Citrix Netscaler Gateway 10.x

Contents

- 1 Introduction
- 2 Prerequisites
  - 2.1 Note on upgrading the Netscaler
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
  - 5.1 Configuring the RADIUS server
  - 5.2 Enabling Session creation with username
  - 5.3 Setting up Swivel Dual Channel Transports
- 6 Citrix Netscaler Gateway Configuration
  - 6.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration
  - 6.2 Citrix Receiver with Netscaler configuration
- 7 Additional Configuration Options
  - 7.1 Netscaler RADIUS Monitor and RADIUS Load Balancer
  - 7.2 Netscaler SSL Bridge
  - 7.3 Login Page Customisation
  - 7.4 Upgrading Netscalers with Custom Pages
  - 7.5 Customisation Overview
    - 7.5.1 Login to Netscaler Command Line
    - 7.5.2 Backup Netscaler files
    - 7.5.3 Customise the login script
      - 7.5.3.1 Requesting a TURing image
    - 7.5.4 Customise the login prompt
      - 7.5.4.1 Additional Languages file modifications
    - 7.5.5 Upload files to Netscaler
    - 7.5.6 Create the boot archive file
    - 7.5.7 Tell the Netscaler to use the customised login pages
    - 7.5.8 Reboot Netscaler to verify files are copied across
  - 7.6 Additional Login Customisation options
    - 7.6.1 Automated TURing Display
    - 7.6.2 Changing the button labels
    - 7.6.3 Requesting the string Index
    - 7.6.4 PINpad
    - 7.6.5 Requesting an SMS
  - 7.7 Challenge and Response
  - 7.8 Image Request button displayed when needed
- 8 Testing
- 9 Uninstall/Removing the integration
- 10 Troubleshooting
  - 10.1 Error Messages
- 11 Known Issues and Limitations
- 12 Additional Information

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.

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.

Note on upgrading the Netscaler

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

Baseline

Tested with Swivel 3.9.6

Citrix Netscaler Gateway NS10.1 Build 121.10

Citrix Netscaler Gateway NS10.5

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.

Swivel Configuration

Configuring the RADIUS server

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

Enabling Session creation with username

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

Setting up Swivel Dual Channel Transports

See Transport Configuration

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.

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

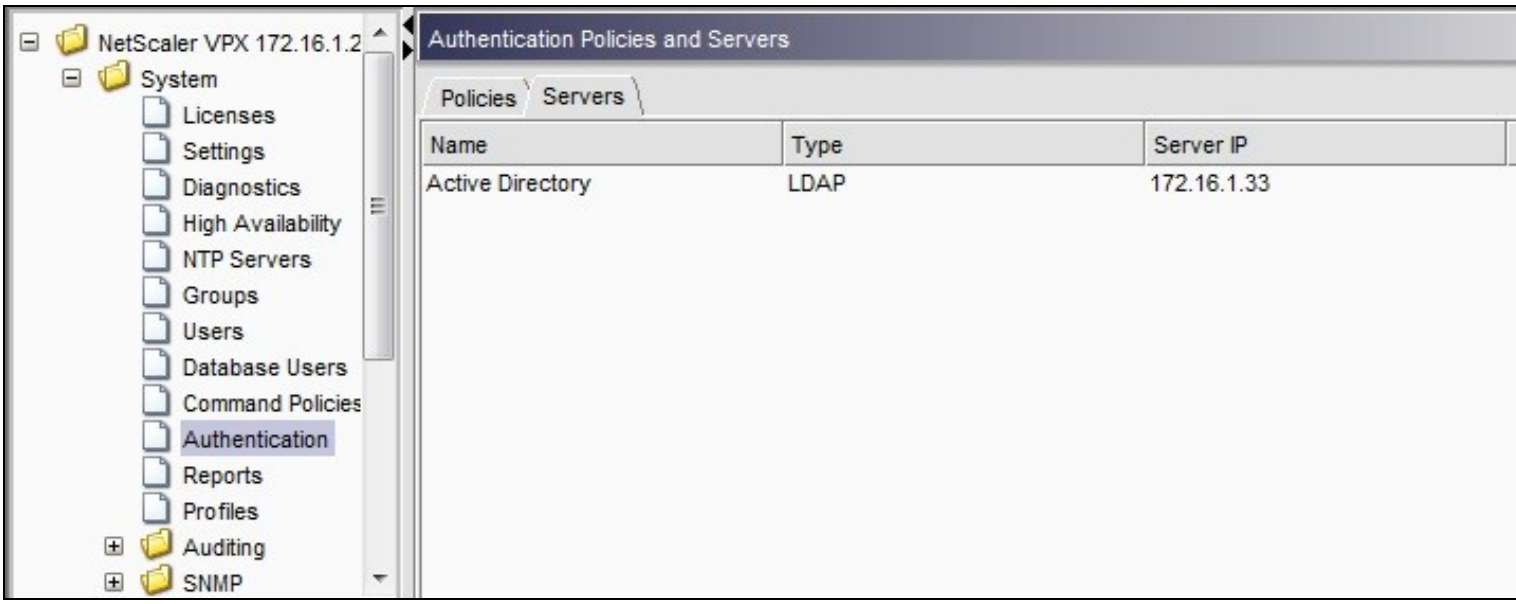
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

