Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 Citrix Access Gateway 5 VPX

1.1 Introduction

Please refer to the documentation located at:

Citrix Access Gateway Standard 5.x

2 Citrix Access Gateway Access Controller 5.0

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

- SMS
- Mobile Phone Client
- Email
- Taskbar utility

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

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

3 Citrix Access Gateway Advanced 4.x

4 Introduction

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

5 Prerequisites

PINsafe 3.x

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

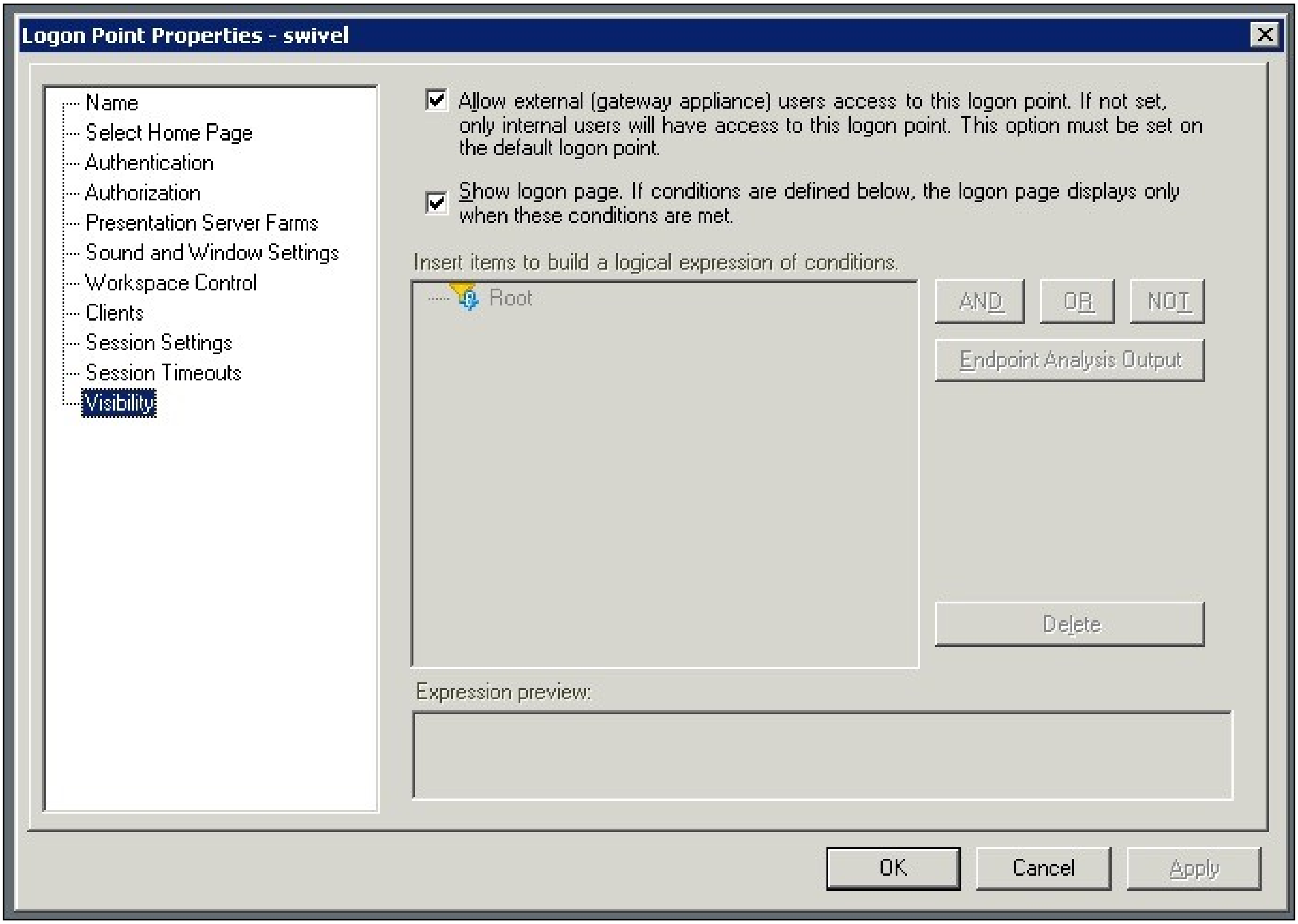
The CAG 4.5.8 integration guide is available here: Citrix Access Gateway Advanced edition 4.5.8

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

Additional Integration supplementary documentation is provided below

6 Installation

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



Logon Point Properties - swivel

☑ Allow external (gateway appliance) users access to this logon point. If not set, only internal users will have access to this logon point. This option must be set on the default logon point.

☑ Show logon page. If conditions are defined below, the logon page displays only when these conditions are met.

Insert items to build a logical expression of conditions.

Expression preview:

7 Additional Installation Options

7.1 Remove automatic TURing image automatically displaying

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

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

to

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

7.2 Prevent browser caching TURing image

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

Example:

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

7.3 Prevent the cursor from automatically entering the OTC field

Remove the following line from Login.ascx

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

7.4 Change the TURing button text

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

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

and change it to

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

7.5 Verifying the Installation

7.6 Uninstalling the PINsafe Integration

7.7 Troubleshooting

7.8 Known Issues and Limitations

7.9 Additional Information

8 Citrix Access Gateway Standard 4.x

9 Introduction

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

10 Prerequisites

Swivel 3.x

Citrix Access Gateway 4.x

11 Baseline

12 Architecture

Authentications are made against Swivel using RADIUS.

13 Installation

14 Swivel Configuration

14.1 Configuring the RADIUS server

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

14.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

14.3 Citrix Access Gateway Standard Edition Integration

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

15 Additional Information

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

16 Citrix Access Gateway Standard 5.x

17 Introduction

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

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

18 Prerequisites

Swivel 3.x

Citrix Access Gateway 5.x

19 Baseline

PINsafe 3.8

CAG Standard 5.0.3

20 Architecture

Authentications are made against Swivel using RADIUS.

21 Installation

22 Swivel Configuration

22.1 Configuring the RADIUS server

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

22.2 Setting up PINsafe Dual Channel Transports

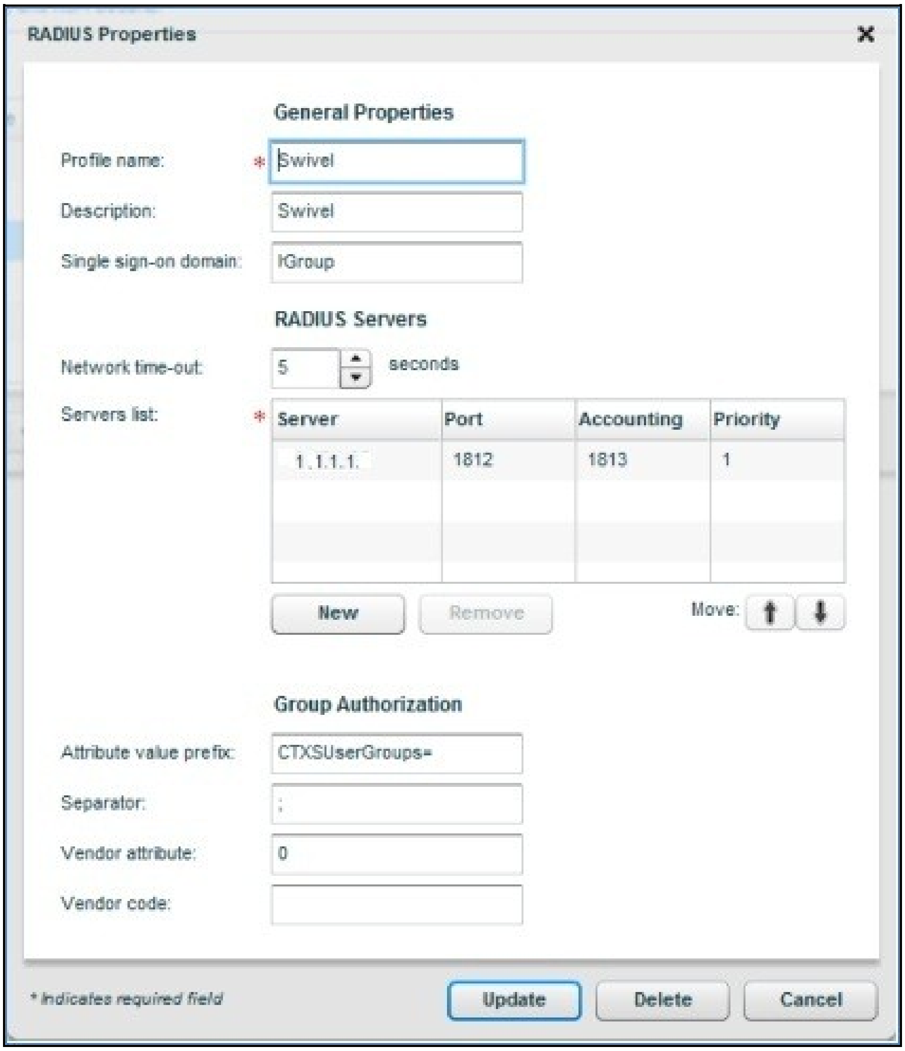
See Transport Configuration

23 Citrix Access Gateway Standard Edition Integration

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

23.1 CAG RADIUS Properties

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



RADIUS Properties

General Properties

Profile name: * Swivel

Description: Swivel

Single sign-on domain: IGroup

RADIUS Servers

Network time-out: 5 seconds

Servers list: *

Server	Port	Accounting	Priority
1.1.1.1.	1812	1813	1

Group Authorization

Attribute value prefix: CTXSUserGroups=

Separator: ;

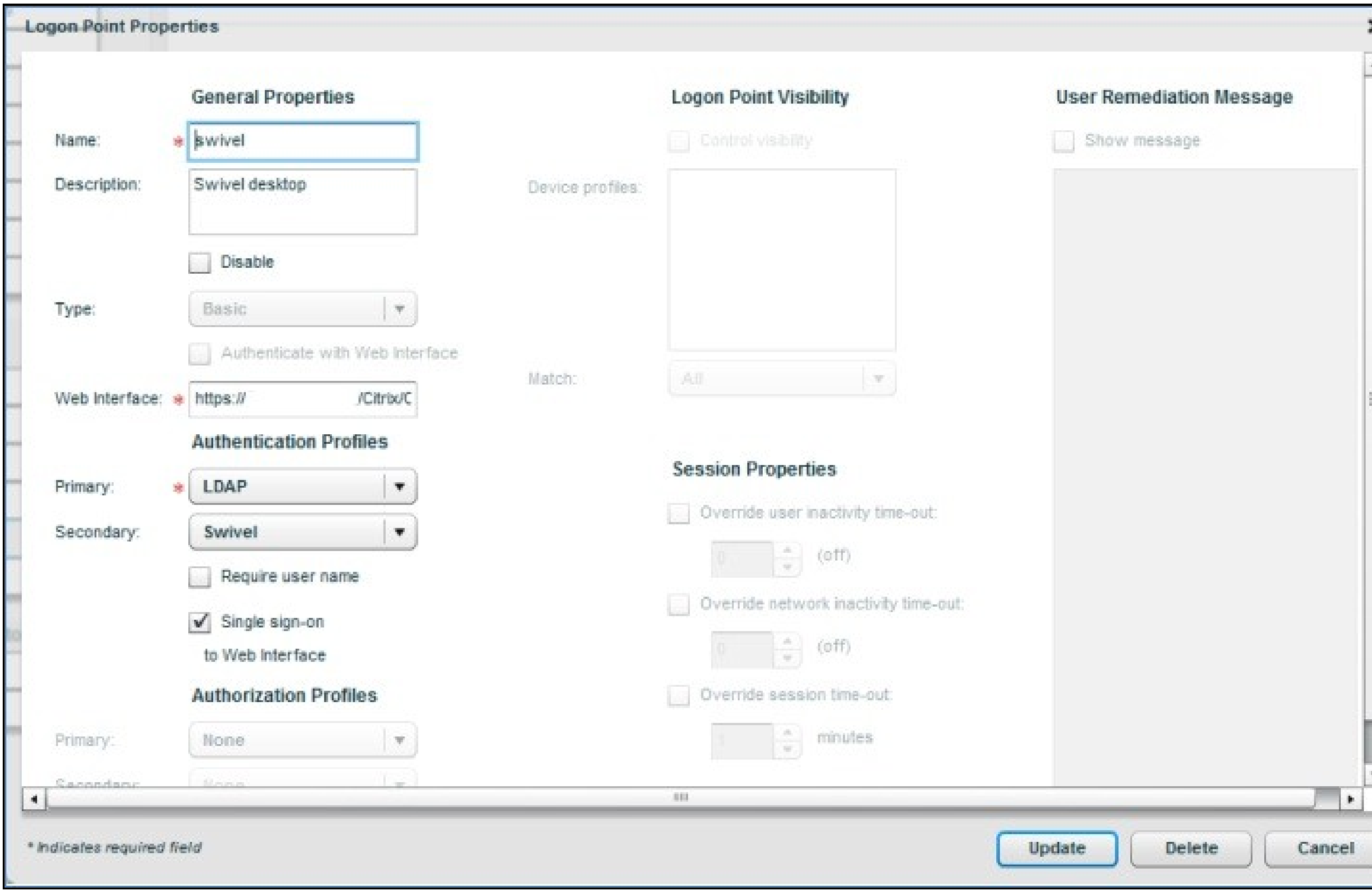
Vendor attribute: 0

Vendor code:

* Indicates required field

23.2 CAG logon Point Properties

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



Logon Point Properties

General Properties

Name: * swivel

Description: Swivel desktop

□ Disable

Type: Basic

□ Authenticate with Web Interface

Web Interface: * https:// /Citrix/C

Authentication Profiles

Primary: * LDAP

Secondary: Swivel

□ Require user name

☑ Single sign-on to Web Interface

Authorization Profiles

Primary: None

Secondary: None

Logon Point Visibility

□ Control visibility

Device profiles:

Match: All

Session Properties

□ Override user inactivity time-out:

0 (off)

□ Override network inactivity time-out:

0 (off)

□ Override session time-out:

minutes

User Remediation Message

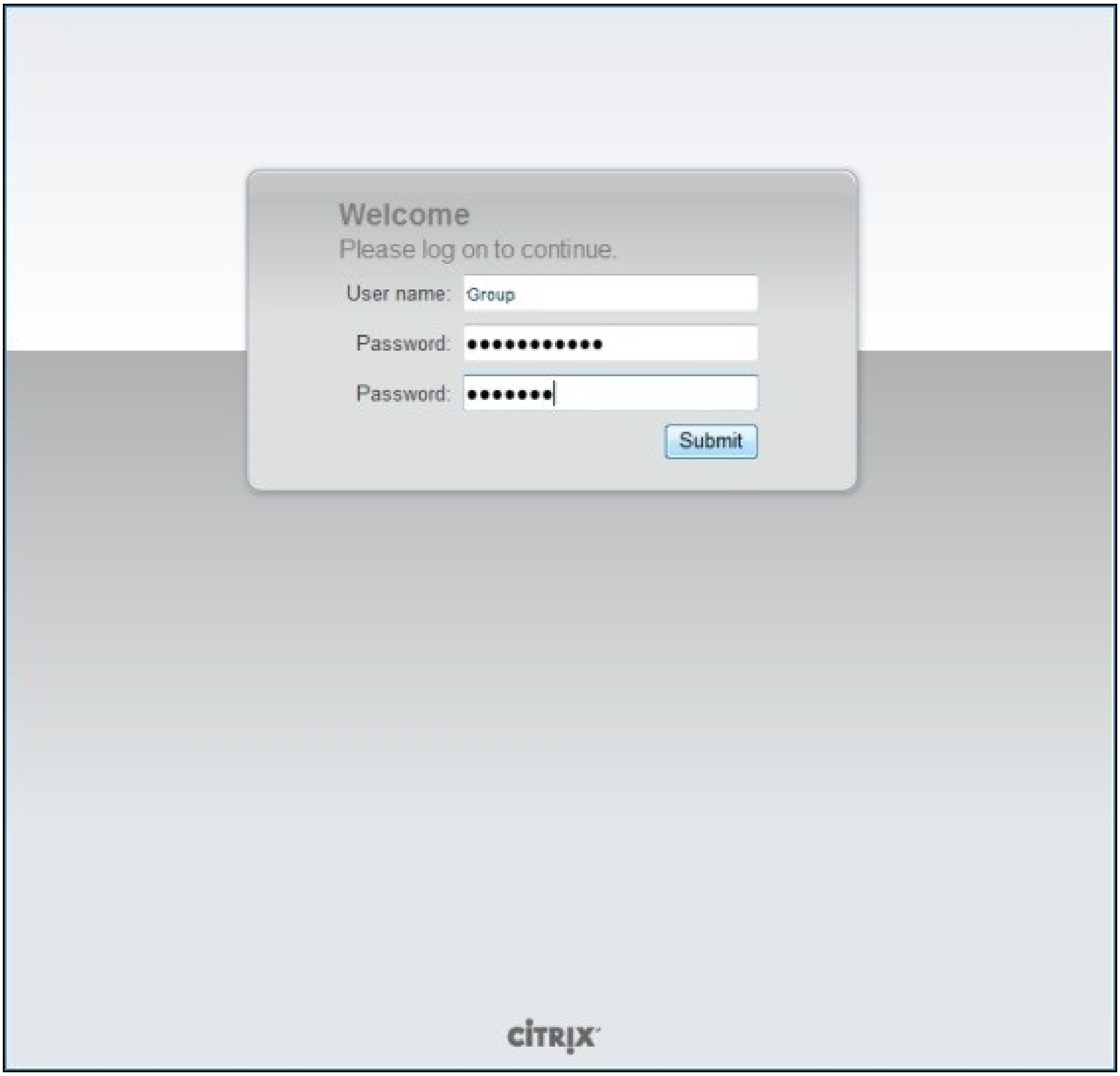
□ Show message

* indicates required field

24 Additional Installation Options

25 Verifying the Installation

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



Welcome
Please log on to continue.

User name: Group

Password: ●●●●●●●●●●●●

Password: ●●●●●●●

26 Uninstalling the PINsafe Integration

27 Troubleshooting

28 Known Issues and Limitations

29 Additional Information

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

30 Citrix Access Gateway Web Interface Proxy

31 Introduction

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

32 Prerequisites

Citrix Access Gateway 5.x

Citrix Web Interface 5.x

PINsafe 3.x

33 Baseline

Citrix Access Gateway 5.0

Citrix Web Interface 5.4

PINsafe 3.8

34 Architecture

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

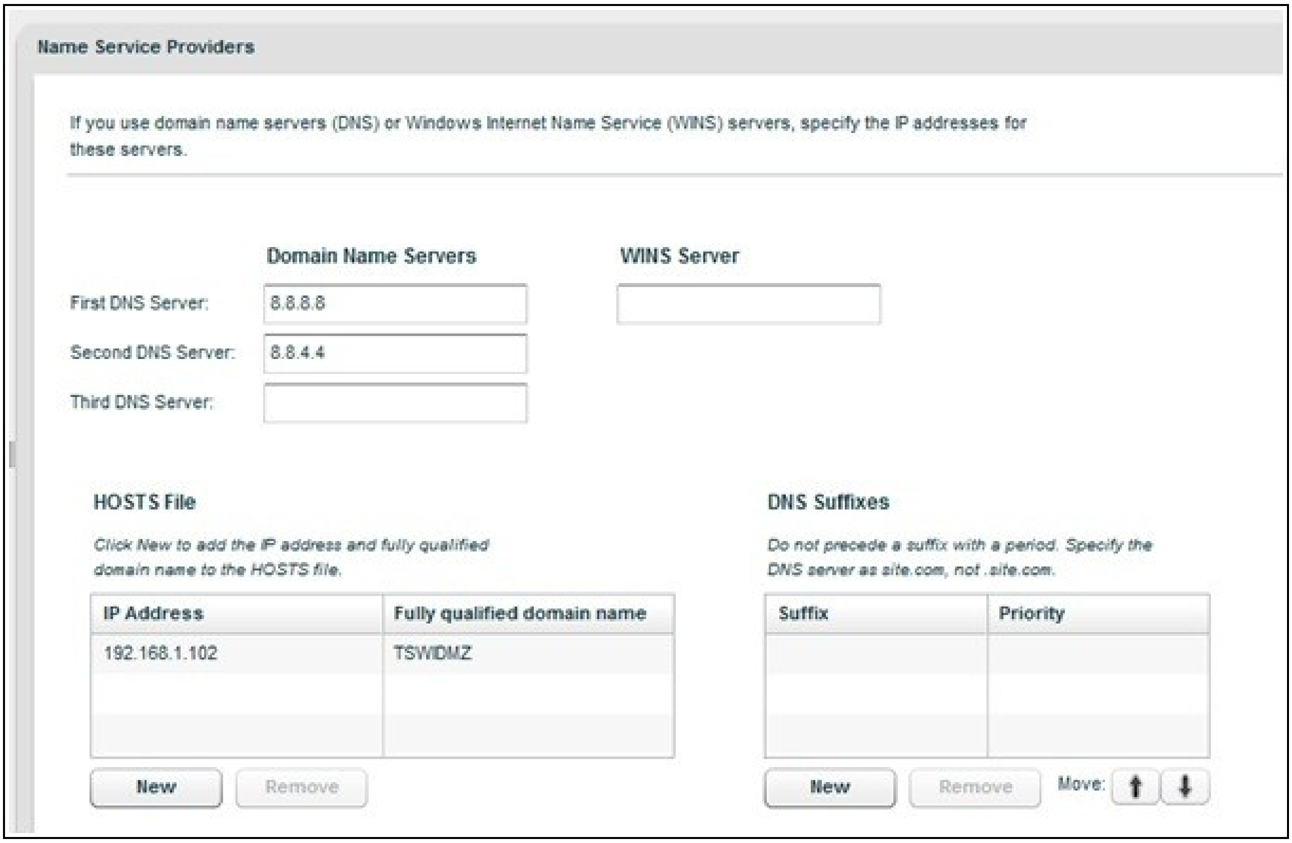
35 Installation

35.1 PINsafe and Web Interface Integration Configuration

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

35.2 CAG Standard and CAG VPX configuration and installation

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



Name Service Providers

If you use domain name servers (DNS) or Windows Internet Name Service (WINS) servers, specify the IP addresses for these servers.

Domain Name Servers

First DNS Server: 8.8.8.8

Second DNS Server: 8.8.4.4

Third DNS Server:

WINS Server:

HOSTS File

Click New to add the IP address and fully qualified domain name to the HOSTS file.

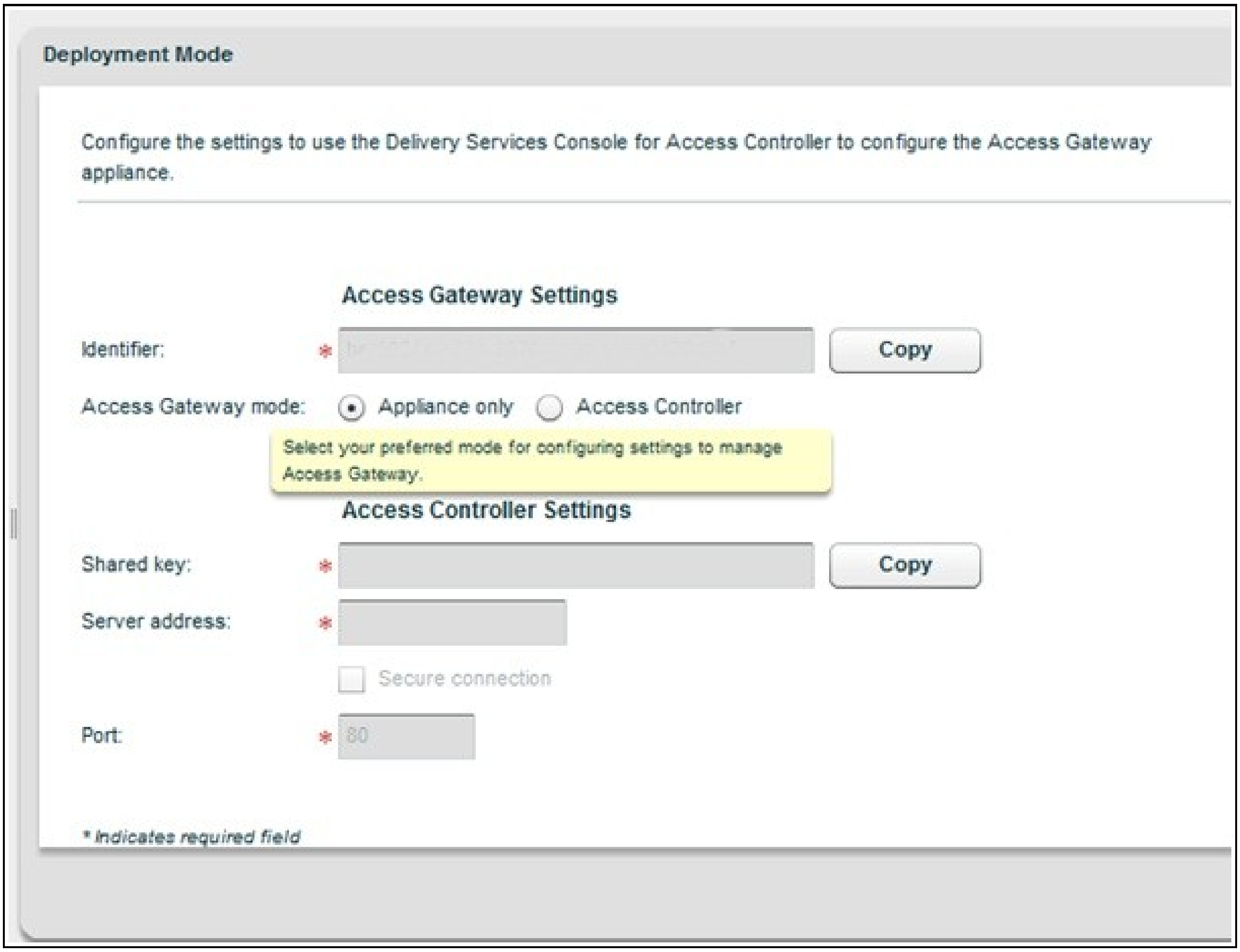
IP Address	Fully qualified domain name
192.168.1.102	TSWIDMZ

DNS Suffixes

Do not precede a suffix with a period. Specify the DNS server as site.com, not .site.com.

Suffix	Priority

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



Deployment Mode

Configure the settings to use the Delivery Services Console for Access Controller to configure the Access Gateway appliance.

Access Gateway Settings

Identifier: * [illegible]

Access Gateway mode: ● Appliance only ○ Access Controller

Select your preferred mode for configuring settings to manage Access Gateway.

Access Controller Settings

Shared key: *

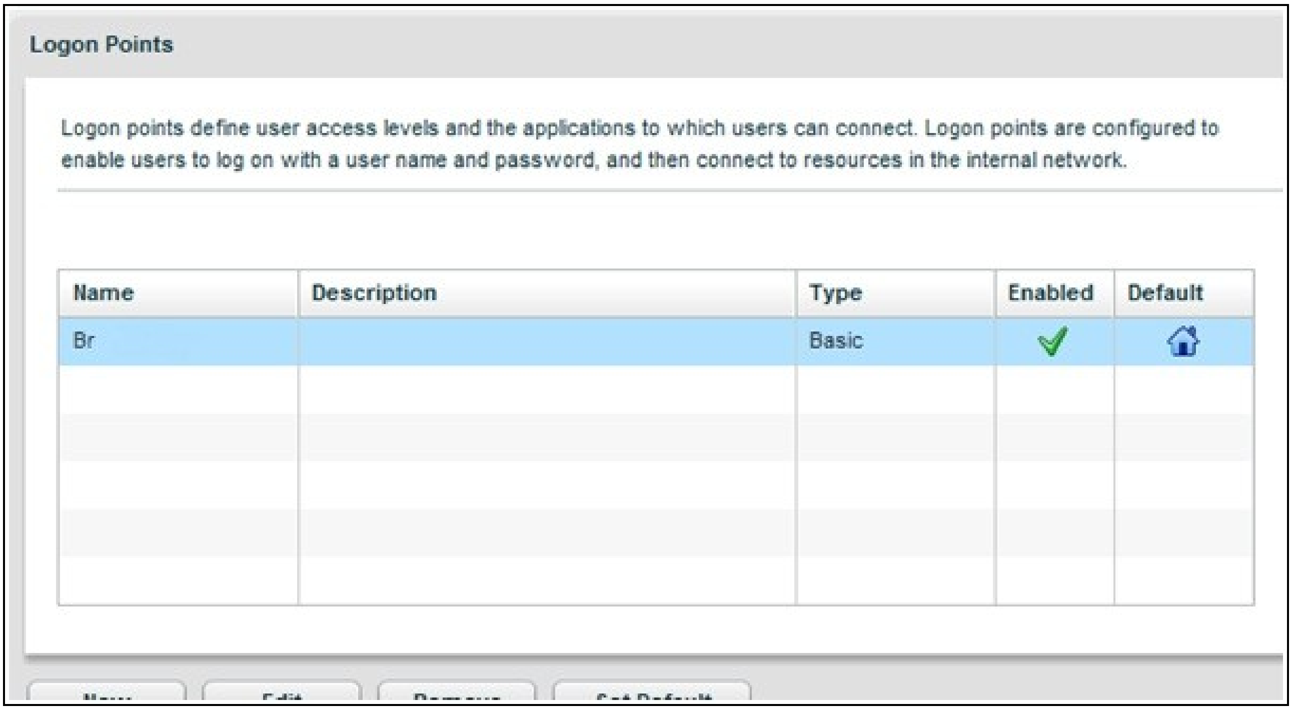
Server address: *

□ Secure connection

Port: * 80

** Indicates required field*

Set the Logon Point as home.

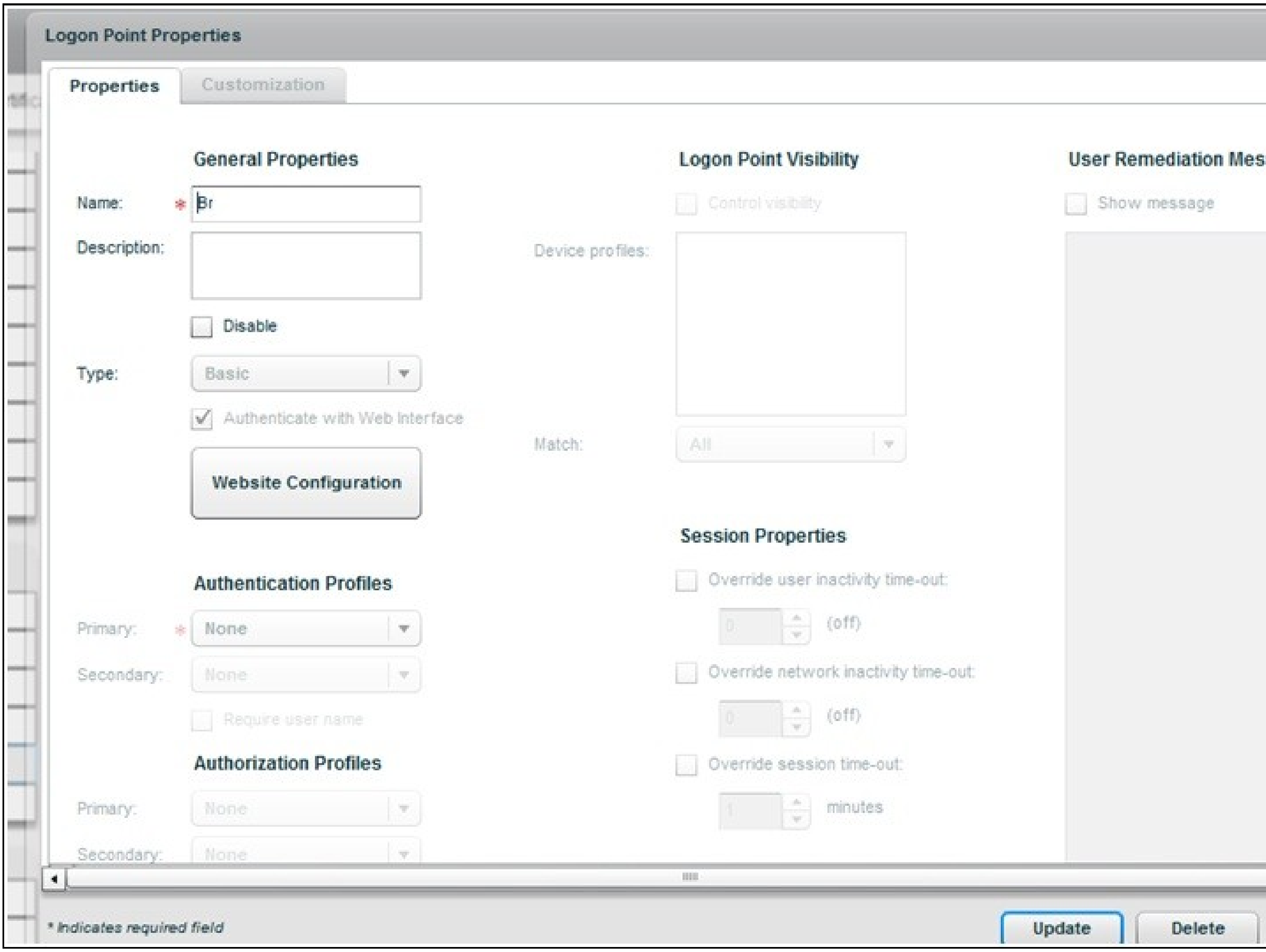


Logon Points

Logon points define user access levels and the applications to which users can connect. Logon points are configured to enable users to log on with a user name and password, and then connect to resources in the internal network.

