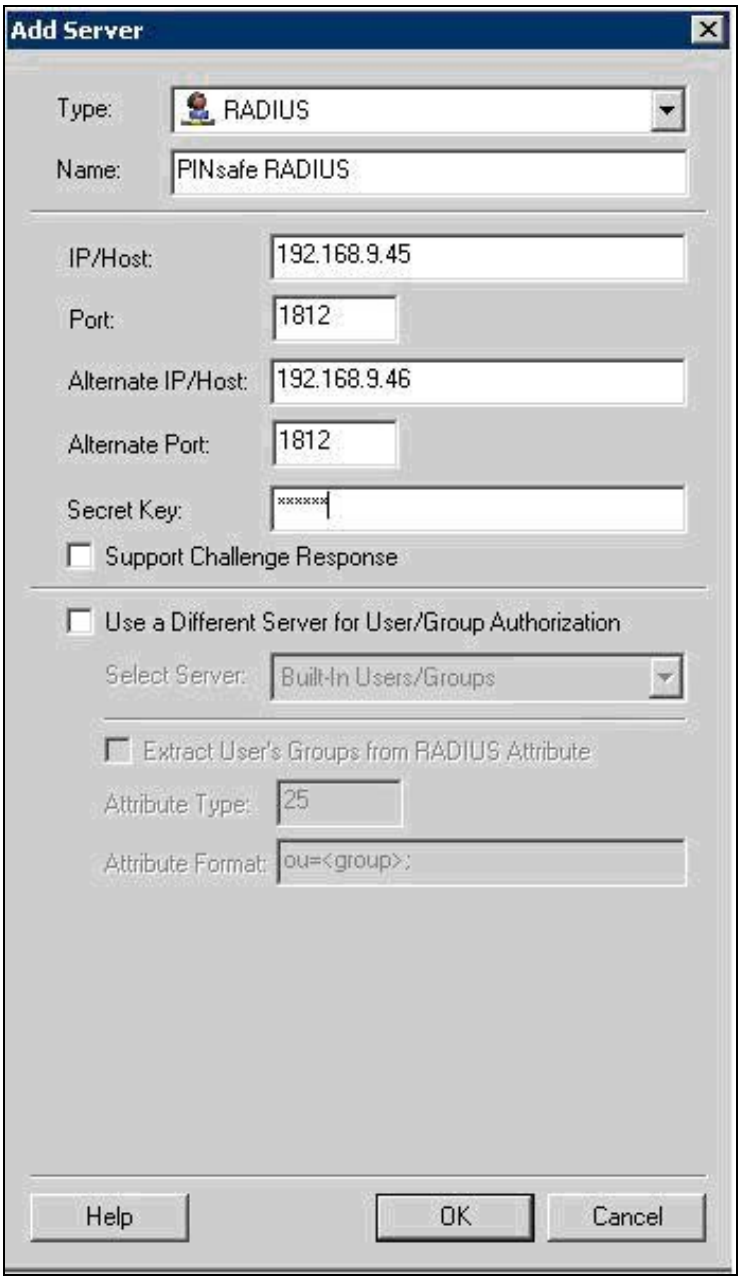
9. Click on Add and apply this repository to the relevant trunk.

10. Ensure User must enter credentials for each server is selected.

11. If AD password is to be entered ensure that an AD authentication server is specified.

12. Activate the configuration

13. Configure Swivel as a RADIUS server



442.5.2.6 Configuring the URL rewriting rules

To allow access to the images.asp

1. Select the required Trunk

2. Select Configure from the Advanced Trunk Configuration

3. Select the ?URL Set? Tab

4. Add a rule to permit access to the images.asp

InternalSite_Rule100

Note: This must be named InternalSite_Rule, example: InternalSite_Rule100 (use a high number to prevent it being overwritten by updates)

With parameters of:

Action: Accept

URL: /internalsite/images/customupdate/images.asp

Note: You can use /internalsite/images/customupdate/* for testing, and add additional rules to check the input.

Parameter: Handle (i.e. handle any parameters. For troubleshooting it may be useful to set this to ignore).

Method: Get

To Allow access to Swivel specific parameters:

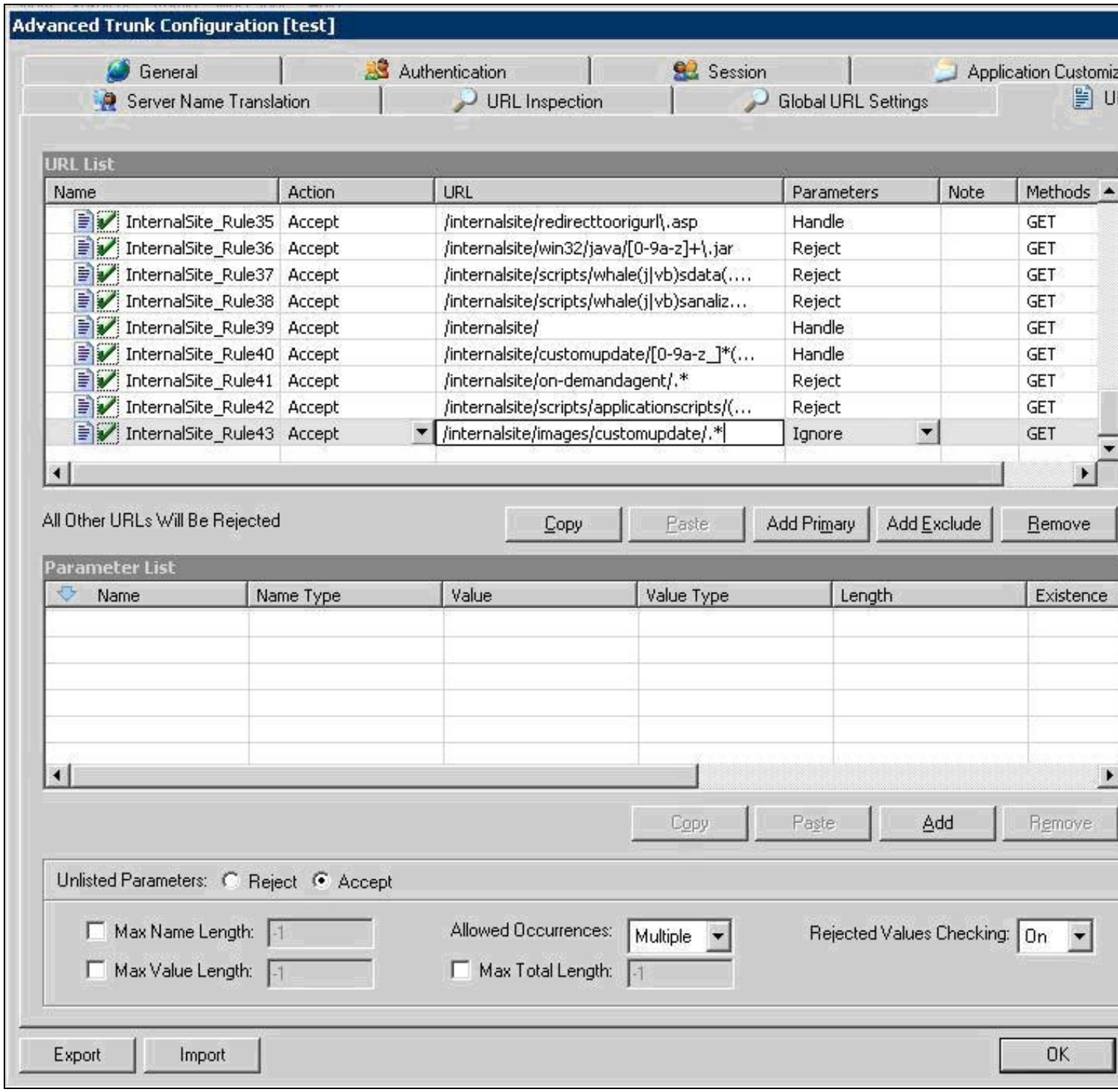
Under Parameters select Add, add the following values:

Parameter 1:

- Name: username
- Name Type: String
- Value: ?[a-z0-9]+? (this is a basic regex and may need changing depending on the users username policy)
- Value Type: String
- Length: 1:100 (may need to up 100 depending on customer username length)
- Existence: Mandatory
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on

Parameter 2:

- Name: random
- Name Type: String
- Value Type: Integer
- Existence: Optional
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on



Edit Rule to allow Access to the validate.asp

1. Select the validate.asp rule (Usually Internal_Rule2)

2. Under Parameters select Ignore

Alternatively add the following to the parameters list:

Turing

SMS

To Allow access to Swivel specific parameters:

Select the InternalSite_Rule2

Under Parameters select Add, add the following values:

Name: swivel

Name Type: String

Value:

Value Type: String

Length: 1:100

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

Also add a Parameter with the following values:

Name: orig_url

Name Type: String

Value:

Value Type: String

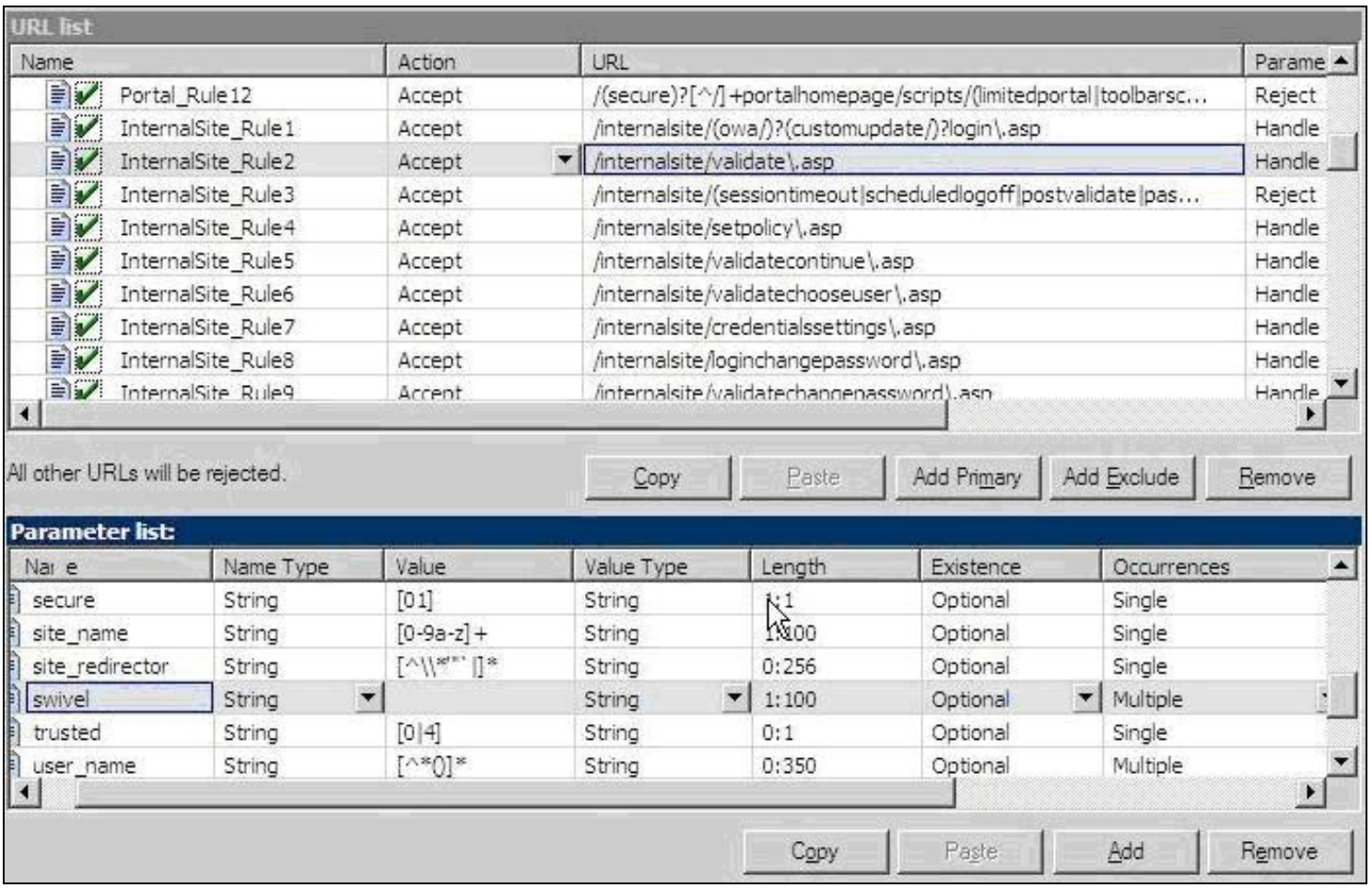
Length: 1:200

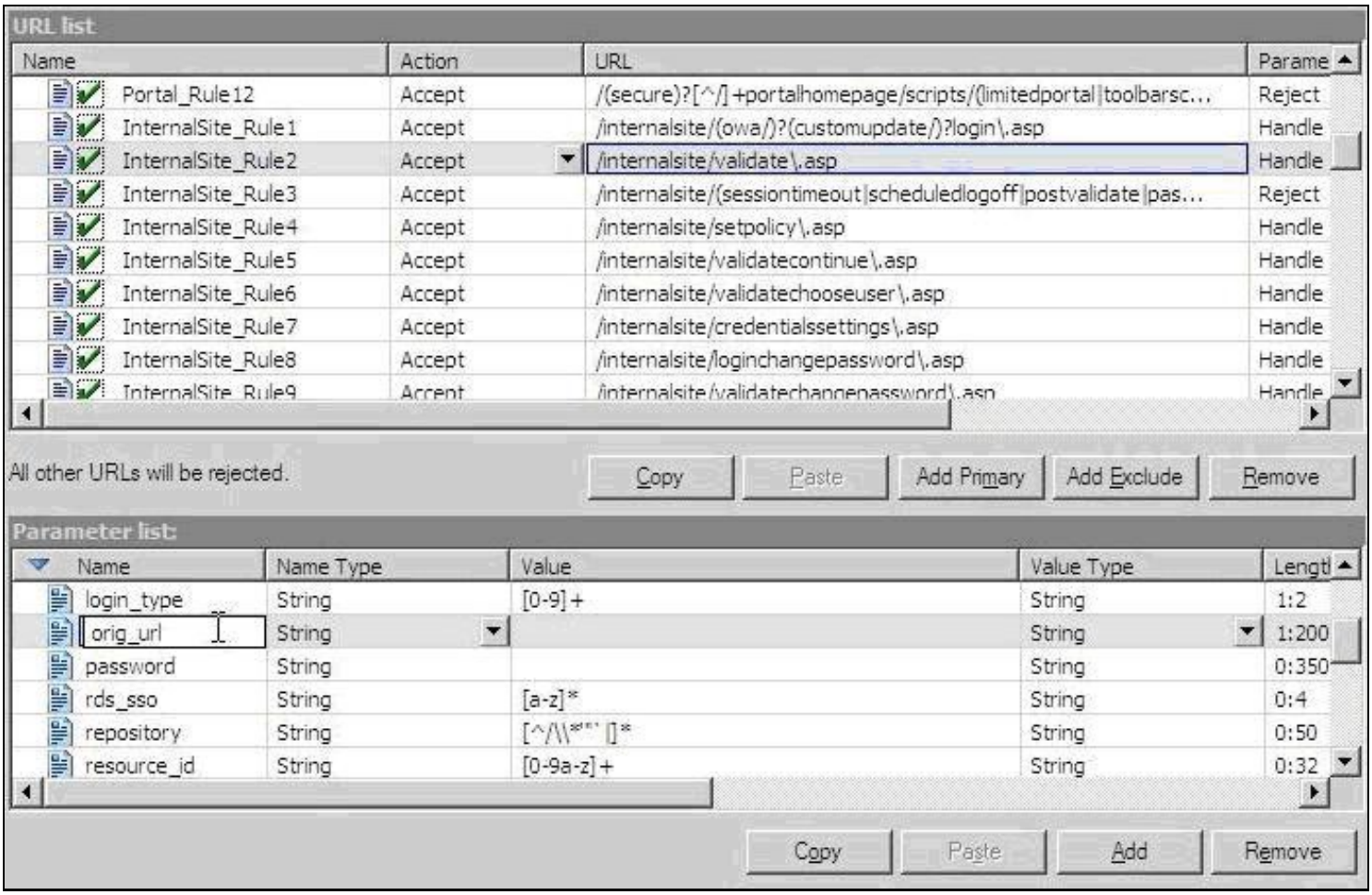
Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on





To allow access to the ChangePIN application

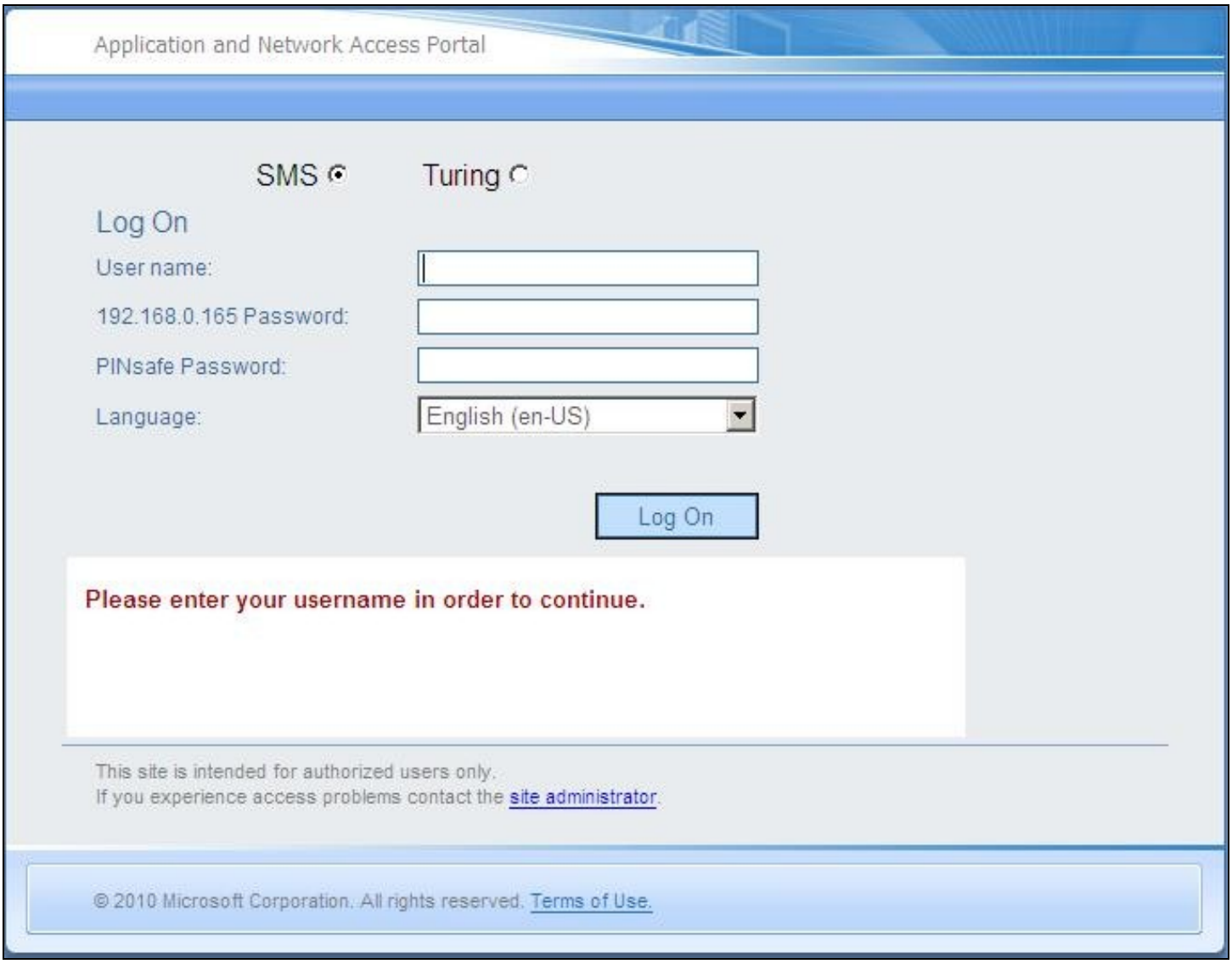
- Select the required Trunk
- Under Applications select Add
- Click the Web Applications Radio App and Generic Web App then Next
- Enter Application name ChangePIN and Application Type: pinsafe then Next
- Enter the ChangePIN IP address, and under path the location of the ChangePIN install (normally changepin), set the port to 8443, then Next
- Select Next
- Check details are correct, specifically https://<IP Address>:8443/changepin and then Finish

NOTE: If changing the IP address then change the IP address in the Application Properties on the Web Servers and the Portal Applications tabs.

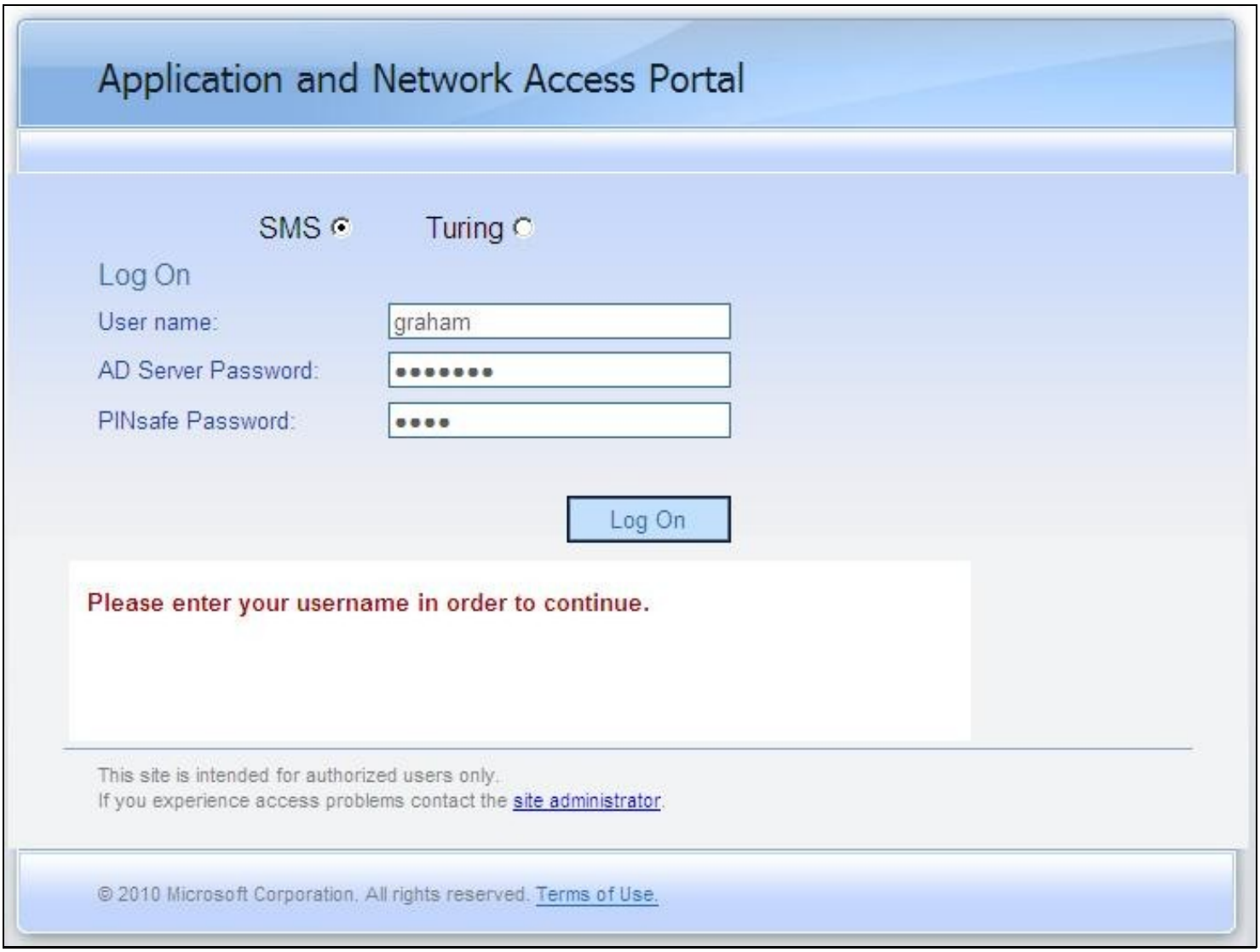
442.6 Verifying the Installation

Browse to the login page, select TURing and enter a username, the Turing image should appear. Test using the SMS option. Check for requests on the Swivel server.

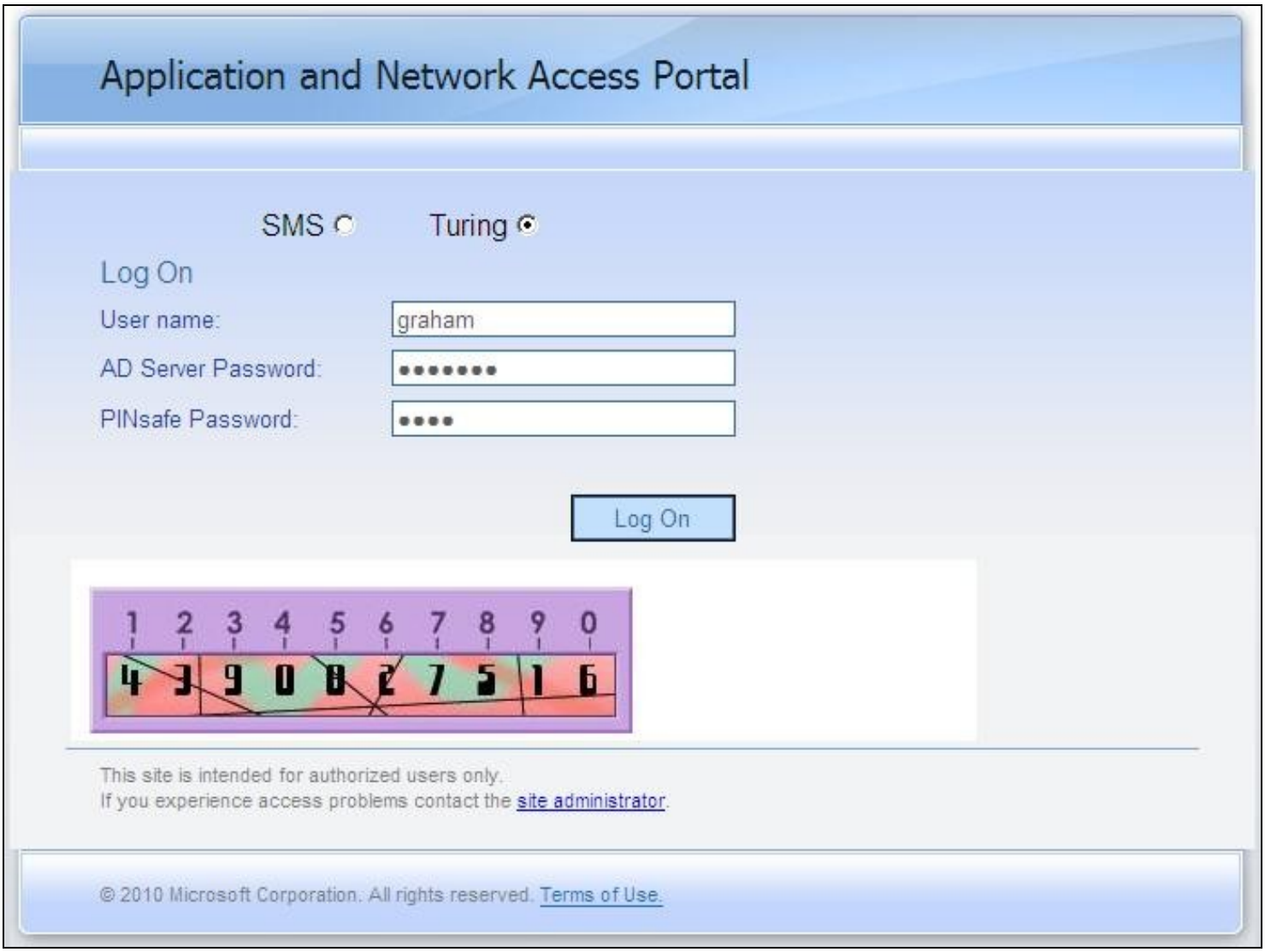
UAG Login Page



UAG login using SMS



UAG login using Turing Single Channel Image



Successful RADIUS authentication

The following user logged into trunk "test" (secure=0): User: admin; Source IP: 192.168.9.87; Authentication Server: PINsafe RADIUS; Session: B9FCC62A-B073-445D-9AAE-2FB1109EE5E6.

442.7 Troubleshooting

Check the Swivel server logs and system event logs for any errors or lack of communication as well as the UAG logs. Attempt a login and if required the TURing image, to generate an event then view it under under Admin/Web Monitor/Event Viewer/Security. Check the ISA server logs.

From a web browser on the UAG check to see if it is possible to generate a Turing image https://<IP address of Swivel server>:8443/proxy/SCImage?username=test

If the changes made in the UAG are not reflected in the login page, allow sufficient time for the rules to be written on the TMG (wait 10 minutes).

Request failed, the URL contains an illegal path. Trunk: test; Secure=0; Application Name: Whale Internal Site; Application Type: InternalSite; Rule: Default rule; Source IP: 192.168.9.87; Method: GET; URL: /InternalSite/Images/customupdate/images.asp?username=admin

URL blocking by the UAG. Check that the image can be rendered and that the URL rewriting rules are correct

The URL /internalsite/images/customupdate/images*.asp contains an illegal path. The rule applied is Default rule. The method is GET.

When the message *The rule applied is Default rule* is seen, it means that no rule has been matched and by default the URL is blocked. In the above example the path is incorrect to images.asp.

Http 500 error

If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

is replaced with

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

Ensure that the UAG can resolve the Swivel server name when hostname is used for connecting by RADIUS. Try with the IP address of the Swivel server.

442.8 Additional Configuration Options

442.8.1 RADIUS Challenge and Response

The UAG and Swivel supports the use of Challenge and Response authentication.

On the Swivel Administration Console ensure two-stage authentication is set to "Yes" for the RADIUS NAS definition. Secondly, under Server -> Dual Channel, ensure On demand authentication is set to "Yes".

In order to use two-stage authentication on Swivel, all users have to have a password defined. There are two ways to manage this: either set a password for each user under user administration, or enable the option to check password with repository (under Policy -> Password), in which case Swivel uses the AD password. Either way, you need to enter the password for Swivel as well as the AD password. (It might be possible, using the repository password option, to have a custom page that copies the AD password to the Swivel password, but this has not been tested).

If the Swivel password is entered correctly, you will be sent a security string, and a second login page will be displayed, to enter your one-time code.

442.8.2 PINpad Integration

PINpad integration can be accomplished using these files, and a slight modification to the installation procedure. Please note that this zip file reflects the relative locations of the 3 files included, starting from "InternalSite". The login page goes into /InternalSite/customupdate and the other two into /InternalSite/images/customupdate.

Please ensure that you have Pinpad enabled on your Swivel virtual or hardware appliance, following the instructions here.

Use pinpad.asp instead of images.asp from the original integration, and edit this in a similar way, replacing the internal URL for the Swivel appliance. Keep everything from "/proxy/SCPinPad" as it is. You will also need to make a similar change to StartSession.asp. One important difference to recognise with this solution is that it makes a session start request explicitly. Therefore, you cannot use the /proxy application. Instead, you must use port 8080 and context /pinsafe on a virtual or hardware appliance. This also means that you must have PINsafe version 3.9.2 or later, since earlier versions do not support PINpad natively. Make sure that the firewall rule is configured appropriately. If you have an earlier version of PINsafe, either upgrade, or use this older solution. If you use the older solution, note the differences below, and ignore any references to StartSession.asp.

Use /customupdate/loginpinpad.asp as the login page.

When configuring the URL rewriting rules, you will need to include pinpad.asp and StartSession.asp in /images/CustomUpdate as accepted pages, unless you have allowed all pages in /images/CustomUpdate. Either set "ignore" for all parameters for these pages, or else permit the following parameters:

- pinpad.asp:
  - sessionid (or username for the old solution)
  - padno
- StartSession.asp
  - username
  - random

NOTE: this login page assumes that PINsafe is the primary authentication. If it is the secondary, you need to edit the login page (loginpinpad.asp) and change the following line

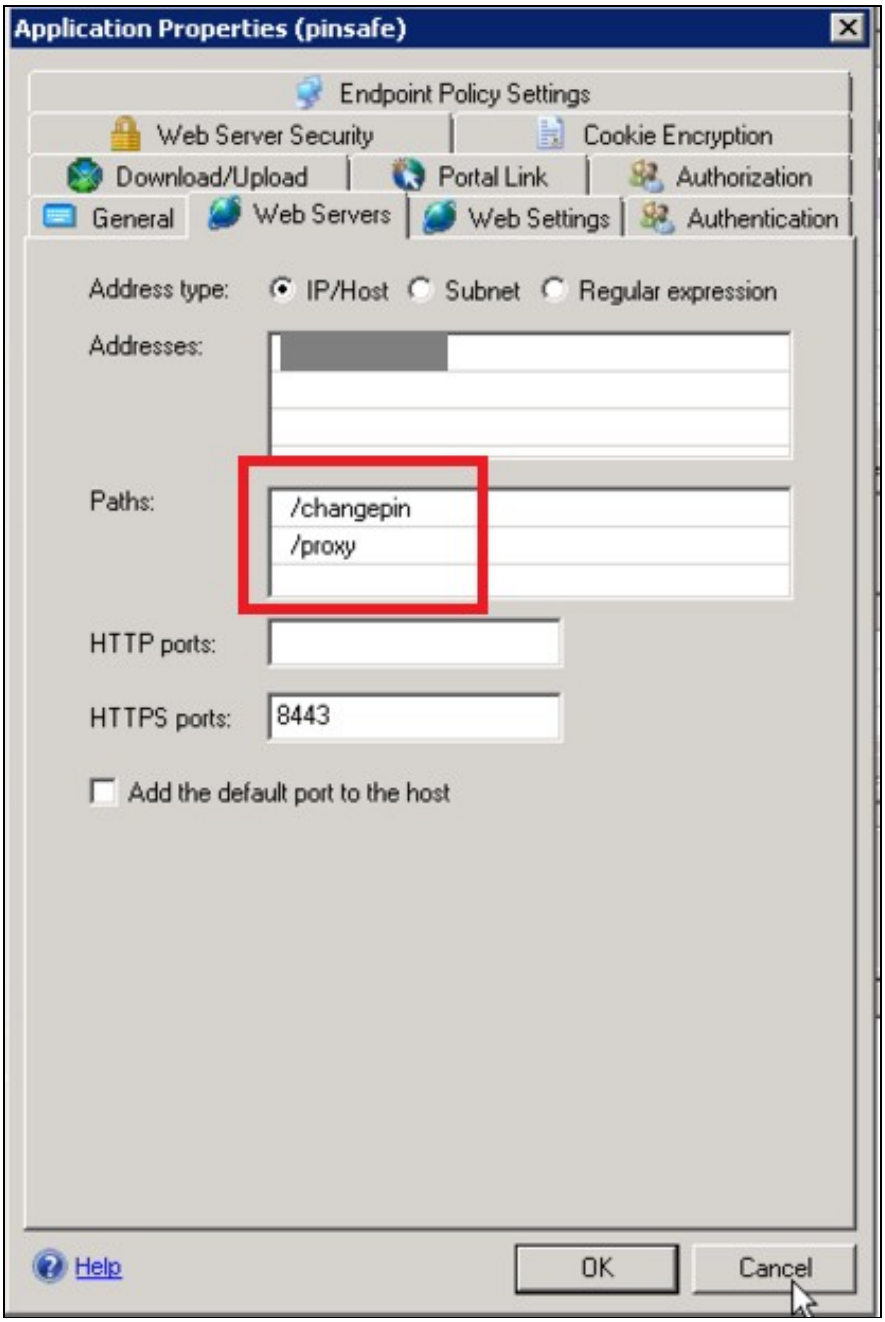
```
var PINSAFE_PASSWORD_INDEX = 0;
```

to this:

```
var PINSAFE_PASSWORD_INDEX = 1;
```

442.8.3 ChangePINpad Integration

When publishing access to ChangePINpad, ensure that you enable the following paths during creation:



This should in turn create the following rules:

pinsafe_Rule1	Accept	/changepin(/.*|$)	Ignore		POST, GET
pinsafe_Rule1_Proxy	Accept	/proxy(/.*|$)	Ignore		POST, GET

Beware that if you add paths to the published application afterwards, the rules for these paths will not be created. So ensure that you enter the paths at creation time.

442.8.4 Button size and aspect ratio

The Button size and aspect ratio is controlled by the settings in the login page:

document.all.otp.innerHTML = '<img src="/InternalSite/customupdate/FetchTuring.asp? username=' + otpusername +'" height="81" width="300">'; }

change the height and width settings to the value that is appropriate.

442.8.5 XML Authentication

Configuring XML authentication (when not using RADIUS)

XML authentication has not been tested with the current version of UAG and is supplied for reference if required, RADIUS authentication is the preferred method of authentication.

Note that when using a Swivel virtual or hardware appliance with a proxy configured, the XML requests need to be made to the https://<IP>:8080/pinsafe address rather than the proxy address. This applies currently to all Swivel virtual or hardware appliance versions.

This step is not required when RADIUS authentication is used. RADIUS authentication is the preferred method of authentication. To enable the token.inc file, create a repository of type ?Other? on the UAG configuration. The repository you create must match the name of the file (ie, if the inc file is called Token.inc, the repository must be named Token).

Configure a Swivel Agent (For XML Authentication)

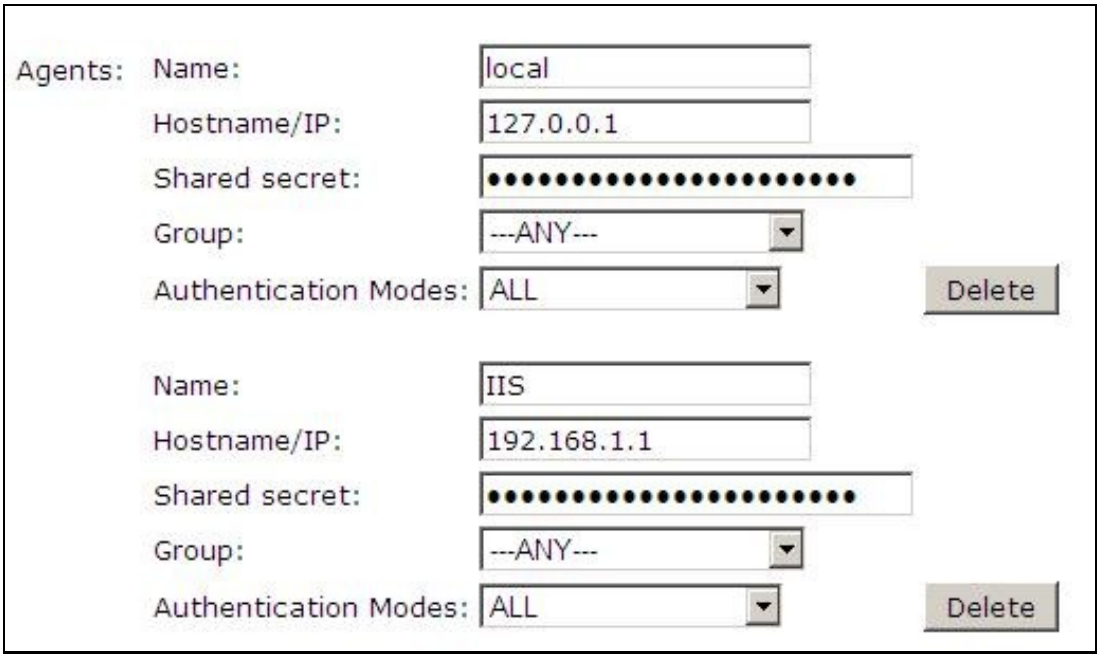
1. On the Swivel Administration Console select Server/Agent

2. Enter a name for the Agent

3. Enter the UAG internal IP address

4. Enter the shared secret

5. Click on Apply to save changes



To create the repository, do the following-

1. Access the UAG configuration GUI.

2. Click on Admin Authentication Users/Group repository

3. Select New to create a new repository

4. In the drop down menu, select ?Other? and in the Name field type in the name of the inc file (See screen shot below)

5. Click on Add and apply this repository to the relevant trunk.

6. Activate the configuration

Edit the file Token.inc with the required shared secret and to represent the Swivel server IP address and Swivel install name, Note for all Swivel installs this needs to point to the PINsafe server on port 8080 and not the proxy port 8443.

```
m_secret = "secret"

objWinHttp.Open "GET", "https://192.168.1.1:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Note If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

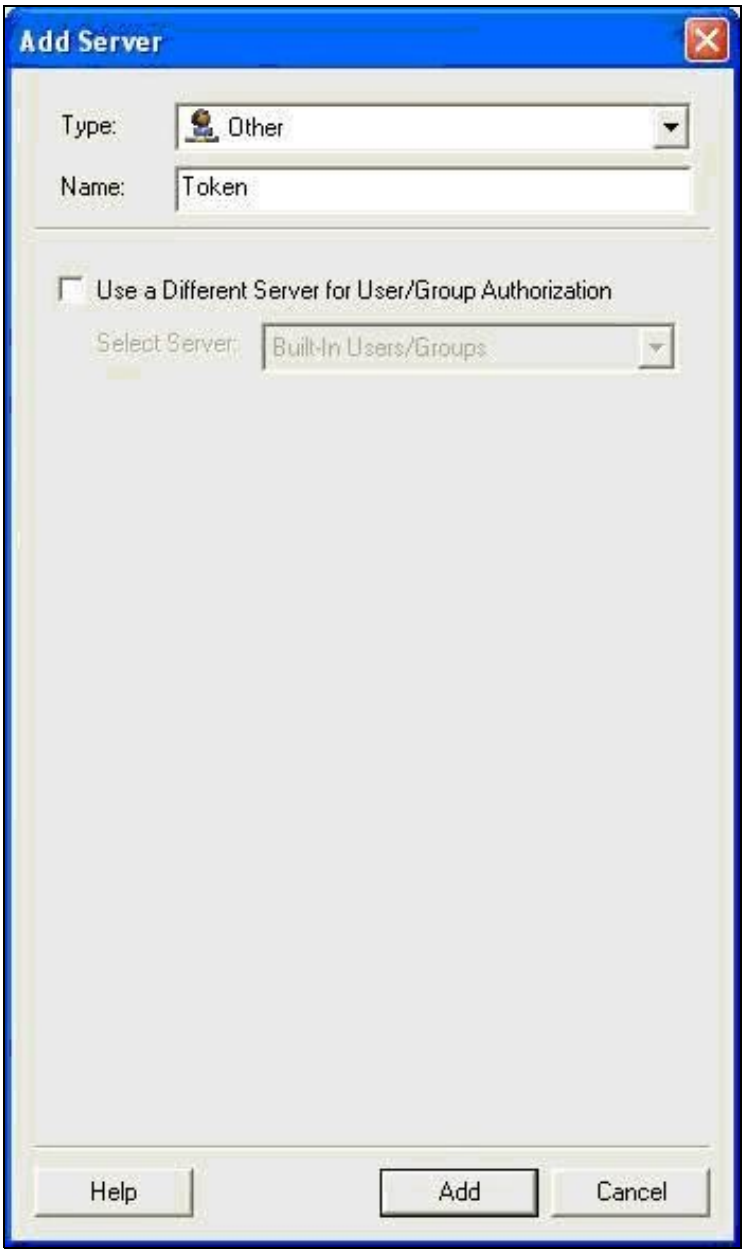
```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

is replaced with

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

Edit the file Portalname1postpostvalidate.inc to represent the PINsafe server IP address and changePIN install name:

```
'response.redirect "https://192.168.1.1:8443/changepin"
g_orig_url = "https://192.168.1.1:8443/changepin"
```



442.9 Known Issues and Limitations

If upgrading the UAG to a higher service pack, the configuration files, particularly login.asp may be overwritten. Verify the files after an upgrade. Also note that the URL rewriting rules may differ from version to version, so these should also be verified.

Upgrading from RTM Update 2, to SP1 will cause the InternalSite rules, on the UAG to be removed, or changed back to defaults.

If the login page is viewed incorrectly as a mobile page then this workaround will allow the correct page to be displayed, and works with Windows 7 and Windows 8.

442.10 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

443 Microsoft Windows Credential Provider Integration (Legacy OS)

444 Introduction

Microsoft Windows Credential Provider is used in the desktop operating systems Windows Vista, 7, 8 and 8.1, and in the server operating systems Windows Server 2008 and 2012, including Remote Desktop Gateway. For newer operating systems (Windows Vista and Server 2012 R2 onwards), see Windows Credential Provider. For integration with the older Windows GINA used in Windows 2000, 2003 and XP see Microsoft Windows GINA login.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

For new features in recent releases of the Credential Provider, see below.

444.1 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel does have the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance.

Q). Is it possible to define users who do not have Swivel authentication? A). Only by using the *Allow Unknown Users* for non Swivel user authentication.

Q). Is it possible to login without AD password, A). No the AD password is required.

445 Prerequisites

Swivel 3.x Server

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled)

Microsoft Windows Vista, 7 or 8 (including 8.1); Microsoft Windows 2008 or 2012 Server (including R2).

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 4.6) or

Swivel Windows Credential Provider 32 bit (version 4.6) or

Both of the above files in a single zip

Documentation only

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

446 Baseline

Swivel 3.7

Windows 7, Windows 2008 Server R2

447 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

447.1 Offline Authentication

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, and cycles through these so there is no limit on the number of authentications which can be made. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

448 Swivel Integration Configuration

448.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent

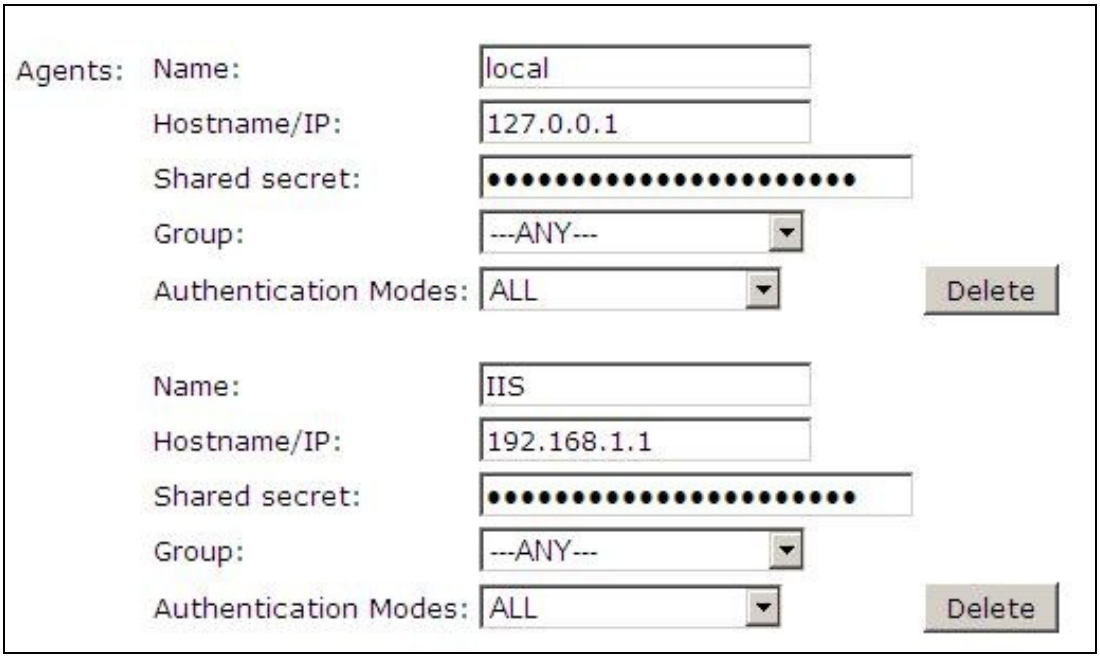
2. Enter a name for the Agent

3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.

4. Enter the shared secret used above on the Credential Provider

5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)

6. Click on Apply to save changes

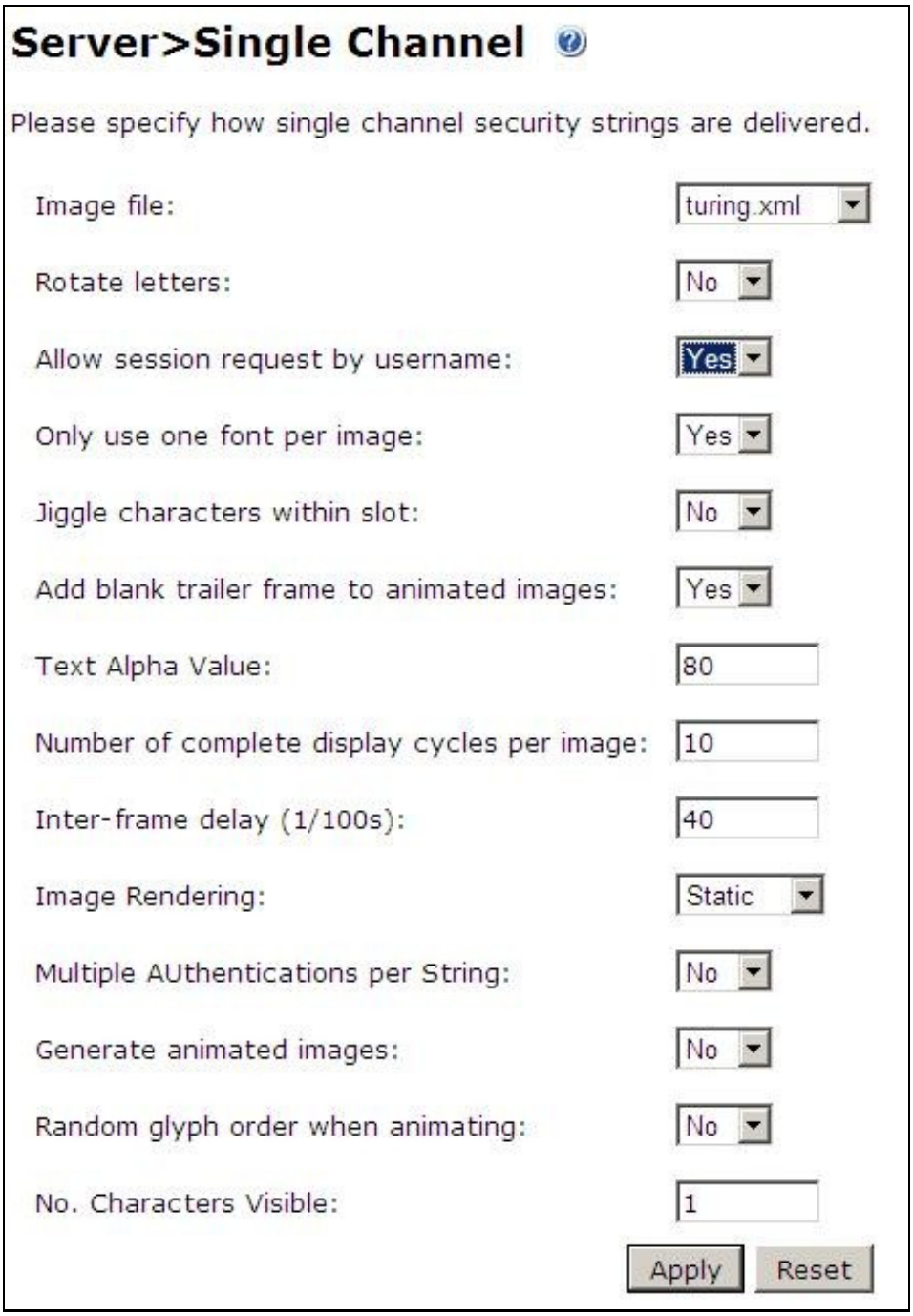


Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

448.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



448.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured)

1. On the Swivel Management Console select Server/Third Party Authentication

2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA)

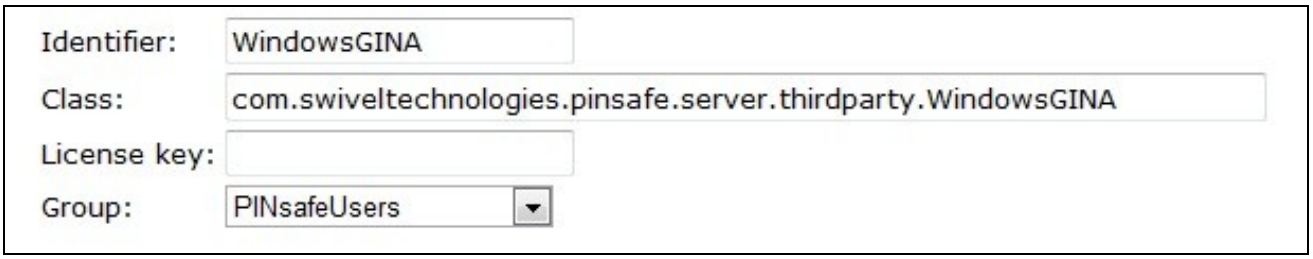
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA

4. For the License Key, leave this empty as it is not required

5. For the Group select a group of users (Note: the option Any cannot be selected)

6. Click Apply to save the settings

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.