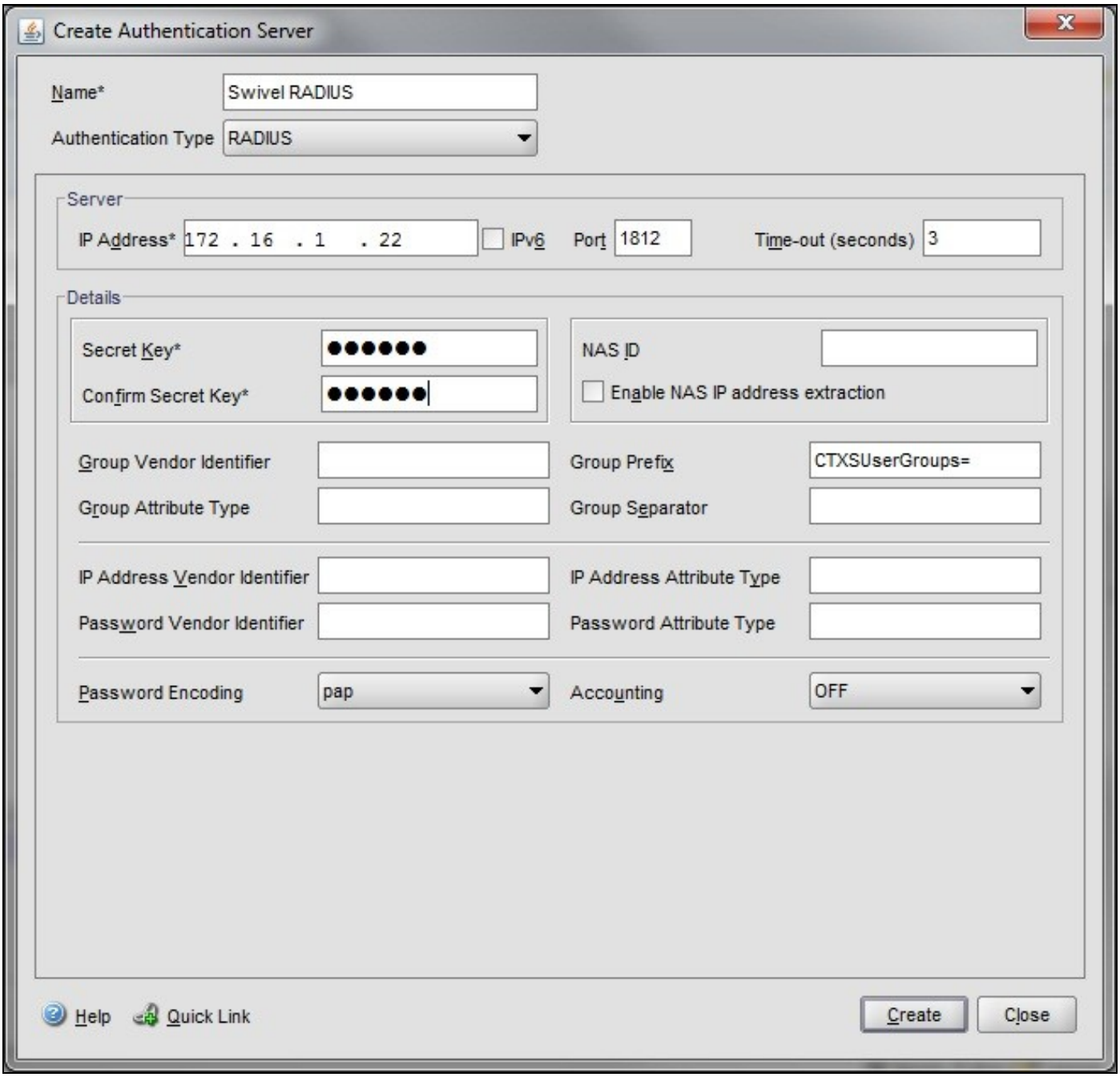
Group Prefix CTXSUserGroups=

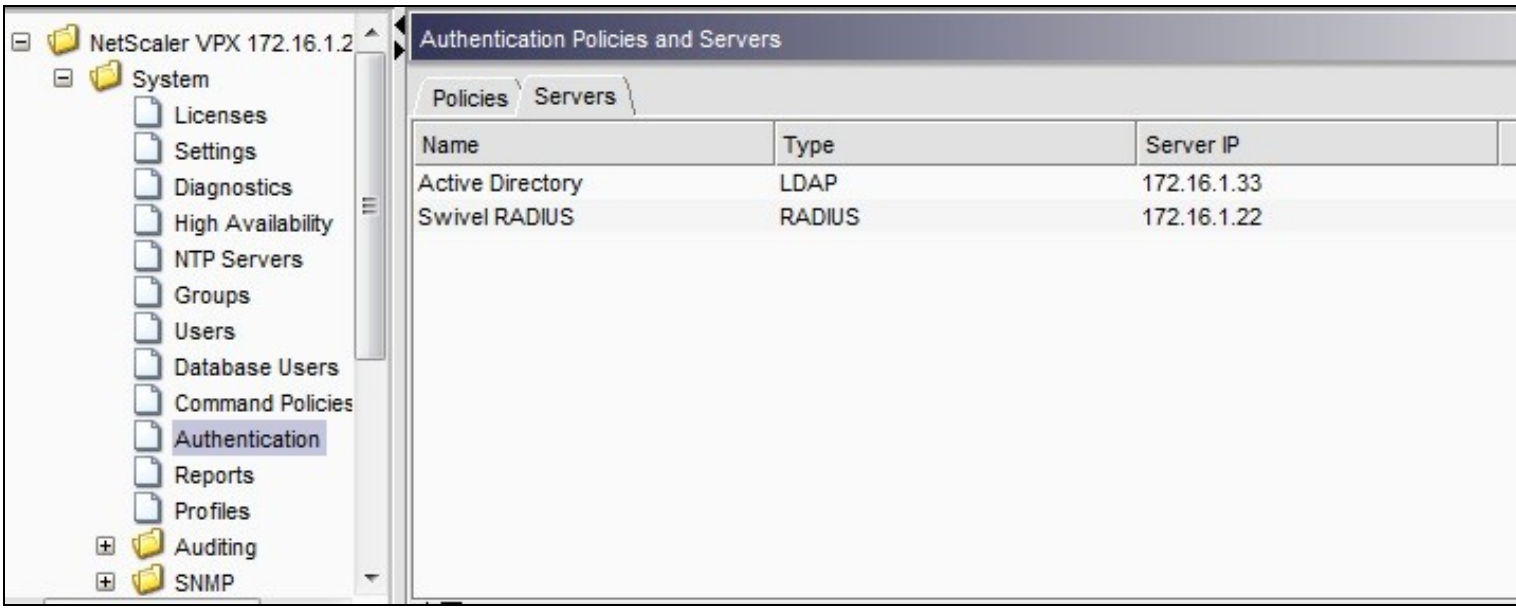
Group Separator ;

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.


NetScaler VPX 172.16.1.2
System
Licenses
Settings
Diagnostics
High Availability
NTP Servers
Groups
Users
Database Users
Command Policies
Authentication
Reports
Profiles
Auditing
SNMP
Authentication Policies and Servers
Policies
Servers
Name
Type
Server IP
Active Directory
LDAP
172.16.1.33