Name	Description	Type	Enabled	Default
Br		Basic	✓	⌂

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



Logon Point Properties

Properties | Customization

General Properties

Name: * Br

Description:

□ Disable

Type: Basic

☑ Authenticate with Web Interface

Authentication Profiles

Primary: * None

Secondary: None

□ Require user name

Authorization Profiles

Primary: None

Secondary: None

Logon Point Visibility

□ Control visibility

Device profiles:

Match: All

Session Properties

□ Override user inactivity time-out:

0 (off)

□ Override network inactivity time-out:

0 (off)

□ Override session time-out:

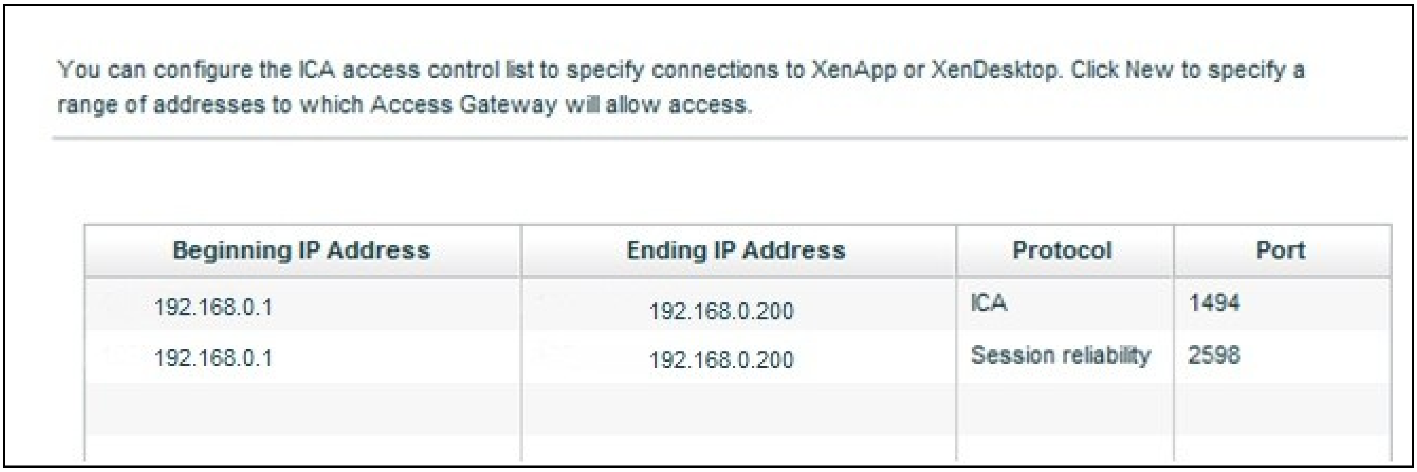
1 minutes

User Remediation Mes

□ Show message

* Indicates required field

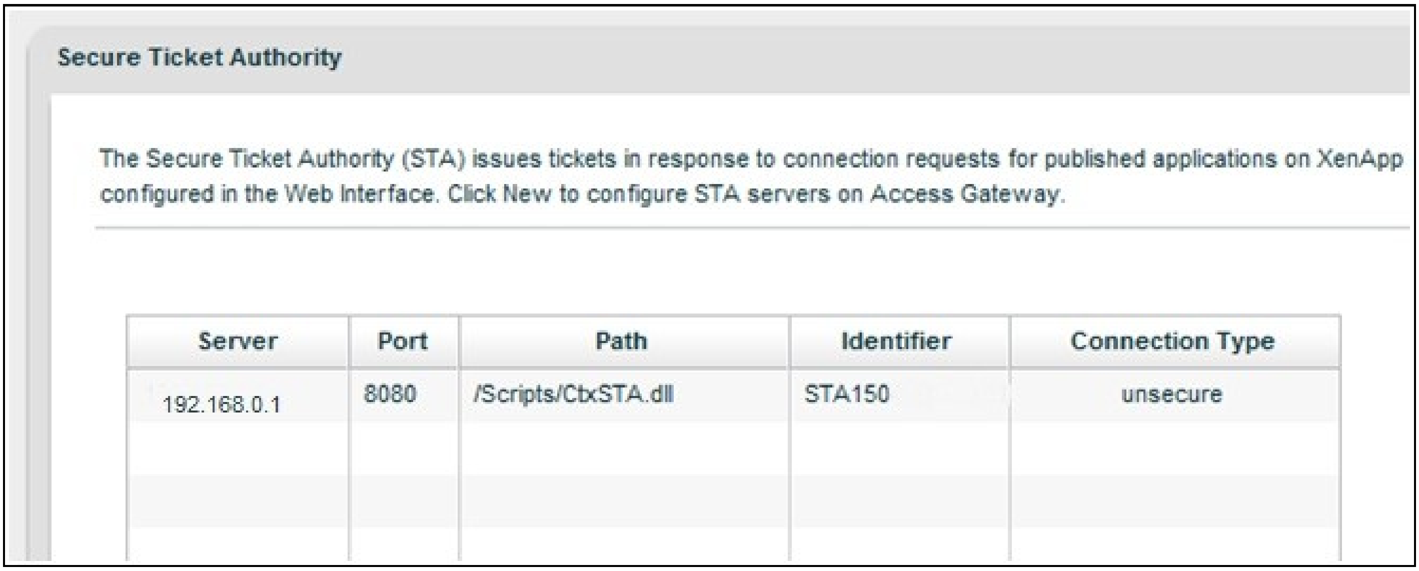
Enter the Web Interface server for the Web Address and Application Type should be WEBINTERFACE.



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

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

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



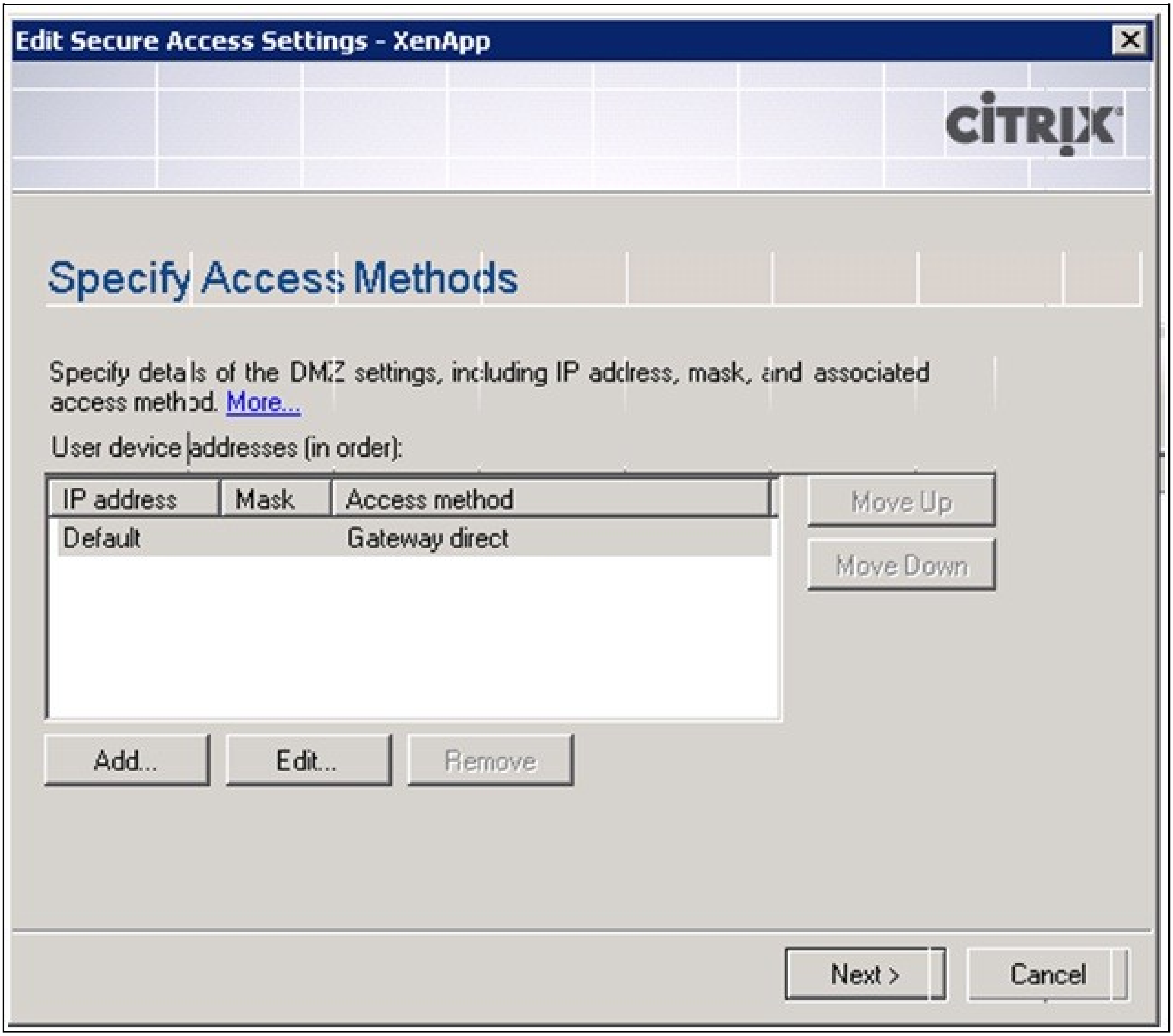
Secure Ticket Authority

The Secure Ticket Authority (STA) issues tickets in response to connection requests for published applications on XenApp configured in the Web Interface. Click New to configure STA servers on Access Gateway.

Server	Port	Path	Identifier	Connection Type
192.168.0.1	8080	/Scripts/CtxSTA.dll	STA150	unsecure

35.3 Citrix Web Interface configuration and installation

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



Edit Secure Access Settings - XenApp

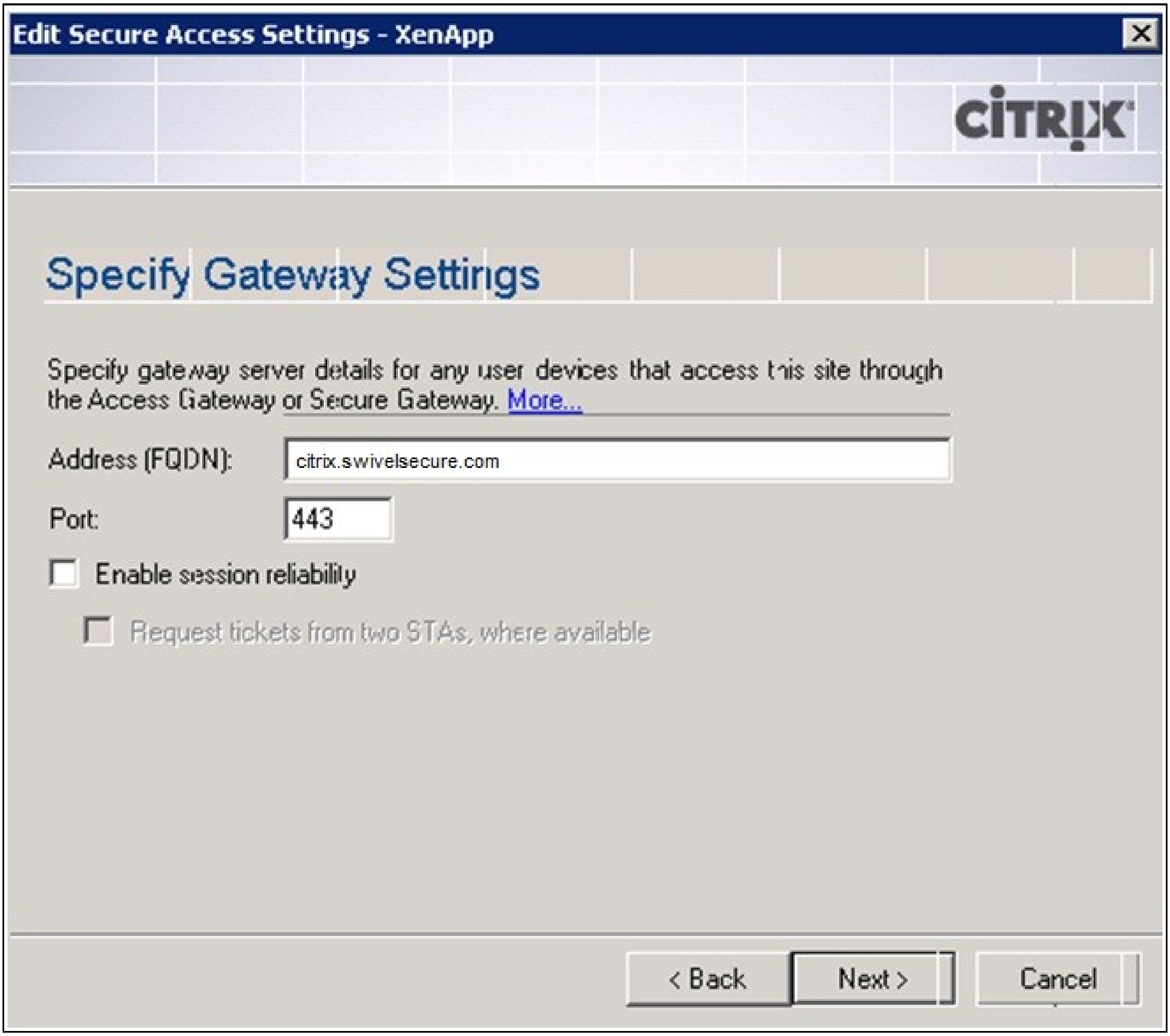
Specify Access Methods

Specify details of the DMZ settings, including IP address, mask, and associated access method. More...

User device addresses (in order):

IP address	Mask	Access method
Default		Gateway direct

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



Edit Secure Access Settings - XenApp

Specify Gateway Settings

Specify gateway server details for any user devices that access this site through the Access Gateway or Secure Gateway. More...

Address (FQDN): citrix.swivelsecure.com

Port: 443

□ Enable session reliability

□ Request tickets from two STAs, where available

35.4 Additional Installation Options

36 Verifying the Installation

Browse to the login page and authenticate with PINsafe credentials.

37 Uninstalling the PINsafe Integration

38 Troubleshooting

39 Known Issues and Limitations

40 Additional Information

41 Citrix Products Integration Matrix

41.1 A guide to PINsafe and Citrix Product Integration

Product Integration

Product	SMS Text	Mobile Phone Client	Taskbar Utility	TURing Image	Index number display	Token
CAG Standard 4 or 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5 with WI authentication	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AAC 4.5	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AC	Yes	Yes	Yes	No	No	Yes
CAG Enterprise (Netscaler) 8 or 9 or 10 10.x	Yes	Yes	Yes	Yes	Yes	Yes
WI 4.5, 4.6, 5.0, 5.1, 5.2, 5.3, 5.4	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
PS 4 with WI	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Receiver	Yes	Yes	Yes	Yes*	Yes*	Yes

CAG = Citrix Access Gateway

AAC = Advanced Access Controller (AAC 4.x)

PS = Presentation Server

WI = Web Interface

Index Number Display is the ability to display the index number in the login page

Yes* When viewed in browser before receiver starts

42 Citrix Access Gateway Enterprise Edition 10

43 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.

44 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.

45 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.

46 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.

47 Swivel Configuration

47.1 Configuring the RADIUS server

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

47.2 Enabling Session creation with username

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

47.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

48 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.

48.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

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

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

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

Name Swivel RADIUS

Authentication type RADIUS

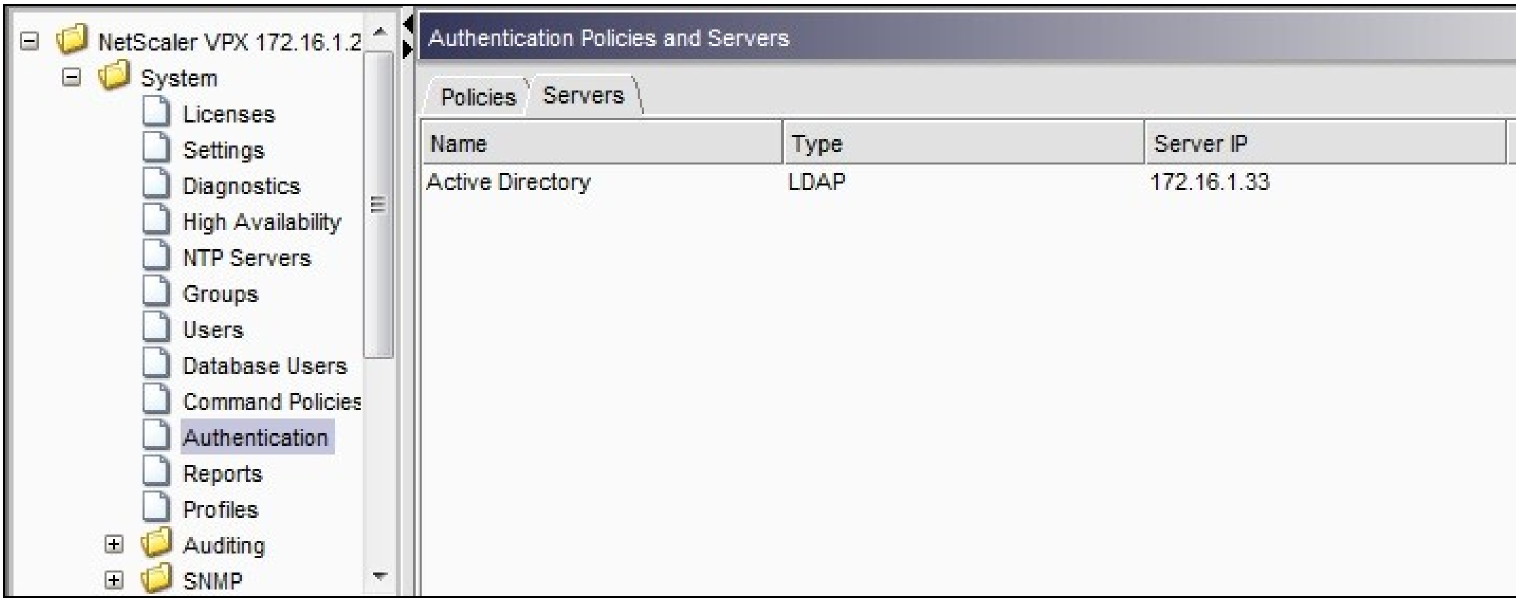
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix CTXSUserGroups=

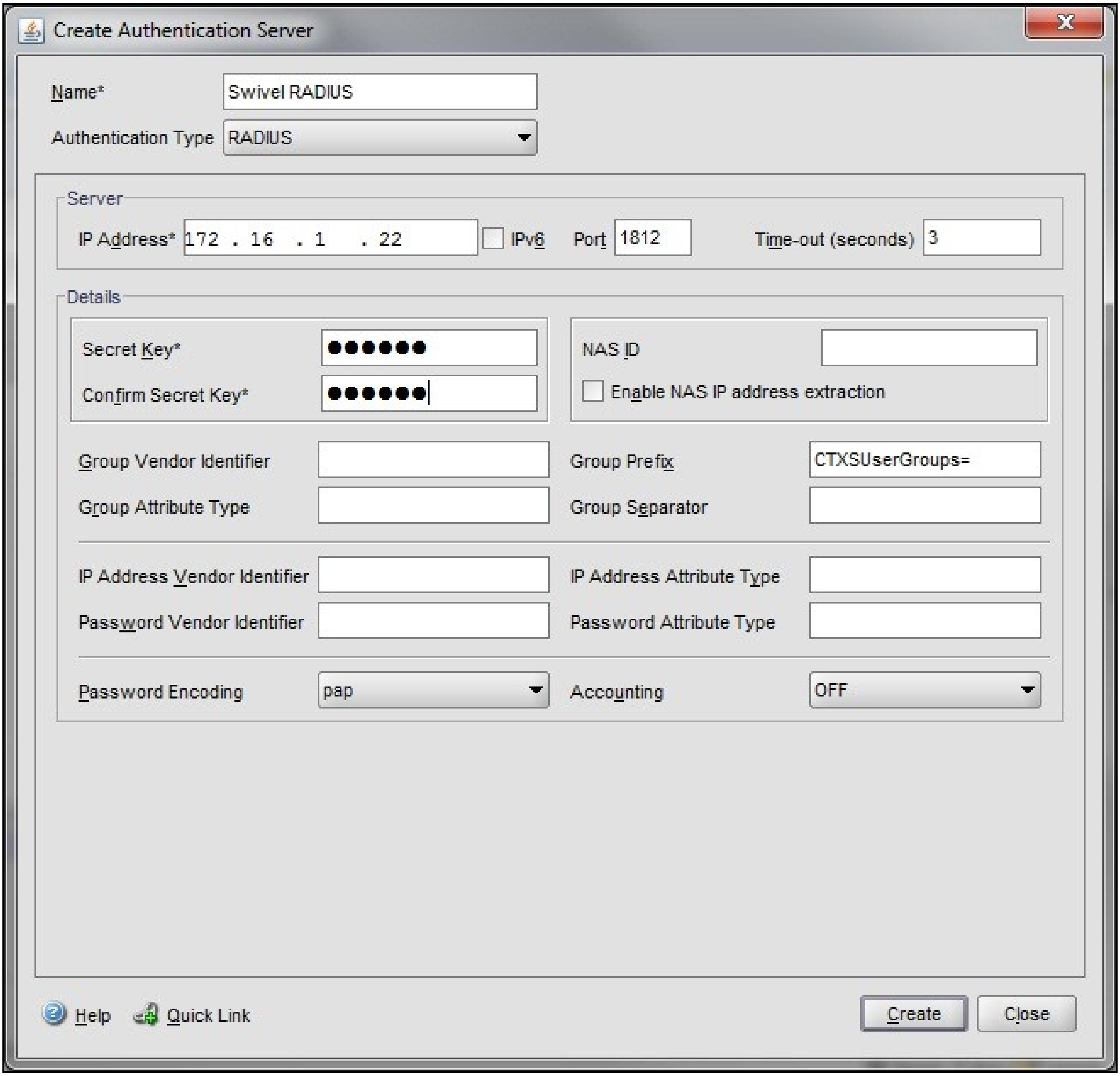
Group Separator ;

When complete click on Create.

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



Name	Type	Server IP
Active Directory	LDAP	172.16.1.33



Create Authentication Server

Name* Swivel RADIUS

Authentication Type RADIUS

Server

IP Address* 172 . 16 . 1 . 22 □ IPv6 Port 1812 Time-out (seconds) 3

Details

Secret Key* ●●●●●●

Confirm Secret Key* ●●●●●●●

NAS ID

□ Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix CTXSUserGroups=

Group Attribute Type

Group Separator

IP Address Vendor Identifier

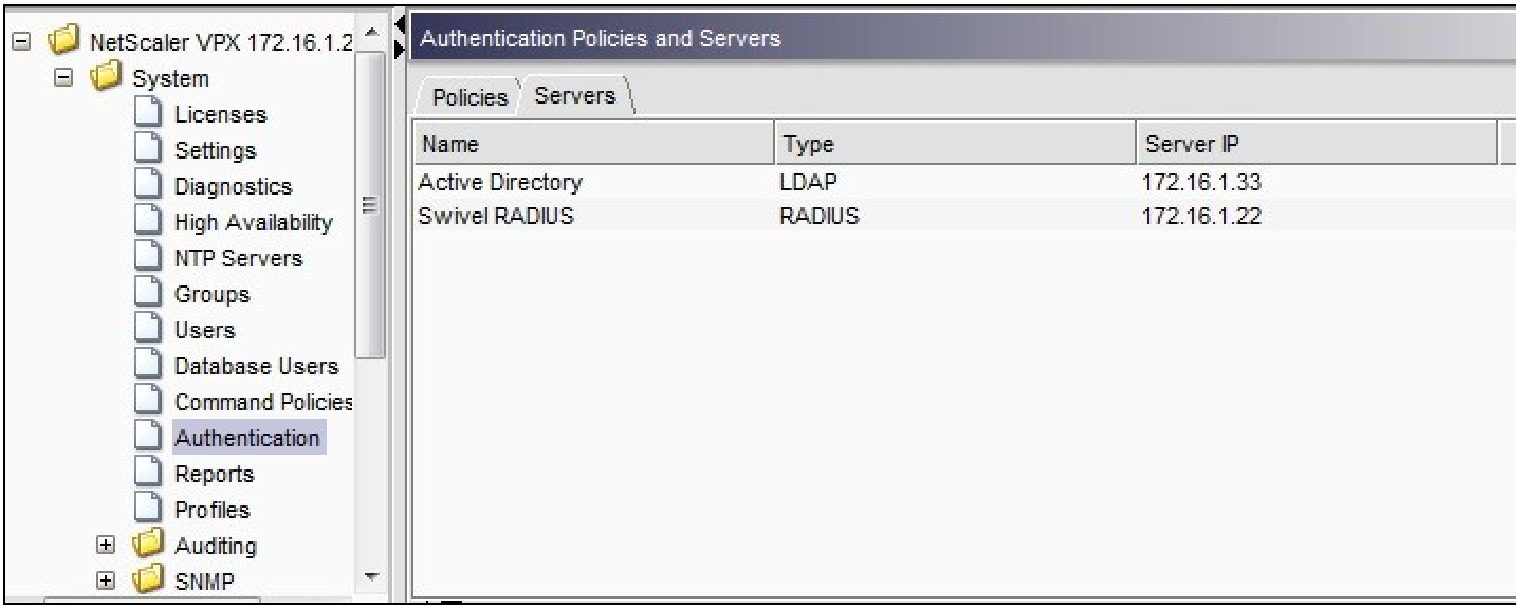
IP Address Attribute Type

Password Vendor Identifier

Password Attribute Type

Password Encoding pap

Accounting OFF



Name	Type	Server IP
Active Directory	LDAP	172.16.1.33
Swivel RADIUS	RADIUS	172.16.1.22

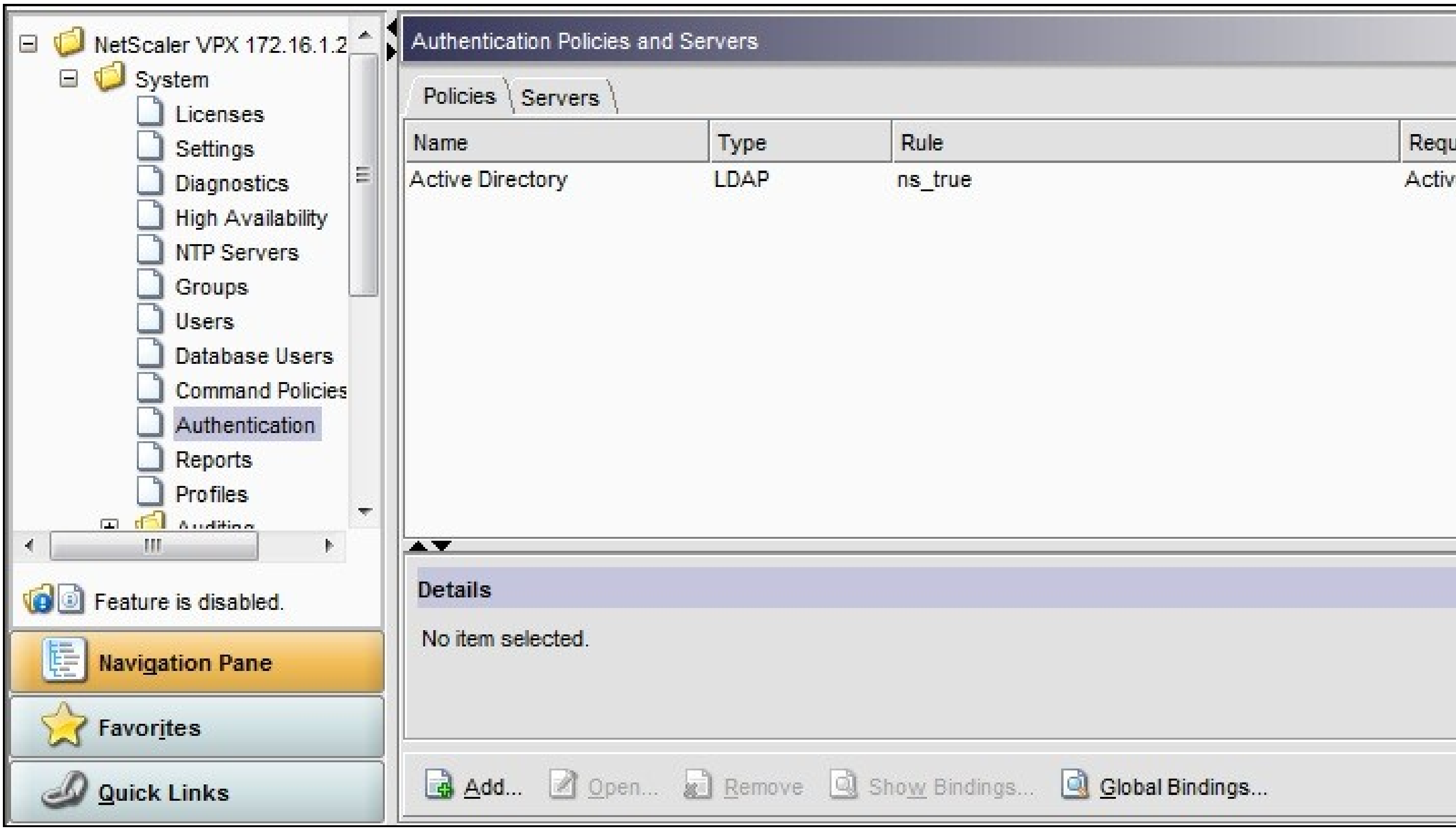
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

Server Swivel RADIUS

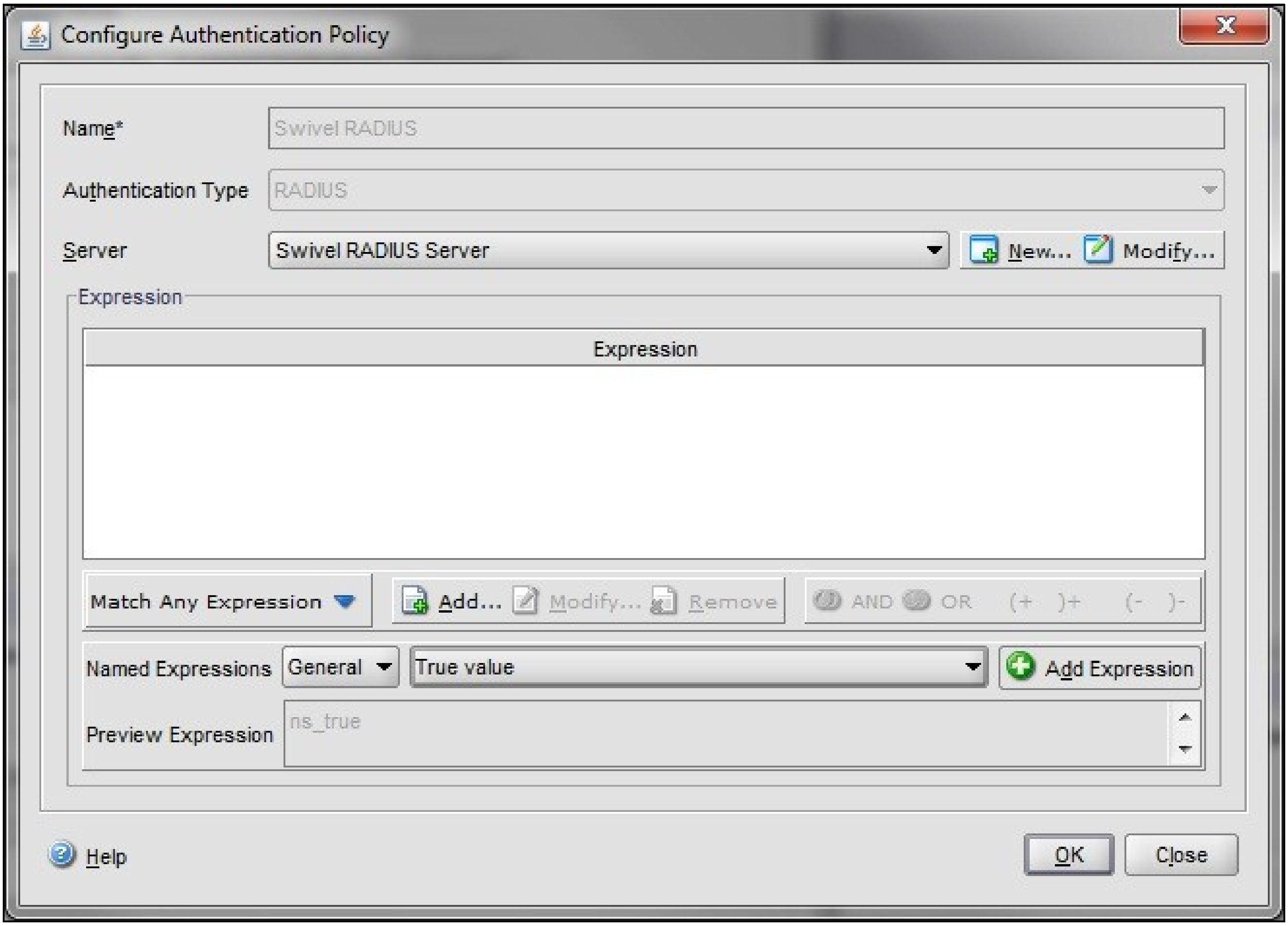
Named Expression True Value (Then click Add Expression so ns_true appears under Expression



Name	Type	Rule	Requ
Active Directory	LDAP	ns_true	Activ

Details

No item selected.



