

Table of Contents

1 Citrix Access Gateway Enterprise Edition 10.....	1
2 Introduction.....	2
3 Prerequisites.....	3
4 Baseline.....	4
5 Architecture.....	5
6 Swivel Configuration.....	6
6.1 Configuring the RADIUS server.....	6
6.2 Enabling Session creation with username.....	6
6.3 Setting up Swivel Dual Channel Transports.....	6
7 Citrix Access Gateway Enterprise Edition Configuration.....	7
7.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.....	7
7.2 Test the RADIUS authentication.....	13
8 Additional Configuration Options.....	14
8.1 Login Page Customisation.....	14
8.2 Additional Login Customisation options.....	15
8.3 Challenge and Response.....	16
8.4 Image Request button displayed when needed.....	16
9 Testing.....	17
10 Uninstall/Removing the integration.....	19
11 Troubleshooting.....	20
12 Known Issues and Limitations.....	21
13 Additional Information.....	22
14 Citrix Access Gateway Enterprise Edition 8.....	23
14.1 Introduction.....	23
14.2 Prerequisites.....	23
14.3 Baseline.....	23
14.4 Architecture.....	23
15 Swivel Configuration.....	24
15.1 Configuring the RADIUS server.....	24
15.2 Enabling Session creation with username.....	24
15.3 Citrix Access Gateway Enterprise Edition Configuration.....	24
15.4 Additional Configuration Options.....	26
15.5 Testing.....	26
15.6 Troubleshooting.....	27
15.7 Known Issues and Limitations.....	27
15.8 Additional Information.....	27
16 Citrix Access Gateway Enterprise Edition 9.....	28
16.1 Introduction.....	28
16.2 Prerequisites.....	28
16.3 Baseline.....	28
16.4 Architecture.....	28
17 Swivel Configuration.....	29
17.1 Configuring the RADIUS server.....	29
17.2 Enabling Session creation with username.....	29
17.3 Citrix Access Gateway Enterprise Edition Configuration.....	29
17.4 Additional Configuration Options.....	35
17.5 Testing.....	37
17.6 Uninstall/Removing the integration.....	39
17.7 Troubleshooting.....	39
17.8 Known Issues and Limitations.....	39
17.9 Additional Information.....	39
18 Citrix Netscaler configuration for Receiver.....	40
19 Introduction.....	41
20 Prerequisites.....	42
21 Netscaler 10.x Configuration for Receiver.....	43
22 Citrix Access Standard Edition Gateway RADIUS authentication.....	47
23 Citrix Access Advanced Edition Gateway RADIUS authentication.....	48
24 Known Issues and Limitations.....	49
25 Citrix Netscaler Gateway 10.x.....	50

Table of Contents

26 Introduction.....	51
27 Prerequisites.....	52
27.1 Note on upgrading the Netscaler.....	52
28 Baseline.....	53
29 Architecture.....	54
30 Swivel Configuration.....	55
30.1 Configuring the RADIUS server.....	55
30.2 Enabling Session creation with username.....	55
30.3 Setting up Swivel Dual Channel Transports.....	55
31 Citrix Netscaler Gateway Configuration.....	56
31.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.....	56
31.2 Citrix Receiver with Netscaler configuration.....	62
32 Additional Configuration Options.....	63
32.1 Netscaler RADIUS Monitor and RADIUS Load Balancer.....	63
32.2 Netscaler SSL Bridge.....	63
32.3 Login Page Customisation.....	65
32.4 Upgrading Netscalers with Custom Pages.....	65
32.5 Customisation Overview.....	66
32.6 Additional Login Customisation options.....	68
32.7 Challenge and Response.....	69
32.8 Image Request button displayed when needed.....	69
33 Testing.....	71
34 Uninstall/Removing the integration.....	73
35 Troubleshooting.....	74
35.1 Error Messages.....	74
36 Known Issues and Limitations.....	75
37 Additional Information.....	76
38 Citrix Netscaler Gateway 11.....	77
39 Introduction.....	78
40 Prerequisites.....	79
40.1 Note on upgrading the Netscaler.....	79
41 Baseline.....	80
42 Architecture.....	81
43 Swivel Configuration.....	82
43.1 Configuring the RADIUS server.....	82
43.2 Enabling Session creation with username.....	82
43.3 Setting up Swivel Dual Channel Transports.....	82
44 Citrix Netscaler Gateway Configuration.....	83
44.1 Citrix NetScaler RADIUS Configuration.....	83
44.2 Citrix Receiver with Netscaler configuration.....	87
45 Additional Configuration Options.....	88
45.1 Netscaler RADIUS Monitor and RADIUS Load Balancer.....	88
45.2 Netscaler SSL Bridge.....	88
45.3 Login Page Customisation.....	94
45.4 Additional Login Customisation options.....	96
45.5 Challenge and Response.....	97
45.6 Image Request button displayed when needed.....	98
46 Testing.....	99
47 Uninstall/Removing the integration.....	100
48 Troubleshooting.....	101
48.1 Error Messages.....	101
49 Known Issues and Limitations.....	102
50 Additional Information.....	103
51 Citrix Netscaler Gateway 12.....	104
52 Introduction.....	105
52.1 Integration Architecture.....	105

Table of Contents

53 Turing Image Integration.....	106
53.1 Rewrite Rules.....	106
53.2 Green Bubble Theme.....	106
53.3 RfWebUI theme.....	107
53.4 X1.....	107
54 Pinpad Integration.....	108
55 Delete previous rules.....	109
56 Adjust Buttons at the login page.....	110
56.1 Edit Password to OTC.....	110
57 Troubleshooting.....	111
58 Netscaler Upgrade from 11 to 12.....	112
59 nFactor ? Customizing UI to Display Images.....	113
60 Backup Configuration.....	114
61 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer.....	115
62 Introduction.....	116
63 Prerequisites.....	117
64 Baseline.....	118
65 Swivel Configuration.....	119
66 Netscaler Configuration.....	120
66.1 Create a Swivel Radius Monitor.....	120
66.2 Create Entries for the Swivel RADIUS Servers.....	123
66.3 Create a Swivel Load Balance Service Group.....	125
66.4 Create A Virtual Server.....	128
66.5 Netscaler RADIUS configuration.....	131
67 Testing.....	132
68 Known Issues.....	133
69 Troubleshooting.....	134

1 Citrix Access Gateway Enterprise Edition 10

2 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.

3 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](#).

4 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.

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.

6 Swivel Configuration

6.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

6.2 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.

6.3 Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

7 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.

7.1 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

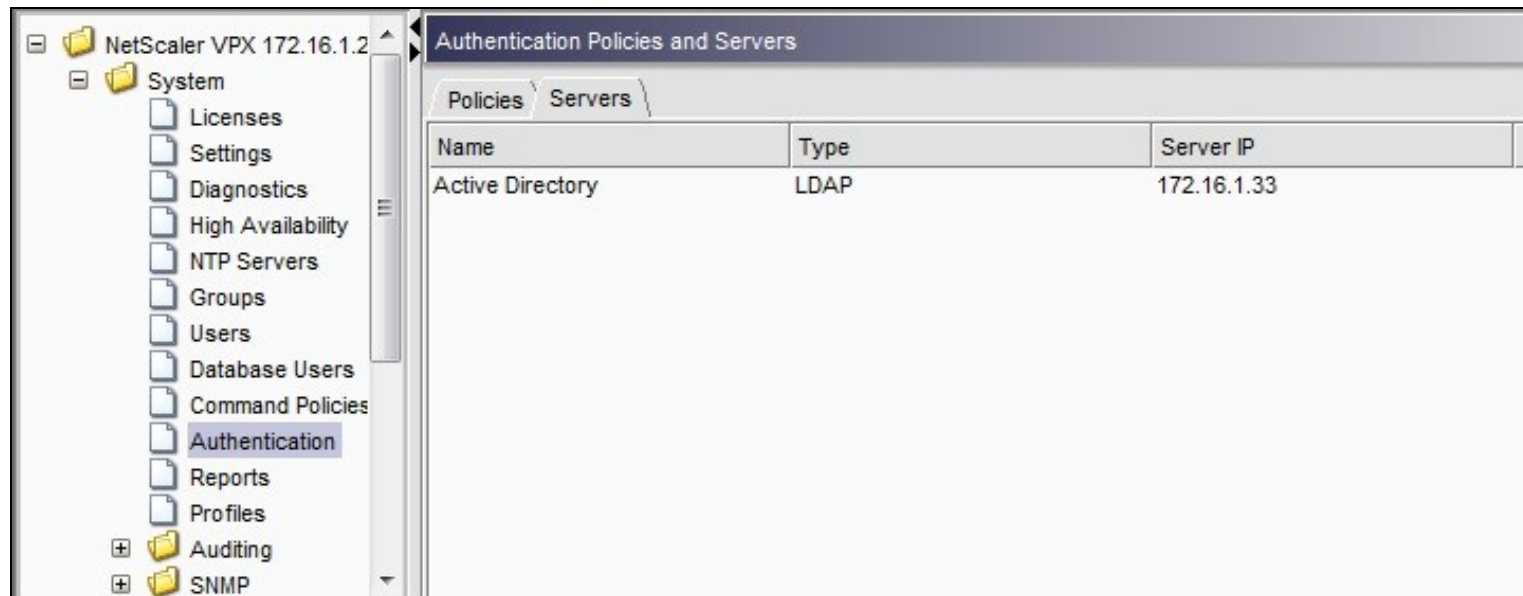
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix 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.