Identifier:
WindowsGINA
Class:
com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
License key:
Group:
PINsafeUsers

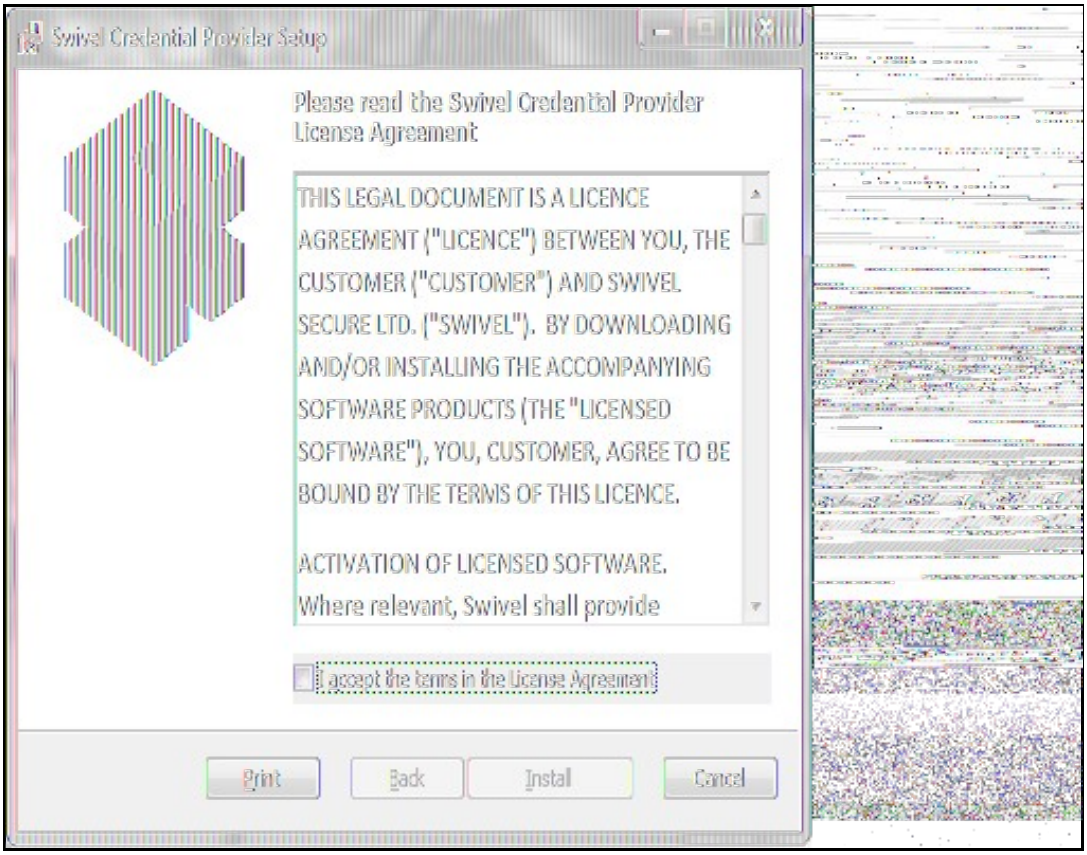
449 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Ensure that the correct Swivel Windows Credential Provider is used: SwivelCredentialProvider_x86.msi for 32-bit or SwivelCredentialProvider_x64.msi for 64-bit.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

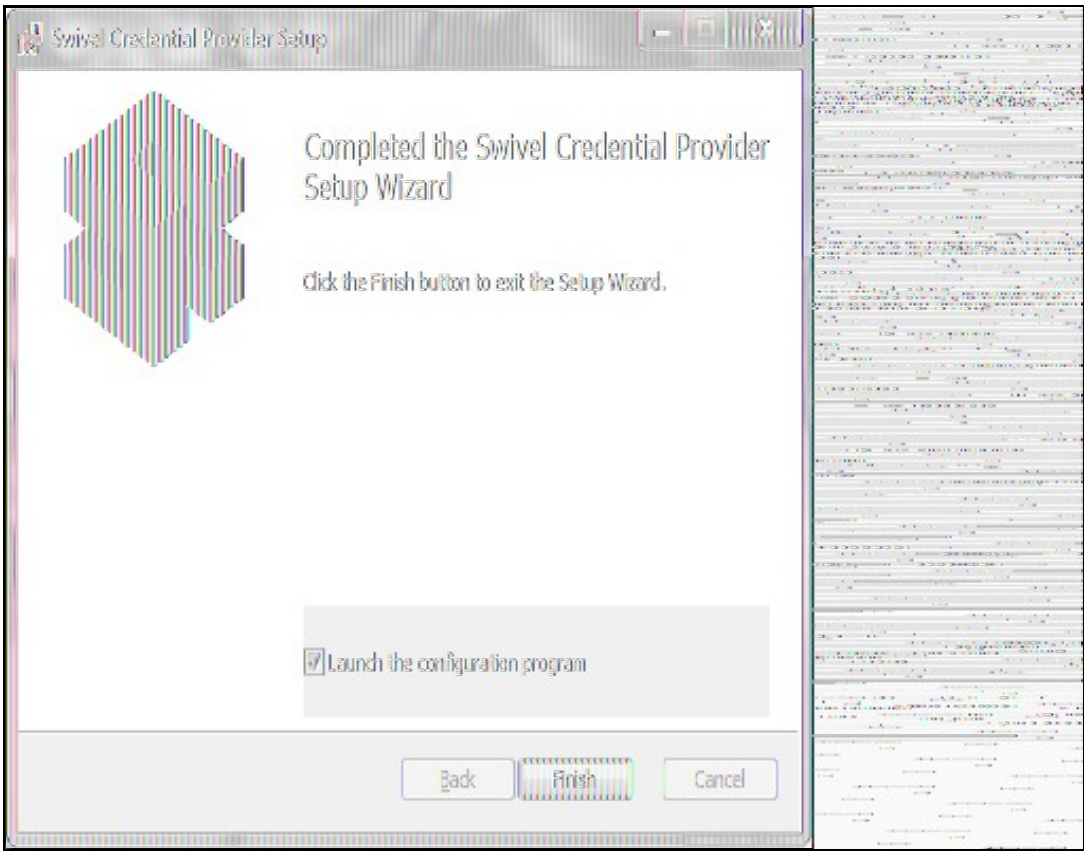
The first page is the licence agreement:



Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

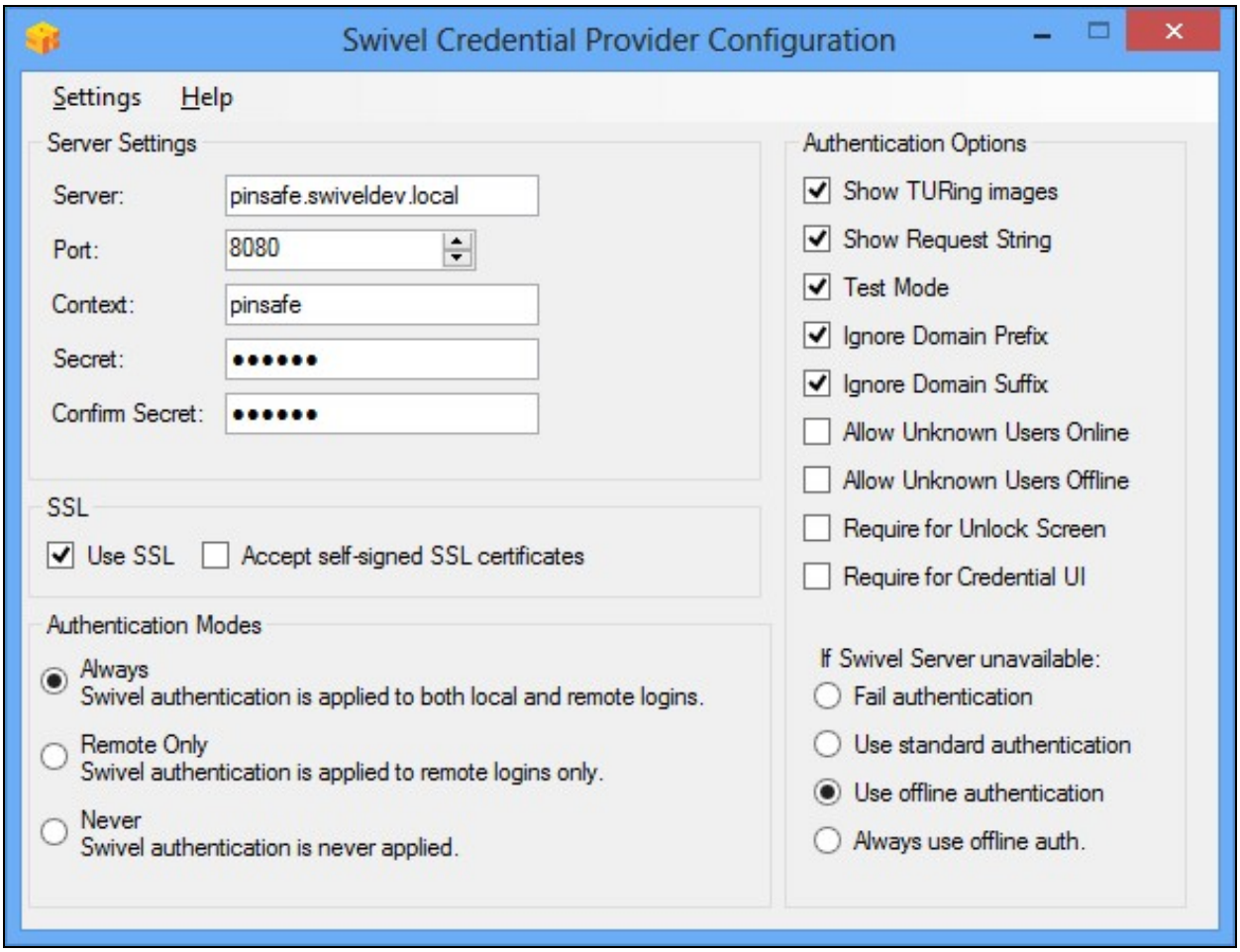
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



Ensure that the tick box is checked for *Launch the configuration program* to configure the Swivel instance then click on Finish.

449.1 Windows Swivel Credential Provider configuration



The following options are available:

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience for use the VIP on a swivel virtual or hardware appliance, see VIP on PINsafe Appliances

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port

Context: The Swivel virtual or hardware appliance or server installation instance

Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts).

Authentication Mode, Always Swivel authentication is required for remote and local logins

Authentication Mode, Remote Only Swivel authentication is required for remote logins only

Authentication Mode, Never Swivel authentication is not used

Show TURing images Show TURing images if requested

Show Request String Show the Request string image to allow the user to obtain a new security string by dual channel

Test Mode With test mode the user can switch user to a standard authentication, see below

Ignore Domain Swivel will remove any domain prefix (domain\username) or suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If offline authentication is used, users that do not have credentials cached locally can authenticate using Windows credentials only. Any OTC entered will be ignored. If the user has previously authenticated in online mode, then they must enter the correct one-time code.

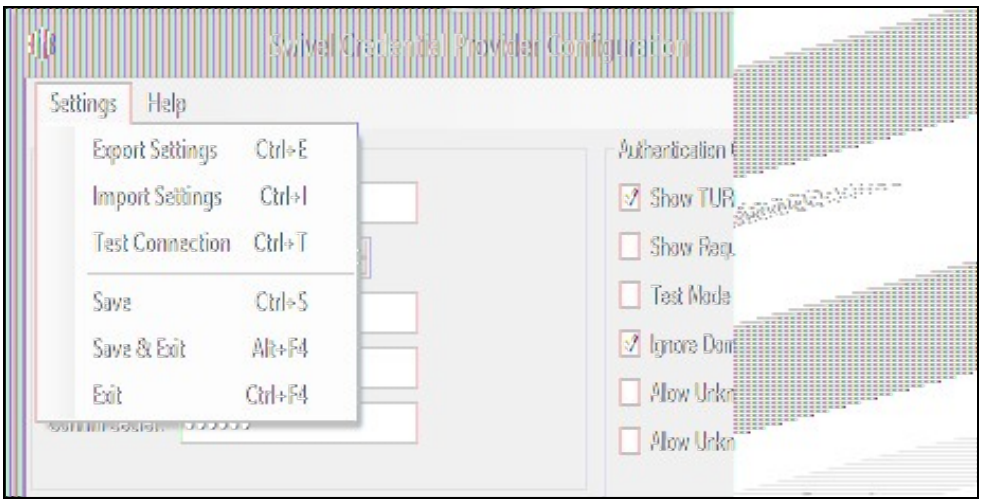
If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog.

Always use local auth A local Turing image is always used and the Swivel server is not contacted. All users must previously have authenticated using online authentication (unless the option "Allow unknown users offline" is enabled).

The remaining options are available from the Settings menu:



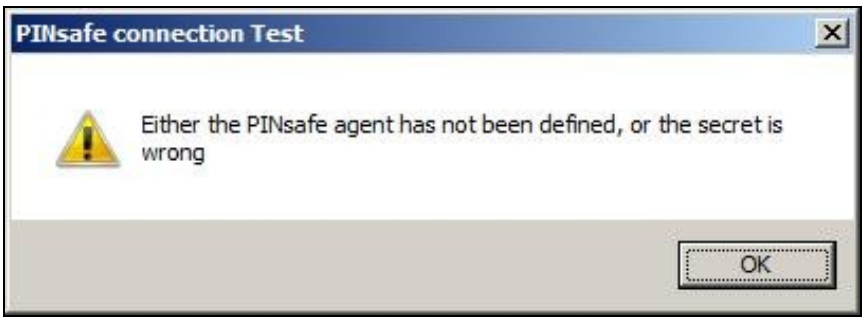
Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

Test Connection Tests link to Swivel server:

A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**

Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**



Save Save the current settings.

Save and Exit Save the current settings and close the program.

Exit Close the program without saving the settings. You will be prompted to confirm if any settings have been changed.

449.2 Additional Installation Options

449.2.1 Manually configuring the Swivel Login

NOTE: It is recommended to use the Swivel Login Configuration Tool where possible.

If it is not possible to use the configuration utility the Swivel Login settings may be edited manually in the registry. The following values found within the "HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\Swivel Credential Provider" key are used by the Login:

PINsafeServer - The name or IP of the Swivel server

PINsafePort - The Swivel server port

PINsafeContext - The Swivel server context

PINsafeSecret - The Swivel agent secret

PINsafeProtocol - 1 for https, 0 for http

PINsafeAllowSelfCert - 1 to allow SSL requests to a Swivel server with certificate errors, 0 not to

PINsafeLoginSelect - determines when Swivel authentication is required: always, remote or disabled.

PINsafeShowTURing - 1 to show the TURing request link, 0 not to

PINsafeRequestString - 1 to show the request string link, 0 not to

PINsafeAllowDefaultLogin - 1 to allow default login if Swivel unavailable, 0 not to

PINsafeUseLocalAuth - When to use local TURing authentication: always, fallback or never.

PINsafeDisableFilter - 1 to enable test mode, 0 to hide the standard authentication option

PINsafeAllowUnknownUsers - 1 to allow unknown users in online mode

PINsafeAllowUnknownOffline - 1 to allow unknown users in offline mode

PINsafeIgnoreDomain - 1 to ignore the domain prefix when checking Swivel users

The following values may be seen in this registry key also, but should not be changed:

PINsafeBackgroundsFolder

PINsafeFontsFolder

PINsafeResourceDLL

PINsafeHelpUrl

Directory

Uninstaller

Version

449.3 Test Mode

In Test Mode the Windows Credential Provider has an additional login that can be used as a standard user login. In test mode the last successful login will be selected for login.

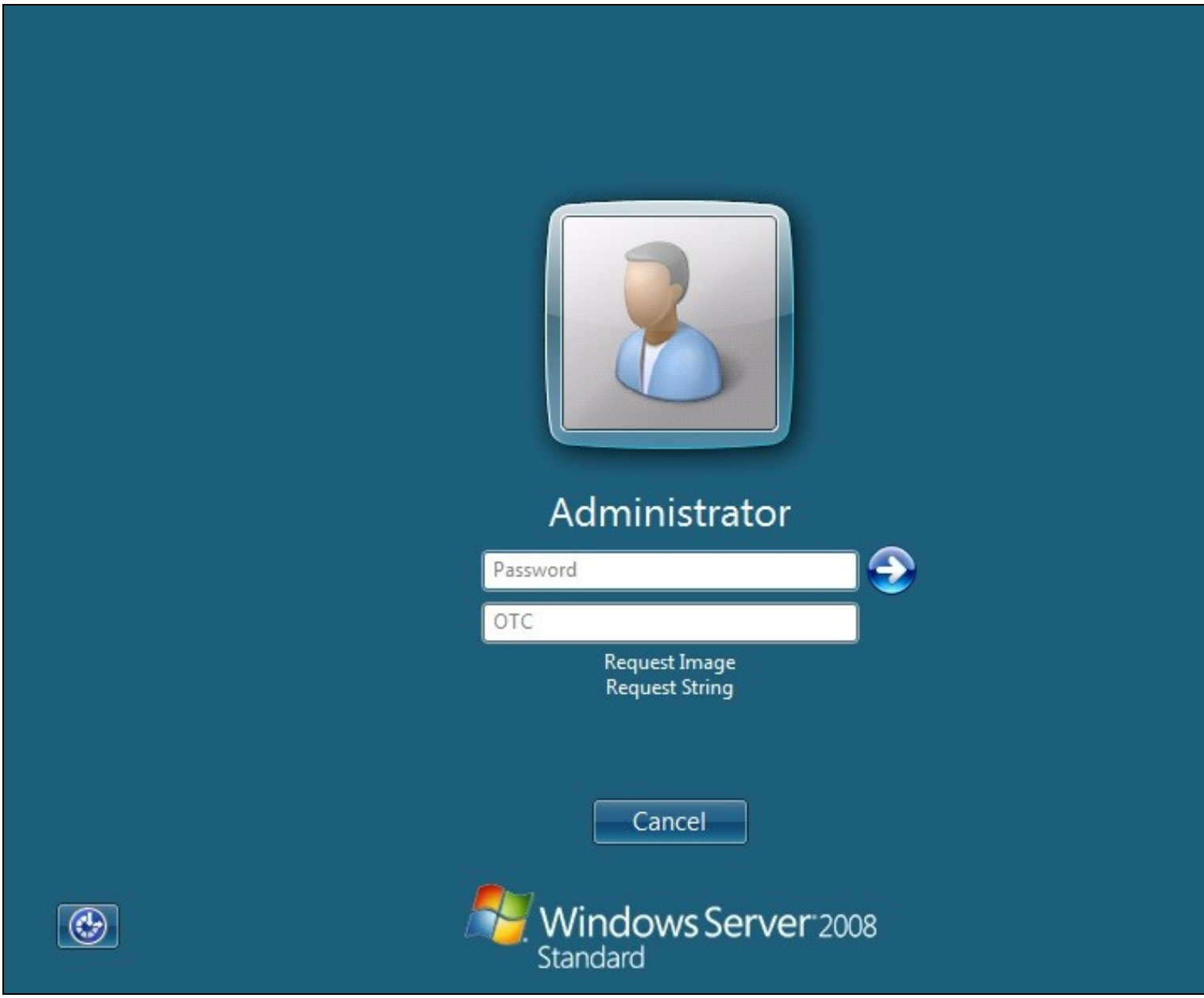
The Swivel credentials will always be on the left, the standard credentials on the right.

449.4 Importing Configurations

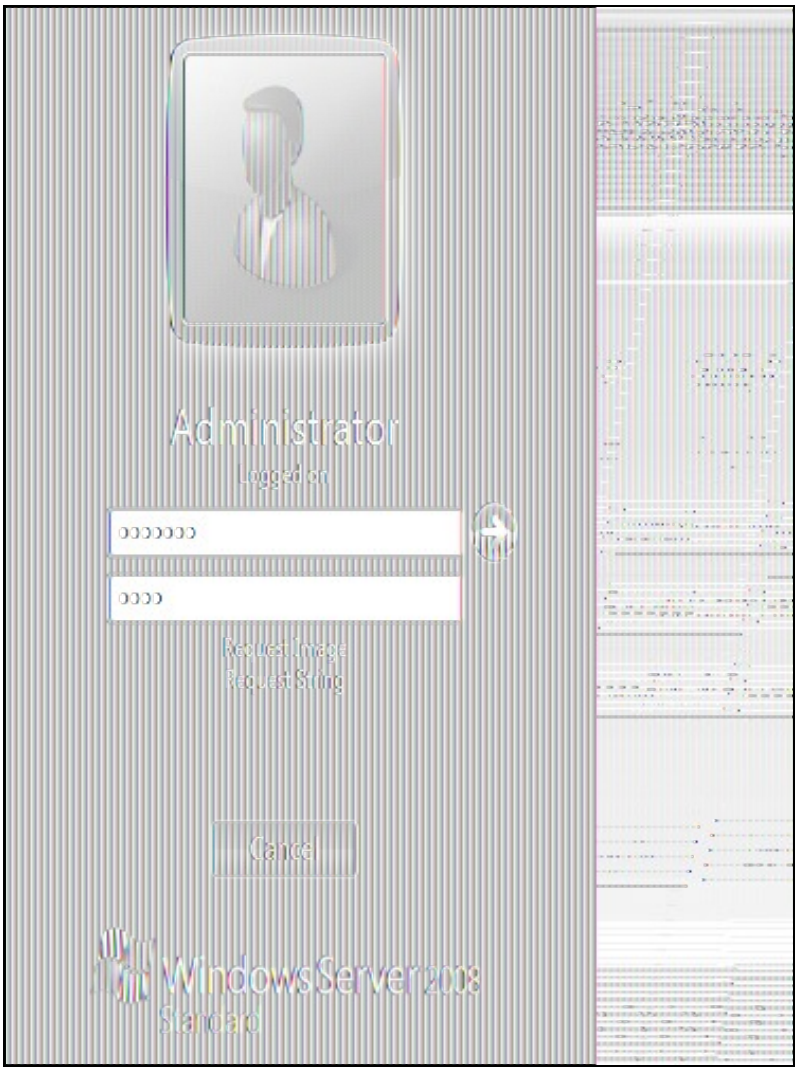
You can import credentials exported from other installations using the Import Settings menu item. Alternatively, if you need to install the Credential Provider on a large number of machines, you can modify the .msi file and replace the blank LoginSettings.xml file included with your own custom version. If you do not have the ability to modify MSI files, you can email your settings to support@swivelsecure.com and request a custom build.

450 Verifying the Installation

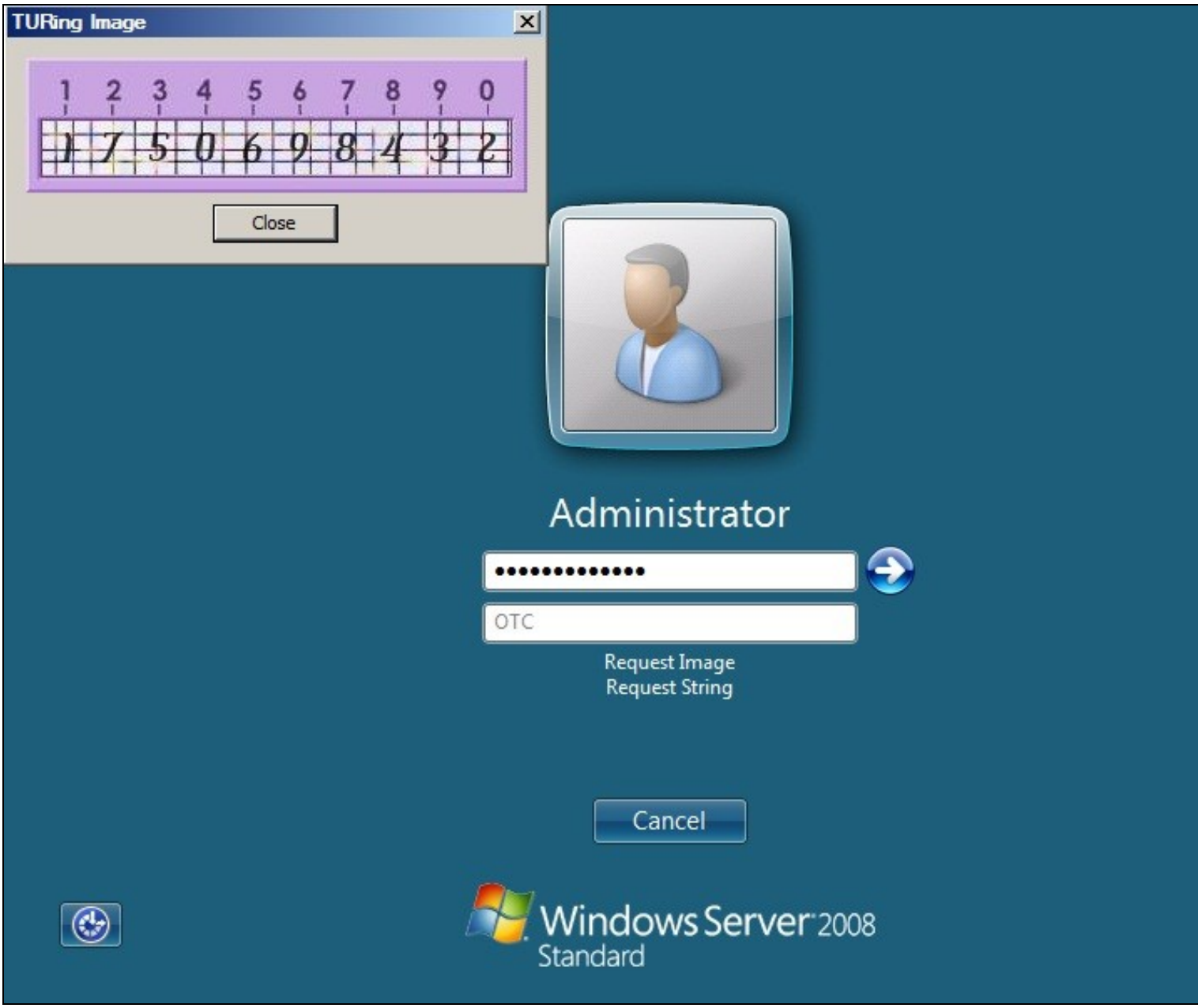
At the windows login a password and OTC login field should be available with Request Image and Request String options available.



If a Dual Channel login is made then the user should be able to enter their OTC. Note the Get Image should not be pressed, otherwise the log will be expecting a Single Channel login for the length of the session timeout (default 2 minutes).



Selecting the Request Image button should generate a Single channel Image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*

A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*

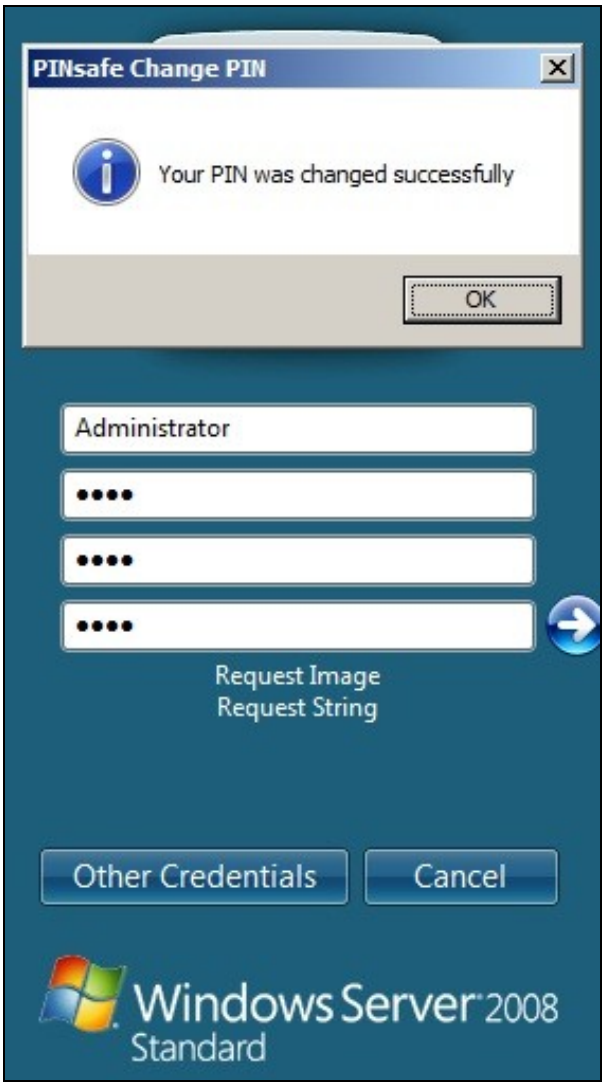
451 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (CTL-Alt-End for remote sessions). With the Windows Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the Other Credentials. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

A successful Change PIN will show the message **Your PIN was changed successfully**



The Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**

452 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

453 Troubleshooting

Test Mode enables you to login using the Standard Windows authentication and not Swivel authentication. If you disable Test Mode the additional logon users disappear and the machine will then be purely using Swivel.

If there is a problem then use Windows Safe Mode to login and enable Test Mode again. Safe Mode uses Standard Windows authentication.

Pressing Ctrl+Alt+Del reverts user back to login screen

A normal login may be attempted after a short period. This can occur as the Windows login screen may appear before a network connection has been made during boot. To prevent the login screen from not being accessible, enable the option in group policy to Wait until network is ready before user logon.

User must select the back button and select Other User to logon

This occurs when the system is running in Test mode. Disable the Test mode to allow normal login.

Change Pin is displayed instead of the logon screen

This has been seen on Dell laptops that have the *Dell Control Point Security Manager* installed. Remove this prior to the Windows Swivel Credential Provider installation.

FLUSHING_IMAGE_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the Swivel log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

Double User Entry at login, enforced test mode when test mode is disabled

Some fingerprint scanning software may cause this issue, this has been seen on an IBM Thinkpad. Check in the registry under the following

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters

look for keys which have values of: Fingerprint Logon Credential Provider Filter

and

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

look for keys which have values of: Fingerprint Logon Credential Provider

To test if these are the cause, on a test system, either remove the fingerprint software (disabling may still leave the registry keys) or backup the keys by exporting them, then remove them.

453.1 Disabling the Swivel Login

If the Swivel Login fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Either run the Swivel Login Configuration and edit the settings or

Using regedit.exe remove the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

Reboot Windows

Following this process the standard Windows Login should be restored allowing access.

453.2 Error Messages

Unable to contact PINsafe server

Version 4.x only supports TLSv1 which means if you are running a version 3 Appliance, you must enable TLSv1 under Tomcat > SSL Protocols > Enable TLS1.0.

Wrong Parameter or **Parameter is incorrect**

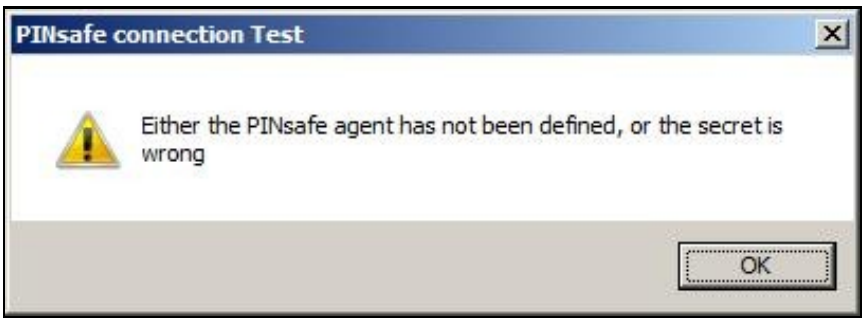
This message is displayed at the Windows login and can have several causes, check the Swivel logs for errors:

- The user must exist in AD and Swivel
- When an incorrect OTC is entered, when using local authentication. Unfortunately, local authentication will not work with the "Connect To" dialog. However, you should still get the remote desktop login displayed, and will be able to authenticate to this.
- The user account is locked in Swivel
- The Swivel Sever Agent has not been configured correctly

Please enter a one-time code first

A One Time Code was not entered in the OTC field during login.

Either the Swivel agent has not been defined, or the shared secret is wrong



AgentXML request failed, error: The agent is not authorised to access the server.

The credential Provider is not permitted to connect to the Swivel server. Add an Agent for communication.

The user name or password is incorrect.

Check Password with Repository: If this setting is enabled against the Agent, then you should disable it to prevent it attempting to check for a password against the repository. This is a potential cause when receiving "The user name or password is incorrect".

AgentXML request failed, error: No suitable authentication method for the user "Administrator" was found. The user may be missing from the user repository or a synchronisation has not yet occurred.

The user Administrator is not defined as a Swivel user

Session start failed for user: x, error: No Data for user was found. or **error: No data for the user was found**
The requested user does not exist in the database. If the user does exist in the repository (e.g. Active Directory) then Swivel needs to sync with that repository.

Dual channel message request failed, error: On-demand dual channel delivery is disabled.

A dual channel message request was made but the On-demand delivery is not enabled. If it should be enabled, on the Swivel Administration console select Server/Dual Channel, then set On-demand delivery to Yes.

AgentXML request contained third party data for a third party class that does not exist. Third Party Class ID: WindowsGINA.

and

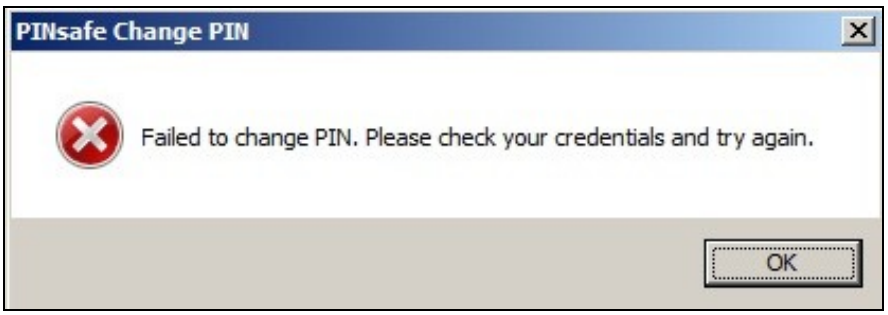
error: The third party class could not be found.

The Third Party Authentication class does not exist or has been created incorrectly. Create the class, see Create a Third Party Authentication

The third party class could not be found

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

Failed to change PIN. Please check your credentials and try again.



The user has failed to change the PIN number. This could occur if the Swivel server cannot be contacted.

Unhandled exception has occurred in your application. If you click Continue the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

The remote Server returned an error: (502) Bad Gateway.

This error has been seen when a Test Connection is made from the Credential Provider and can be caused by being unable to connect to the Swivel server. Check for network settings such as proxy settings on the local server, and if an SSL connection is required.

454 Release Notes

454.1 Release of Version 4.6

4.6.2.1, released 27th June 2016.

The main change in version 4.6 is that there is better support for offline authentication: it has been observed in previous versions that the strings ran out after a number of offline authentications. This has now been resolved.

There is a known issue with version 4.6, in that it requires Microsoft Update KB2999226 to have been applied. This should be applied automatically by Windows Update, but if you have a problem installing or running the program, check that this update has been applied.

454.2 Release of Version 4.5

4.5.4.1, released 4th February 2015.

Version 4.5 includes the following fixes and enhancements over previous versions:

- Swivel authentication is optionally applied to the Unlock screen as well as the login screen
- Swivel authentication may be disabled (and by default is disabled) when connecting to remote computers
- The image window resizes dynamically depending on the type of image. The scale option is on the Settings drop-down menu.

454.3 Release of Version 4.4

Version 4.4 includes the following fixes and enhancements over the previous releases:

- It is fully-compatible with Windows 8 and Windows 2012 Server.
- It switches to single-channel mode if local authentication is enabled and the Swivel server is not available.
- Unlike the previous beta, version 4.3, this version is compatible with ALL Windows Operating Systems from Windows Vista onwards.
- If the user's password has expired, they are correctly redirected to the change password page.
- A problem which occasionally caused crashes when entering the username has now been resolved.
- You can now import settings exported from other installations.
- The installer is now a standard Windows MSI file. This makes it possible to customise the installation to contain your company's settings file, if you have the tools to modify MSI files. Alternatively, you can send your exported settings to support@swivelsecure.com, who can create a custom installer for your organisation.

455 Known Issues and Limitations

This version of the Swivel Credential Provider is not compatible with the Swivel version 3 appliance. An update will be available shortly.

The Swivel Windows Credential Provider does not support the use of

- Pinpad
- Animated gifs

for Single Channel authentication.

It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.

Local authentication only works in single channel mode: the dual channel strings are not available offline. To use offline authentication, TURing image display must be enabled, even if normal authentication is dual channel.

If a Swivel server has been configured with a Single Channel login configuration that is not viewable, the following options are available to recover access:

- Login using dual channel
- Login using an image generated elsewhere such as on the Swivel Administration console or Taskbar on another server
- Alter the settings on the Swivel server to serve a permitted image
- Login offline if permitted
- Login to safe mode as described elsewhere

In Windows 8 and Windows Server 2012, the Credential Provider appears as a single key icon, which you must select before logging on. In some cases, where Windows should show the last used credential, you will need to click the back arrow and then select the Credential Provider. A similar problem occurs with the Unlock screen. An updated version, specific to Windows 8 and Windows Server 2012, will be released in due course.

By default, the credential provider assumes that administrator is the local administrator, rather than the domain administrator, so you have to explicitly state the domain name to logon as domain administrator. This is a feature of the default credential provider as well.

In the Swivel administration console, the Windows GINA menu item is present, but there are no configurable options, so is not selectable.

456 Microsoft Windows Small Business Server 2011

457 Introduction

Built on Windows Server 2008 R2, Windows SBS 2011 Standard includes Microsoft Exchange Server 2010 SP1, Microsoft SharePoint Foundation 2010 and Windows Software Update Services.

This configuration document outlines how to integrate Swivel with Microsoft Small Business Server 2011 authentication in addition to the Swivel authentication.

458 Prerequisites

Microsoft Small Business Server 2011

Swivel 3.x server

Swivel Small Business Software.

459 Baseline

Swivel 3.9

460 Architecture

The SBS makes authentication requests against the Swivel server by XML.

461 Installation

461.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

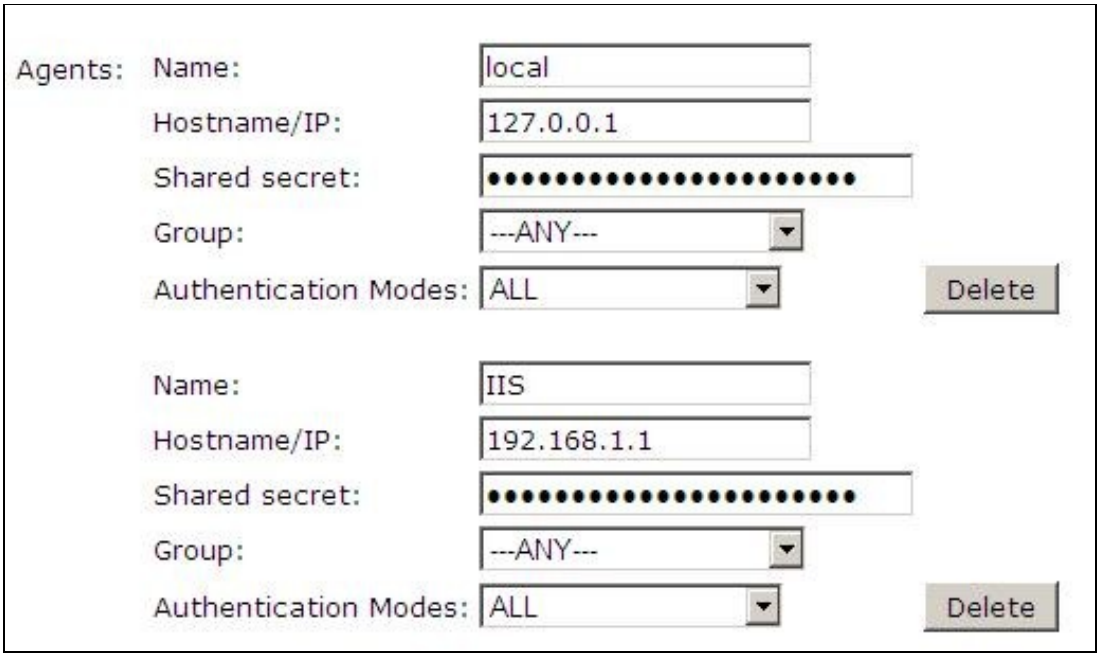
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the SBS

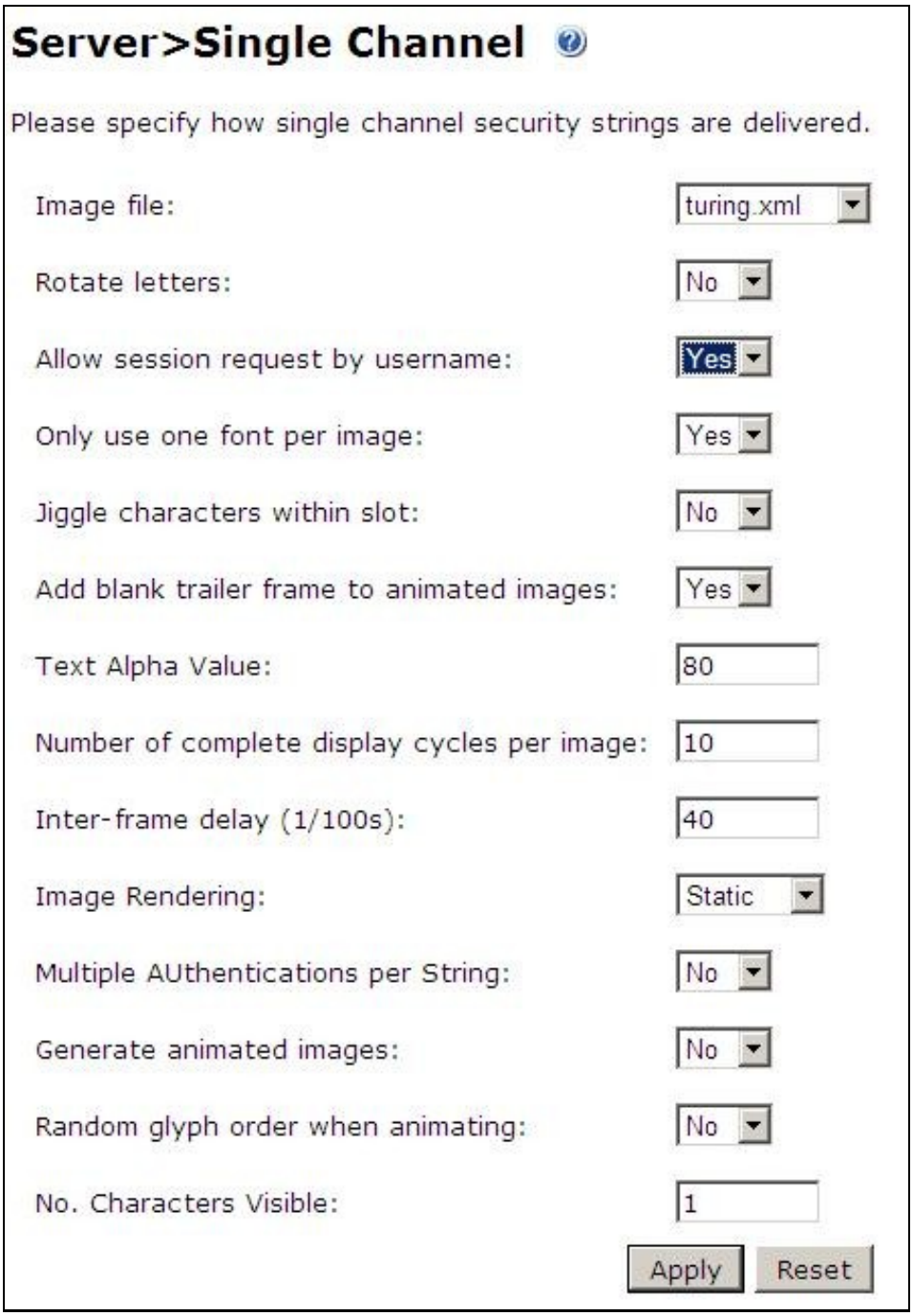
5. Click on Apply to save changes



Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



461.2 Configure the SBS 2011

1. Extract the files from the zip folder

2. Copy all the DLLs from the Bin folder to the Bin folder of the SBS application (by default C:\Program Files\Windows Small Business Server\Bin\WebApp\RemoteAccess).

3. Copy pinsafe_image.aspx from the AccountPage folder of the zip to the AccountPage folder of the SBS application.

4. Backup the existing SBS server Logon.aspx. Modify the existing Logon.aspx on the SBS server by locating the relevant sections in the customised Swivel Logon.aspx and copying to the SBS server Logon.aspx. Search for "Swivel Customisation Start". There are three separate sections. Copy each section into the existing Logon.aspx file (the end of the section is marked by "Swivel Customisation End"). It should be clear from the original file where the sections should go.

5. Backup the existing SBS server web.config. Modify the existing web.config on the SBS server by locating the relevant sections in the customised Swivel web.config and copying to the SBS server web.config. There are three sections to change, marked as before. The first one adds the Swivel filter as a HTTP module. The second adds an exclusion to default authorization, so that the TURing image can be displayed without having to authenticate. The third is the list of settings for the PINsafe server. You may find you have to create the <appSettings> section as well as inserting the settings, or you may find that there is a single, empty <appSettings /> entry. In the latter case, replace that with the entire <appSettings> section in the custom file. You will need to change the value="" entries to match the PINsafe settings for your local environment.

6. Finally, restart IIS (this may not be strictly necessary, but it's always best to make sure).

462 Verifying the Installation

463 Troubleshooting

464 Additional Configuration Options

465 Known Issues and Limitations

466 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

467 Netgear

468 Introduction

This article explains how to integrate the Netgear SSL VPN product set with PINsafe. This article has been created based on the Netgear FVS336G v2 Product. It is assumed that other products that support Banner Text in the same way (such as the SRX5308) can be integrated in the same way. The Netgear FVS336G v2 Product allows a proxy to be created to PINsafe by creating access through a firewall rule.

Note that a firmware upgrade maybe required to support this integration.

469 Baseline

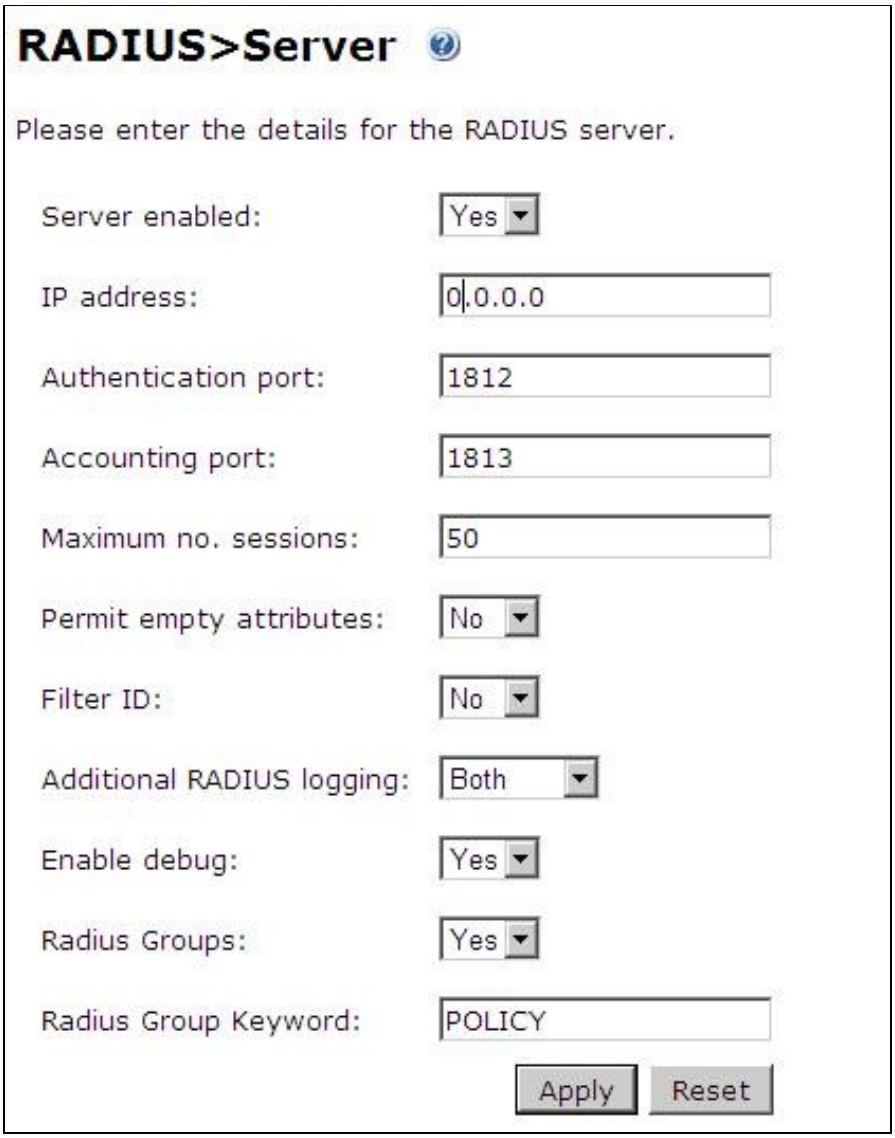
This integration is based on FVS336G v2, Firmware 3.0.7-13 and 3.0.7-24 with PINsafe Version 3.8

470 PINsafe configuration

470.1 Configuring the RADIUS server

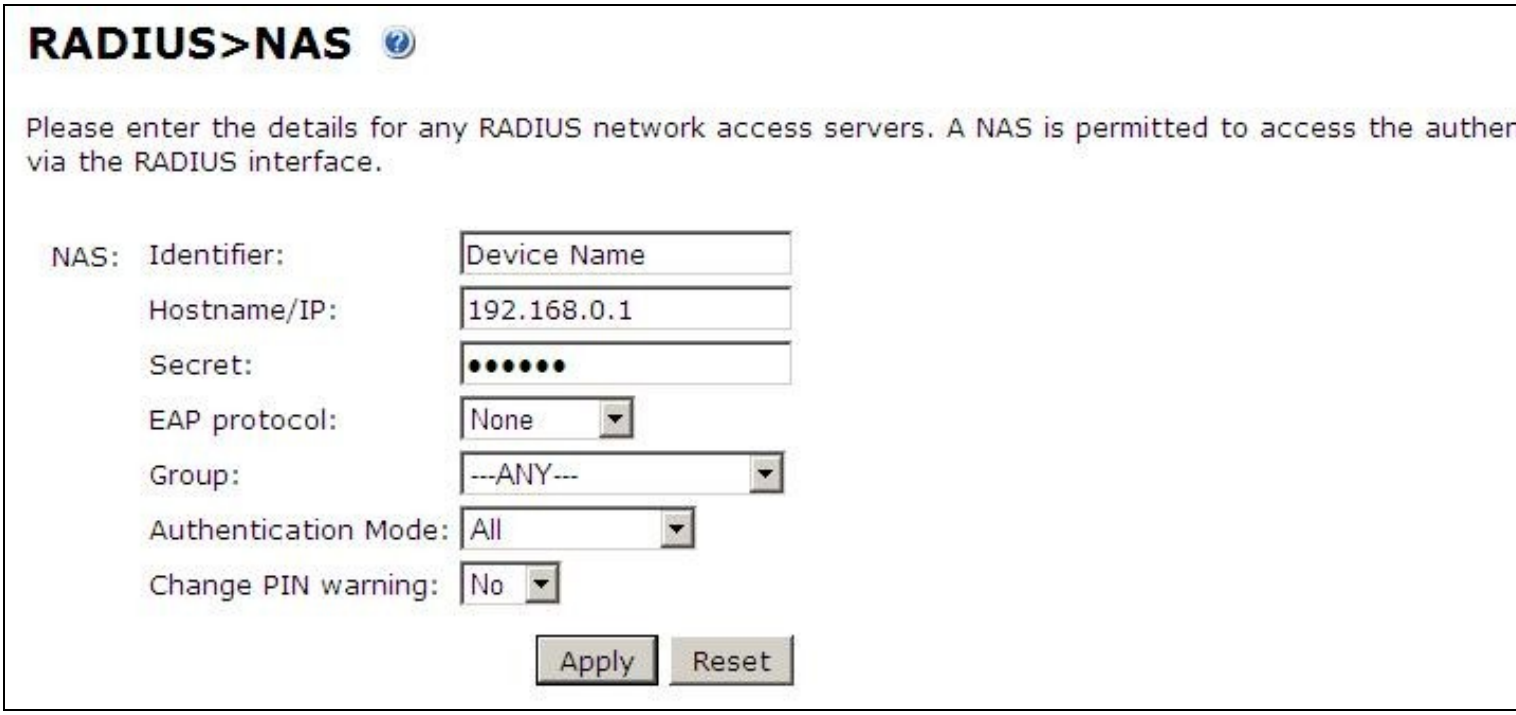
Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

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



470.1.1 Setting up the RADIUS NAS

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



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

470.1.2 Enabling Session creation with username

The PINsafe server can be configured to return an image stream 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 PINsafe username:

Virtual or hardware appliance

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

For a software only install see Software Only Installation

For further information see Single Channel How To Guide

470.1.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

471 Netgear Configuration

471.1 Configuring the Domain

To create a portal whereby users have to use PINsafe in order to authenticate, you need to configure a domain on the Netgear SSL VPN.

To do this go to the Users -> Domain page and create a new Domain.

For this Domain, set it to use RADIUS PAP and enter the IP address of the PINsafe server and set the shared secret. Then set the domain to use the Portal pages created previously.

On the PINsafe server ensure that the RADIUS server is enabled and create a NAS entry for the Netgear SSL VPN.

Now when a user goes to the login page they can select the PINsafe domain created.

The credentials they submit will be submitted to PINsafe via RADIUS and if correct access will be granted.

471.2 Single Channel TURing Integration

This is not required where dual channel authentication through SMS, Mobile Client is used.

471.2.1 Create a Firewall Access Rule

Create a rule to allow traffic from the WAN to the Swivel virtual or hardware appliance. The Netgear device will proxy the request. Since this will open up a port to PINsafe from the WAN, it is recommended to use a Swivel virtual or hardware appliance with its proxy port protection on port 8443, and/or configure an IP filter to prevent access to the administration console. See Filter IP How to Guide On the Netgear Prosafe Administration Console select Security/Firewall/LAN WAN Rules then below Inbound Services click on the *add* button and create a rule to allow traffic with the following settings:

Service Name: HTTP (You may need to create a port for 8080 or 8443)

Action/Filter: Allow Always

LAN Server IP Address: PINsafe server IP address

LAN Users:

WAN Users: ANY

Destination WAN1

Bandwidth Profile: None

An entry should appear in the Inbound Services

471.2.2 Modify the Login Page

This section explains how to modify the SSL Login page to include a TURing image. **Note that the banner text is limited to 256 Characters, the example shown is approx 250 characters, so no additions should be made and using a long pinsafe host name may cause issues**

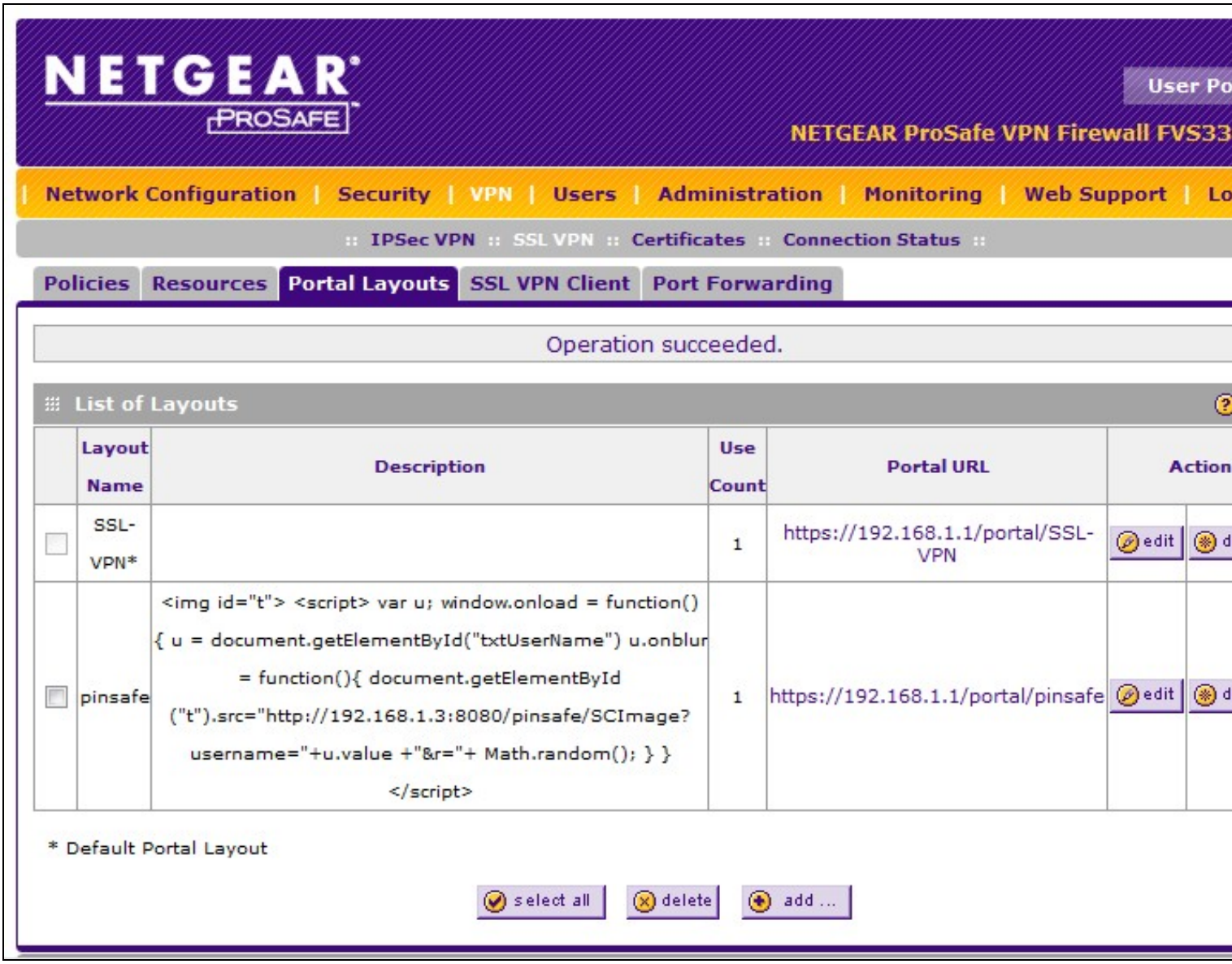
To create the PINsafe login page go to the VPN -> SSL VPN -> Portal Layouts and create a new portal layout.

In the Banner Text section of the portal layout page, enter the following text

```
<img id="t">
<script>
var u;
window.onload = function(){
u = document.getElementById("txtUserName");
u.onblur = function(){
document.getElementById("t").src="http://192.168.1.3:8080/pinsafe/SCImage?username="+u.value +"&r="+Math.random();
}
}
</script>
```

Replacing 192.168.1.3 with the IP address of you PINsafe server. Note that there is a maximum of 256 characters allowed for this so if you PINsafe hostname is long, you may need to removed the "&r="+Math.random() text to compensate.

