Citrix Access Gateway Enterprise Edition 9

Contents

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.

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.

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

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 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.

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:
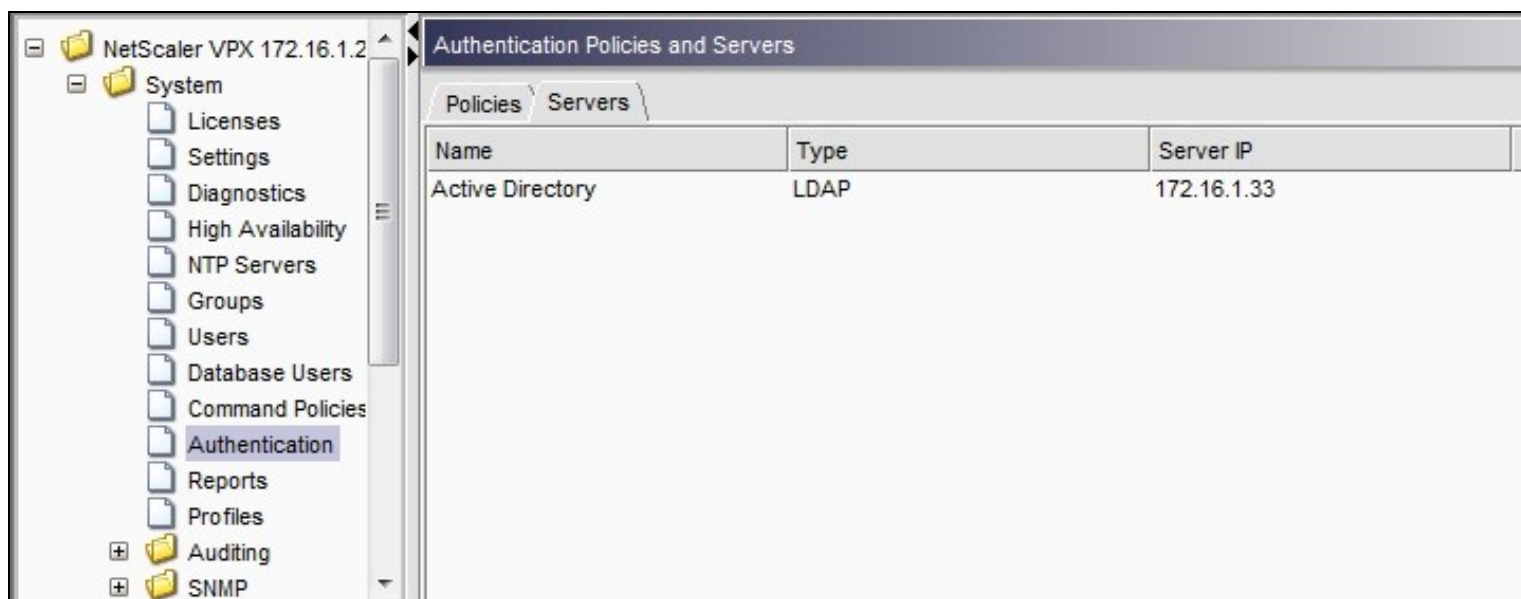
Name Swivel RADIUS

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* ●●●●●●   NAS ID _____

Confirm Secret Key* ●●●●●●   ☐ 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 _____
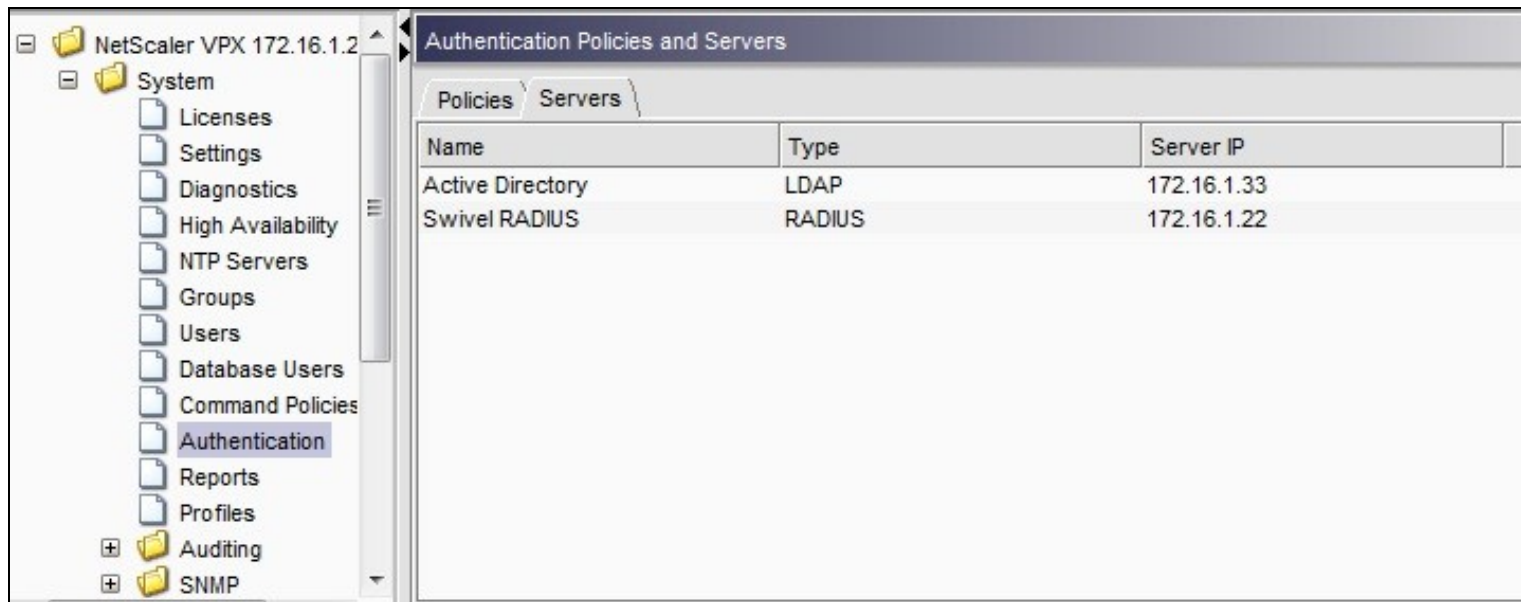
Password Encoding pap   Accounting OFF

