

Citrix Access Gateway Enterprise Edition 10

Contents

- 1 Introduction
- 2 Prerequisites
- 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 Access Gateway Enterprise Edition Configuration
 - ◆ 6.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration
 - ◆ 6.2 Test the RADIUS authentication
- 7 Additional Configuration Options
 - ◆ 7.1 Login Page Customisation
 - ◇ 7.1.1 Customisation Overview
 - ◇ 7.1.2 Login to Netscaler Command Line
 - ◇ 7.1.3 Backup Netscaler files
 - ◇ 7.1.4 Customise the login script
 - 7.1.4.1 Requesting a TURING image
 - ◇ 7.1.5 Customise the login prompt
 - 7.1.5.1 Additional Languages file modifications
 - ◇ 7.1.6 Upload files to Netscaler
 - ◇ 7.1.7 Copy the modified files from run time to file storage
 - ◇ 7.1.8 Reboot Netscaler to verify files are copied across
 - ◆ 7.2 Additional Login Customisation options
 - ◇ 7.2.1 Automated TURING Display
 - ◇ 7.2.2 Changing the button labels
 - ◇ 7.2.3 Requesting the string Index
 - ◇ 7.2.4 PINpad
 - ◇ 7.2.5 Requesting an SMS
 - ◆ 7.3 Challenge and Response
 - ◆ 7.4 Image Request button displayed when needed
- 8 Testing
- 9 Uninstall/Removing the integration
- 10 Troubleshooting
- 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 10.0 (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.

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](#).

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.

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 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 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 CTXUserGroups=