Configure Authentication Policy

Name* Swivel RADIUS

Authentication Type RADIUS

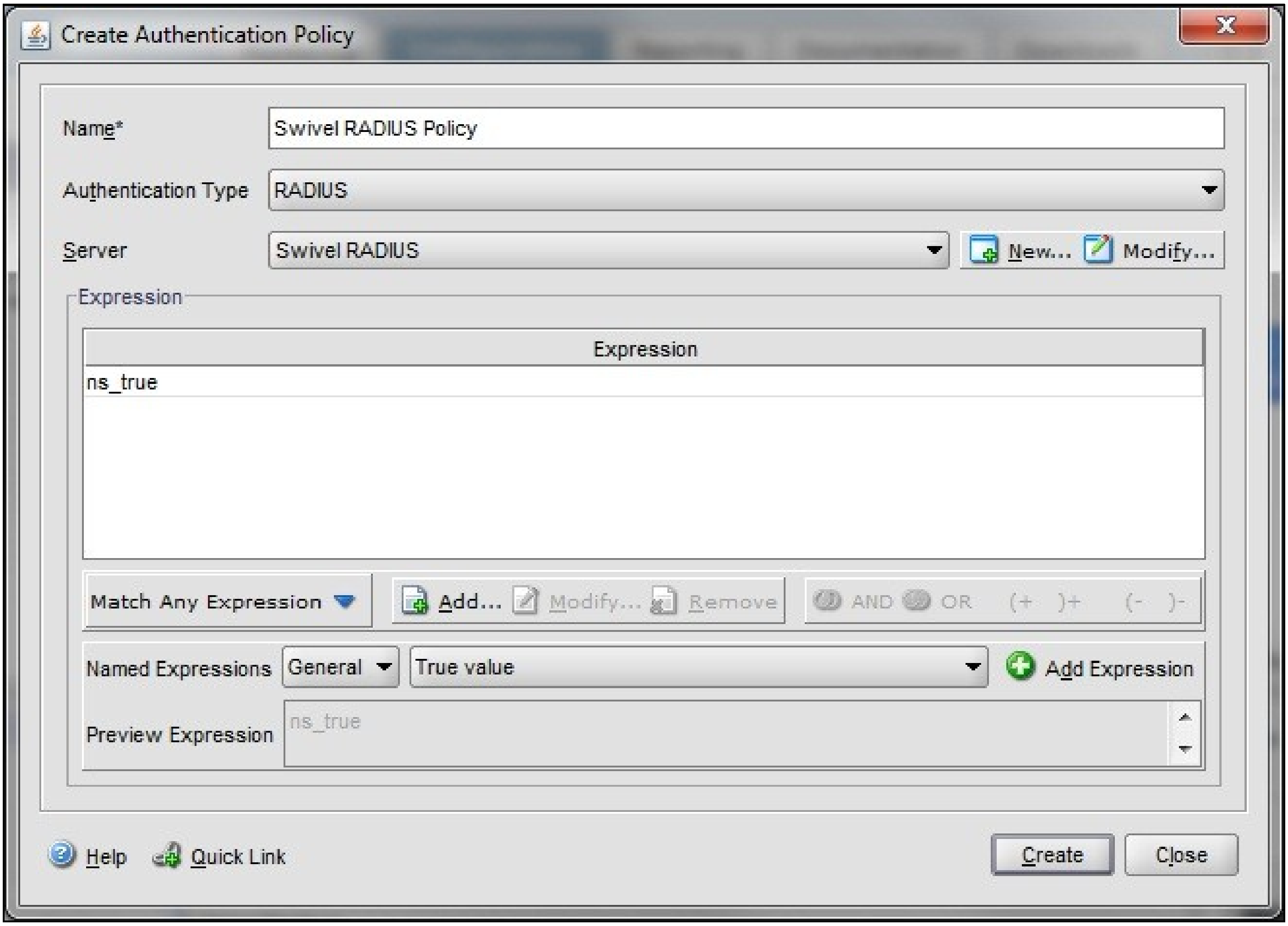
Server Swivel RADIUS Server

Expression

Match Any Expression

Named Expressions General True value

Preview Expression ns_true



Name* Swivel RADIUS Policy

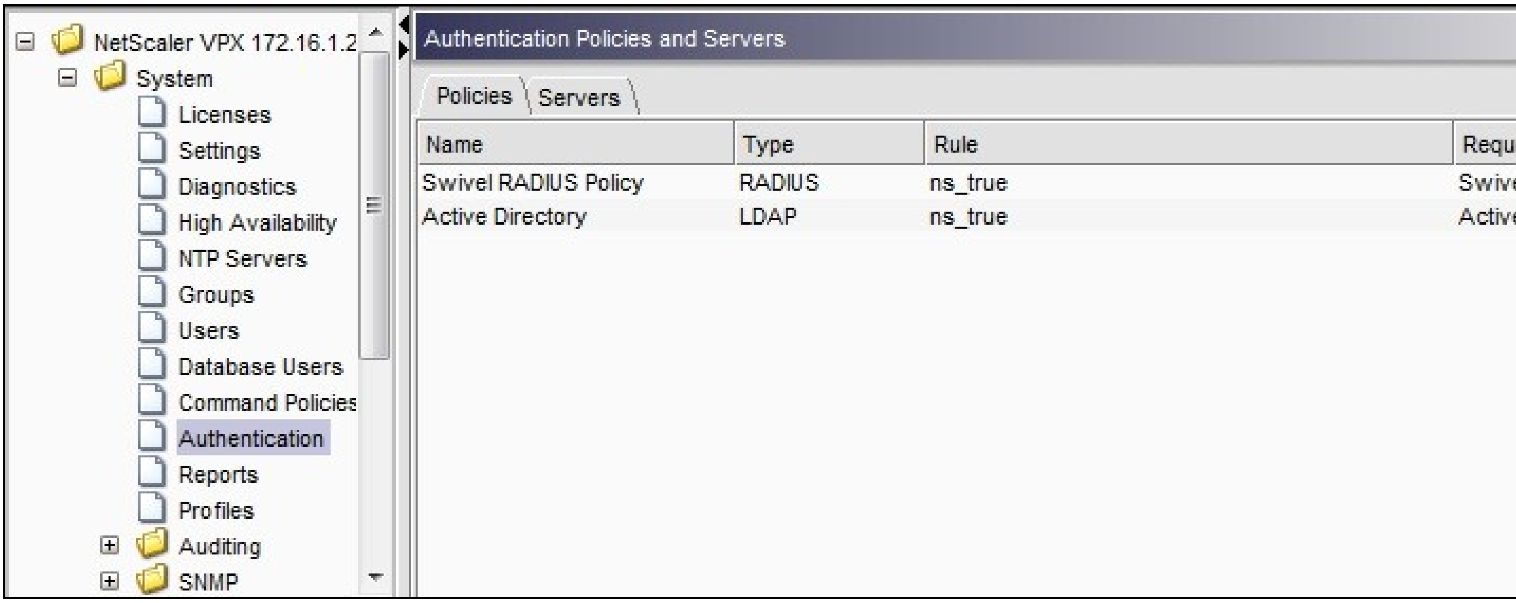
Authentication Type RADIUS

Server Swivel RADIUS

Expression
ns_true

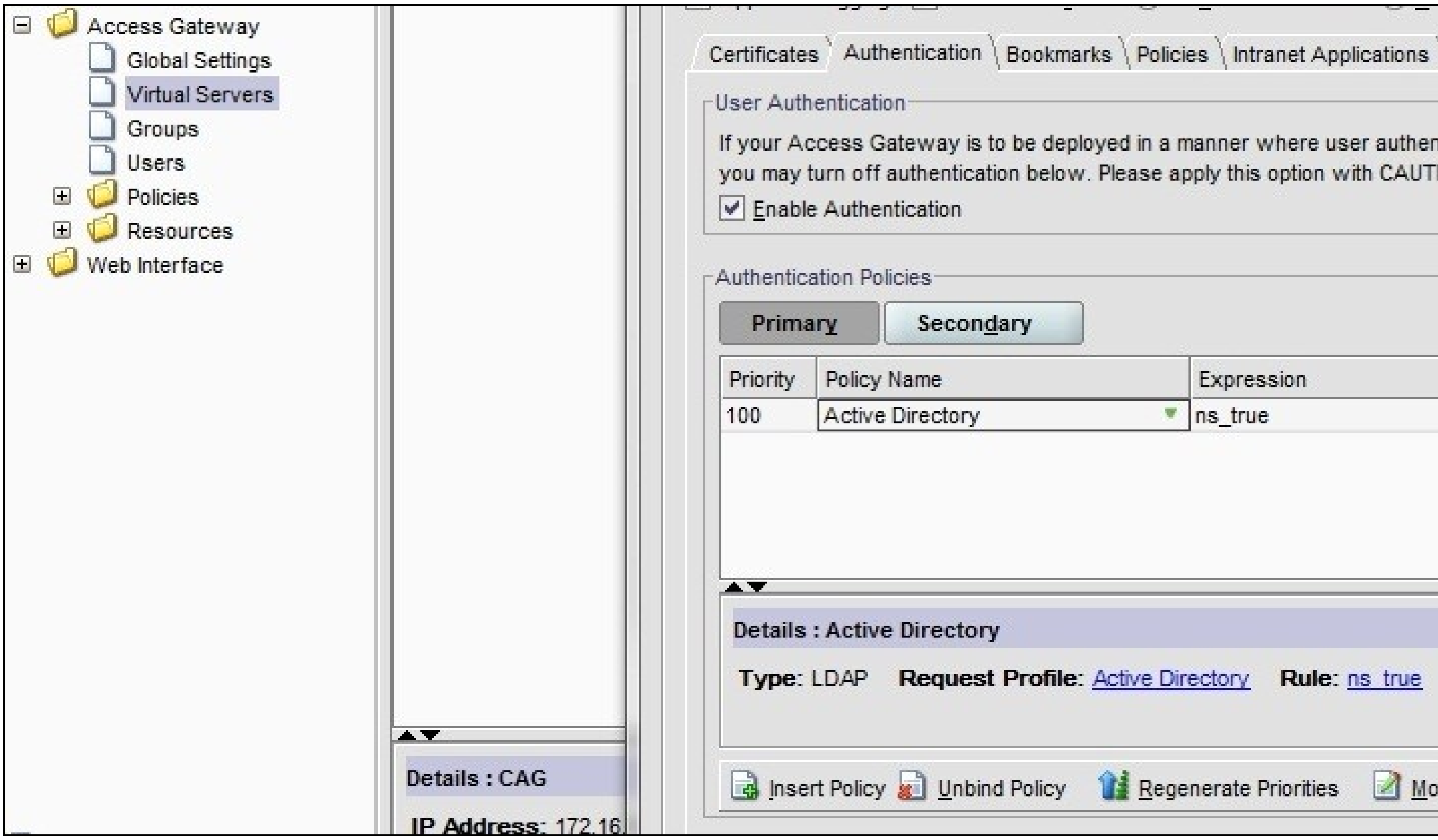
Named Expressions General True value

Preview Expression ns_true



Name	Type	Rule	Requ
Swivel RADIUS Policy	RADIUS	ns_true	Swive
Active Directory	LDAP	ns_true	Active

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



User Authentication

If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUTI

☑ Enable Authentication

Authentication Policies

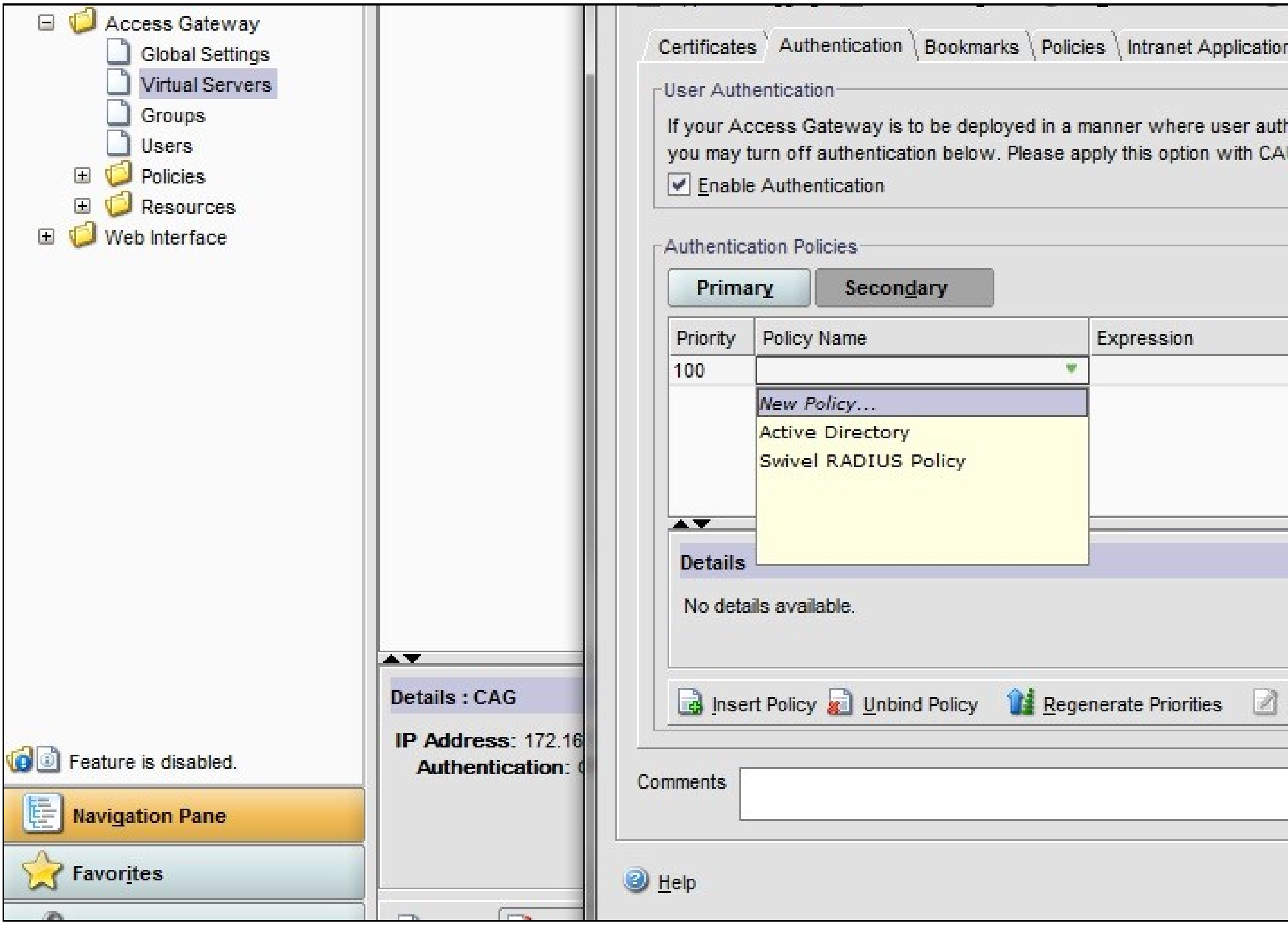
Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

Type: LDAP Request Profile: Active Directory Rule: ns_true

Details : CAG

IP Address: 172.16



If your Access Gateway is to be deployed in a manner where user auth
you may turn off authentication below. Please apply this option with CA

☑ Enable Authentication

Priority	Policy Name	Expression
100		

Details

No details available.

Feature is disabled.

Details : CAG

IP Address: 172.16

Authentication:

48.2 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.

49 Additional Configuration Options

49.1 Login Page Customisation

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

49.1.1 Customisation Overview

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

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

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

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

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

49.1.2 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
```

49.1.3 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
```

49.1.4 Customise the login script

49.1.4.1 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

49.1.5 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).

49.1.5.1 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
```

49.1.6 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.

49.1.7 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.

49.1.8 Reboot Netscaler to verify files are copied across

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

49.2 Additional Login Customisation options

49.2.1 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%;"
```

49.2.2 Changing the button labels

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

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

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

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

49.2.3 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

49.2.4 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

49.2.5 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

49.3 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.

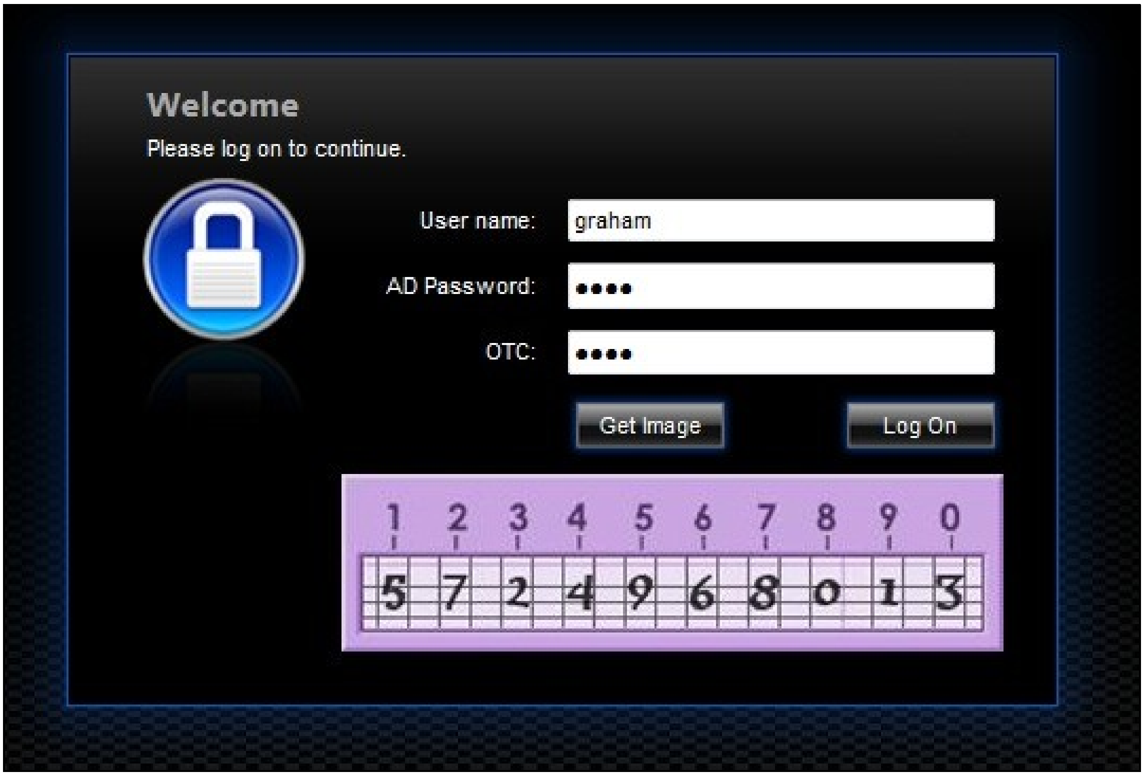
49.4 Image Request button displayed when needed

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

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

50 Testing

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



Welcome

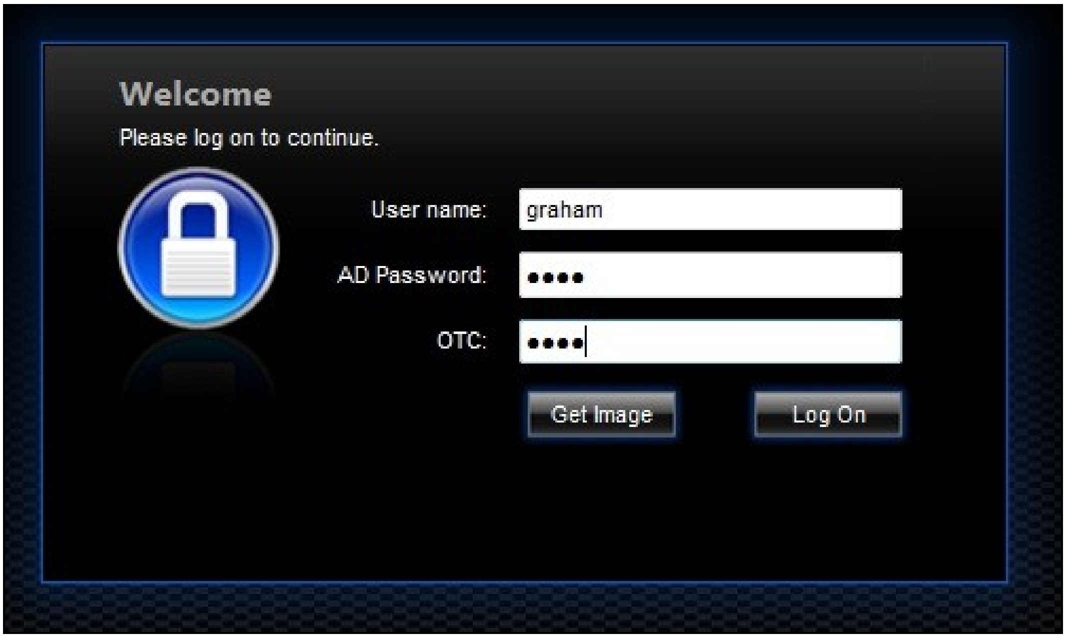
Please log on to continue.

User name: graham

AD Password: ●●●●

OTC: ●●●●

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



Welcome

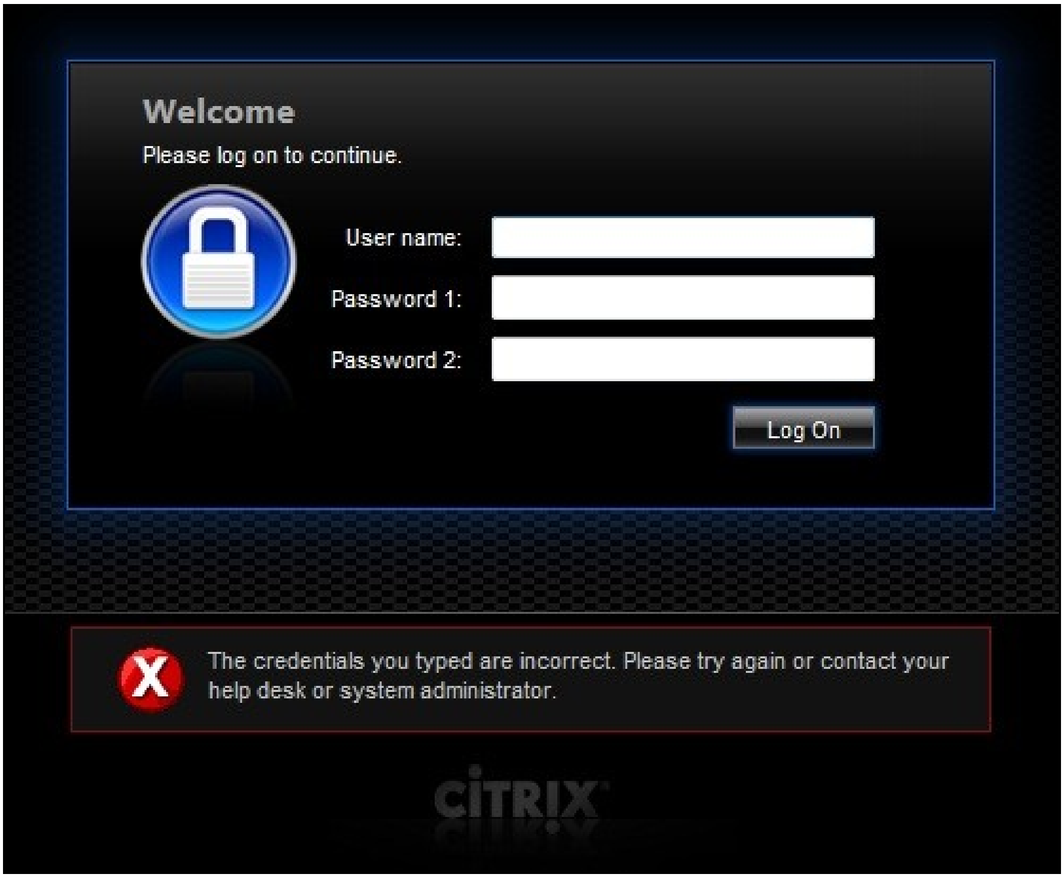
Please log on to continue.

User name: graham

AD Password: ●●●●

OTC: ●●●●

If the incorrect credentials are used then the login should fail

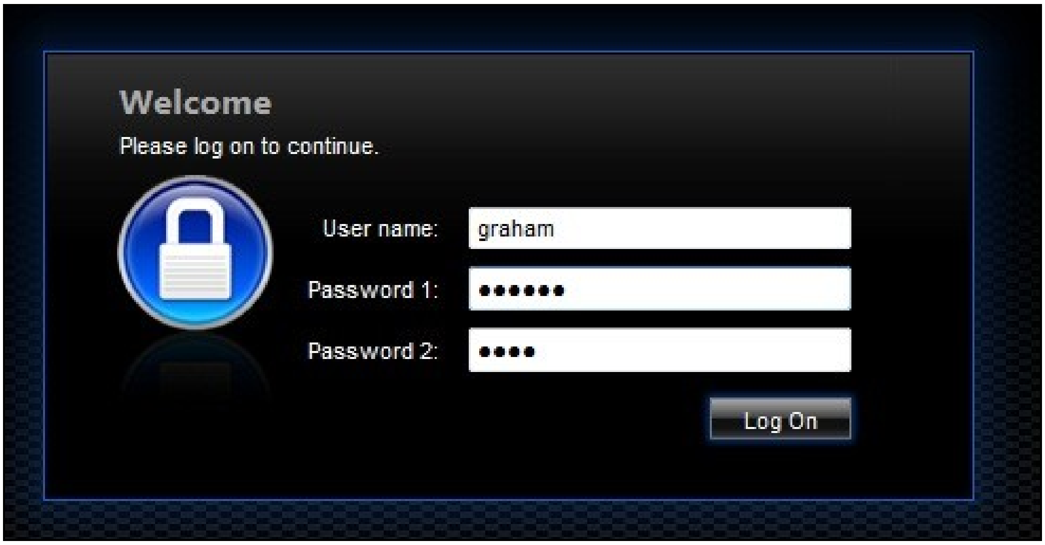


Welcome

Please log on to continue.

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

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



Welcome

Please log on to continue.

User name: graham

Password 1: ●●●●●●

Password 2: ●●●●

51 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.

52 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

53 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

54 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

55 Citrix Access Gateway Enterprise Edition 8

55.1 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.

55.2 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

55.3 Baseline

PINsafe 3.5

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

55.4 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.

56 Swivel Configuration

56.1 Configuring the RADIUS server

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

56.2 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.