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



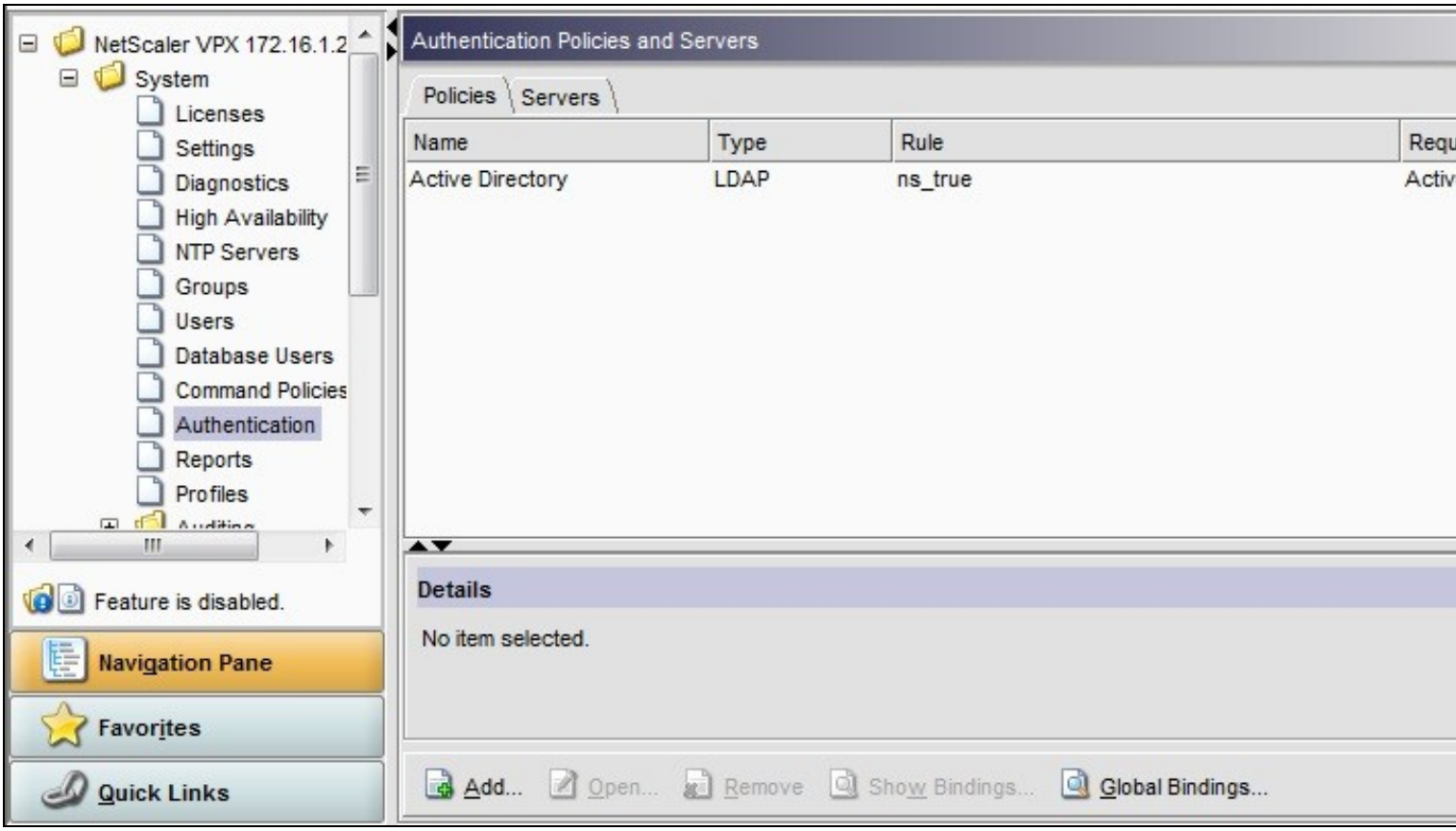
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