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

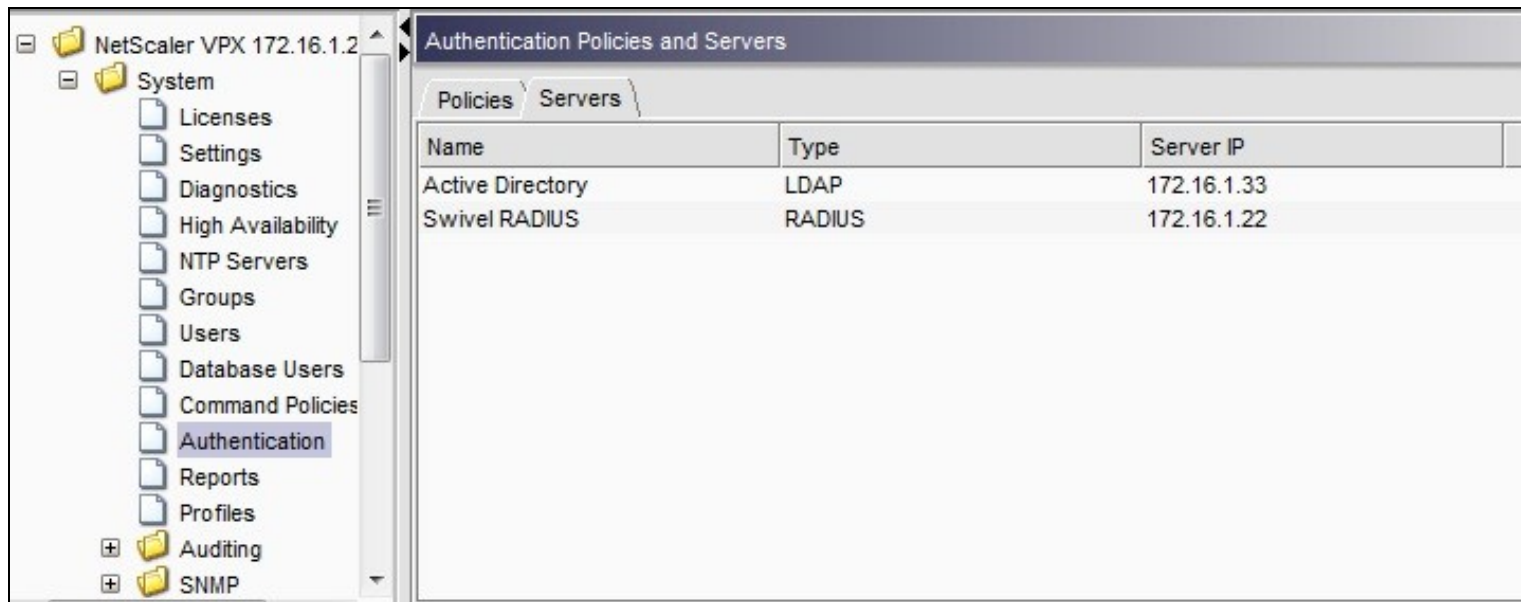
OFF

Help

Quick Link

Create

Close



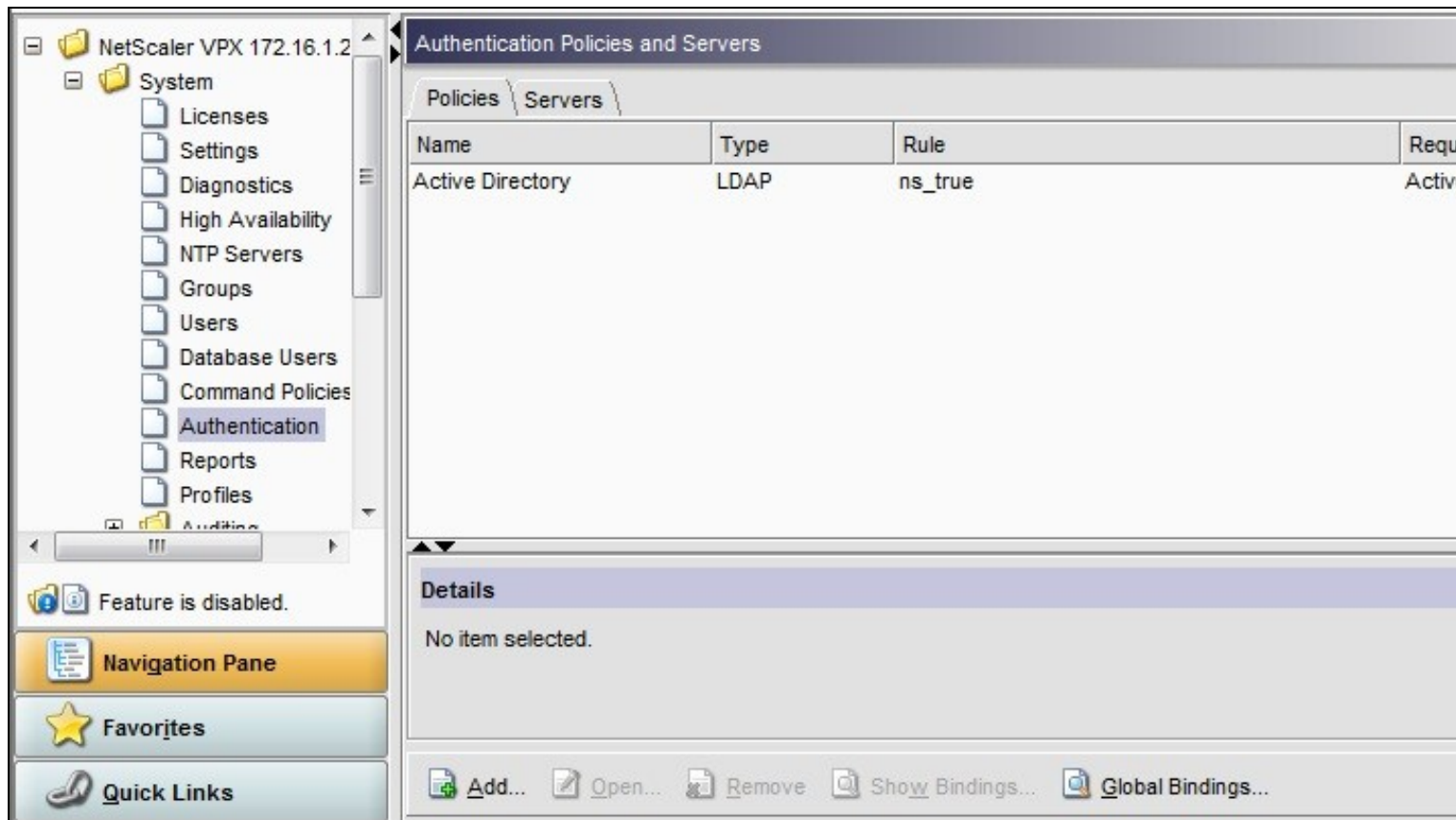
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:



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*


Authentication Type

Server  **New...**  **Modify...**




Expression

Expression

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

Named Expressions  **Add Expression**

Preview Expression

 **Help**  **OK**  **Close**

Create Authentication Policy

Name*

Authentication Type

Server [New...](#) [Modify...](#)

Expression

Expression
ns_true

Match Any Expression ☐ AND ☐ OR

Named Expressions [+ Add Expression](#)

Preview Expression

[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

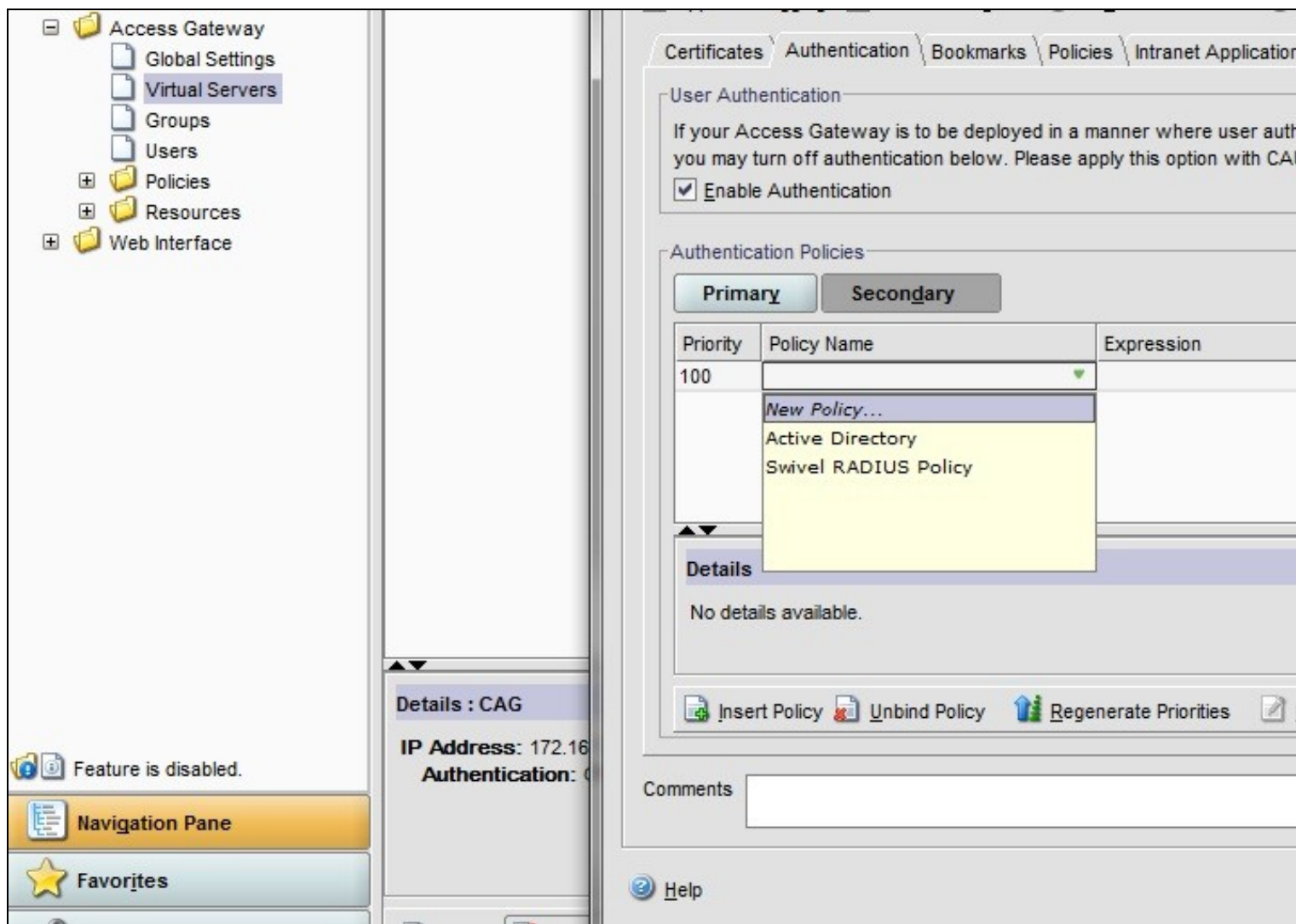
Type: LDAP Request Profile: [Active Directory](#) Rule: [ns_true](#)

Insert Policy

Unbind Policy

Regenerate Priorities

More...



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.

8 Additional Configuration Options

8.1 Login Page Customisation

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

8.1.1 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 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.

8.1.2 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
```

8.1.3 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
```

8.1.4 Customise the login script

8.1.4.1 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](#)

8.1.5 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).

8.1.5.1 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
```

8.1.6 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.

8.1.7 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.

8.1.8 Reboot Netscaler to verify files are copied across

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

8.2 Additional Login Customisation options

8.2.1 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%;"
```

8.2.2 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".

8.2.3 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](#)

8.2.4 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](#)

8.2.5 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](#)

8.3 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.

8.4 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('');
        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>');
    }
}
```

9 Testing

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



The screenshot shows a login interface with a dark blue background. At the top left, there is a circular icon with a white padlock. To the right of the icon, the text "Welcome" is displayed in a bold, white font, followed by "Please log on to continue." in a smaller, white font. Below this, there are three input fields: "User name:" with the value "graham", "AD Password:" with four black dots, and "OTC:" with four black dots. To the right of the "OTC:" field, there are two buttons: "Get Image" and "Log On". Below the input fields, there is a Turing image, which is a grid of numbers. The grid has 10 columns and 2 rows. The top row contains the numbers 1 through 0. The bottom row contains the numbers 5, 7, 2, 4, 9, 6, 8, 0, 1, 3.

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



The screenshot shows the same login interface as the previous one, but the "OTC:" field is now filled with four black dots and a cursor is visible at the end of the field. The "Get Image" and "Log On" buttons are still present.

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



10 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.

11 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

12 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](#)

13 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

14 Citrix Access Gateway Enterprise Edition 8

14.1 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.

14.2 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

14.3 Baseline

PINsafe 3.5

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

14.4 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.

15 Swivel Configuration

15.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

15.2 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.

15.2.1 Setting up PINsafe Dual Channel Transports

See [Transport Configuration](#)

15.3 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](#)

15.3.1 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 regularly 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:

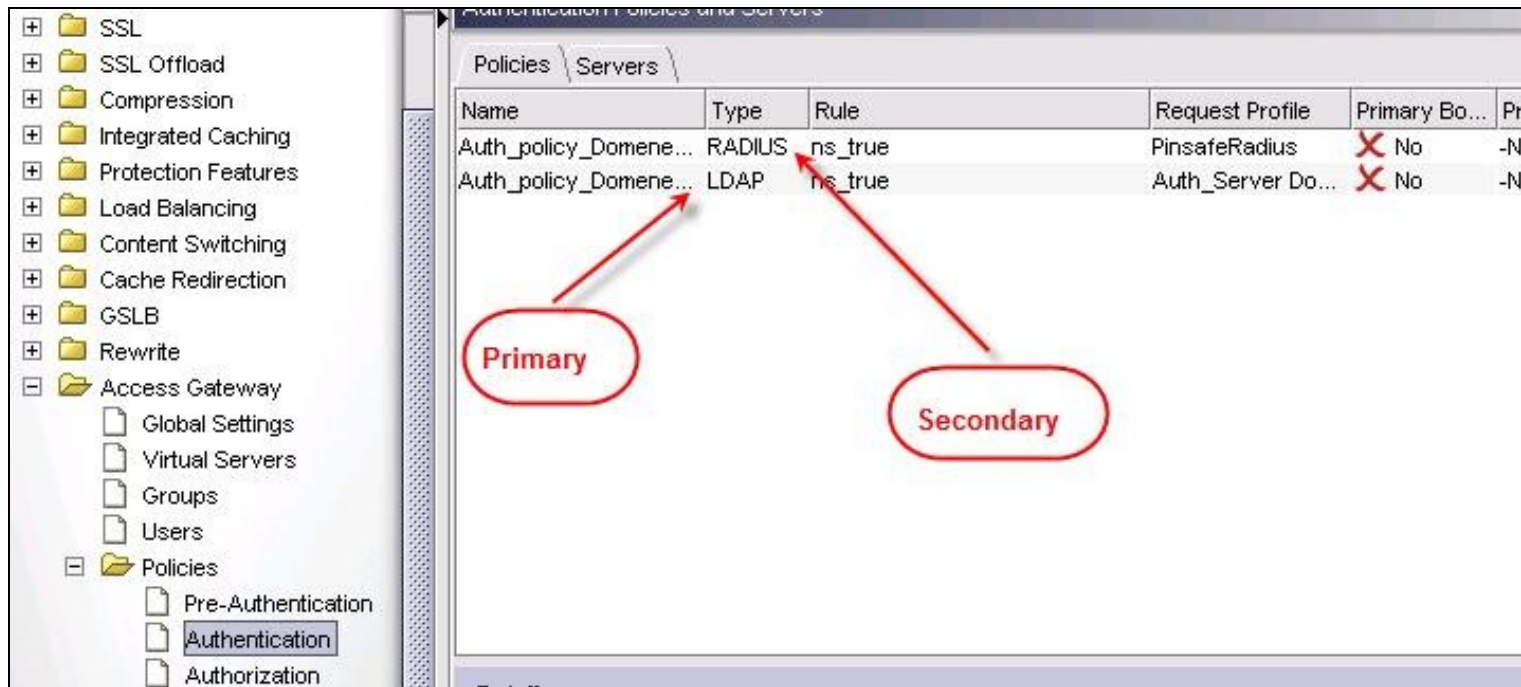
```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod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

15.3.2 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

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.