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

X

Name*Swivel RADIUS

Authentication TypeRADIUS

Server

IP Address*172 . 16 . 1 . 22

☐ IPv6

Port1812

Time-out (seconds)3

Details

Secret Key*

●●●●●●

Confirm Secret Key*

●●●●●●

NAS ID

☐ Enable NAS IP address extraction

Group Vendor Identifier

Group PrefixCTXSUserGroups=

Group Attribute Type

Group Separator

IP Address Vendor Identifier

IP Address Attribute Type

Password Vendor Identifier

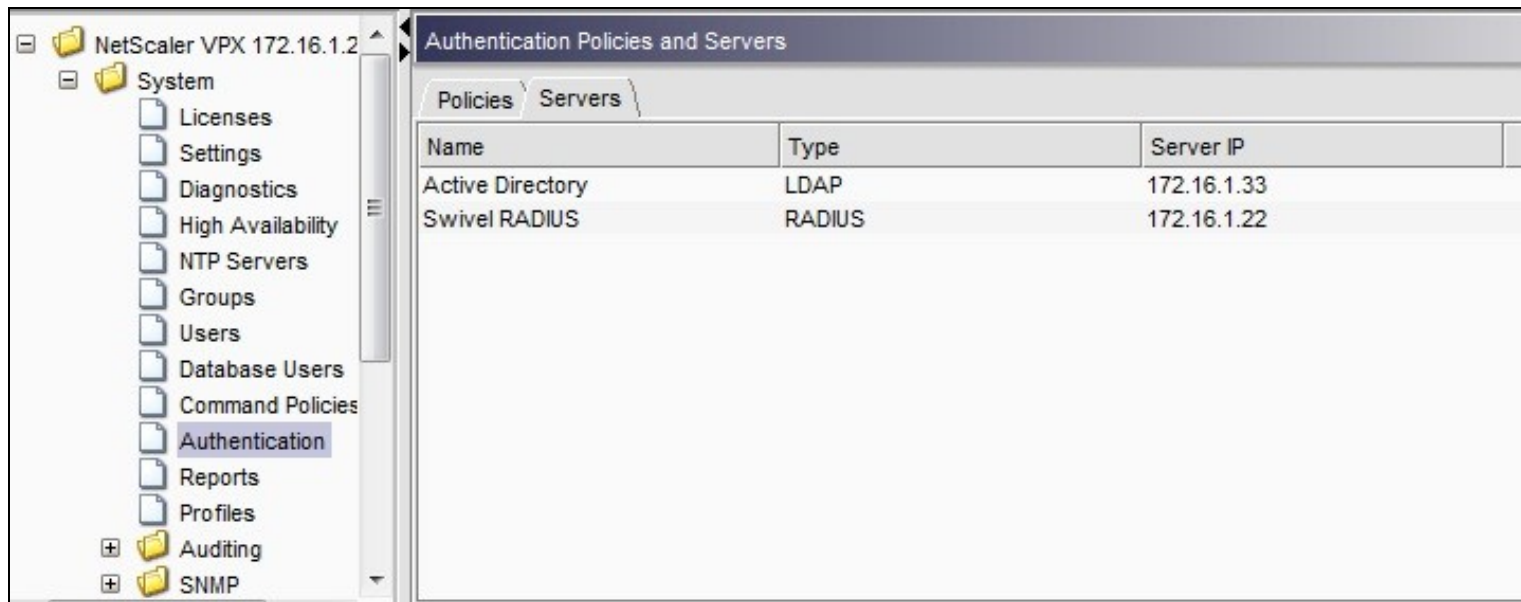
Password Attribute Type

Password Encodingpap

AccountingOFF

HelpQuick Link

CreateClose



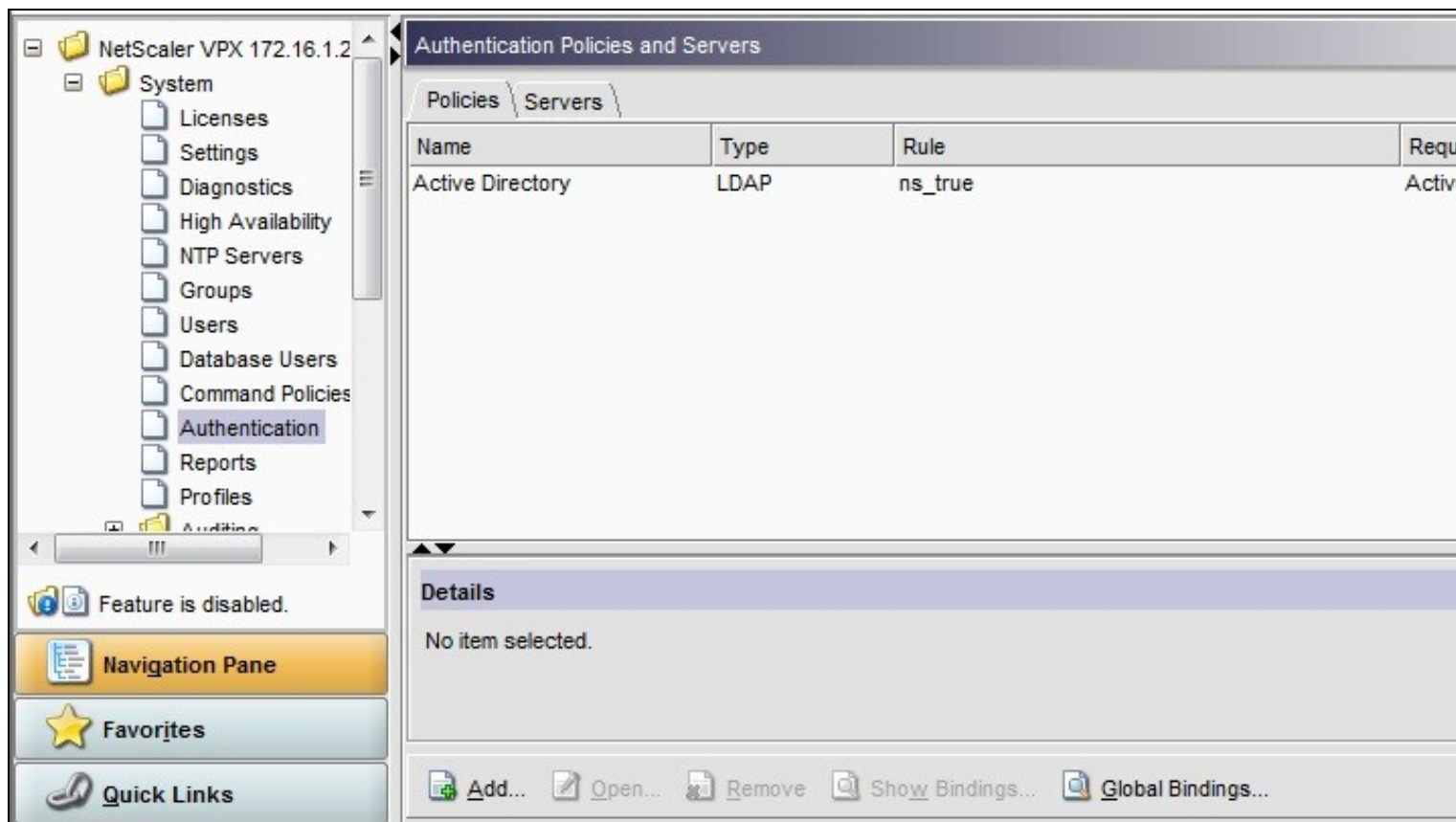
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:


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	Require
Swivel RADIUS Policy	RADIUS	ns_true	Swivel
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 authentication is required, you may turn off authentication below. Please apply this option with CAUTION.