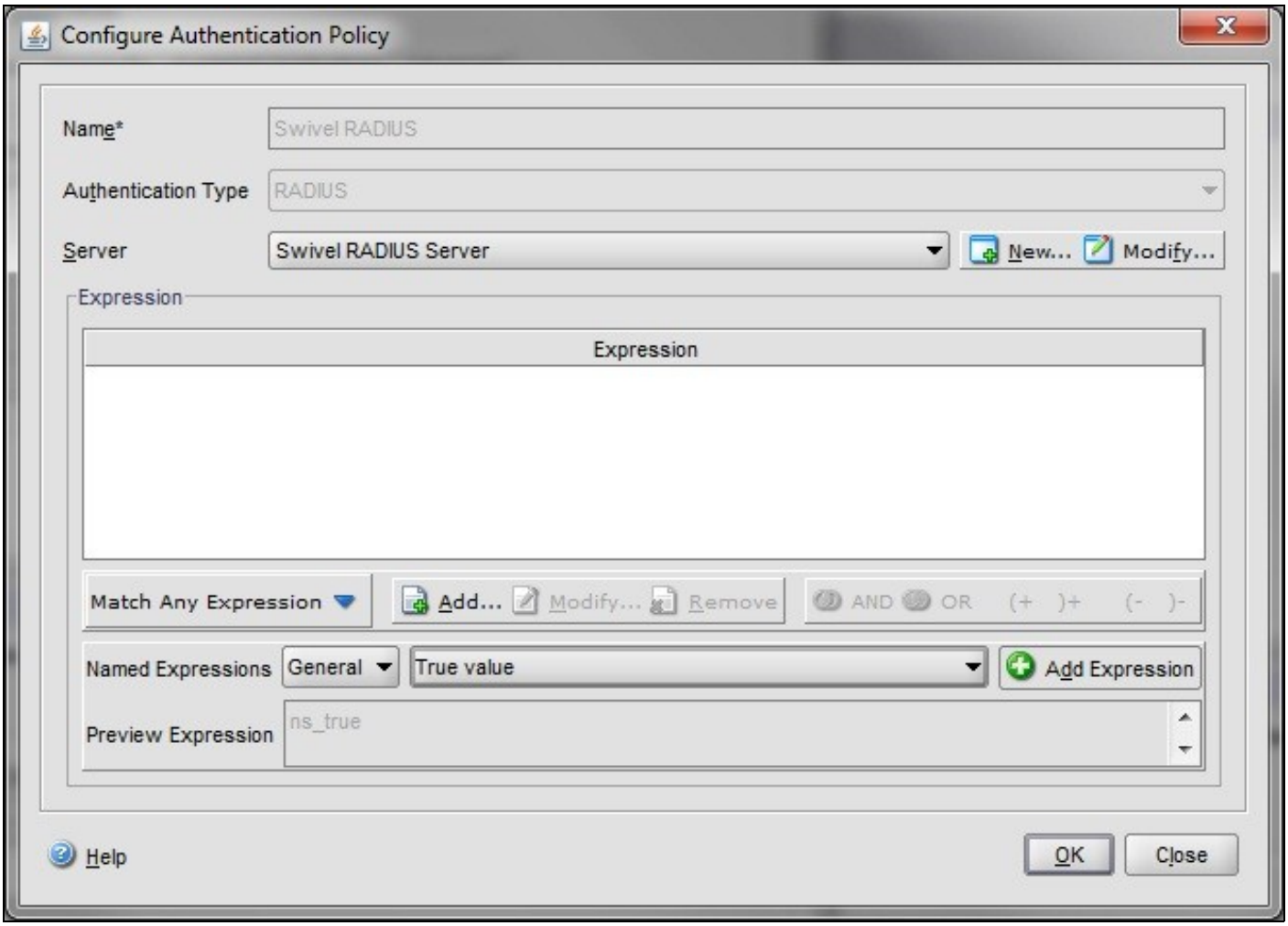
Name Swivel RADIUS Policy

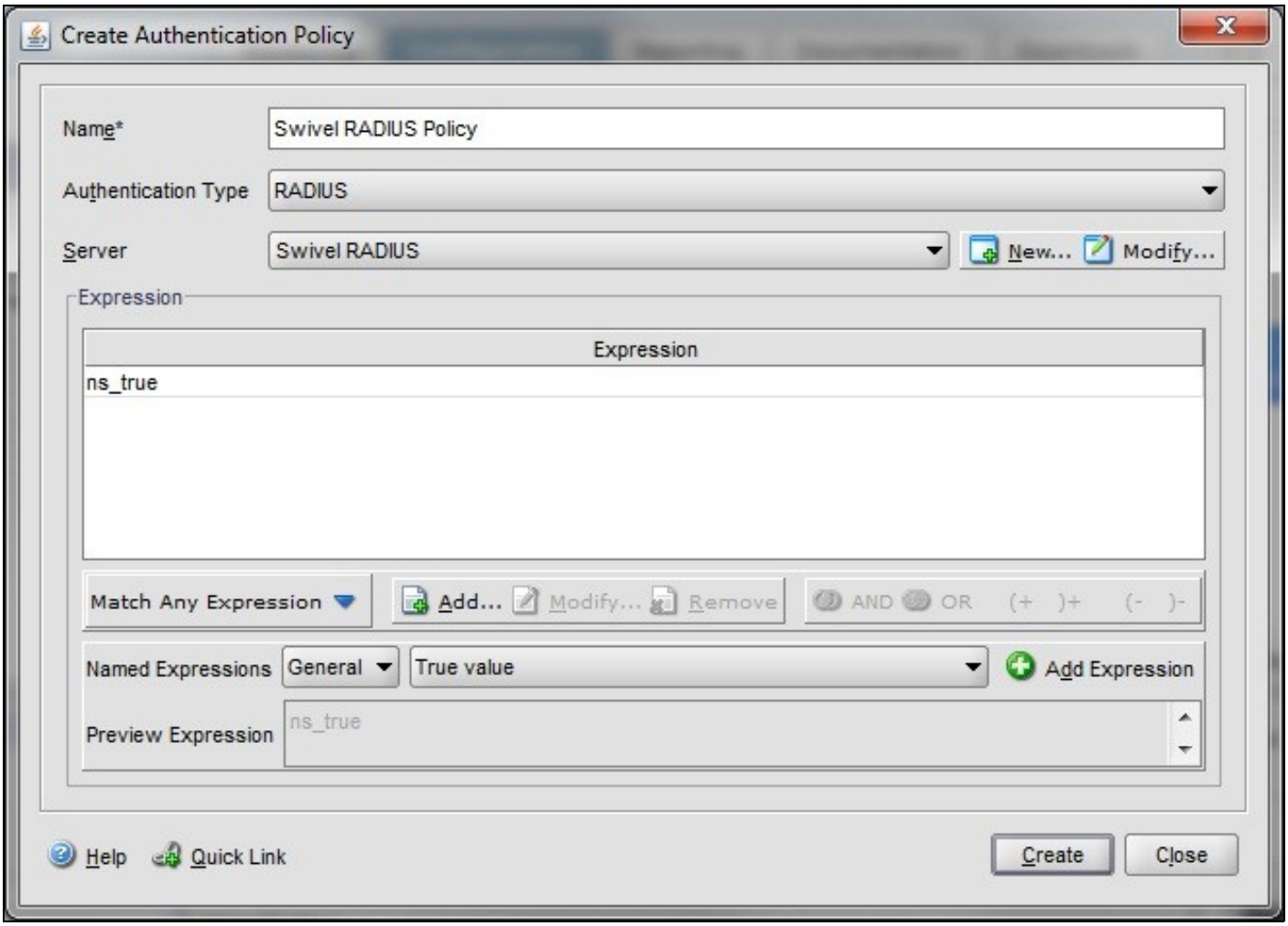
Authentication Type RADIUS

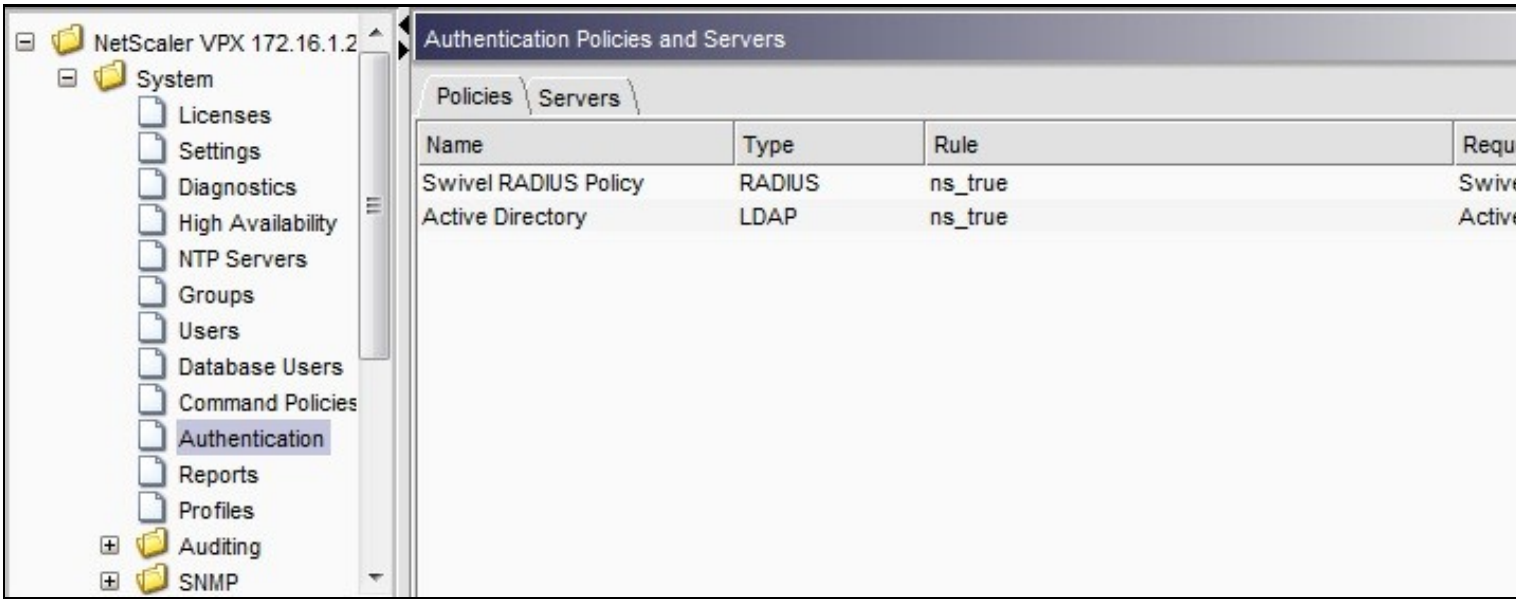
Server Swivel RADIUS