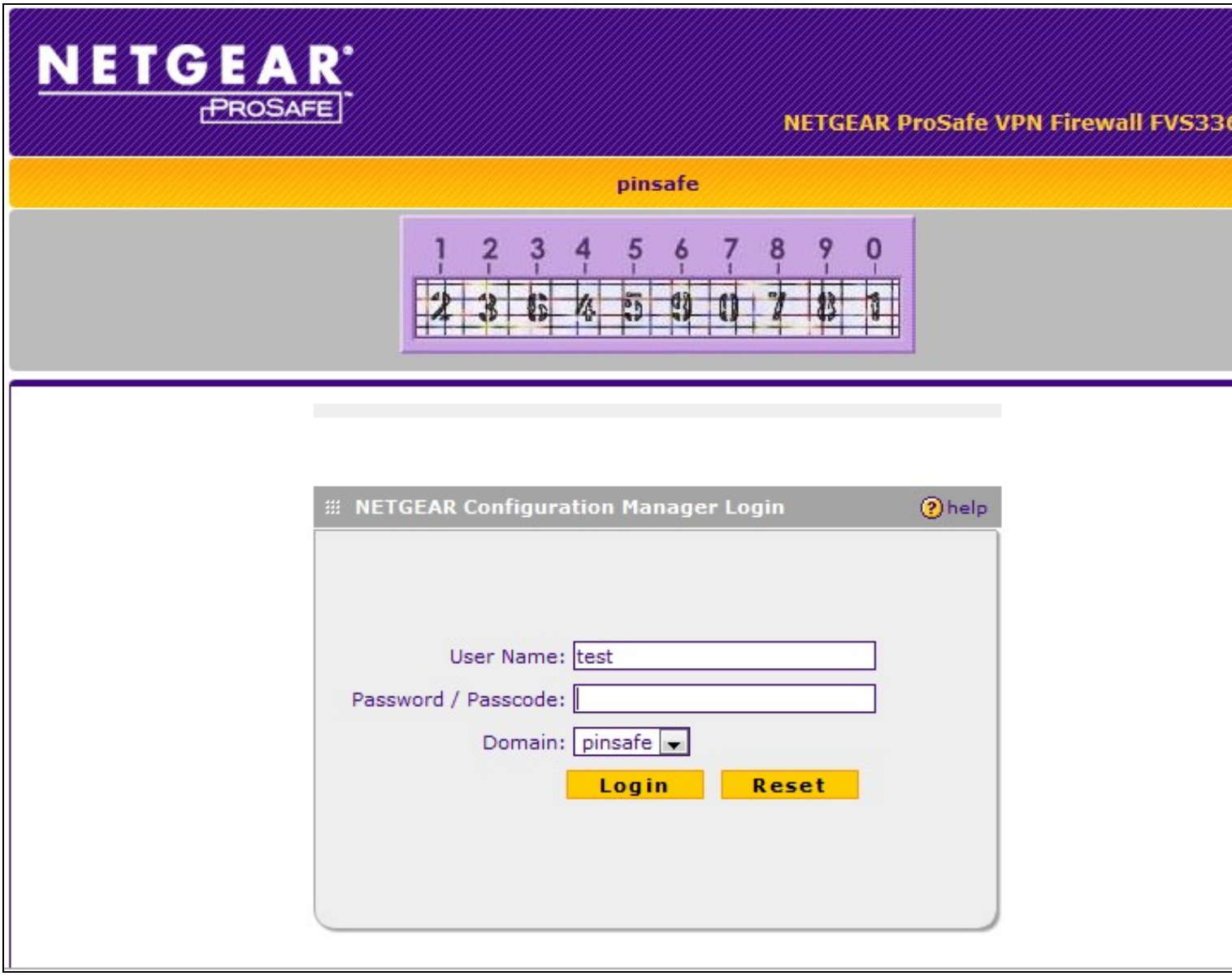
Also note if you are integrating with a virtual or hardware appliance the format will be https on port 8443, and it will be /proxy instead of /pinsafe



Once this portal page is complete you can test that the image is being included correctly by navigating to the login page, in this example https://192.168.1.1/portal/pinsafe.

A similar modification can be completed to request a dual channel image (replace SCImage with DCMessage) or request the index of the security string to be used (replace SCImage with DCIndexImage)

The image should appear when you tab away from the username field.



471.3 Additional Configuration Options

The login can be configured to use AD by using Check Password with Repository on PINsafe. The user would enter the AD password followed by the One time Code, example: ADPasswordOTC password9573. Use of this requires PAP authentication.

See Password_How_to_Guide#Check_password_with_repository

471.4 Known issues

The length of text within the banner may vary between versions, a slightly shorter version of the text without the random number to ensure the image is not cached is given below:

```
<img id="t">
<script>
var u;
window.onload = function(){
u = document.getElementById("txtUserName")
u.onblur = function(){
document.getElementById("t").src="http://192.168.1.3:8080/pinsafe/SCImage?username="+u.value;
}
}
</script>
```

472 Netilla Integration

Netilla Integration Guide

473 Nortel VPN Integration

Nortel VPN Gateway

Integration Guide

Version 1.0 March 2009

474 Introduction

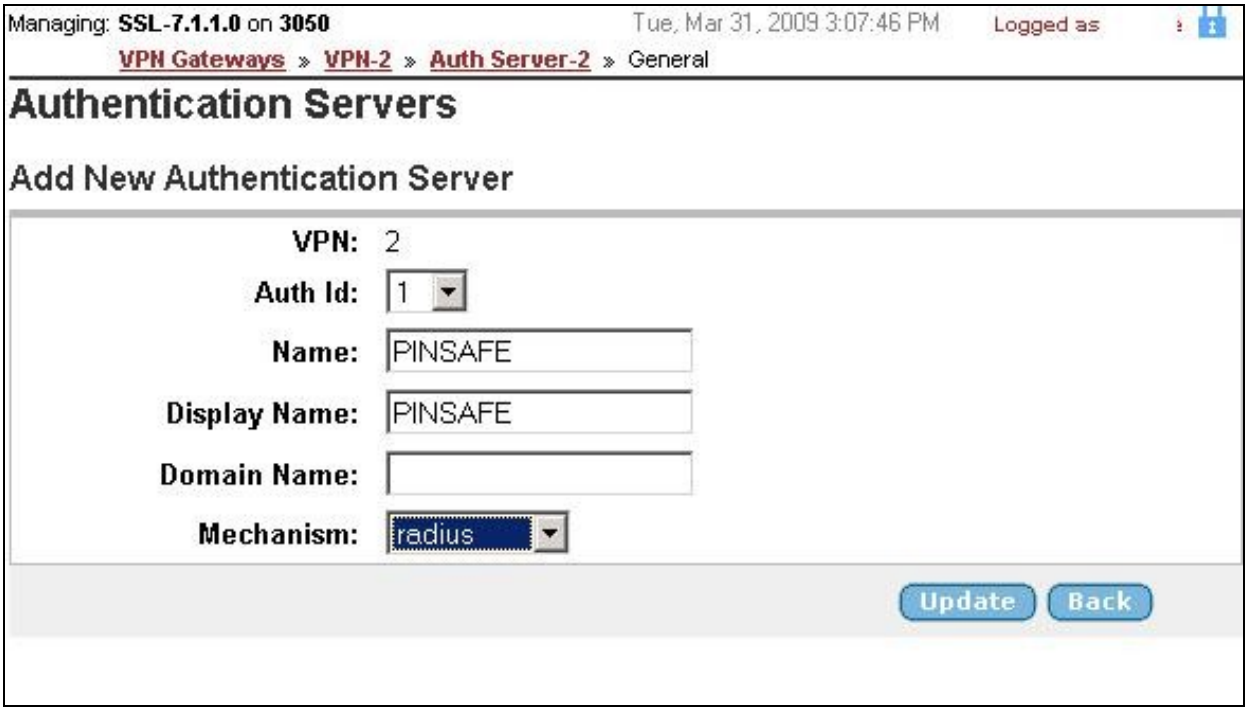
This document describes how to integrate PINsafe with the Nortel VPN Gateway. The integration is based on Nortel 3050 Release 7.1.1.0 This guide covers the Nortel integration only and does not cover the general steps required for configuring the VPN Gateway. This integration requires the PINsafe server to be available from the internet. An appliance install can use the proxy to protect the PINsafe server in this respect.

475 RADIUS Integration

The main integration required is to get the Nortel VPN Gateway to use RADIUS for authentication and to use PINsafe as its RADIUS server.

To do this on the VPN Gateway Config screen select the VPN Gateway you wish to integrate with PINsafe and then select the Authentication option.

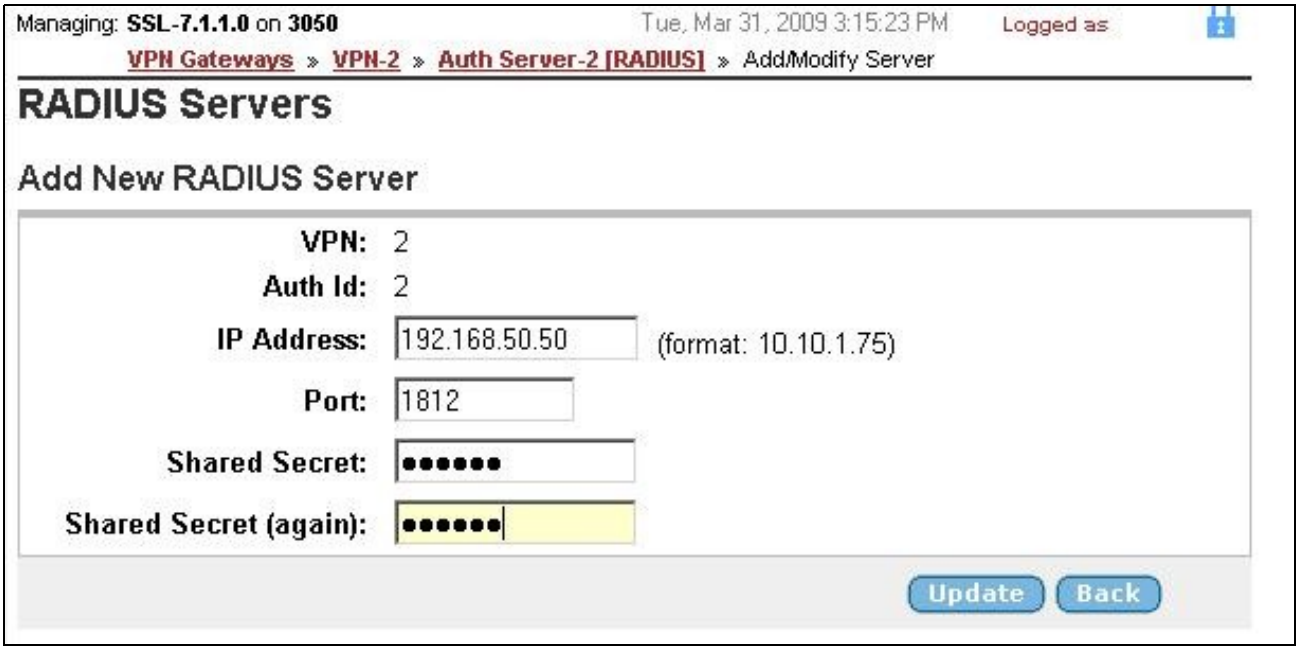
A new authentication server needs to be created. To do this select the Add option and create a new Authentication Server called PINSAFE. The domain name can be left blank.



Then select Update.

Once this stage has been completed the authentication server you have just added will appear on the Authentication Servers screen. Select the server to configure the details. The only essential element is on the Servers tag.

Select this tag and enter the details of the PINsafe server on this screen and click Update.



You must now click Apply on the top right of the screen for these changes to take effect

The VPN is now configured to use PINsafe for authentication. The Nortel allows multiple authentication servers to be defined, if you only wish to use PINsafe then on the Authentication Order tab ensure that it is the only server defined.

You now need to configure PINsafe to accept authentication requests from the Nortel VPN gateway

To do this ensure that the RADIUS server is active and running on the same ports as defined on the Nortel VPN gateway. A NAS then needs to be added that has entries for IP address and shared secret that match those of the Nortel VPN Gateway.

The value for IP address that you need to enter may need to match that of the VPN host defined on the Config ? Hosts screen on the VPN.

476 TURING Integration

The Nortel VPN Gateway supports login page customization and this allows a TURing image to be requested and displayed on the logon page to allow seamless integration between PINsafe and the Nortel VPN Gateway.

This is achieved by going to the VPN Gateway ? Portal page and selecting the Login tab.

The html code required to include the TURing image can then be inserted. A sample is shown below.

```
<script language="JavaScript">
function addButton(e){
var t = document.getElementById('f');
var d = t.getElementsByTagName('td');
d[3].innerHTML = '<input name="user" id="user" size="20" type="text" onblur = "ShowTuring()">';
var i = d.length - 1;
var h = d[i - 1].innerHTML;
d[i-1].innerHTML = h + '  <input type=button name=btnTuring value="Get Another Image" onclick=ShowTuring()>';
var ta = t.getElementsByTagName('table')[0];
r = ta.insertRow(2);
c1 = r.insertCell(0);
c2 = r.insertCell(1);
c1.innerHTML = ' ';
c2.innerHTML = '<img id=turing style="visibility:hidden;">';
r = ta.insertRow(3);
c1 = r.insertCell(0);
c2 = r.insertCell(1);
c1.innerHTML = ' ';
c2.innerHTML = '<font color="red">* Case Sensitive<br></font>';>
}

function ShowTuring() {
ppText = document.getElementById("ptext");
if(ppText != null){
 ppText.innerHTML = "One-Time Code:";
}
var img = document.getElementById("turing");
var usr = document.getElementById("user").value;
var imgUrl = "http://83.111.60.59:81/pinsafe/SCImage?username=";
if (usr=="") {
 alert ("Please enter your username first!");
 document.getElementById("user").focus();
}else{
 //Set the image SRC and make it visible
 var t = document.getElementById('f');
 var d = t.getElementsByTagName('td');
 img.src = imgUrl + usr + "&random=" + Math.ceil(10000*Math.random());
 img.style.visibility = "visible";
 }
}
</script>
```

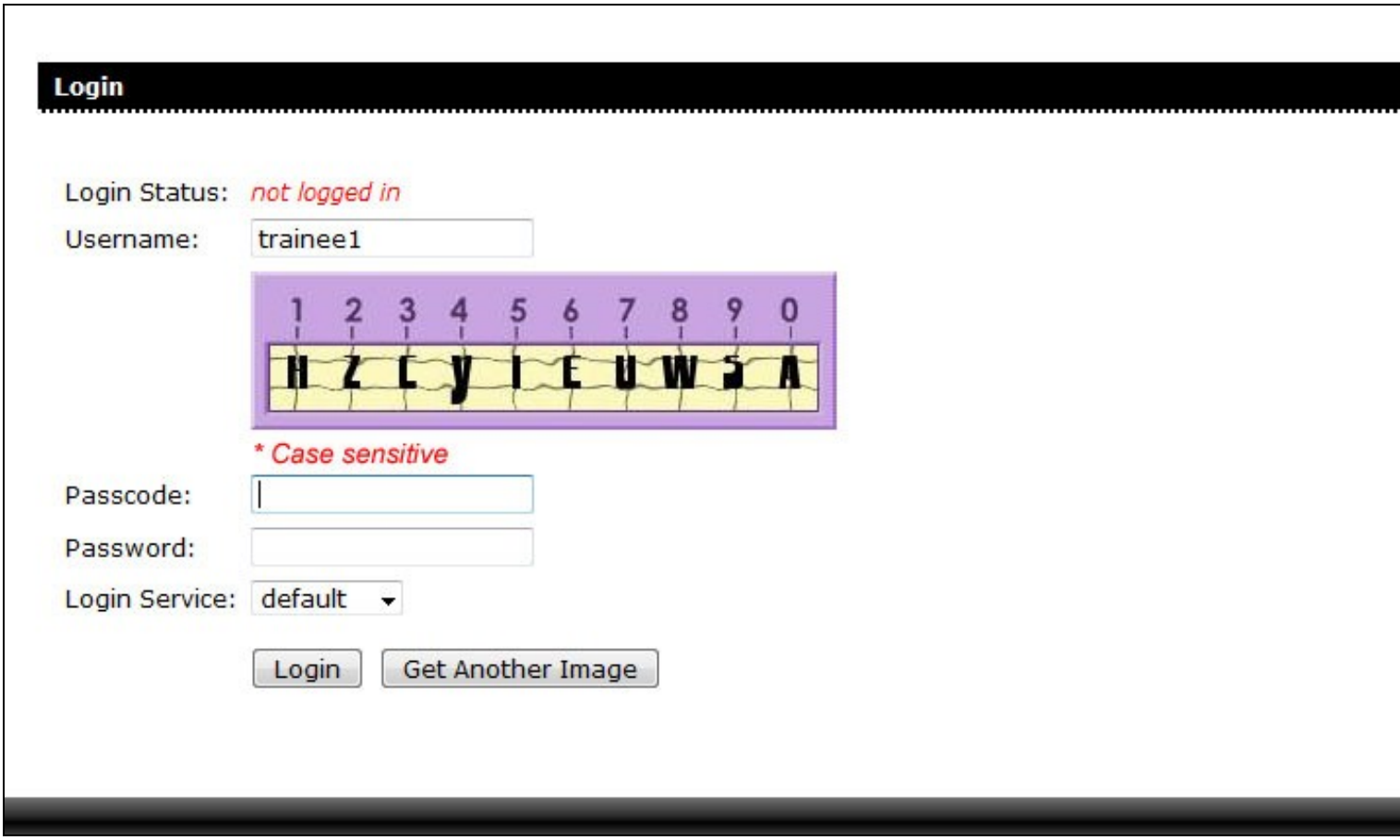
```
<script  language="JavaScript" type="text/javascript">
window.onload = addButton;
</script>
```

The url http://pinsafe:8080/pinsafe/SCImage?username= needs to be changed to match the IP address of the PINsafe server. Note that for an appliance this is likely to be in the format https://pinsafe:8443/proxy/SCImage?username=

Once these changes have been inserted click UPDATE.

You must now click Apply on the top right of the screen for these changes to take effect

You can then view the modified page by going to the ip address associated with the VPN on the Config ? VPN Screen.



477 Notes

This integration requires the PINsafe server to be available from the internet. An appliance install can use the proxy to protect the PINsafe server in this respect.

To test the integration ensure that there is a user that exists on both PINsafe and the VPN Gateway and check the PINsafe logs to see that it is receiving the authentication requests.

478 OpenVPN integration

478.1 Introduction

This article describes how to integrate an existing OpenVPN server with PINsafe, to allow VPN authentication with a Username and One Time Code (OTC) using SMS, mobile phone clients, and the Taskbar. The Single Channel TURing image is not directly displayed within the login.

478.2 Prerequisites

- Linux OpenVPN server installation.
- PINsafe installation with network port UDP 1812, accessible from OpenVPN server device.
- OpenVPN Client

478.3 Baseline

The Swivel integration was tested with the following versions

Linux OpenVPN server CentOS/RHEL openvpn-2.2.0-3.el6.rf.x86_64

OpenVPN Client 2.1 rc19

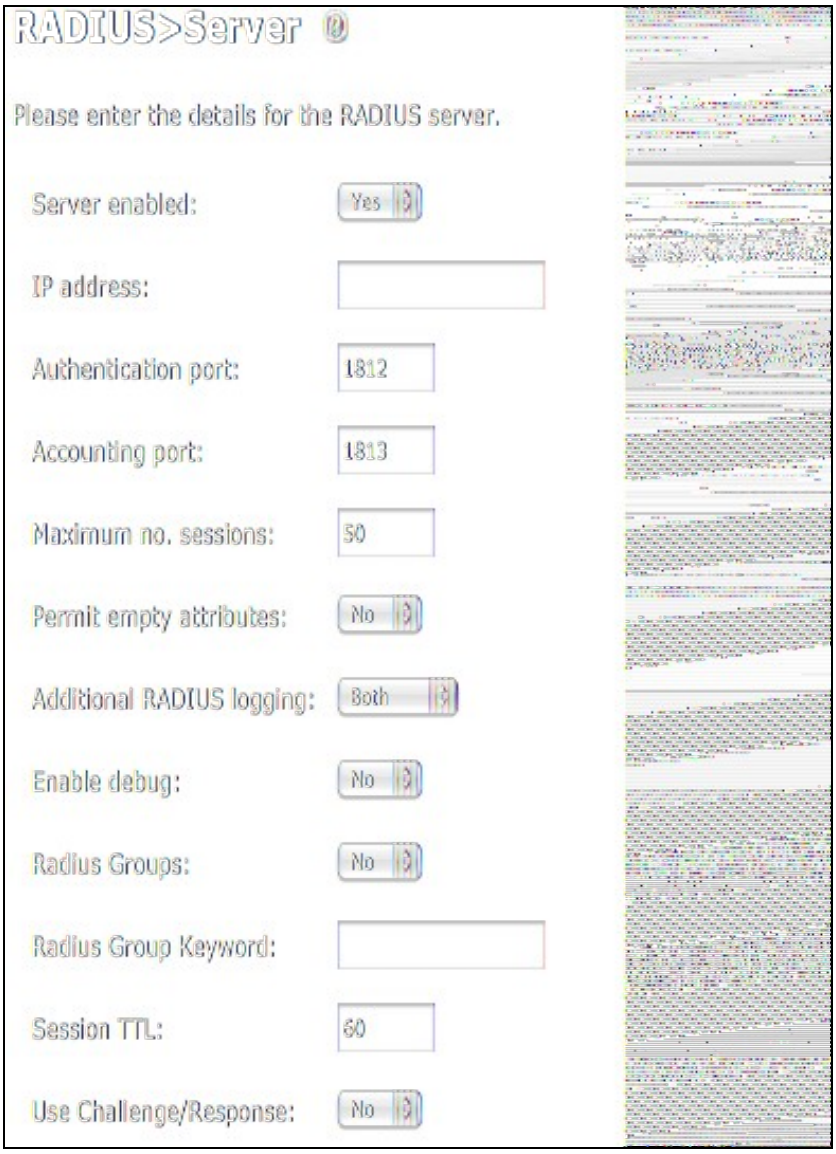
Swivel 3.8

478.4 Integration

478.4.1 PINsafe Integration

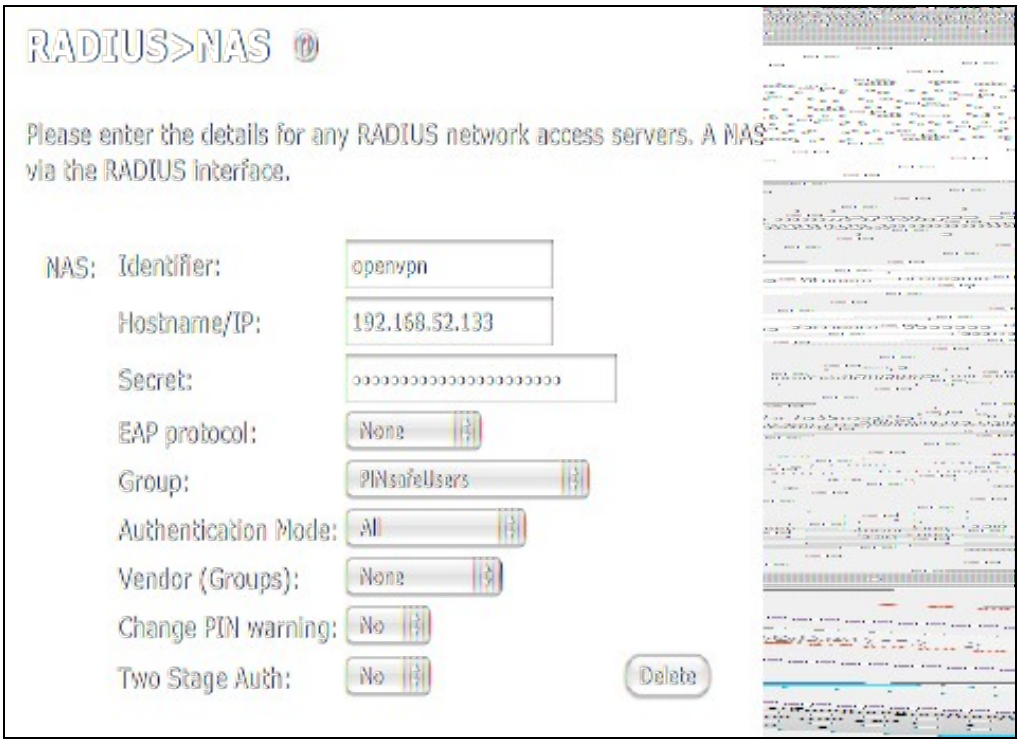
On the Swivel appliance

1.-) Configure and enable RADIUS Server:



Set the option *Server Enabled* to Yes

2.-) Create a new NAS (Network Access Server)



- **Identifier:** Descriptive name of the openvpn server (hostname)
- **Hostname/IP:** OpenVPN Server IP address (as seen by PINsafe. Note if any NAT is required)
- **Secret:** Same secret password set in openVPN file /etc/pam_radius.conf
- **Group:** The PINsafe group permitted to authenticate

478.4.2 OpenVPN Server Integration

In the **OpenVPN Server device** (assumed to be a RHEL/CENTOS), the package **pam_radius** RPM should be installed.

To achieve that run the command *"yum install pam_radius"*.

Edit the openvpn configuration file. By default this file should be **/etc/openvpn/openvpn.conf**.

Add the line:

```
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so openvpn
```

IMPORTANT UPDATE In OpenVPN Server openvpn-2.2.1-1.el6.x86_64 the plugin location changes to **/usr/lib64/openvpn/plugin/lib/openvpn-auth-pam.so**. It is hihgly recommended to perform a search for file **openvpn-auth_pam** to ensure everything will work smooth.

Edit the file **/etc/pam_radius.conf** and add a line with next format:

```
IP_Pinsafesecret   timeout
```

where:

IP_Pinsafe is the IP address where PINsafe installation is.

secret is the password that will be used for the RADIUS communication with PINsafe RADIUS Server.

timeout is the time in seconds that will be defined to wait until a connection attempt with pinsafe server is terminated.

```
Example: "192.168.52.25 secret 10"
```

Edit the file **/etc/pam.d/openvpn** and add after lines at the beginning with

```
account required pam_radius_auth.so
auth required pam_radius_auth.so no_warn try_first_pass
```

On the **OpenVPN server** a service restart will be needed:

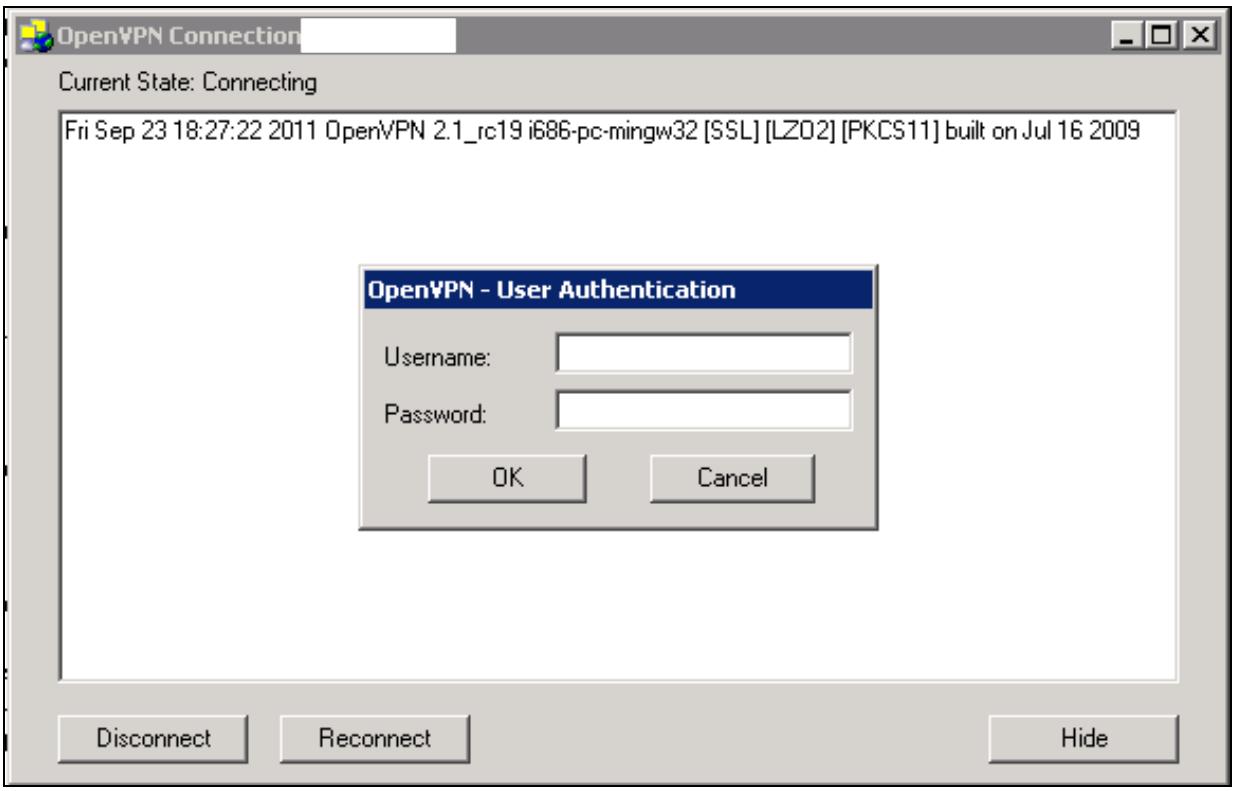
```
"/etc/init.d/openvpn restart" or "service openvpn restart"
```

478.4.3 OpenVPN Client Integration

On the client **OpenVPN configuration file**, add the following line:

```
"auth-user-pass"
```

When the client application starts it will prompt with a window before starting the connection for authentication information:



OpenVPN-GUI for Windows

Tunnelbick for Mac OSX

479 Palo Alto Networks Integration

479.1 Introduction

This document describes steps to configure a Palo Alto Networks Firewall with Swivel as the authentication server using RADIUS with SMS, Mobile Phone Client, and Taskbar Authentication. The solution is tested with a Palo Alto Networks GlobalProtect client.

479.2 Prerequisites

Palo Alto Networks Firewall

Palo Alto Networks documentation

Swivel 3.x, 3.5 or later for RADIUS groups

479.3 Baseline

Palo Alto Networks PA-2050

Palo Alto Networks Software 4.1.6

Palo Alto Networks GlobalProtect Client 1.14 and 1.15

Swivel 3.8

479.4 Architecture

The Palo Alto Networks makes authentication requests against the PINsafe server by RADIUS.

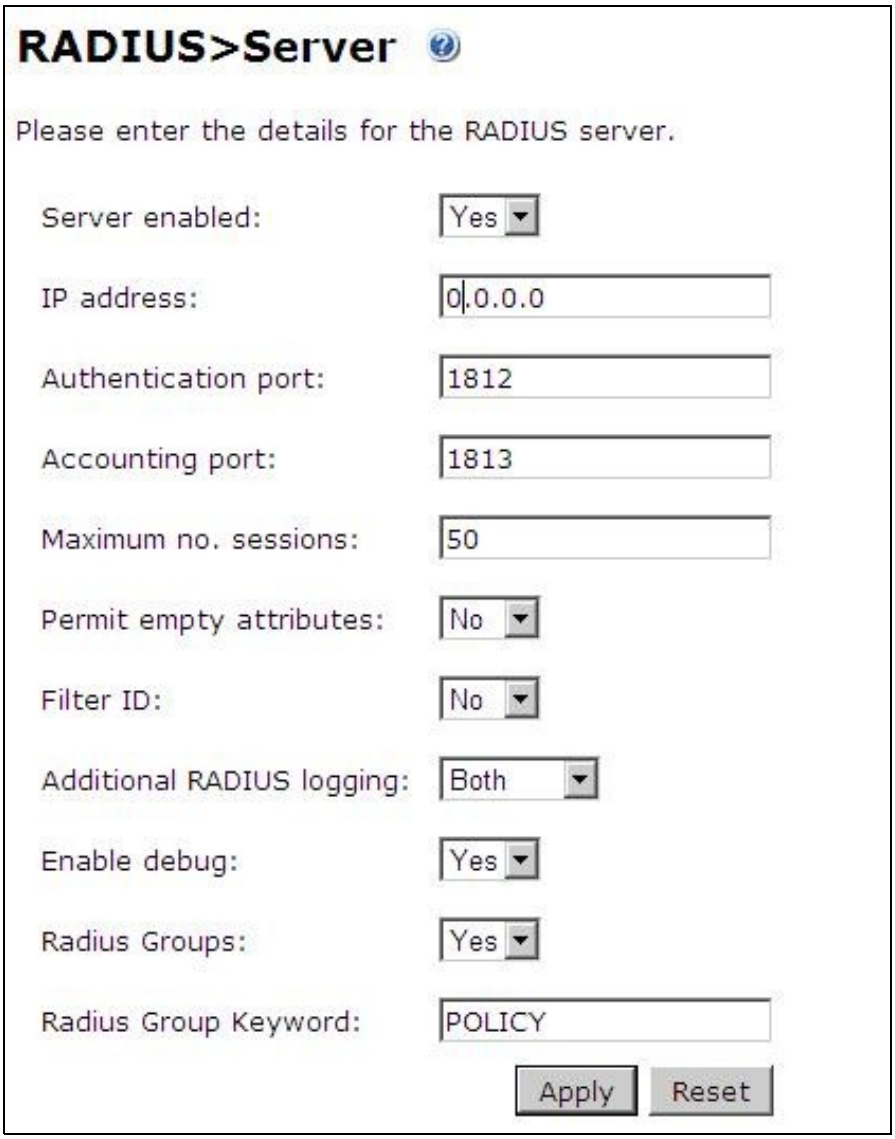
479.5 Swivel Configuration

479.5.1 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 to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

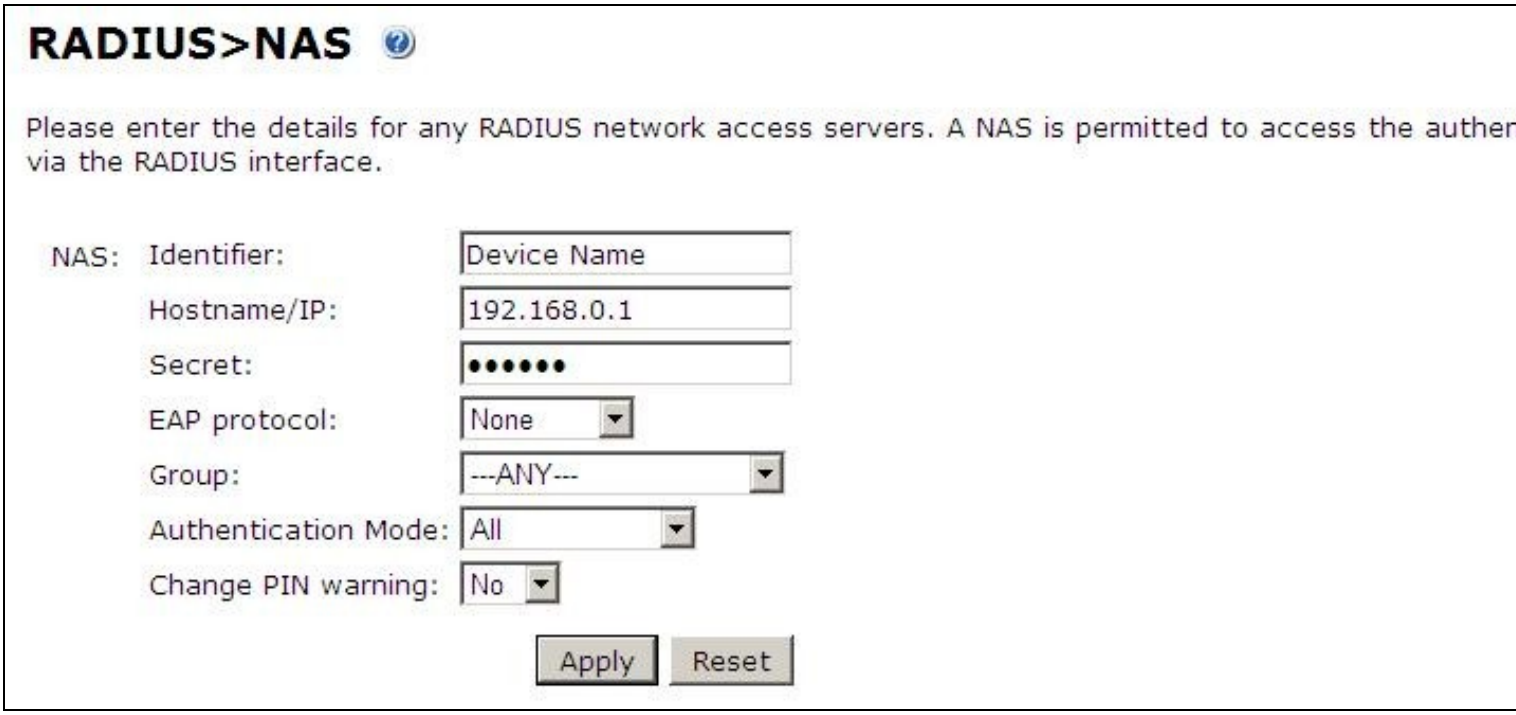
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

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



479.5.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe 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 PINsafe server and VPN RADIUS configuration.



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.

479.5.3 Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

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

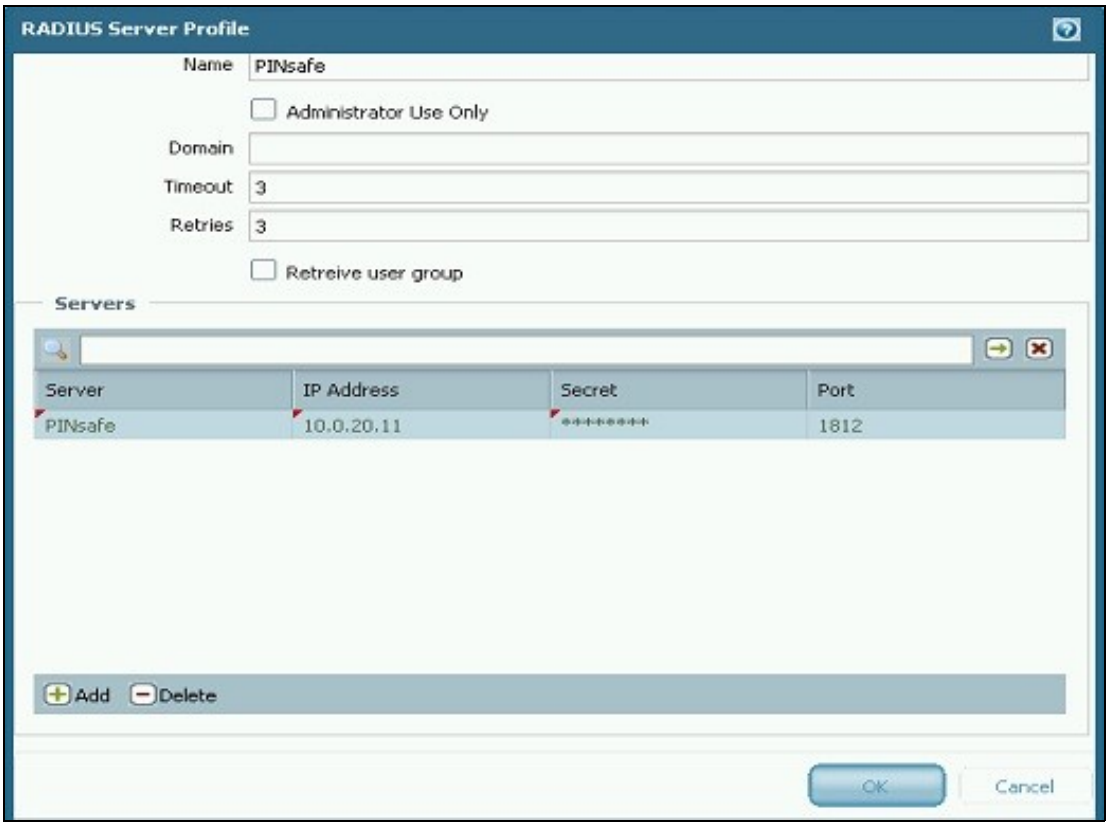
https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installationr

479.6 Palo Alto Networks Configuration

479.6.1 Create a RADIUS Server Profile

On the Palo Alto Networks Administration console select the Device tab then Server Profiles and then RADIUS, and click on Add.



Enter the following information:

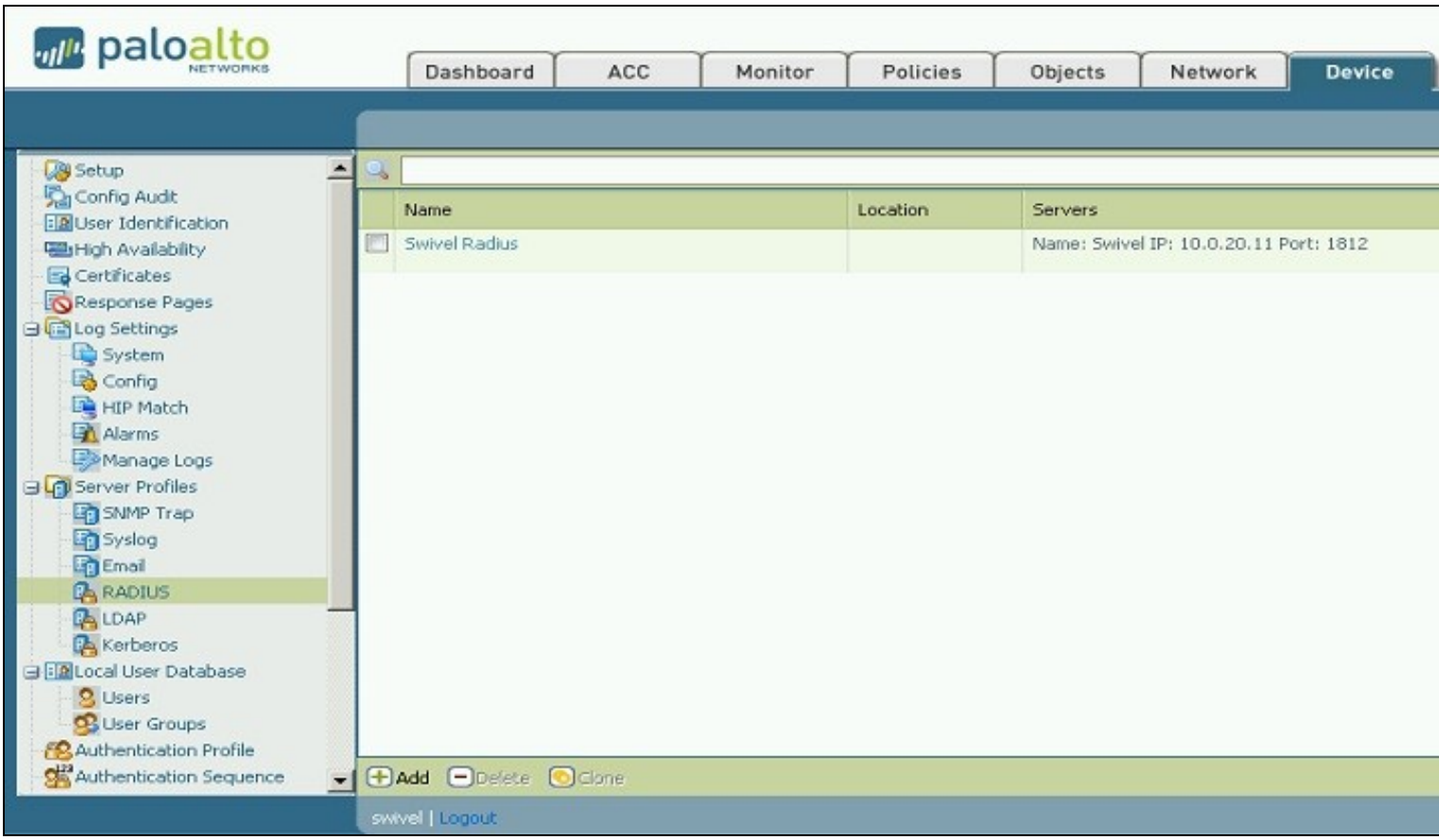
Name Descriptive name for the authentication server

Domain A domain to be appended to the authentication request

IP address or hostname of the Swivel server

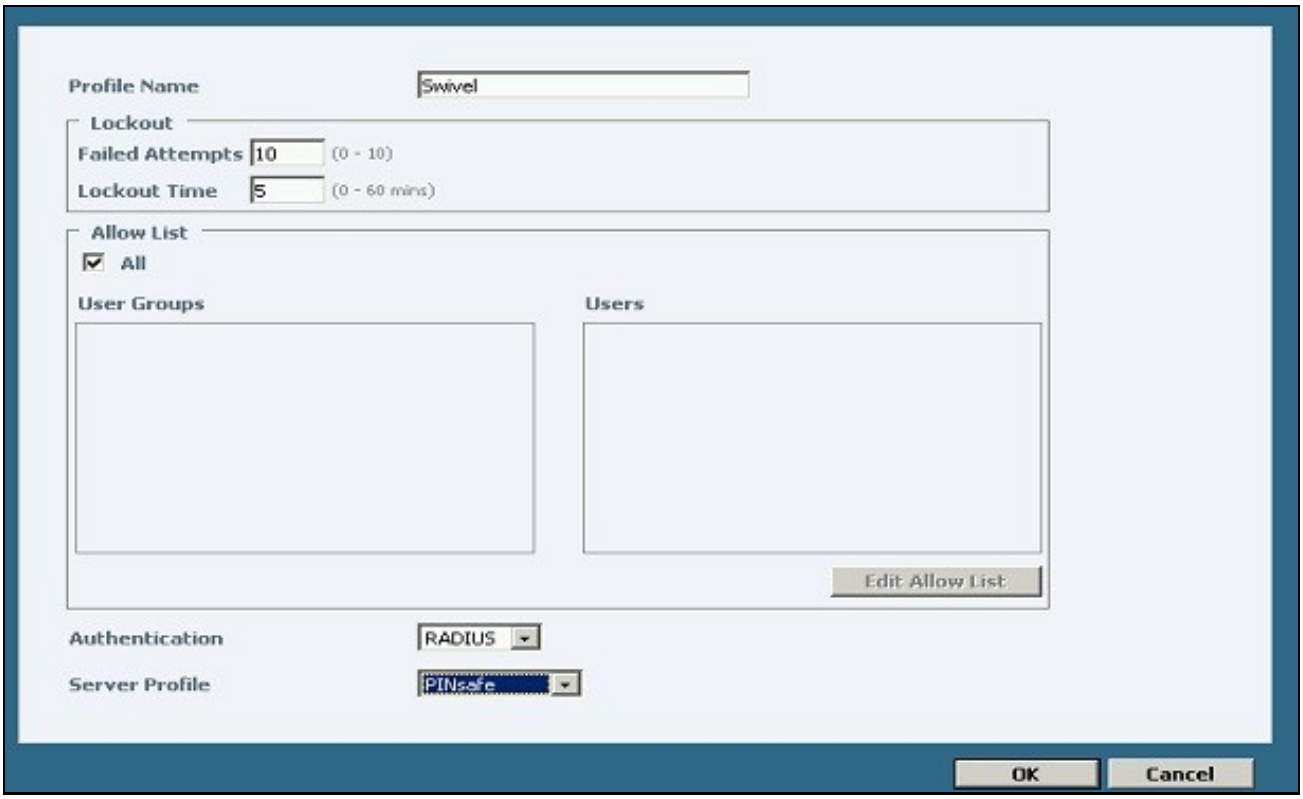
Shared secret as entered on the PINsafe server

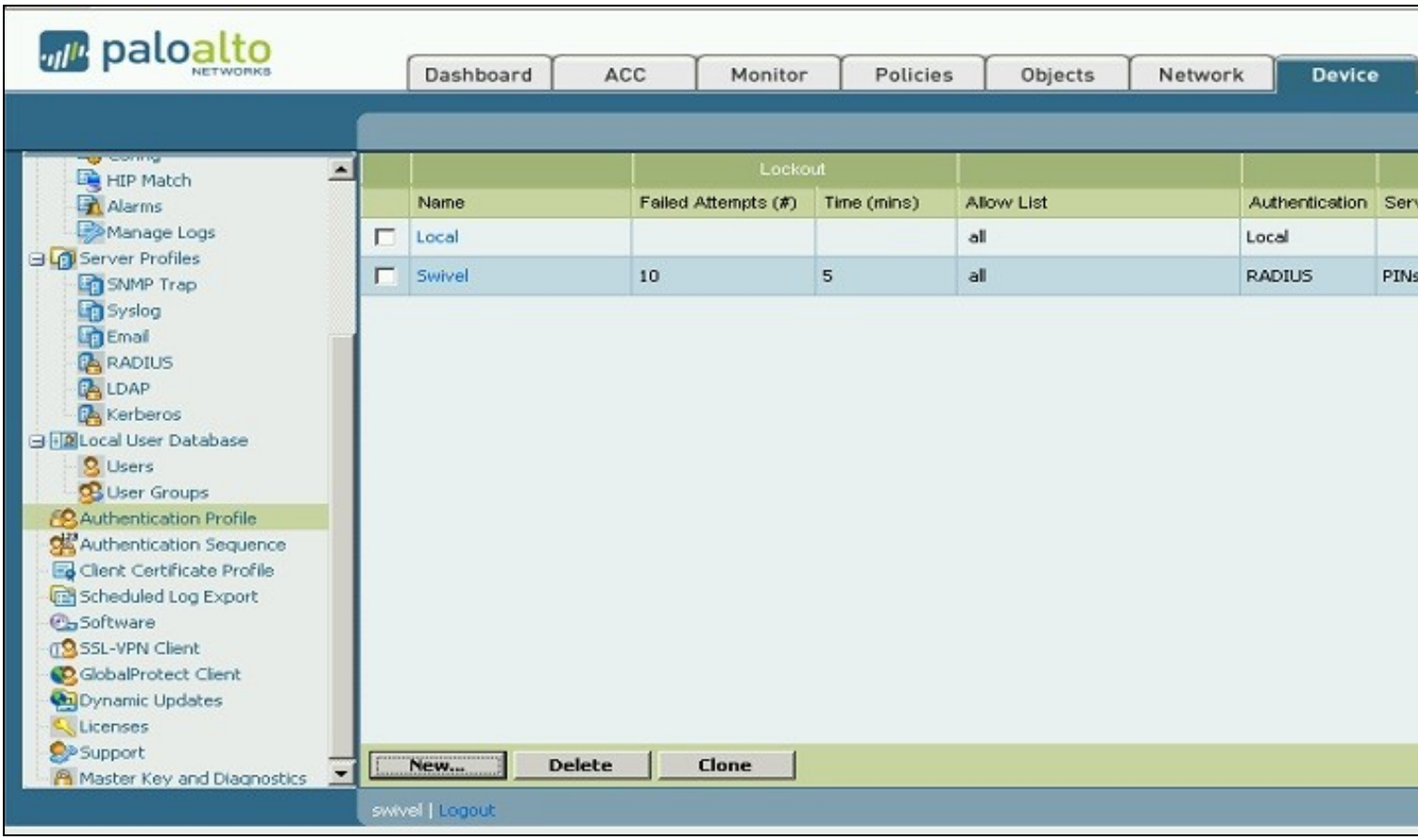
Port usually 1812 by default



479.6.2 Create an Authentication Profile

On the Palo Alto Networks Administration console select the Device tab then Authentication profiles, and click on New. Enter a name and select RADIUS as the authentication type, and the Swivel server for the profile.

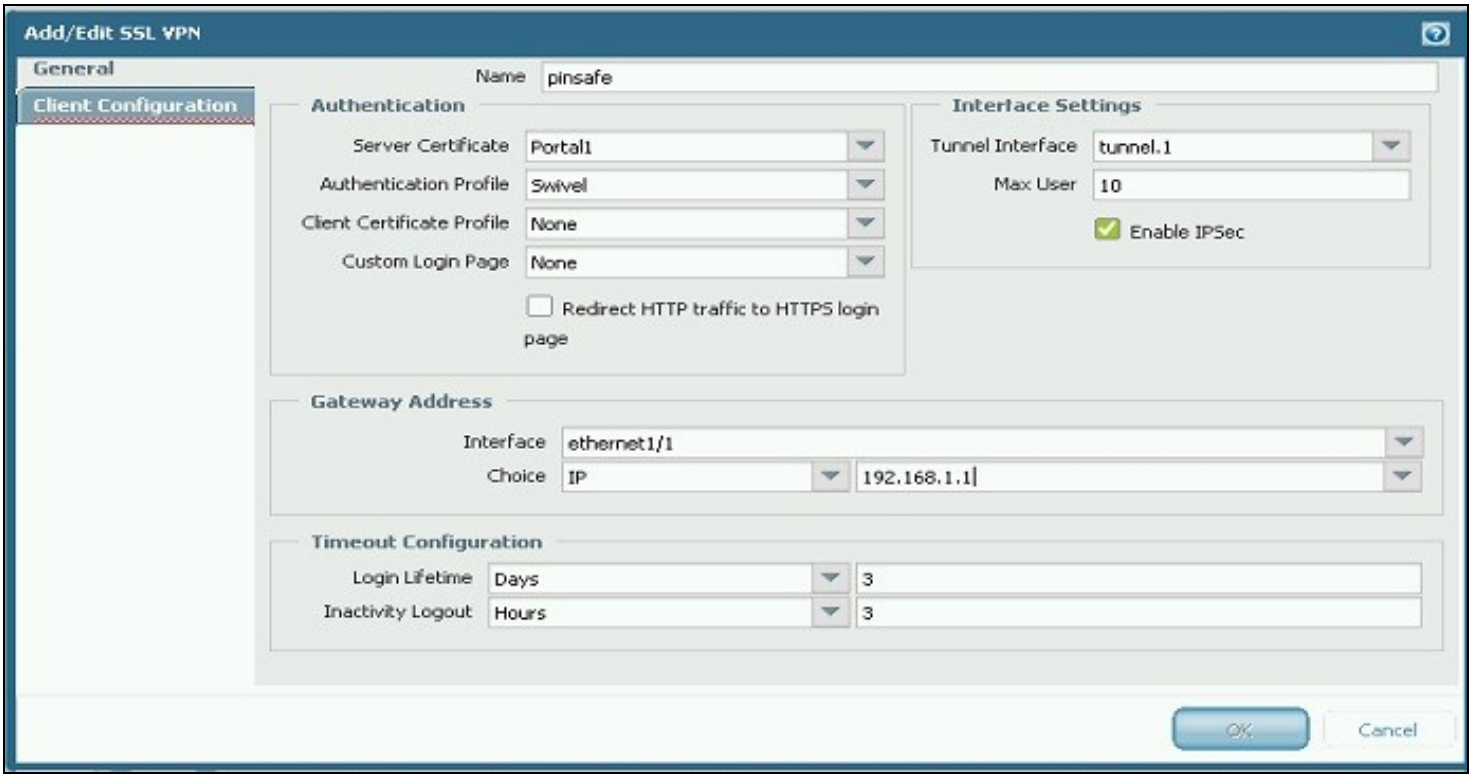




479.6.3 Configure the GlobalProtect Portal to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Portal or configure a new one by clicking on New.