Configure Authentication Server

Name* PinsafeRadius

Authentication Type RADIUS

Server

IP Address Port 1812 Time-out (seconds) 3

Details

Secret Key* Confirm Secret Key*

NAS ID

☐ Enable NAS IP address extraction

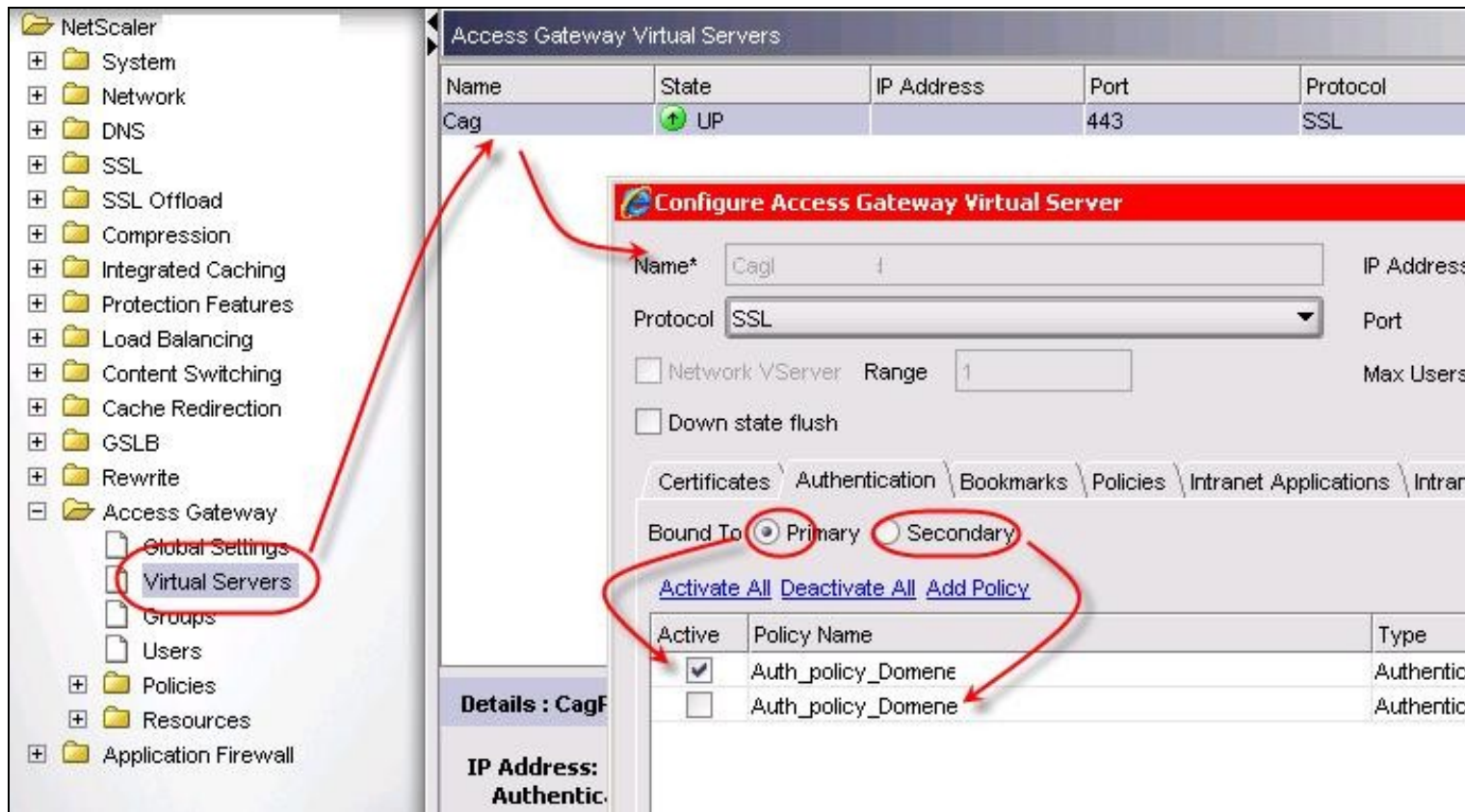
Group Vendor Code Attribute Value Prefix CTXSUserGroups=

Group Attribute Type Separator ;

Vendor Identifier Attribute Type

Password Encoding pap Accounting OFF

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.



15.4 Additional Configuration Options

15.4.1 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.1 supports RADIUS Challenge and Response

15.4.2 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('');
        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>');
    }
}
```

15.5 Testing

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

Log In

User Name: test

One-Time Code:

GetImage

Login

1234567890

3214967805

15.6 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Image from PINsafe server absent

15.7 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 [\[1\]](#)

15.8 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

16 Citrix Access Gateway Enterprise Edition 9

16.1 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.

16.2 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](#).

16.3 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

16.4 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.

17 Swivel Configuration

17.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

17.2 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.

17.2.1 Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

17.3 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.

17.3.1 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

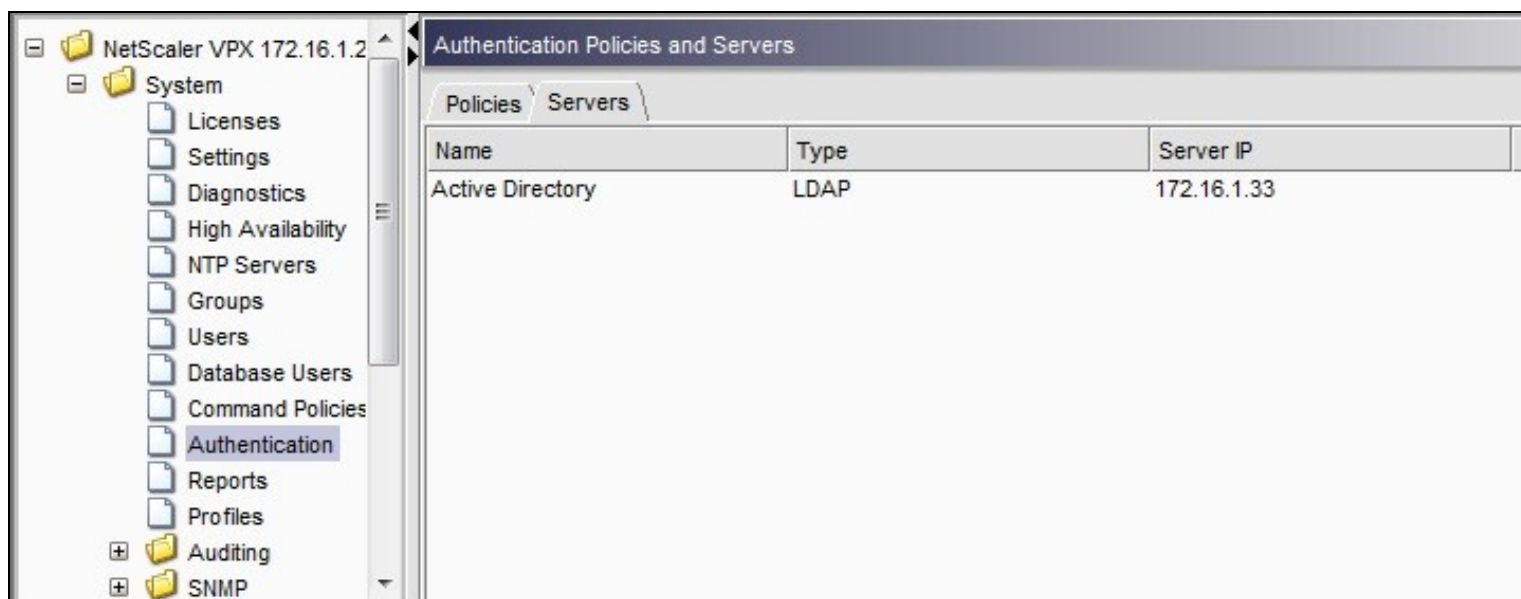
Authentication type RADIUS

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

Group Prefix CTXUserGroups=

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

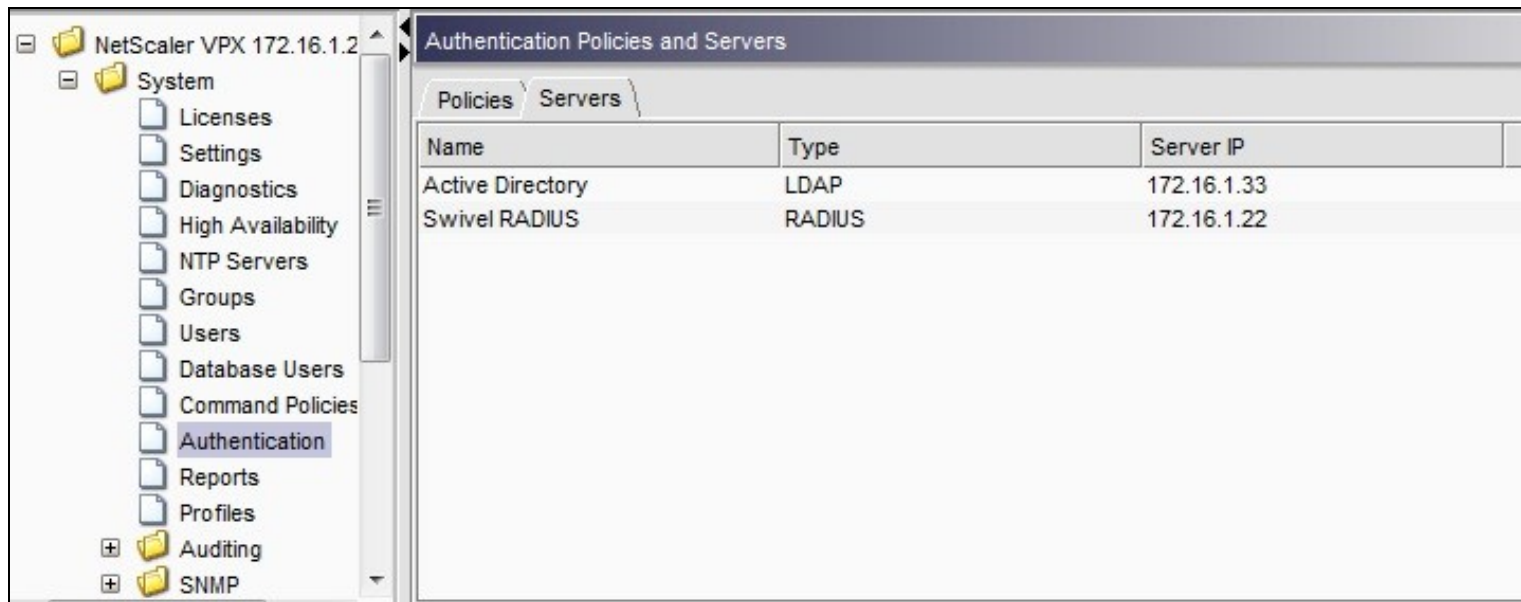
Help

Quick Link

Create

Close

30



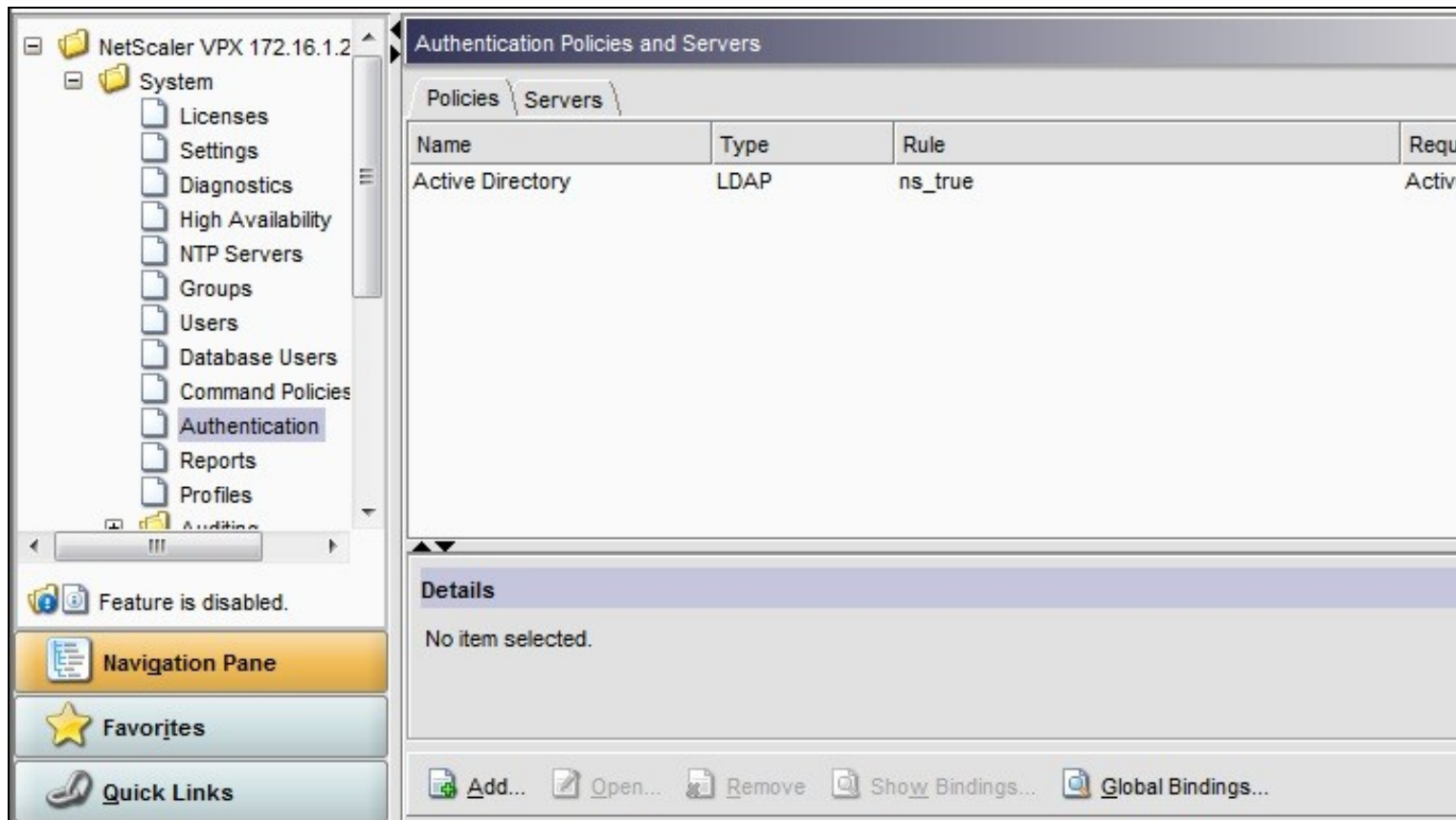
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:



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*


Authentication Type

Server  **New...**  **Modify...**




Expression

Expression

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

Named Expressions  **Add Expression**

Preview Expression

 **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

CertificatesAuthenticationBookmarksPoliciesIntranet 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

PrimarySecondary

Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

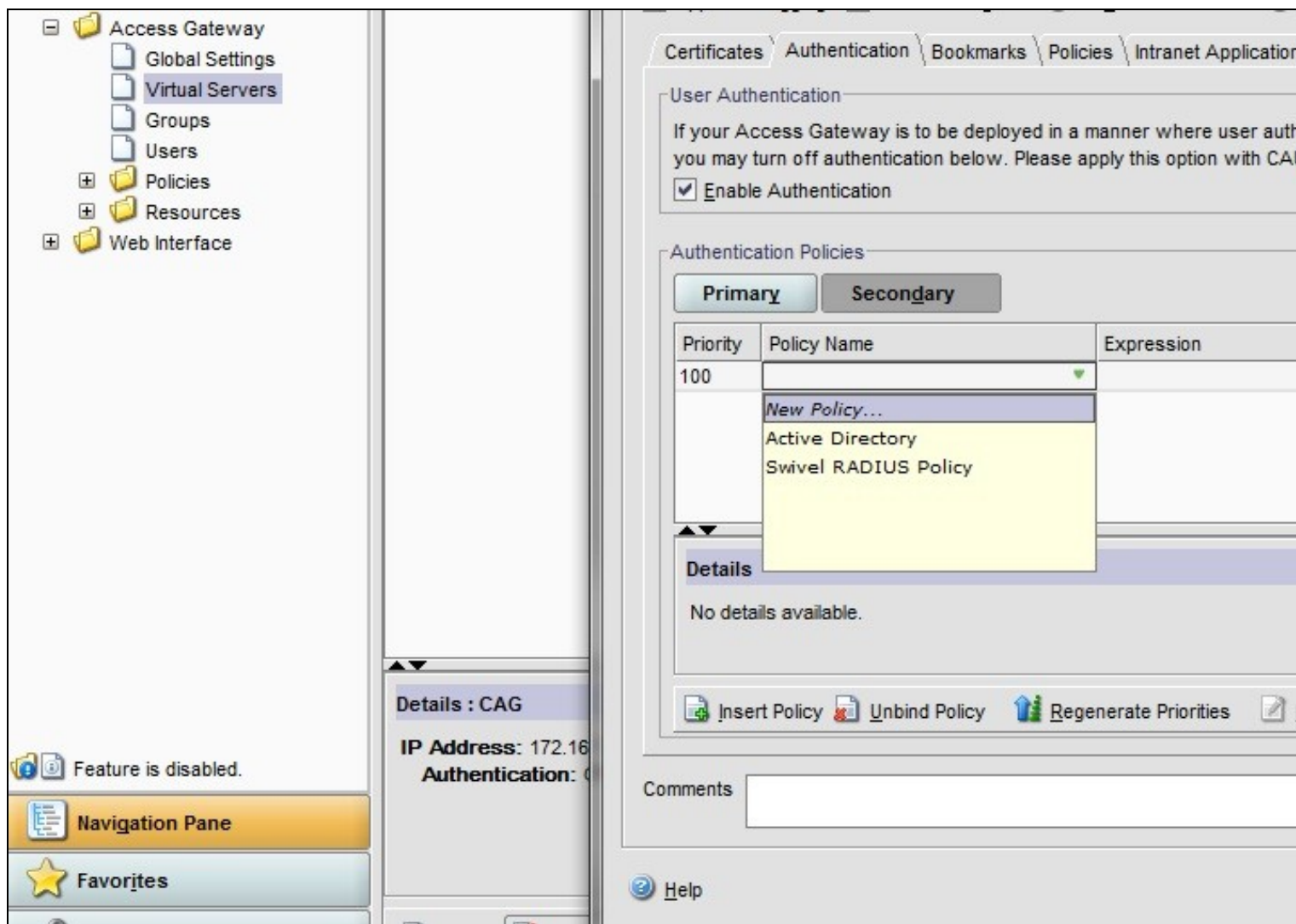
Type: LDAPRequest Profile: Active DirectoryRule: ns_true

Insert Policy

Unbind Policy

Regenerate Priorities

Mo



17.4 Additional Configuration Options

17.4.1 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.

17.4.1.1 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".

17.4.1.2 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";
```