☒ Enable Authentication

Authentication Policies

Primary

Secondary

Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

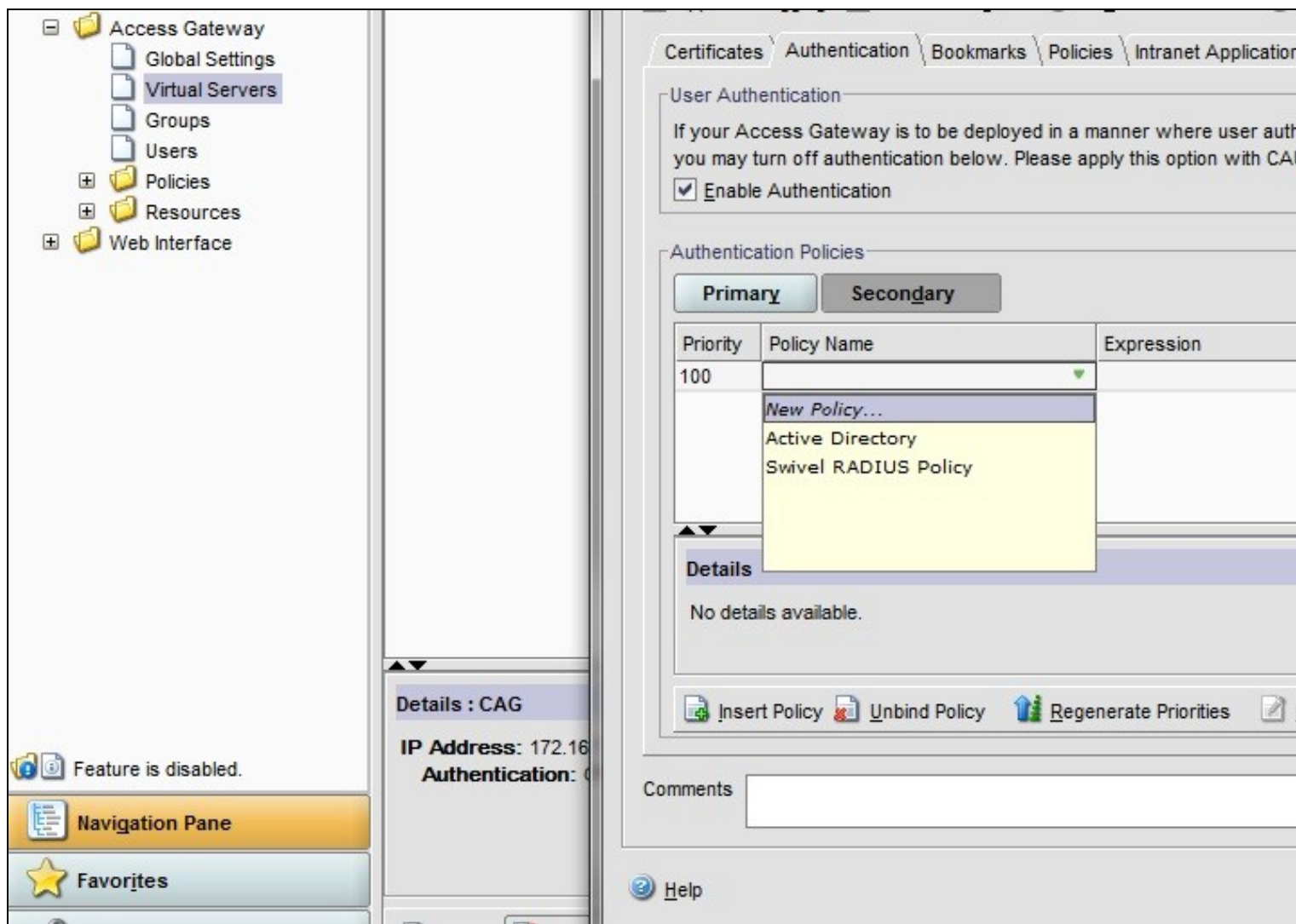
Type: LDAP Request Profile: [Active Directory](#) Rule: [ns_true](#)

Insert Policy

Unbind Policy

Regenerate Priorities

More...



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.

Additional Configuration Options

Login Page Customisation

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

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 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.

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.

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
```

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
```

Customise the login script

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](#)

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).

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
```

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.

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.

Reboot Netscaler to verify files are copied across

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

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 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 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](#)

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](#)

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](#)

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.

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('');  
    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

Welcome
Please log on to continue.



User name:

AD Password:

OTC:

If the incorrect credentials are used then the login should fail

Welcome
Please log on to continue.



User name:

Password 1:

Password 2:



The credentials you typed are incorrect. Please try again or contact your help desk or system administrator.

CITRIX

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.

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

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](#)

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