56.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

56.3 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

56.3.1 Login Page Customisation

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

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

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

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

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

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

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

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

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

For a software only install see Software Only Installation

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

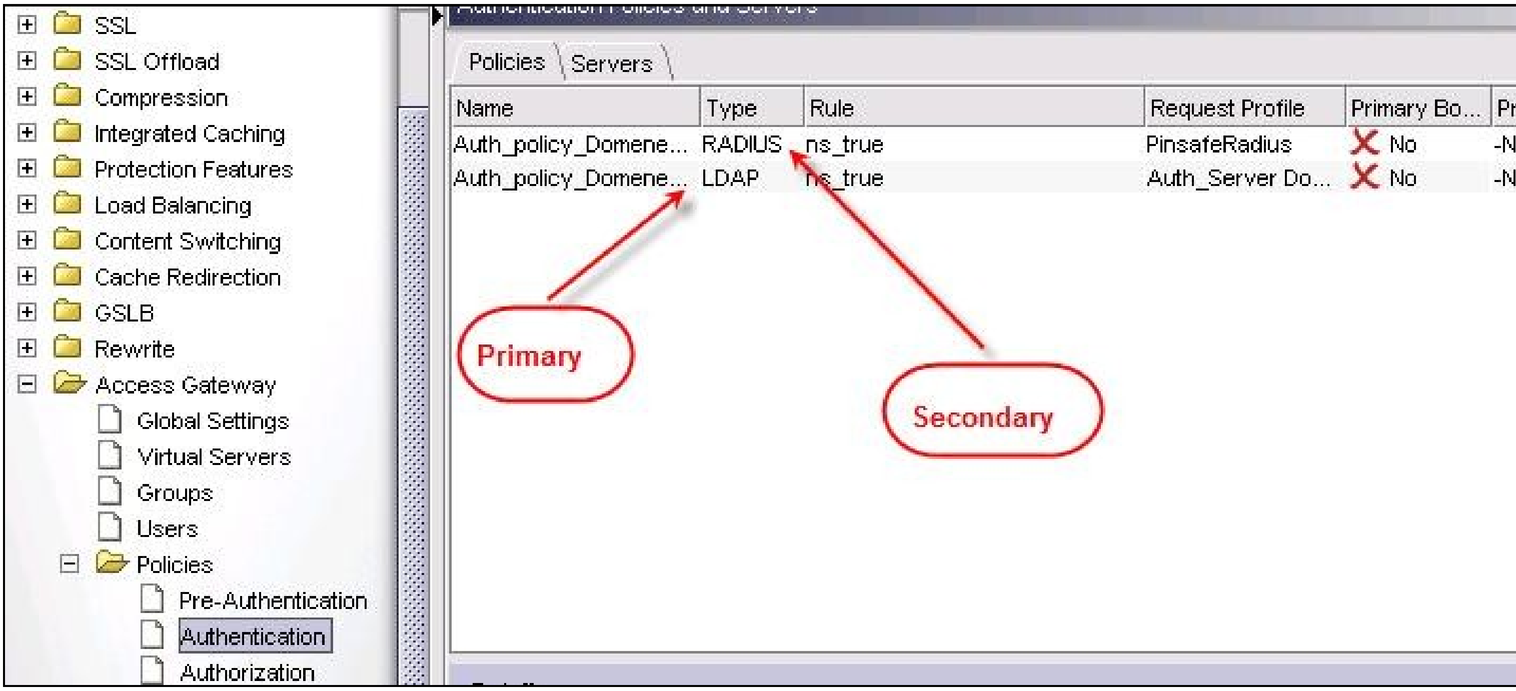
```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod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

56.3.2 Citrix Advanced Access Gateway Enterprise Edition RADIUS Cofiguration

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

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

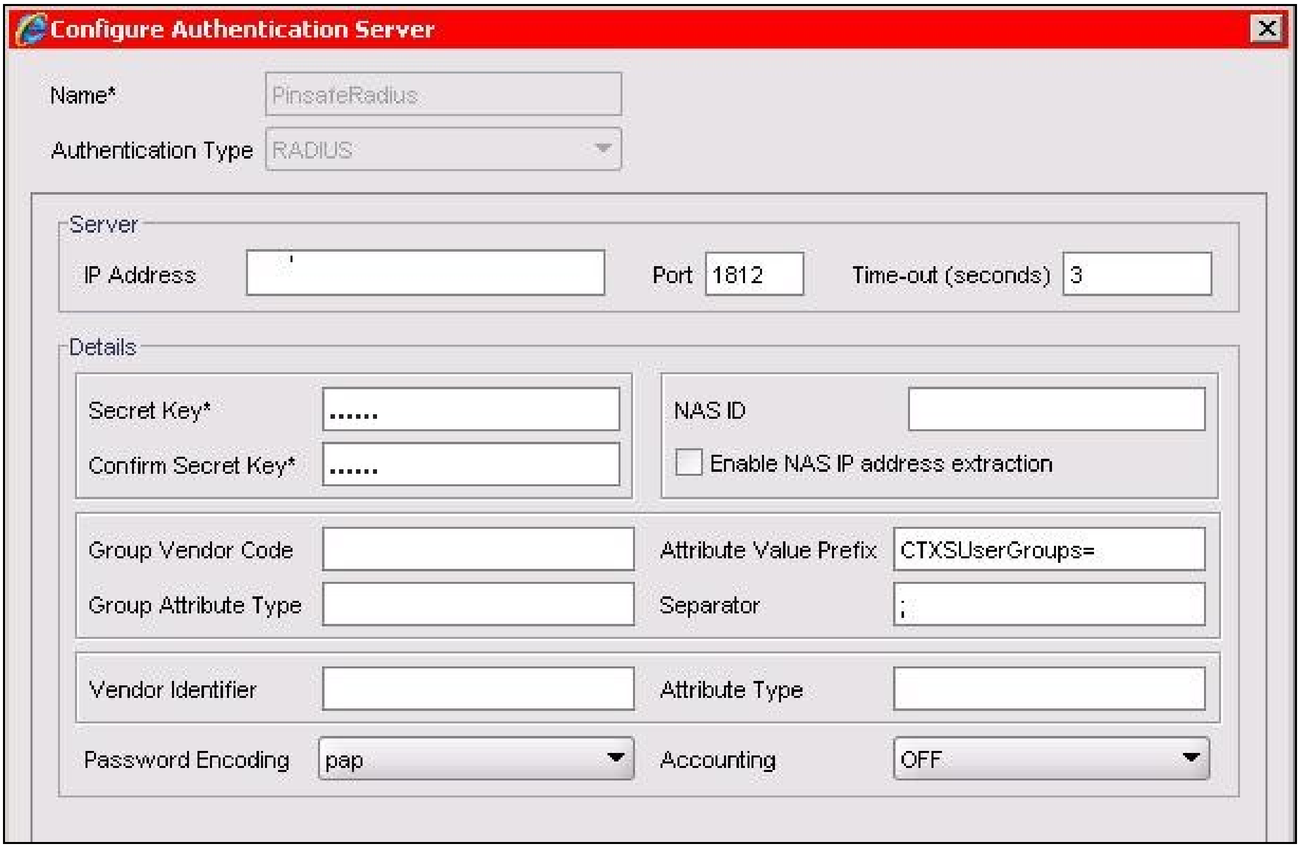
Create a new Authentication policy (under the Netscaler->System->Authentication menu). The policy must specify RADIUS and then the PINsafe server must be added as a RADIUS server.



Name	Type	Rule	Request Profile	Primary Bo...	Pr
Auth_policy_Domene...	RADIUS	ns_true	PinsafeRadius	✗ No	-N
Auth_policy_Domene...	LDAP	ns_true	Auth_Server Do...	✗ No	-N

Primary

Secondary


Configure Authentication Server

Name*	PinsafeRadius
Authentication Type	RADIUS

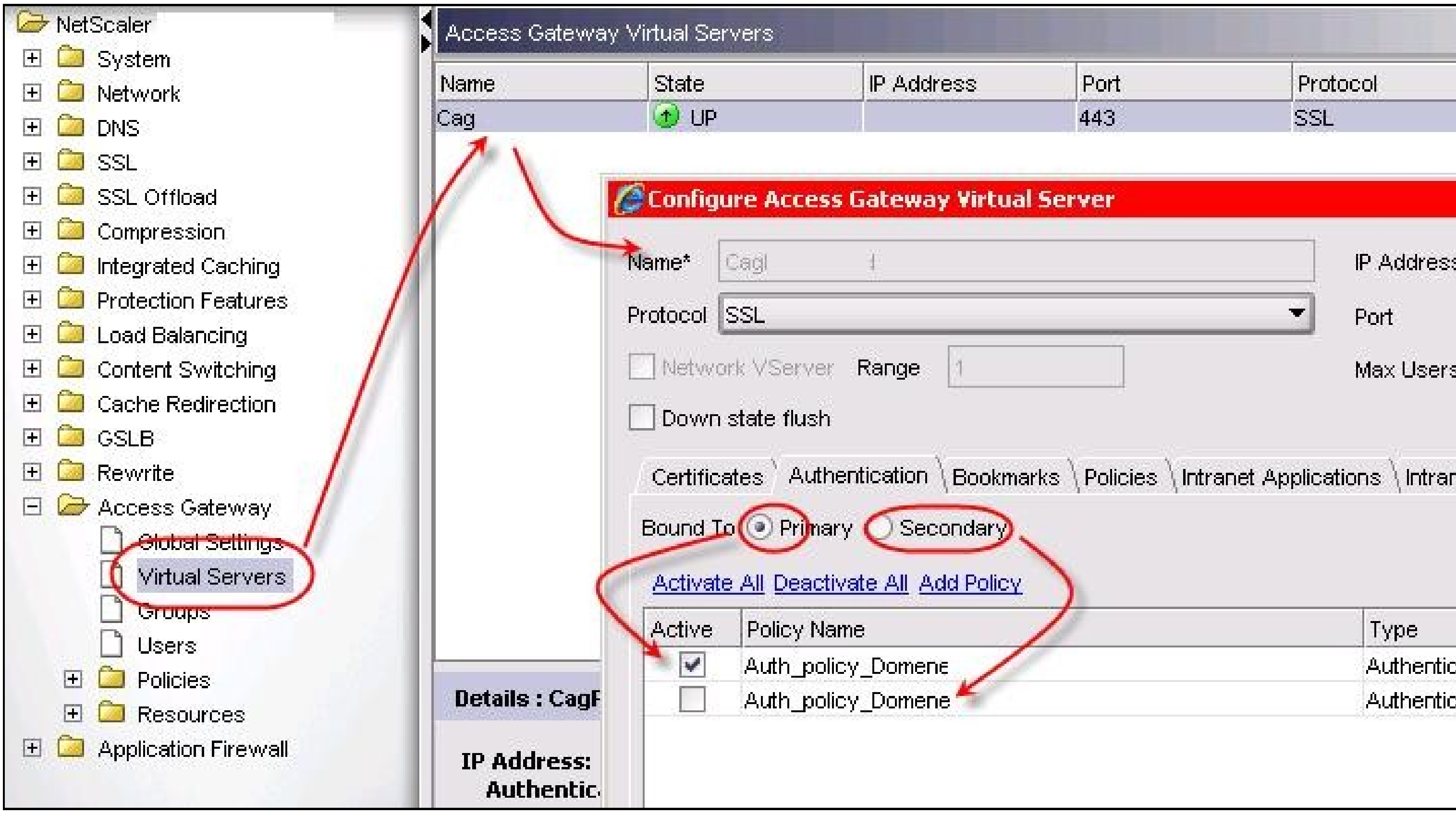
Server

IP Address		Port	1812	Time-out (seconds)	3

Details

Secret Key*	......	NAS ID	
Confirm Secret Key*	......	☐ 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.



Access Gateway Virtual Servers

Name	State	IP Address	Port	Protocol
Cag	UP		443	SSL

Configure Access Gateway Virtual Server

Name* Cagl
IP Address
Protocol SSL
Port
□ Network VServer Range 1
Max Users
□ Down state flush

Bound To ● Primary ○ Secondary

Active	Policy Name	Type
☑	Auth_policy_Domene	Authentic
□	Auth_policy_Domene	Authentic

Details : CagF

IP Address:
Authentic.

56.4 Additional Configuration Options

56.4.1 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.1 supports RADIUS Challenge and Response

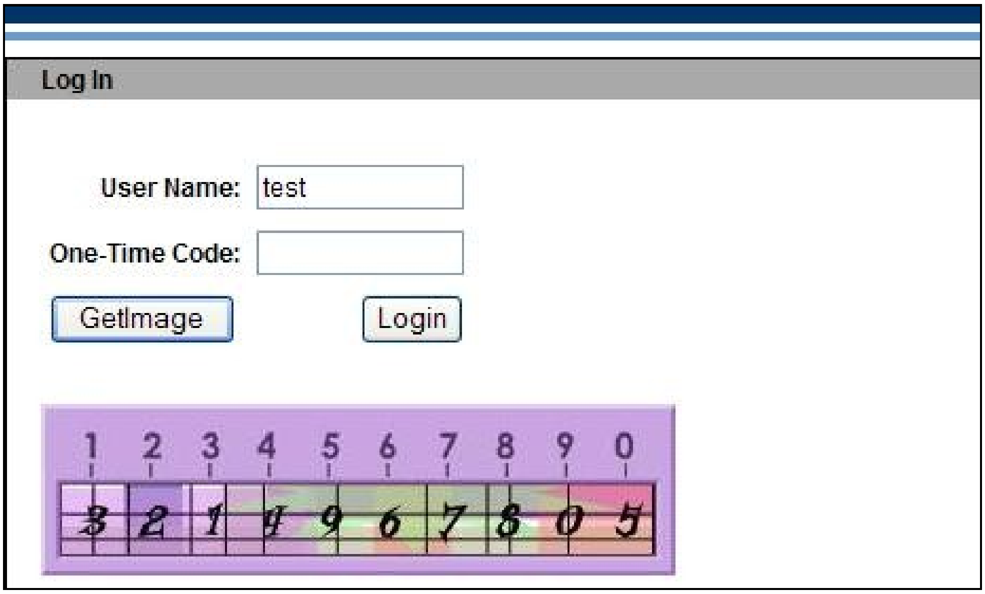
56.4.2 Image Request button displayed when needed

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

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

56.5 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:

56.6 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Image from PINsafe server absent

56.7 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]

56.8 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

57 Citrix Access Gateway Enterprise Edition 9

57.1 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.

57.2 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.

57.3 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

57.4 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.

58 Swivel Configuration

58.1 Configuring the RADIUS server

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

58.2 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.

58.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

58.3 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.

58.3.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

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

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

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

Name Swivel RADIUS

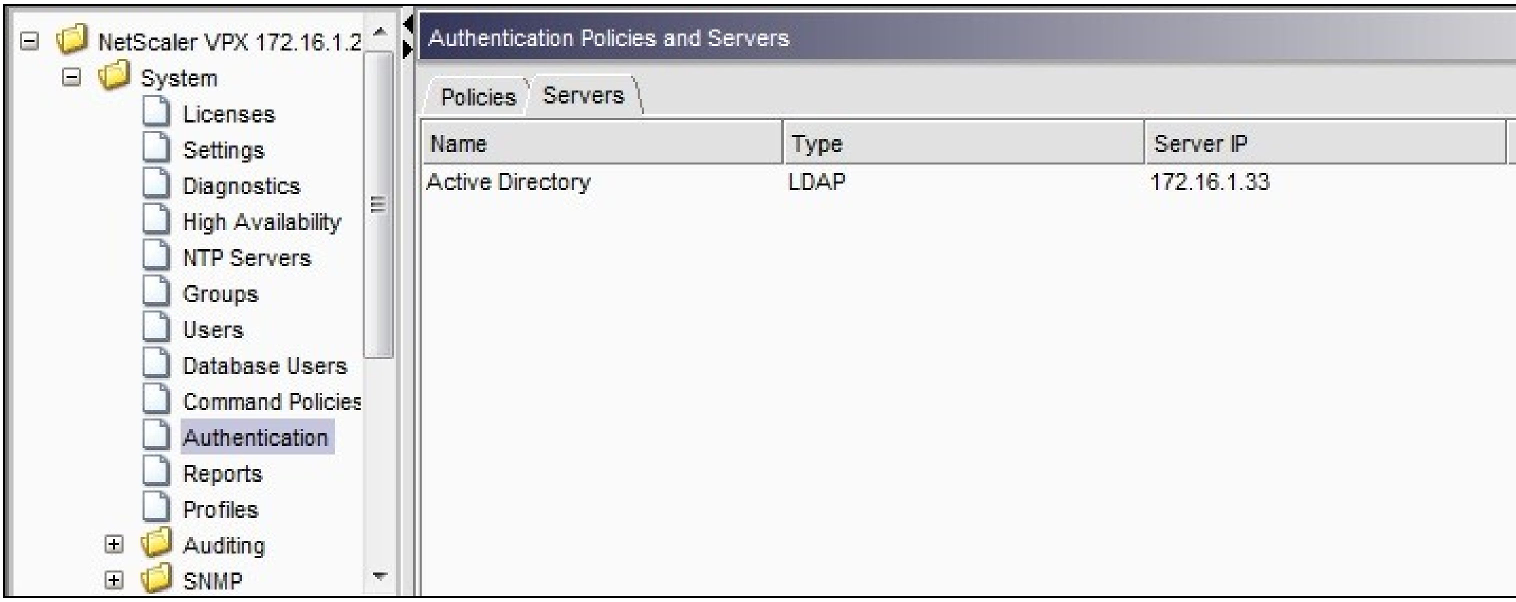
Authentication type RADIUS

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

Group Prefix CTXSUserGroups=

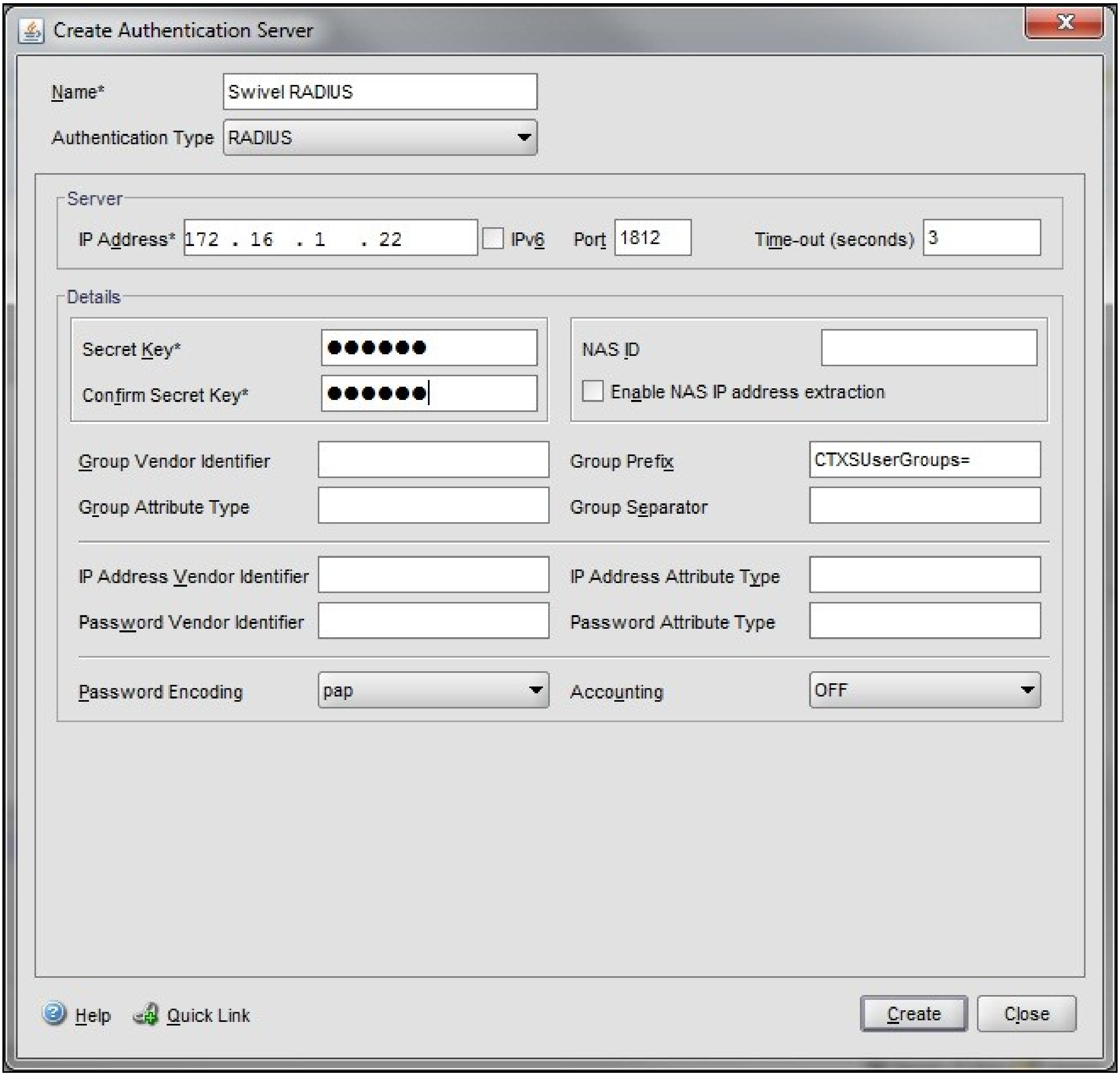
Group Separator ;

When complete click on Create.



Authentication Policies and Servers

Name	Type	Server IP
Active Directory	LDAP	172.16.1.33



Create Authentication Server

Name* Swivel RADIUS

Authentication Type RADIUS

Server

IP Address* 172 . 16 . 1 . 22 □ IPv6 Port 1812 Time-out (seconds) 3

Details

Secret Key* ●●●●●●

Confirm Secret Key* ●●●●●●

NAS ID

□ Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix CTXSUserGroups=

Group Attribute Type

Group Separator

IP Address Vendor Identifier

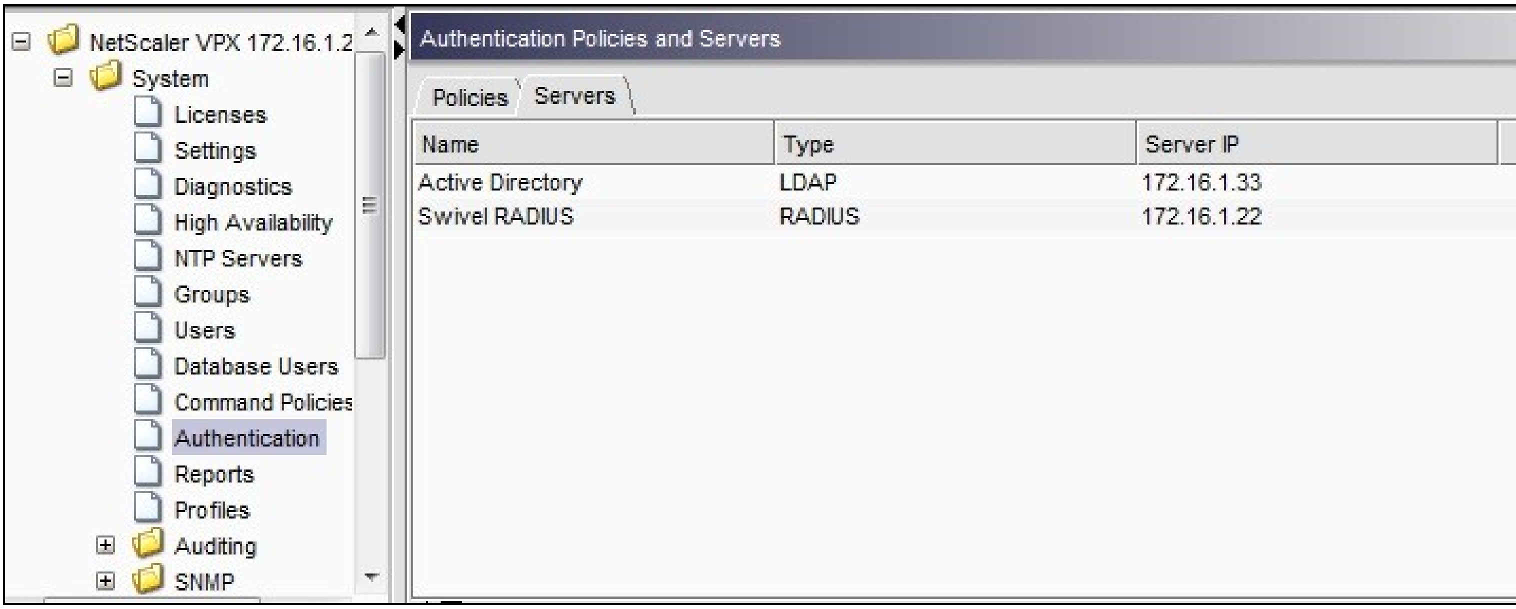
IP Address Attribute Type

Password Vendor Identifier

Password Attribute Type

Password Encoding pap

Accounting OFF



Name	Type	Server IP
Active Directory	LDAP	172.16.1.33
Swivel RADIUS	RADIUS	172.16.1.22

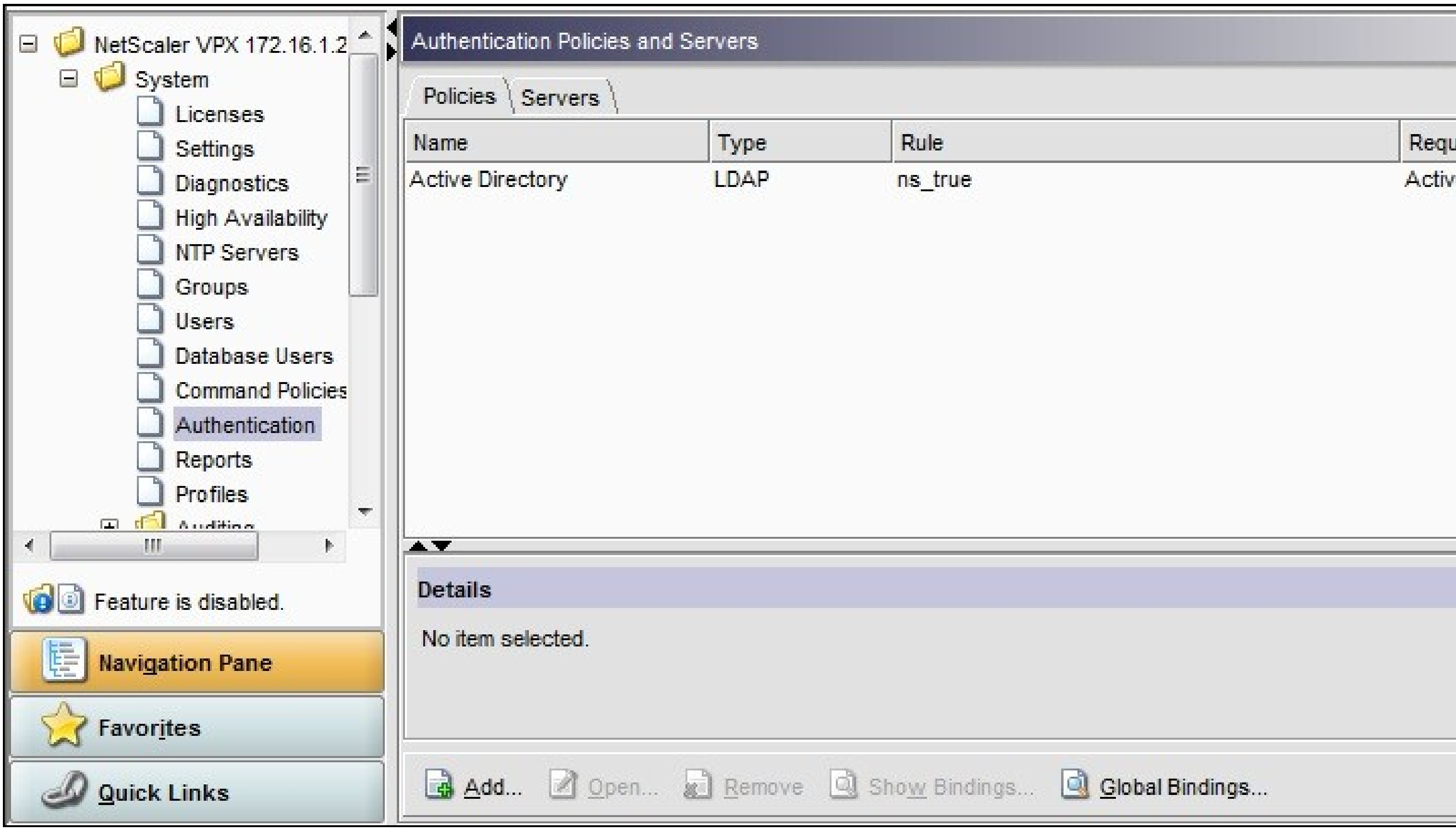
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

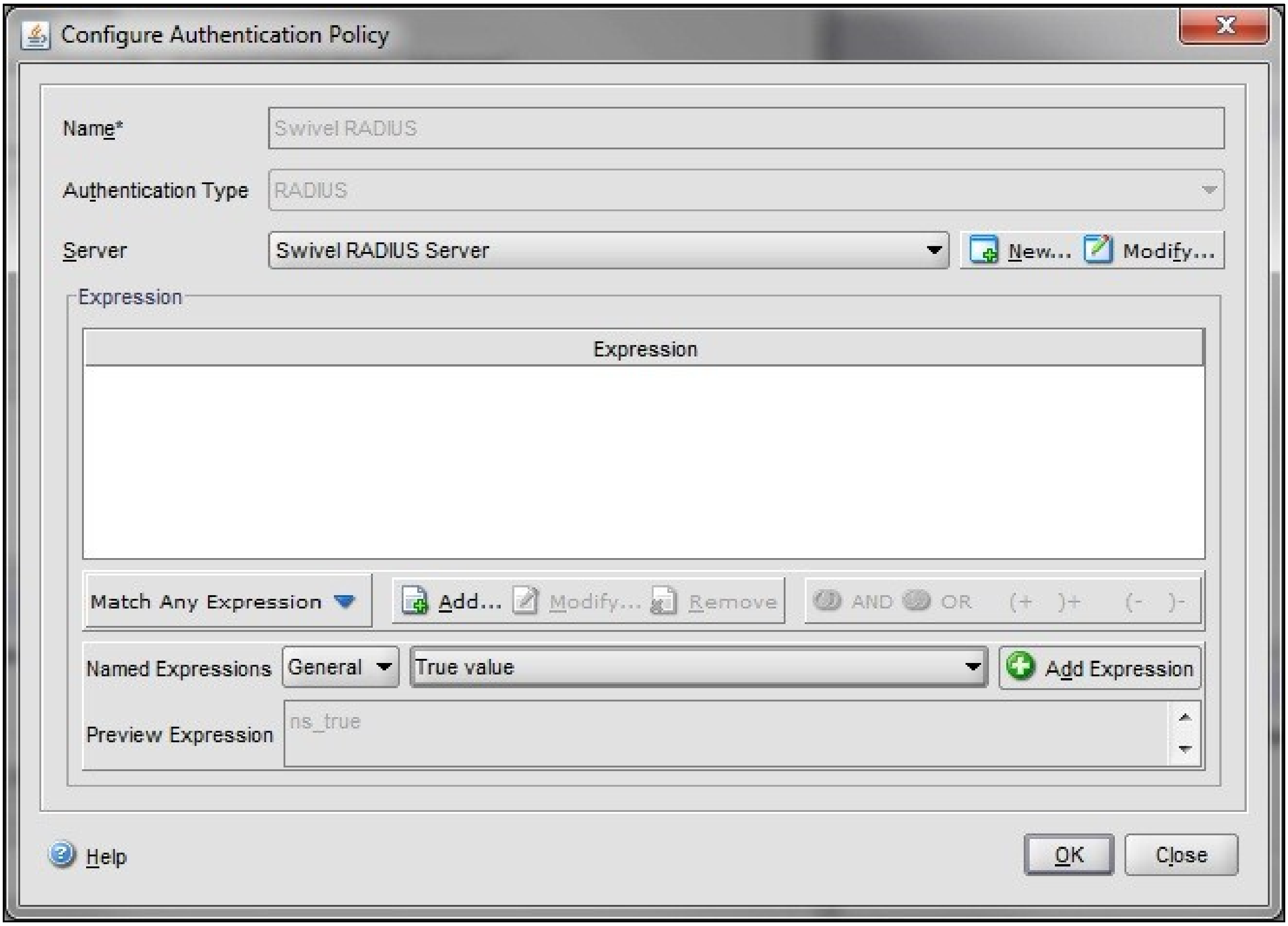
Server Swivel RADIUS

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



Name	Type	Rule	Requ
Active Directory	LDAP	ns_true	Activ

No item selected.



Configure Authentication Policy

Name* Swivel RADIUS

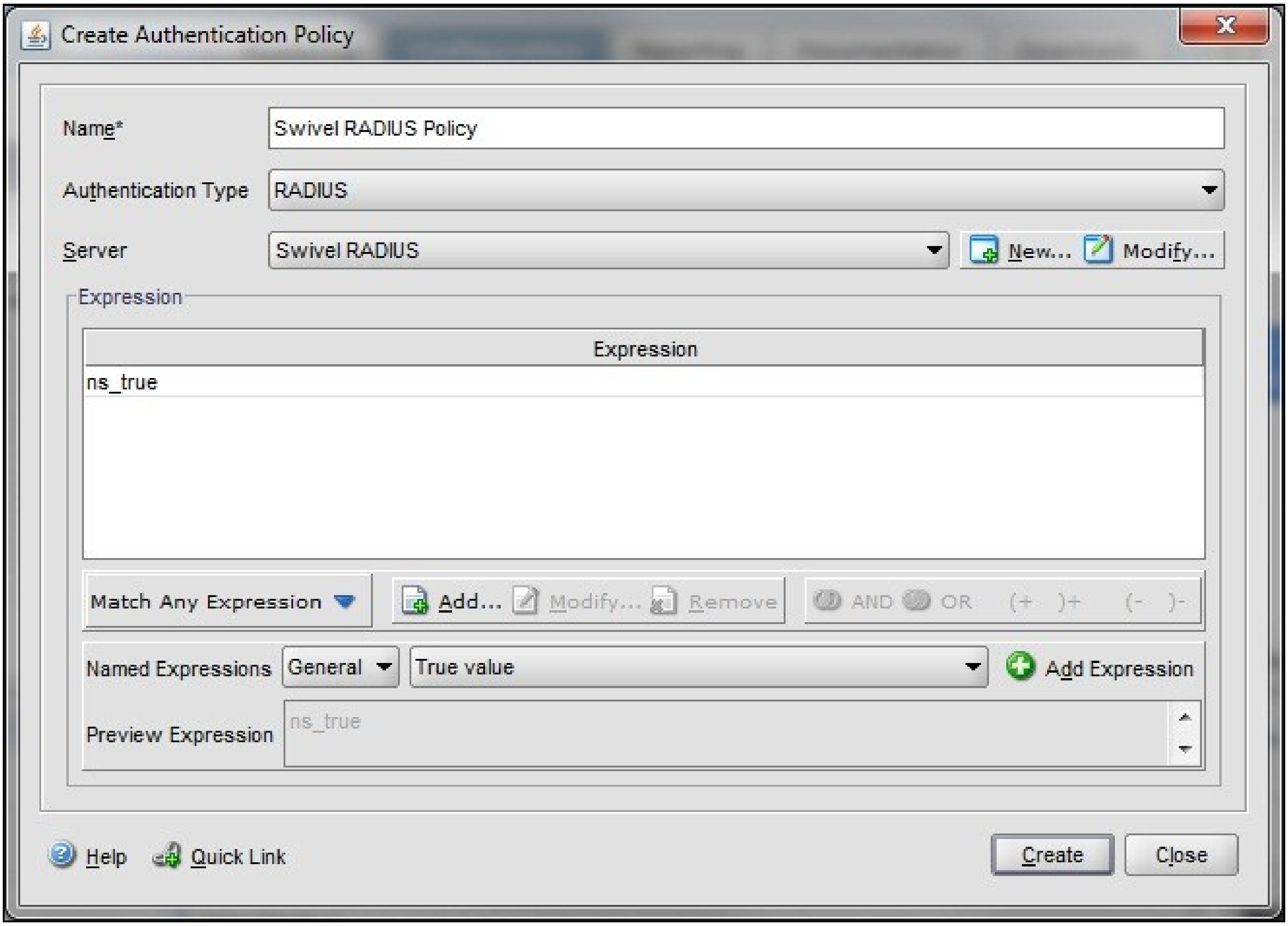
Authentication Type RADIUS

Server Swivel RADIUS Server

Expression

Named Expressions General True value

Preview Expression ns_true



Create Authentication Policy

Name*: Swivel RADIUS Policy

Authentication Type: RADIUS

Server: Swivel RADIUS

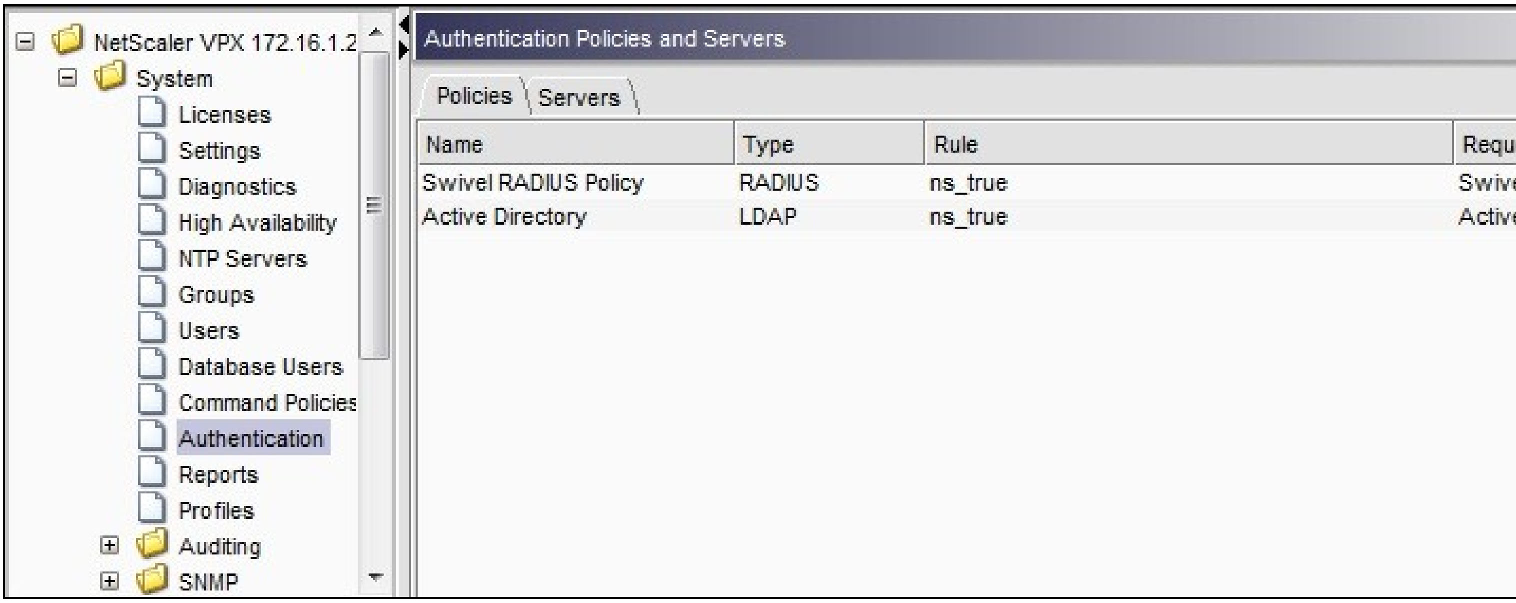
Expression

Expression
ns_true

Match Any Expression

Named Expressions: General, True value

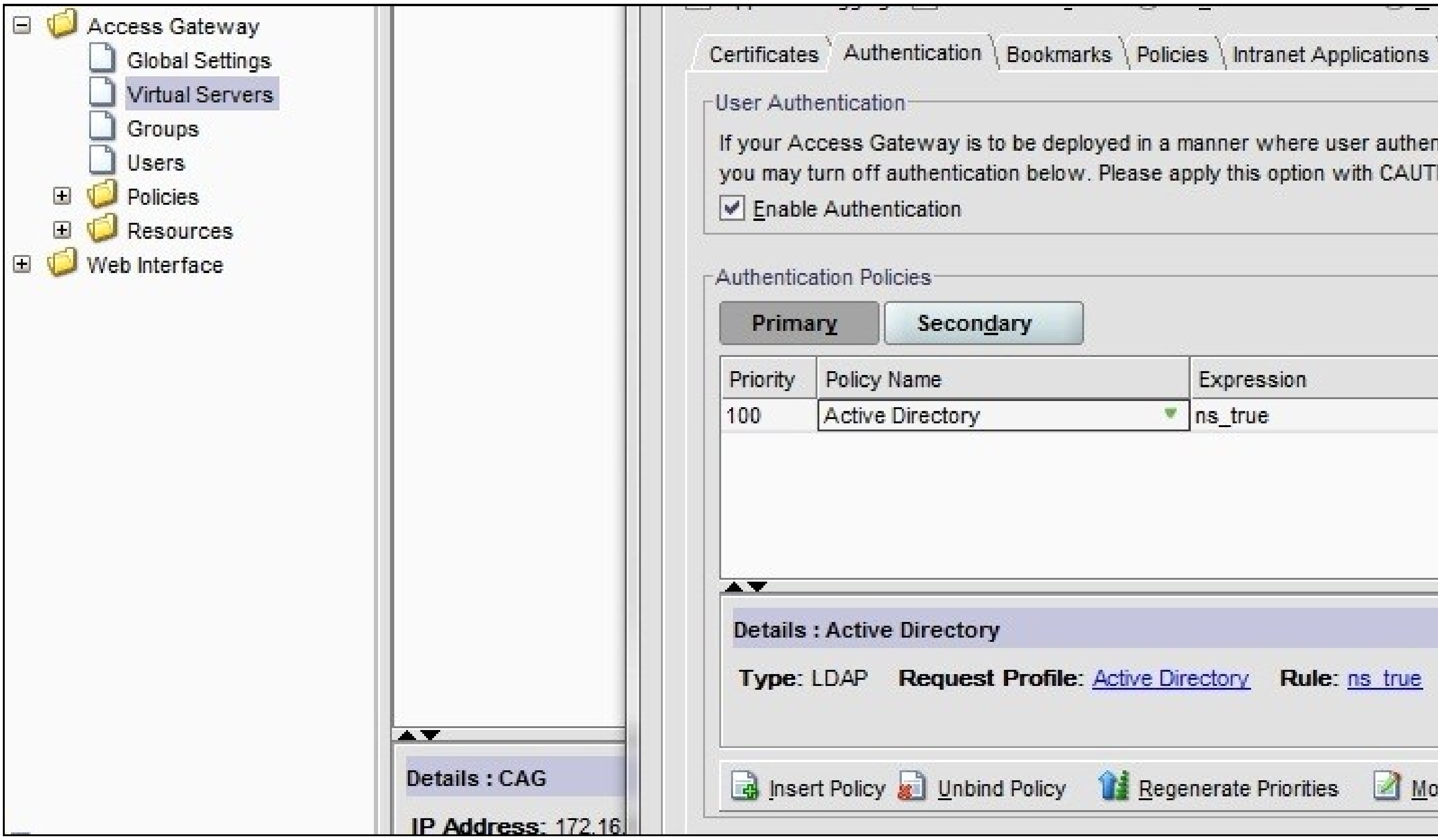
Preview Expression: ns_true



Authentication Policies and Servers

Name	Type	Rule	Requ
Swivel RADIUS Policy	RADIUS	ns_true	Swive
Active Directory	LDAP	ns_true	Active

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



IP Address: 172.16

User Authentication

If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUTI

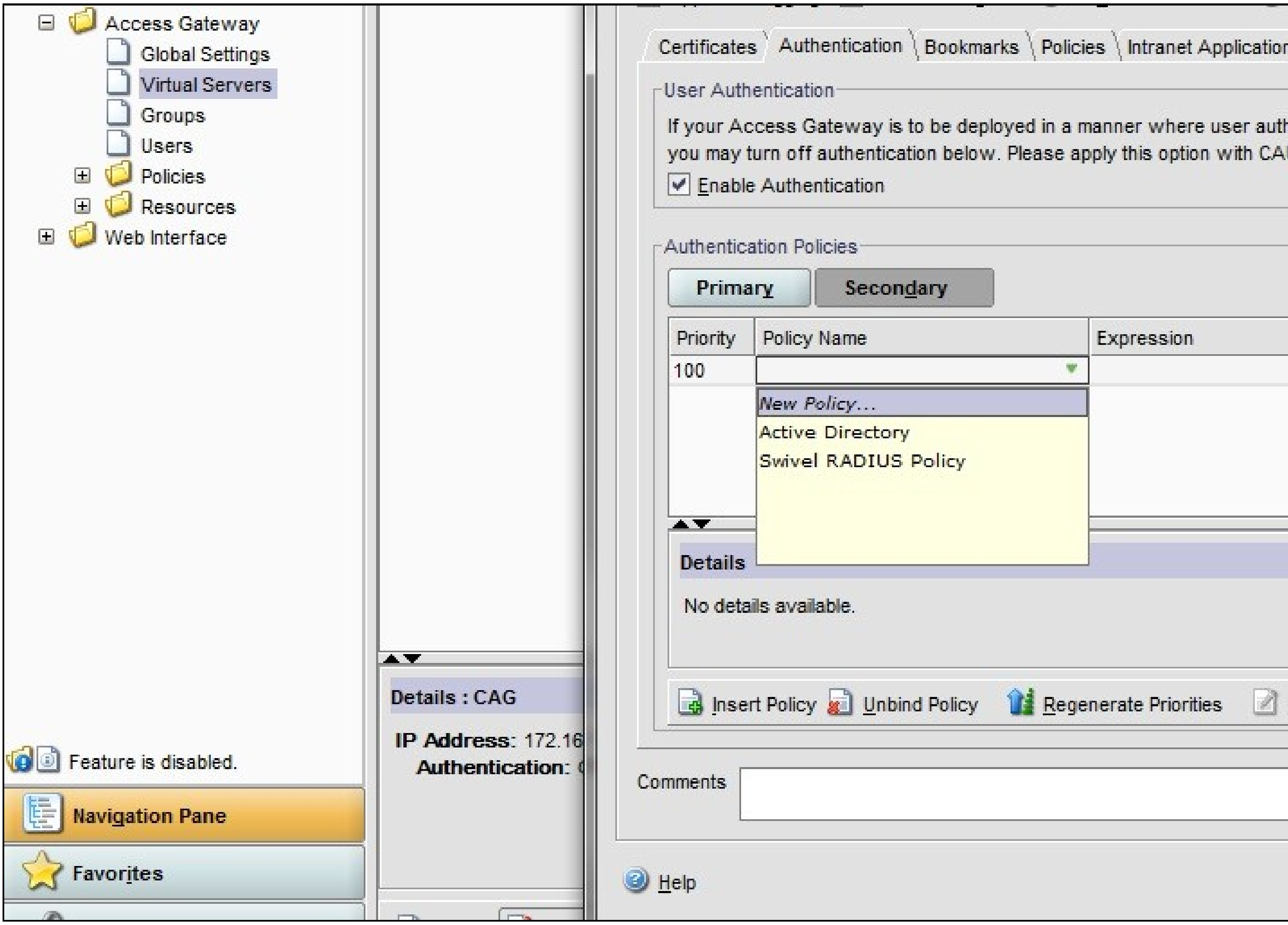
☑ Enable Authentication

Authentication Policies

Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

Type: LDAP Request Profile: Active Directory Rule: ns_true



Feature is disabled.

If your Access Gateway is to be deployed in a manner where user auth
you may turn off authentication below. Please apply this option with CA

☑ Enable Authentication

Priority	Policy Name	Expression
100		

No details available.

Details : CAG

IP Address: 172.16
Authentication: (

58.4 Additional Configuration Options

58.4.1 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.

58.4.1.1 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".

58.4.1.2 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";
```