17.4.1.3 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
```

17.4.1.4 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](#)

17.4.2 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.

17.4.3 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('');  
        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>');  
    }  
}
```

17.5 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

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



17.6 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.

17.7 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.

17.8 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 [\[1\]](#)

17.9 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

18 Citrix Netscaler configuration for Receiver

19 Introduction

Citrix Receiver is a lightweight software client that allows access to virtual desktops and apps including Windows, Web or SaaS apps on any PC, Mac, netbook, tablet or smartphone.

For further information on using Receiver see [Citrix Receiver](#)

20 Prerequisites

Citrix receiver Client

Swivel Appliance or Server

Citrix Netscaler

21 Netscaler 10.x Configuration for Receiver

To allow Primary and Secondary Authentication using Citrix receiver clients the following policies are required. On the Netscaler Access Gateway select Netscaler Gateway then Virtual Servers, click on the required server then Open. Click on the Authentication tab, and create a policy for RADIUS authentication and a Policy for LDAP authentication for the Primary and Secondary authentication. The below assumes that the Primary authentication server is LDAP and the secondary authentication server is RADIUS for methods other than Receiver authentication.

Configure NetScaler Gateway Virtual Server

Name*

citrix

Protocol*

SSL

☐ Network VServer

Range

1

Failed Login Timeout

60

☒ SmartAccess Mode

☐ Basic Mode

☐ AppFlow Logging

☐ Down state flush

☒ Double Hop

IP Address*

Port*

Max Users

Max Login Attempts

Certificates

Authentication

Bookmarks

Policies

Intranet Applications

Intranet IPs

Published Applications

Advanced

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☒ Enable Authentication

Authentication Policies

Primary

Secondary

Group Extraction

Priority	Policy Name	Expression	Policy
90	policy_RADIUS_primary	REQ.HTTP.HEADER User-Agent CONTAINS Receiver	S
100	policy_LDAP_primary	REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver	W

Details

No item selected.

Insert Policy

Unbind Policy

Regenerate Priorities

Comments

Help

Configure NetScaler Gateway Virtual Server

Name* IP Address*

Protocol* Port*

☐ Network VServer Range Failed Login Timeout Max Users

☒ SmartAccess Mode ☐ Basic Mode ☐ AppFlow Logging ☐ Down state flush ☒ Double Hop Max Login Attempts

Certificates Authentication Bookmarks Policies Intranet Applications Intranet IPs Published Applications Advanced

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☐ Enable Authentication

Authentication Policies

Primary Secondary Group Extraction

Priority	Policy Name	Expression	P
90	policy_RADIUS_secondary	REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver	S
100	policy_LDAP_secondary	REQ.HTTP.HEADER User-Agent CONTAINS Receiver	W

Details

No item selected.

Insert Policy Unbind Policy Regenerate Priorities

Comments

Help

To create the Policy, click on Insert Policy, then from the drop down Tab below Policy name, click on Insert Policy and enter the following:

Name Name of the Policy

Authentication Type Usually LDAP and the RADIUS authentication servers

Server The authentication server for the above

Under Expression click on Add and select the following:

Expression Type General

Flow Type REQ

Protocol HTTP

Qualifier Header

Operator CONTAINS or NOTCONTAINS

Value Receiver

Header Name

Click on OK then create. Double click on the Priority to set the priority to 90 or 100 as appropriate.

Create policies for each as below.

Receiver settings for Netscaler 10.0 and 10.1

Authentication Server	Protocol	Priority	Value
Primary	LDAP	90	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
Primary	RADIUS	100	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
Standby	LDAP	90	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
Standby	RADIUS	100	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver

Multiple Authentication servers can be created by multiple entries of the same priority, such as AD servers.

Receiver settings for Netscaler 10.5

Authentication Server	Protocol	Priority	Value
Primary	LDAP	90	(REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS) (REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS HTML5)
Primary	RADIUS	100	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
Standby	LDAP	90	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
Standby	RADIUS	100	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver (REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS HTML5)

Configure Authentication Policy

Name*

policy_RADIUS_primary

Authentication Type

RADIUS

Server

Swivel RADIUS

New...

Modify...

Expression

Expression

REQ.HTTP.HEADER User-Agent CONTAINS Receiver

Match Any Expression

Add...

Modify...

Remove

AND

OR

(+)+

(-)-

Named Expressions

General

Client is from different geographical...

Replace Expression

Preview Expression

ns_farclient

Help

OK

Close

Modify Expression

Expression Type

General

Flow Type

REQ

Protocol

HTTP

Qualifier

HEADER

Operator

CONTAINS

Value*

Receiver

Header Name*

User-Agent

Length

Offset

0

Help

OK

Close

46

22 Citrix Access Standard Edition Gateway RADIUS authentication

The following article describes adding RADIUS authentication to the Citrix Access Standard Edition for Citrix Receiver. The RADIUS authentication needs to be set as the primary authentication and AD as the Secondary authentication.

<http://support.citrix.com/article/CTX121093>

23 Citrix Access Advanced Edition Gateway RADIUS authentication

The following article describes adding RADIUS authentication to the Citrix Access Advanced Edition for Citrix Receiver.

<http://cdn.ws.citrix.com/wp-content/uploads/2009/08/iphone-receiver-admin.pdf>

24 Known Issues and Limitations

It has been observed by our customers that the Citrix Receiver only launches successfully on the Android platform when accessing links via the Mozilla Firefox browser (at the time this article was written)

25 Citrix Netscaler Gateway 10.x

26 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 Servers 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.

27 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](#).

27.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used [upgrading Netscalers with Custom Pages](#)

28 Baseline

Tested with Swivel 3.9.6

Citrix Netscaler Gateway NS10.1 Build 121.10

Citrix Netscaler Gateway NS10.5

29 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.

30 Swivel Configuration

30.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

30.2 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.

30.3 Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

31 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.

31.1 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

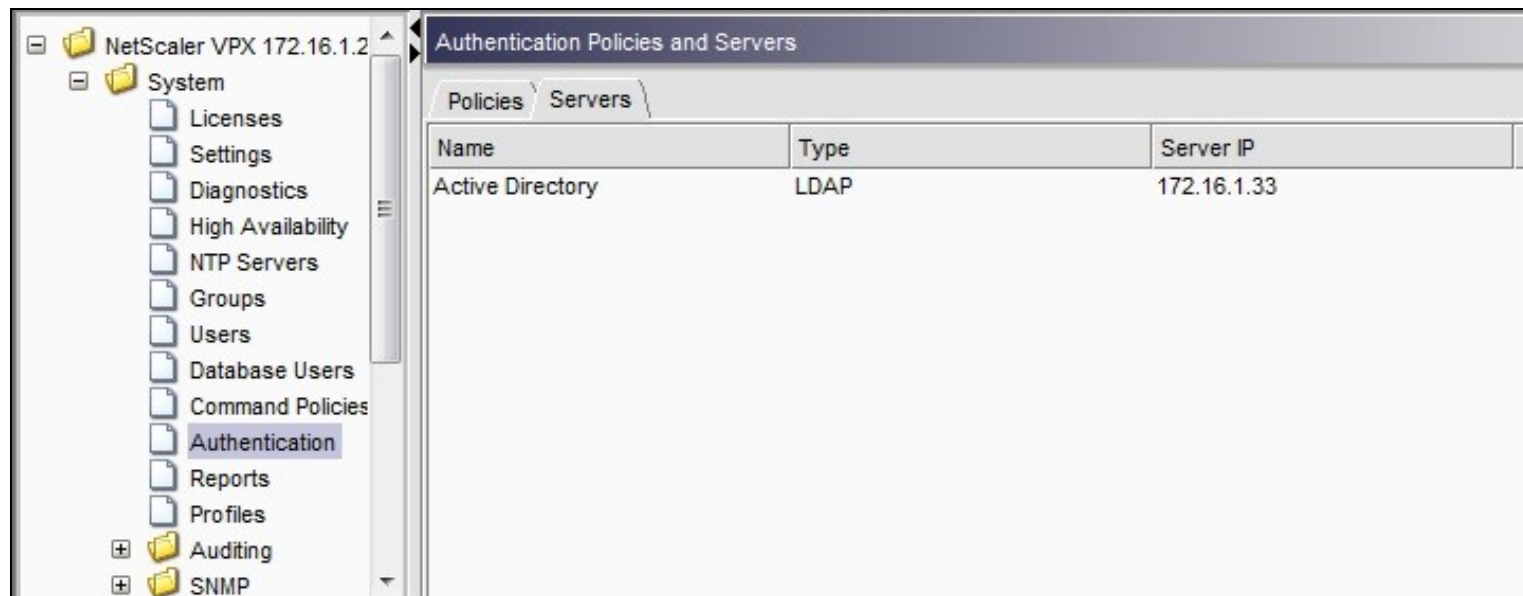
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix 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.