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

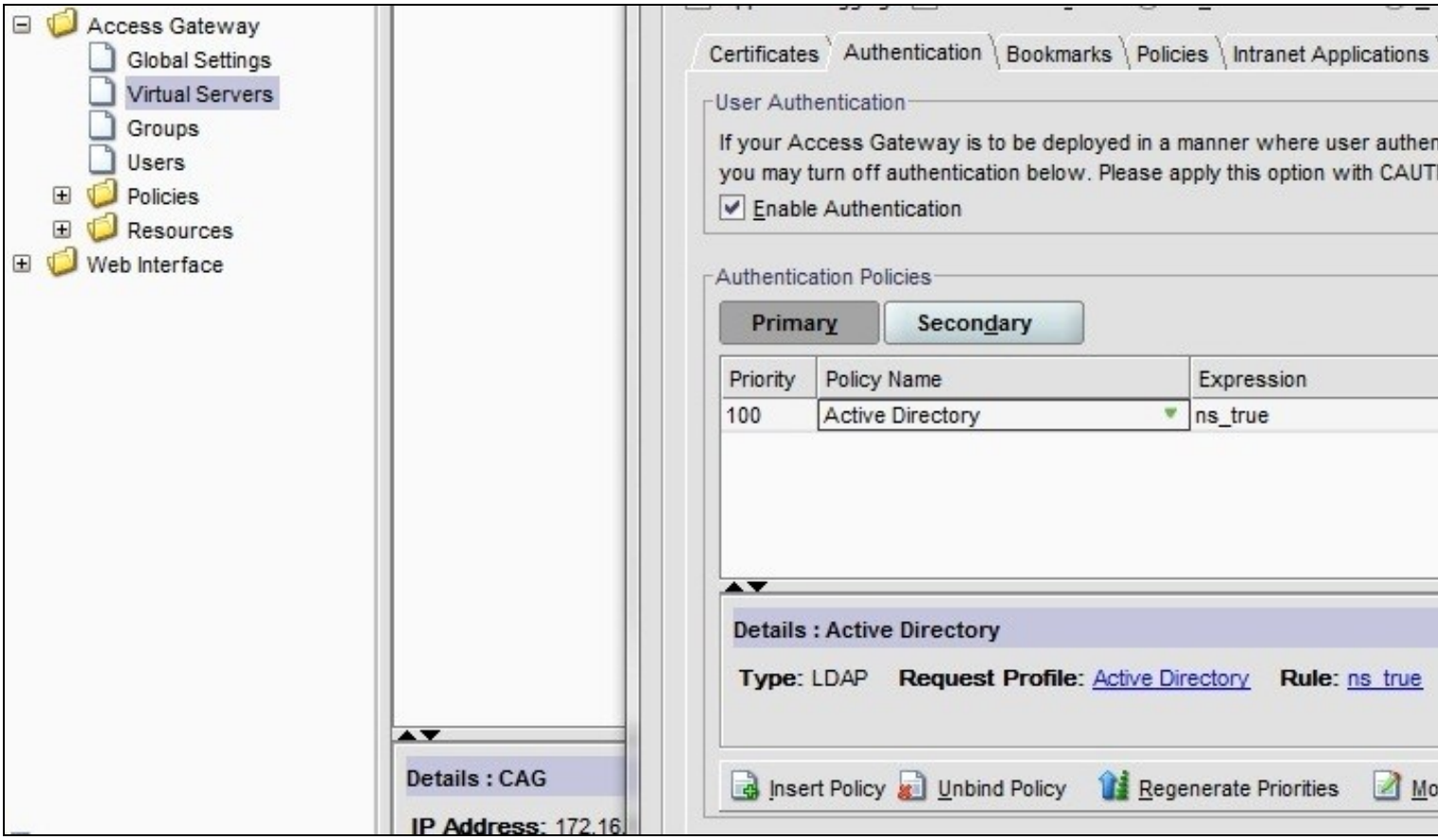


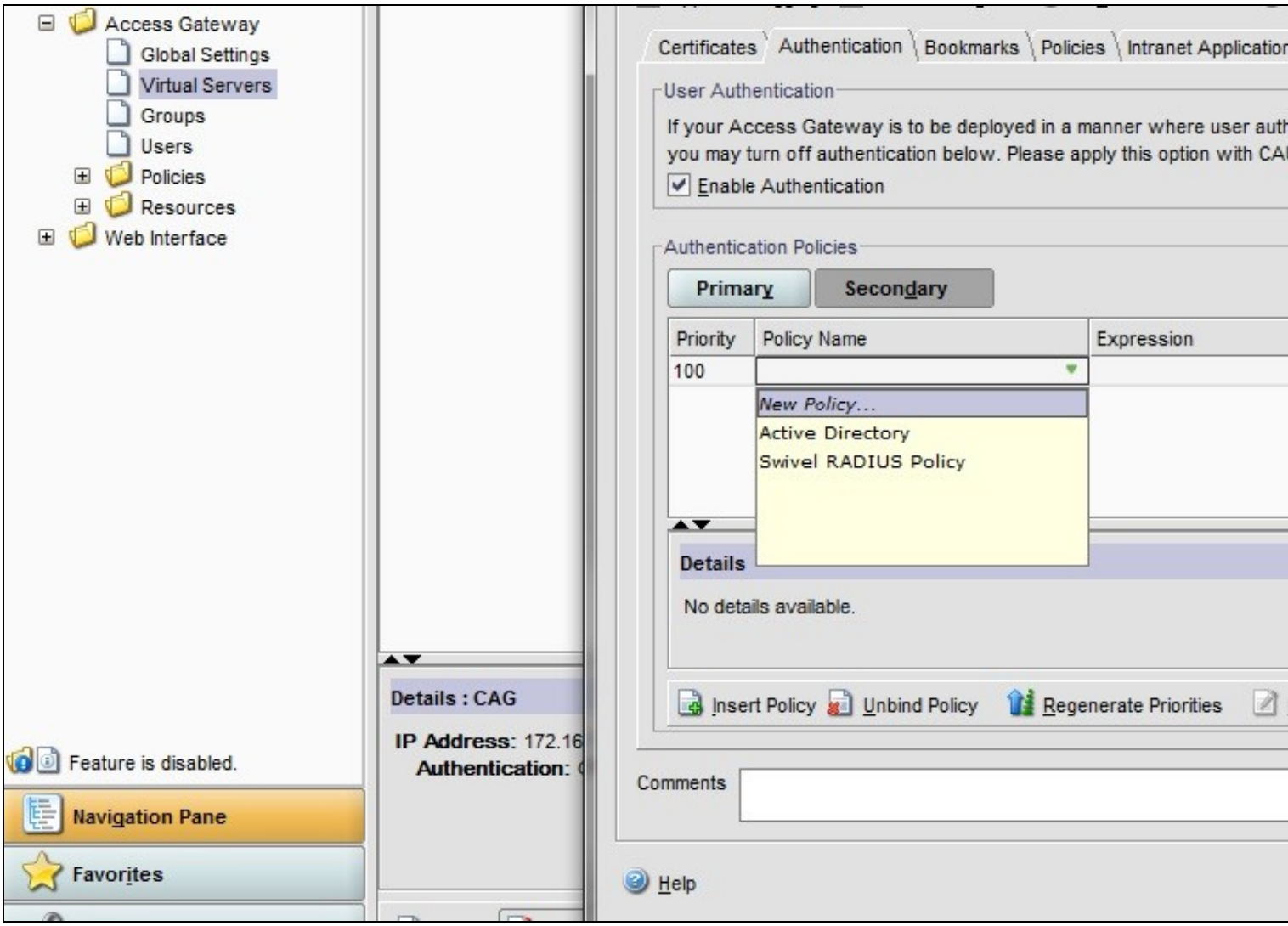

Configure Authentication Policy
Name*
Swivel RADIUS
Authentication Type
RADIUS
Server
Swivel RADIUS Server
New...
Modify...
Expression
Expression
Match Any Expression
Add...
Modify...
Remove
AND
OR
(+)+
(-)-
Named Expressions
General
True value
Add Expression
Preview Expression
ns_true
Help
OK
Close