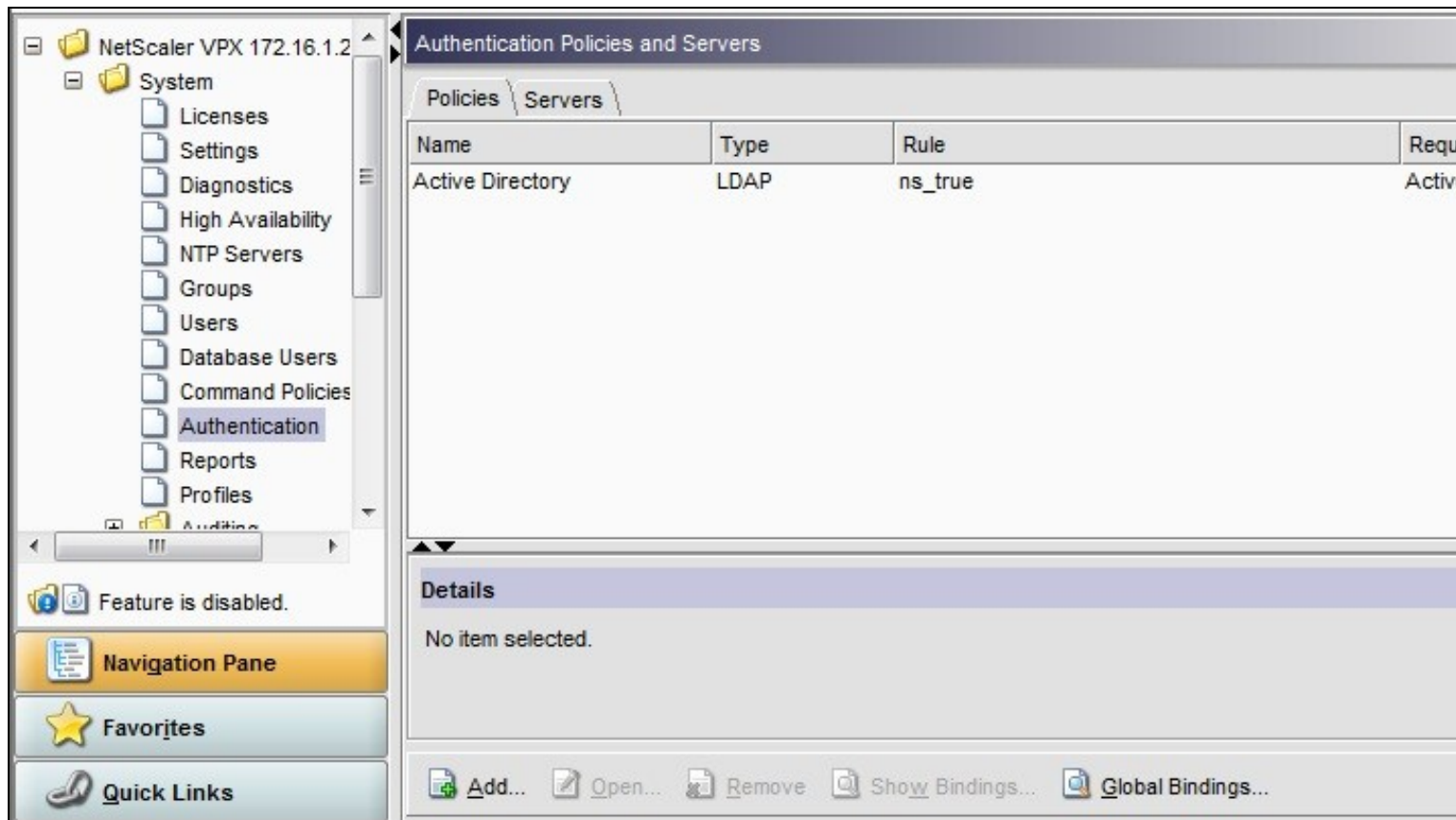⊘ Help ⚙ Quick Link   Create   Close

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

Create Authentication Policy

Name*   Swivel RADIUS Policy

Authentication Type   RADIUS

Server   Swivel RADIUS   New...   Modify...