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

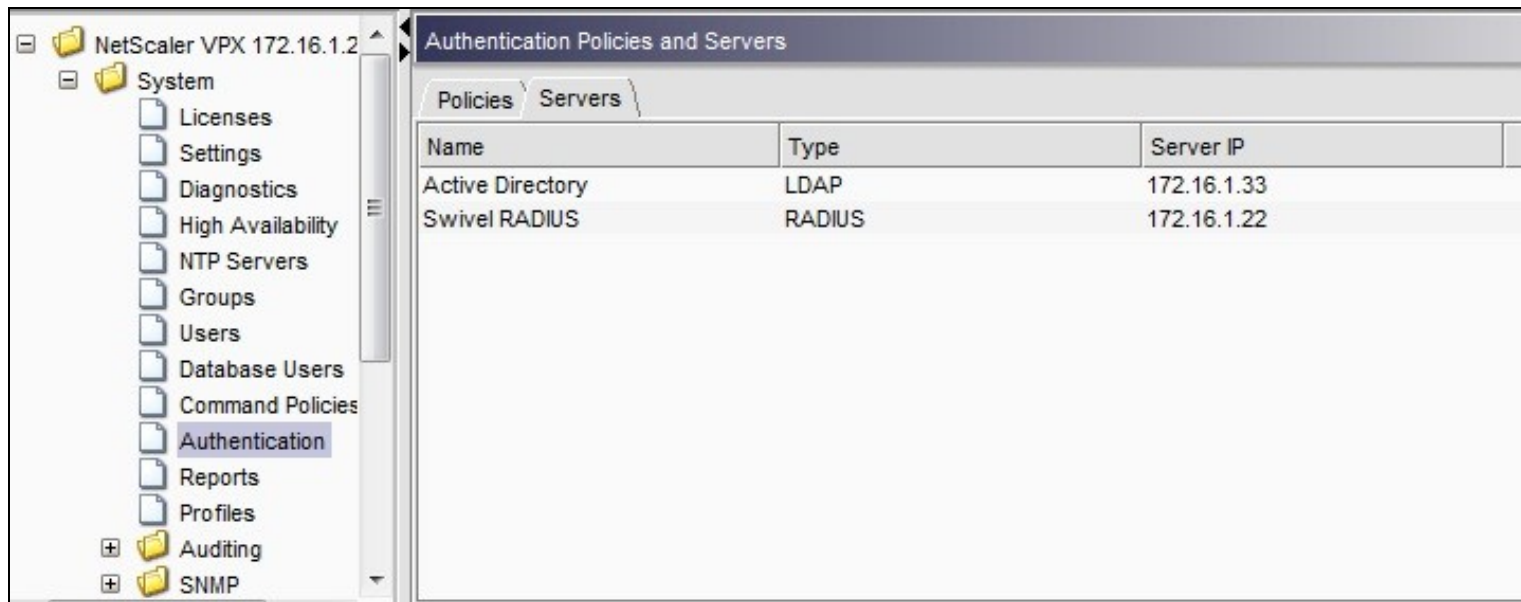
OFF

Help

Quick Link

Create

Close



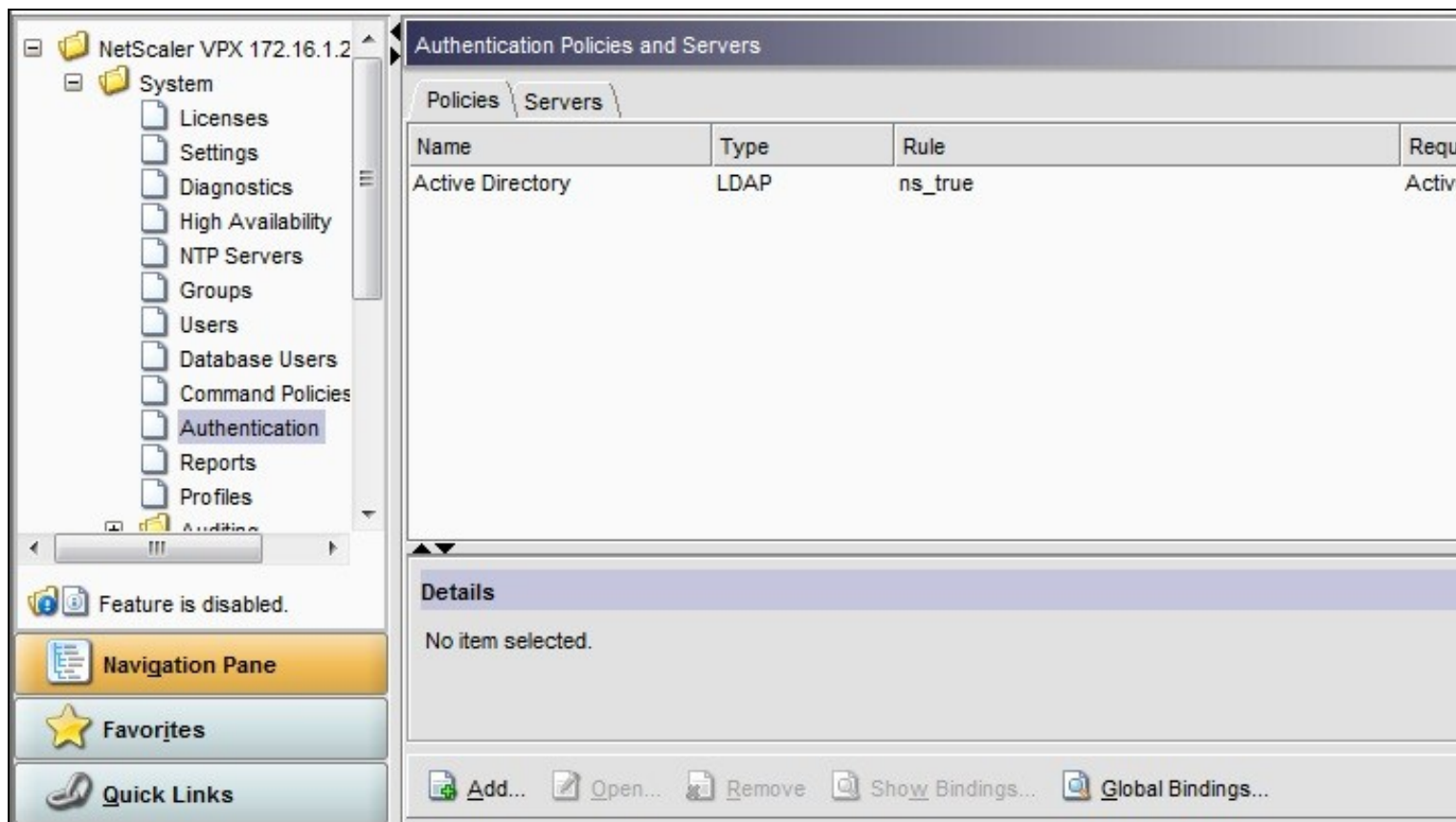
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:



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*


Authentication Type

Server  **New...**  **Modify...**




Expression

Expression

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

Named Expressions  **Add Expression**

Preview Expression

 **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

CertificatesAuthenticationBookmarksPoliciesIntranet 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

PrimarySecondary

Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

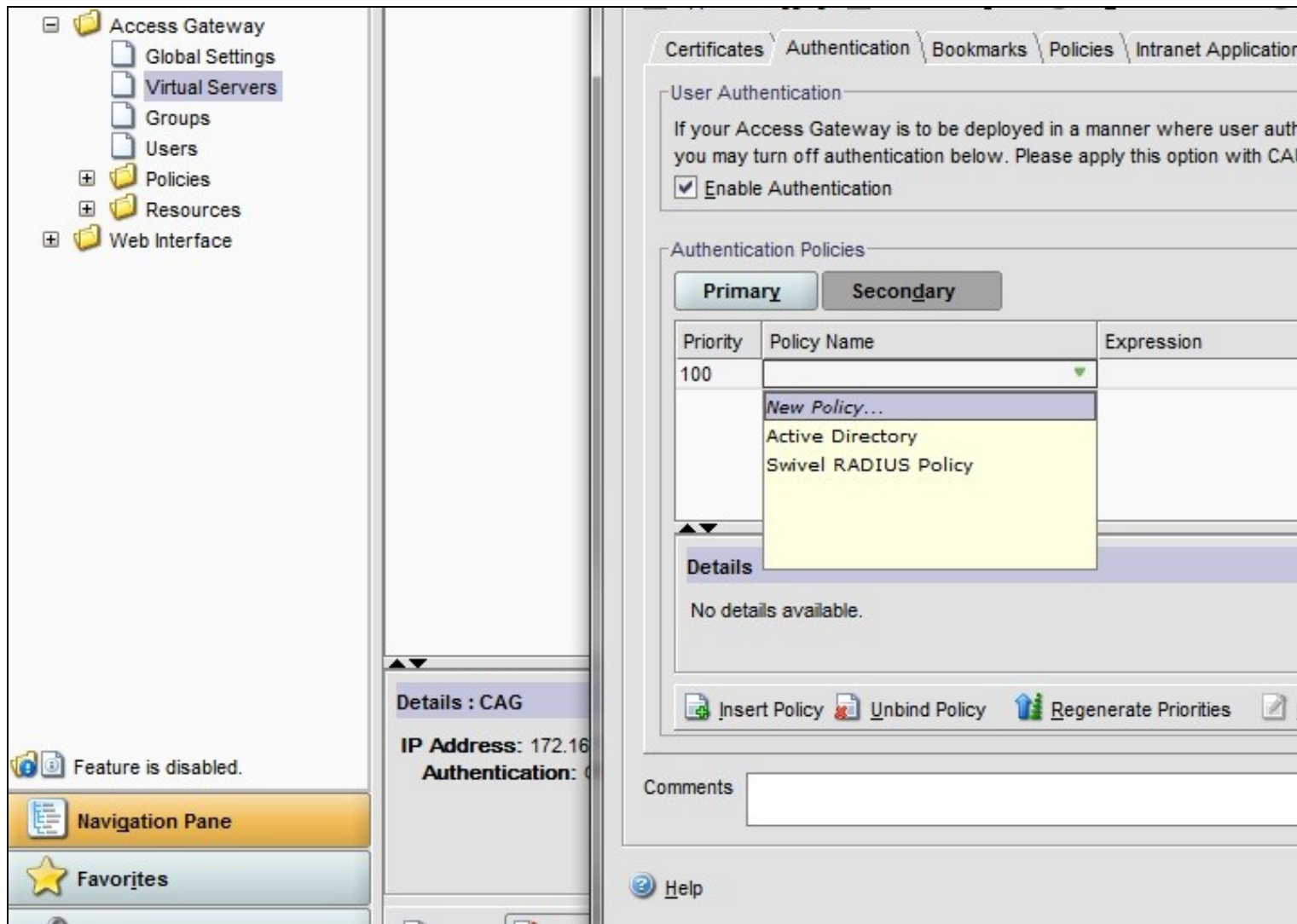
Type: LDAPRequest Profile: Active DirectoryRule: ns_true

Insert Policy

Unbind Policy

Regenerate Priorities

Mo



31.2 Citrix Receiver with Netscaler configuration

See [Citrix Netscaler configuration for Receiver](#)

32 Additional Configuration Options

32.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See [Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer](#)

32.2 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 Address 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**

Create Virtual Server (Load Balancing)

Name*
Swivel-SSL-Bridge

Protocol*
SSL_BRIDGE

☐ Network VServer Range
1

☒ Directly Addressable

☒ State

☒ AppFlow Logging

☐ Enable DNS64

☐ Bypass AAAA Requests

☒ IP Address Based

☐ IP Pattern Based

IP Address*
10 . 10 . 10 . 10

Port*
8443

Traffic Domain ID

Services

Service Groups

Policies

Method and Persistence

Advanced

Profiles

SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dr
<input checked="" type="checkbox"/>	Swivel_8443	192.168.12.111	8443	SSL_BRID...	UP	1	

Add...

Open...