58.4.1.3 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
```

58.4.1.4 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

58.4.2 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.

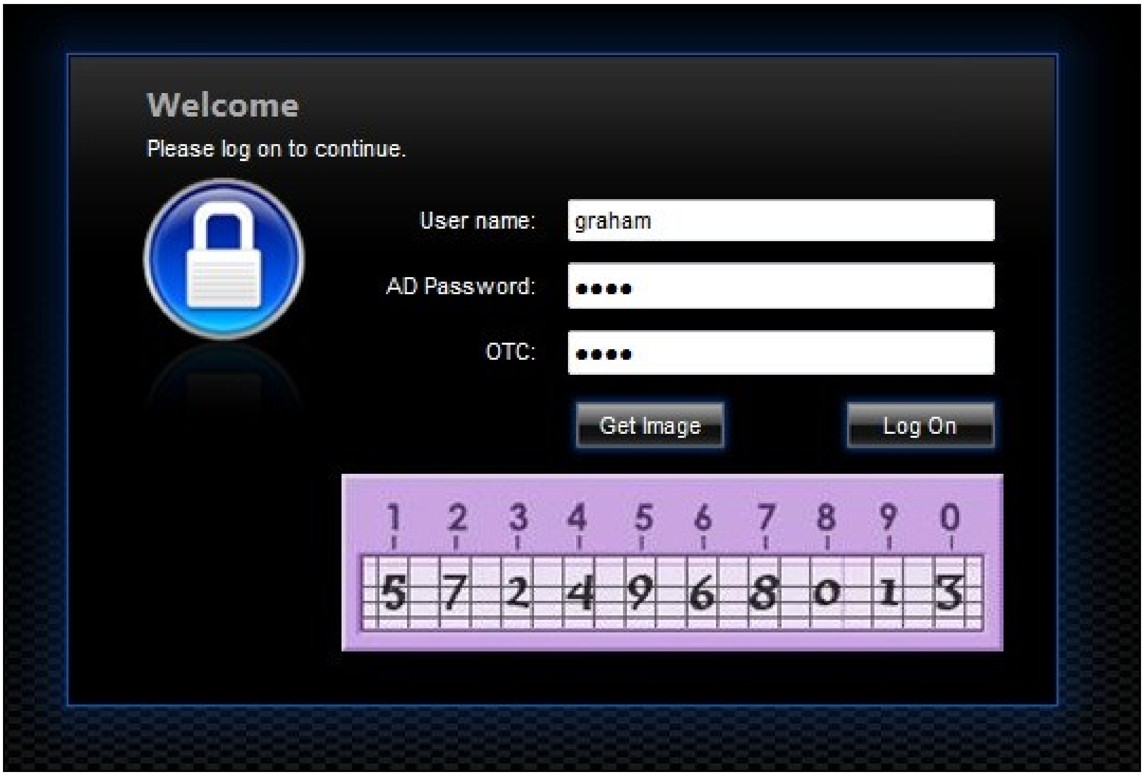
58.4.3 Image Request button displayed when needed

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

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

58.5 Testing

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



Welcome

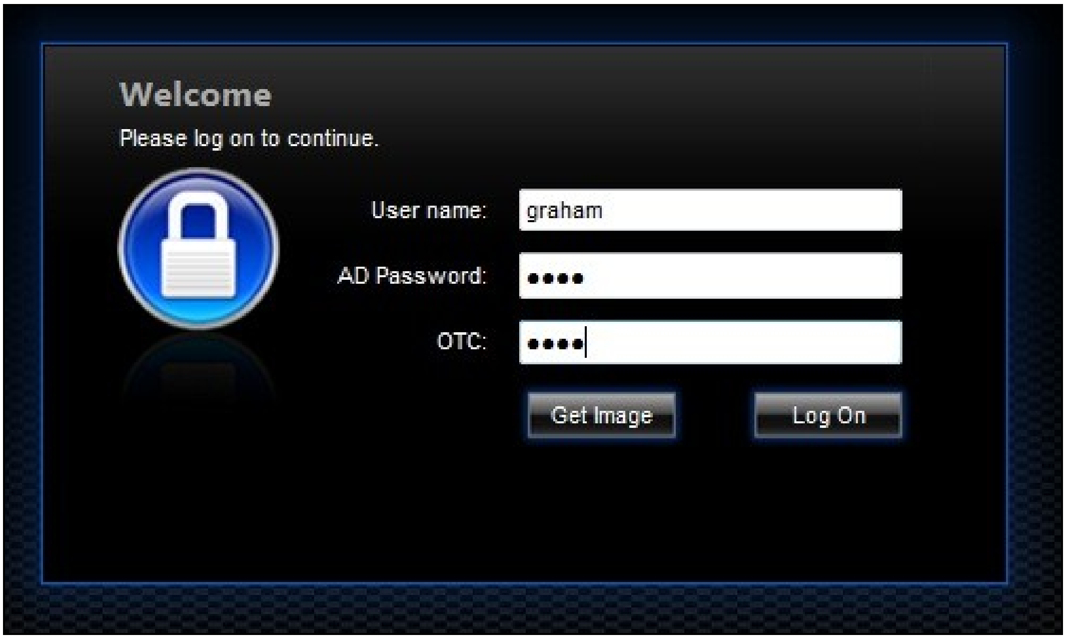
Please log on to continue.

User name: graham

AD Password: ●●●●

OTC: ●●●●

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



Welcome

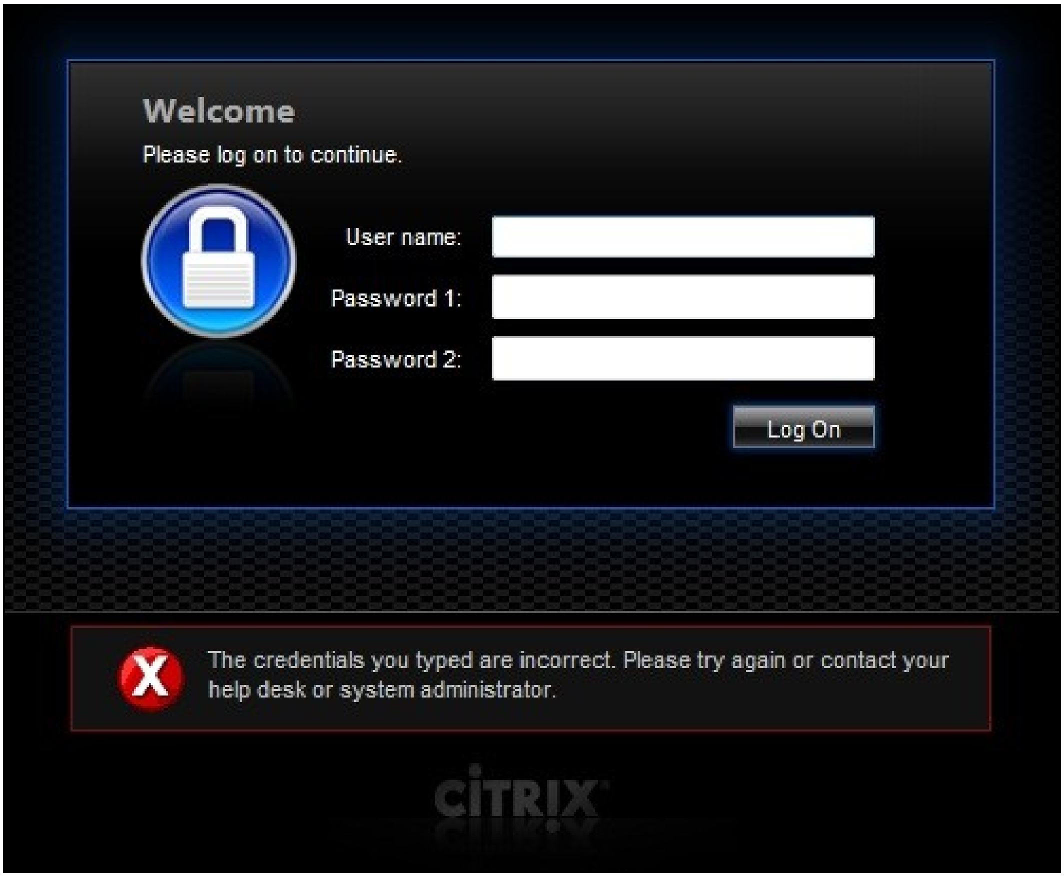
Please log on to continue.

User name: graham

AD Password: ●●●●

OTC: ●●●●

If the incorrect credentials are used then the login should fail



Welcome

Please log on to continue.

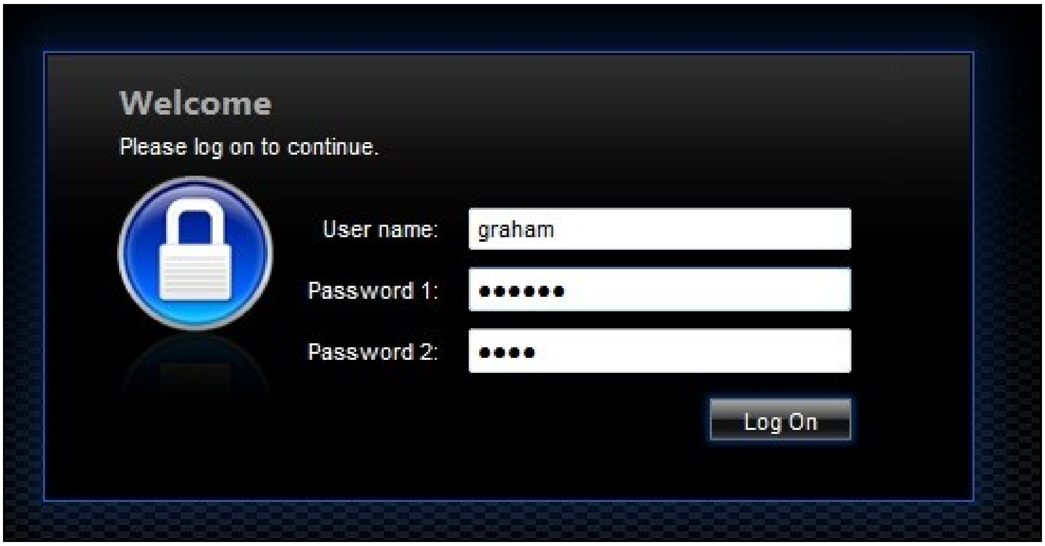
User name:

Password 1:

Password 2:

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

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



Welcome

Please log on to continue.

User name: graham

Password 1: ••••••

Password 2: ••••

58.6 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.

58.7 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.

58.8 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]

58.9 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

59 Citrix Netscaler configuration for Receiver

60 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

61 Prerequisites

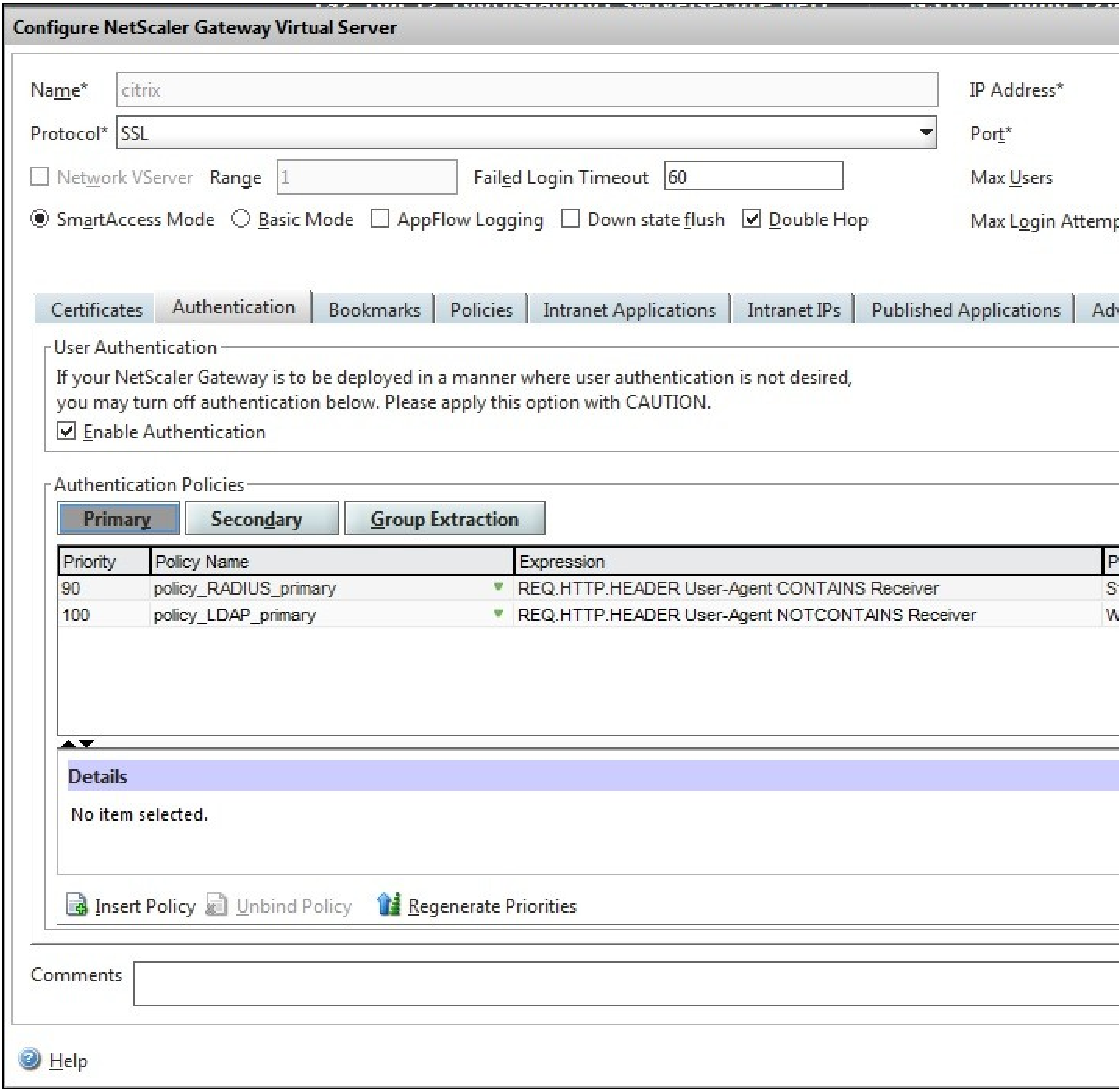
Citrix receiver Client

Swivel Appliance or Server

Citrix Netscaler

62 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 Attemp

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

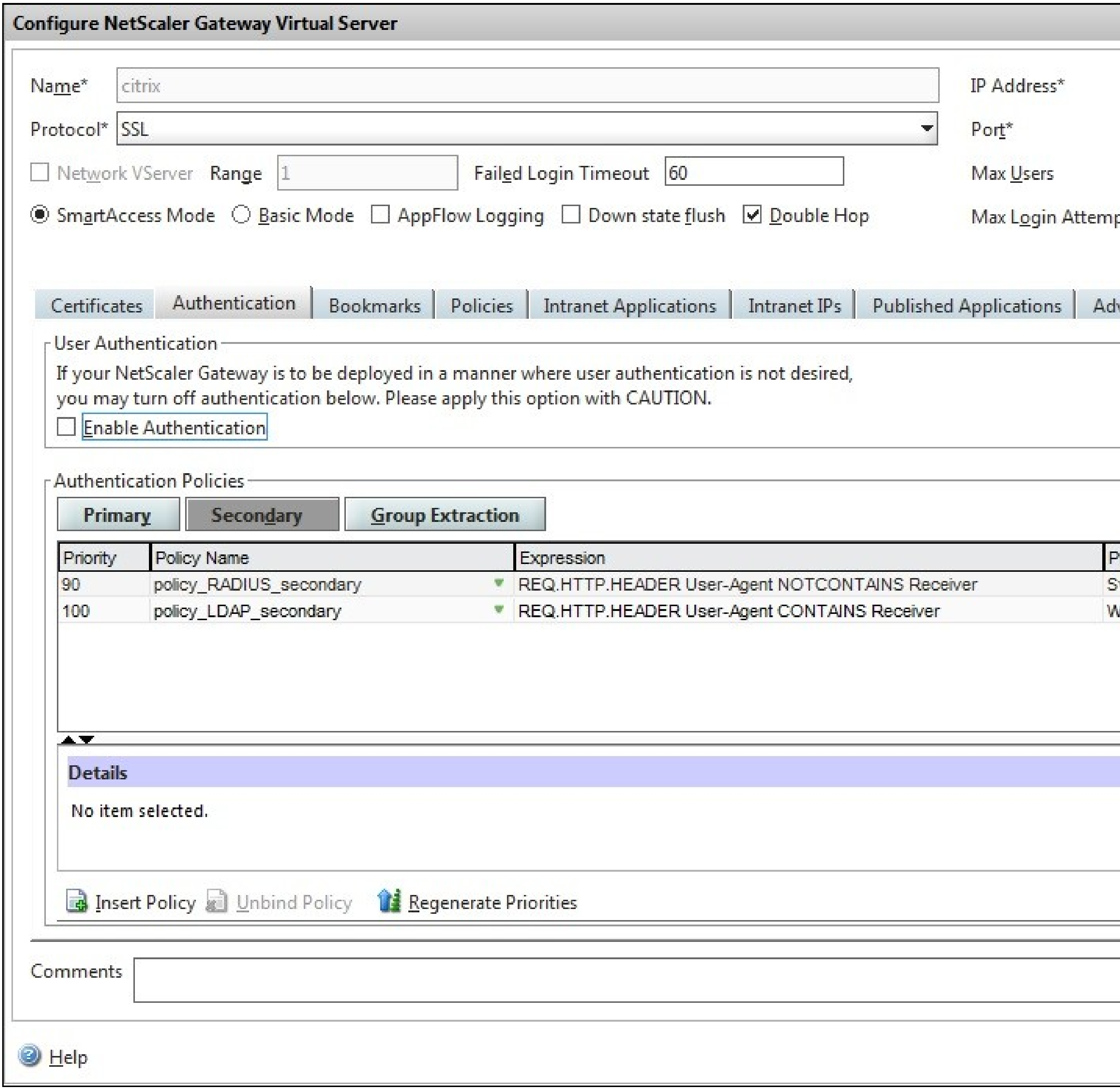
Authentication Policies

Priority	Policy Name	Expression	P
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.

Comments



Configure NetScaler Gateway Virtual Server

Name* citrix

IP Address*

Protocol* SSL

Port*

□ Network VServer Range 1 Failed Login Timeout 60

Max Users

● SmartAccess Mode ○ Basic Mode □ AppFlow Logging □ Down state flush ☑ Double Hop

Max Login Attemp

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

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.

Comments

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.

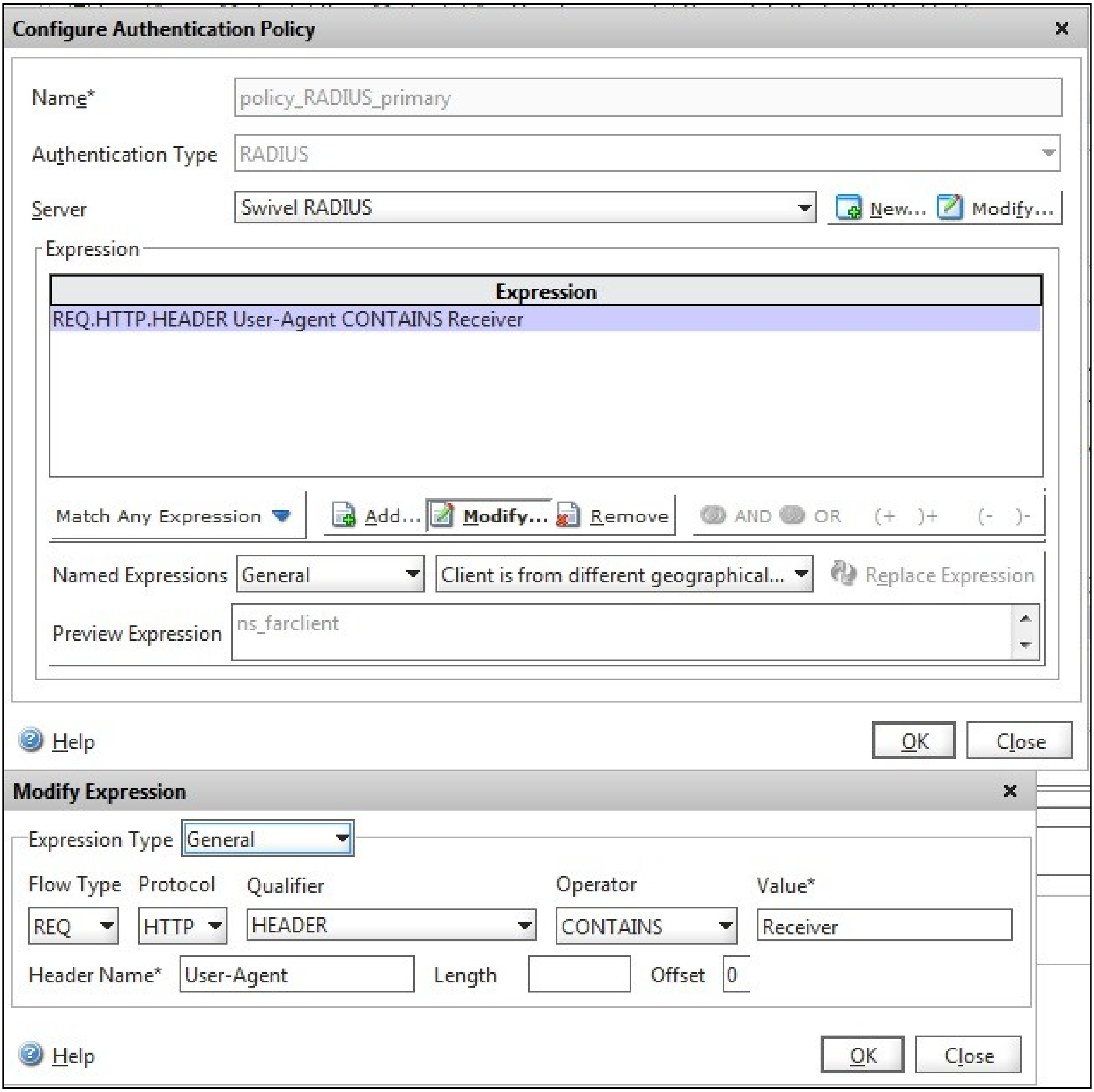
Receiver settings for Netscaler 10.0 and 10.1

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	EQ.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

Expression

Expression
REQ.HTTP.HEADER User-Agent CONTAINS Receiver

Match Any Expression

Named Expressions General — Client is from different geographical...

Preview Expression ns_farclient

Modify Expression

Expression Type General

Flow Type	Protocol	Qualifier	Operator	Value*
REQ	HTTP	HEADER	CONTAINS	Receiver

Header Name* User-Agent Length Offset 0

63 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

64 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

65 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)

66 Citrix Netscaler Gateway 10.x

67 Introduction

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 10.1 and 10.5 (Netscaler VPN). Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

For version 10.0 refer to Citrix Access Gateway Enterprise Edition 10

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

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

It covers the following steps.

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

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

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

68 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.

68.1 Note on upgrading the Netscaler

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

69 Baseline

Tested with Swivel 3.9.6

Citrix Netscaler Gateway NS10.1 Build 121.10

Citrix Netscaler Gateway NS10.5

70 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.

71 Swivel Configuration

71.1 Configuring the RADIUS server

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

71.2 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.

71.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

72 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.

72.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

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

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

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

Name Swivel RADIUS

Authentication type RADIUS

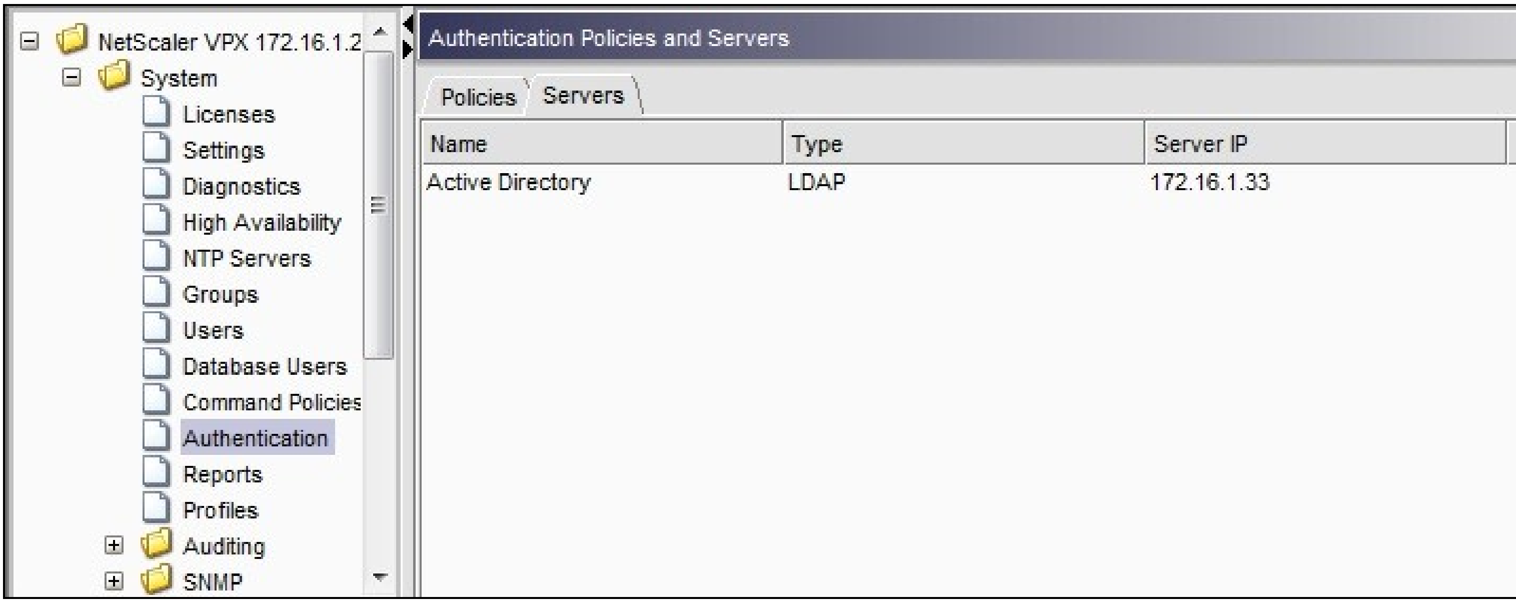
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix CTXSUserGroups=