Expression

Expression
ns_true

Match Any Expression   Add...   Modify...   Remove   AND   OR   (+)+   (-)-

Named Expressions   General   True value   Add Expression

Preview Expression   ns_true

Help   Quick Link   Create   Close

- 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	Rule	Requ
Swivel RADIUS Policy	RADIUS	ns_true	Swive
Active Directory	LDAP	ns_true	Active

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 CAUTI

☑ Enable Authentication

Authentication Policies

| Primary | Secondary |

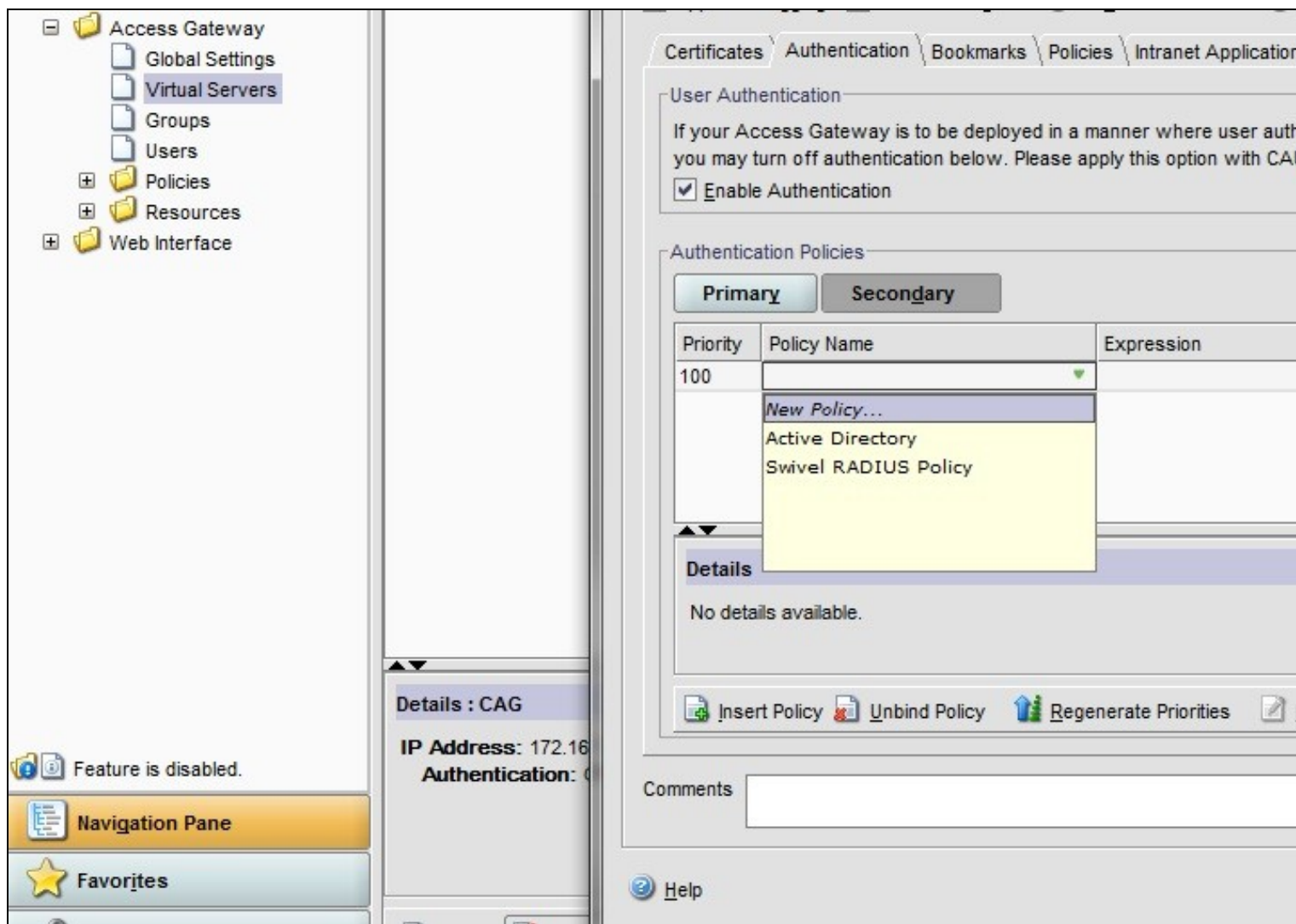| Priority	Policy Name	Expression
100	Active Directory ▾	ns_true

Details : Active Directory

Type: LDAP   **Request Profile:** Active Directory   **Rule:** ns_true

Insert Policy   Unbind Policy   Regenerate Priorities   Mo

Additional Configuration Options

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.

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".

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";
```


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
```


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

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.

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.

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