Remove

Comments

Help

Create

Click Add and enter the required details.

Create Service

Service Name*Swivel_8443Server*192.168.12.111

Protocol*SSL_BRIDGEPort*443

Traffic Domain

☒ Enable ServiceNumber of Active Clients

Change State☒ Enable Health Monitoring☒ AppFlow Logging

MonitorsPoliciesProfilesAdvancedSSL Settings

Available

Monitors

arp

nd6

ping

http

tcp-ecv

http-ecv

udp-ecv

dns

ftp

tcps

https

Add >

< Remove

Configured

Monitors	Weight	State	Passive
tcp	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Comments

Help

CreateClose

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.

System

AppExpert

Traffic Management

Load Balancing

Virtual Servers

Services

Service Groups

Monitors

Metric Tables

Servers

Persistency Groups

Content Switching

DNS

SSL

SSL Offload

Optimization

Security

NetScaler Gateway

Show Unlicensed Features

NetScaler > Traffic Management > Load Balancing

Add...

Open..

Remove

Action

Name	State	Effective State
Swivel-SSL-Bridge		

Create Virtual Server (Load Balancing)

Name*Swivel-SSL-Bridge

Protocol*SSL_BRIDGE

☐ Network VServer
 Range 1

☒ Directly Addressable
 ☒ State

☐ Enable DNS64
 ☐ Bypass AAAA

Services

Service Groups

Pol

[Activate All](#)
[Deactivate All](#)

Active	Service Name
<input type="checkbox"/>	Swivel_8443

Add...

Open...

Remove

Comments

Help

32.3 Login Page Customisation

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

32.4 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.

32.5 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.

32.5.1 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
```

32.5.2 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
```

32.5.3 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.

32.5.3.1 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](#)

32.5.4 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).

32.5.4.1 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
```

32.5.5 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

32.5.6 Create the boot archive file

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

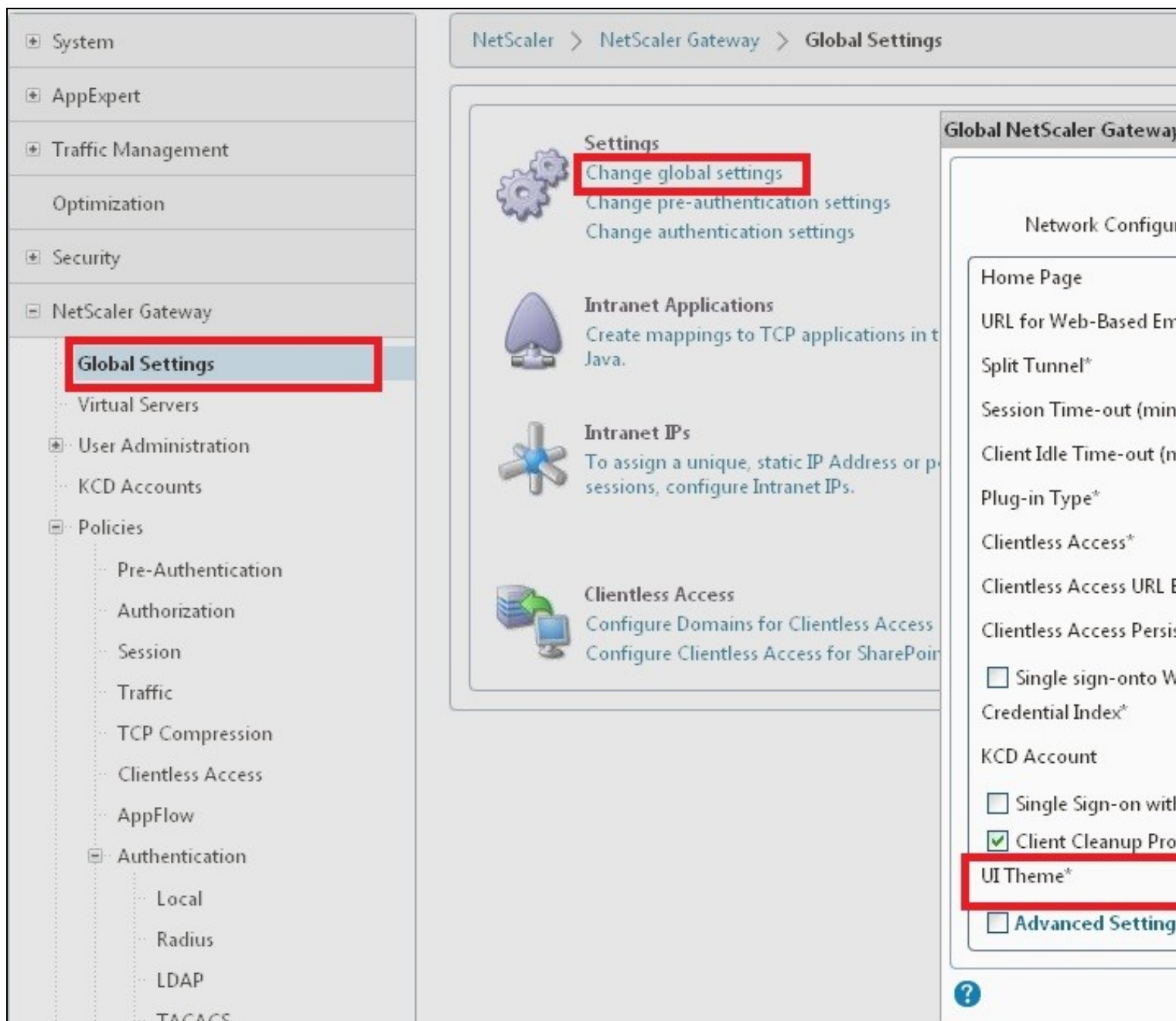
This should create the customtheme.tar.gz file used at boot time, and list all the files used.

32.5.7 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 default index.html, and if a new custom page is required, then the custom index.html will need to be copied back.



32.5.8 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.

32.6 Additional Login Customisation options

32.6.1 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%;"
```

32.6.2 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".

32.6.3 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](#)

32.6.4 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](#)

32.6.5 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](#)

32.7 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 function code:

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

32.8 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('');
    }
}
```



```

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>');
}
}

```

33 Testing

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



The screenshot shows a login interface with a dark blue background. At the top left, there is a circular icon with a white padlock. To the right of the icon, the text "Welcome" is displayed in a bold, white font, followed by "Please log on to continue." in a smaller, white font. Below this, there are three input fields: "User name:" with the value "graham", "AD Password:" with four black dots, and "OTC:" with four black dots. To the right of the "OTC:" field, there are two buttons: "Get Image" and "Log On". Below the input fields, there is a Turing image, which is a grid of numbers. The grid has 10 columns and 2 rows. The top row contains the numbers 1 through 0. The bottom row contains the numbers 5, 7, 2, 4, 9, 6, 8, 0, 1, 3.

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



The screenshot shows the same login interface as the previous one, but the "OTC:" field is now filled with the numbers "5724968013". The "Get Image" button is still visible, but it is not being clicked. The "Log On" button is also visible.

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



34 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.

35 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.

35.1 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;"><span id="User_name" class="CTXMSAM_LogonFont"></span></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 prevent 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 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.

36 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 [\[1\]](#)

37 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

38 Citrix Netscaler Gateway 11

39 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 Servers 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](#).

40 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.

40.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used [upgrading Netscalers with Custom Pages](#)

41 Baseline

Tested with Swivel 3.10.4

Citrix Netscaler Gateway NS11.0 Build 62.0

42 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.

43 Swivel Configuration

43.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

43.2 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.

43.3 Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

44 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.

44.1 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

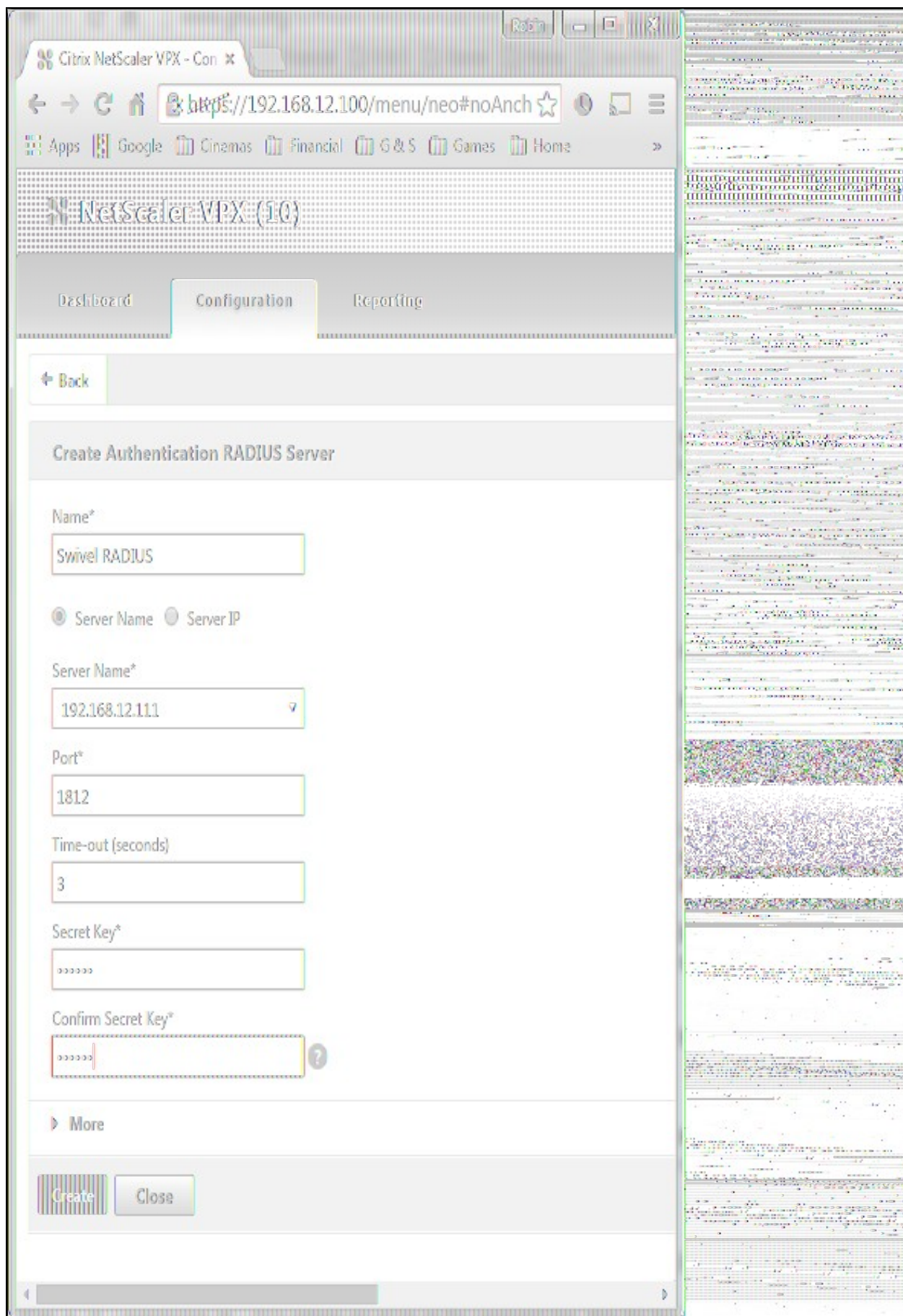
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix 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 (10) HA Status ● Not Configured

Dashboard Configuration Reporting

System

- Licenses
- Settings
- Diagnostics
- High Availability
- NTP Servers
- Reports
- Profiles
- + Partition Administration
- + User Administration
- Authentication
 - Local
 - RADIUS**
 - LDAP
 - TACACS
- + Auditing
- + SNMP
- + AppFlow
- + Cluster
- + Network
- + Web Interface
- + WebFront
- Backup and Restore
- + AppExpert

NetScaler > System > Authentication > RADIUS > Servers

Policies Servers

Add Edit Delete

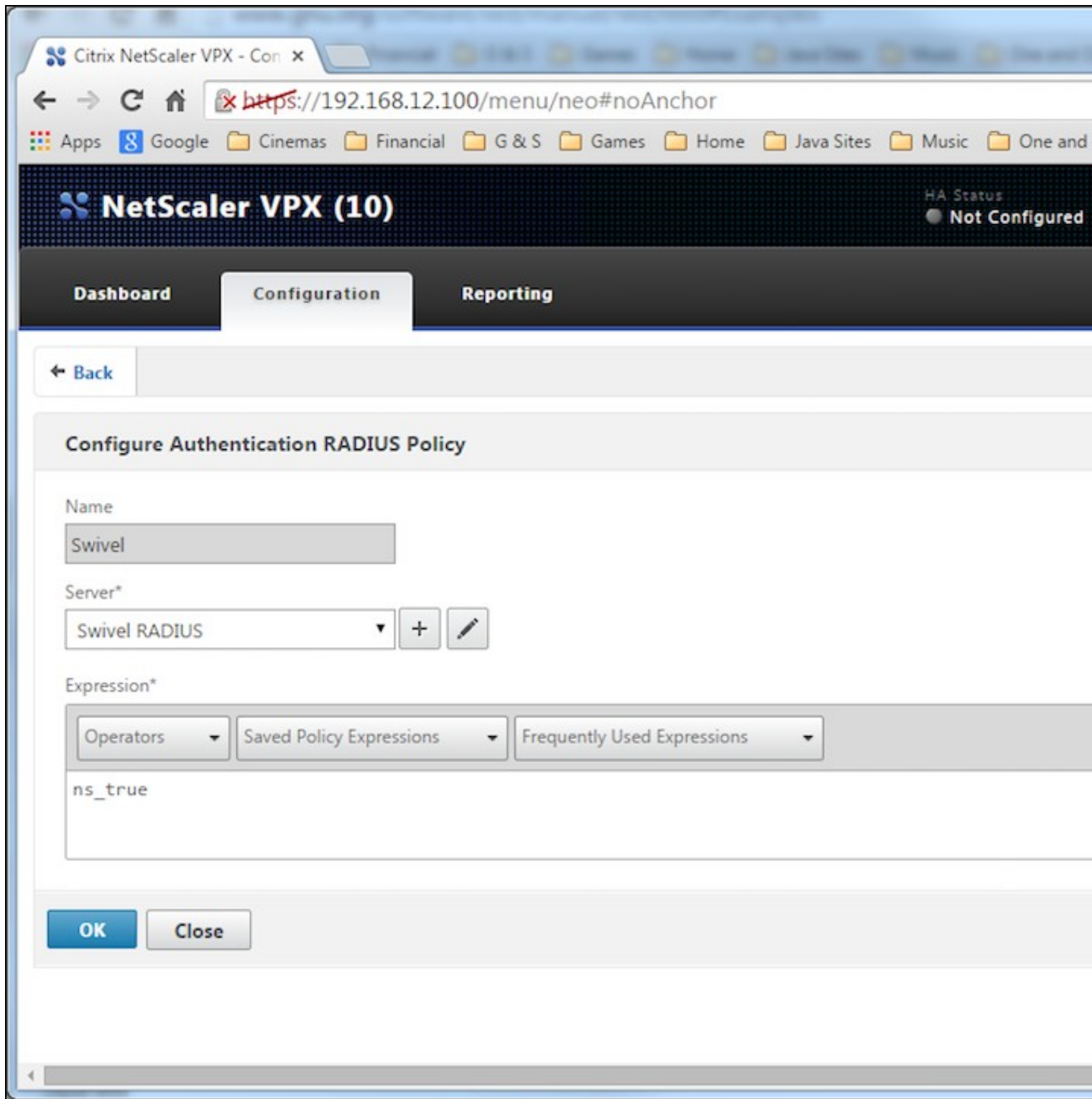
Name	Server Name	IP Address
Swivel RADIUS		192.168.12.111

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.

Citrix NetScaler VPX - Con x

← → ↻ 🏠 <https://192.168.12.100/menu/neo#noAnchor>

Apps Google Cinemas Financial G & S Games Home Java Sites Music One and One Reference Shopping

← Back

VPN Virtual Server

Basic Settings

Name	Demo	Maximum Users	0
IPAddress	10.40.242.185	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	Up	ICA Only	true
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	true	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificates

1 Server Certificate

No CA Certificate

Authentication

Primary Authentication

1 LDAP Policy

Secondary Authentication

1 RADIUS Policy

Profiles

Net Profile -

44.2 Citrix Receiver with Netscaler configuration

See [Citrix Netscaler configuration for Receiver](#)

45 Additional Configuration Options

45.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See [Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer](#)

45.2 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.

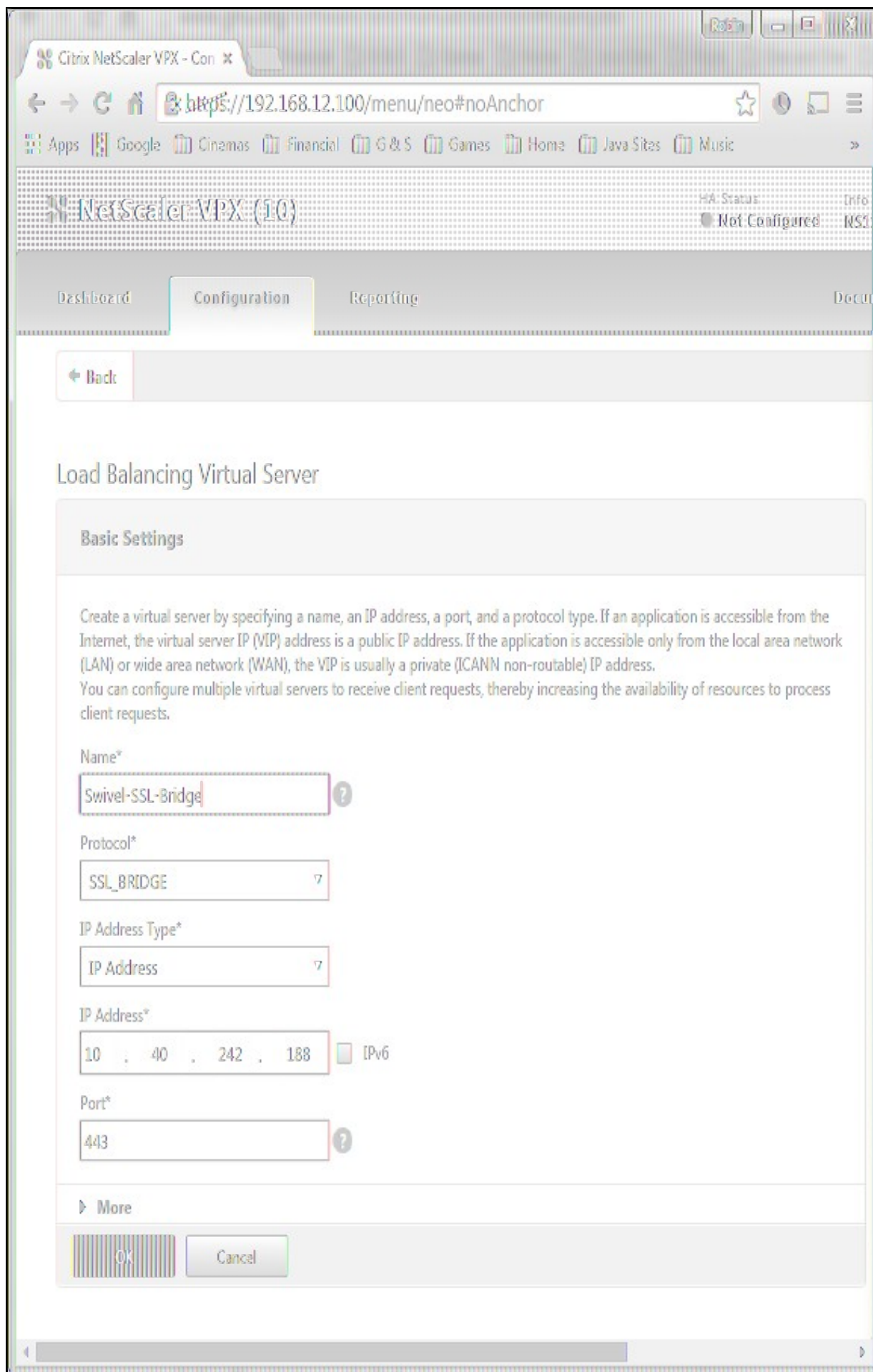
Name Name of the SSL Bridge

Protocol select SSL_Bridge

Select IP Address Based

IP address Enter the public IP Address

Port Enter the internet-facing port number, usually 443



Citrix NetScaler VPX - Con x

← → ↻ 🏠 <https://192.168.12.100/menu/neo#noAnchor>

📁 Apps 📁 Google 📁 Cinemas 📁 Financial 📁 G & S 📁 Games 📁 Home 📁 Java Sites 📁 Music 📁 One and One 📁 Reference 📁 Shopping 📁 T

NetScaler VPX (10) HA Status: Not Configured Info: NS11.0 62

Dashboard Configuration Reporting Documentation

+ System

+ AppExpert

— Traffic Management

— Load Balancing

Virtual Servers

Services

Service Groups

Monitors

Metric Tables

Servers

Persistency Groups

+ Content Switching

+ DNS

+ SSL

NetScaler > Traffic Management > Load Balancing > Virtual Servers

Add Edit Delete Enable Disable Statistics Action

Name	State	Effective State	IP Address	Port	Protocol	Method
▶ Swivel-SSL-Bridge	Up	Up	10.40.242.188	8443	SSL_BRIDGE	LEASTCONNECT
▶ 192.168.12.102_80	Down	Down	192.168.12.102	80	HTTP	LEASTCONNECT
▶ 78.40.242.185_80	Down	Down	78.40.242.185	80	HTTP	LEASTCONNECT
▶ 192.168.12.114_80	Down	Down	192.168.12.114	80	HTTP	LEASTCONNECT
▶ Swivel LB RADIUS	Up	Up	192.168.12.115	1812	RADIUS	ROUNDROBIN

After creating the virtual server, select it and then Edit

← 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

1

Listen Policy Expression **NONE**

NONE

Range

1

Redirection Mode

IP

RHI State

PASSIVE

AppFlow Logging

ENABLED

Services and Service Groups

1. Load Balancing Virtual Server Service Binding

2

No Load Balancing Virtual Server ServiceGroup Binding

2

Persistence

Persistence **SSLSESSION**

Time-out (mins) 2

Done

Select "Load Balancing Virtual Server Service Binding"

The screenshot shows the Citrix NetScaler VPX configuration interface. The browser address bar displays `https://192.168.12.100/menu/neo#noAnchor`. The page title is "NetScaler VPX (10)". The top navigation bar includes "Dashboard", "Configuration", "Reporting", "Documentation", and "Downloads". The "Configuration" tab is active, and the "Load Balancing Virtual Server Service Binding" page is displayed. The page shows a table with one binding entry: "Swivel_8443" with IP address "192.168.12.111", port "8443", protocol "SSL_BRIDGE", state "Up", weight "1", and persistence cookie "-NA-". The "Add Binding" button is highlighted.

NetScaler VPX (10)

HA Status: Not Configured Info NS11.0 62.10.nc Logout

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Virtual Server Service Binding

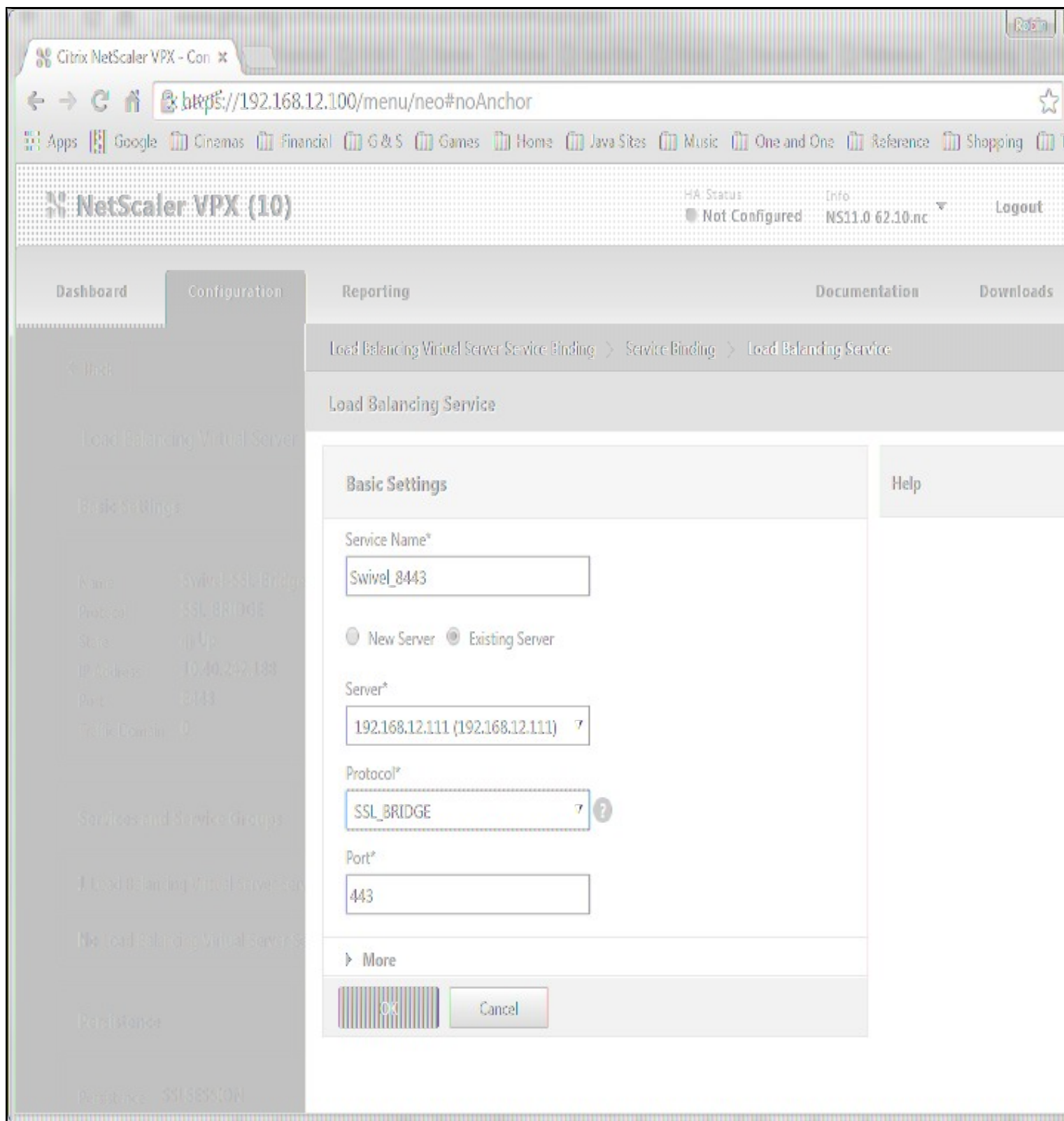
Load Balancing Virtual Server Service Binding

Add Binding Edit Binding Unbind Edit Service Bound Monitors

Service Name	IP Address	Port	Protocol	State	Weight	Persistence Cookie
Swivel_8443	192.168.12.111	8443	SSL_BRIDGE	Up	1	-NA-

Close

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.

45.3 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.

45.3.1 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.

45.3.2 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.

45.3.3 Customising an Existing Theme

45.3.3.1 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.

45.3.3.2 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
```

45.3.3.3 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
```

45.3.3.4 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".

45.3.3.5 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.

45.3.3.6 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.

45.3.3.7 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.

45.3.3.8 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.

45.3.3.9 Select the custom theme

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

45.3.3.10 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.

45.3.3.11 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.

45.3.4 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](#).

45.4 Additional Login Customisation options

45.4.1 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".

45.4.2 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".

45.4.3 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=password]').val(passwordPassedIn);
        $('[name=login]').val(usernamePassedIn);
        //alert("GO " + usernamePassedIn);
        document.getElementsByName("vpnForm")[0].submit();
    }
});

```

Before the closing </SCRIPT> tag

45.5 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.