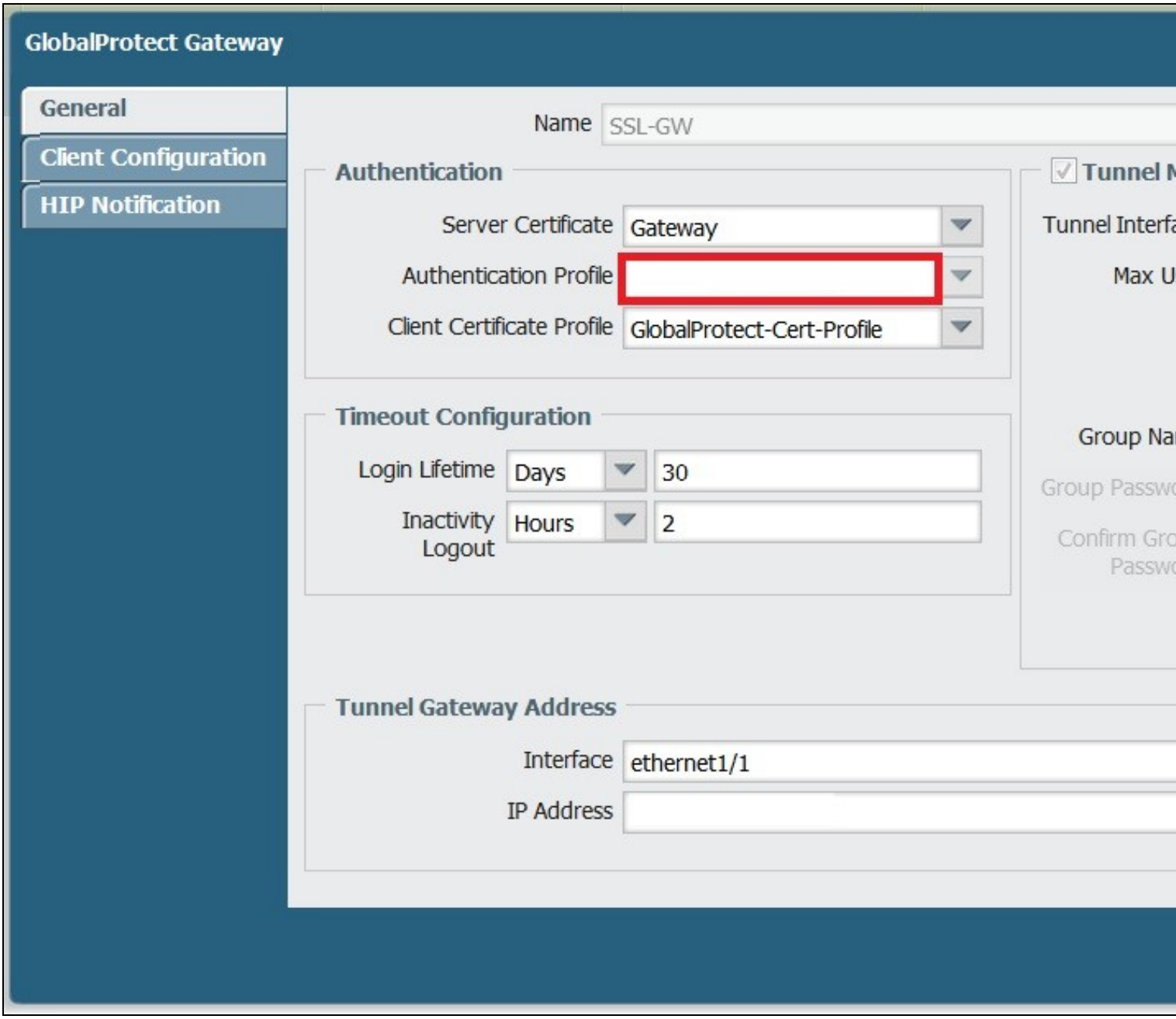
Configure the **Authentication Profile** to use the authentication profile created above.



479.6.4 Configure the GlobalProtect Gateway to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Gateway or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.

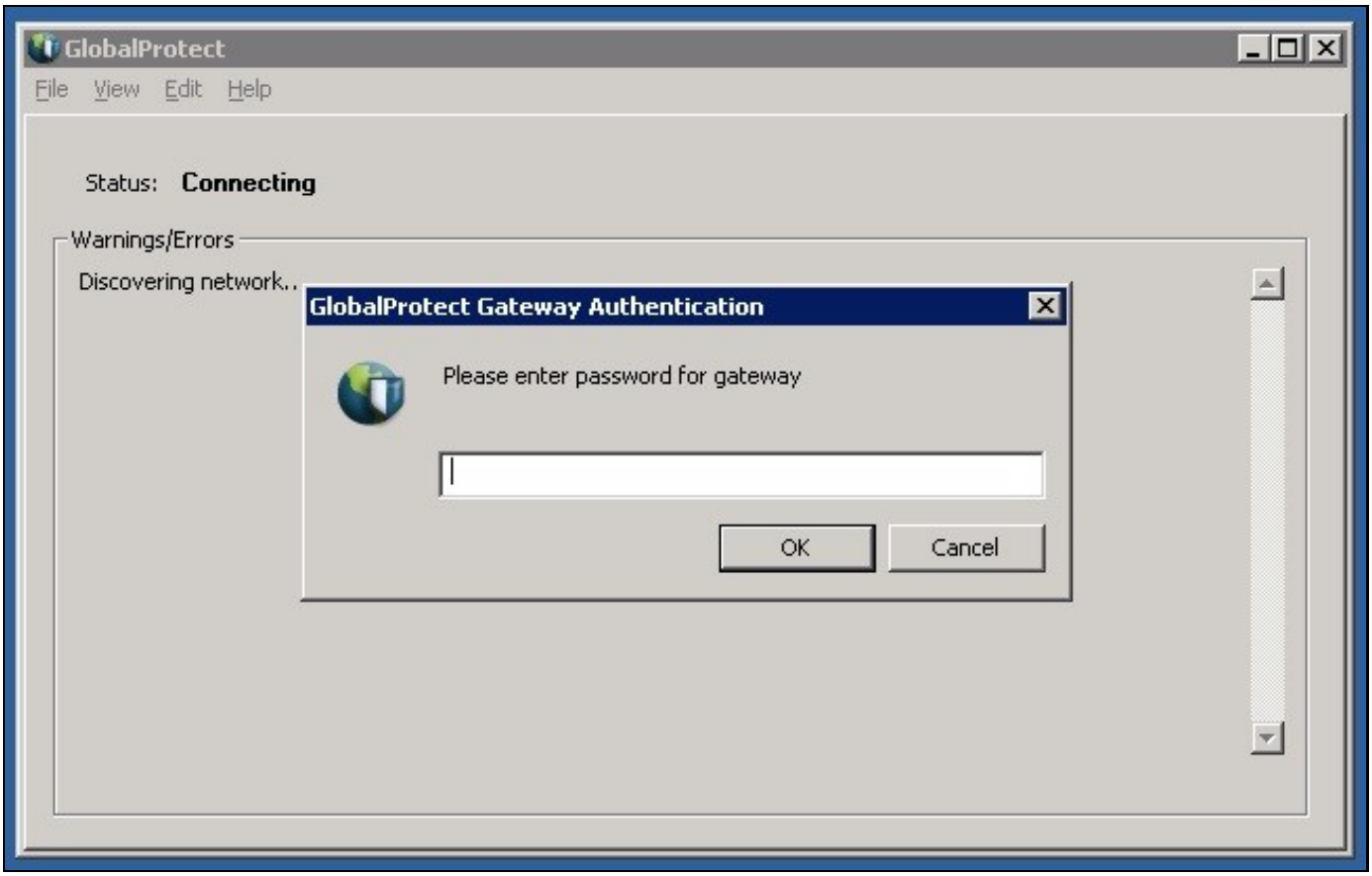


479.7 Additional Configuration Options

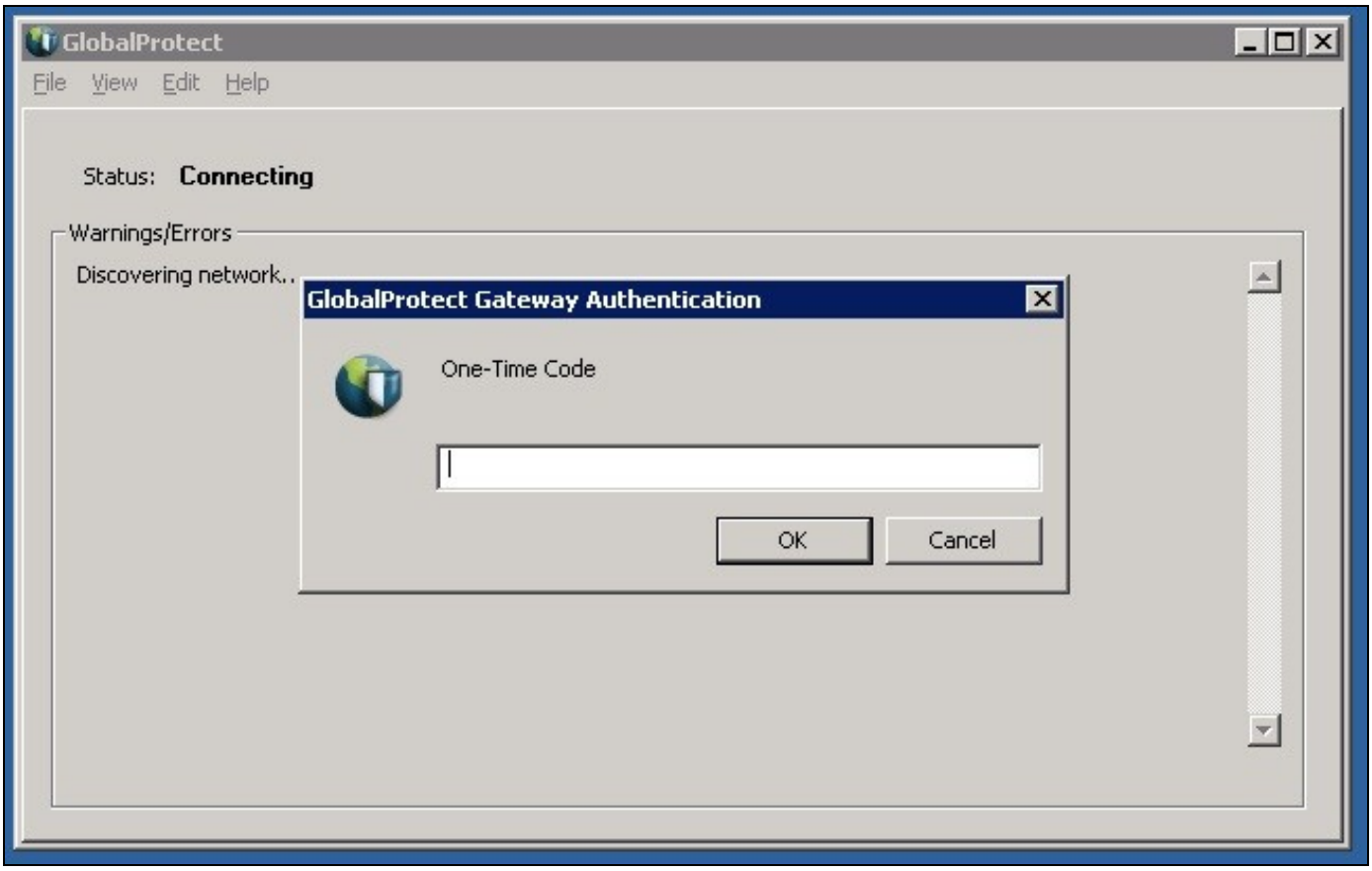
479.7.1 Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide.

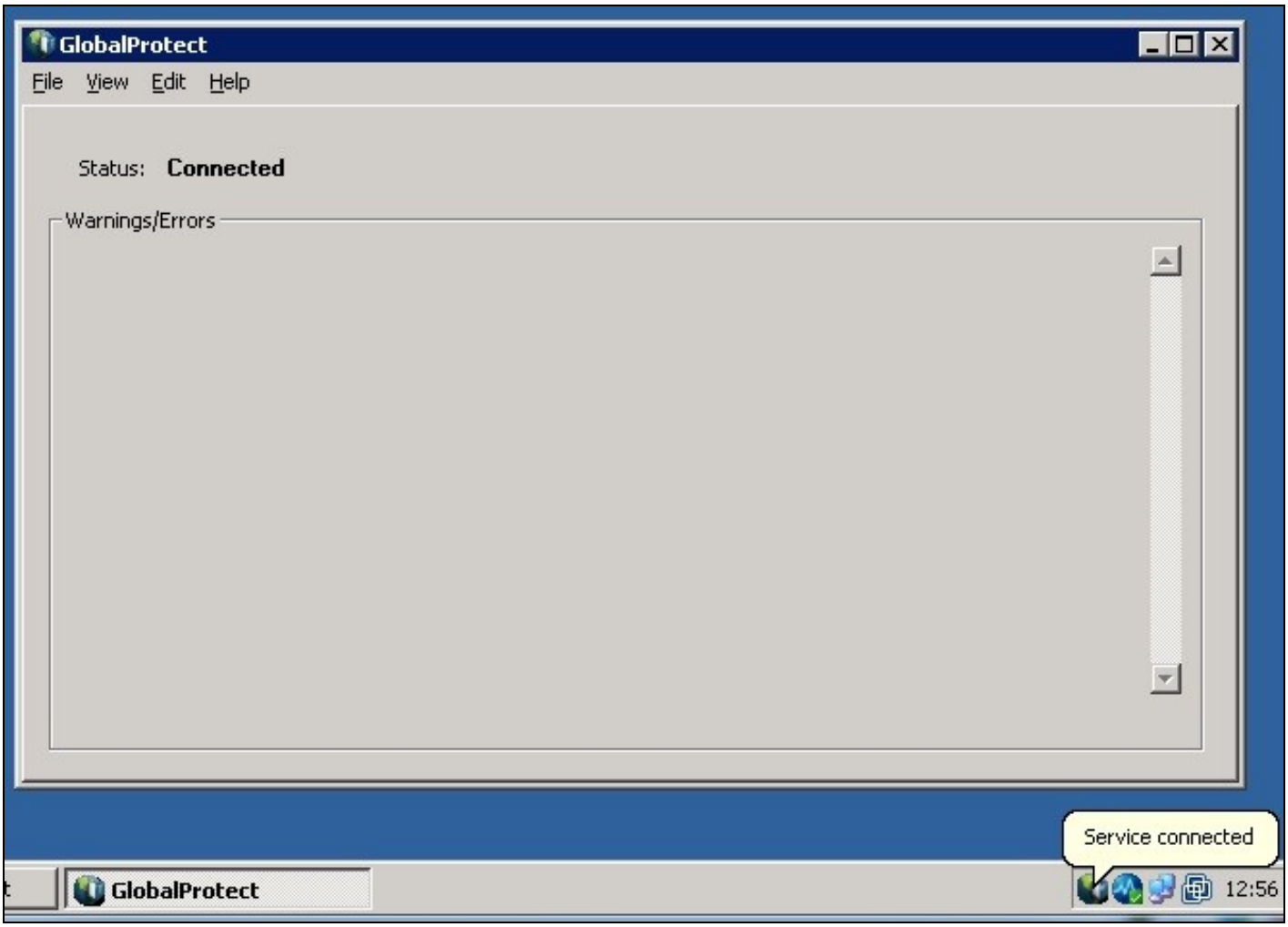
Enter Password



Enter OTC



IF OTC is correct then connection will be established



479.8 Testing

Connect to the GlobalProtect Client and authenticate using RADIUS authentication.

479.9 Troubleshooting

Check the PINsafe logs for RADIUS requests.

479.10 Known Issues and Limitations

None

479.11 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

480 Salesforce.com

481 Introduction

This document covers the integration of Swivel with Salesforce.com.

482 Prerequisites

Salesforce.com Adminisrative Account

Swivel virtual or hardware appliance or server

PINsafe salesforce software Download and unzip the salesforce.war file

The Swivel server needs to be accessible accross the internet for the Salesforce.com server to connect, and the IDP is usually deployed so that it can also be access from the Internet. For security using a Swivel hardware or virtual appliance, the IDP is usually deployed in /webapps2 and accessible on port 8443 (or using a PAT on the appliance using 443)

483 Baseline

Salesforce 11, 12

Swivel 3.8, 3.9

484 Architecture

Salesforce.com users authenticate using SAM-L authentication against Swivel

485 Installation

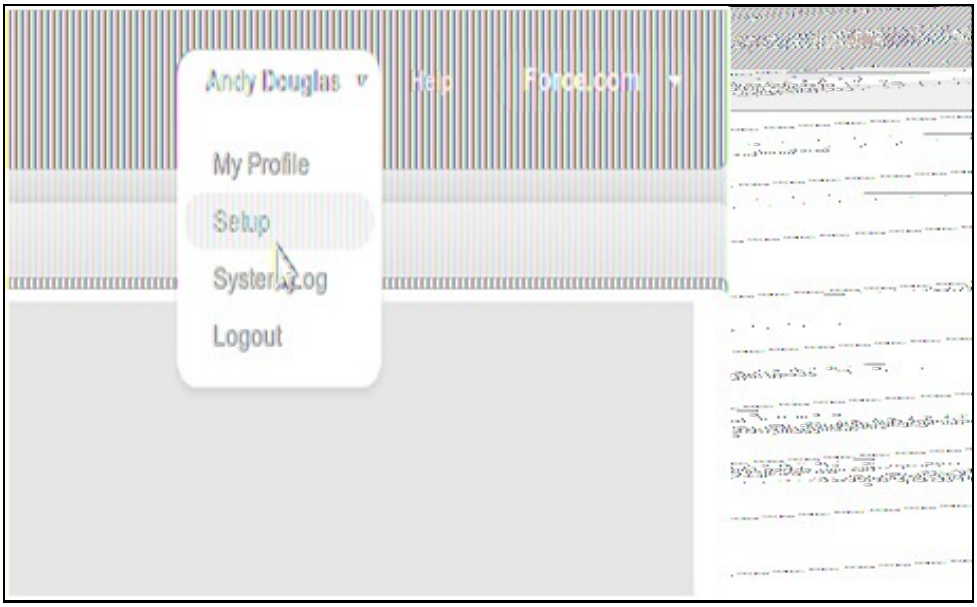
485.1 Salesforce.com Configuration

485.1.1 Allow Authentication

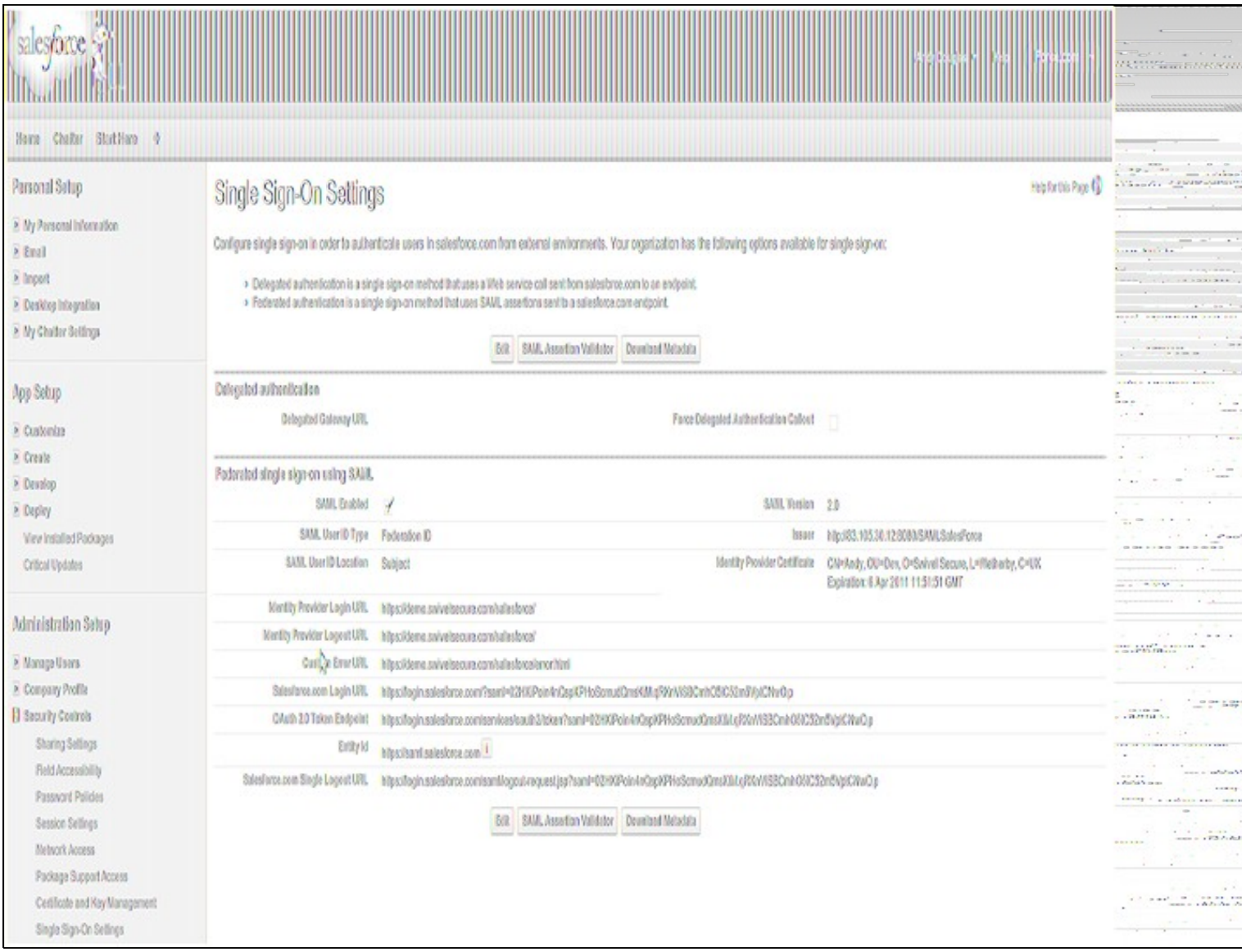
Contact Salesforce.com to enable Federated SSO

485.1.2 Configure Single Sign On

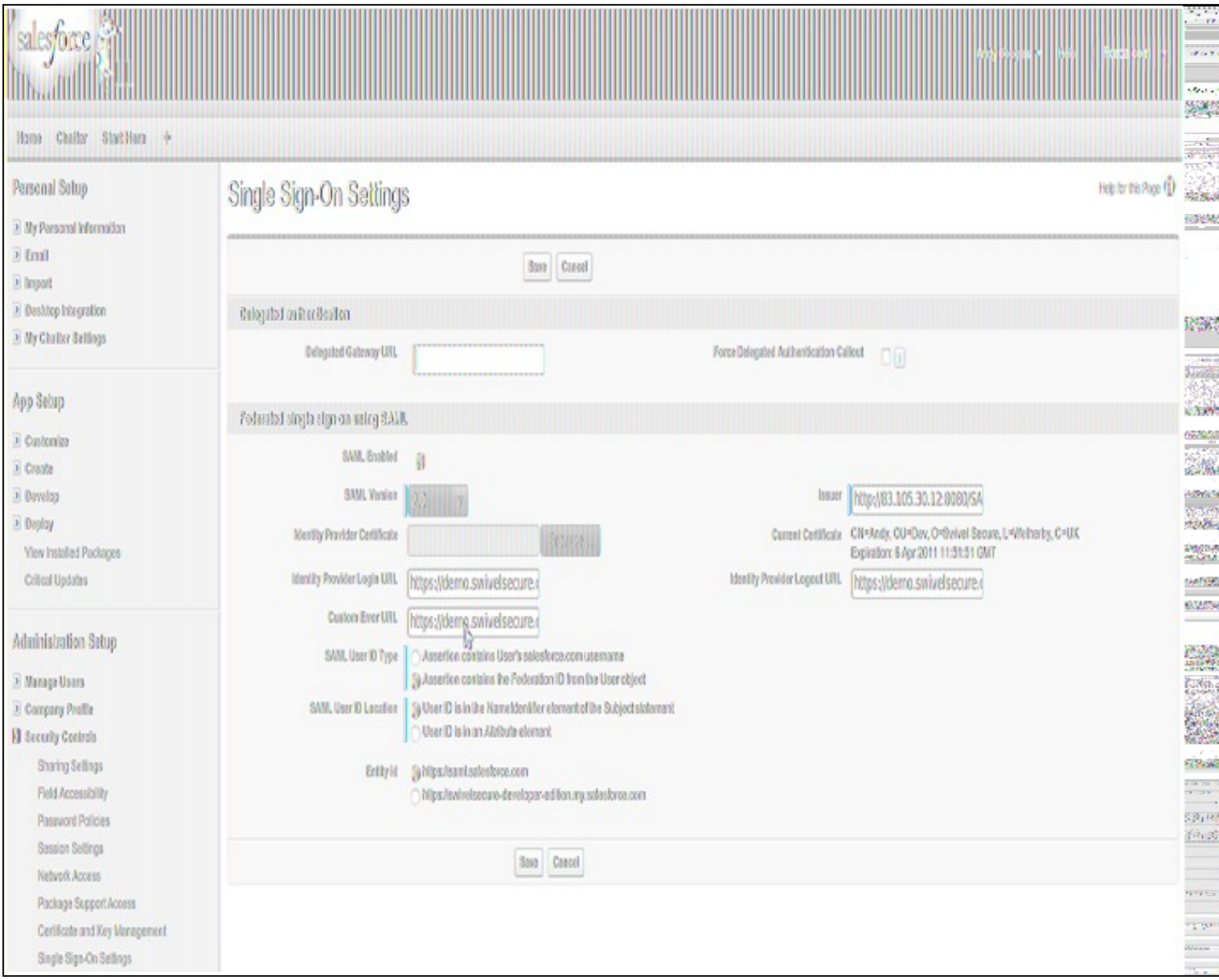
Using an administrative user logon to Salesforce.com and select 'Setup' from the top right button with the the user name on.



Each version of Salesforce is slightly different but each should have a screen similar to the below reached from Setup->Administrative Setup->Security Controls->Single Sign-On Settings



Click on Edit. At this point you should get something similar to the screen below:



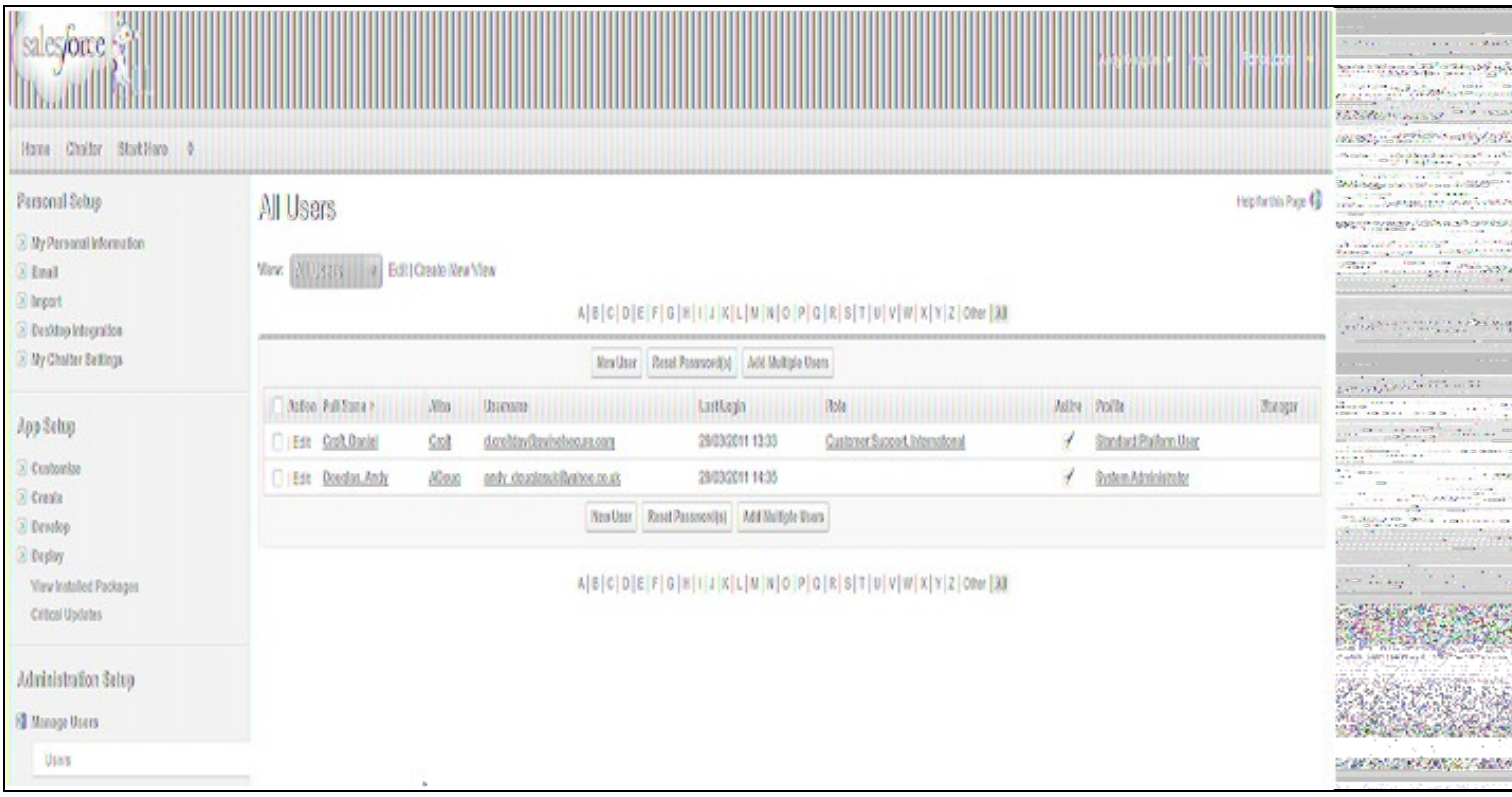
a) upload the certificate and set the issuer

b) set the login URL and logout URL to point to the instance of salesforce-pinsafe you will have running (pointing to the instance is fine as it will re-direct to the logon page automatically)

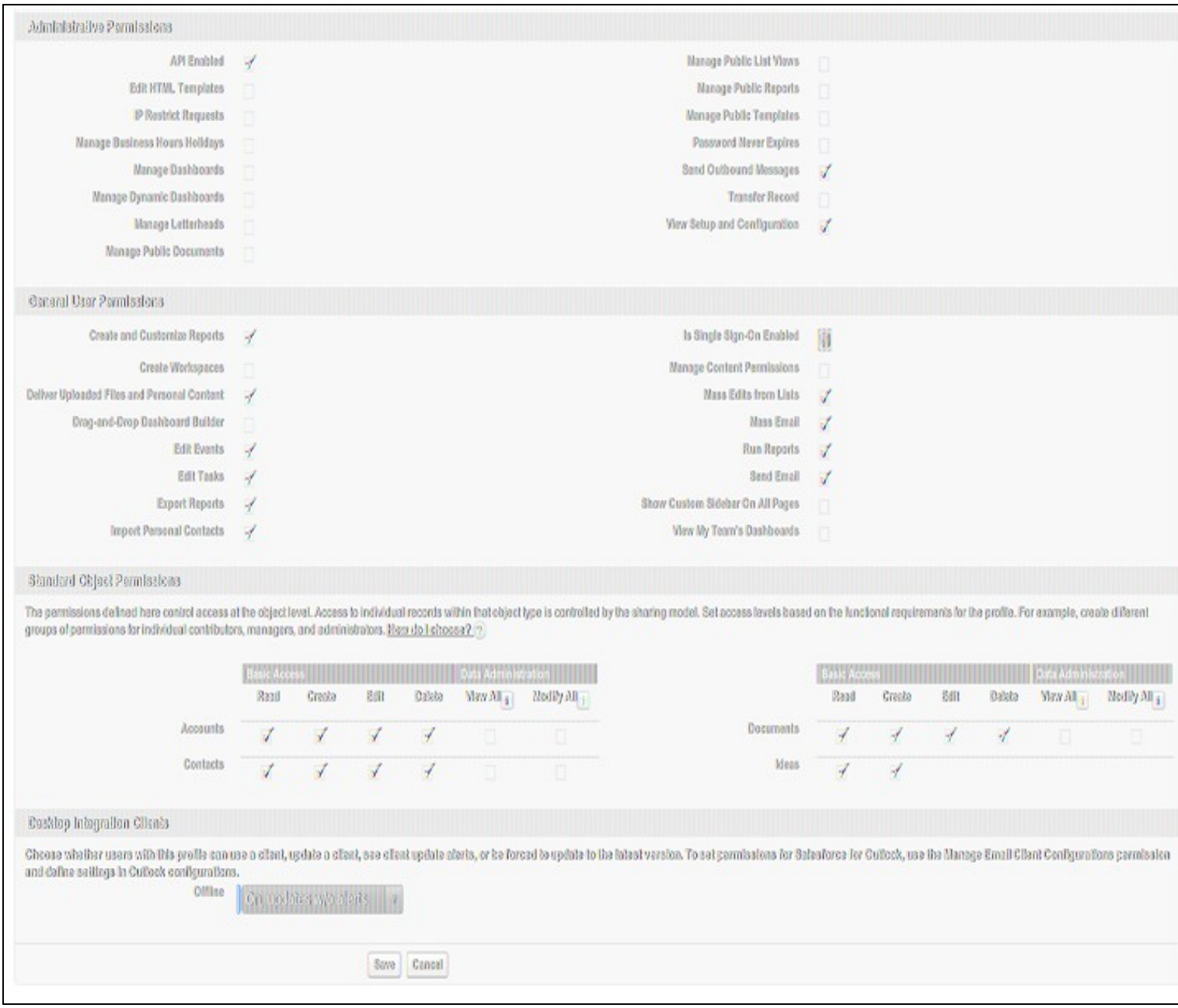
c) set the remaining settings as above

Entity ID The issuer in SAML requests generated by Salesforce, and is also the expected audience of any inbound SAML Responses. If you don?t have domains deployed, this value is always Entity ID https://saml.salesforce.com. If you have domains deployed, Salesforce recommends that you use your custom domain name.

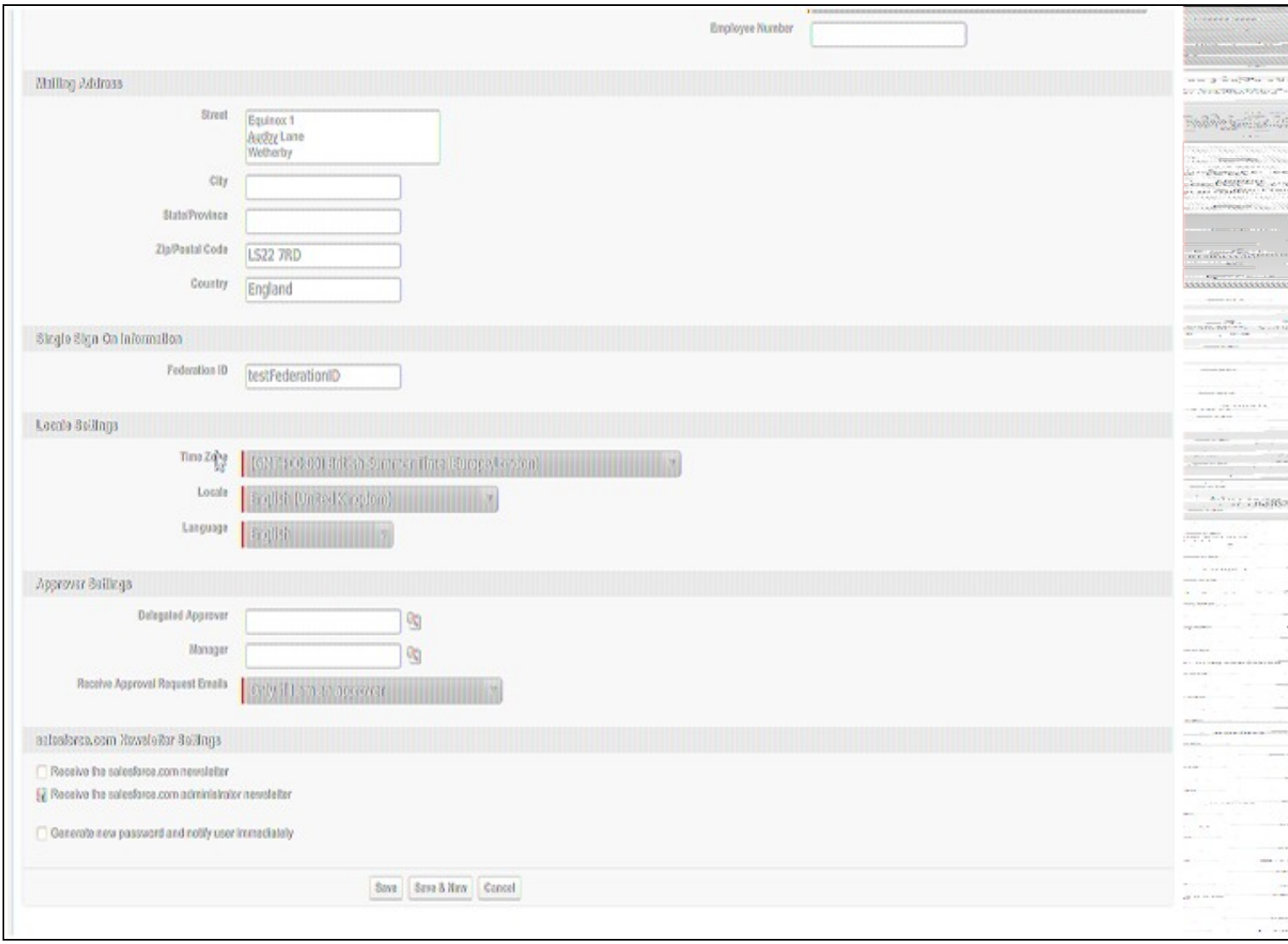
Ensure the users that you wish to use SSO are using a profile that has SSO enabled. Click Manage Users->Users. The profile assigned to each user is on the right hand side.



Click on the profile and find the SSO option as shown below, ensure it is enabled. If it isn't then click edit and enable it.



Ensure the users have a Federation ID which will map to their Swivel username. Click Manage Users->Users, select a user then enter the Federation ID



485.2 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

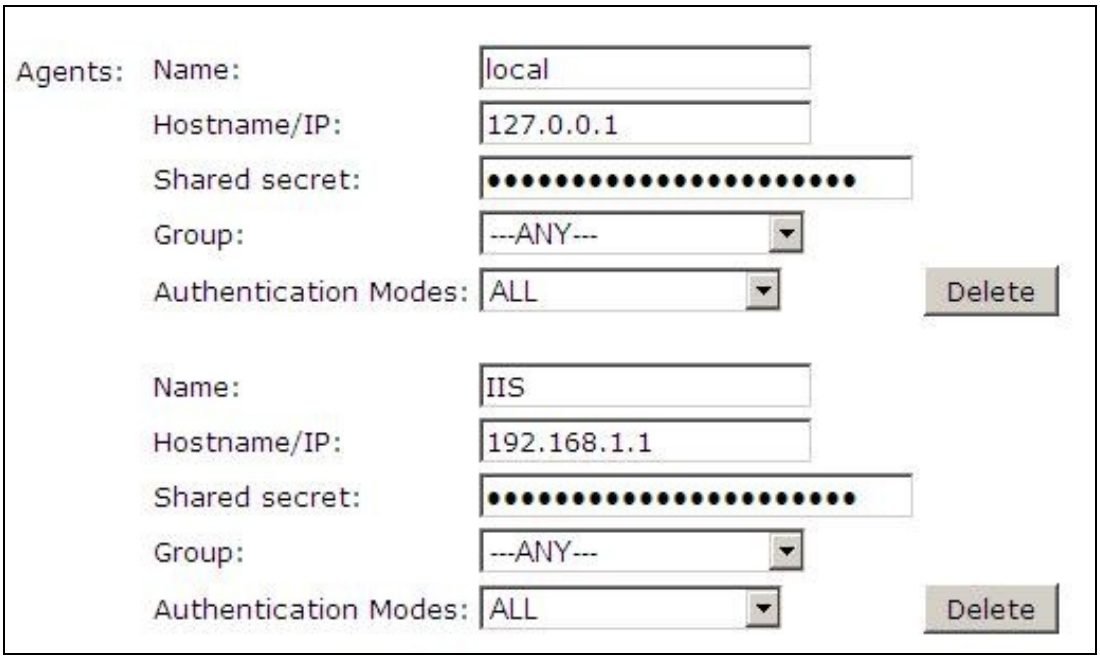
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the IP address or hostname for the server where the salesforce.war is installed, if installed on the same server as the Swivel server use 127.0.0.1 or localhost, a default entry may already exist for this

4. Enter the shared secret to be used above on the below server configuration.

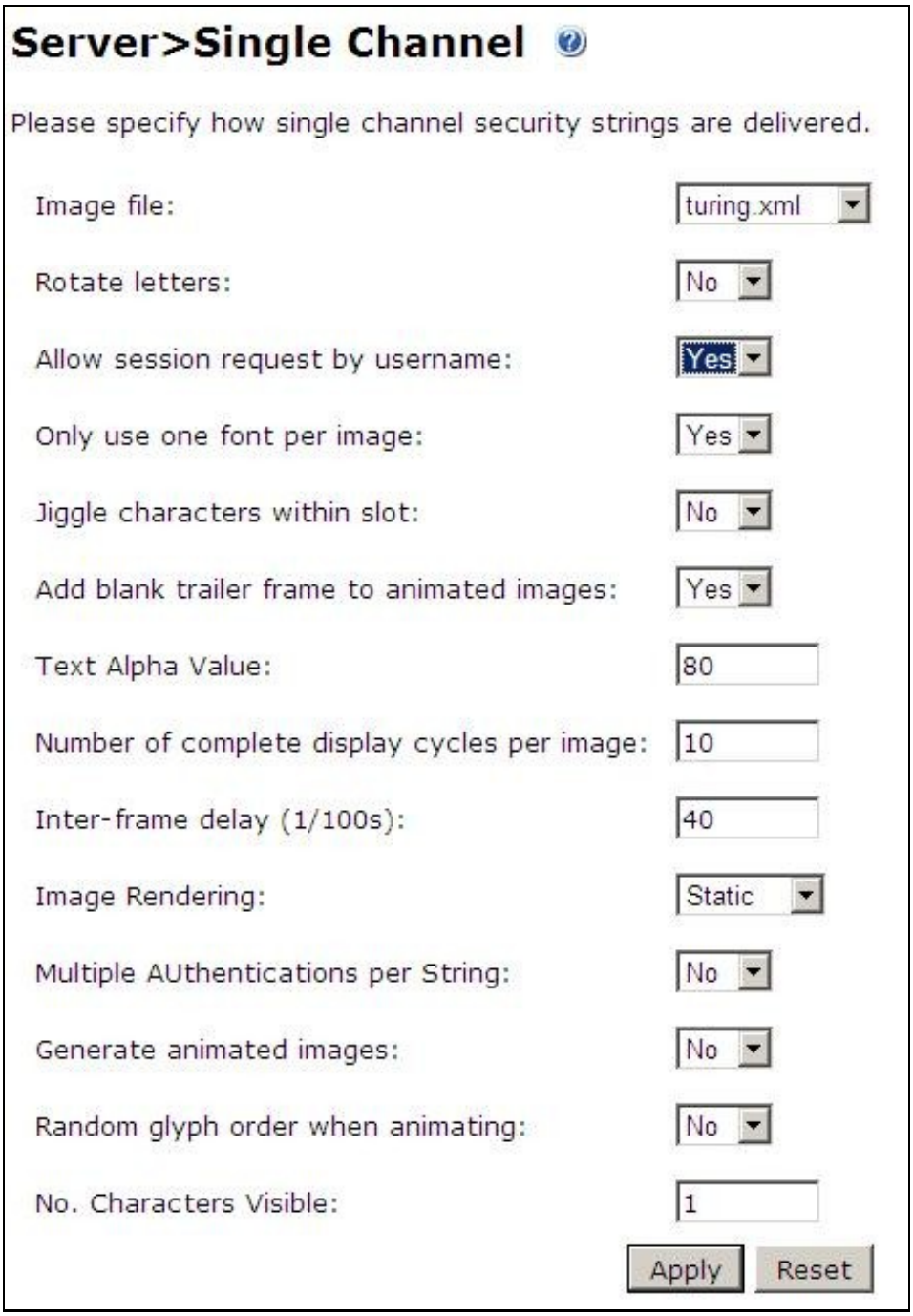
5. Click on Apply to save changes



Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



485.3 Access Device or Application Integration

Client Side Installation

1.The SAML-salesforce war (salesforce.war) should be placed near a Swivel installation on a webserver. This could be a Swivel virtual or hardware appliance. On a Swivel virtual or hardware appliance this would need to be copied to the /usr/local/tomcat/webapps2 folder.

2.Inside the saleforce war exists a properties file (WEB-INF->settings.xml). Initially this will look something like:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">

<properties>
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="port">8080</entry>
<entry key="context">pinsafe</entry>
<entry key="imagessl">true</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imageport">8443</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
<entry key="salesforceURL">https://login.salesforce.com/?saml=02HKiPoin4nQspKPHoScmudQmsKtM.qRKnViSBCmhO5IC52m5VptCNwO.p</entry>
<entry key="audience">https://saml.salesforce.com</entry>
```

```
<entry key="certificateIssuer">http://83.105.30.12:8080/SAMLSalesForce</entry>
<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsaprivkey.der</entry>
<entry key="certificate">./keys/pinsafe/ssl/dsacert.pem</entry>
</properties>
```

These settings should be changed to match, additional field values may need to be created as above:

- The settings for the local Swivel server

For a Swivel virtual or hardware appliance the settings may be:

```
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="context">pinsafe</entry>
<entry key="port">8181</entry>
<entry key="imagessl">true</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imageport">8443</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
```

For a Swivel software install the settings may be:

```
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="context">pinsafe</entry>
<entry key="port">8080</entry>
<entry key="imagessl">false</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">pinsafe</entry>
<entry key="imageport">8080</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
```

- The settings as per the salesforce setup (Setup->Administrative Setup->Security Controls->Single Sign-On Settings)
- The location of the keys (which must match the certificate installed in salesforce)

```
<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsaprivkey.der</entry>
```

485.4 Key and Certificate Generation

see Key and Certificate Generation

485.5 Additional Installation Options

486 Verifying the Installation

In a browser, go to the root URL for the saml-salesforce client. This will redirect to the logon page. Logging in as a user will send a saml assertion for the username you logged in as. If this username matches to a FederationID for a user in Saleforce (see above) then you will be logged in as that user

487 Uninstalling the Swivel Integration

488 Troubleshooting

489 Known Issues and Limitations

490 Additional Information

491 SonicWall NSA Integration

491.1 SonicWall NSA PINsafe integration with SMS

The SonicWALL Network Security Appliance (NSA) Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and antispyware with the application-level control of SonicWALL Application Firewall.

The appliances have SSL VPN capability with which PINsafe can provide Two Factor Authentication using SMS with RADIUS authentication.

If Strong authentication is required using TURing, then the image needs to be displayed to the user such as the use of a Taskbar, Web page etc. The use of TURing is not covered in this document.

491.2 Overview

491.2.1 Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL Network Security Appliance configured for local authentication. Tested with 5.2 and 5.8

491.2.2 Baseline

PINsafe 3.x

NSA 240, SonicOS Enhanced 5.2.0.1-21o

491.2.3 Architecture

The NSA appliance was the firewall/SSL VPN device with the PINsafe server located within the DMZ.

491.3 Installation

491.3.1 Configuring the PINsafe server

Configure PINsafe as a RADIUS server, from the RADIUS/server menu, enter the RADIUS server details and then select Enable RADIUS server. From the RADIUS/NAS menu enter a name for the SonicWALL NAS appliance and its IP address and a shared secret key.

491.3.2 Configuring the SonicWALL NSA Appliance User Settings

Select Users, then Settings, and on the menu for Authentication Method for Login: select RADIUS

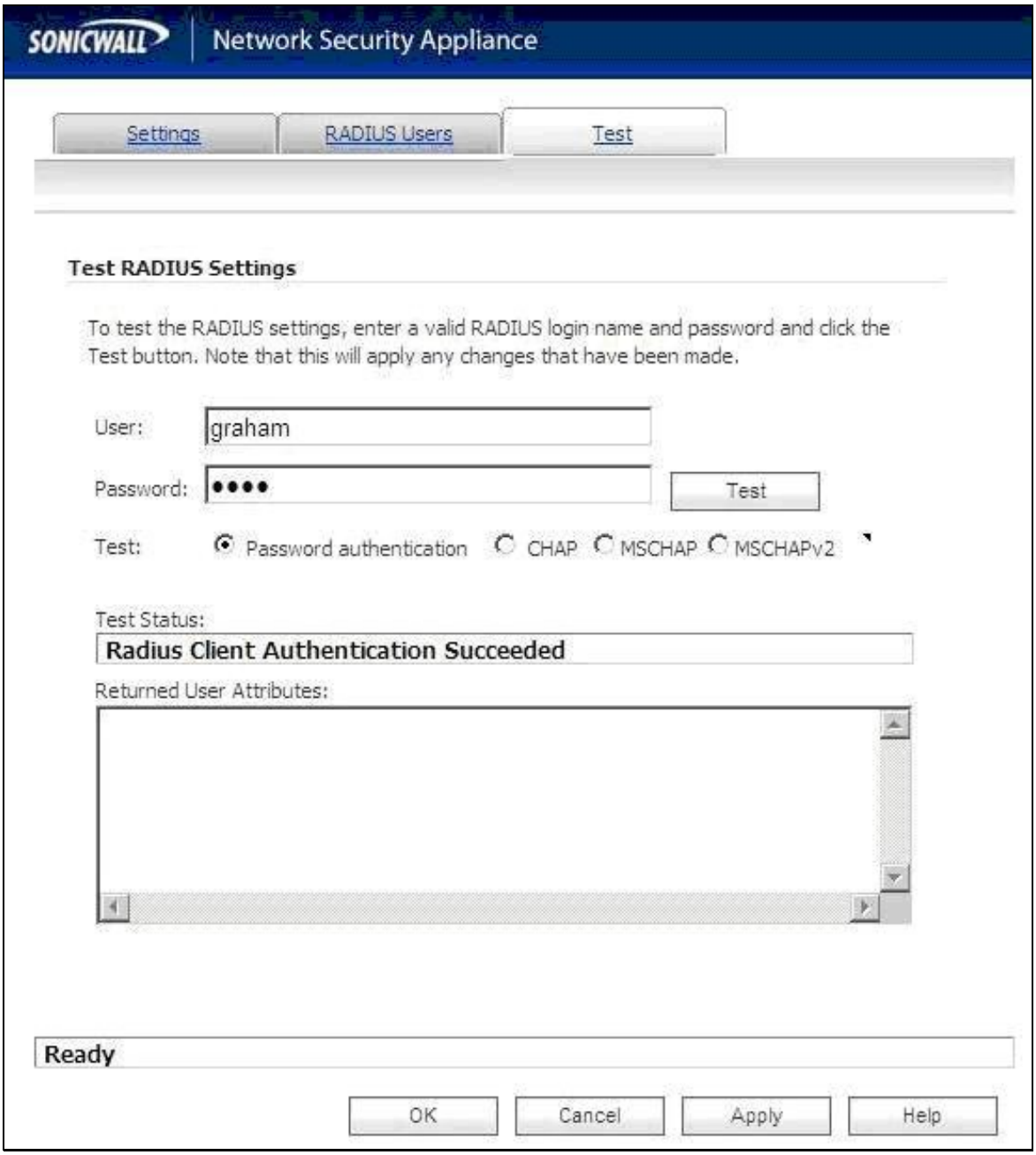
491.3.3 Configuring the SonicWALL NSA Appliance RADIUS settings

From the Users\Settings menu click on Configure button next to the RADIUS option, then select the Settings tab and in the Primary Server IP Address field, enter the IP address of the PINsafe server and the shared secret key, and the required port.

Select the RADIUS Users tab, and ensure there is no tick in the allow only users listed locally box. Enter any other required information.

491.3.4 Testing SonicWALL NSA Appliance RADIUS configuration

Select the Test tab, and enter a Username and a One Time Code in the password field from the users SMS, click on the Test button (Once only), and the returned attributes will verify if the test has worked, or alternatively, enter 1234, and check for a Authentication Rejected message.



491.3.5 Known Issues and Limitations

It is not currently possible to embed the Turing image into the login page, however other options such as the Taskbar utility or a web page can be used.

491.3.6 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 or the local SonicWALL office http://www.sonicwall.com/emea/Support.html.

492 SonicWall SMA Appliances

For Integration with the SonicWall SMA Appliances see SonicWall SSL VPN Integration

493 SonicWall SRA EX appliances

For Integration with the SonicWall SRA EX appliances see SonicWall SSL VPN Integration

494 SonicWall SSL VPN Integration

494.1 Introduction

Swivel can provide Two Factor authentication such as SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

If Strong authentication is required using Single Channel such as TURing, Pinpad then the image can be displayed in the login page or in the Taskbar. The image is served from the PINsafe server to the client.

This document will use the following steps:

- Configuring the PINsafe server
- Configuring the SonicWall login page
- Configuing the SonicWall authentication

To use the Single Channel Image such as the Turing Image, the PINsafe server must be made accessible. The client requests the images from the PINsafe server, and is usually configured using Network Address Translation, often with a proxy server. The PINsafe virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

494.2 Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL SSL VPN

Swivel login script for the SonicWall SSL VPN

The customisation script can be downloaded from here

A customisation script that also includes refresh for the TURing is [1] here

Swivel server must be accessible by client when using Single Channel Images, such as the TURing Image.

494.3 Baseline

SonicWALL SMA

SonicWALL SRA

SonicWALL SSL VPN 200 and 4200 and Firmware 3.5 onwards

SonicOS SSL-VPN 7.5.0.6-23sv

494.4 Architecture

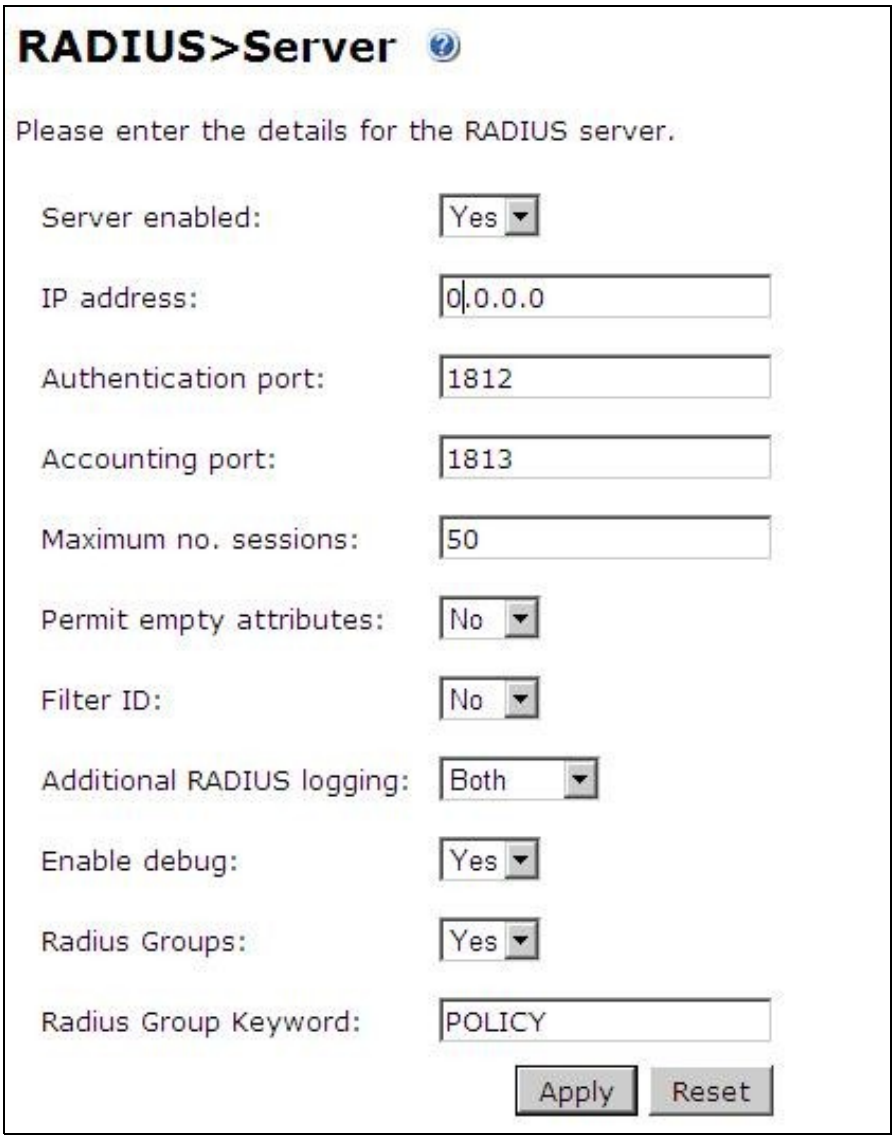
The SSL VPN appliance and the Swivel server are usually located within the DMZ. Authentication requests are made from the SonicWall SSL VPN using RADIUS.

494.5 Swivel Configuration

494.5.1 Configuring the RADIUS server

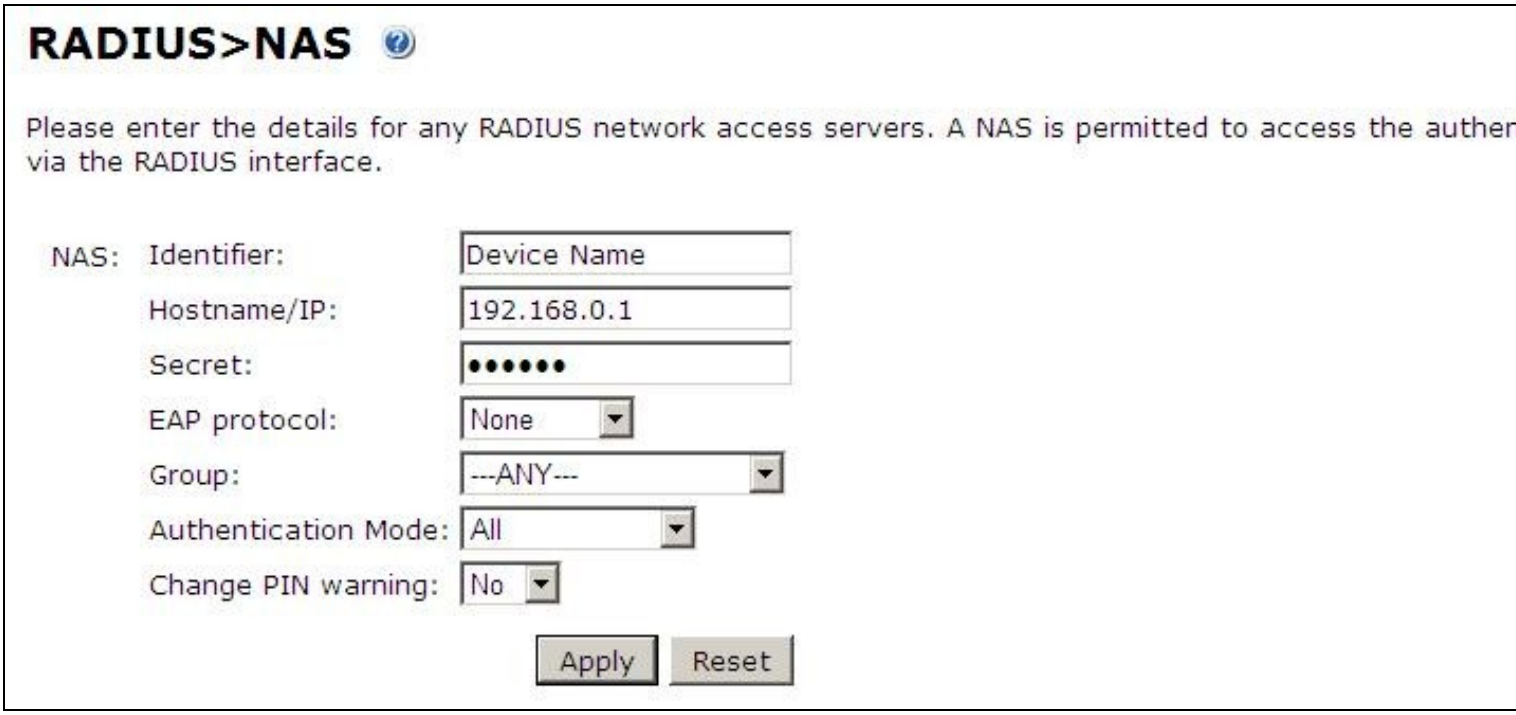
Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the Swivel server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

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



494.5.2 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 SonicWall SSL VPN server. The IP address has been set to the IP of the VPN virtual or hardware appliance, and the secret that will be used on both the Swivel appliance and VPN RADIUS configuration.



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.

494.5.3 Enabling Session creation with username

The Swivel appliance can be configured so that it returns an image stream containing a TURing image by presenting the username via the XML API or the SCImage servlet. It is this mechanism that is used to return the TURing image to the VPN sign in page.

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 PINsafe username:

Virtual or hardware appliance

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

For a software only install see Software Only Installation

For further information see Single Channel How To Guide

494.5.4 Setting up Swivel Dual Channel Transports

See Transport Configuration

494.5.5 Using AD Password Authentication

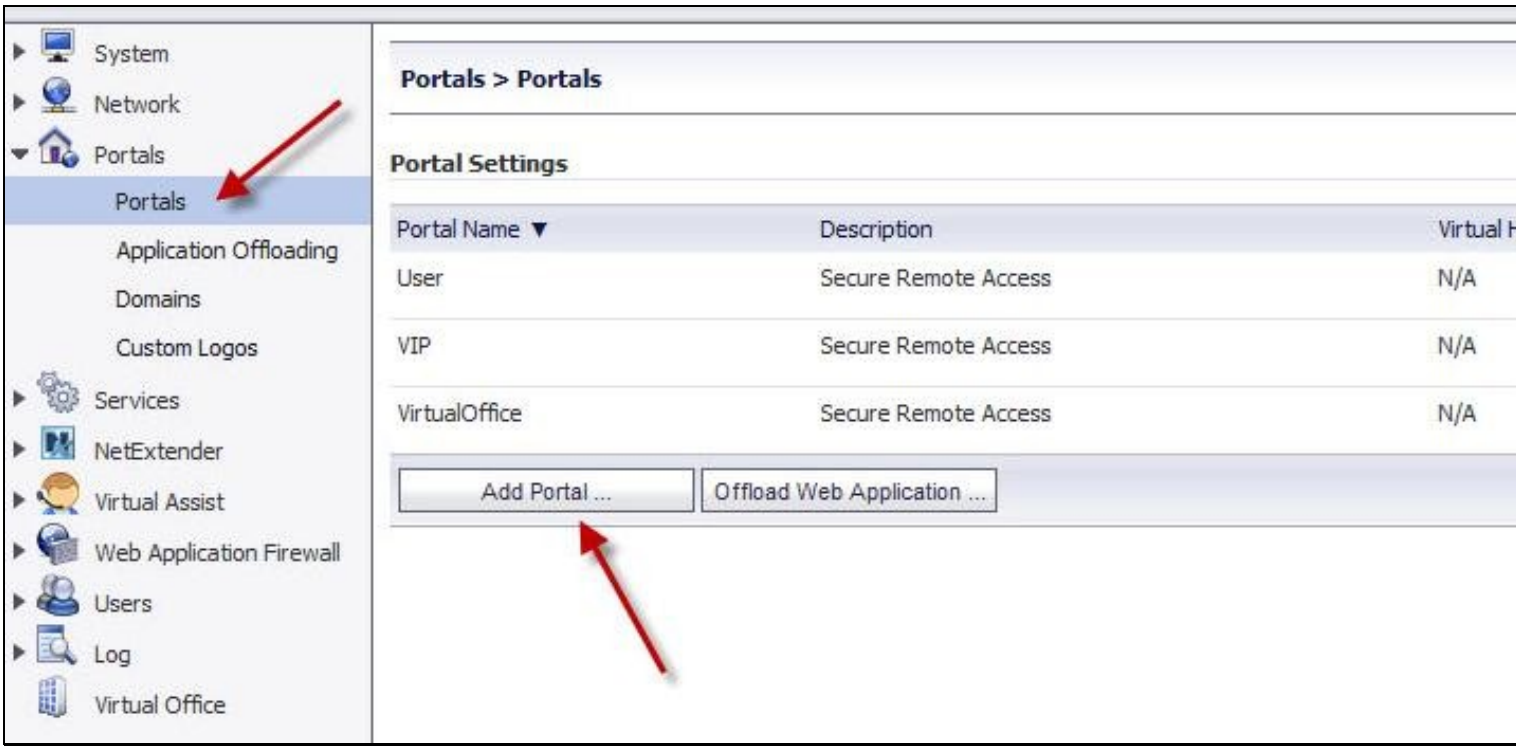
This is an option to enter the AD password of users for authentication

See Check Password With Repository

494.6 SonicWall SSL VPN Configuration

494.6.1 Login Page Customisation

On the SonicWall SSL VPN select Portals, then click on Add Portal to open the add portal page.



Enter the following information:

Portal Name: Name for the Portal, Example, PINsafe

Portal Site Title: Name for Portal Site, Example Virtual Office

Portal Banner Title: Name for Page, Example Virtual Office

Login Message: optional login message. If the Single channel TURing image is to be used then the login script needs to be pasted into this section. Ensure the relevant scripts are modified with the External IP NAT address of the PINsafe server:

```
$('#psImage').attr('src', 'https://192.168.0.35:8443/proxy/SCImage?username=' + encodeURIComponent(username));
```

For a PINsafe virtual or hardware appliances this would need to be:

https://192.168.0.35:8443/proxy/SCImage?username=

For a software only install see Software Only Installation

Portal URL: The name of the login portal

Display custom login page: Ensure this is ticked

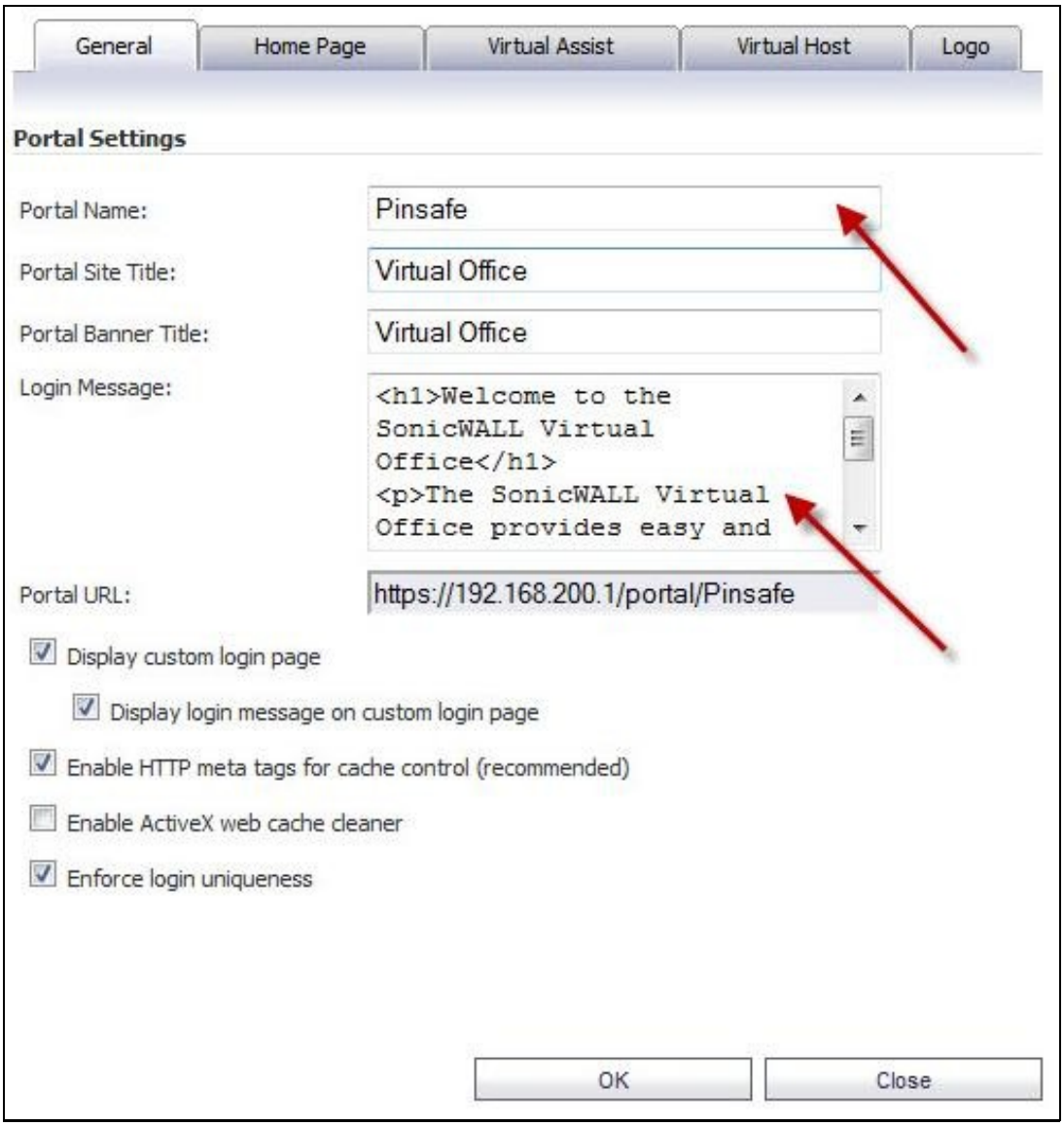
Display login message on custom login page: Ensure this is ticked

Enable HTTP meta tags for cache control (recommended): Usually selected

Enable ActiveX web cache cleaner: Optional

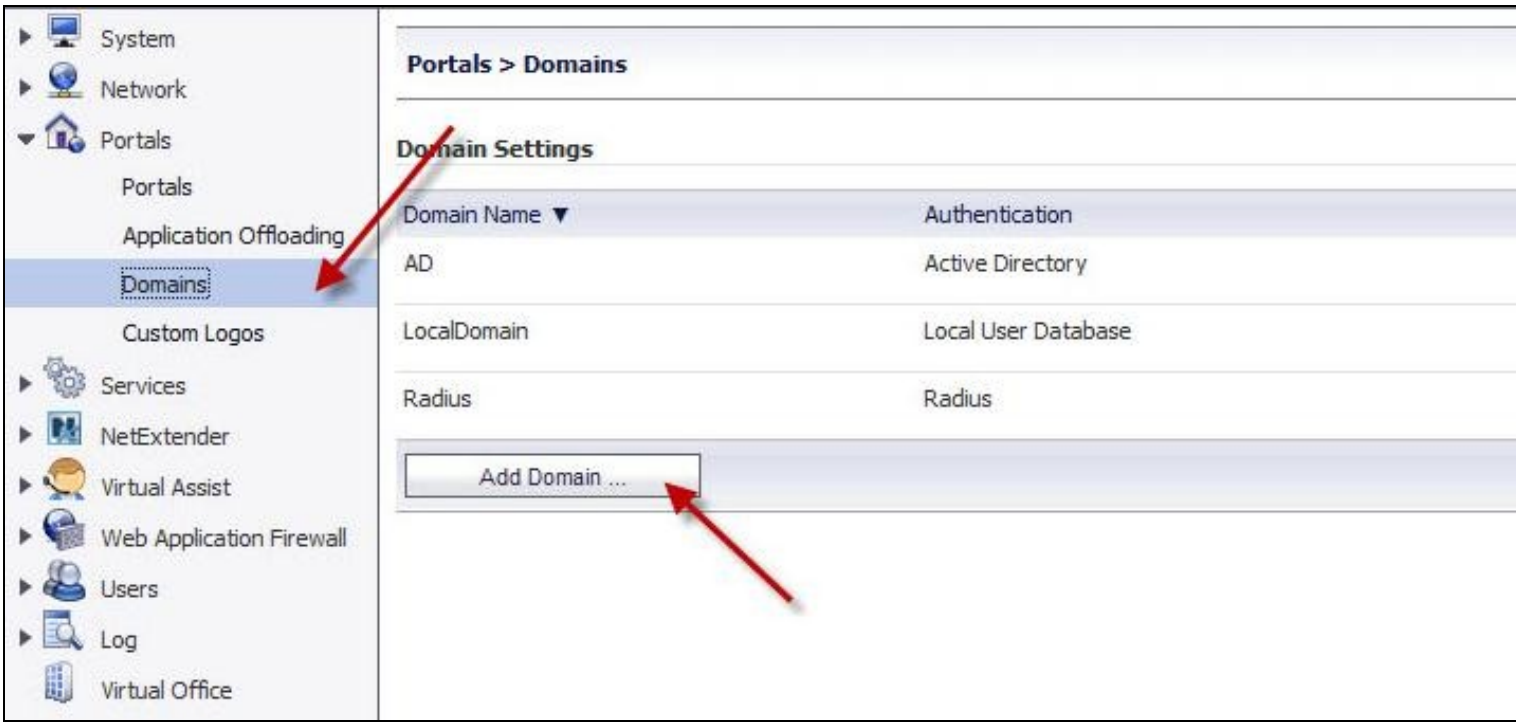
Enforce login uniqueness: Ensure this is ticked

Click OK to save the settings.



494.6.2 Configuring SonicWall SSL VPN Domain Settings

On the SonicWall SSL VPN select Portals then domains and click on Add Domain.



On the Add Domain page configure the Authentication server

Authentication type: select RADIUS

Domain name: Name for the domain

Authentication Type: Select the required authentication

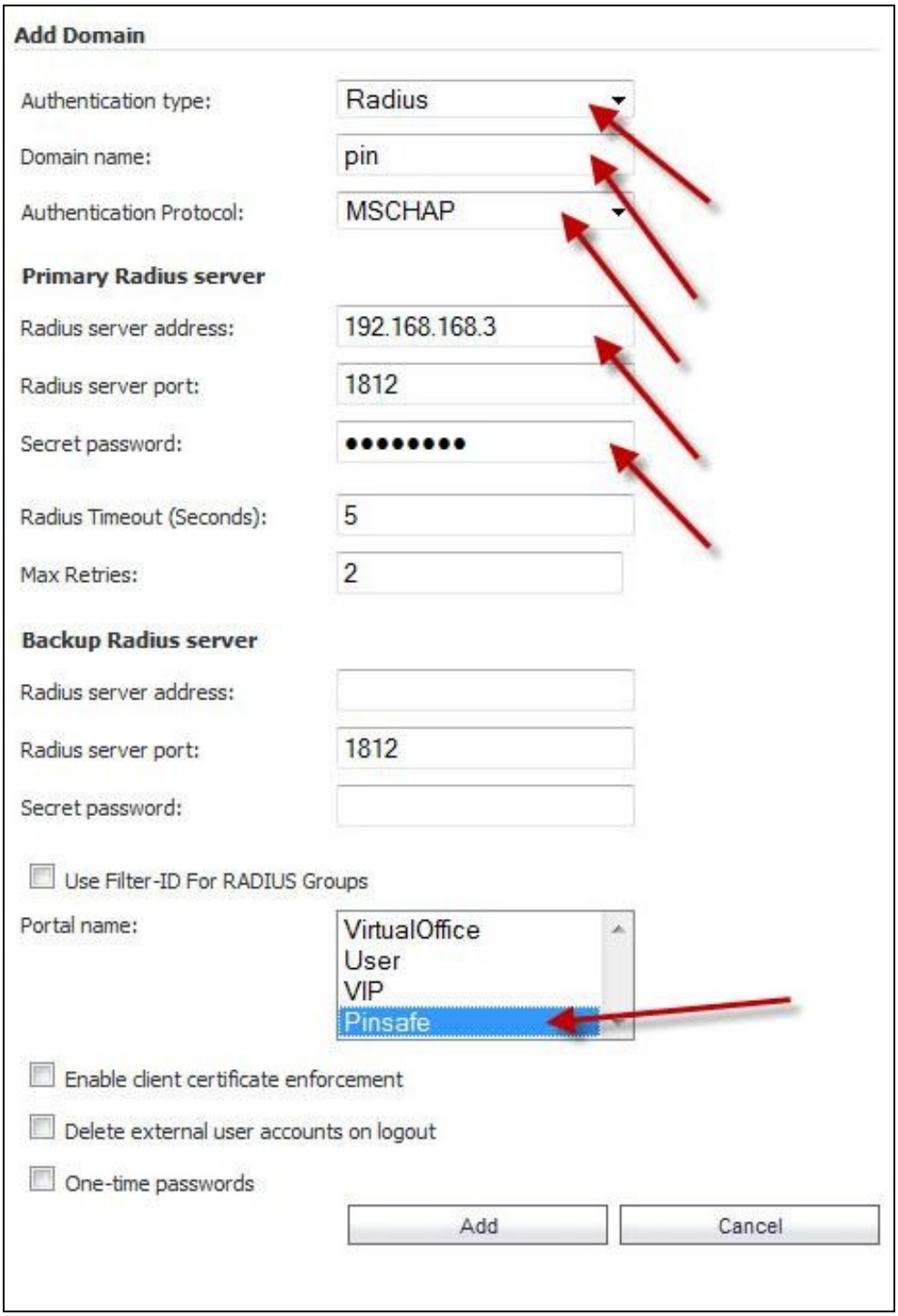
RADIUS server address: Hostname or IP address of the PINsafe server

RADIUS server port: Usually 1812

Secret password: Enter a shared secret that needs to be also entered on the PINsafe server NAS entry

Portal Name: Select the Portal Name created above.

Click OK to save the settings.

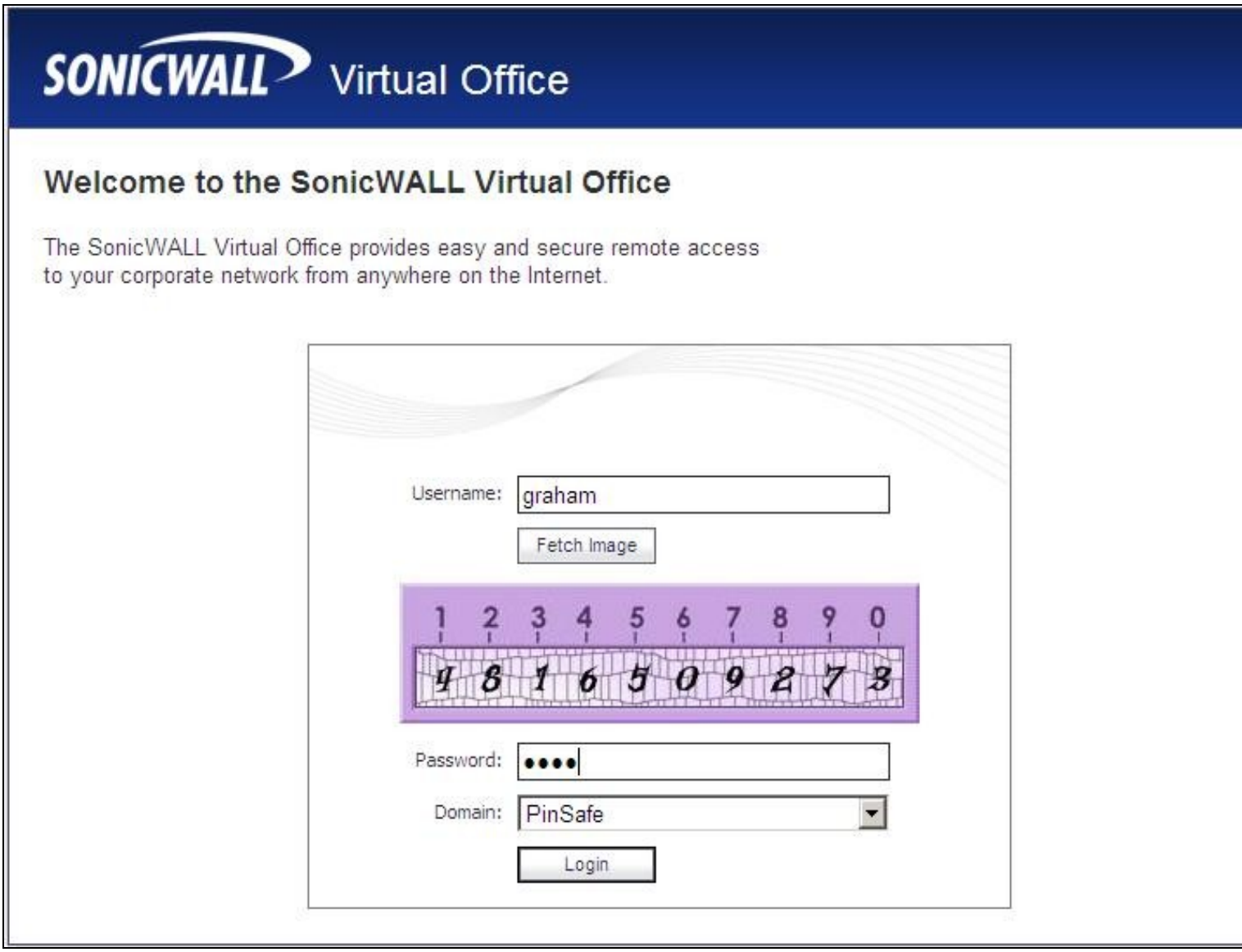


494.7 Additional Configuration Options

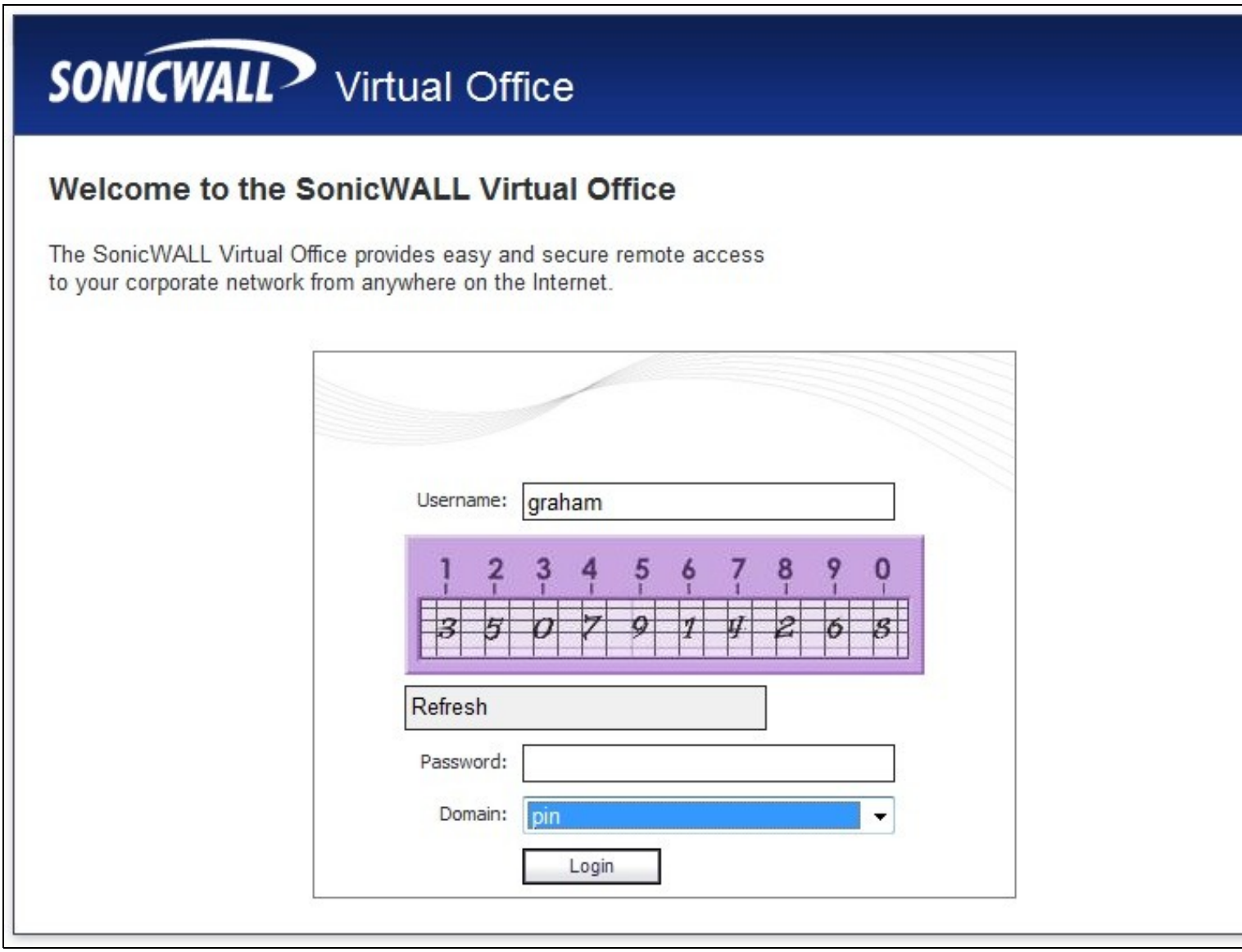
494.8 Testing

Browse to the login page and verify the login

Login page showing the TURing image where OTC is entered as the Password



Login page showing the TURing image with where OTC is entered as Passsword and a *Refresh* Image button



494.9 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Users can bypass Swivel authentication

When a user authenticates using RADIUS, a local account may be created on the SonicWall. With some SSO policies the user may then not be required to sign in using RADIUS authentication. Verify the SSO policy and adjust as required.

494.10 Known Issues and Limitations

None

494.11 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

495 Stonesoft Integration

496 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.

497 Prerequisites

Stonesoft Firewall

Swivel 3.x

Modified login page for TURing

Modified login page for PINpad

498 Baseline

Stonesoft 4.9.9|1050

Swivel 3.9

499 Architecture

Stonesoft makes authentication requests against the Swivel server by RADIUS.

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

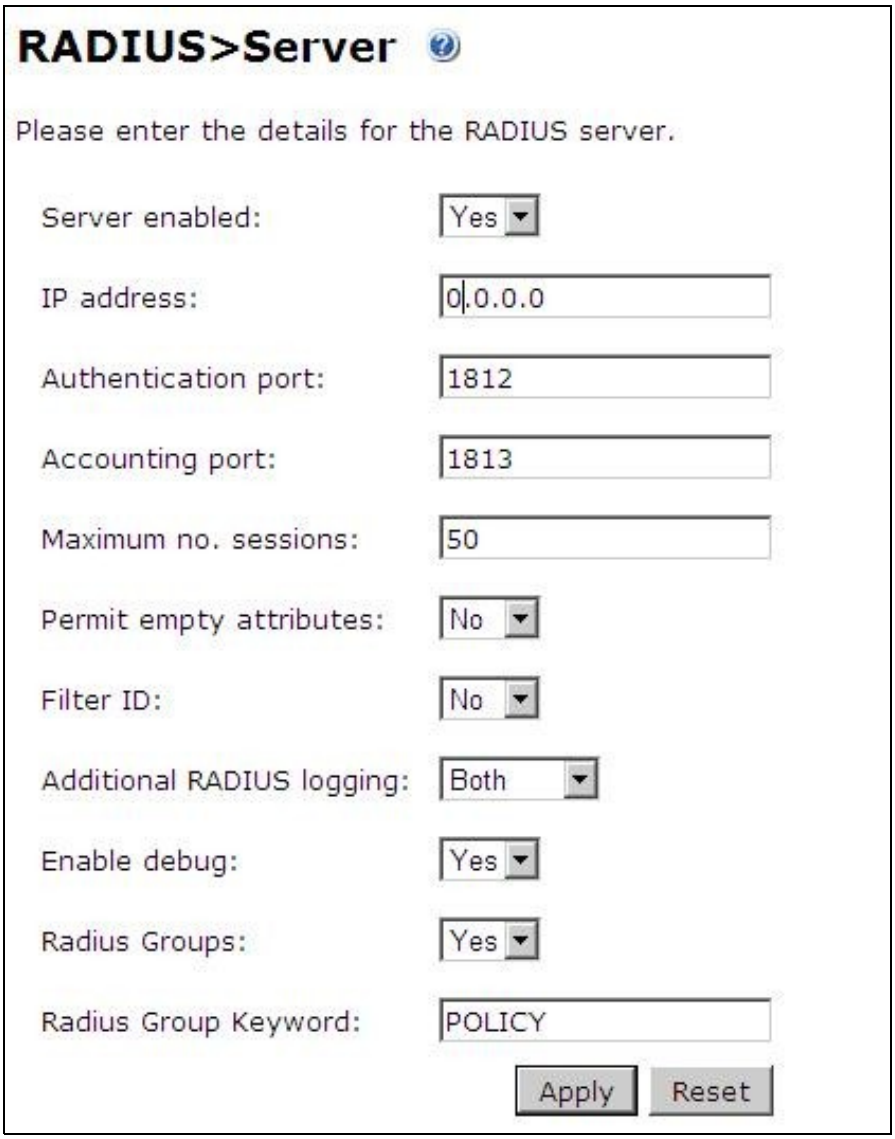
500 Swivel Configuration

500.1 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.

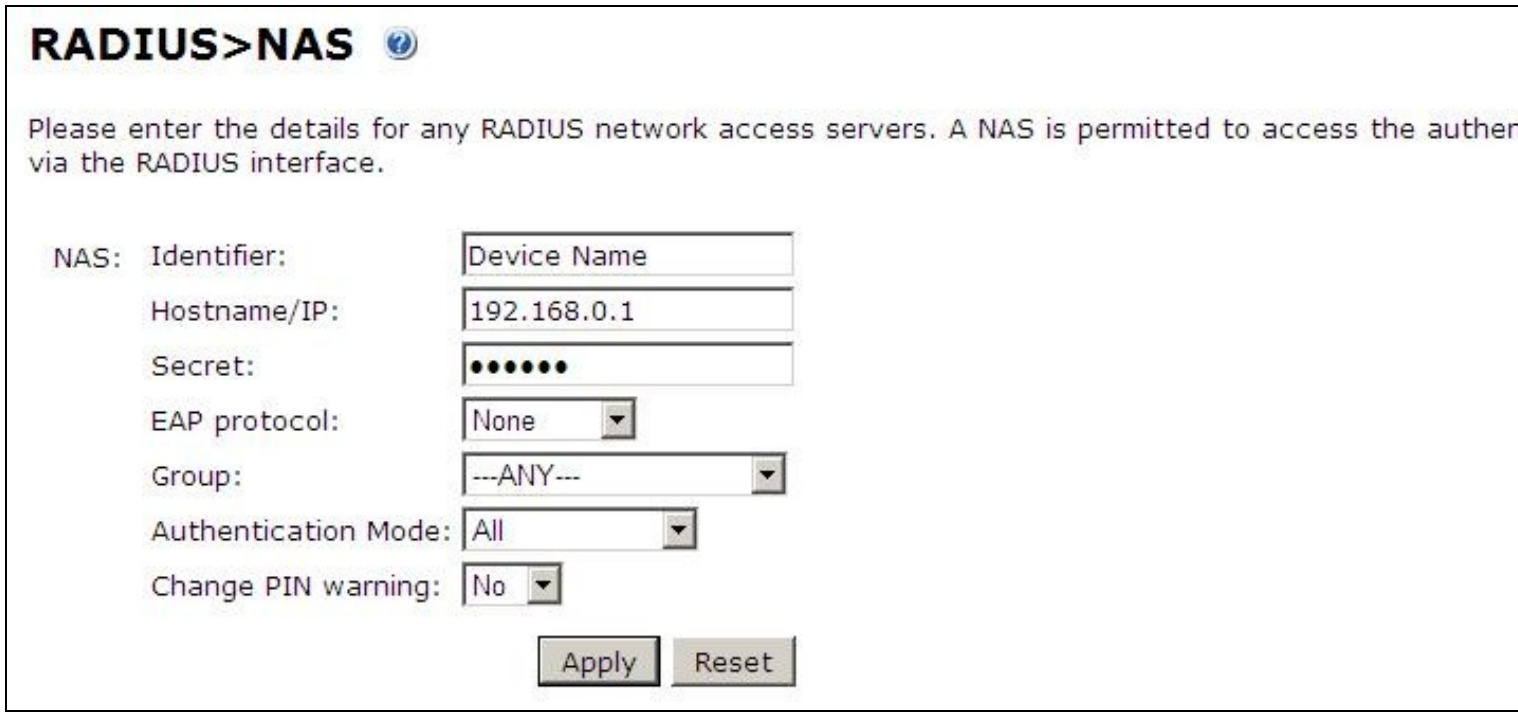
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

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



500.2 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.



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.

500.3 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

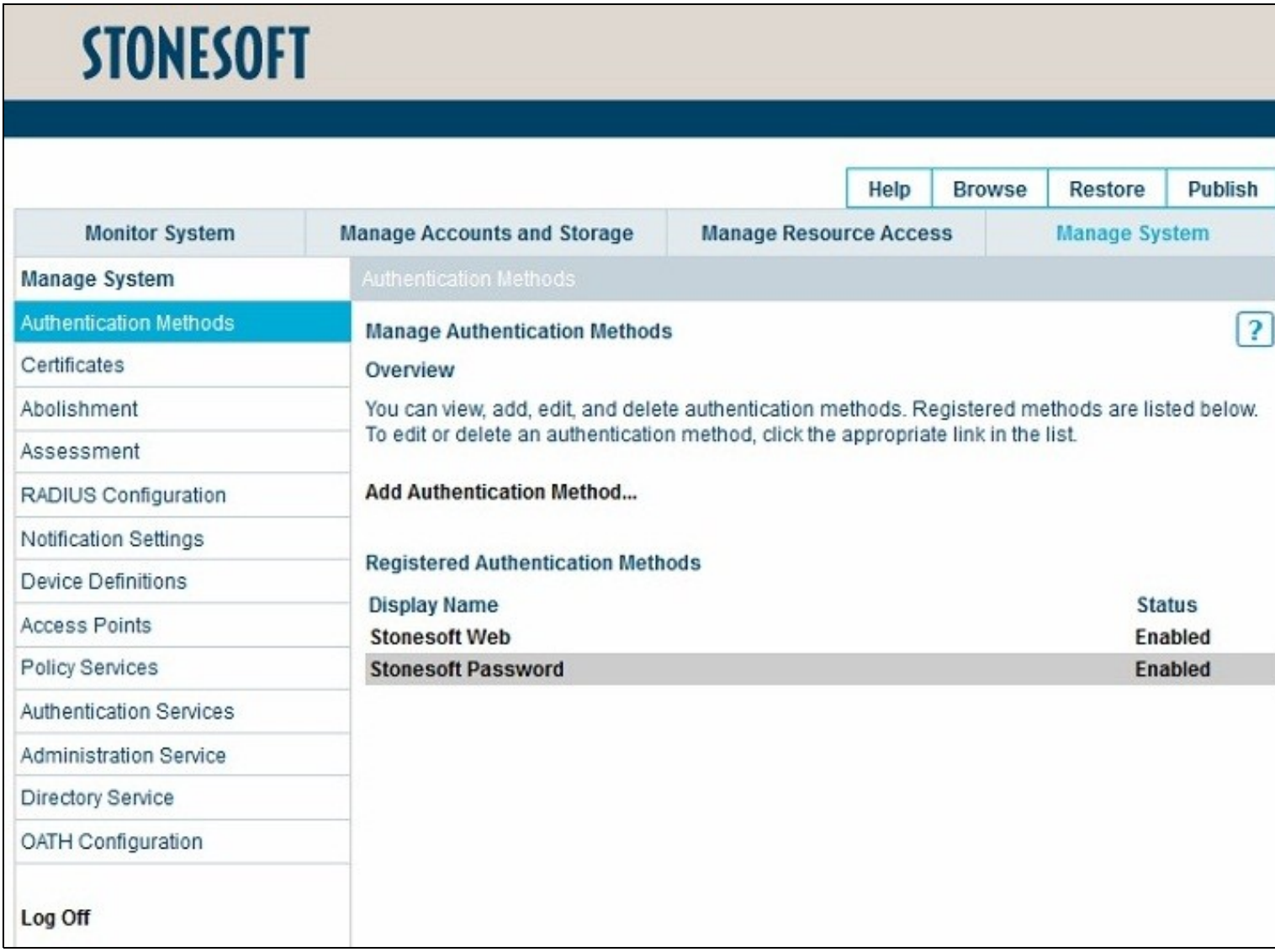
https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installation

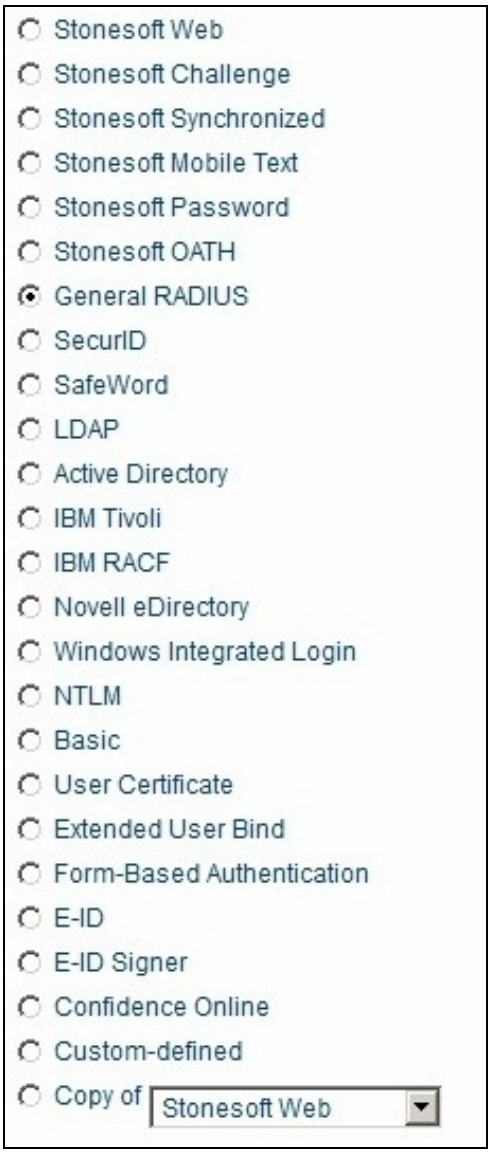
501 Stonesoft Configuration

501.1 Create a Radius Authentication Method

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



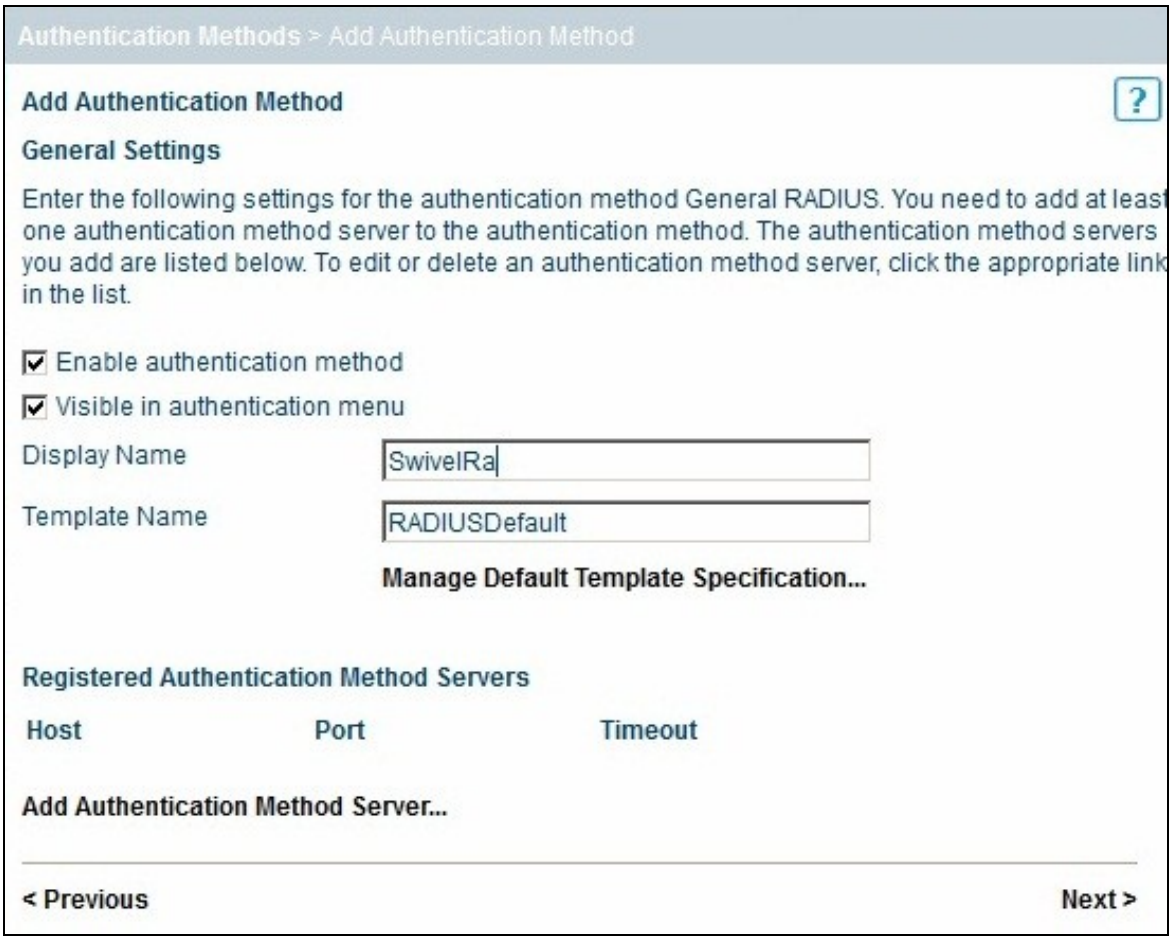
Select the *General RADIUS* authentication method



Ensure the following are checked:

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

Enter a Display Name, then click on Next.



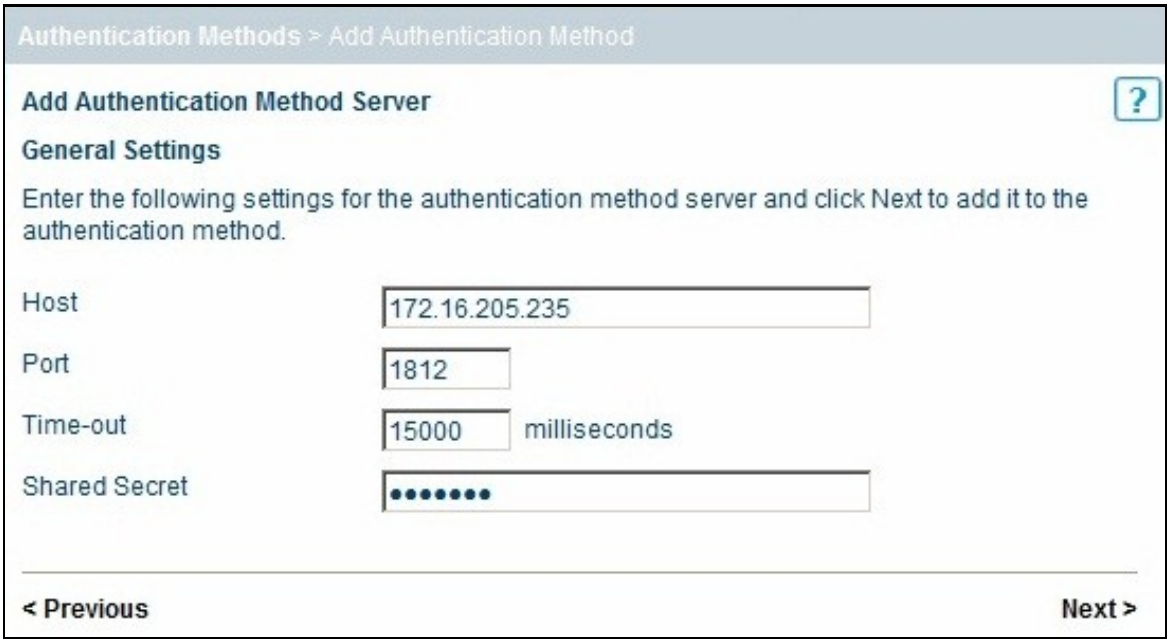
Enter the following information and when complete click Next:

Host: Hostname/IP address of the Swivel server

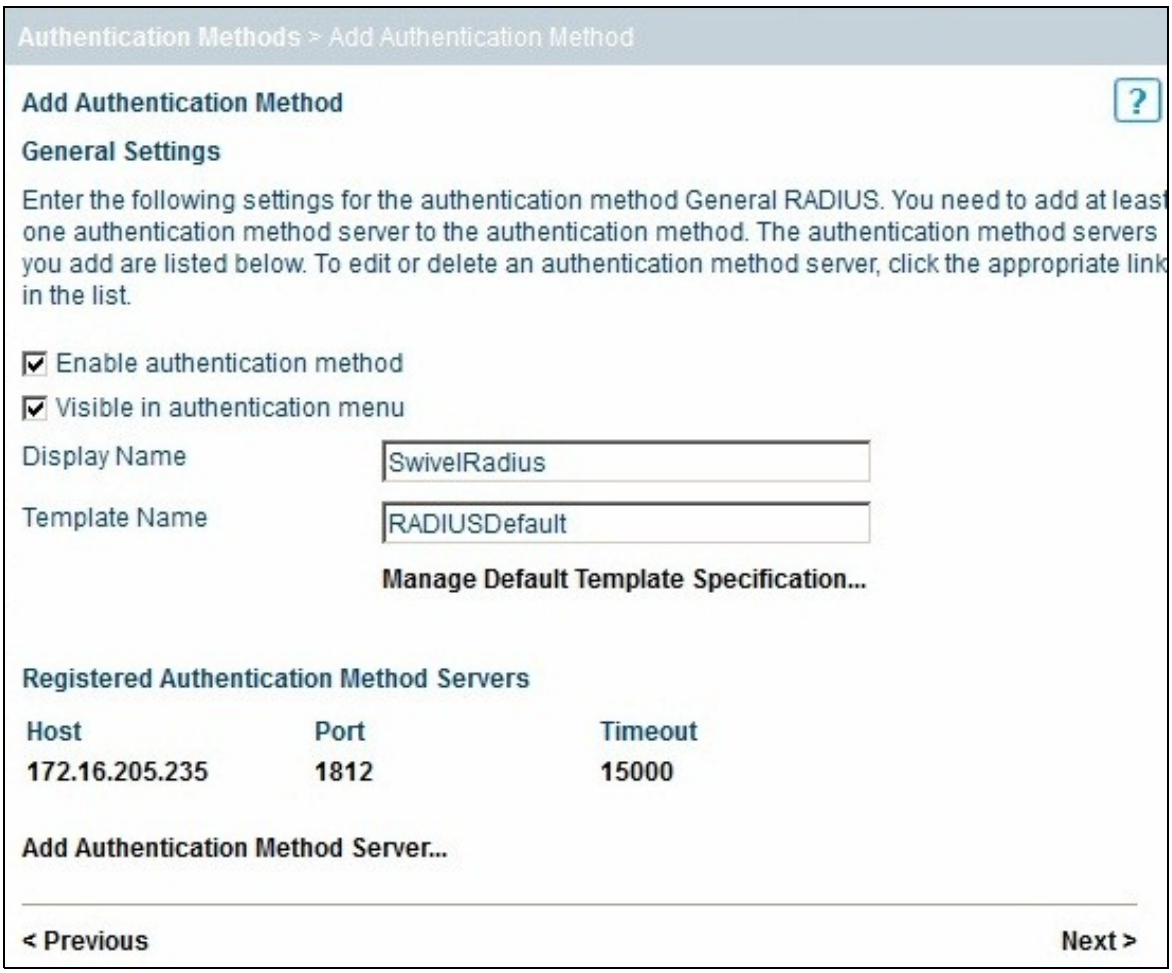
Port: RADIUS authentication port, 1812 is the default for Swivel

Time-out: default 15000 milliseconds

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

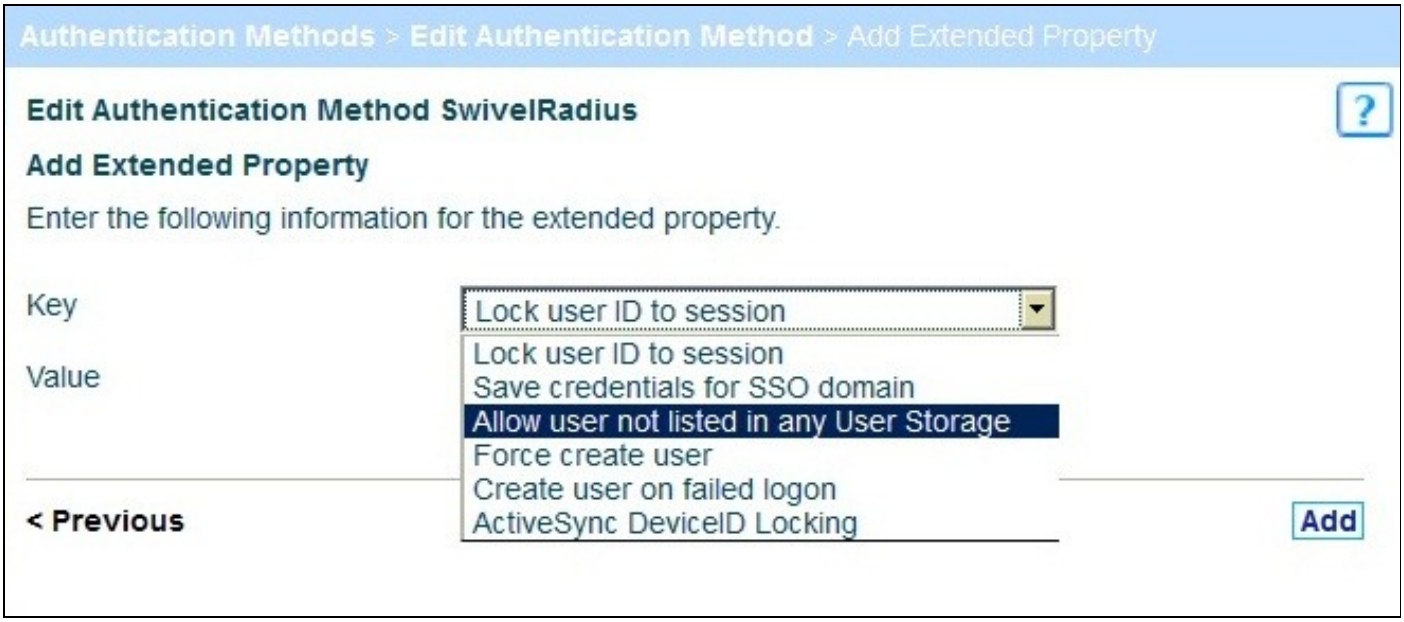


Leave the RADIUS Reply settings as default unless a specific RADIUS configuration is required



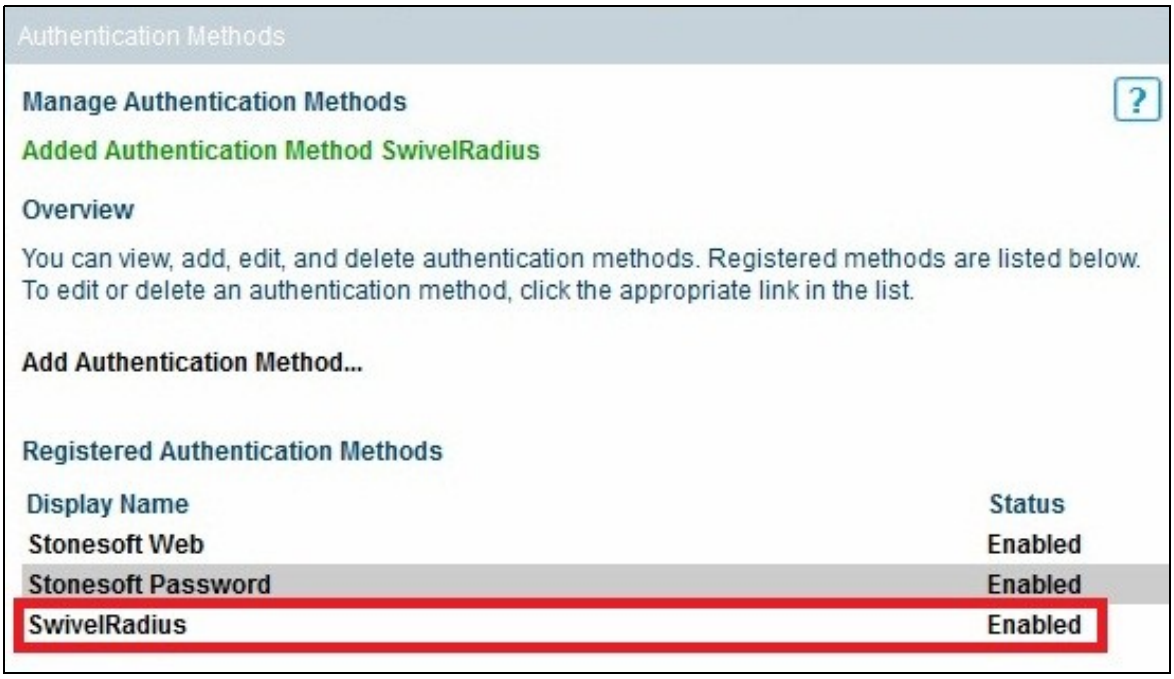
On the Extended Properties page click on Add Extended Property then select *Allow user not listed in any User Storage* and set it to *true*

The *Reveal RADIUS reject reason* can be used for troubleshooting if set to true.

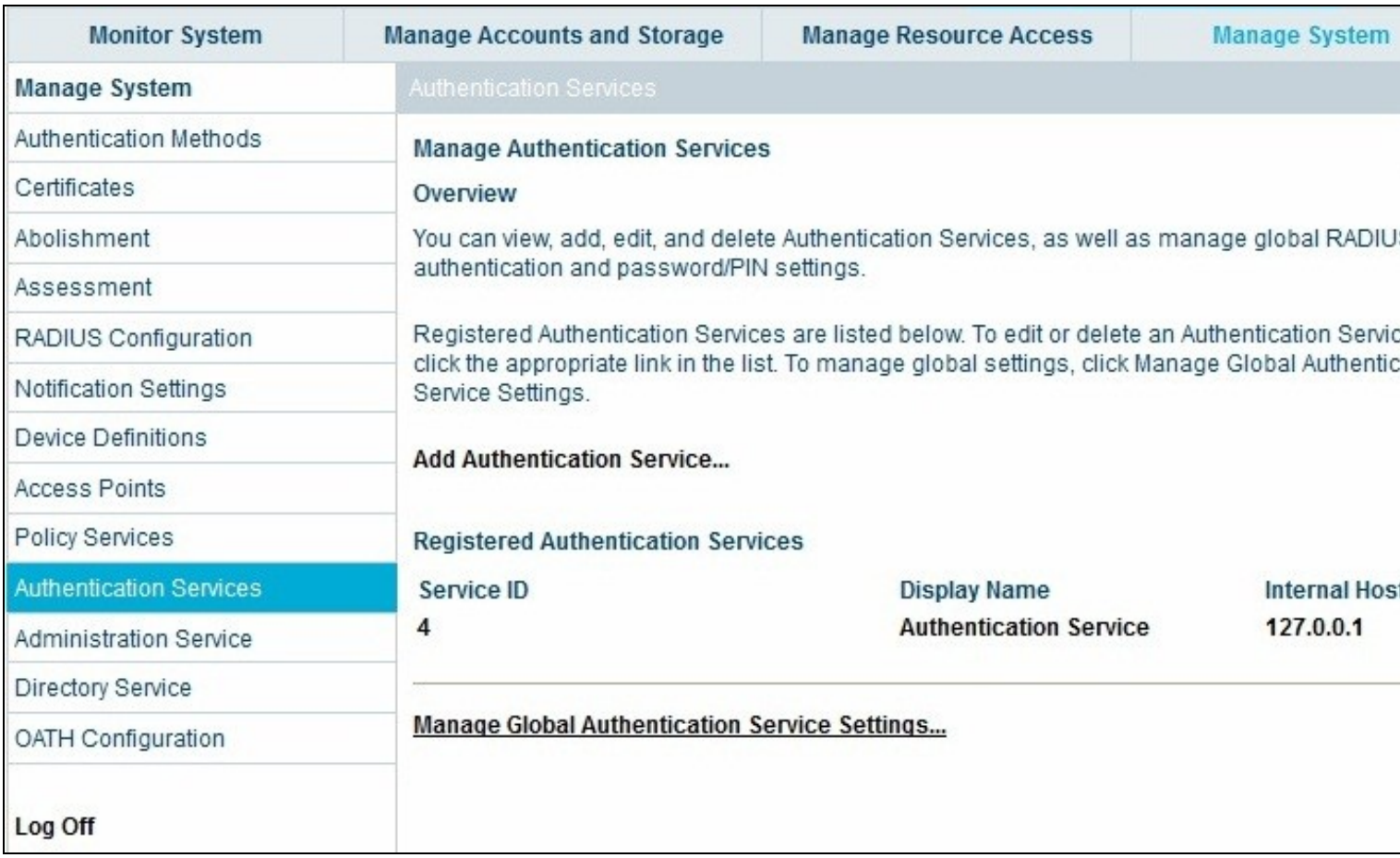


possibly not use: Stonesoft Authentication Method RADIUS Extended Properties.jpg

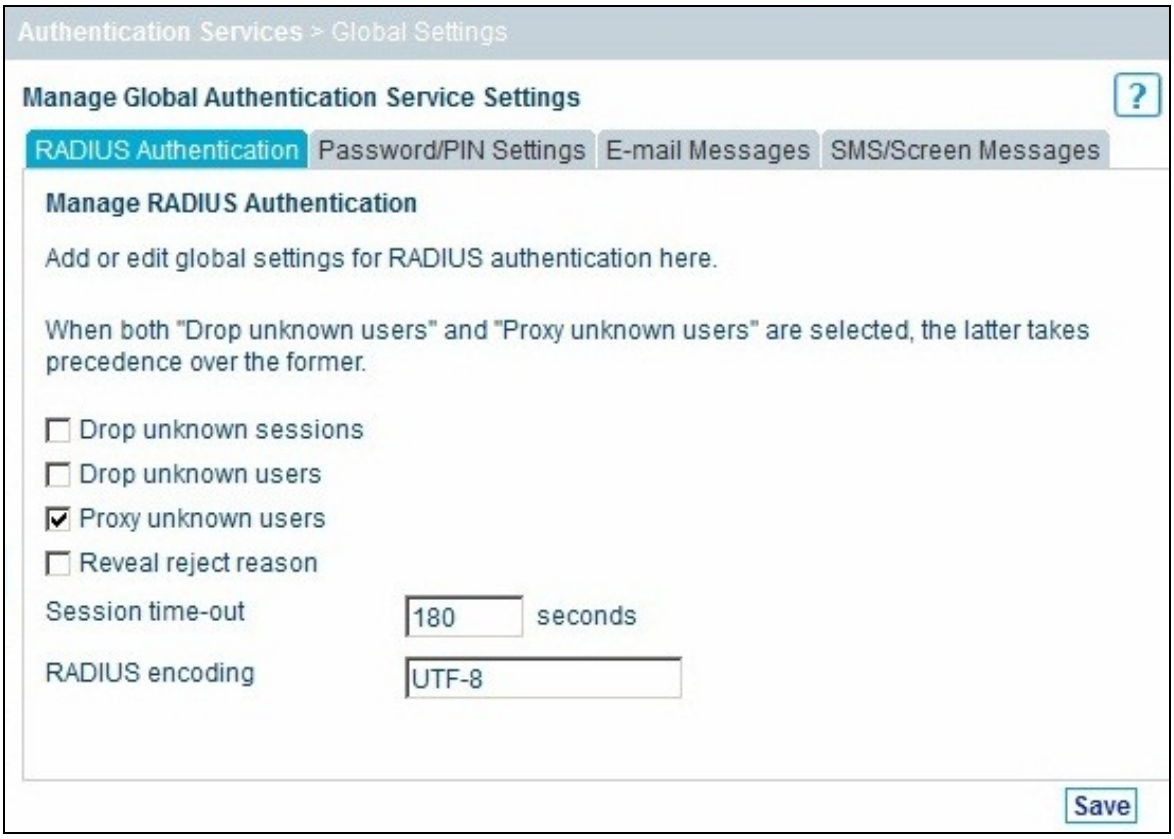
The configured RADIUS authentication method will appear under the list of *Registered Authentication Methods*.



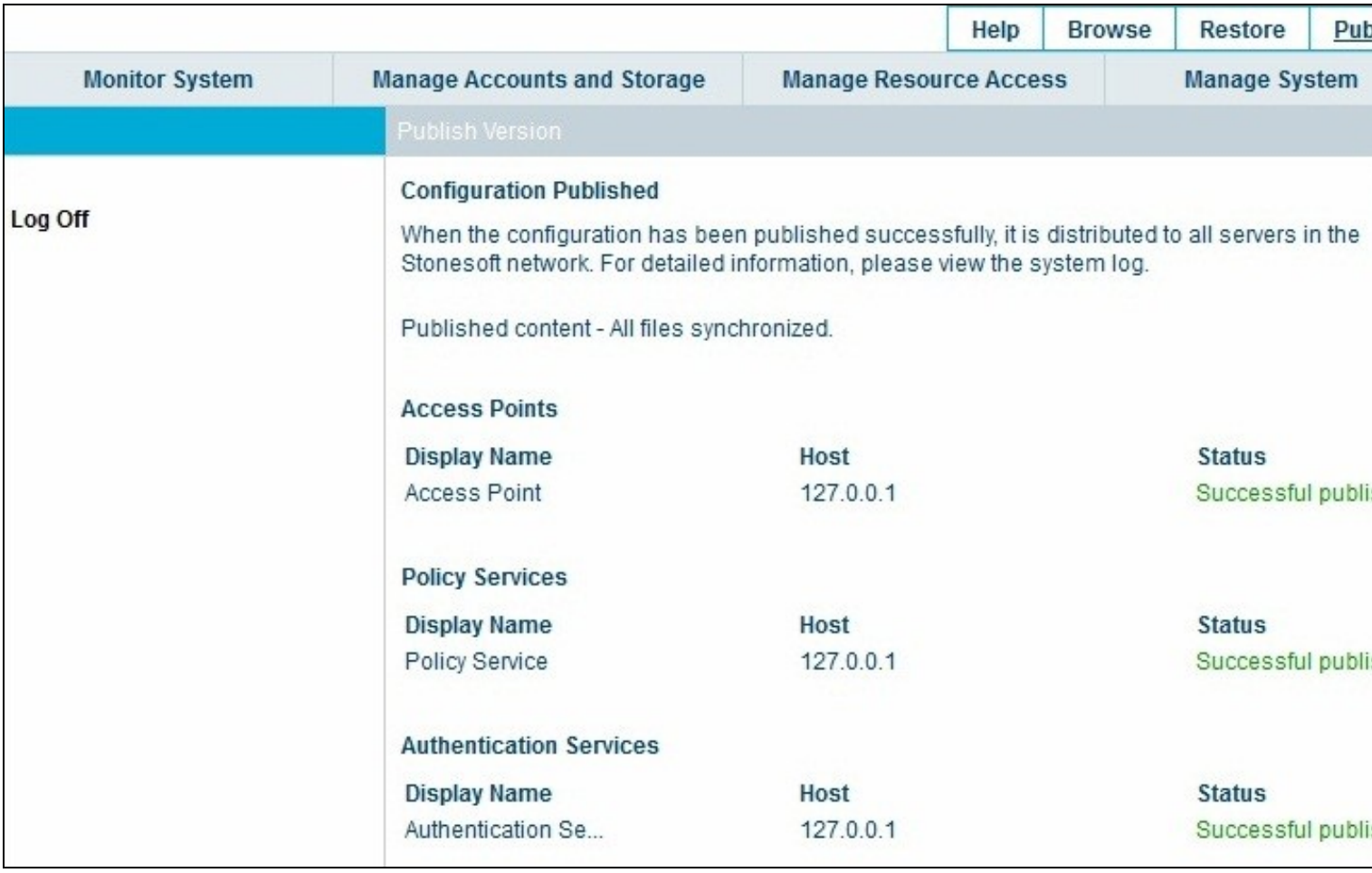
Select *Authentication Services* then *Add Authentication Service*



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



When the configuration is complete then select publish



501.2 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.

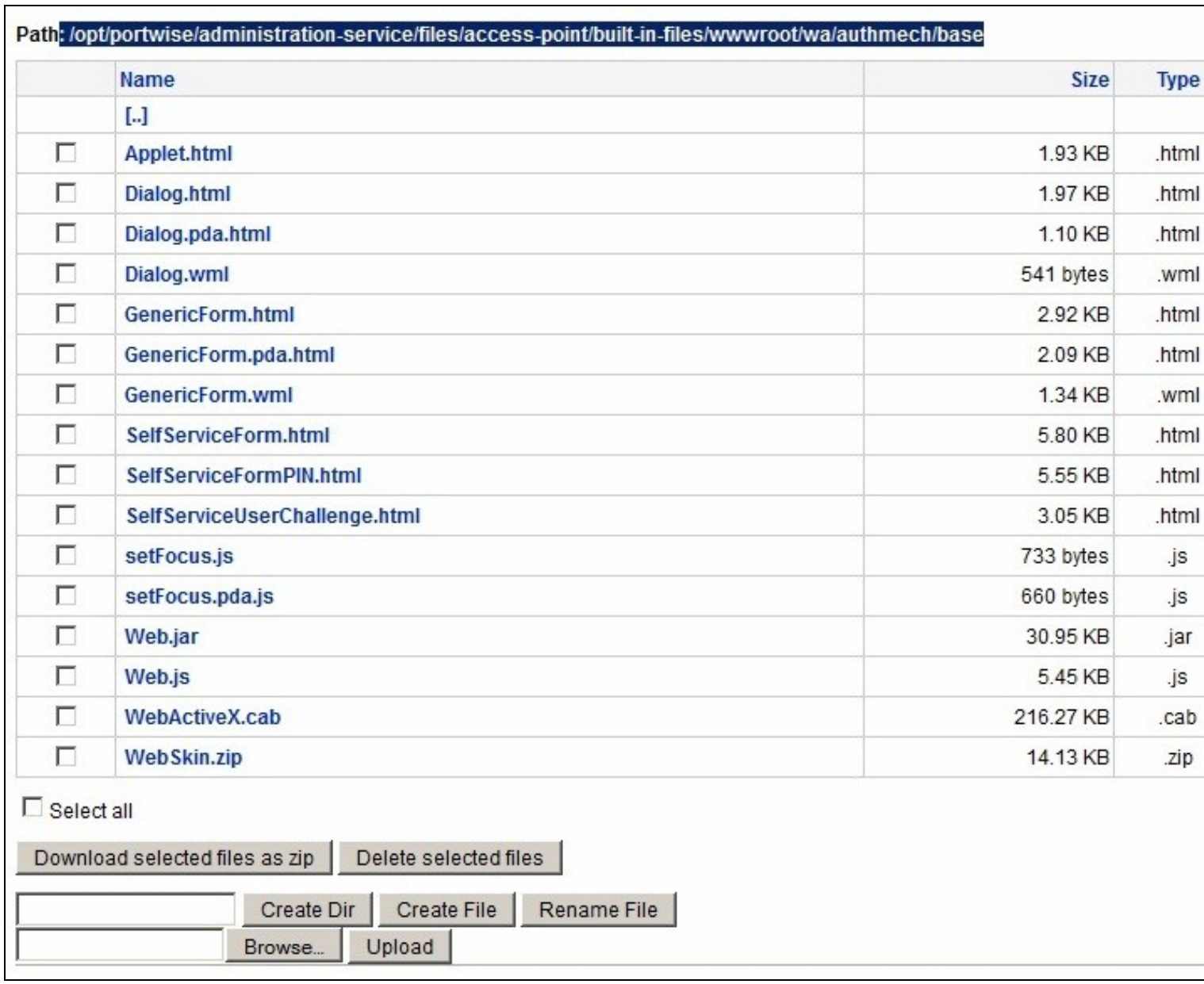
501.3 Login Page Customisation

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*

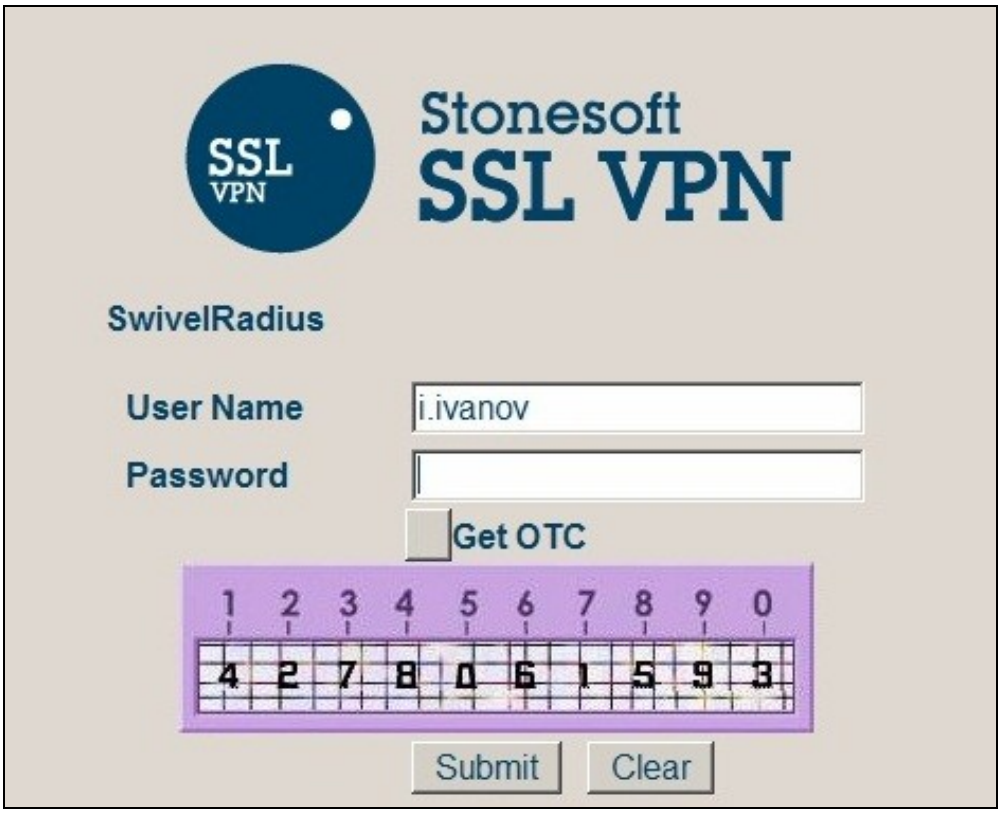


502 Testing

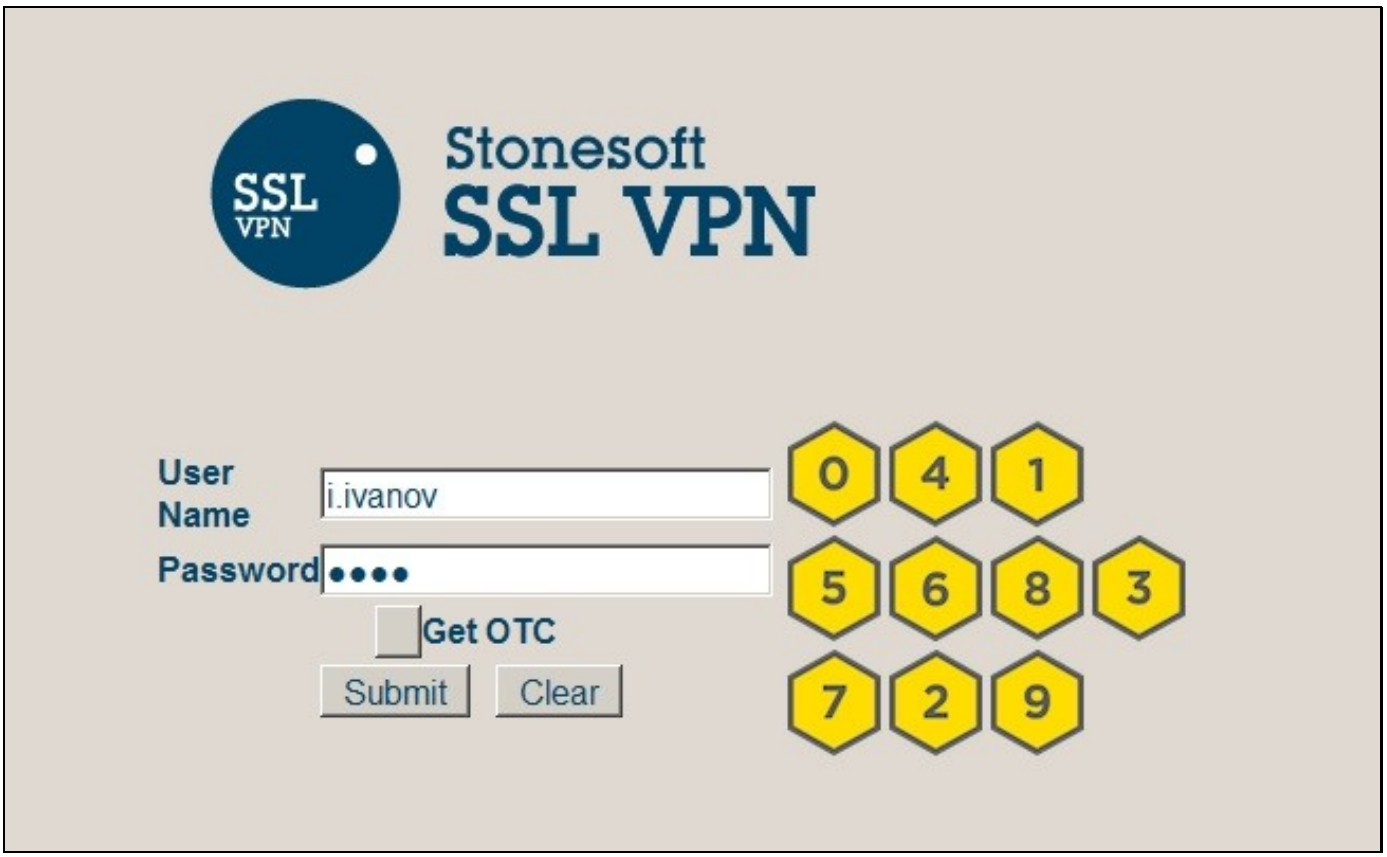
Browse to the login page and view the login page for the required configuration.

Stonesoft login page with Dual Channel using SMS, Mobile Client

Stonesoft login page with Single Channel TURing image



Stonesoft login page with PINpad



503 Additional Configuration Options

503.1 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.

504 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

505 Known Issues and Limitations

None

506 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

507 Swivel Windows Credential Provider

508 Introduction

Version 5 of the Credential Provider is now released. Documentation on it can be found at Windows Credential Provider. This documentation is out of date, and is not being maintained

This version has been tested on Windows 8, Windows 10 and Windows Server 2012 R2

The current version only works for 64 bit operating systems.

Swivel Windows Credential Provider is used in the desktop operating systems Windows 8 and 10 and the server operating system Windows Server 2012. For integration with Windows Vista and 7 and Server 2008, see Microsoft Windows Credential Provider Integration.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using TURing.
- **PINpad** Lets the user sign into windows by using PINpad.
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.

NOTE: One Touch is not currently supported.

508.1 Downloads

Swivel Windows Credential Provider 64 bit (version 5.1.0)

508.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel has the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance. There is also a "Trusted Users" list where specific users can be added.

Q). Is it possible to define users who do not have Swivel authentication? A). Yes either by the *Allow Unknown Users* for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password, A). No the AD password is required.