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



Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

Additional Configuration Options

Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

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

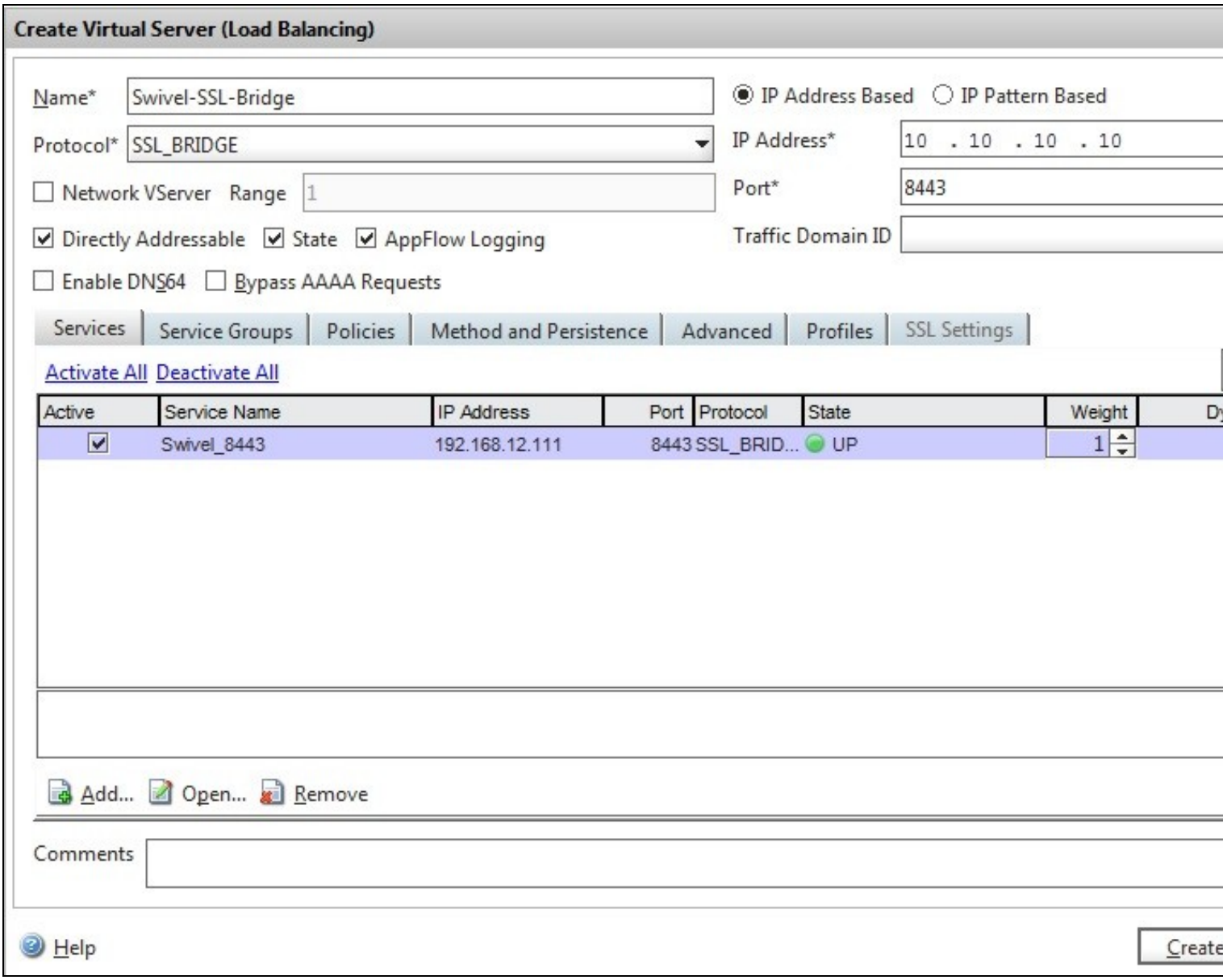
Select IP Adress Based

Protocol select SSL_Bridge

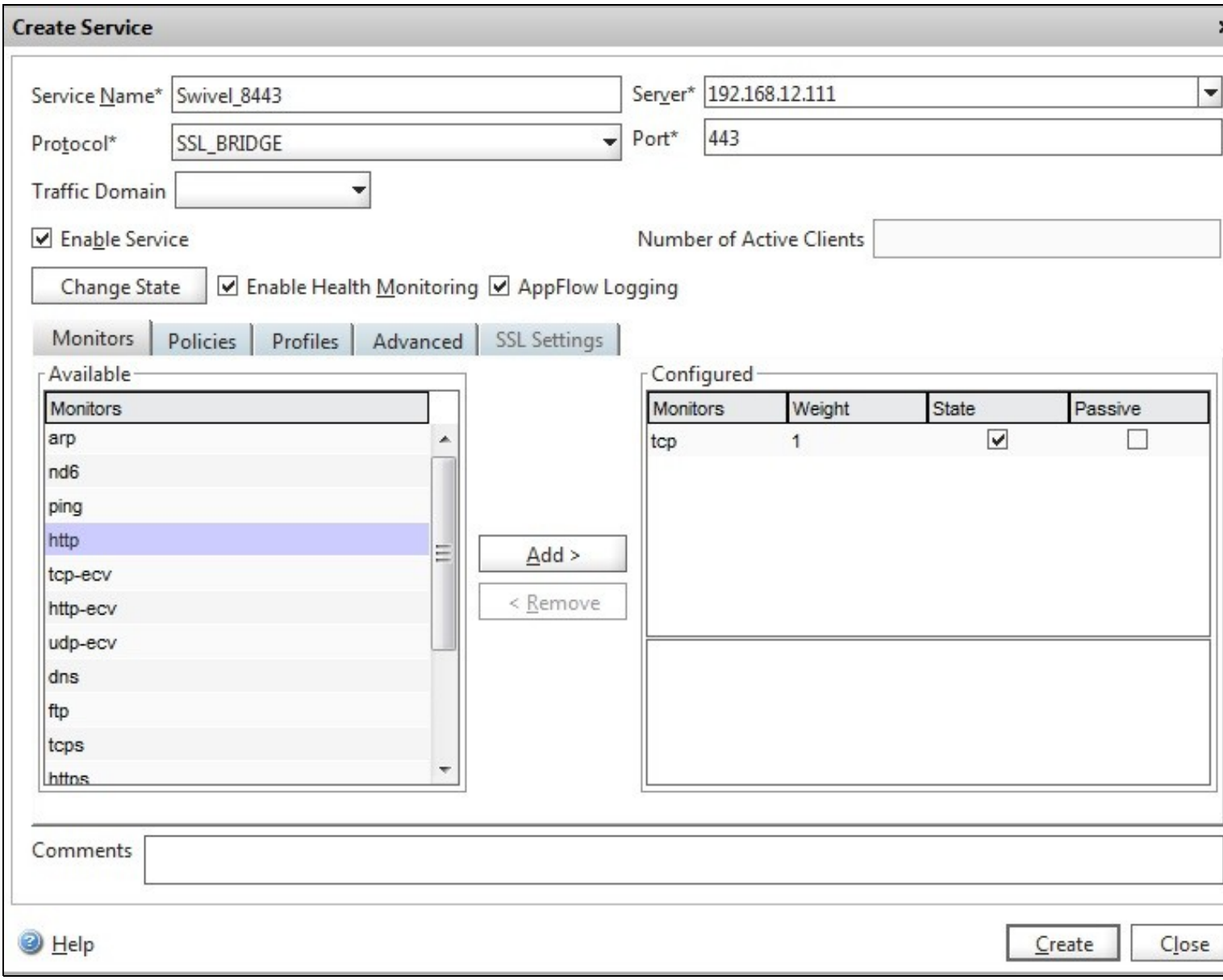
IP address Enter the public IP Address

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.



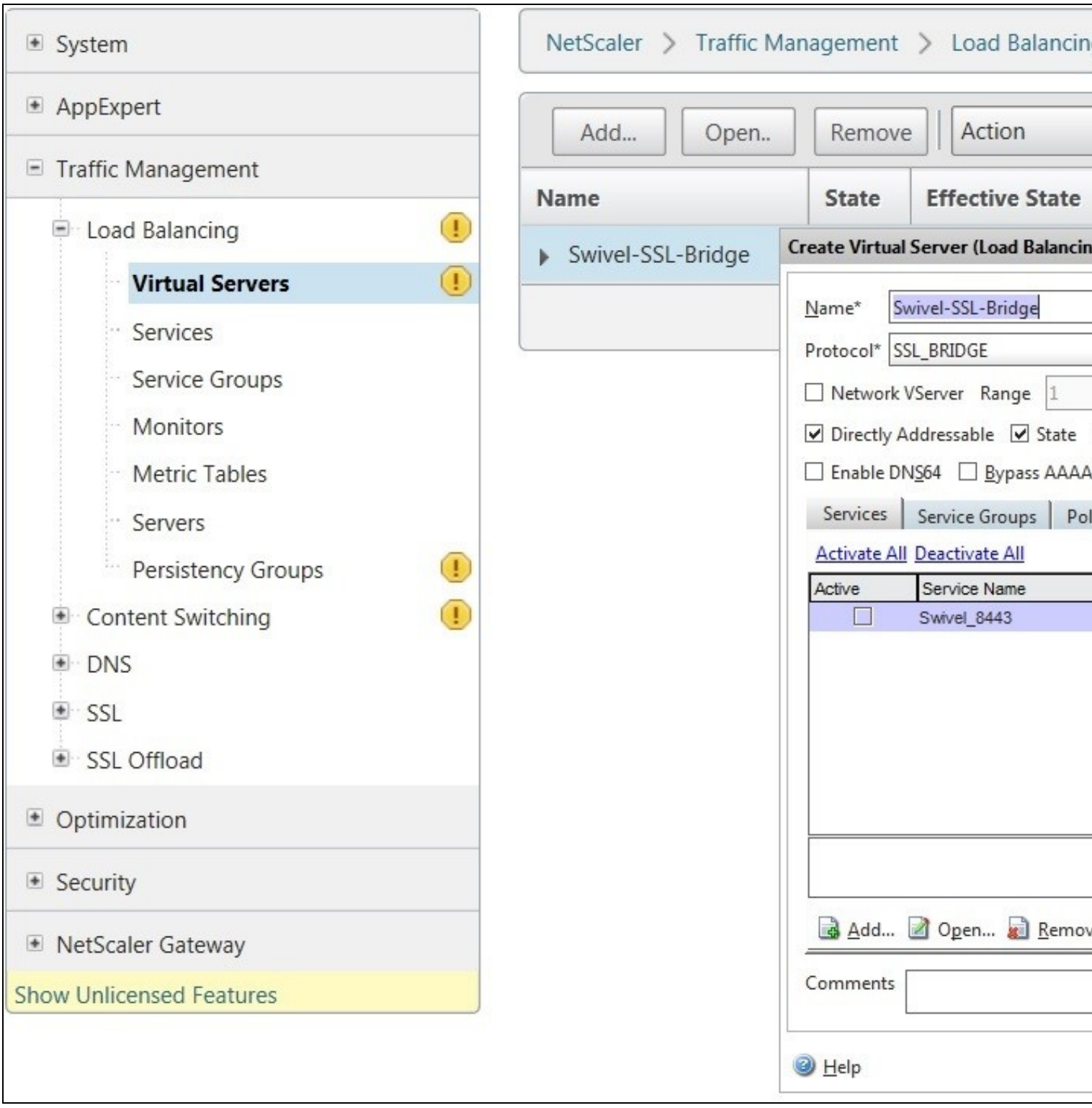
Service Name Name of the SSL Bridge

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.



Login Page Customisation

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

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.

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.

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
```

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
```

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.

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

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).