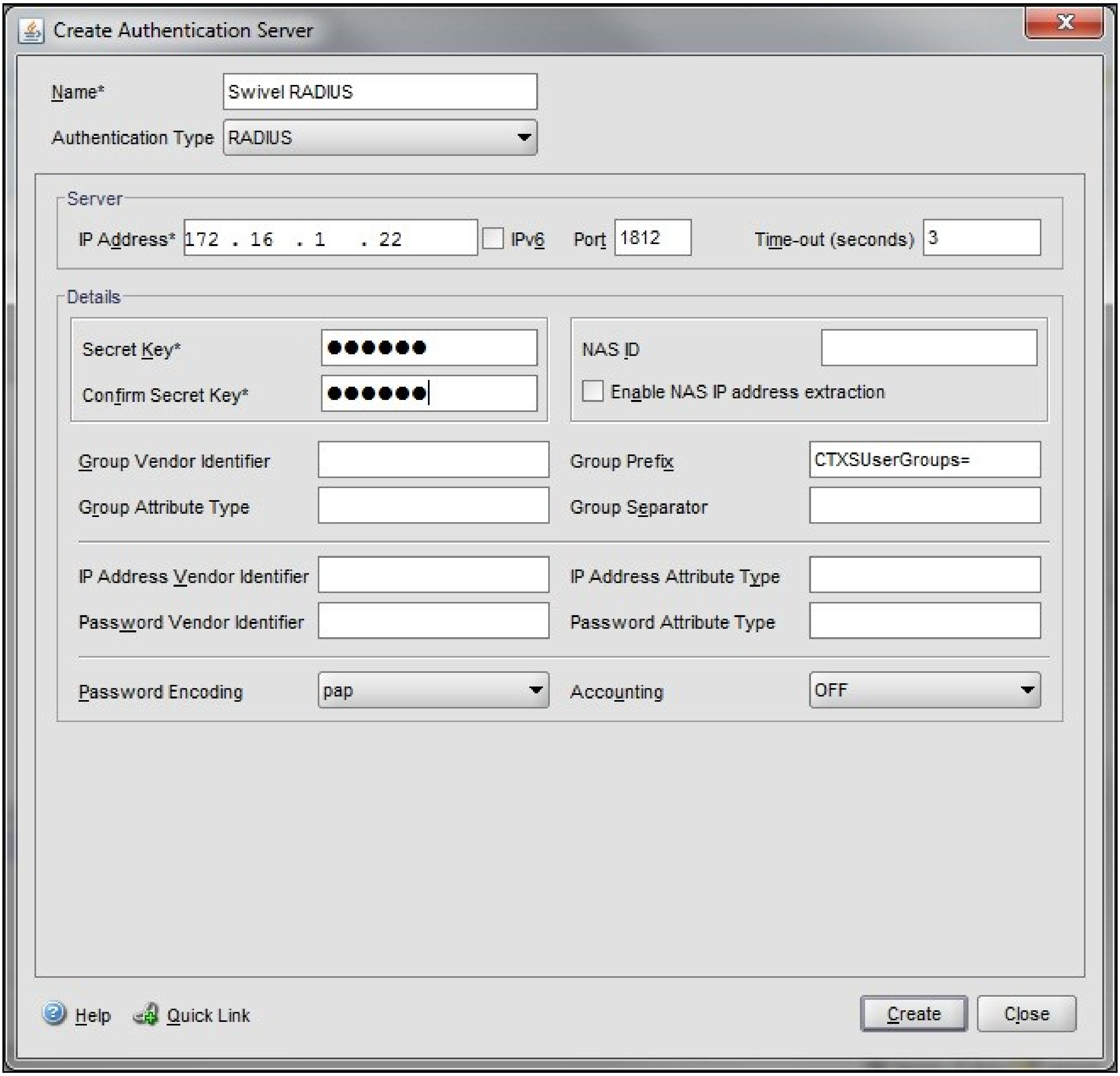
Group Separator ;

When complete click on Create.

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



Name	Type	Server IP
Active Directory	LDAP	172.16.1.33



Create Authentication Server

Name* Swivel RADIUS

Authentication Type RADIUS

Server

IP Address* 172 . 16 . 1 . 22 □ IPv6 Port 1812 Time-out (seconds) 3

Details

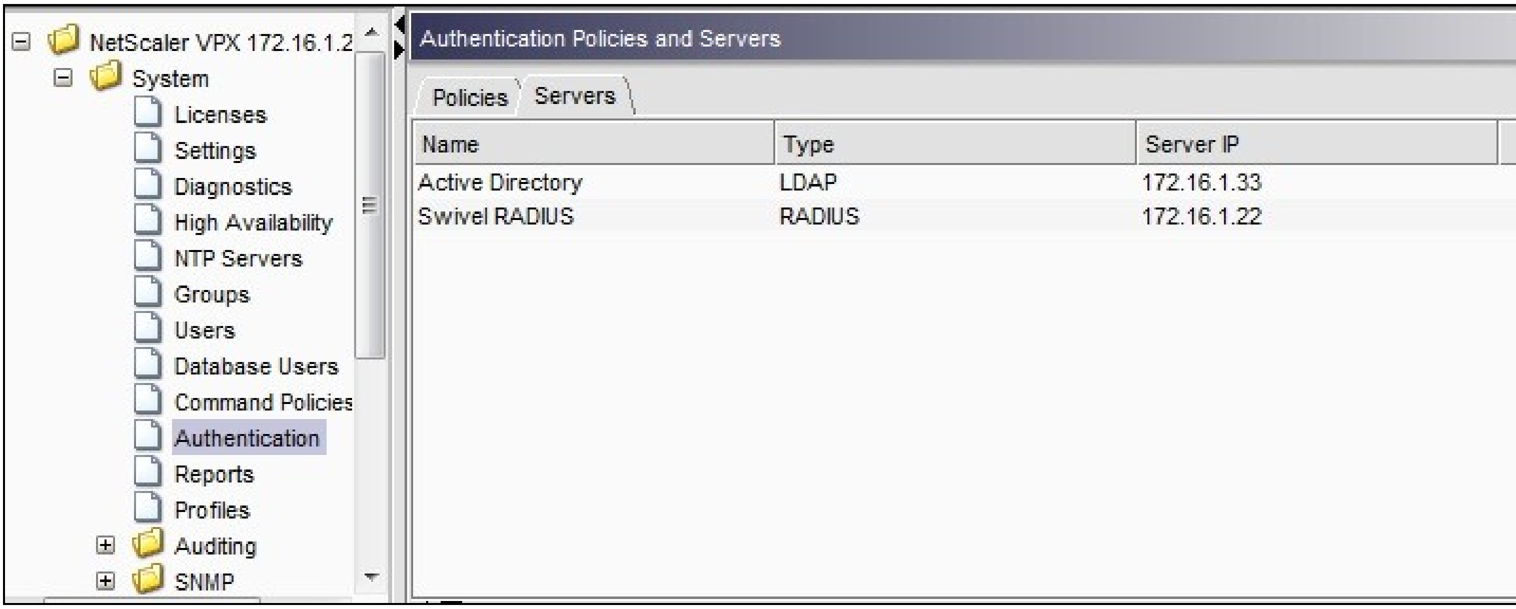
Secret Key* ●●●●●●

Confirm Secret Key* ●●●●●●

NAS ID

□ Enable NAS IP address extraction

Group Vendor Identifier		Group Prefix	CTXSUserGroups=
Group Attribute Type		Group Separator	
IP Address Vendor Identifier		IP Address Attribute Type	
Password Vendor Identifier		Password Attribute Type	
Password Encoding	pap	Accounting	OFF



Authentication Policies and Servers

Name	Type	Server IP
Active Directory	LDAP	172.16.1.33
Swivel RADIUS	RADIUS	172.16.1.22

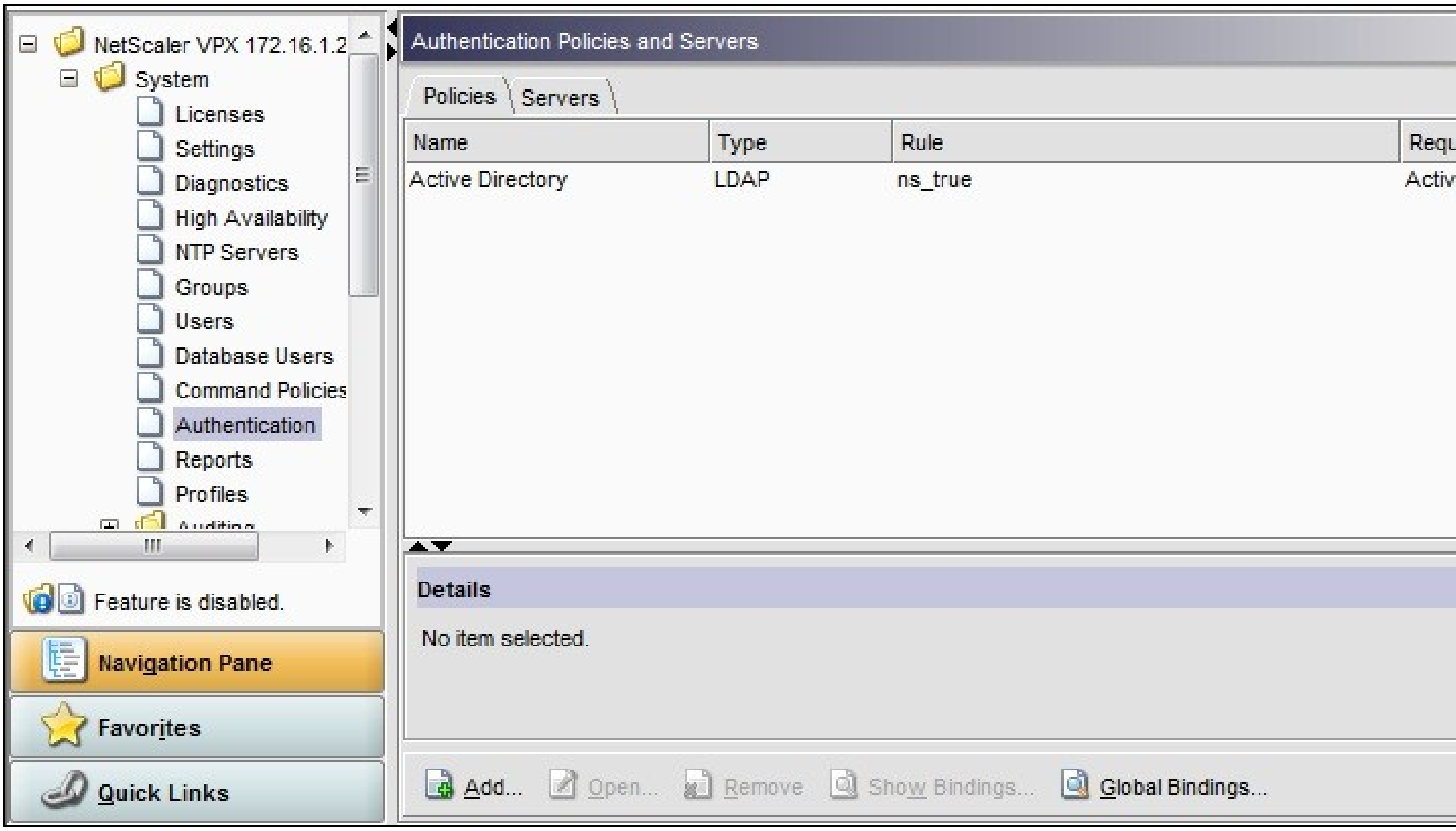
Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

Server Swivel RADIUS

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

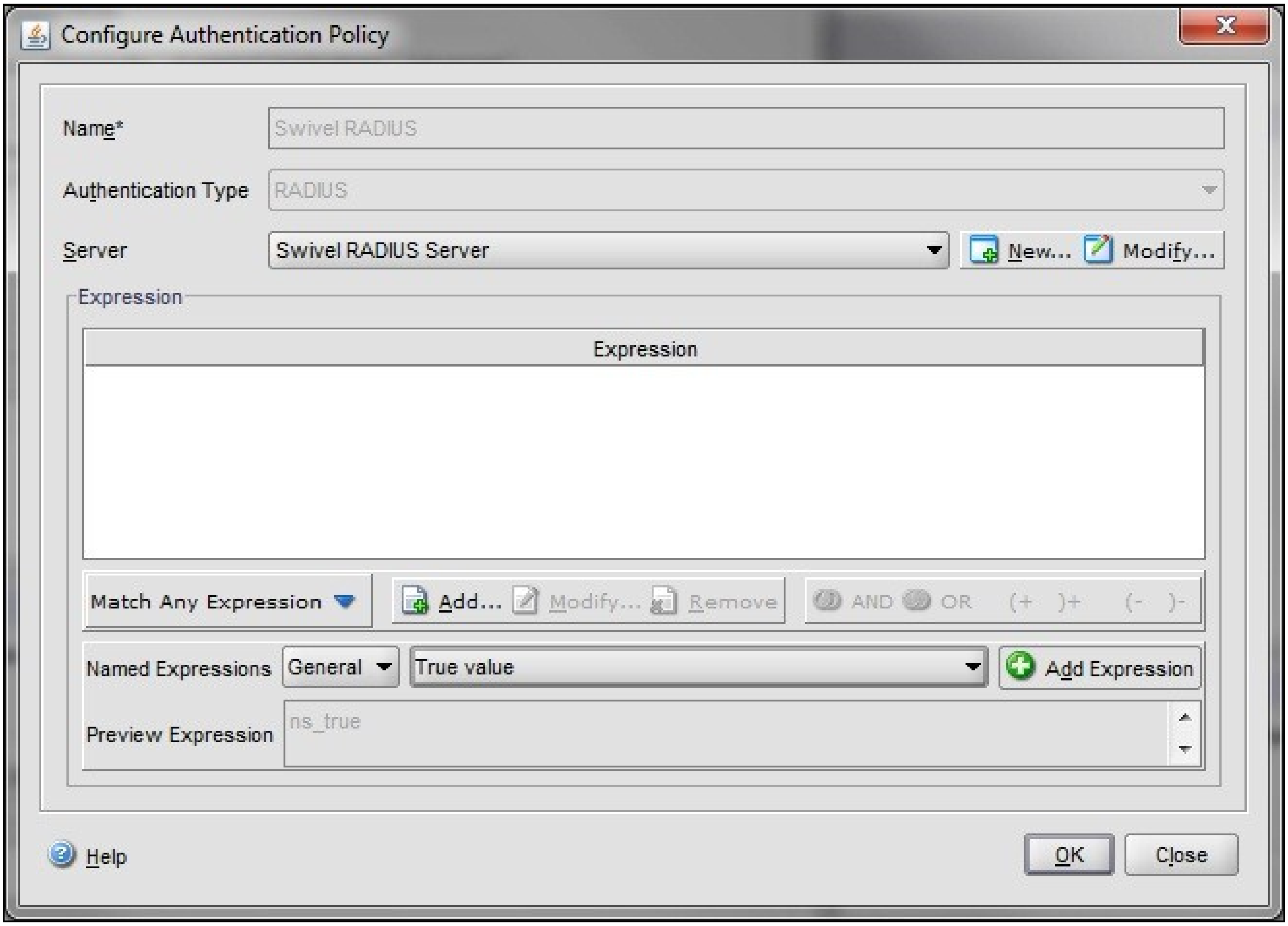


Authentication Policies and Servers

Name	Type	Rule	Requ
Active Directory	LDAP	ns_true	Activ

Details

No item selected.



Configure Authentication Policy

Name* Swivel RADIUS

Authentication Type RADIUS

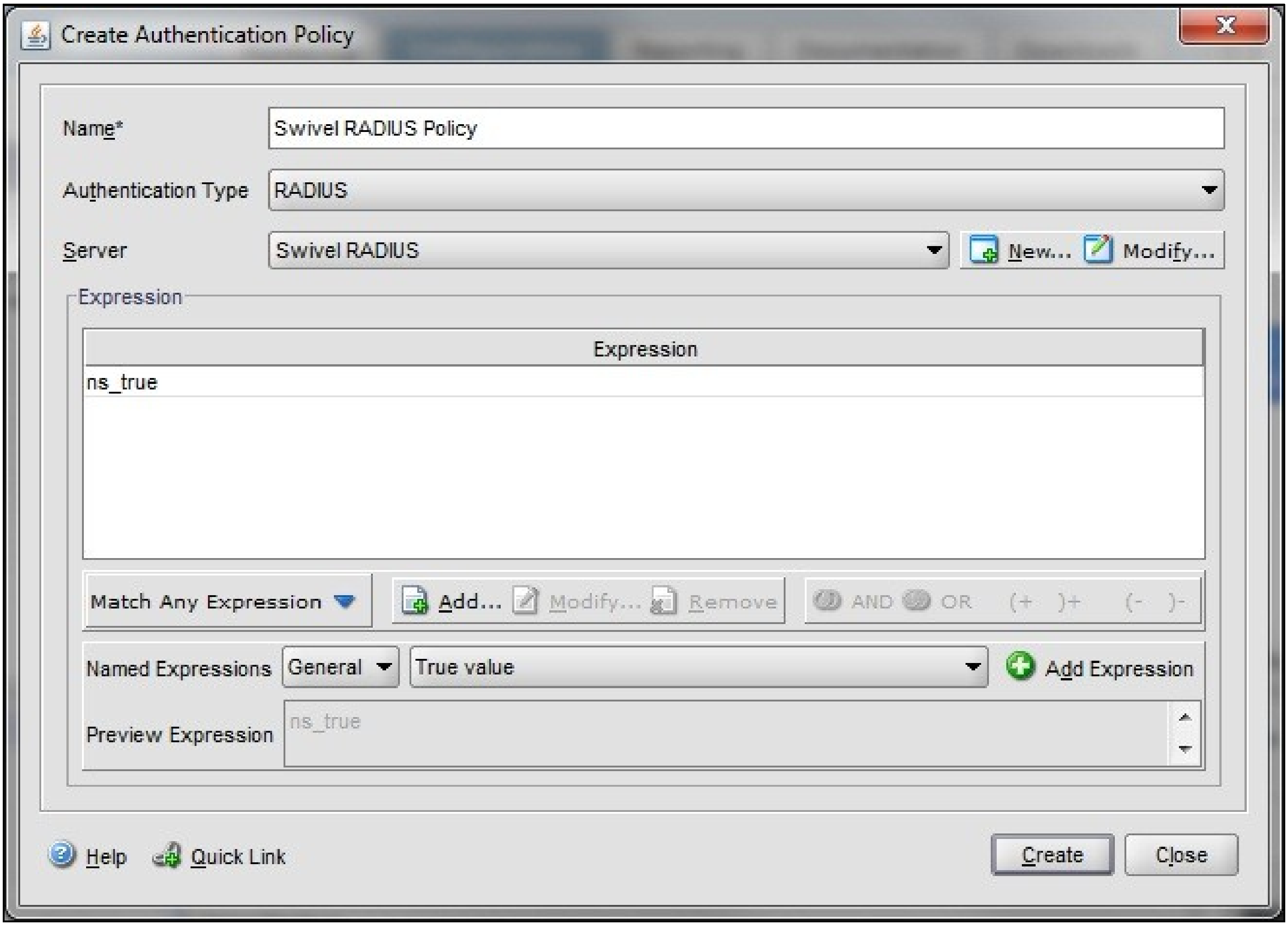
Server Swivel RADIUS Server

Expression

Match Any Expression

Named Expressions General True value

Preview Expression ns_true



Create Authentication Policy

Name* Swivel RADIUS Policy

Authentication Type RADIUS

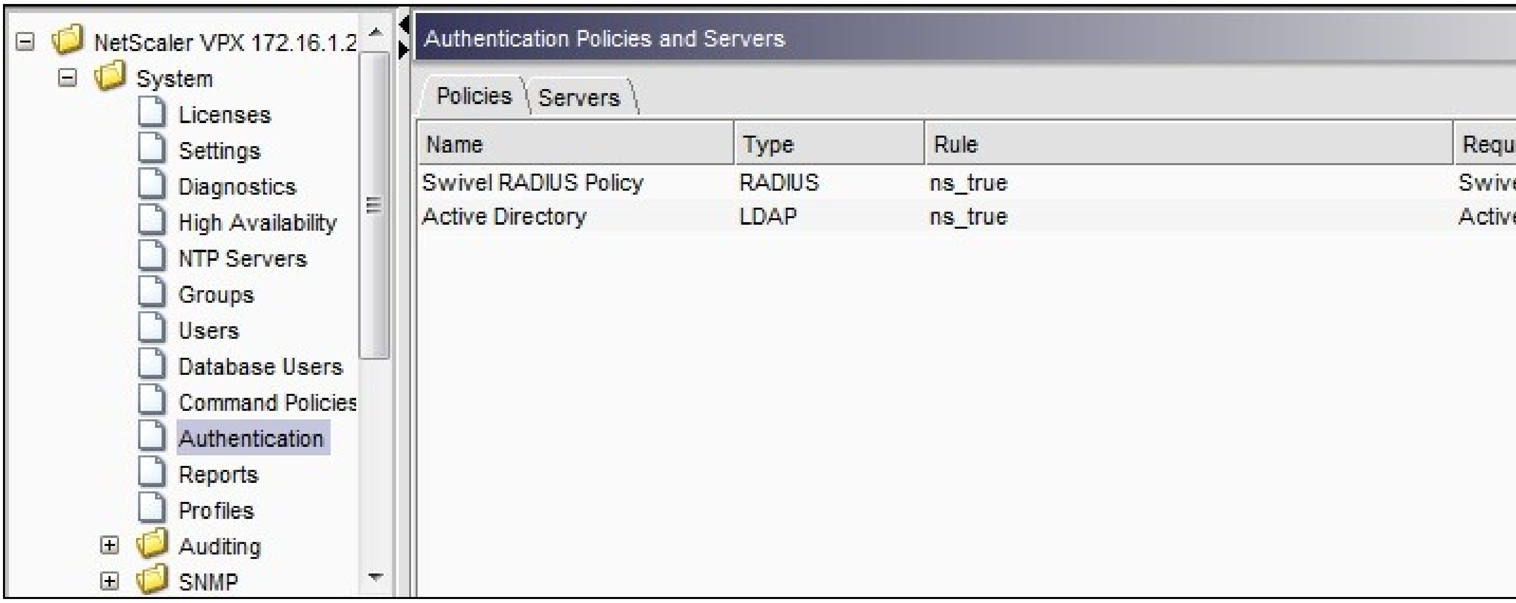
Server Swivel RADIUS

Expression

Expression
ns_true

Named Expressions General True value

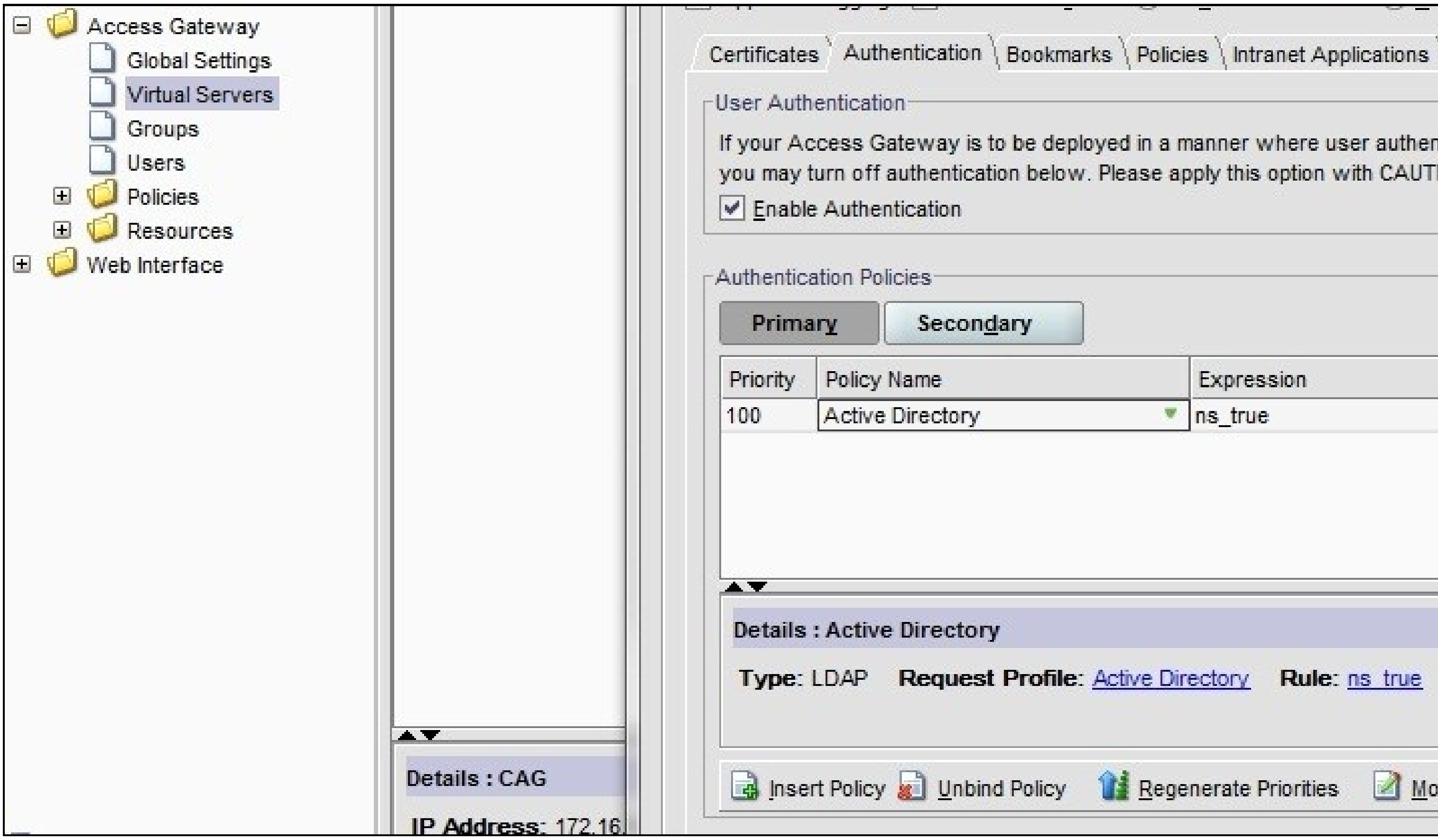
Preview Expression ns_true



Authentication Policies and Servers

Name	Type	Rule	Requ
Swivel RADIUS Policy	RADIUS	ns_true	Swive
Active Directory	LDAP	ns_true	Active

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



User Authentication

If your Access Gateway is to be deployed in a manner where user authen
you may turn off authentication below. Please apply this option with CAUT

☑ Enable Authentication

Authentication Policies

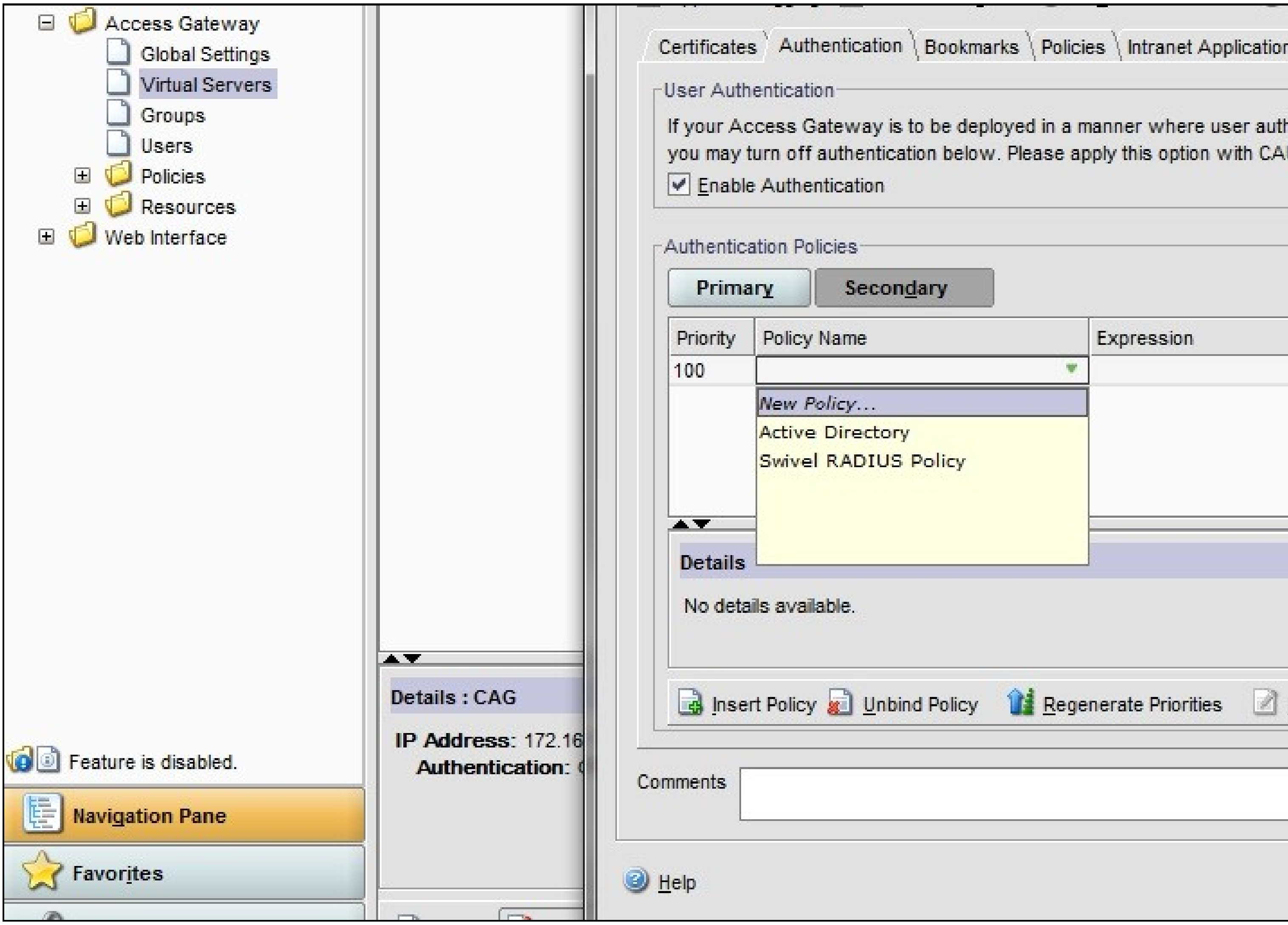
Priority	Policy Name	Expression
100	Active Directory	ns_true

Details : Active Directory

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

Details : CAG

IP Address: 172.16



Feature is disabled.

IP Address: 172.16

Authentication: (

If your Access Gateway is to be deployed in a manner where user auth
you may turn off authentication below. Please apply this option with CA

☑ Enable Authentication

Priority	Policy Name	Expression
100		

No details available.

72.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

73 Additional Configuration Options

73.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

73.2 Netscaler SSL Bridge

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

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

Name Name of the SSL Bridge

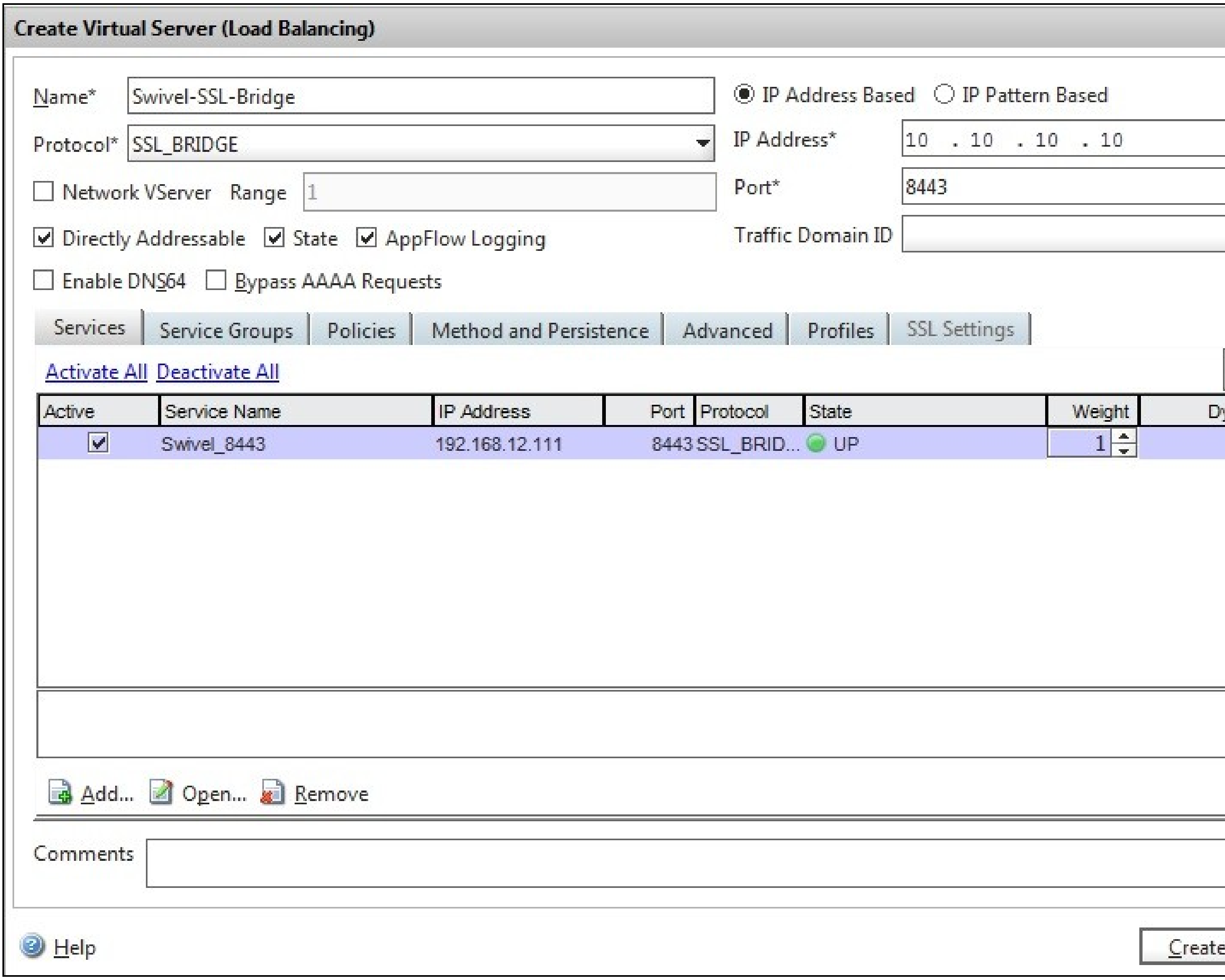
Select IP Adress Based

Protocol select SSL_Bridge

IP address Enter the public IP Address

Port Enter the Swivel instance port number, usually 8443

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



Create Virtual Server (Load Balancing)

Name* Swivel-SSL-Bridge

● IP Address Based ○ IP Pattern Based

Protocol* SSL_BRIDGE

IP Address* 10 . 10 . 10 . 10

□ Network VServer Range 1

Port* 8443

☑ Directly Addressable ☑ State ☑ AppFlow Logging

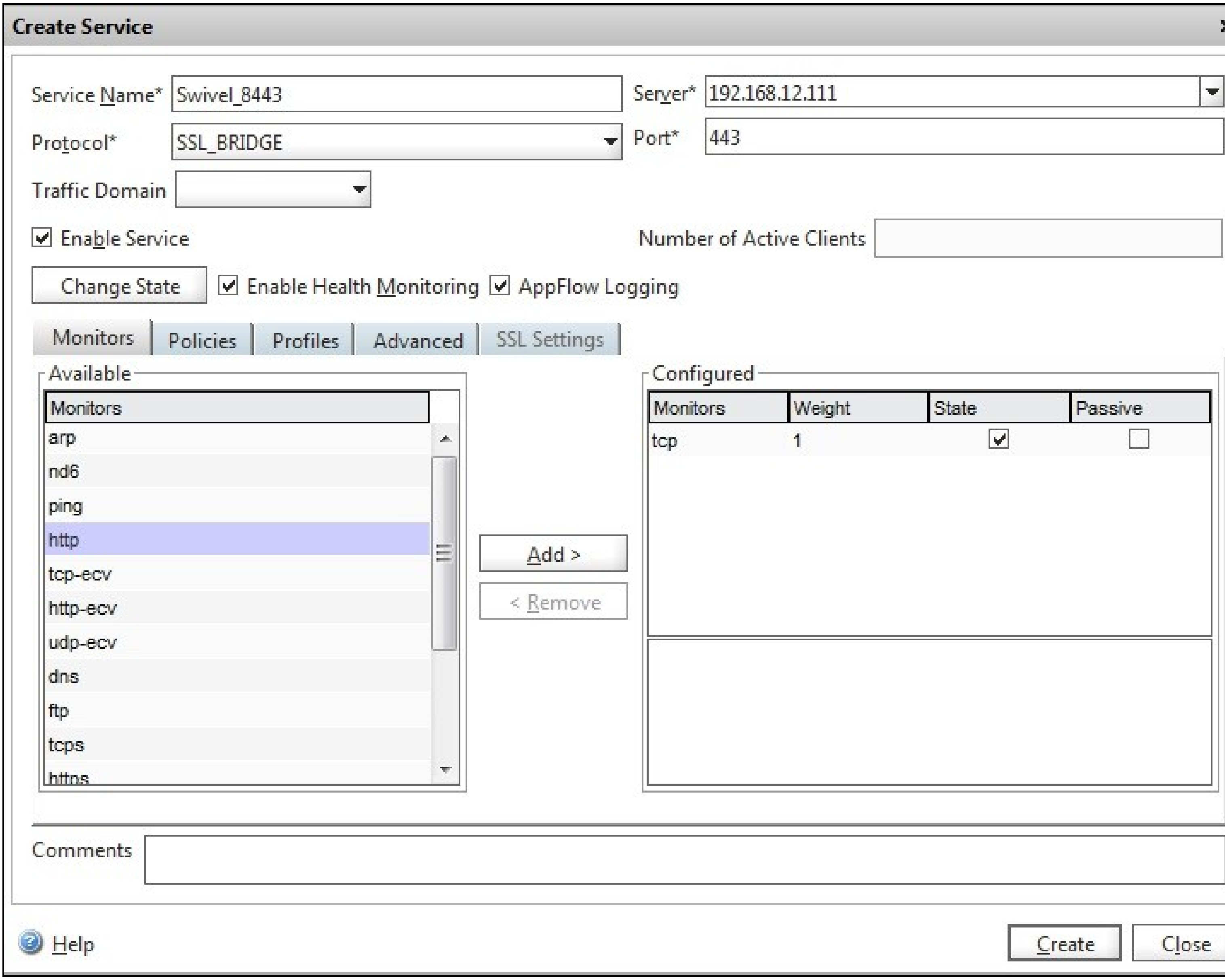
Traffic Domain ID

□ Enable DNS64 □ Bypass AAAA Requests

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dy
☑	Swivel_8443	192.168.12.111	8443	SSL_BRID...	● UP	1	

Comments

Click Add and enter the required details.



Create Service

Service Name* Swivel_8443

Server* 192.168.12.111

Protocol* SSL_BRIDGE

Port* 443

Traffic Domain

☑ Enable Service

Number of Active Clients

☑ Enable Health Monitoring ☑ AppFlow Logging

Configured

Monitors	Weight	State	Passive
tcp	1	☑	□

Comments

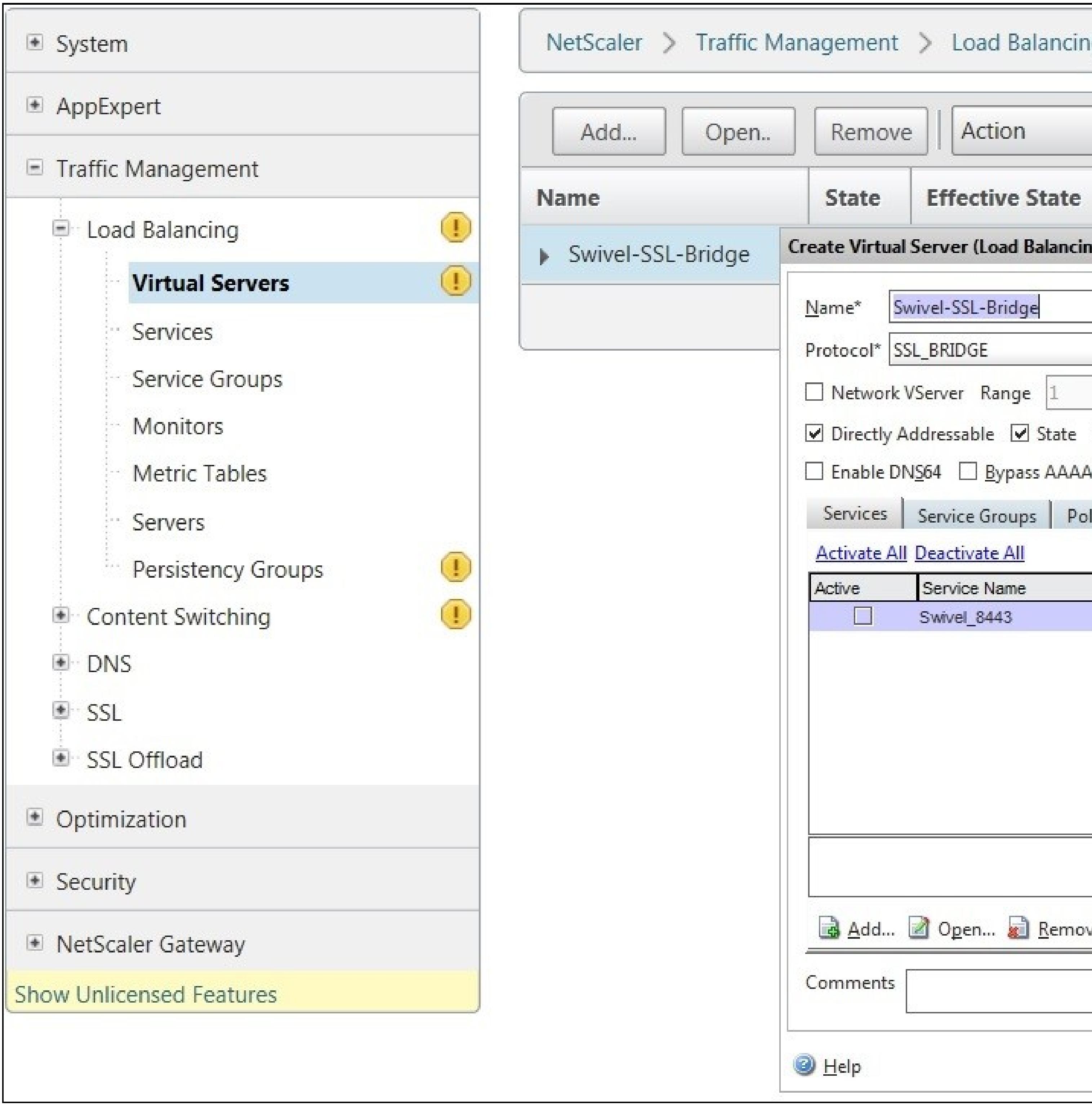
Service Name Name of the SSL Bridge

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.



Swivel-SSL-Bridge

Name* Swivel-SSL-Bridge

Protocol* SSL_BRIDGE

□ Network VServer Range 1

☑ Directly Addressable ☑ State

□ Enable DNS64 □ Bypass AAAA

Active	Service Name
□	Swivel_8443

Comments

73.3 Login Page Customisation

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

73.4 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.

73.5 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.

73.5.1 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
```