509 Prerequisites

Swivel version 3.11.3 or later.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1) and 10 or Windows Server 2012.

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 5.1.0)

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

510 Baseline

Swivel 3.10.4

Windows 8, 10, Server 2012 R2.

511 Installation

511.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Windows 8, 8.1 and 10 the computer must be restarted.
- On Windows Server 2012 R2 the Administration account can be signed out rather than doing a full restart.

511.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, keeping the default name.
2. Copy this file and the installation file onto the new computer, they must be in the same location (example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

512 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

512.1 Offline Authentication

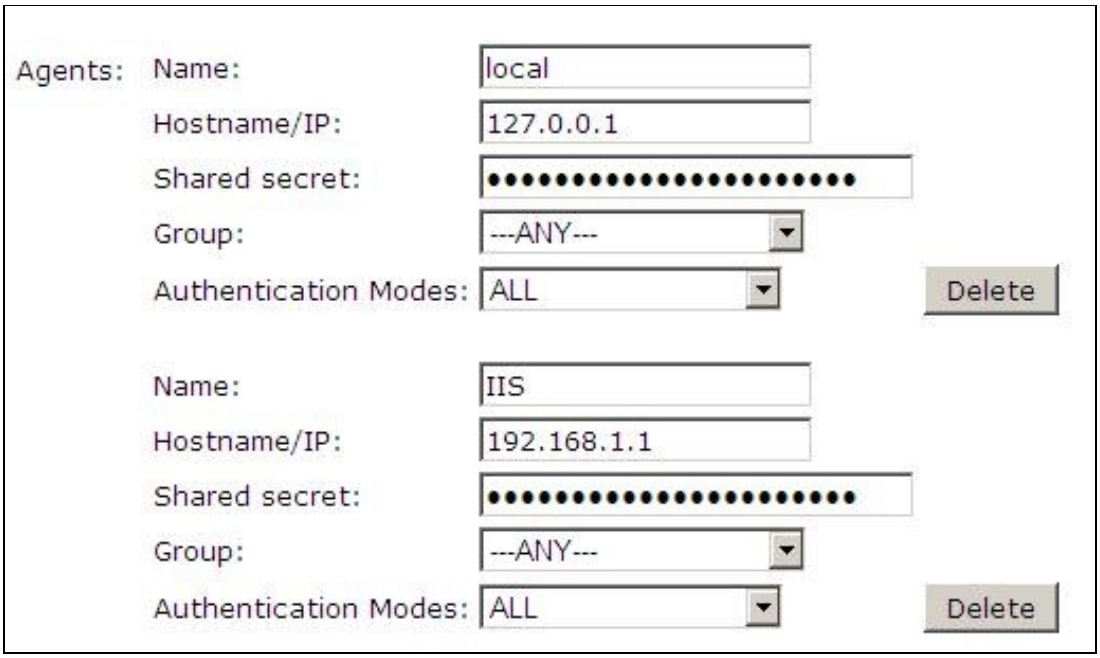
Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, when one is shown then it's classed as used and will not be re-shown, if the user makes a successful offline authentication then the number of strings will be replenished however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

Update: from version 5.4 onwards, offline is also supported for OATH tokens and for mobile app in OATH mode. This requires Sentry version 4.0.5 or later.

513 Swivel Integration Configuration

513.1 Configure a Swivel Agent

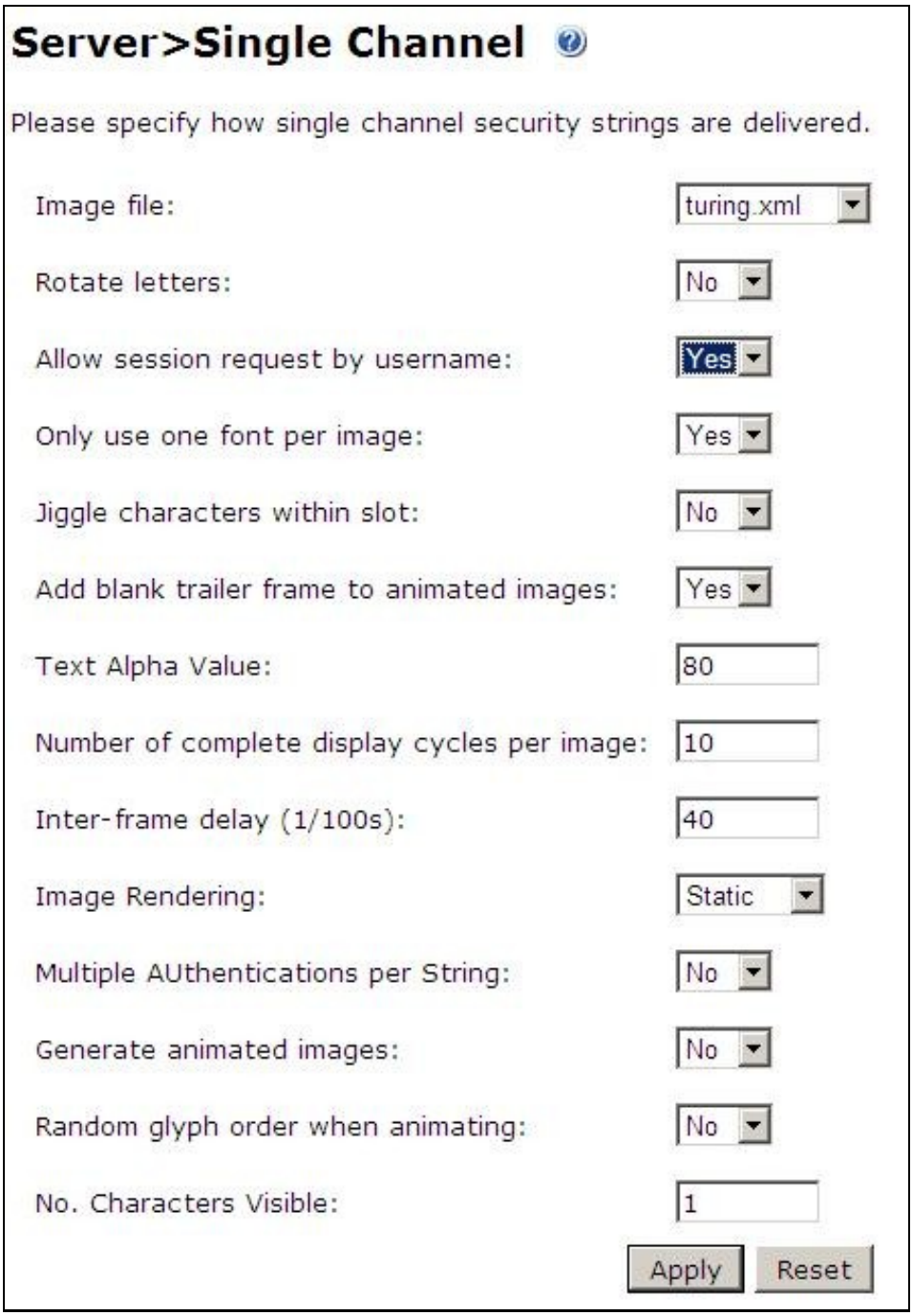
1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
4. Enter the shared secret used above on the Credential Provider.
5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail).
6. Click on Apply to save changes.



Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

513.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel.
2. Ensure ?Allow session request by username? is set to YES.

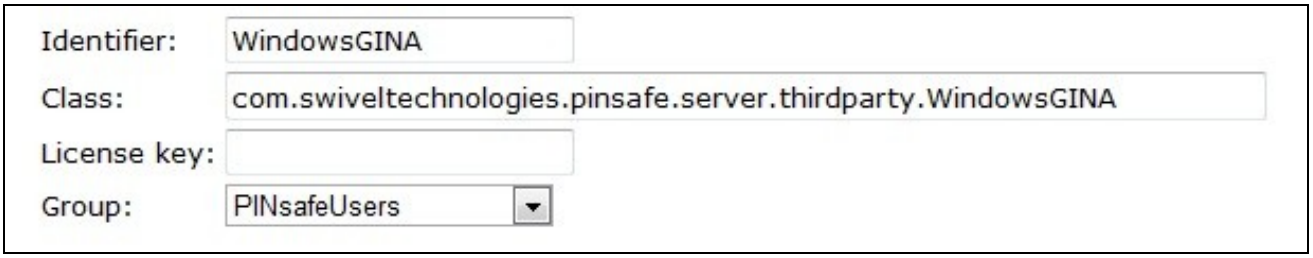


513.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured).

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA).
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. For the License Key, leave this empty as it is not required.
5. For the Group select a group of users (Note: the option Any cannot be selected).
6. Click Apply to save the settings.

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.

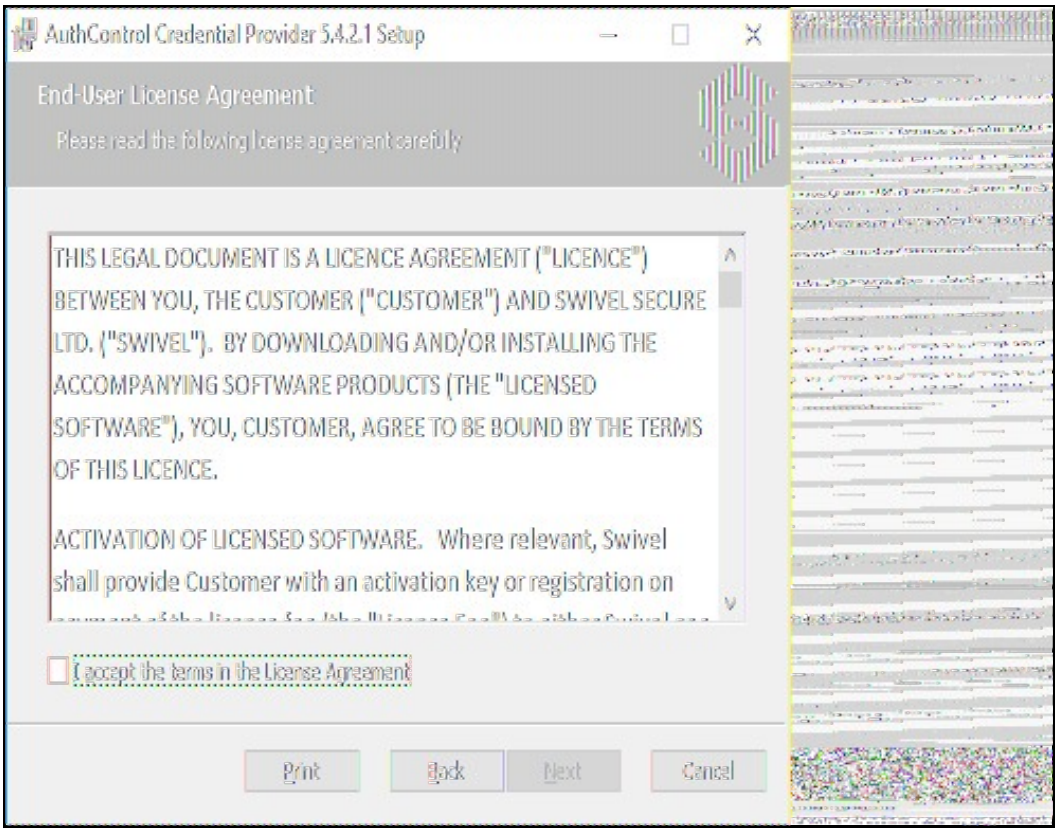


514 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

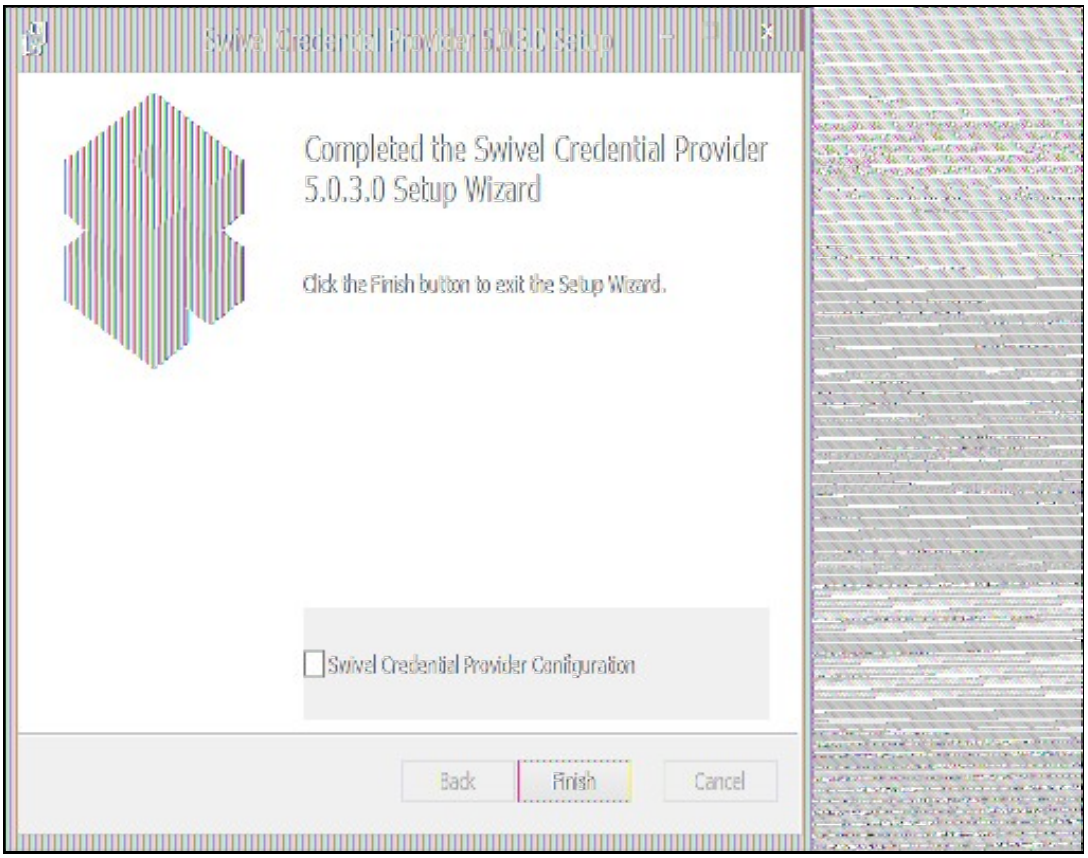
The first page is the licence agreement:



Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

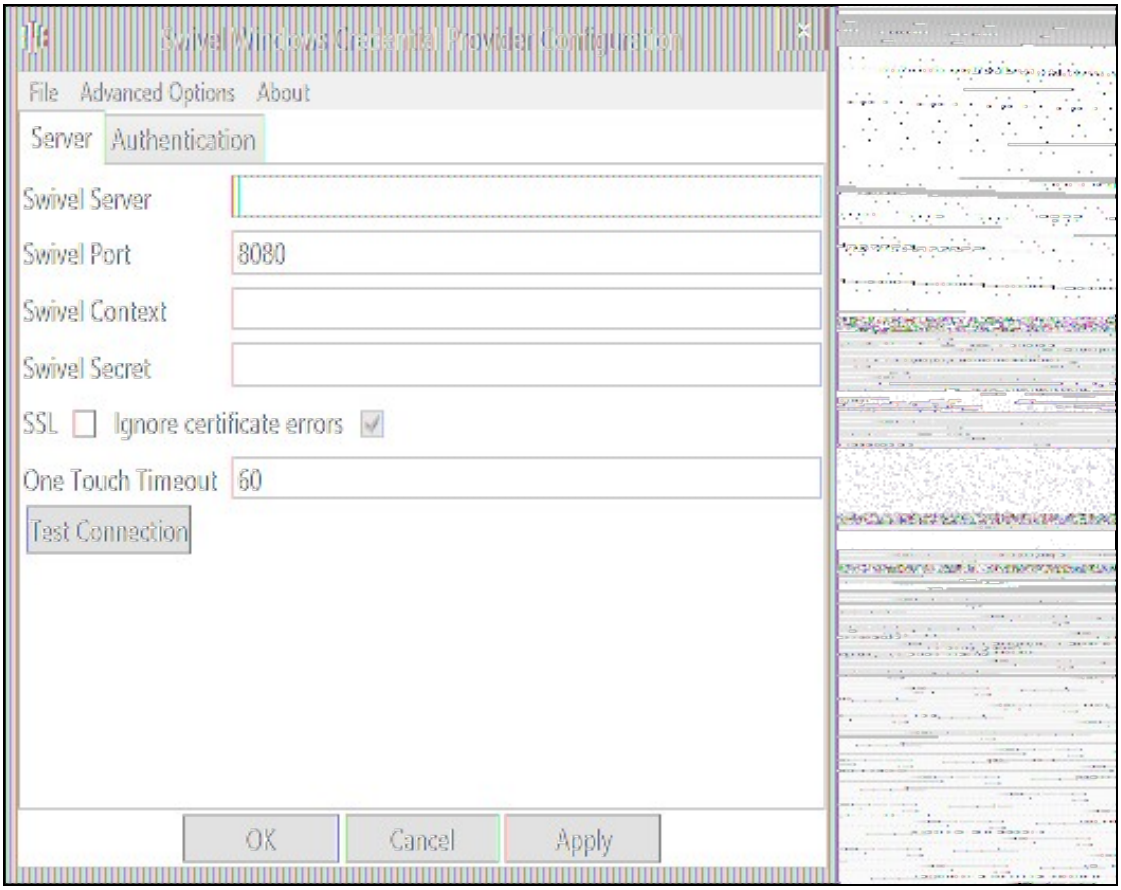
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



514.1 Windows Swivel Credential Provider configuration

514.1.1 Server



Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

Context: The Swivel virtual or hardware appliance or server installation instance.

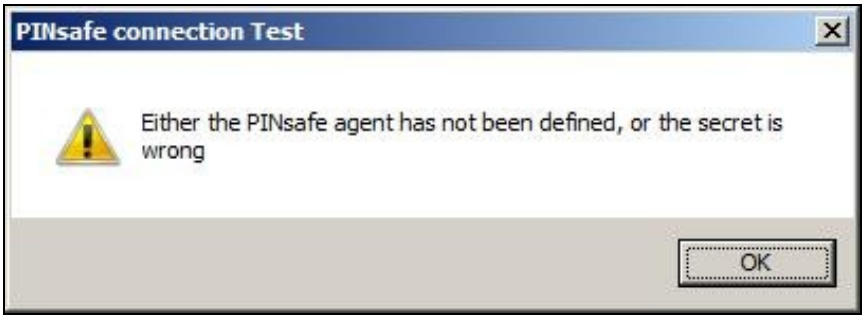
Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

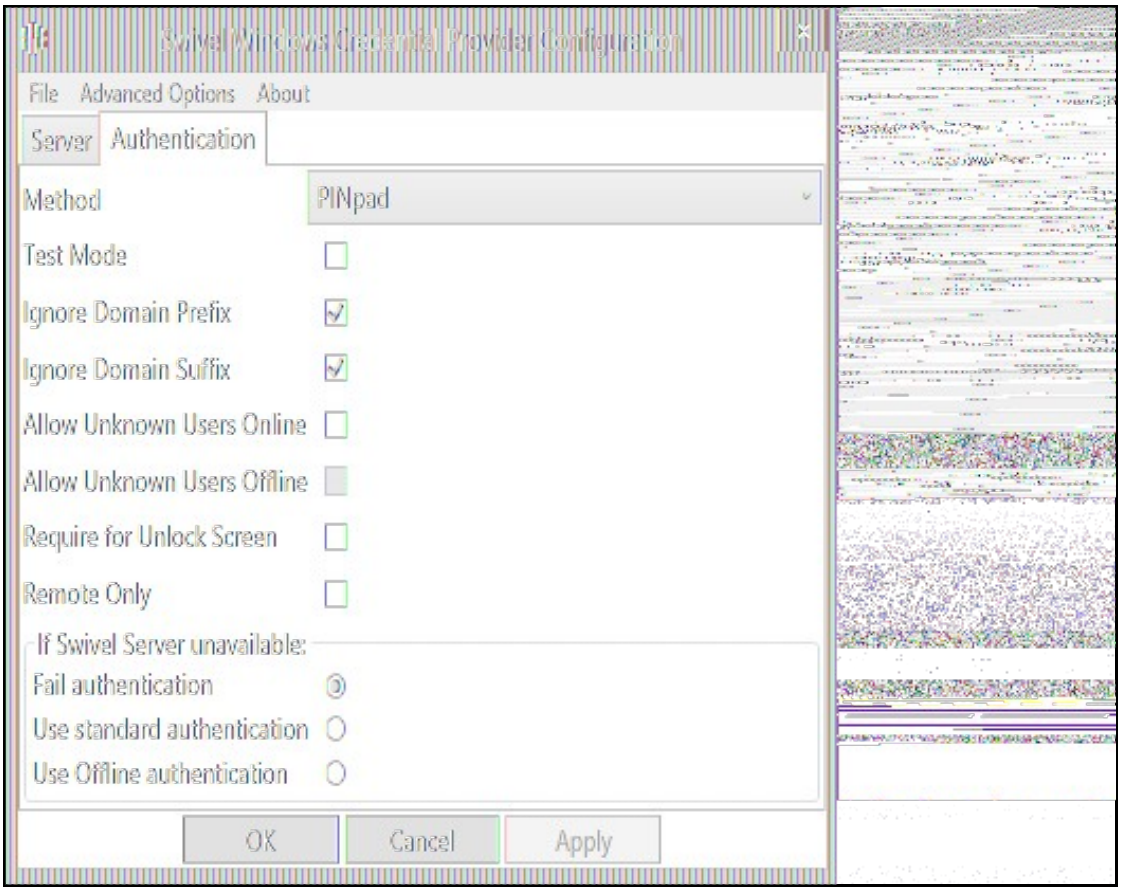
Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**

Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



514.1.2 Authentication



Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

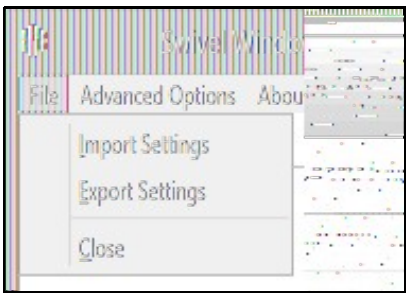
Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

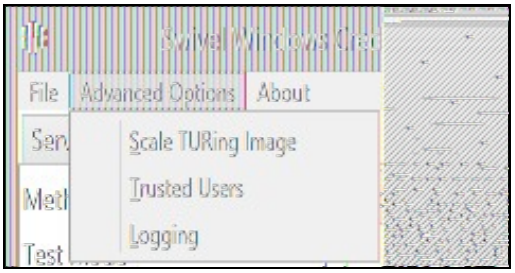
514.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

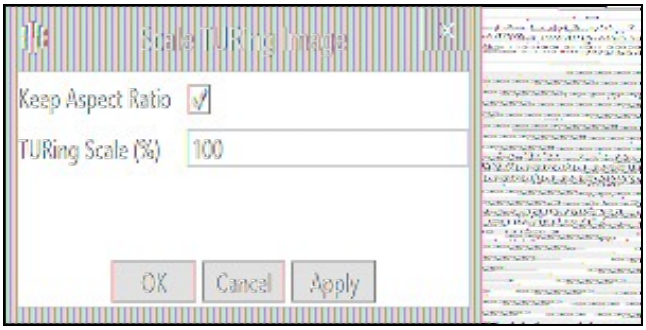
514.1.4 Advanced Options



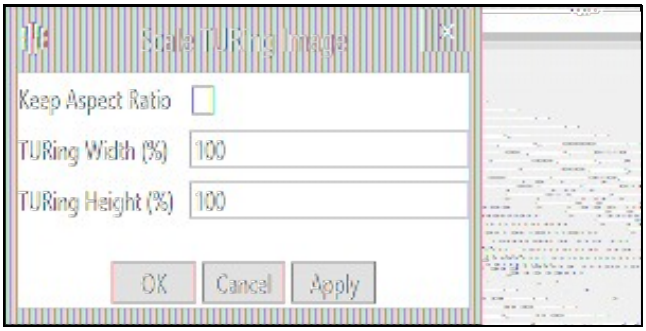
514.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

If **Keep Aspect Ratio** is selected then select the scale (%) of the TURing.

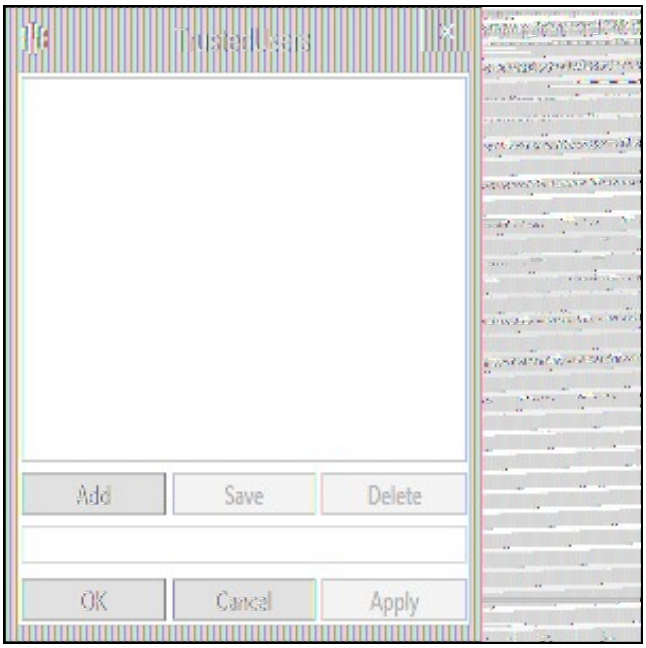


If its not selected then you can select the width and hight independently.



514.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

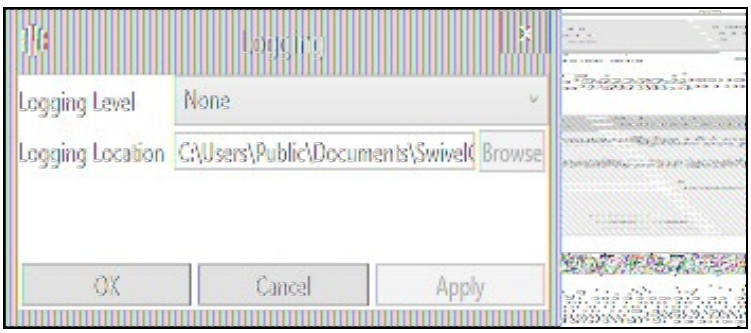
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

514.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.

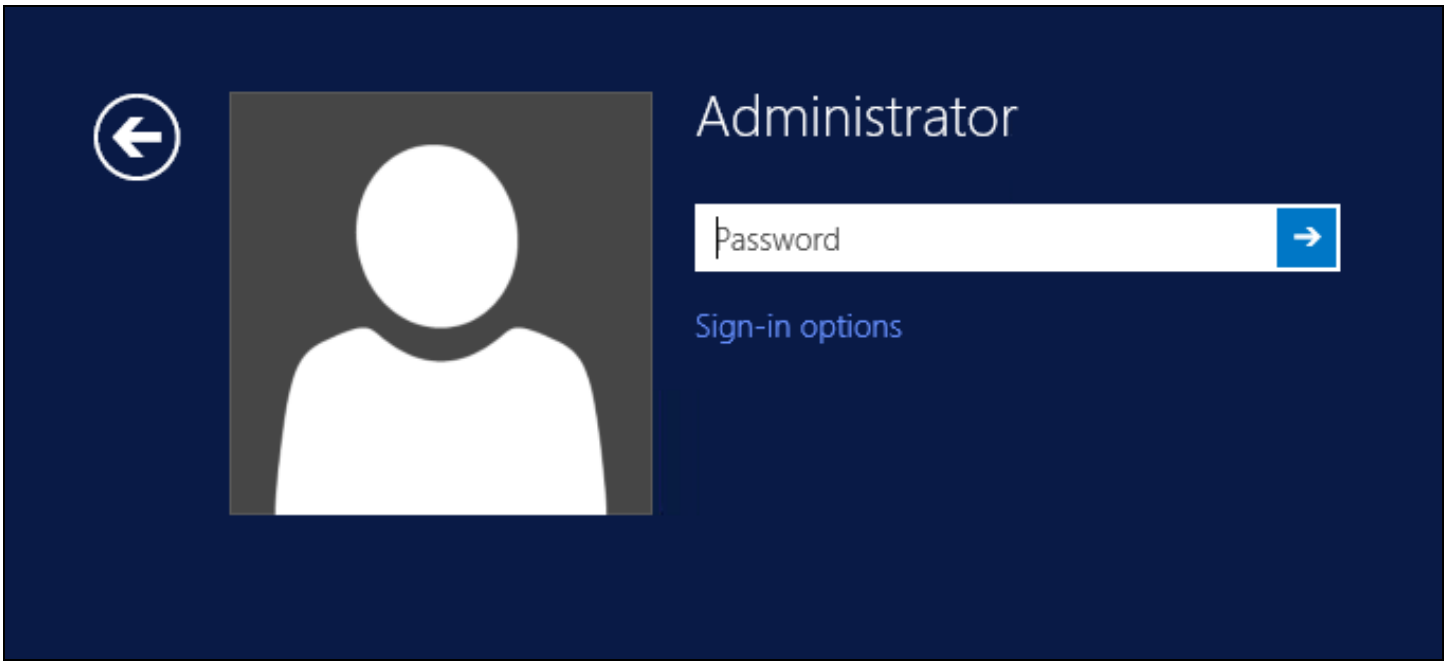


""Logging Level"" The account of message that will be logged.

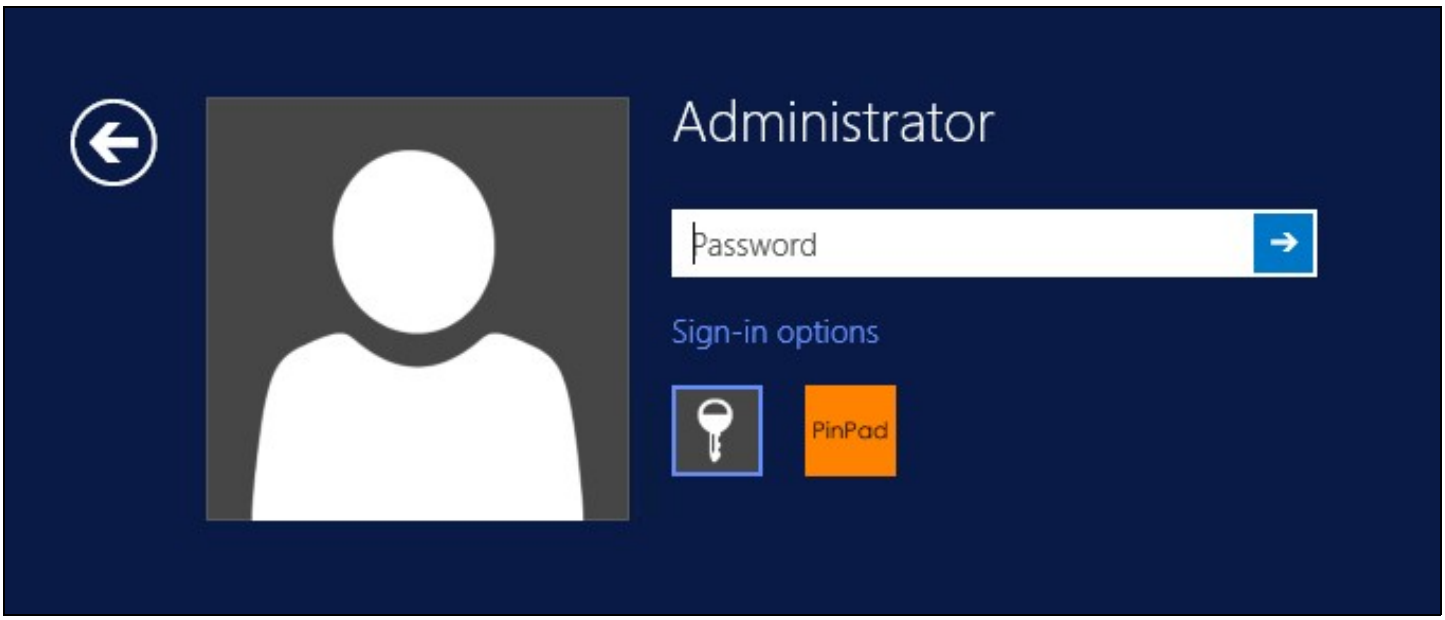
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

514.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

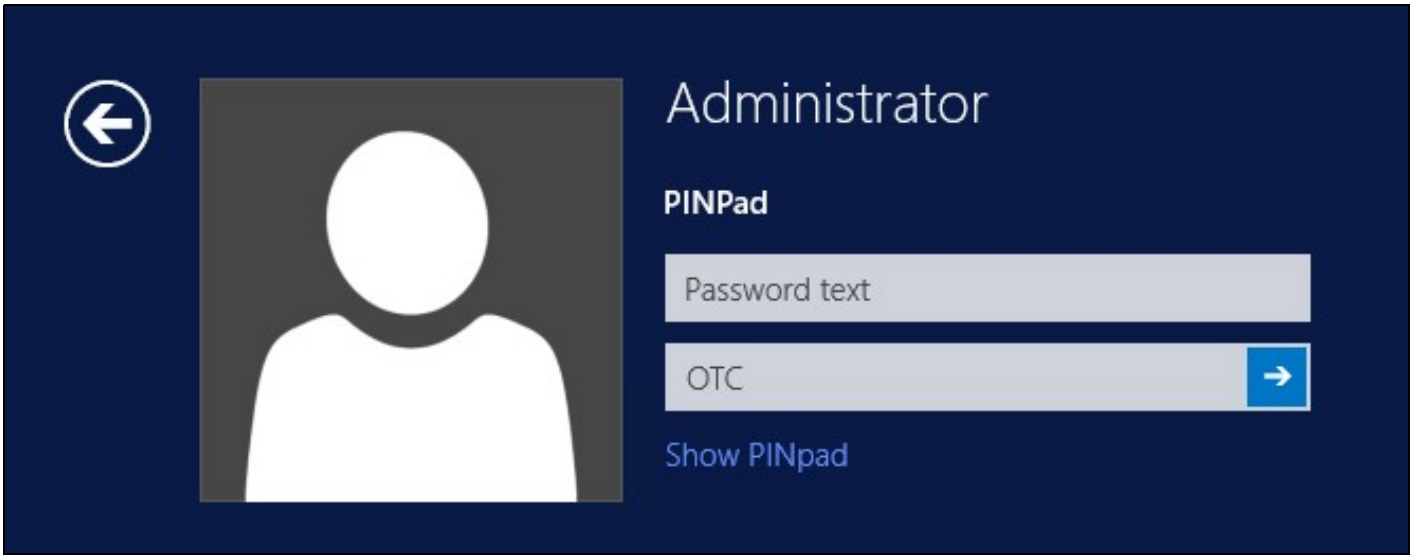
514.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

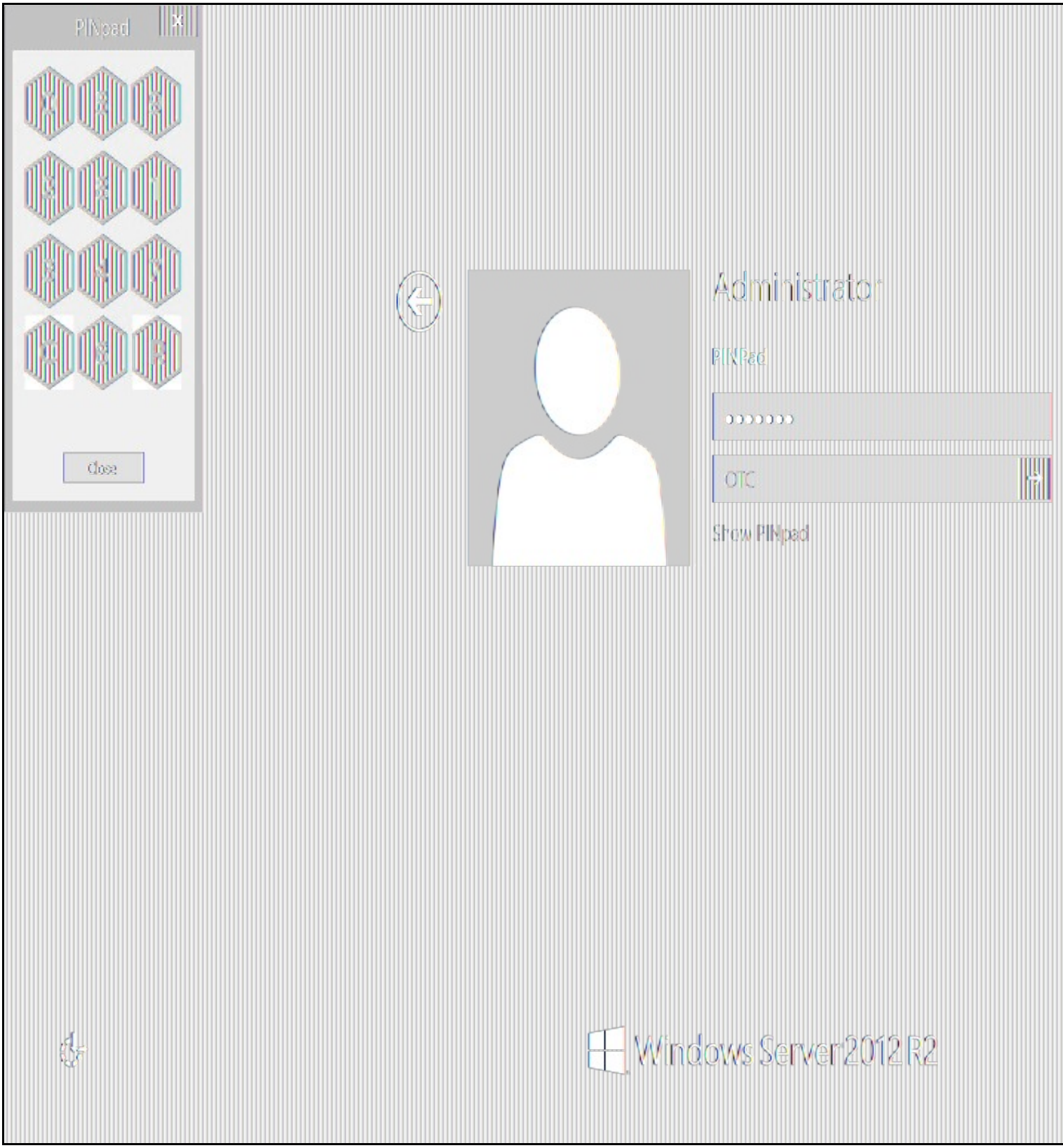
515 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*.

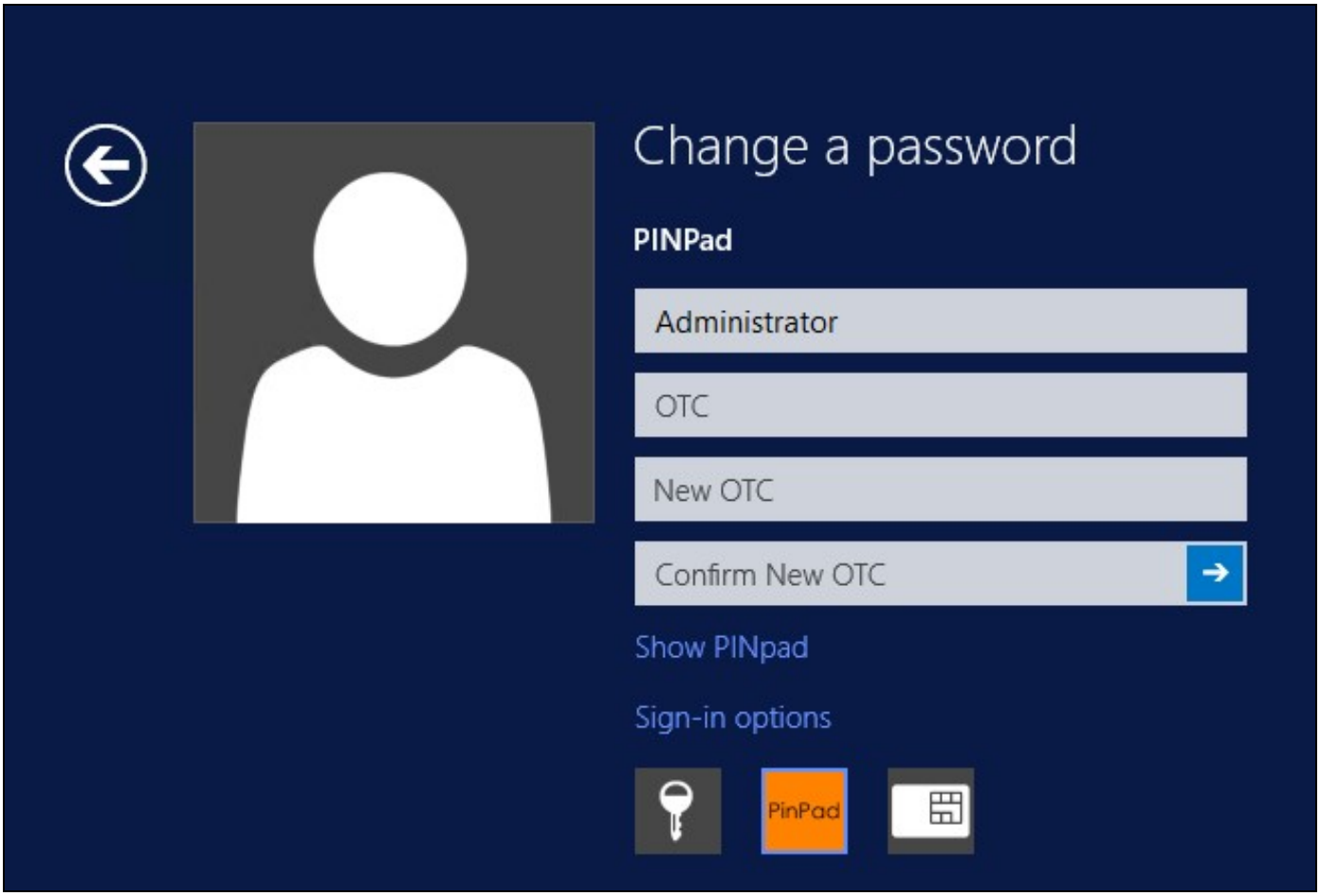
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*.

516 ChangePIN

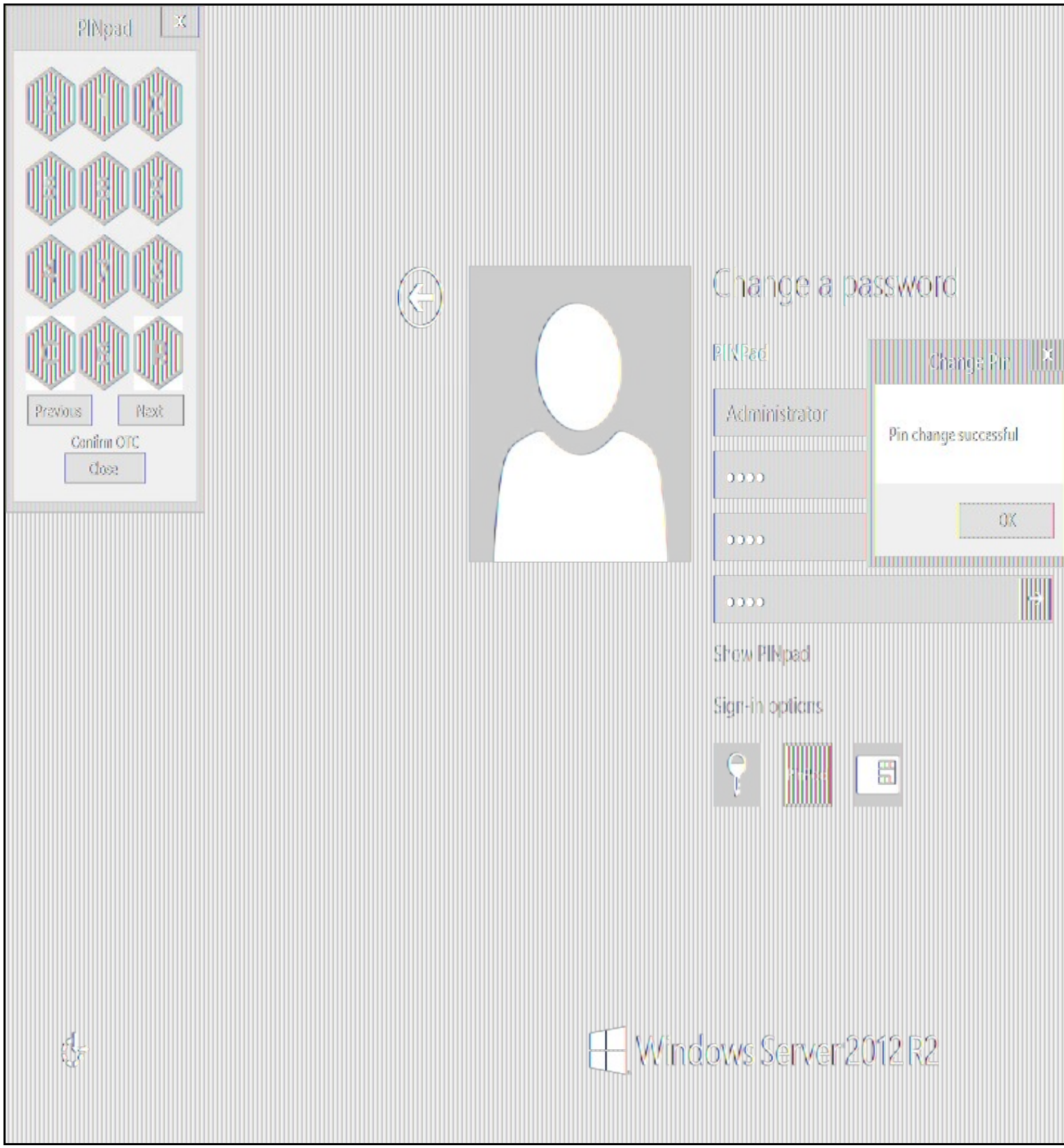
A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

517 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

517.1 Disabling the Credential Provider

If the Credential Provider needs to be disabled temporarily, use the following procedure:

If the credential provider is preventing the machine starting normally, boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Using regedit.exe, edit the following registry keys. Add a DWORD value named "disabled" to each one, set to 1. To re-enable it, you can set disabled to 0, rather than deleting the value.
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
- Uninstall the Credential Provider.
- Using regedit.exe, remove the following registry keys:
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_CLASSES_ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

518 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and request an new TURing.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

519 VMware View (Horizon)

519.1 Introduction

This document describes steps to configure VMware View with Swivel as the authentication server. The solution is tested with VMware View 5.1. using RADIUS authentication protocol with SMS, Token, Mobile Phone Client, and Taskbar Authentication

The VMware View Client also functions on a number of mobile phone client devices including iPhone, iPad and Android.

519.2 Credits

Swivel would like to thank the following contributors to this document:

Barry Coombs (VMware vExpert) of Computerworld Systems LTD www.computerworld.co.uk

519.3 Prerequisites

VMware View 5.1 or higher

VMware View documentation

Swivel 3.x,

519.4 Baseline

VMware View 5.1

Swivel 3.8

519.5 Architecture

The VMware View makes authentication requests against the Swivel server by RADIUS.

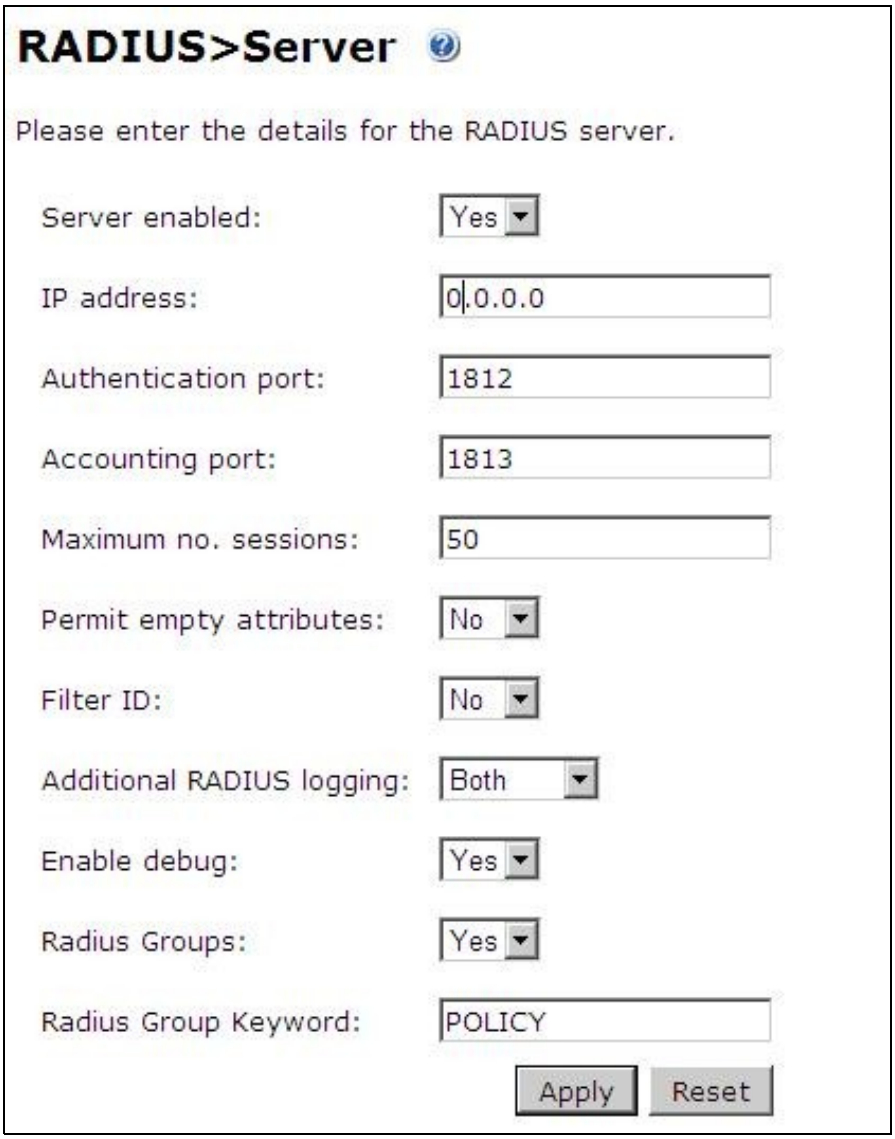
519.6 Swivel Configuration

519.6.1 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 to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

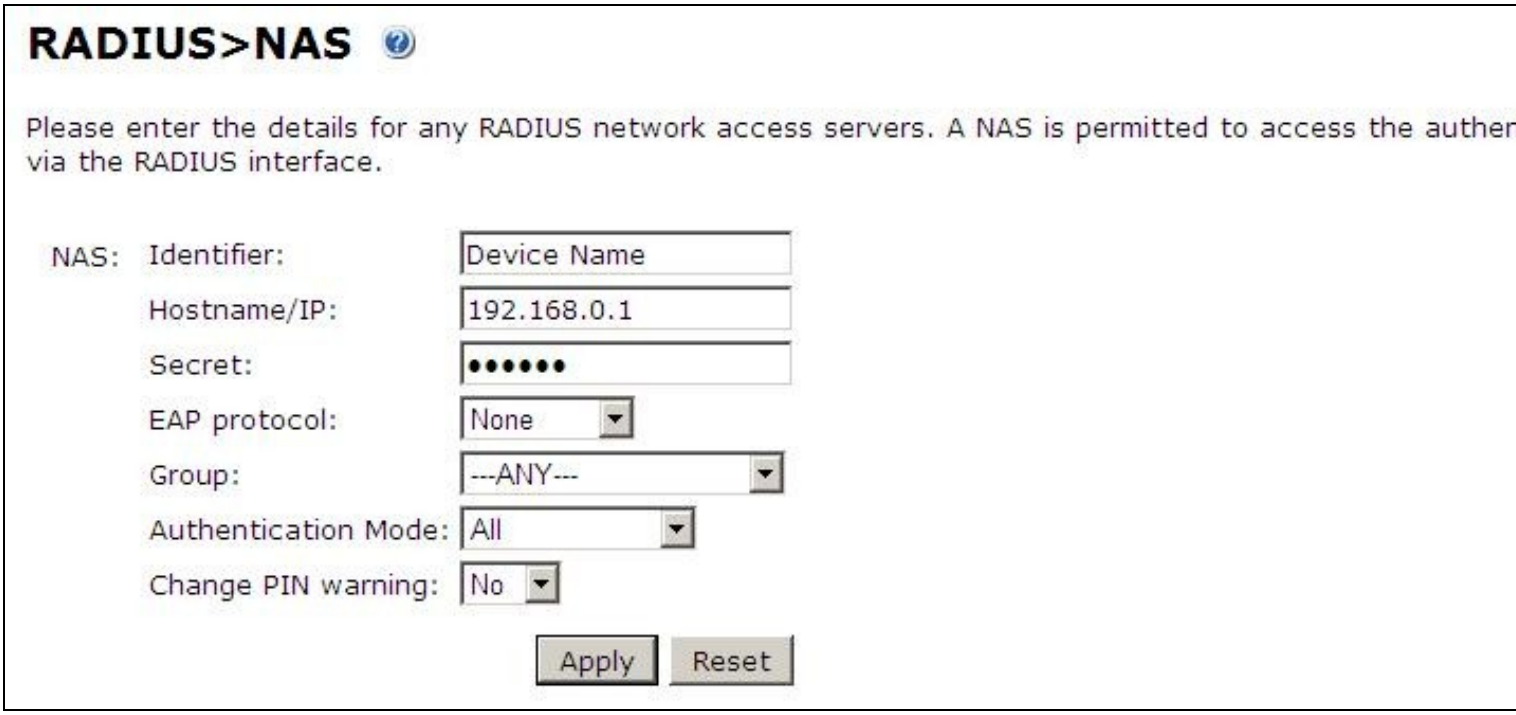
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

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