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
```

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

Create the boot archive file

```
mkdir /var/ns_gui_custom
```

```
cd /netscaler
```

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

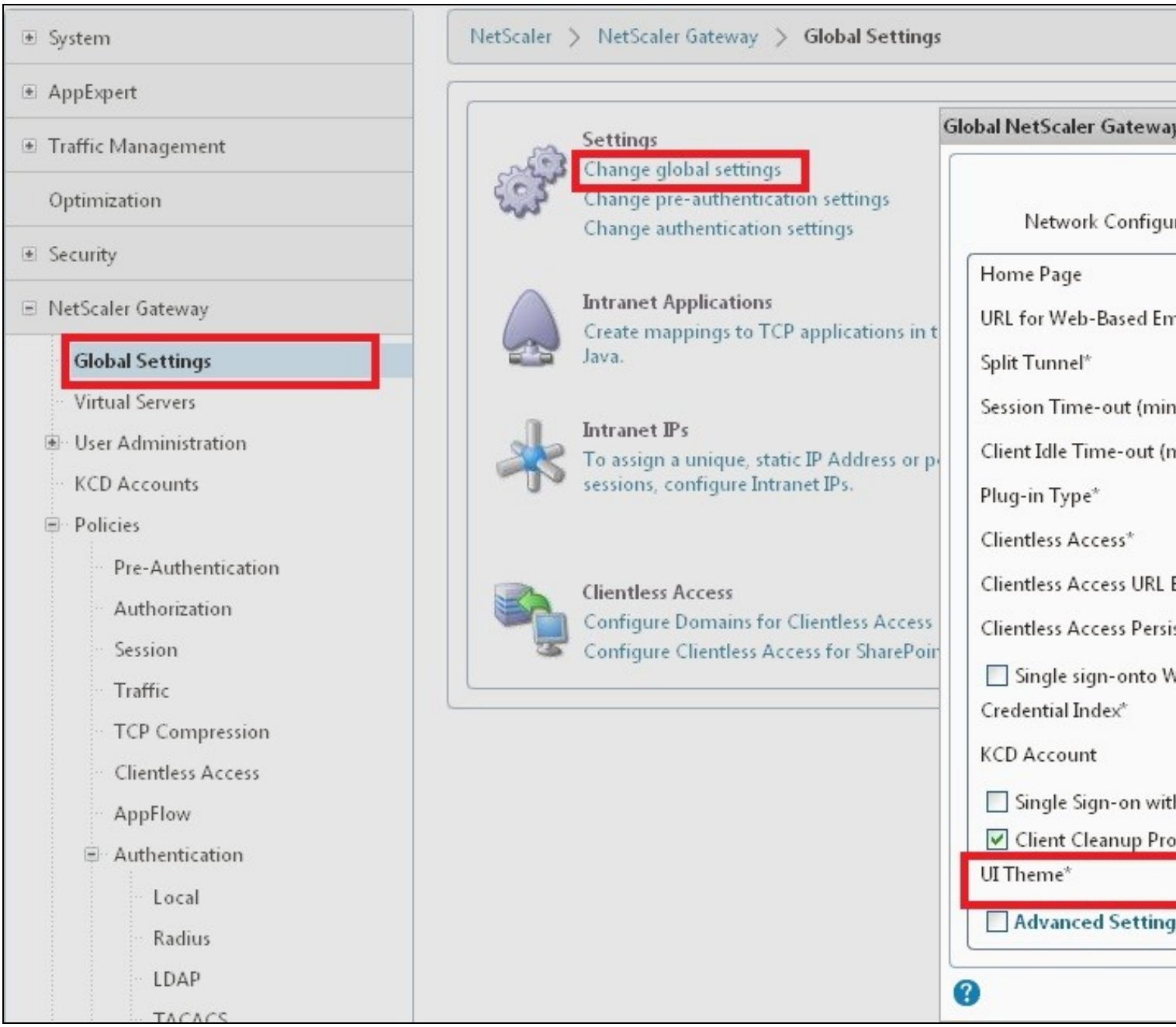
This should create the customtheme.tar.gz file used at boot time, and list all the files used.

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.



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.

Additional Login Customisation options

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%;"
```

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".

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

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

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

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");}
```

Image Request button displayed when needed

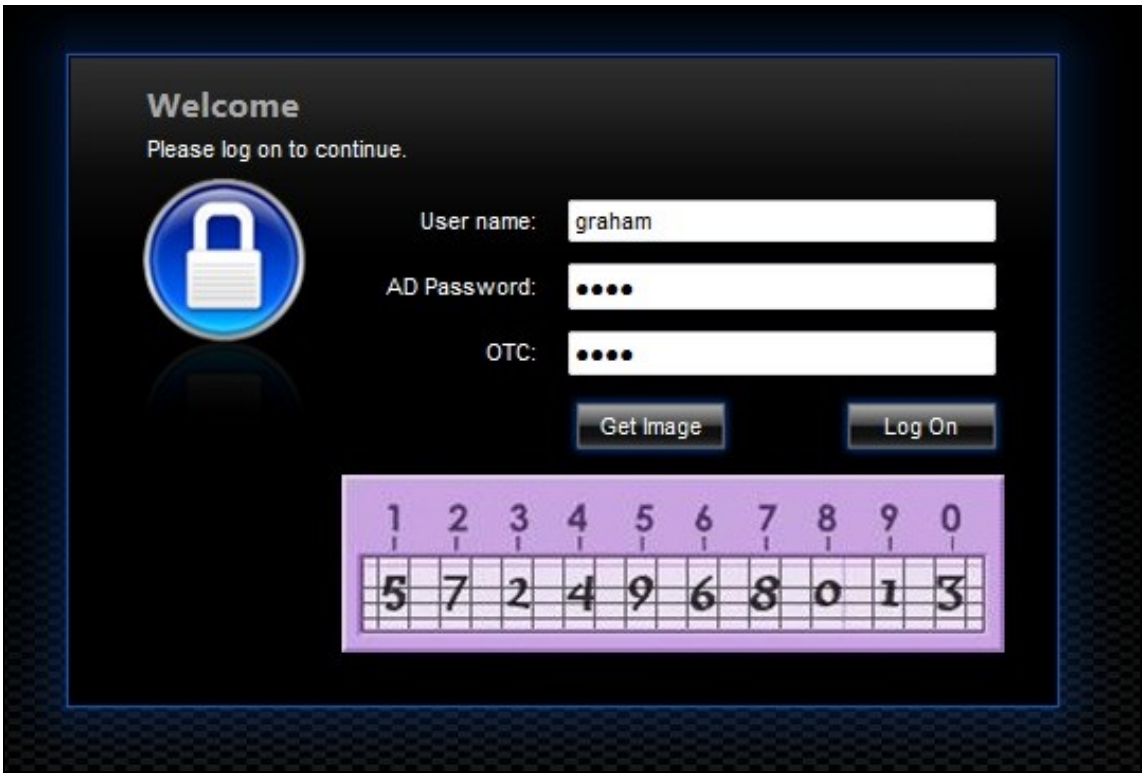
The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel 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>');
  }
}
```

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

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.

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.

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.

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]

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