73.5.2 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
```

73.5.3 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.

73.5.3.1 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

73.5.4 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).

73.5.4.1 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
```

73.5.5 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

73.5.6 Create the boot archive file

```
mkdir /var/ns_gui_custom

cd /netscaler

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

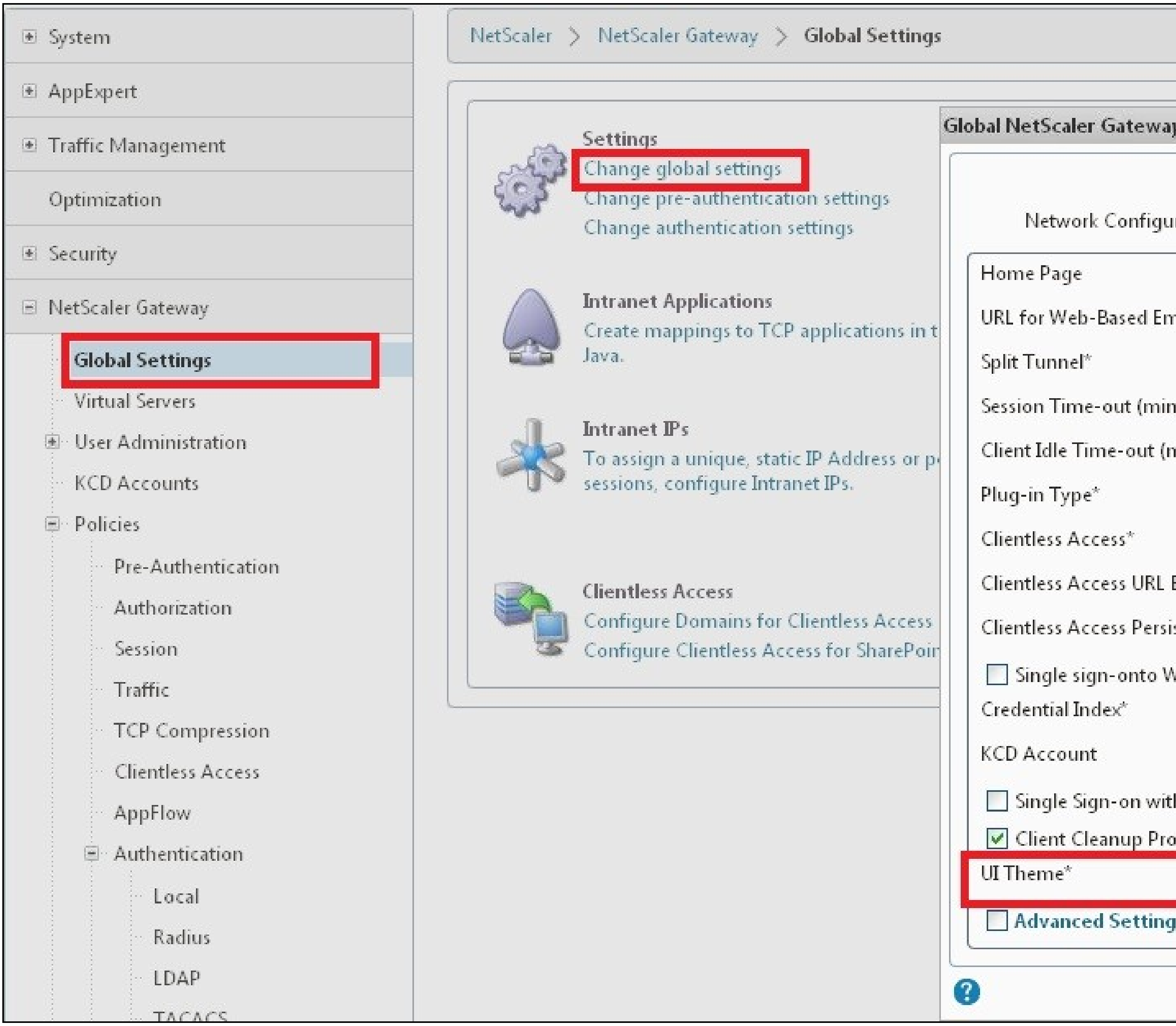
This should create the customtheme.tar.gz file used at boot time, and list all the files used.

73.5.7 Tell the Netscaler to use the customised login pages

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

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

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



73.5.8 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.

73.6 Additional Login Customisation options

73.6.1 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%;"
```

73.6.2 Changing the button labels

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

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

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

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

73.6.3 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

73.6.4 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

73.6.5 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

73.7 Challenge and Response

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

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

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

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

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

Must be changed to:

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

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

Example fucnction code:

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

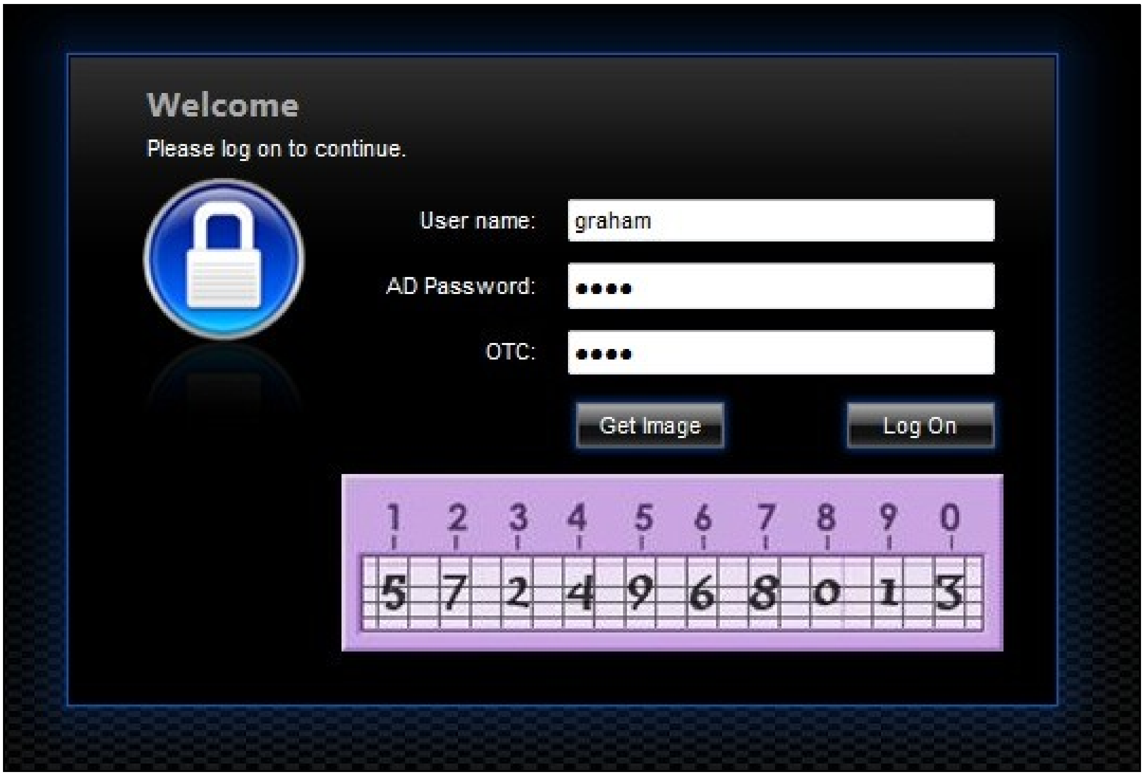
73.8 Image Request button displayed when needed

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

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

74 Testing

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



Welcome

Please log on to continue.

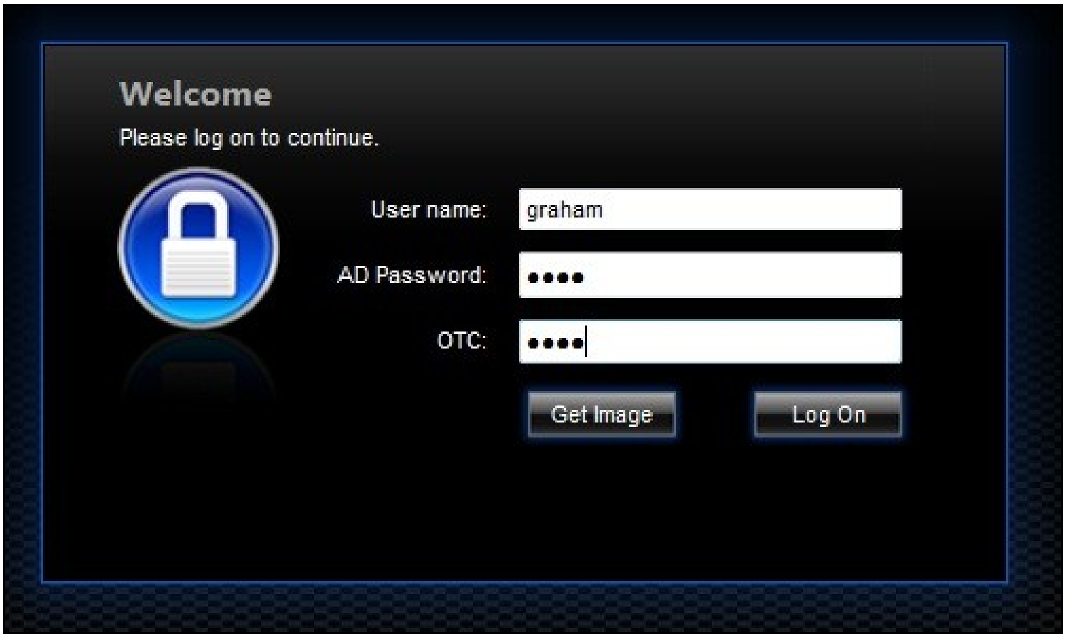
User name: graham

AD Password: ●●●●

OTC: ●●●●

1	2	3	4	5	6	7	8	9	0
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



Welcome

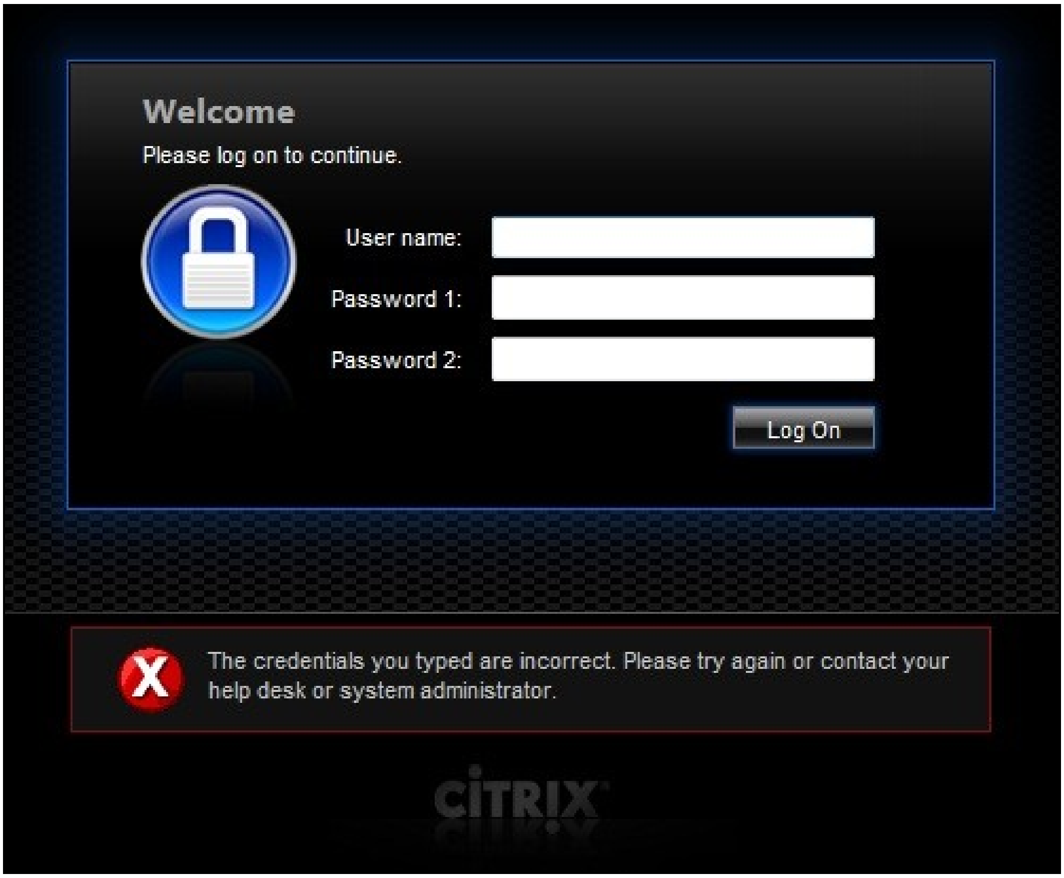
Please log on to continue.

User name: graham

AD Password: ●●●●

OTC: ●●●●

If the incorrect credentials are used then the login should fail



Welcome

Please log on to continue.

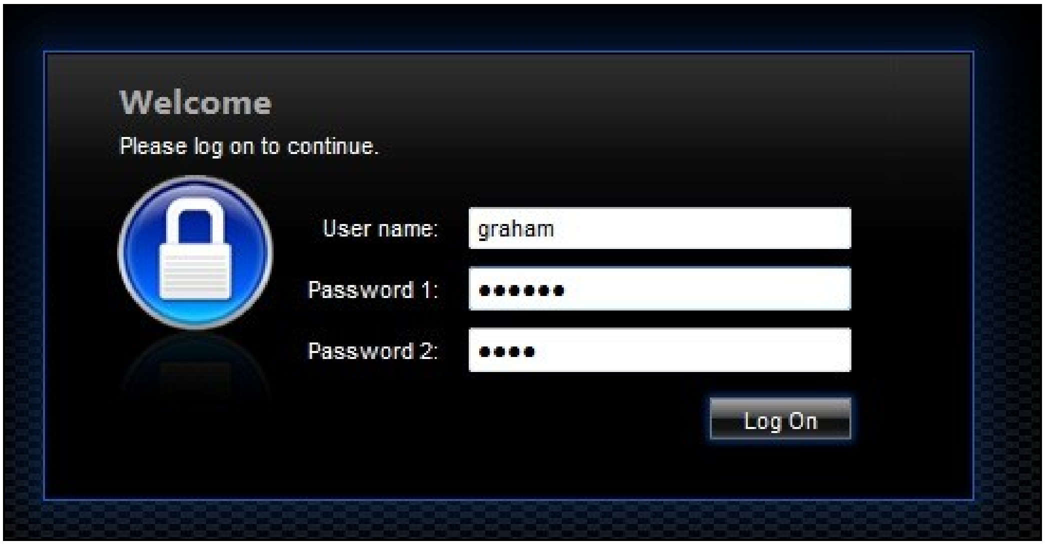
User name:

Password 1:

Password 2:

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

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



Welcome

Please log on to continue.

User name: graham

Password 1: ●●●●●●

Password 2: ●●●●

75 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.

76 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.

76.1 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 preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

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

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

After making the changes, reboot the system to login.

77 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]

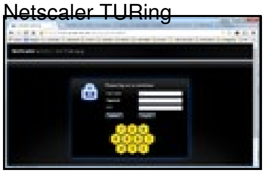
78 Additional Information

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

79 Citrix Netscaler Gateway 11

80 Introduction

-

  Netscaler TURing
- 

  Netscaler PINpad

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

It covers the following steps.

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

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

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

81 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.

81.1 Note on upgrading the Netscaler

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

82 Baseline

Tested with Swivel 3.10.4

Citrix Netscaler Gateway NS11.0 Build 62.0

83 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.

84 Swivel Configuration

84.1 Configuring the RADIUS server

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

84.2 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.

84.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

85 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.

85.1 Citrix NetScaler RADIUS Configuration

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

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

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

Name Swivel RADIUS

Server Name The name or IP address of the Swivel server

Port 1812

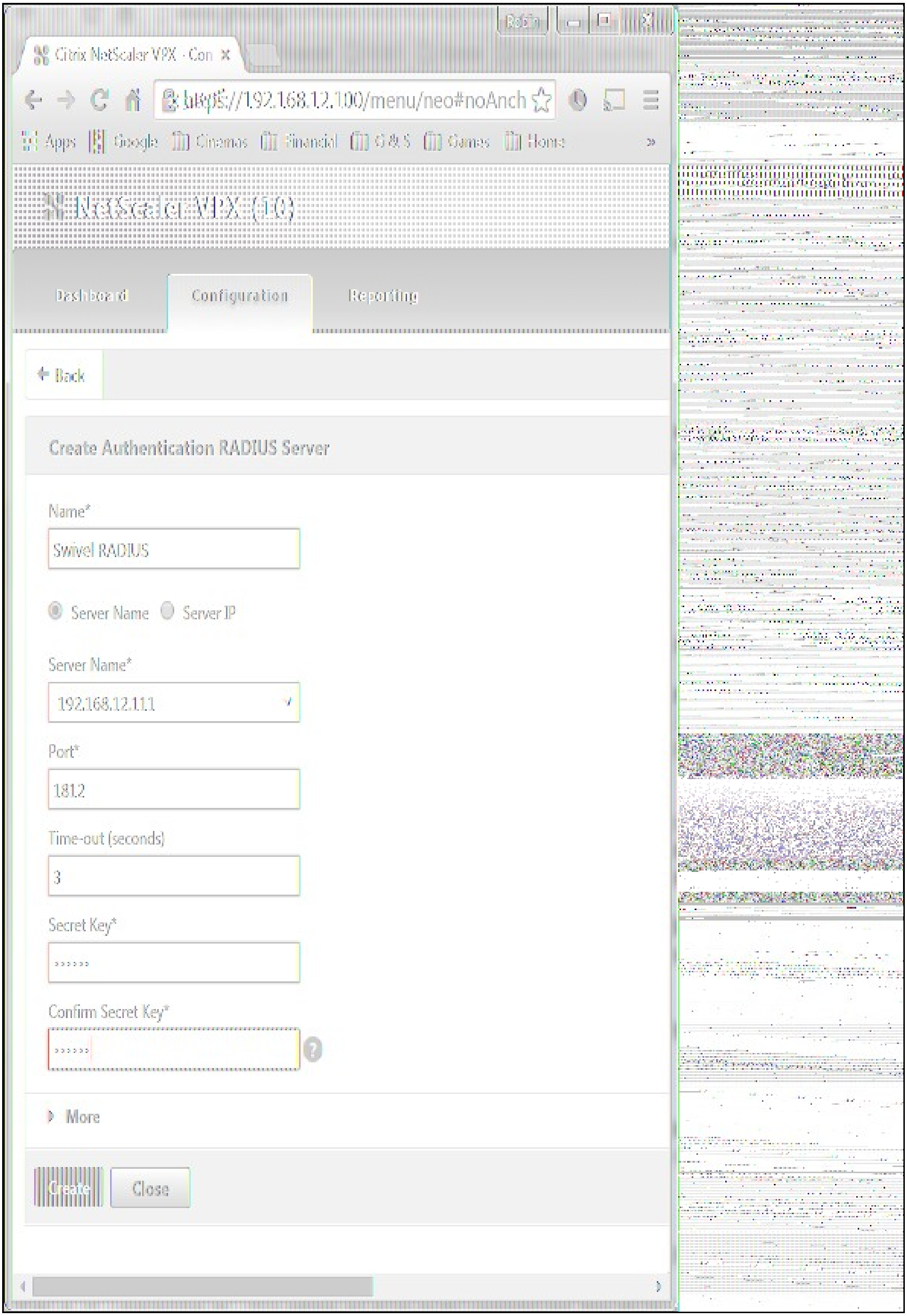
Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix CTXSUserGroups=

Group Separator ;

When complete click on Create.