519.6.2 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 NAS Client. The IP address has been set to the IP of the NAS Client, and the secret ?secret? assigned that will be used on both the Swivel server and the NAS Client.



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.

519.6.3 Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

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

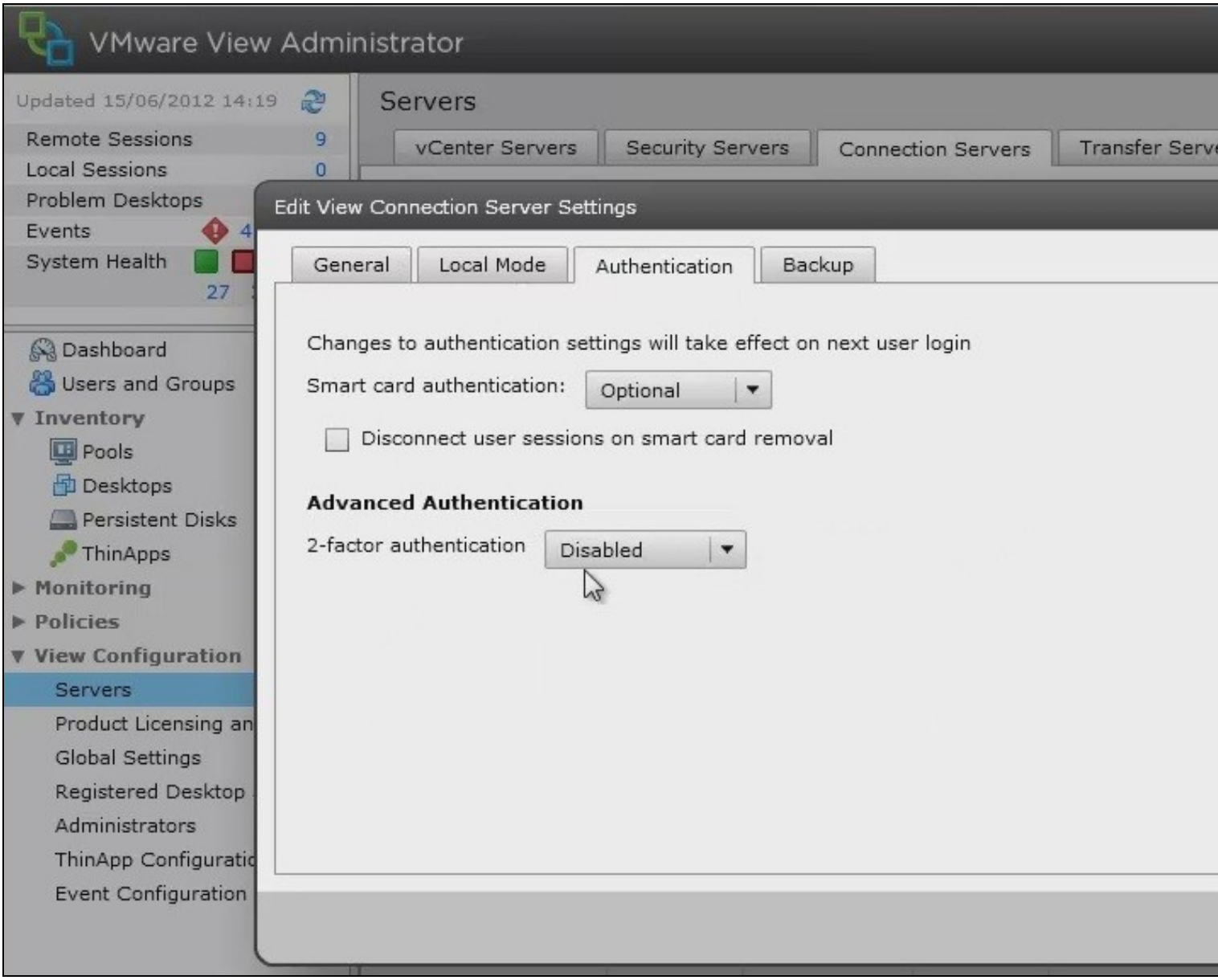
For a software only install see Software Only Installation

519.7 VMware View Configuration

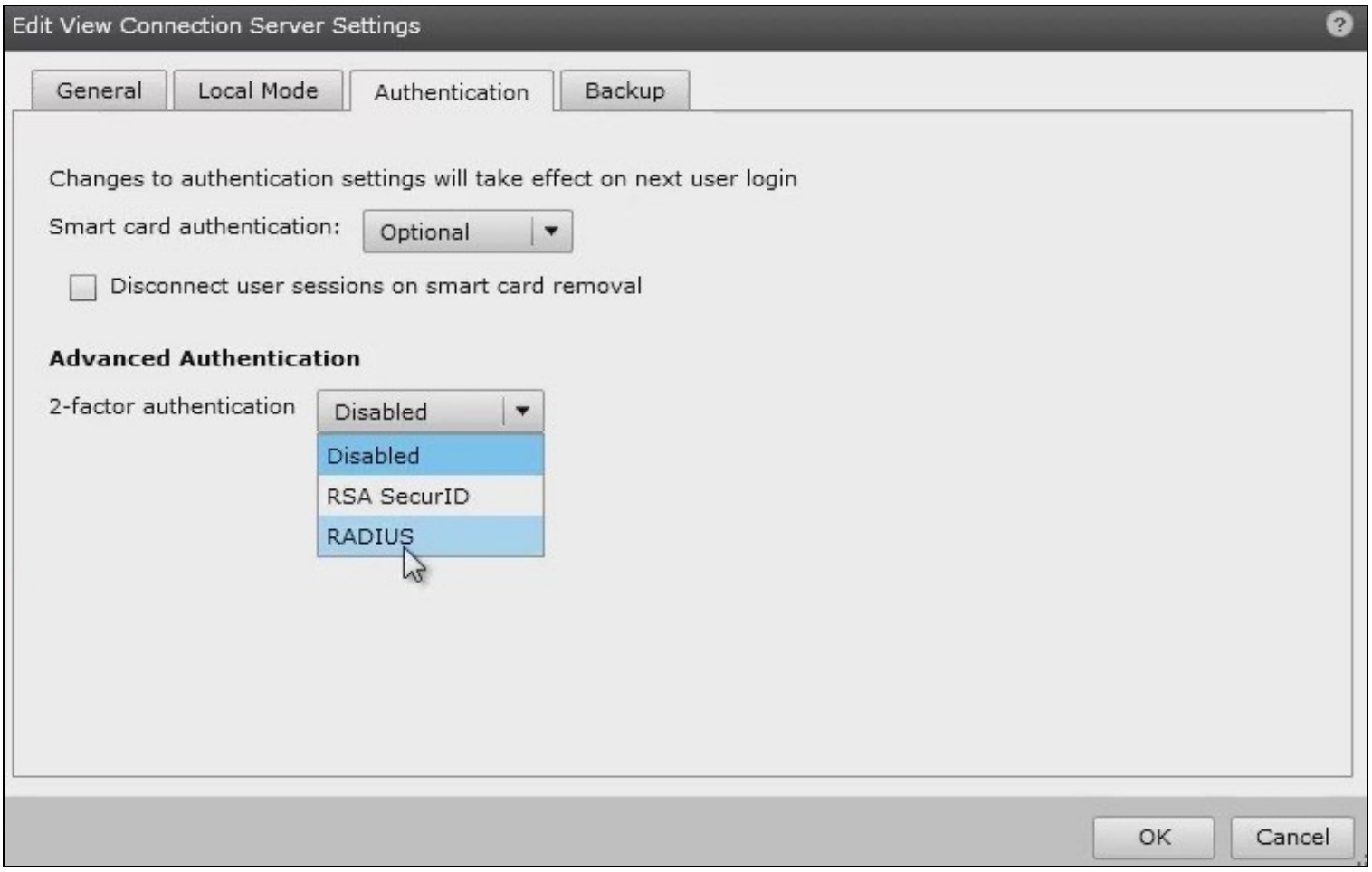
Ensure that the VMware View is fully functioning using standard authentication, then start the Swivel integration configuration.

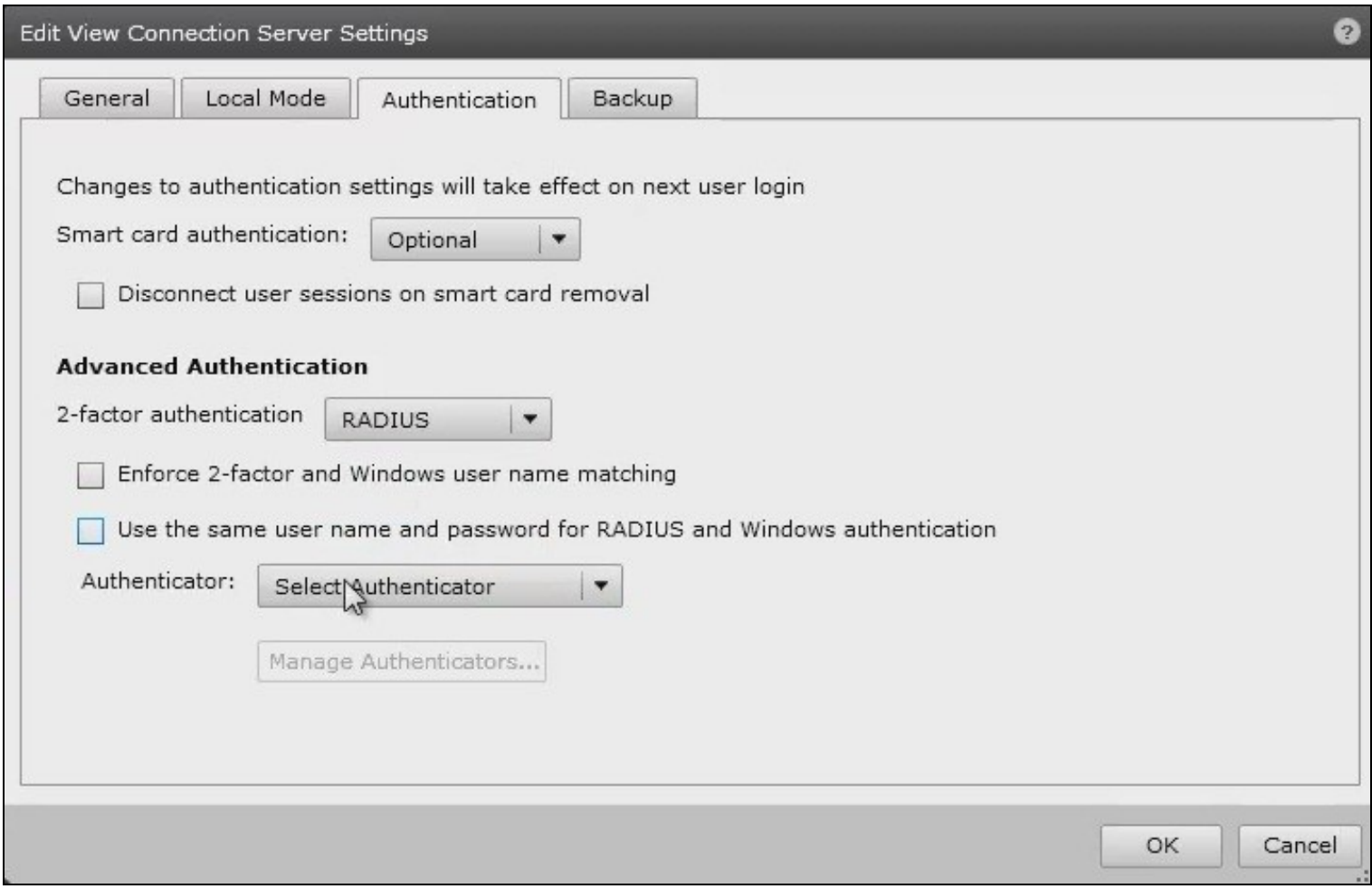
519.7.1 Create a Radius Authentication Server Group

On the VMware View Administrator select **View Configuration**, then **Servers**, select the **Connection Servers** tab and then **Edit** to bring up the Edit View Connection Server Settings and select the **Authentication** tab.



Under Advanced Authentication choose, for 2-factor authentication, the **RADIUS** tab.


Edit View Connection Server Settings
General
Local Mode
Authentication
Backup
Changes to authentication settings will take effect on next user login
Smart card authentication:
Optional
Disconnect user sessions on smart card removal
Advanced Authentication
2-factor authentication
Disabled
Disabled
RSA SecurID
RADIUS
OK
Cancel



Under Authenticator select Create new, this opens the Add RADIUS Authenticator screen, this allows a Primary and Secondary RADIUS authentication servers to be configured, enter the following:

Label: A label shown to clients

Primary Authentication Server

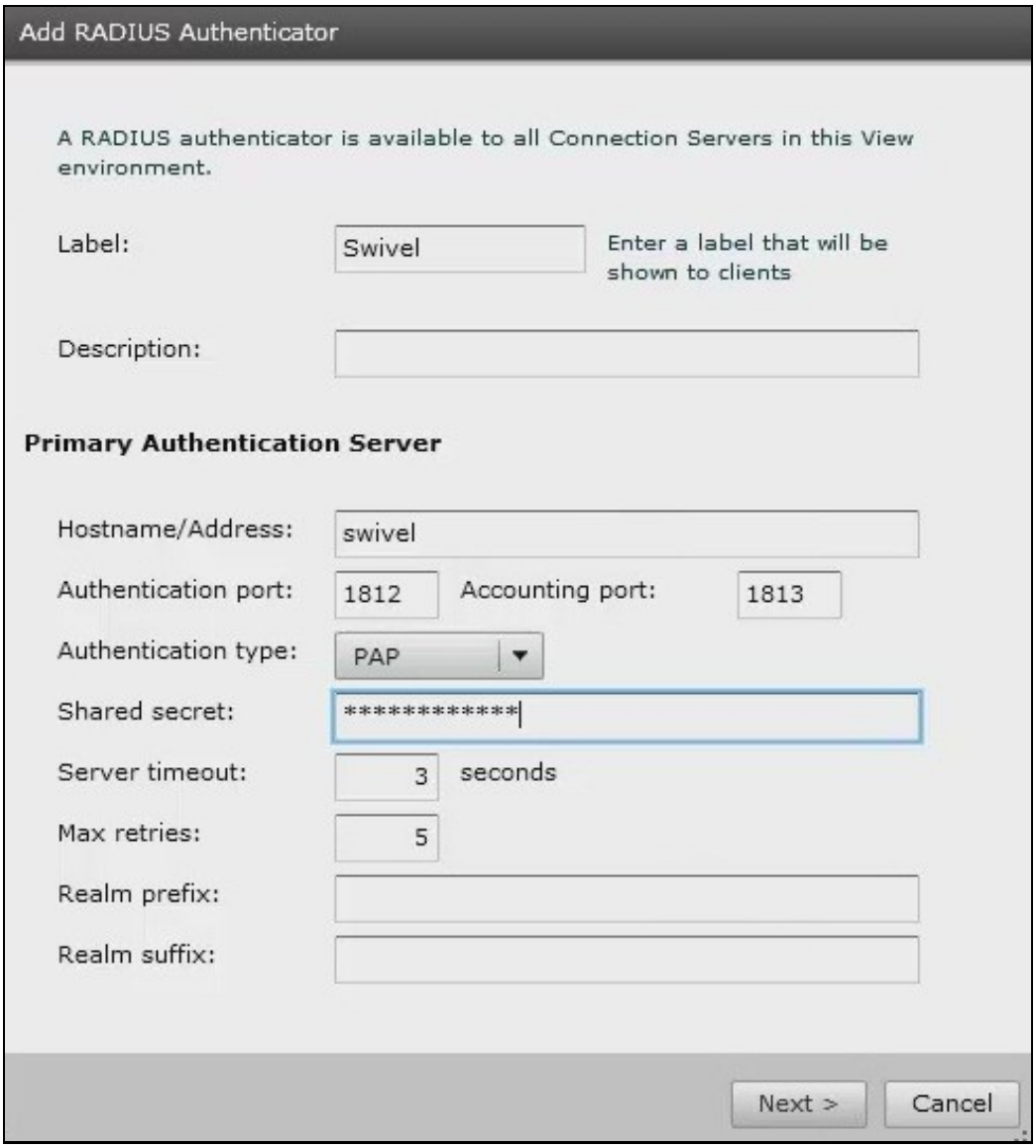
Hostname/Address: IP address of the Swivel server (This must not be a Swivel VIP for Active/Active appliances)

Authentication Type: select RADIUS authentication type, use PAP for initial setup.

Shared secret: The shared secret, the same as entered on the Swivel server

Domain Prefix: Allows a domain name to be added, and to be sent to the Swivel server in the format domain\username

Domain Suffix: Allows a domain name to be added, and to be sent to the Swivel server in the format username@domain



Clicking OK returns to to the Authentication tab.

It is possible to specify here the option **Enforce 2-factor and Windows name matching** so that the AD username is used for the Swivel authentication.

519.8 Additional Configuration Options

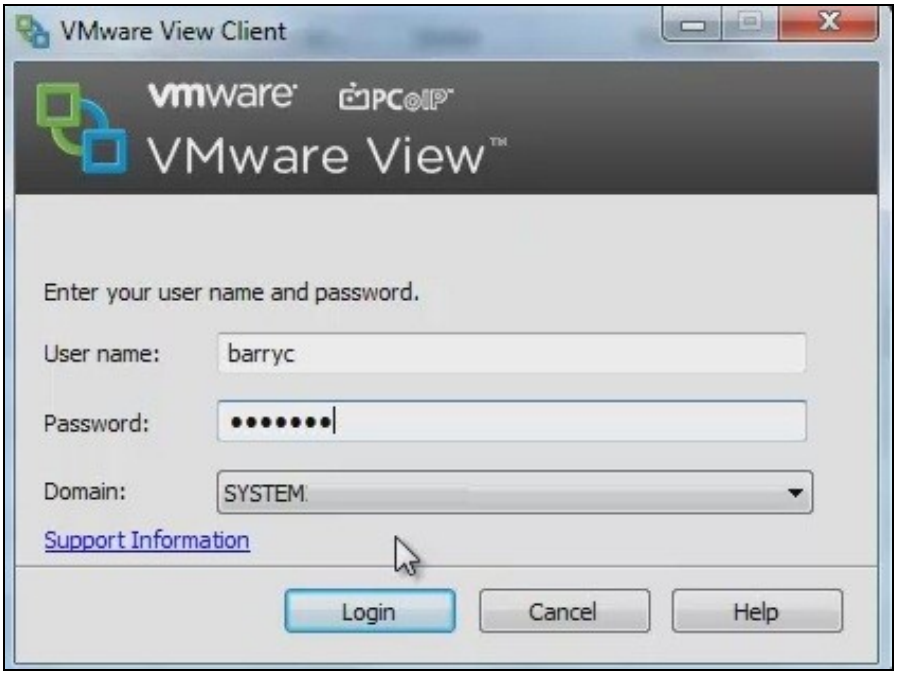
519.8.1 Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide. Using the option to allow the Same Username and Password for Windows and RADIUS authentication allows the AD username and password to be entered once and then challenge for a One Time Code.

519.9 Testing

The VMware View client will display fields for Username and Password. The username should be entered followed by the Swivel One Time Code in the Passcode field.

If the OTC is correct the user will be prompted for a AD Password



519.10 Troubleshooting

Check the Swivel logs for RADIUS requests. RADIUS requests should be seen even if the OTC is incorrect.

519.11 Known Issues and Limitations

None

519.12 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

520 WatchGuard Firebox

521 Overview

For the Watchguard Firebox integration refer to the following document WatchGuard Firebox Swivel Integration:

522 Windows Credential Provider

523 Introduction

Swivel Secure AuthControl Desktop (formerly Windows Credential Provider) is used in the desktop operating systems Windows 8, 10 and 11 and the server operating system Windows Server 2012 and 2019. For integration with Windows Vista and 7 and Server 2008, use version 5.3 or later, or see Microsoft Windows Credential Provider Integration (Legacy OS).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using TURing.
- **PINpad** Lets the user sign into windows by using PINpad.
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.
- **Push** for Windows 8 and Server 2012 R2 onwards.
- **Fingerprint** (From v5.4.2 onwards and requires AuthControl Sentry v4.0.5) Lets the user sign into windows using Biometric Fingerprint.

523.1 Downloads

Latest Release Versions:

Swivel AuthControl Desktop 64-bit version MSI 5.7.42.1 NOTE: this is the latest release. Documentation has not yet been updated to reflect the changes in this version.

Swivel AuthControl Desktop 64-bit version MSI 5.7.31.1

Swivel AuthControl Desktop 64-bit version executable 5.7.31.1

Swivel AuthControl Desktop 32-bit version MSI 5.7.31.1

If you have difficulties downloading these files, please contact teamsupport@swivelsecure.com for an alternative method.

The two versions install identical products. The difference is that the executable will copy the current settings from version 5.x and reapply them after installation. The MSI will always overwrite the settings with either blank settings or the contents of acd.xml or scps.xml if provided (see later). As of 5.7, old settings are no longer removed on upgrade, but that only applies to the version that is uninstalled, so upgrading to 5.7 from an earlier version will still remove the old settings.

Settings from versions earlier than 5 cannot be imported automatically on upgrade: you will need to export the settings, uninstall the version 4 credential provider and then install the new version and import the settings.

Important: the Credential Provider requires Microsoft Visual Studio C++ redistributable to work. Recent operating systems already include this, but it will need to be installed on older operating systems if it has not already been installed. You can retrieve it from here. If you have already installed the credential provider, it is not necessary to uninstall it before installing the redistributable.

Note that this article has not yet been fully updated to reflect the changes in version 5.6 or 5.7. See below for release notes.

Older Versions:

Swivel AuthControl Desktop 64-bit version executable 5.6.10.1

NOTE: we discovered a bug in version 5.6.3.1 whereby the stored secret fails to be decrypted at unpredictable times. We therefore recommend using the following version, 5.6.10.1, which stores the secret unencrypted. This version also fixes a problem with Push authentication, which did not work in 5.6.3.1 or 5.6.9.1.

Swivel AuthControl Desktop 64-bit version MSI 5.6.10.1

Swivel AuthControl Desktop 64-bit version executable 5.5.11.1

Swivel AuthControl Desktop 64-bit version MSI 5.5.11.1

Swivel AuthControl Credential Provider 64 bit version 5.4.4.2

Swivel AuthControl Credential Provider 64 bit version 5.4.3.2

Swivel AuthControl Credential Provider 64 bit version 5.4.2.1

Swivel AuthControl Credential Provider 64 bit version 5.3.1.5

Swivel Windows Credential Provider 64 bit version 5.1.1

Swivel Windows Credential Provider 64 bits version 5.3.0.1

523.2 Swivel Credential Provider FAQ