45.5.1 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.

45.6 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).

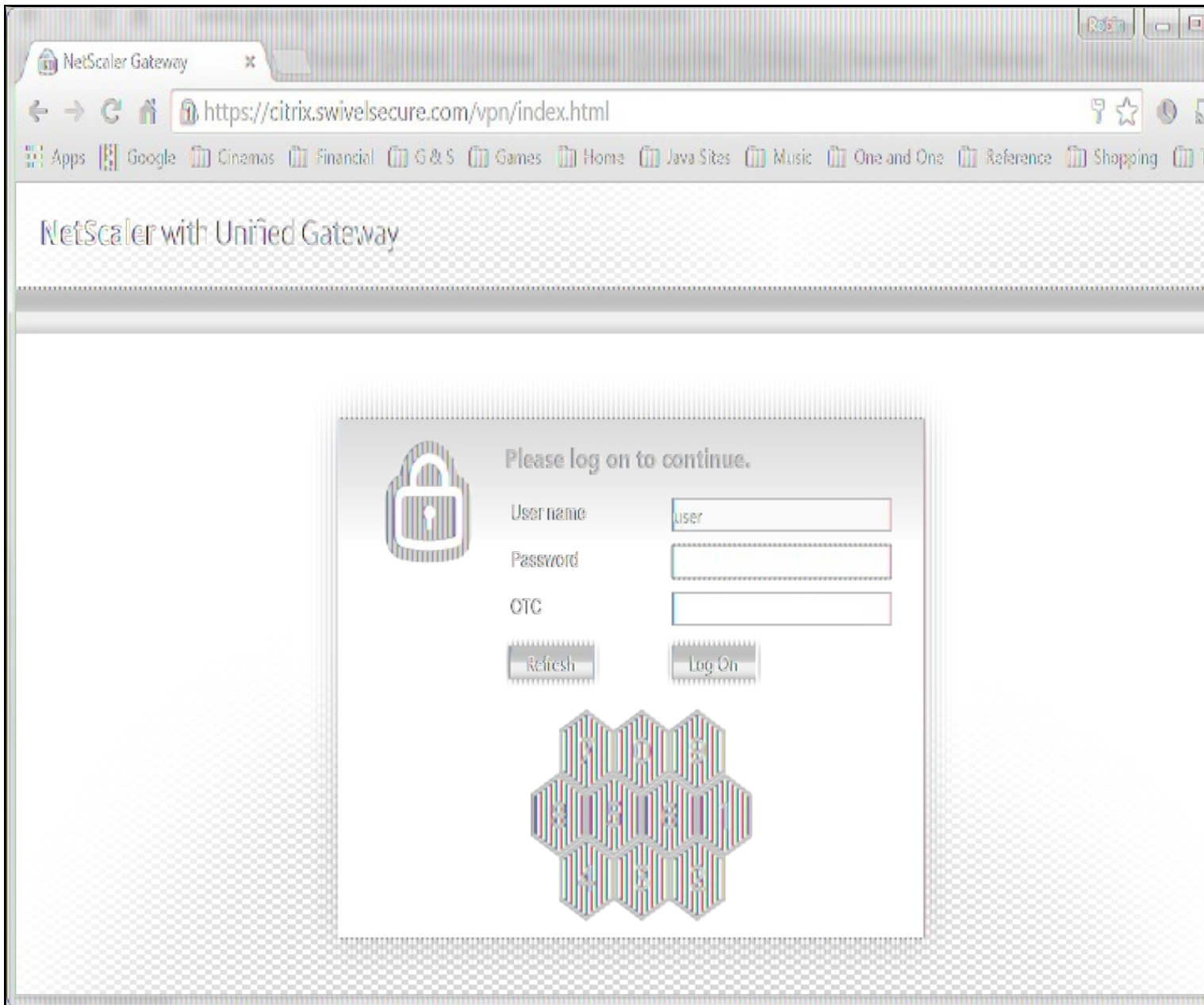
```

function ns_showpinsafe()
{
    var pspwc = ns_getcookie("pwcount");
    if ( pspwc == 2 )
    {
        document.write('<td>');
        document.write('');
        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>');
    }
}

```

46 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.



47 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.

48 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.

48.1 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;"><span id="User_name" class="CTXMSAM_LogonFont"></span></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 prevent 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 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.

49 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

50 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

51 Citrix Netscaler Gateway 12

52 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 Servers 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.

52.1 Integration Architecture

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

53 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.

53.1 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\"></script>}"
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
```

53.1.1 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.

53.2 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\"></script>}"
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\"+\nvar 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.

53.3 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

53.4 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(1000000)" 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\"+\nvar pinsafeUrl = \"\"https://sentry.swiveldev.com:8443/prox
add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js

```

54 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\"></script>\r\n"}
add rewrite action ReAct_Insert_Pinpad replace_all "HTTP.RES.BODY(1000000)" q|"form.append(field_errormsg);\r\n\tvar refresh_button=${\r\n<input type=\"button\" value=\"Refresh\" />\r\n}"
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/SCPInPad\\\";\"
add responder action ResAct_pinpad.css respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"div.pinpadHidden { display : none; }\r\n\"+\"div.pinpadVisible { display : block; }\"
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
```

55 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.

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.

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

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

[illegible]

- 110

57 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

58 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 ...
```

59 nFactor ? Customizing UI to Display Images

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

60 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>

61 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

62 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.

63 Prerequisites

Swivel HA solution

Netscaler 10.x

64 Baseline

Swivel 3.10.3

Netscaler 10.5

65 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](#).

66 Netscaler Configuration

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

66.1 Create a Swivel Radius Monitor

On the Netscaler Administration console Configuration 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

Create Monitor

Name*

Swivel RADIUS Monitor

Type*

RADIUS

Standard Parameters

Special Parameters

Response Codes

+

3

x

User Name*

test

Password*

.....

RADIUS Key*

.....

NAS ID

NAS IP

.

.

.

Create

Close

Configure Monitor

Name

Swivel RADIUS Monitor

Type

RADIUS

Standard Parameters

Special Parameters

Response Codes

+

2-3

x

User Name*

non-swivel

Password*

.....

RADIUS Key*

.....

NAS ID

NAS IP

0

.

0

.

0

.

0

OK

Close

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

122

66.2 Create Entries for the Swivel RADIUS Servers

On the Netscaler Administration console Configuration 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**

Create Server

Server Name*

Swivel Primary

☒ IP Address ☐ Domain Name

IPAddress*

192 . 168 . 12 . 116 ☐ IPv6

Traffic Domain

▼

+

?

☒ Enable after Creating

Comments

Create

Close

Create Server

Server Name*

Swivel Standby

☒ IP Address

☐ Domain Name

IPAddress*

192 . 168 . 12 . 117

☐ IPv6 ?

Traffic Domain

▼

+

☒ Enable after Creating

Comments

Create

Close

Click Create to create the Server

+ 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

NetScaler > Traffic Management > Load Balancing > Servers

Add

Edit

Delete

Action

Name	State
▶ Swivel Standby	Enabled
▶ Swivel Primary	Enabled
▶ 192.168.12.111	Enabled
▶ 127.0.0.1	Enabled

Integrate with Citrix Products

XenMobile

XenApp and XenDesktop

66.3 Create a Swivel Load Balance Service Group

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

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

Load Balancing Service Group

Basic Settings

Name*

Swivel LB Service Group

Protocol*

RADIUS

Traffic Domain

Cache Type*

SERVER



AutoScale Mode



☐ Cacheable

☒ State

☒ Health Monitoring

☒ AppFlow Logging

Number of Active Connections

Comments



OK

Cancel

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.

Service Group Member

☐ IP Based
 ☒ Server Based

Server Name*

Swivel Primary

Port*

1812

Weight

1

Server Id

Hash Id

☒ State

Create Close

Service Group Member

☐ IP Based
 ☒ Server Based

Server Name*

Swivel Standby

Port*

1812

Weight

1

Server Id

Hash Id

☒ State

Create Close

66.3.1 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.

ServiceGroup Binding > Load Balancing Service Group > Load Balancing Monitor Binding

Load Balancing Monitor Binding

Select Monitor*

Swivel RADIUS Monitor

Binding Details

Weight

☐ State

☐ Passive

Bind Close

Click **Bind** to add it, then Done.

66.4 Create A Virtual Server

On the Netscaler Administration console Configuration Tab select Traffic management/Load Balancing/**Virtual Servers**, then Add. Enter a **Name** for the Virtual Server **IP Address**, **Protocol** and **Port**.

Load Balancing Virtual Server

Basic Settings

Name*
Swivel LB Virtual Server

Protocol*
RADIUS

IP Address Type*
IP Address

IP Address*
192 . 168 . 12 . 115 ☐ IPv6

Port*
1812 ?

► More

OK Cancel

Click OK to create the entry

66.4.1 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.

Load Balancing Virtual Server

Basic Settings

Name	Swivel LB RADIUS
Protocol	RADIUS
State	DOWN
IP Address	192.168.12.115
Port	1812
Traffic Domain	0

Listen Priority	-
Listen Policy Expression	-
Range	1
Redirection Mode	IP
RHI State	PASS
AppFlow Logging	ENAB

Service

No Load Balancing Virtual Server Service Binding

Traffic Settings

Health Threshold	0
Client Idle Time-out	120
Minimum Autoscale Members	0
Maximum Autoscale Members	0
ICMP Virtual Server Response	PASSIVE

Priority Queuing	OFF
Sure Connect	OFF
Down State Flush	ENABLED

Service Group

No Load Balancing Virtual Server ServiceGroup Binding

Done

Click on the Service Group, it will appear at the bottom allowing it to be selected, and then click on **Select Service Group Name** to choose the required service group created earlier.

ServiceGroup Binding > Service Groups

Service Groups

Add

Edit

Delete

Manage Members

Statistics

Action ▼

	Service Group Name	State	Effective State	Protocol	Max Clients	Max Requests	M
<input checked="" type="radio"/>	▶ Swivel LB Service Group	ENABLED	UP	RADIUS	0	0	

OK

Close

Then click **Bind**

66.4.2 Add the Method to the Virtual Server

Select Method and then from the **Load Balancing Method** drop down select **ROUNDROBIN** then click on OK.

Method

Load Balancing Method*

ROUNDROBIN ▼ ?

New Service Startup Request Rate

New Service Request unit*

PER_SECOND ▼

Increment Interval

OK

Click Done and the Virtual server should be created.

NetScaler > Traffic Management > Load Balancing > Virtual Servers						
<div> Add Edit Delete Enable Disable Statistics Action ▼ </div>						
Filters: <div>RADIUS X</div>						
Name	State	Effective State	IP Address	Port	Protocol	Method
▶ RADIUS Virtual Server	Up	Up	192.168.12.115	1812	RADIUS	ROUNDROBIN

66.5 Netscaler RADIUS configuration

The Netscaler can now be configured to use the new Virtual Server as its RADIUS servers following the original documentation.

67 Testing

When functioning RADIUS entries will be seen in the Swivel RADIUS logs for each test.

Try RADIUS authentications and see which Swivel server that receives them. Stopping one RADIUS server should indicate on the Virtual Servers that health is degraded, i.e. 50% for two servers.

68 Known Issues

The load balancing can produce a large number of logs.

69 Troubleshooting