```
Q). Does the Credential provider support offline authentication?
A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is a

Q). Do all users have to authenticate using Swivel?
A). Swivel has the option to Allow Unknown Users. Users known to Swivel will be prompted for authentication in this instance. There is also a

Q). Is it possible to define users who do not have Swivel authentication?
A). Yes either by the Allow Unknown Users for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password?
A). Yes, there is an option to log in without the AD password, but you must previously have logged in with the AD password.
```

524 Prerequisites

Swivel version 3.11.3 or later. For password caching, version 4.0.4 or later is required.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1), 10 and 11 or Windows Server 2012 (including R2) and Windows Server 2019. Version 5.3 and later have backward support for Windows Vista or later, and Windows Server 2008 or later.

Microsoft.Net Framework version 4.5.

AuthControl Windows Credential Provider 64-bit - see above for links.

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

525 Baseline

Swivel 3.11.3

Windows 8, 10, 11 Server 2012 R2, Server 2019.

526 Installation

526.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Desktop Windows versions the computer must be restarted.
- On Windows Server versions the Administration account can be signed out rather than doing a full restart.

526.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file either "acd.xml" or "scps.xml". Alternatively, you can export the settings as encrypted and name the file "acd.enc". Note that for the file to be imported automatically you must not specify a password (the default password will be used).
2. Copy this file and the installation file onto the new computer. They must be in the same location (for example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

NOTE: in version 5.6.9.1 and later builds, the configuration file can be named "acd.xml" instead of "scps.xml". The latter will be used by preference if both files exist.

Alternatively, you can build an pre-configured installer executable. Please contact Swivel Secure support to get the necessary build script.

1. Extract the files from the zip link above into a folder
2. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file "acd_in.xml".
3. Replace acd_in.xml in the extracted folder with your customised one
4. Compile the executable using ACDInstall.nsi with Nullsoft installation system. If you don't have a copy of Nullsoft, it can be downloaded from here.

527 Release Notes

527.1 AuthControl Desktop 5.7

527.1.1 New Features

527.1.1.1 Generate offline strings outside ACD

The credential manager application allows you to authenticate to Sentry and to download offline security strings. These strings can then be exported to another machine and used there to authenticate users offline

527.1.1.2 All displayed text is customisable

The configuration program allows you to customise the text displayed in the Windows credential. Additionally, you can copy the customised text to the same folder as the ACD installer and it will be imported to the target machine on installation. Currently, only one set of strings is possible per installation, but it is hoped in the future to support multiple languages.

527.1.1.3 Proxy for Sentry connections

You can optionally specify an HTTP proxy for connecting to the Sentry server.

527.1.1.4 Enhancements to Import and Export Settings

Version 5.6 introduced encrypted settings files using a password. Version 5.7 expands on this by allowing for a fixed password, used automatically if encryption is selected but no password is given. Automatic import of settings on installation works with encrypted settings, provided the fixed password is used for encryption. Automatic import of settings will look for the following file names, in this order:

- scps.xml (previously the only name that worked)
- acd.xml
- scps.enc ? assumes the settings are encrypted using the default password
- acd.enc ? as above

Note that the MSI installation no longer deletes the old settings on uninstallation. However, this only applies to upgrading FROM 5.7 or reinstalling. Since the settings are deleted by uninstalling the old version, upgrading from a version older than 5.7 will still remove the old settings.

527.1.1.5 Change PIN for locked users

Previously, if a user attempted to log in and the account was locked due to PIN expiry, authentication would fail. Now, the PIN change screen is shown. It should be noted that in order to change a PIN when the account is locked, you need Sentry version 4.1.4 or later.

527.1.1.6 Optionally, OTC field is not shown initially for Other User

It is possible to specify that the OTC field is not initially shown for the ?Other User? credential. This is the credential that is shown with an empty username field. In the case where users unknown to Sentry are permitted to log on without MFA, it might be preferable not to show the OTC field, in case it is not required. If a user logs in with username and password, and it is subsequently discovered that an OTC is required, the login form is redisplayed with the OTC field.

527.1.1.7 Offline OATH works with On Demand credential

Previously, offline OATH only worked if the authentication method was set to ?Other Two-Factor? (and that not reliably ? see bug fixes). Now it also works with ?On Demand?.

527.1.2 Bug Fixes / Improvements

527.1.2.1 Error messages displayed for PIN change errors

Previously, if an error occurred in the PIN change screen, no message was displayed. The screen was simply redisplayed with no additional information. Now, an error is displayed on the screen indicating why the PIN change failed.

527.1.2.2 Improved configuration for Single Sign-On

In 5.6 and earlier, the use of Single Sign-On (SSO) to check if MFA is required was indicated simply by providing a port and context for SSO. This could result in the settings being entered when they were not really needed, just because the fields are there. Version 5.7 shows a check-box to indicate that SSO is active. Activating SSO will display a pop-up dialog requesting the SSO settings, which includes a host name as well as port and context, so the SSO server does not have to be the same as the Sentry Core.

527.1.2.3 Push authentication not working

Version 5.6 (prior to 5.6.10.1) did not support Push authentication due to incompatible changes in the code. Version 5.7 now supports Push correctly.

527.1.2.4 Offline OATH not working

Version 5.6 did not always work for OATH if the token details were stored locally. This was due to an error in the encryption code that affected several features. This has now been corrected.

527.1.2.5 Fixed problems with Secret not encrypting/decrypting on occasions

This problem was caused by the same encryption issue as the previous one. As a workaround, versions 5.6.9.1 and 5.6.10.1 were released with the secret being stored unencrypted, as it was in version 5.5 and earlier. Now that the encryption issue has been resolved, the secret is once again stored in encrypted format, although the encryption is not backward-compatible with 5.6, so copying the secret registry entry from 5.6 to 5.7 will not work. Exporting and importing will work, provided the secret is not encrypted in the export file.

527.1.2.6 Allow unknown users online

It was discovered that version 5.6 did not correctly handle the situation where users were not known to Sentry but could authenticate with password only. This has now been fixed.

528 Architecture

Swivel is installed as a Windows Credential Provider. When a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

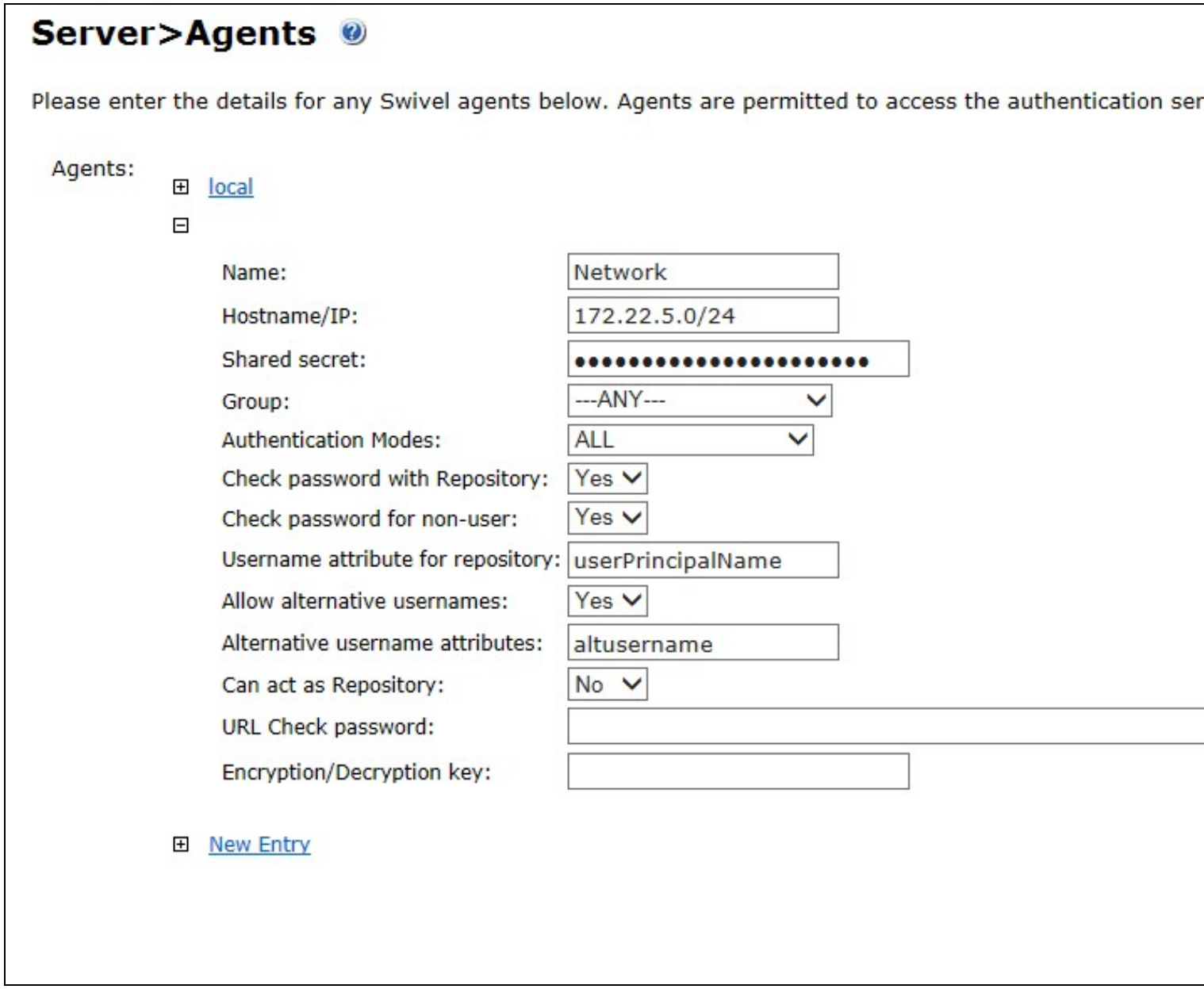
528.1 Offline Authentication

Swivel allows offline authentication using single channel or OATH, but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication: when one is shown then it's classed as used and will not be re-shown. If the user makes a successful offline authentication then the number of strings will be replenished: however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled. The exception is that OATH authentication is also supported offline, provided the user has previously authenticated online using the same token.

529 Swivel Integration Configuration

529.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can use an individual IP address for the Credential Provider, such as 192.168.0.99, or you can specify an IP address range like 192.168.0.0/24, which means the first 24 bits, or 3 numbers, are significant or you (i.e. 192.168.0.x).
4. Enter the shared secret used above on the Credential Provider.
5. Select a group, or leave it as "Any" to allow all users to authenticate.
6. Click on Apply to save changes.

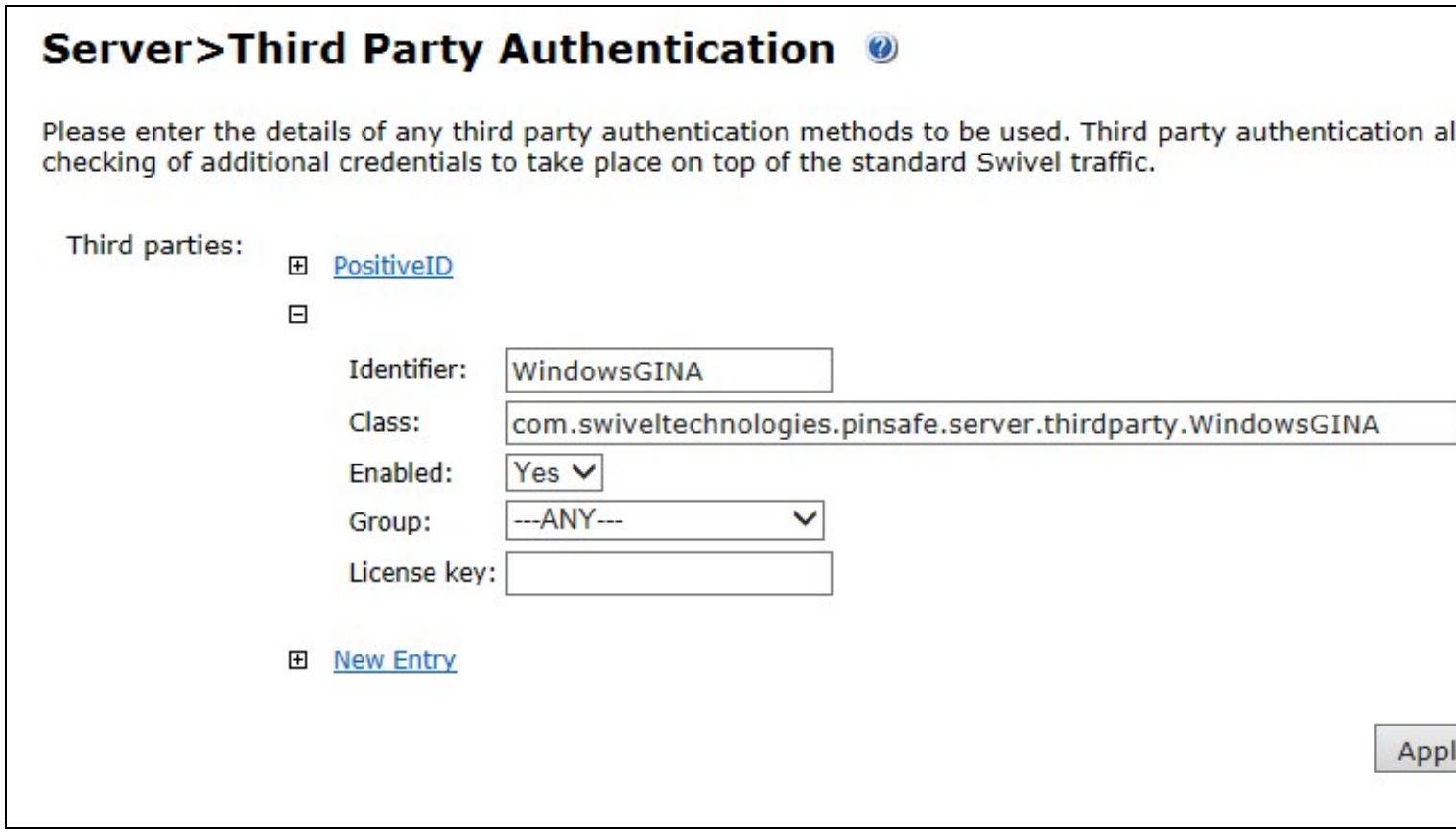


Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

529.2 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. The name must be exactly as shown. This entry should already exist, but check that the settings are as shown.

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name: WindowsGINA.
3. For the Class: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. Ensure that Enabled is set to Yes.
5. For the Group select a group of users, or Any to allow any users to authenticate using this third party.
6. For the License Key, leave this empty as it is not required.
7. Click Apply to save the settings.

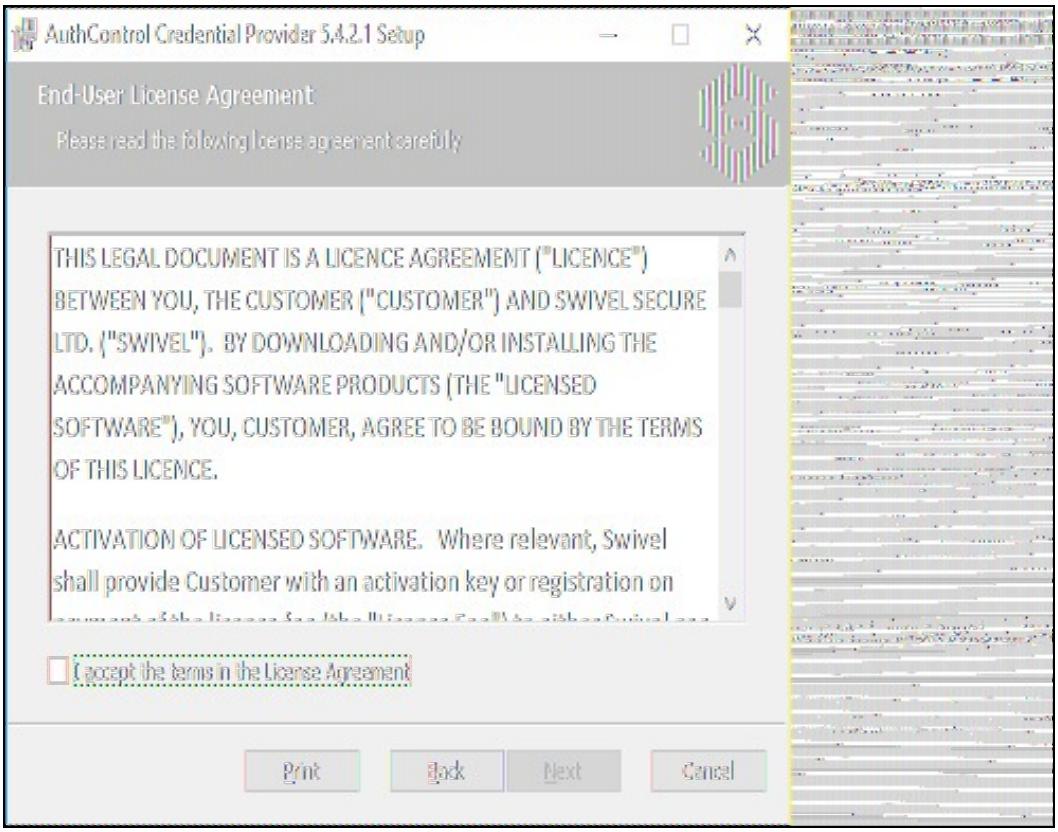

Server>Third Party Authentication
Please enter the details of any third party authentication methods to be used. Third party authentication al
checking of additional credentials to take place on top of the standard Swivel traffic.
Third parties:
PositiveID
Identifier:
WindowsGINA
Class:
com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
Enabled:
Yes
Group:
---ANY---
License key:
New Entry
Appl

530 Microsoft Windows AuthControl Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:

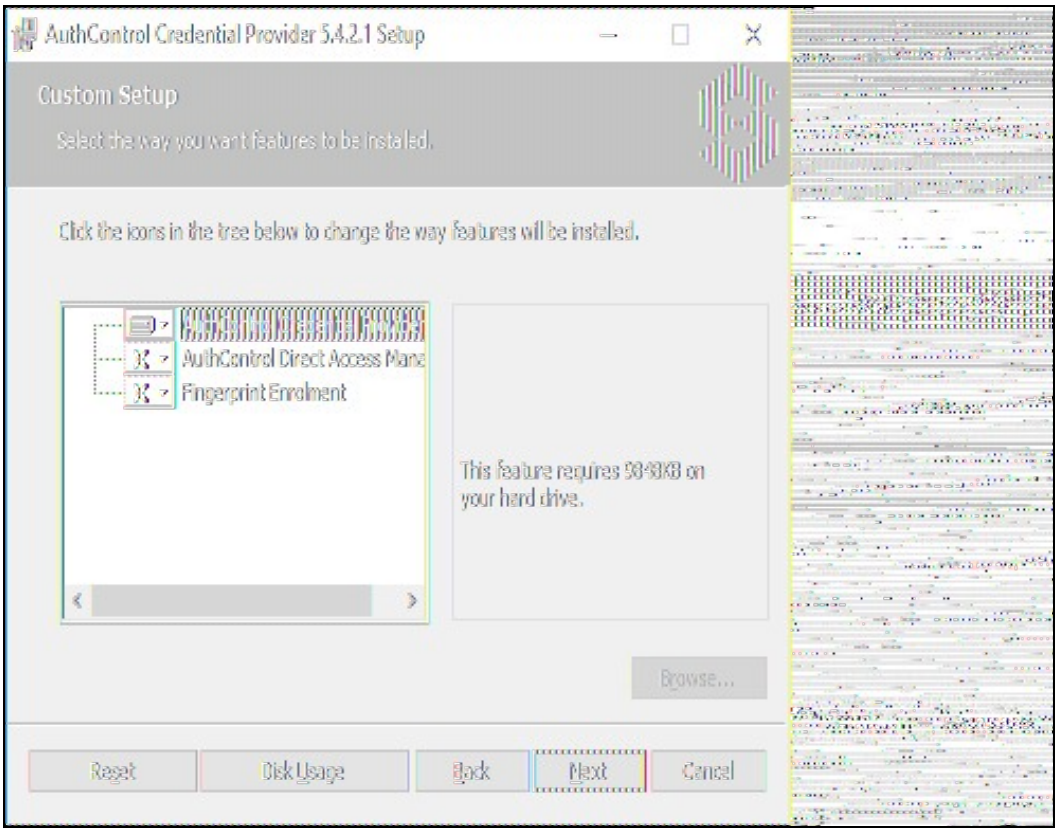


Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

Select the neccessary addons:

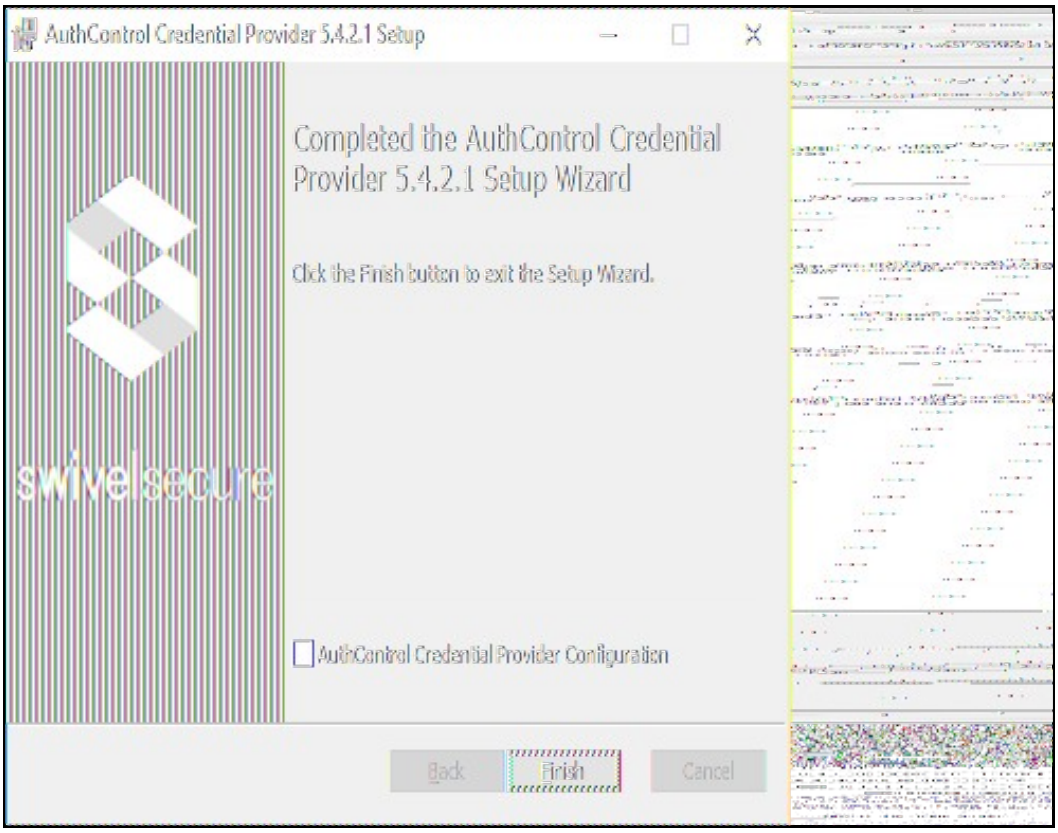
AuthControl Direct Access Manager - for integration with Direct Access

Fingerprint Enrolment - for Biometric Fingerprint enrolment and use Biometric authentication



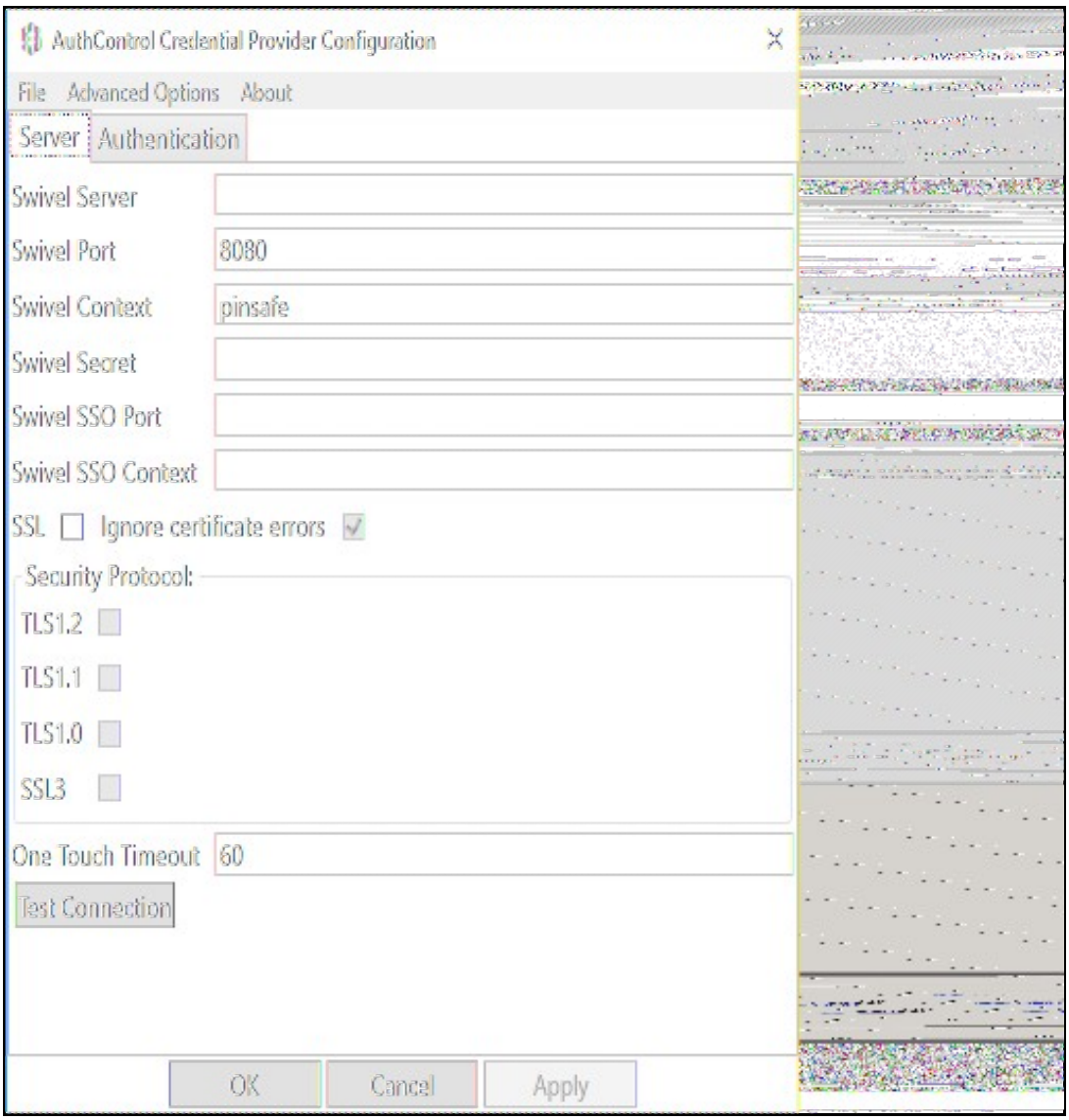
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



530.1 AuthControl Credential Provider configuration

530.1.1 Server



Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

Context: The Swivel virtual or hardware appliance or server installation instance.

Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

SSO Port: (Sentry v4.0.5 required) The AuthControl Sentry SSO port to allow RBA usage. (ex: 8443)

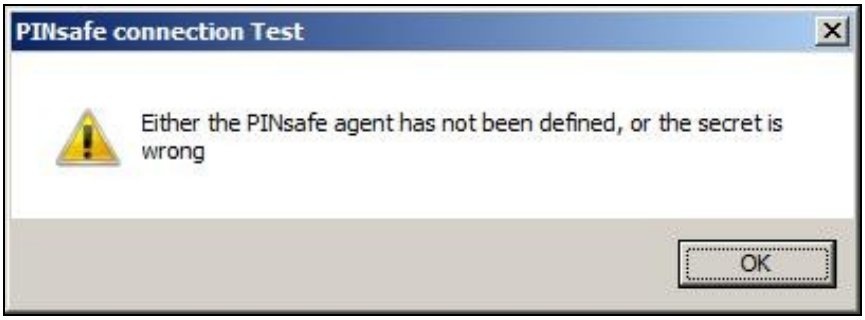
SSO Context: (Sentry v4.0.5 required) The AuthControl Sentry SSO context to allow RBA usage. (ex: sentry)

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

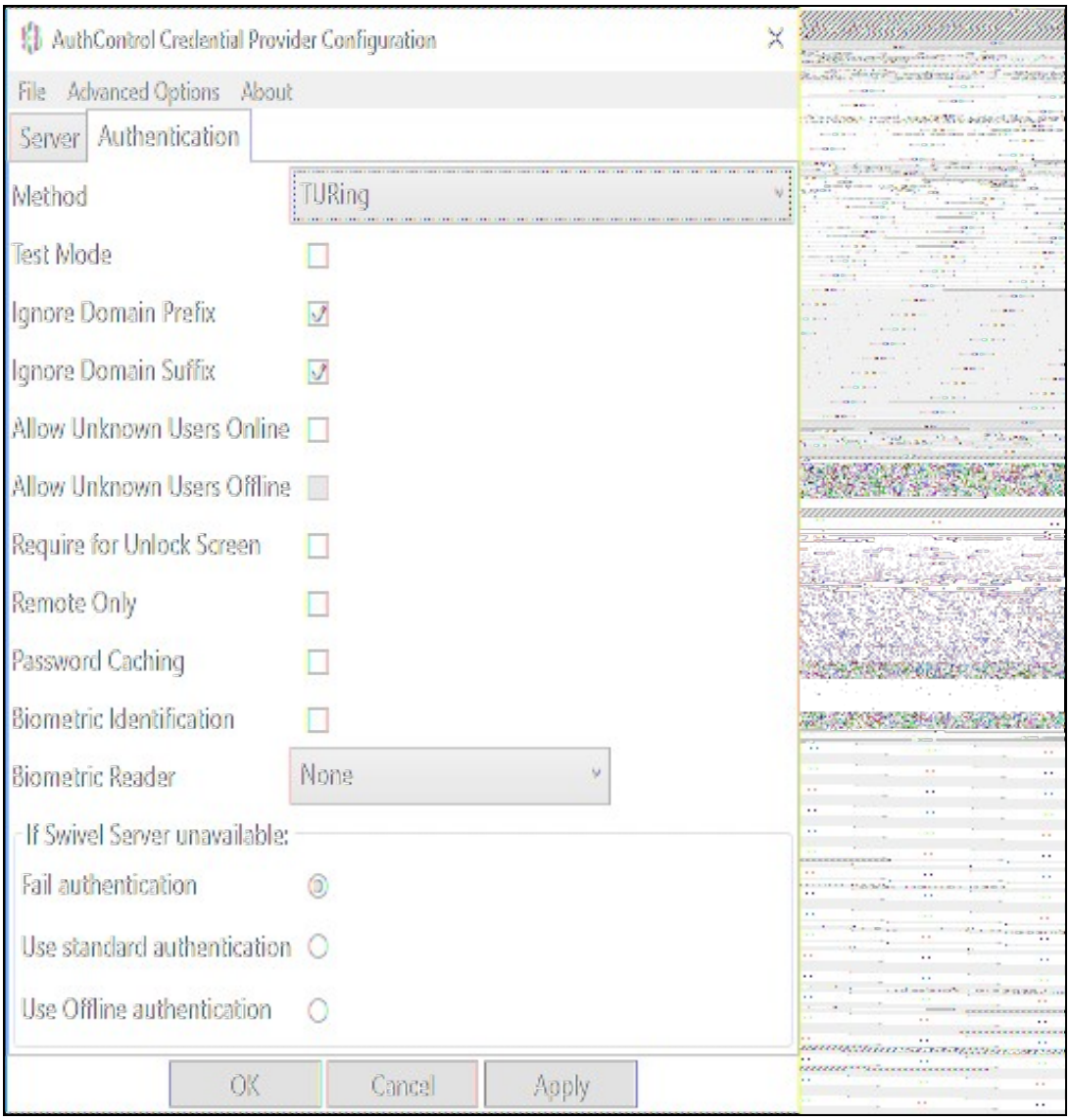
Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**

Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



530.1.2 Authentication



Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

Password Caching Allows to cache the password and login using only 2fa. This option only works online.

Biometric Identification Allows to use the Biometric Reader to obtain the username.

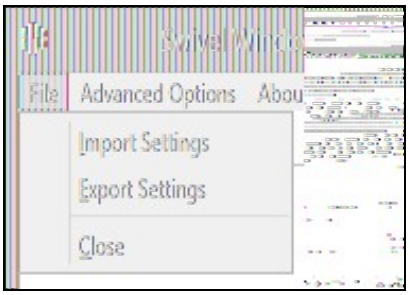
Biometric Reader The type of Biometric Reader: Nitgen or Native Laptop.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

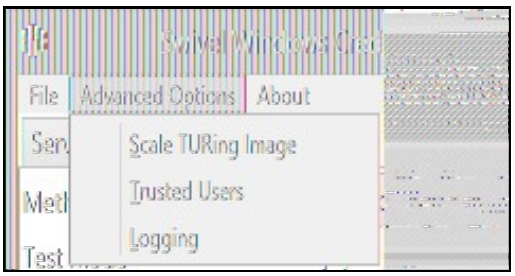
530.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

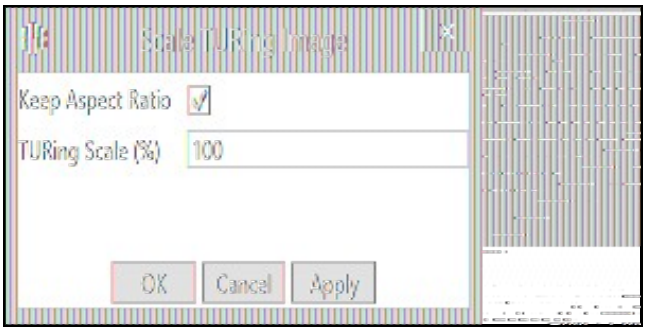
530.1.4 Advanced Options



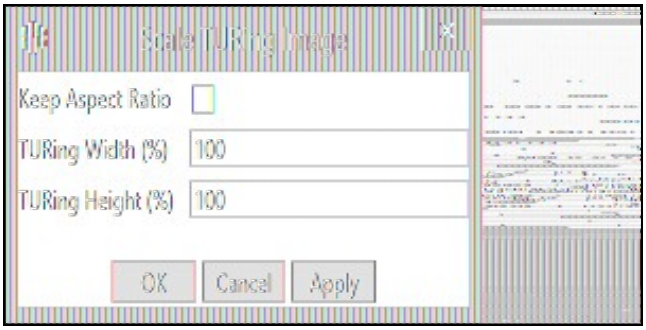
530.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

If **Keep Aspect Ratio** is selected then select the scale (%) of the TURing.

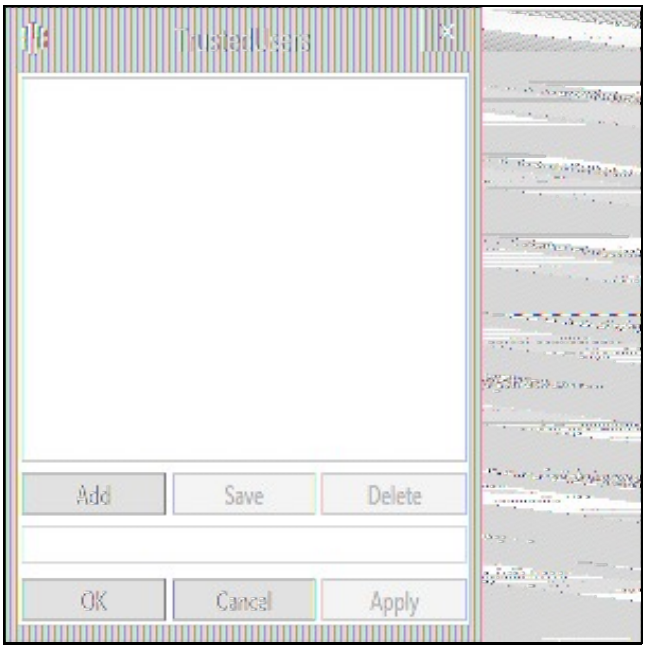


If its not selected then you can select the width and hight independently.



530.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

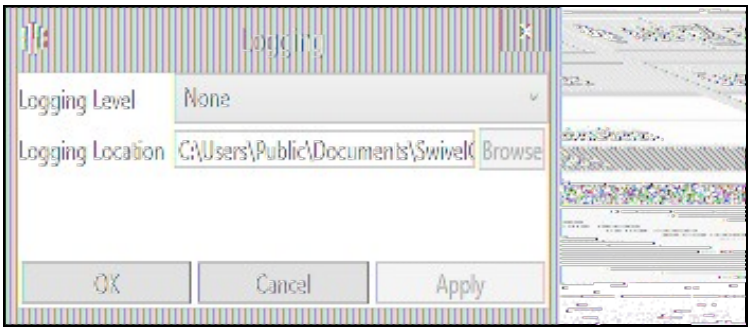
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

530.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.

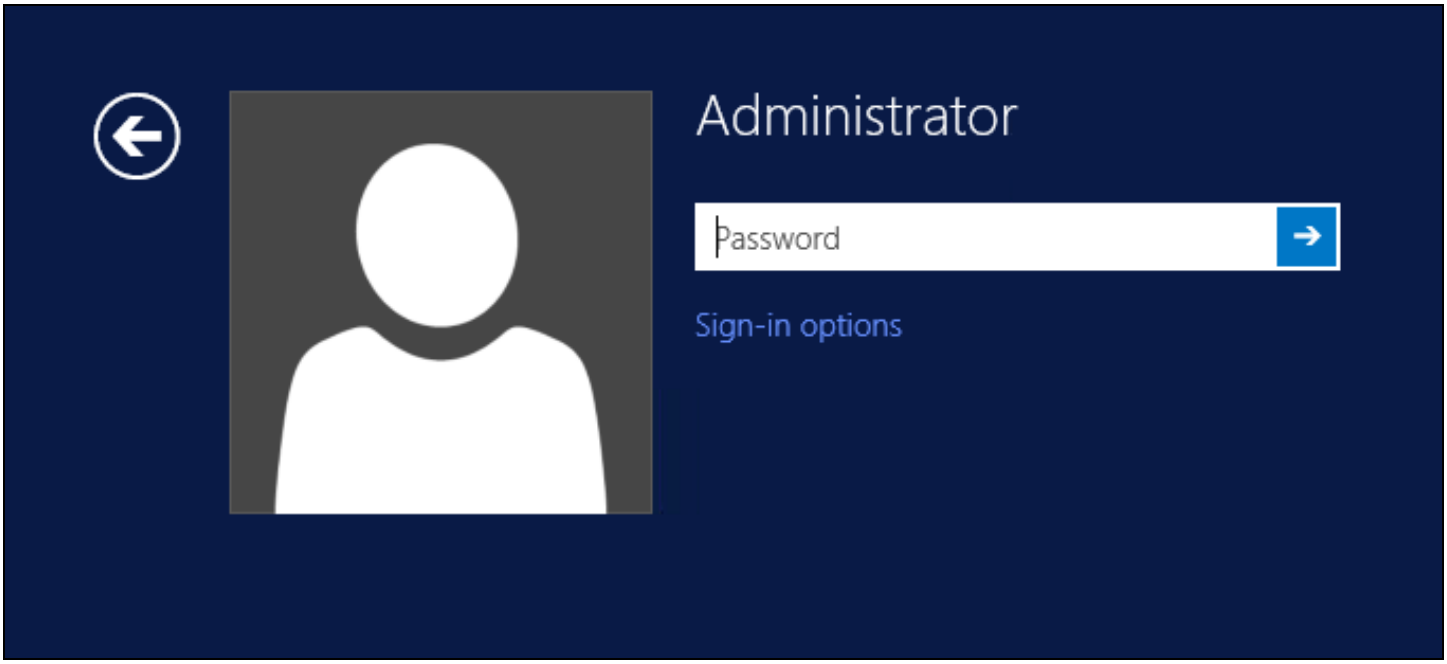


""Logging Level"" The account of message that will be logged.

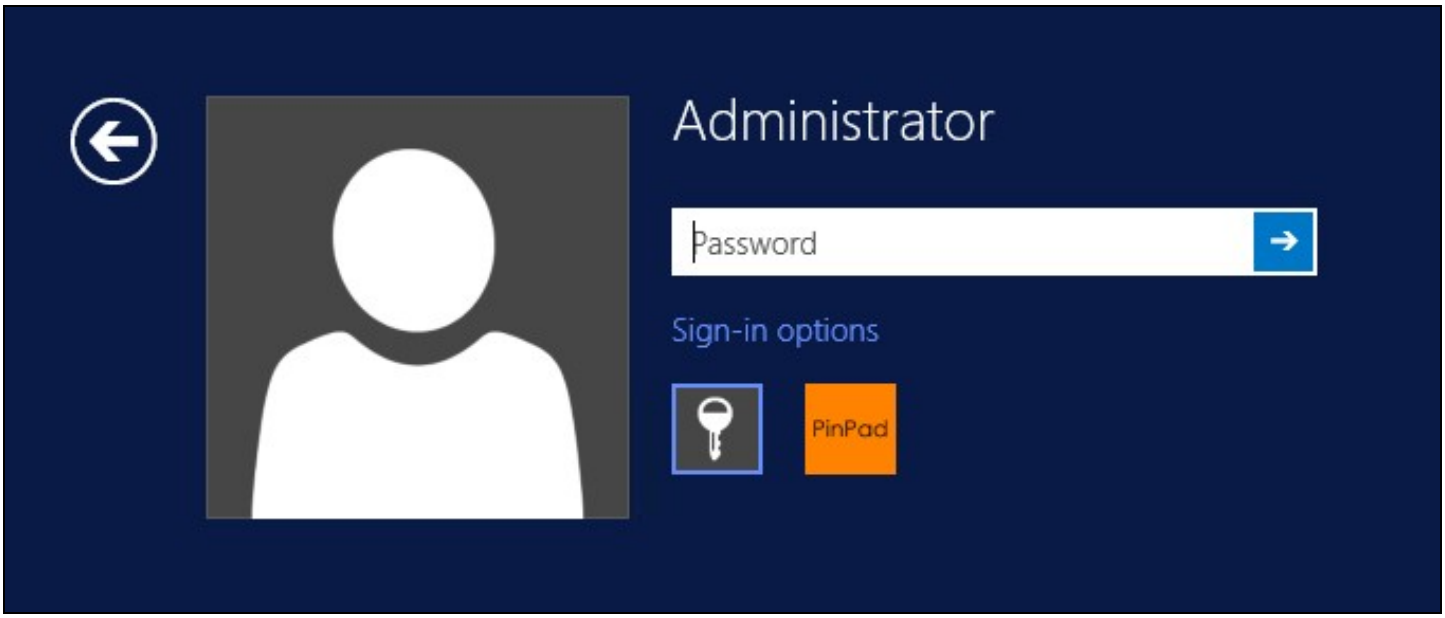
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

530.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

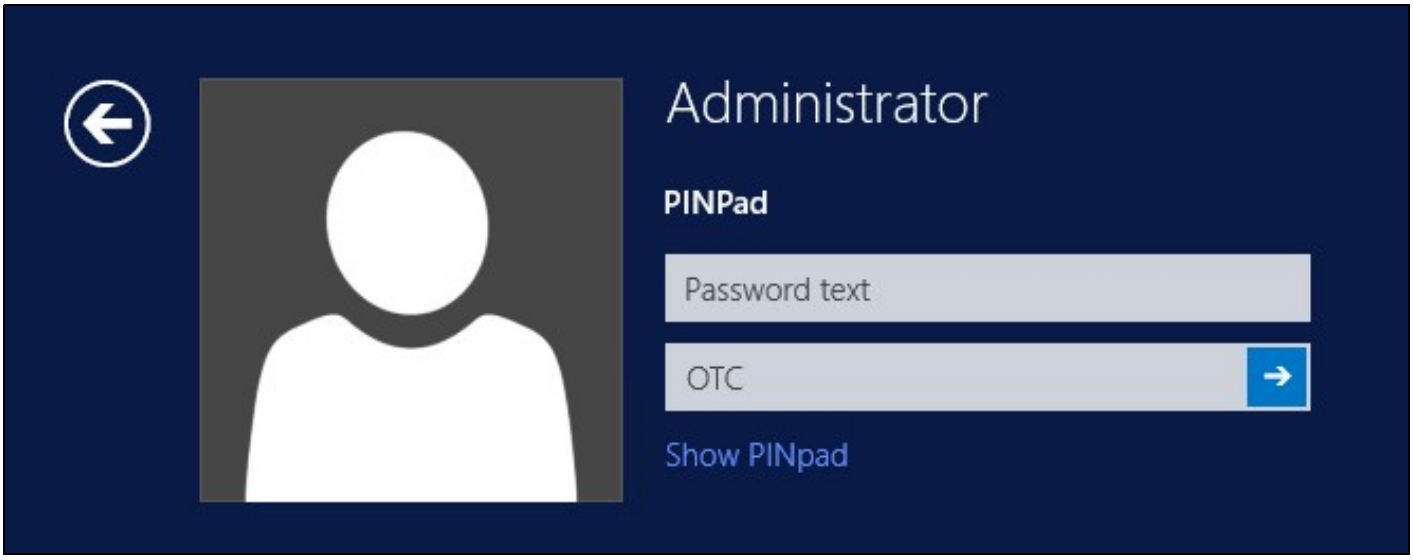
530.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

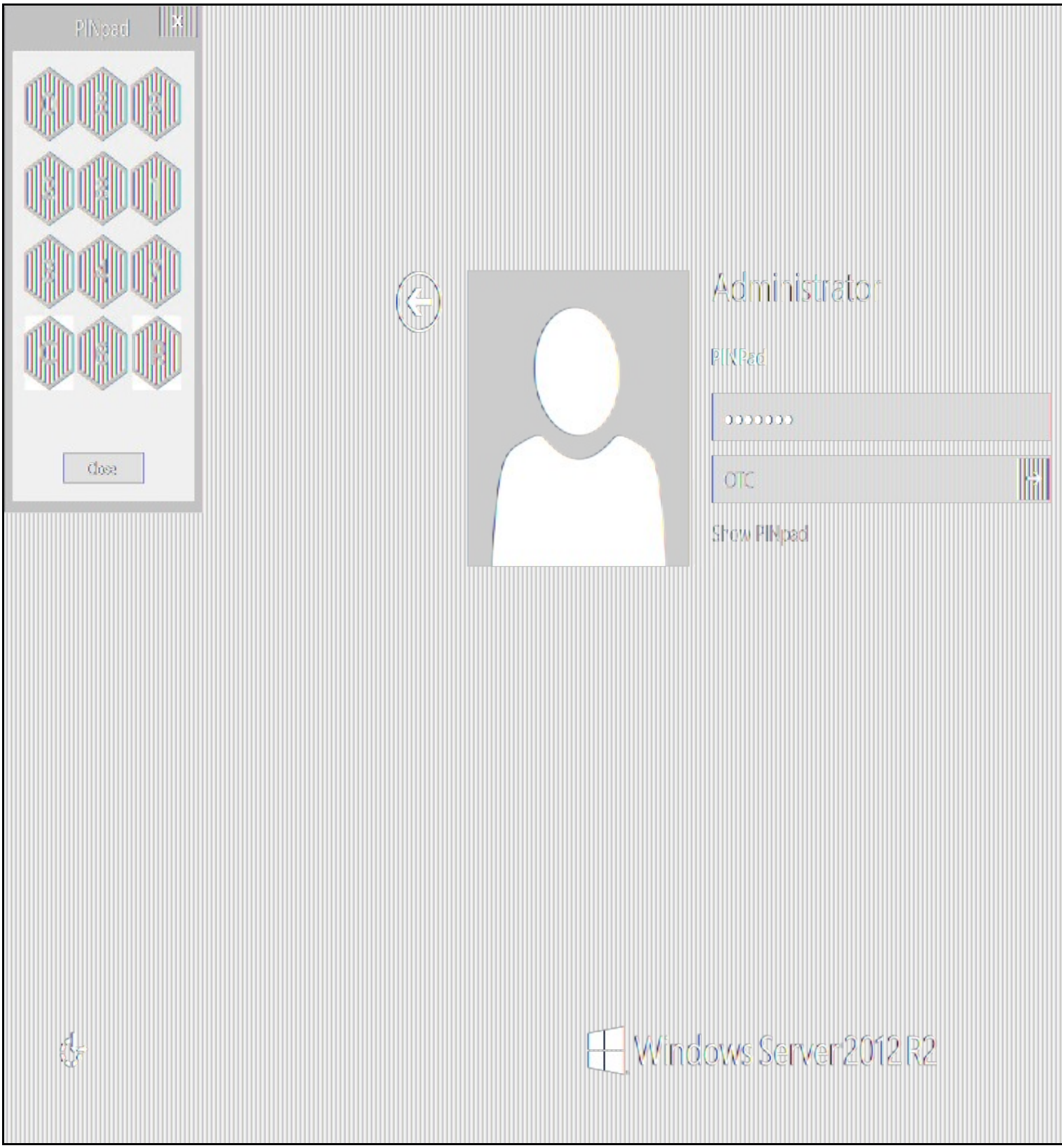
531 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*.

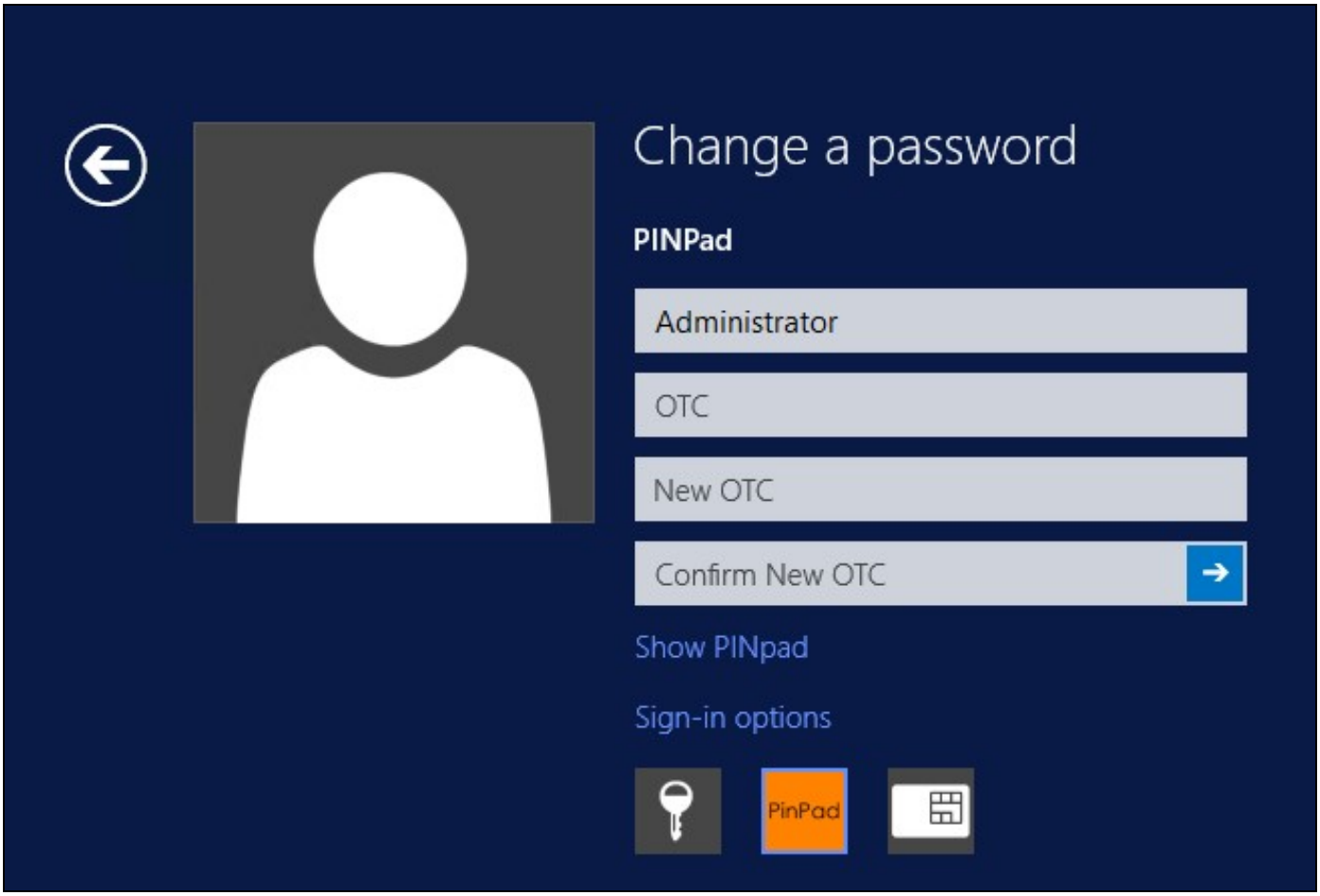
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*.

532 ChangePIN

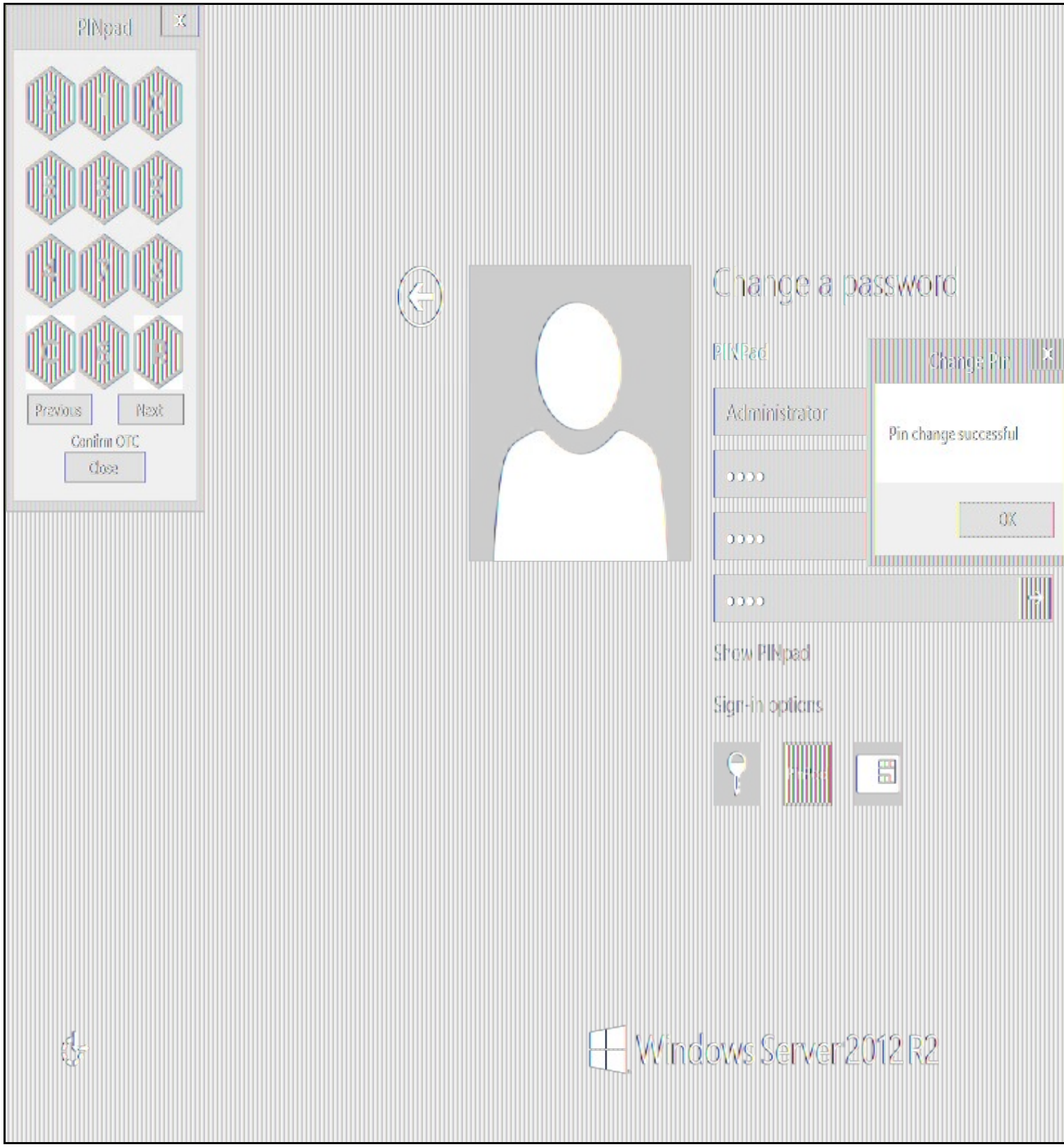
A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

533 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

533.1 Disabling the Credential Provider

If the Credential Provider fails to load correctly it can be disabled using the following process:

Boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works. Experience suggests that the first two options do not work in Windows 10.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Uninstall the Credential Provider.
- Using regedit.exe add or alter the following registry values:
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
- Using regedit.exe remove the following registry keys:
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - "HKEY_CLASSES_ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

The third option disables the credential provider, whereas the others actually remove it.

533.2 Temporarily Disabling the Credential Provider Remotely

If there is a problem with the Swivel Secure appliance, and you need to disable the AuthControl Credential Provider on a number of machines temporarily, you can do this using a PowerShell script.

533.2.1 Enabling Powershell Remoting

In order to be able to run PowerShell scripts on remote machines, you need to enable the WinRM service on both the target machines and the machine running the script. This article provides a step-by-step guide on setting up PowerShell remoting.

533.2.2 Setting up a List of Computers

The first step is to get a list of computers that you want to disable. This article suggests three alternative methods: hard-code the list in your script, read it from a file, or query the Active Directory. The last is only useful if you want to run the script on every computer on your domain. We will use the second method in our example, so assume there is a list of computer names, one per line, in "CPComputers.txt". This also assumes that the list is in the directory from which you are running the script, so you might want to use a full path in your script.

533.2.3 Setting up Credentials

For completeness, we will describe how to set up credentials to connect to the remote machines. If you are able simply to use the current logged-in user credentials on all remote PCs, then you can ignore this part.

To initialize a credential for use on the remote computers, use the following PowerShell command:

```
$cred = Get-Credential domain\adminuser
```

Replace "domain\adminuser" with the qualified name of the user whose credentials you will be using: note that you must include the domain. You will be prompted for the user's password.

If you are using the current user's credentials, leave off -Credential $cred from the Enter-PSSession command below.

533.2.4 The Script

Here is an example script for disabling the Credential Provider on a number of remote computers:

```
$cred = Get-Credential domain\adminuser
$computers = Get-Content -Path ".\CPComputers.txt"
foreach ($pc in $computers) {
 Enter-PSSession -ComputerName $pc -Credential $cred
 $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA
 if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 1 }
 $credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
 if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 1 }
 Exit-PSSession
}
```

533.2.5 Known Limitations

Be aware that running this script may not immediately disable the Credential Provider. You may need to wait a few minutes, or restart the computer, for the change to take effect.

533.2.6 Re-enabling the Credential Provider

To re-enable the Credential Provider, use the same script, but change the Disabled Value to 0 in two lines. So the script between Enter-PSSession and Exit-PSSession becomes

```
 $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA
```

```
if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 0 }
$credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 0 }
```

534 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local (offline) authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and request an new TURing.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

535 Windows Credential Provider with RBA

536 Introduction

From AuthControl Sentry v4.0.5, you can use your RBA rules with AuthControl Credential Provider to disable 2fa in case the user has enough points.

537 Prerequisites

AuthControl Credential Provider v5.4.2

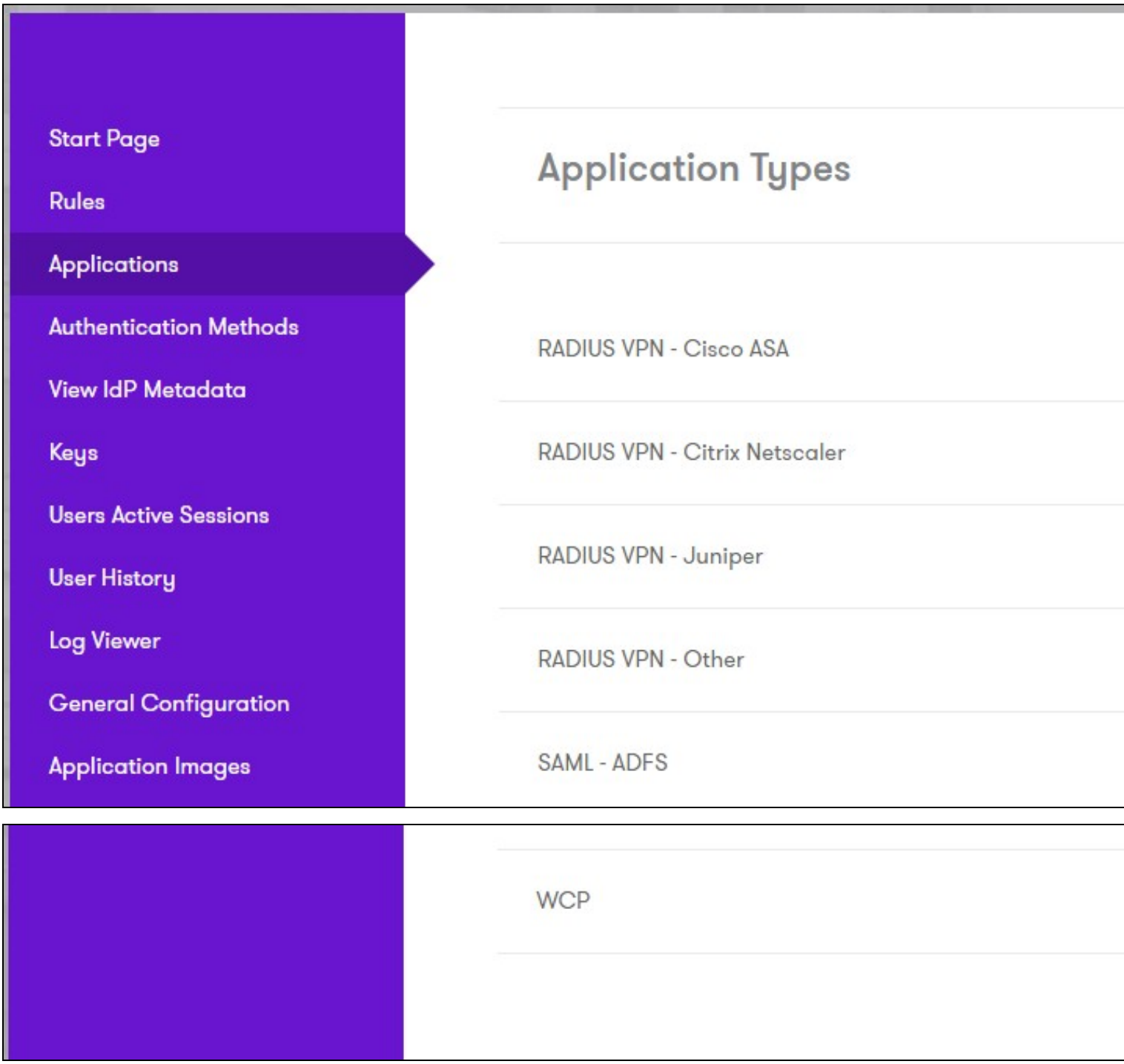
AuthControl Sentry v4.0.5

538 Limitations

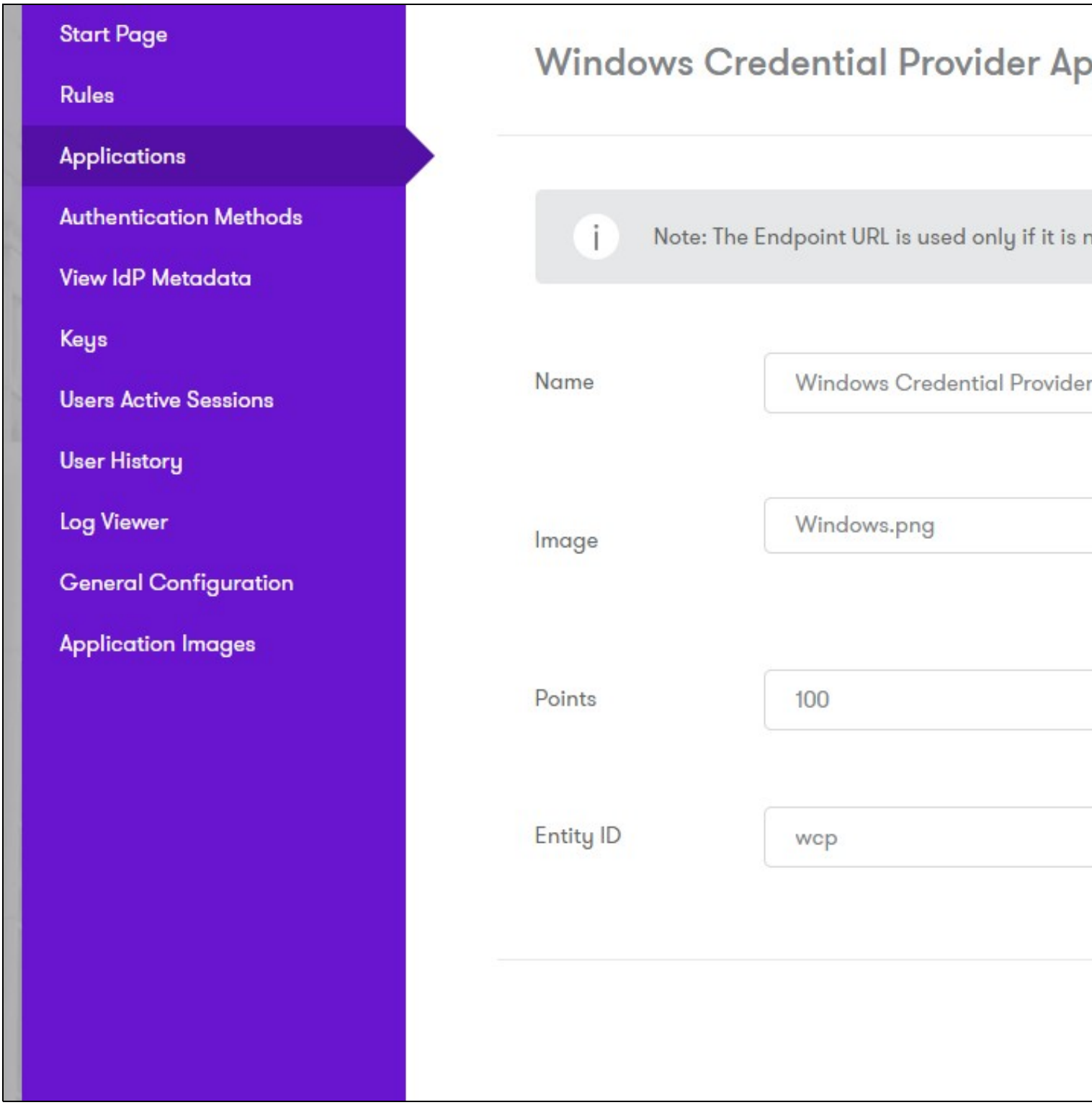
Certificate rule does not work with WCP

539 RBA Configuration

In AuthControl Sentry SSO administration page you have a new application type WCP. Add a new application.



Select WCP.

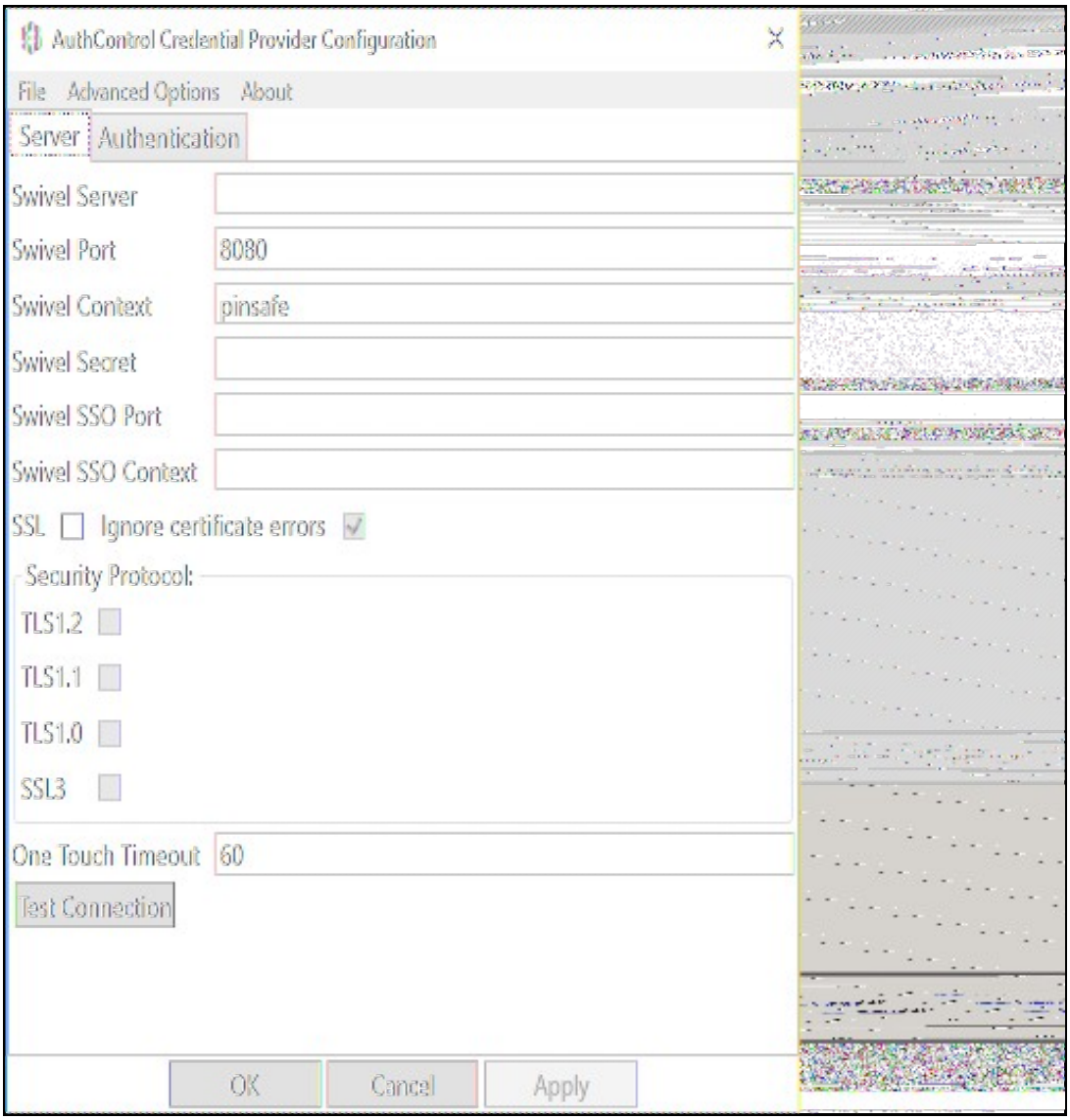


Enter a name, the required points for authentication without 2fa, **the entity ID must be wcp** and click Save.

If you haven't configure any rules, please look at Authcontrol v4 Sentry SSO and Adaptive Authentication.

540 WCP Configuration

Open AuthControl Credential Provider Configuration



enter the Swivel SSO Port as 8443 and Swivel SSO Context as sentry. This will enable the check for RBA rules in WCP.

541 Authenticating

When you try to login now it will check for the rules. If the user has enough points, it will allow authentication without using 2fa.

542 RBA with fingerprint

If you have Biometric Identification active, you can use this to give more points to RBA and disable 2fa.