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



Create Authentication RADIUS Server

Name*: Swivel RADIUS

● Server Name ○ Server IP

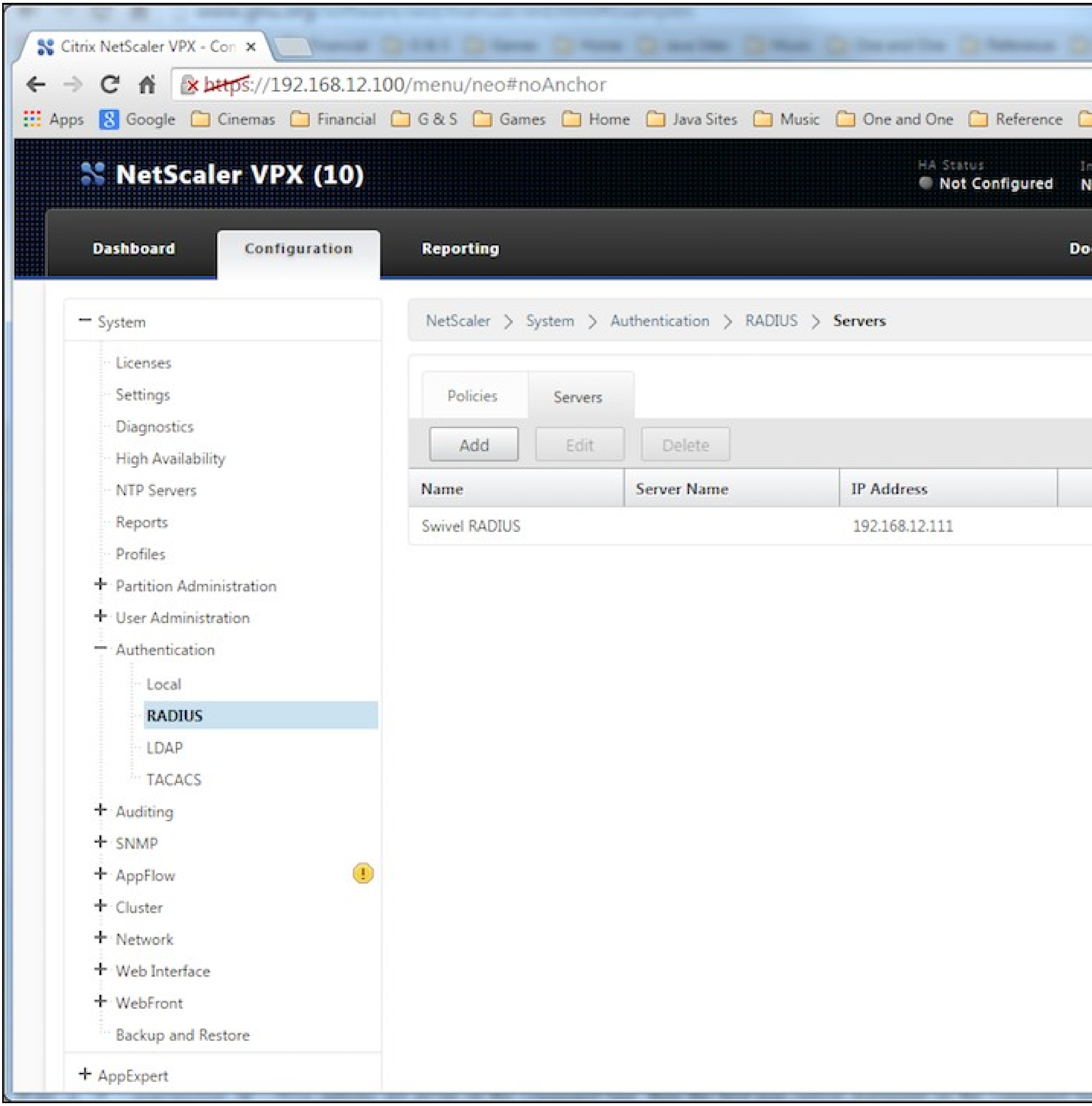
Server Name*: 192.168.12.111

Port*: 1812

Time-out (seconds): 3

Secret Key*: ••••••

Confirm Secret Key*: ••••••



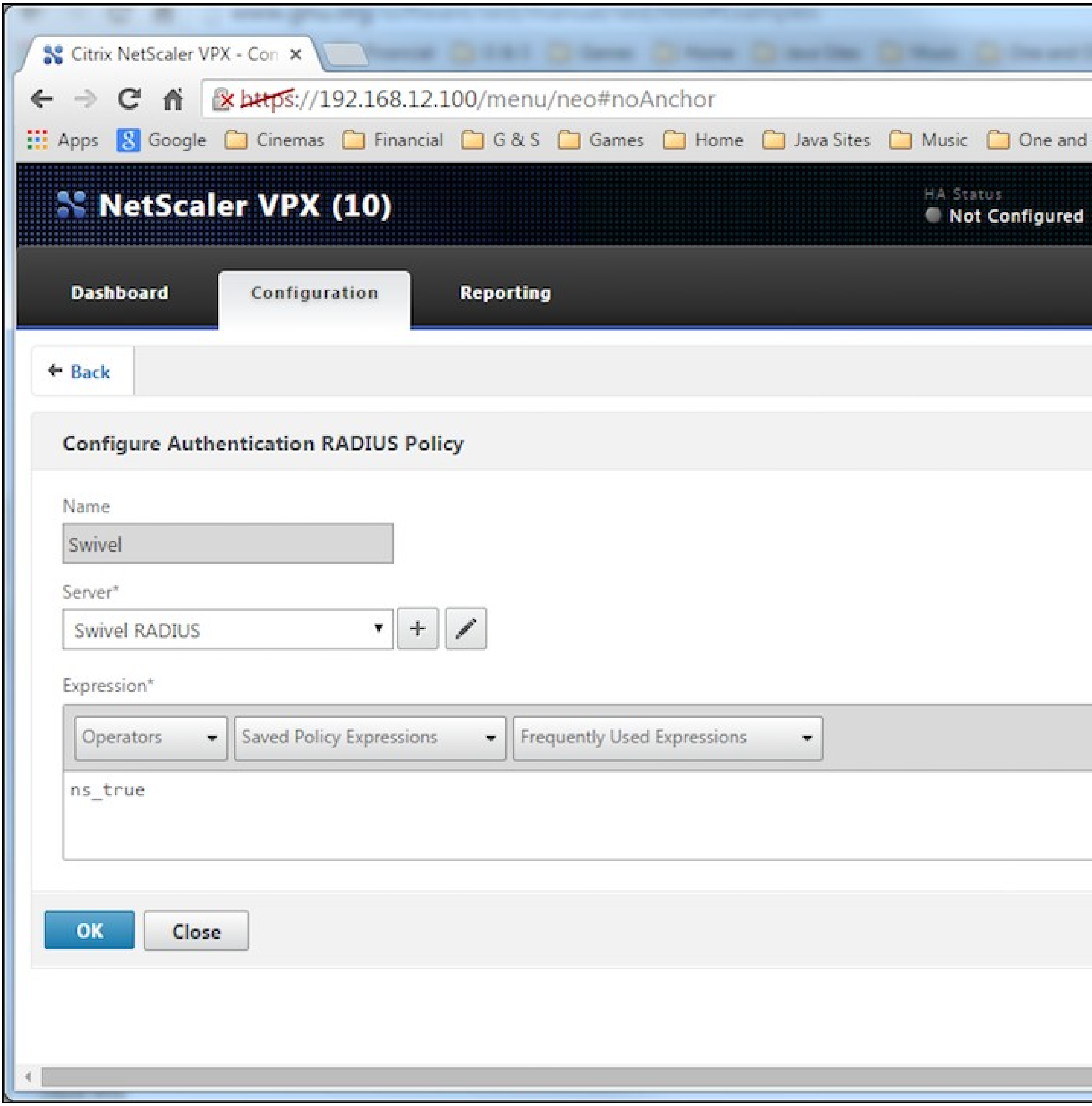
Name	Server Name	IP Address
Swivel RADIUS		192.168.12.111

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



Configure Authentication RADIUS Policy

Name

Swivel

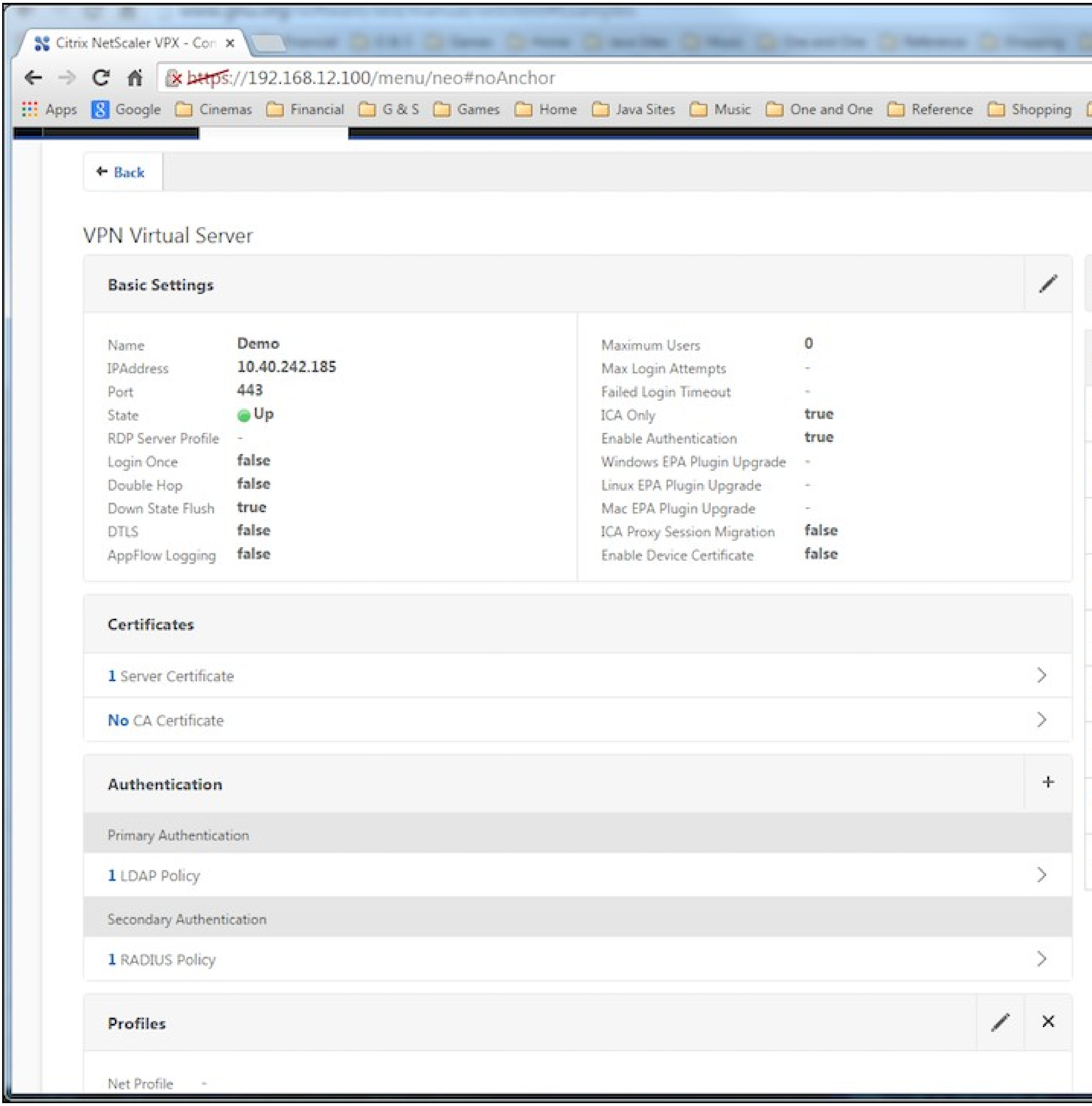
Server*

Swivel RADIUS

Expression*

```
ns_true
```

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.



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 -

85.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

86 Additional Configuration Options

86.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

86.2 Netscaler SSL Bridge

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

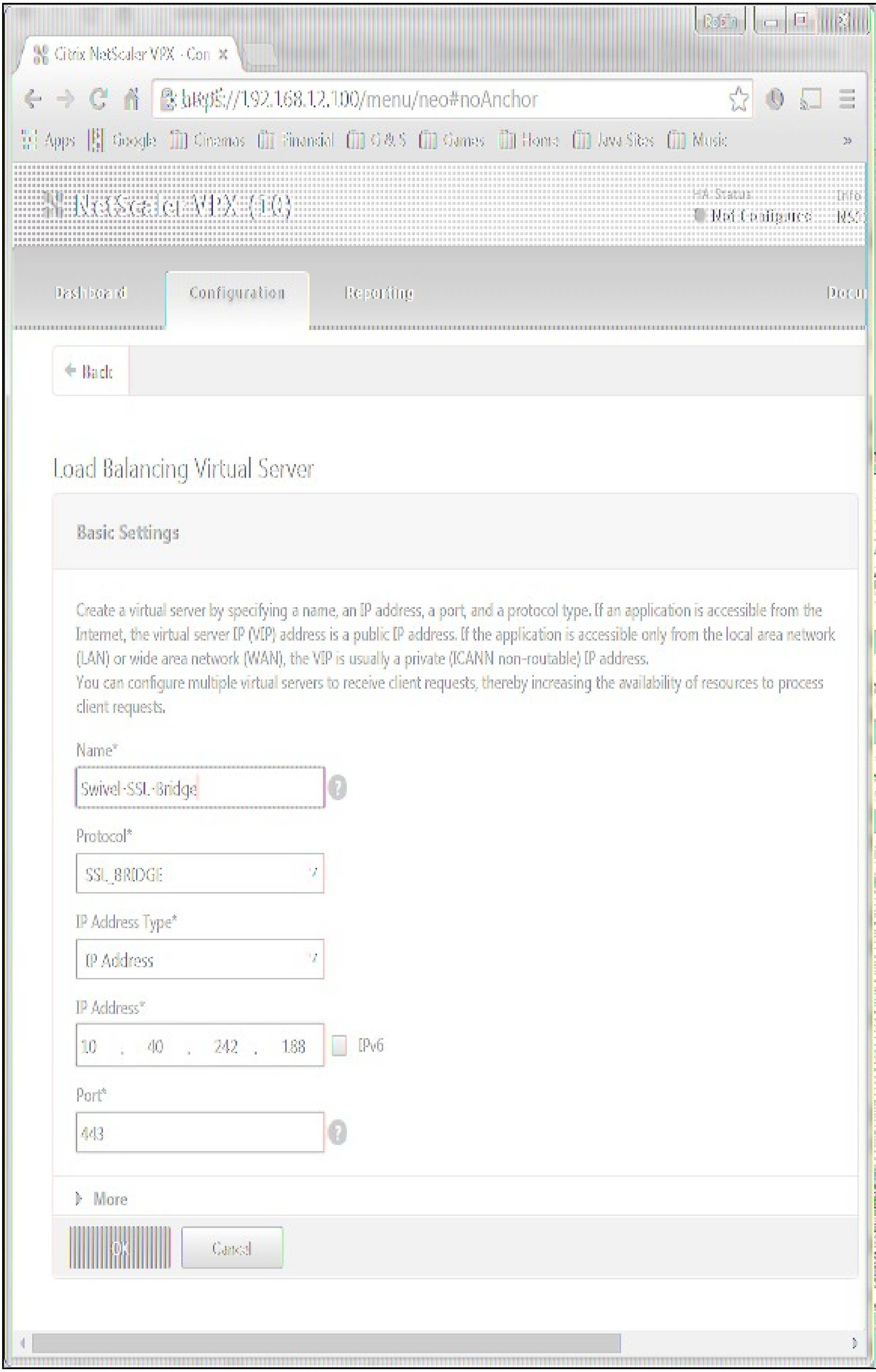
Name Name of the SSL Bridge

Protocol select SSL_Bridge

Select IP Adress Based

IP address Enter the public IP Address

Port Enter the internet-facing port number, usually 443



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

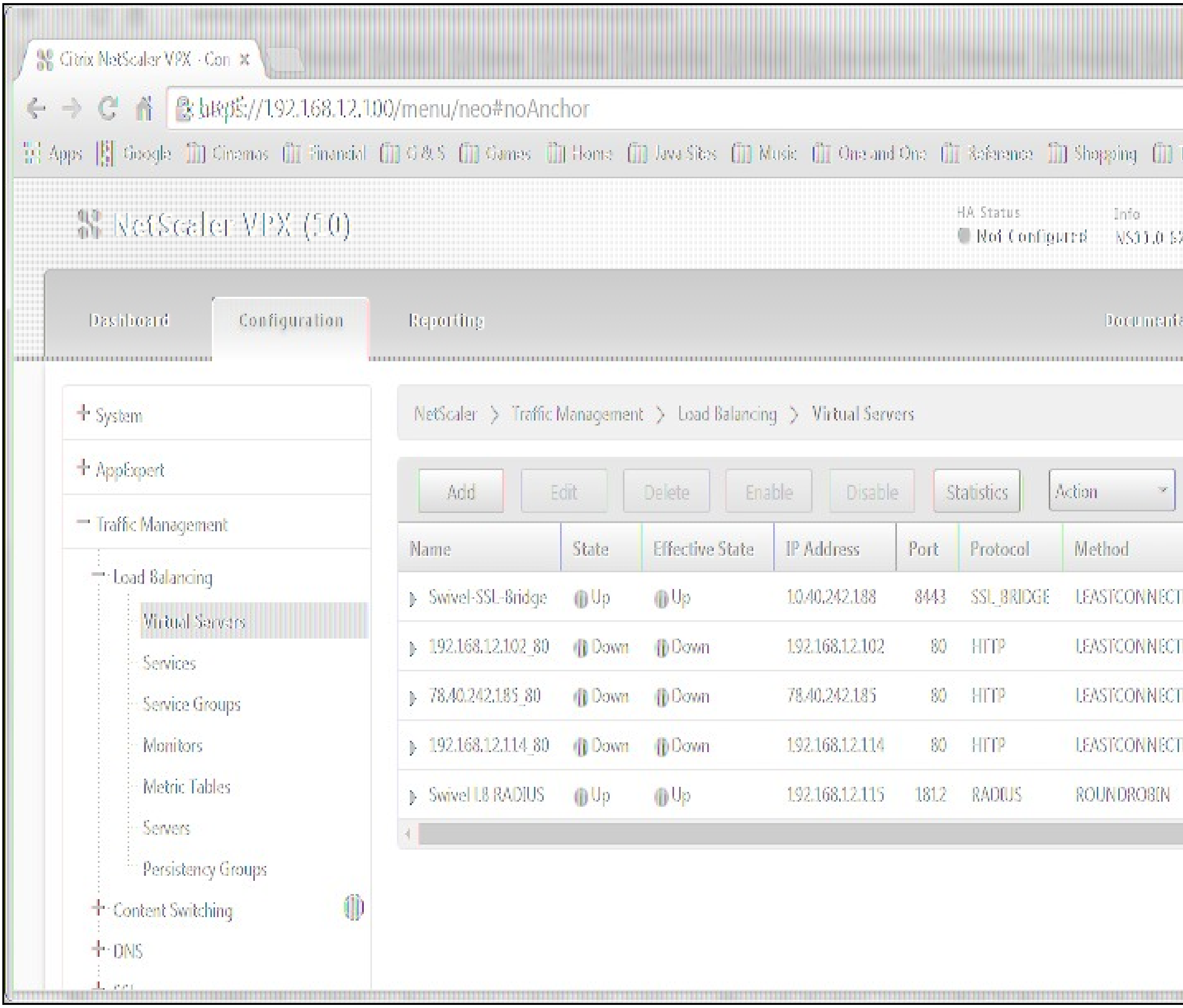
Name*: Swivel-SSL-Bridge

Protocol*: SSL_BRIDGE

IP Address Type*: IP Address

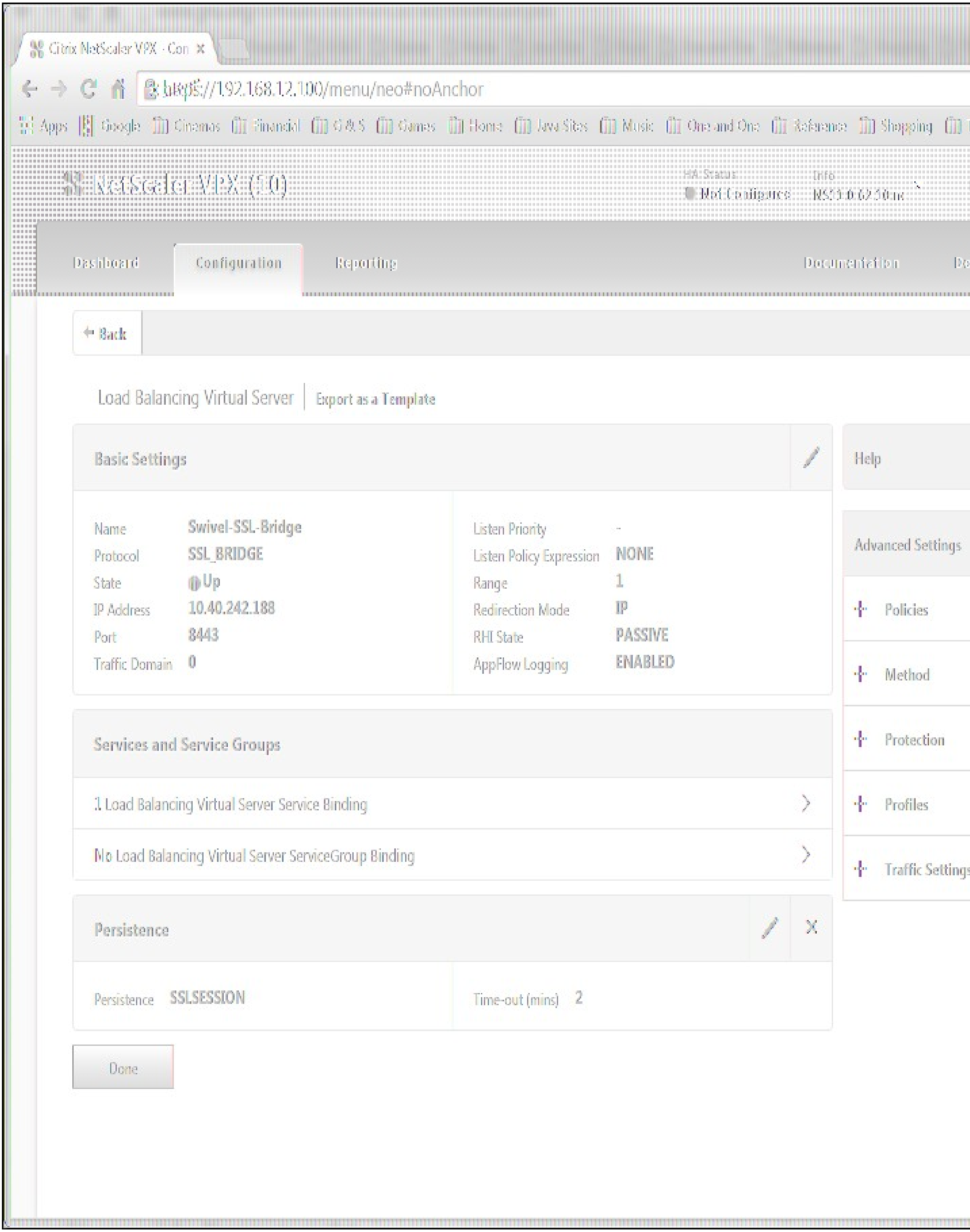
IP Address*: 10 . 40 . 242 . 188 □ IPv6

Port*: 443



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 L8 RADIUS	Up	Up	192.168.12.115	1812	RADIUS	ROUNDROBIN

After creating the virtual server, select it and then Edit



Load Balancing Virtual Server

Basic Settings

Name	Swivel-SSL-Bridge	Listen Priority	-
Protocol	SSL_BRIDGE	Listen Policy Expression	NONE
State	Up	Range	1
IP Address	10.40.242.188	Redirection Mode	IP
Port	8443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED

Services and Service Groups

1 Load Balancing Virtual Server Service Binding

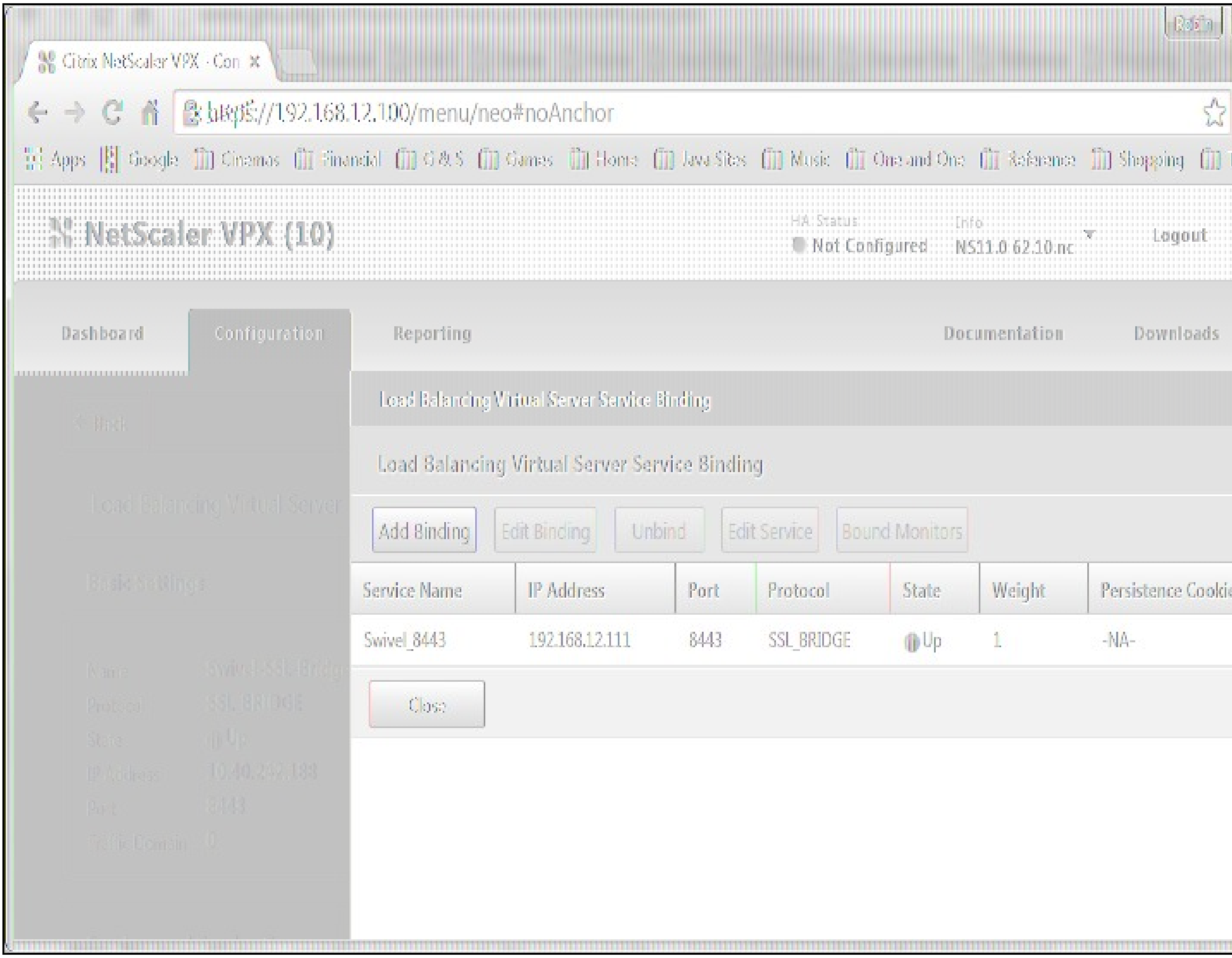
No Load Balancing Virtual Server ServiceGroup Binding

Persistence

Persistence SSLSESSION

Time-out (mins) 2

Select "Load Balancing Virtual Server Service Binding"



Load Balancing Virtual Server

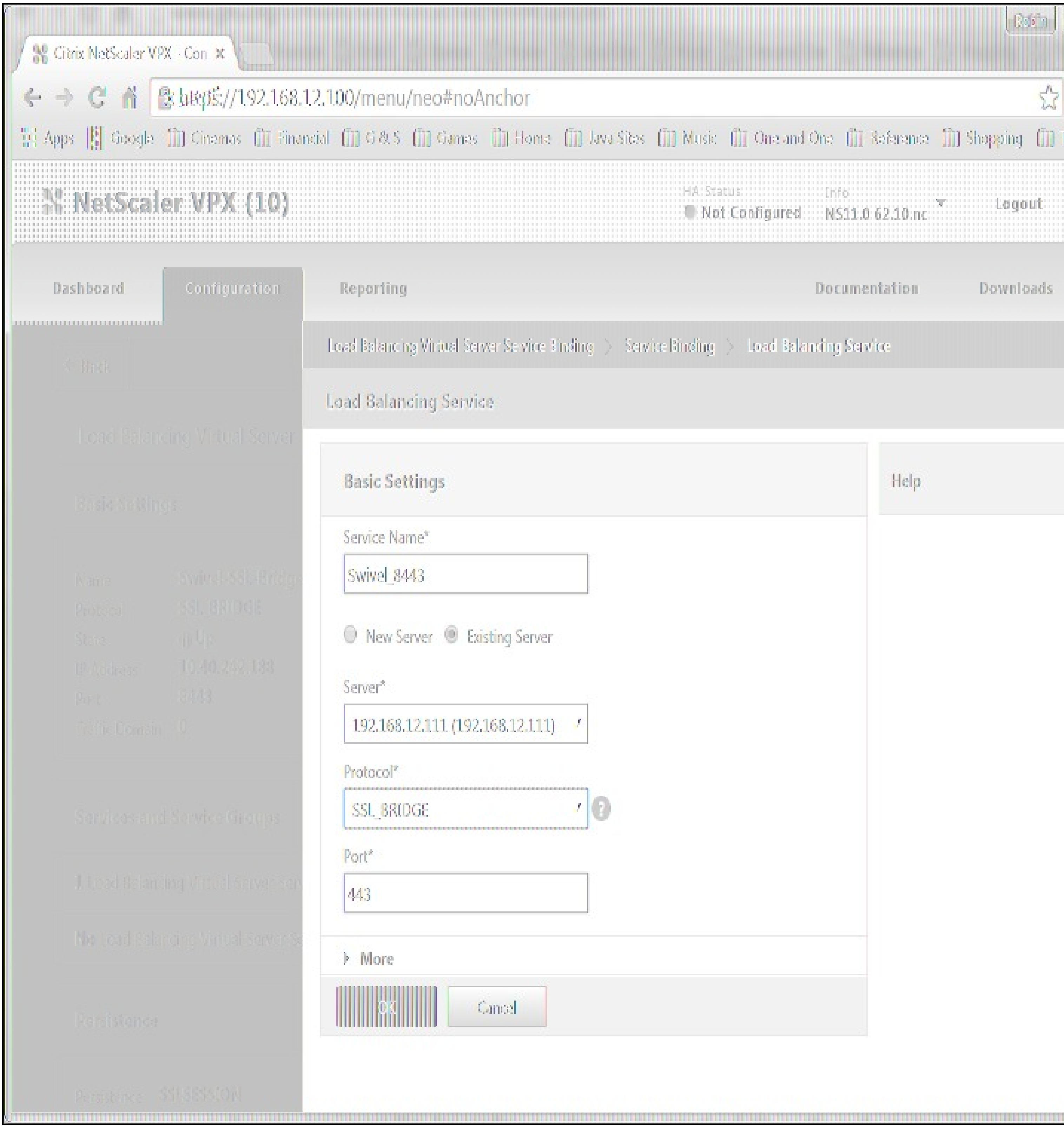
Basic Settings

Name Swivel-SSL-Bridge
Protocol SSL_BRIDGE
State Up
IP Address 10.40.242.188
Port 8443
Traffic Domain 0

Load Balancing Virtual Server Service Binding

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

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



Load Balancing Service

Basic Settings

Service Name* Swivel_8443

○ New Server ● Existing Server

Server* 192.168.12.111 (192.168.12.111)

Protocol* SSL_BRIDGE

Port* 443

Name Swivel SSL Bridge

Protocol SSL_BRIDGE

State Up

IP Address 10.40.242.188

Port 8443

Traffic Domain 0

1 Load Balancing Virtual Server Ser

No Load Balancing Virtual Server S

Persistence SSLSESSION

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.

86.3 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.

86.3.1 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.

86.3.2 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.

86.3.3 Customising an Existing Theme

86.3.3.1 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.

86.3.3.2 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
```

86.3.3.3 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
```

86.3.3.4 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".

86.3.3.5 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.

86.3.3.6 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.

86.3.3.7 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.

86.3.3.8 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.

86.3.3.9 Select the custom theme

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

86.3.3.10 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.

86.3.3.11 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.

86.3.4 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.

86.4 Additional Login Customisation options

86.4.1 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".

86.4.2 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".

86.4.3 One Touch

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

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

Refer to VPN_OneTouch_Integration

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

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

var QueryString = function () {
 // This function is anonymous, is executed immediately and
 // the return value is assigned to QueryString!
 var query_string = {};
 var query = window.location.search.substring(1);
 var vars = query.split("&");
 for (var i=0;i<vars.length;i++) {
   var pair = vars[i].split("=");
        // If first entry with this name
   if (typeof query_string[pair[0]] === "undefined") {
     query_string[pair[0]] = pair[1];
      //  alert(pair[0] + "," + pair[1]);
```

```
        // If second entry with this name
   } else if (typeof query_string[pair[0]] === "string") {
     var arr = [ query_string[pair[0]], pair[1] ];
     query_string[pair[0]] = arr;
       //alert(pair[0] + "," + arr);
        // If third or later entry with this name
   } else {
     query_string[pair[0]].push(pair[1]);
   }
 }
   return query_string;
} ();

$(document).ready(function(){
 usernamePassedIn = QueryString["username"];
 passwordPassedIn = QueryString["password"];

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

 }
});
```

Before the closing </SCRIPT> tag

86.5 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.

86.5.1 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.

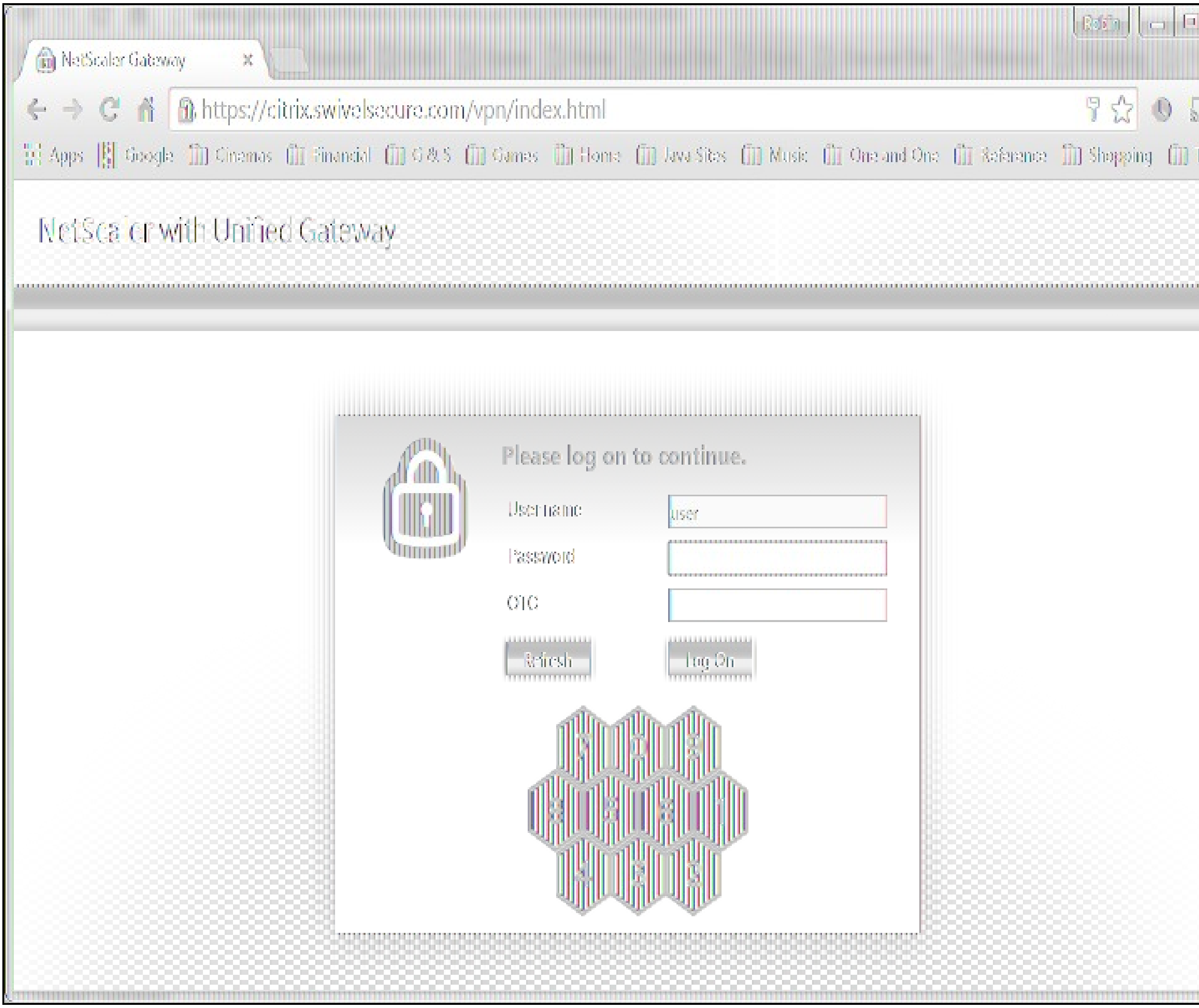
86.6 Image Request button displayed when needed

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

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

87 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.



NetScaler Gateway
https://citrix.swivelsecure.com/vpn/index.html
Apps Google Cinemas Financial O & S Games Home Java Sites Music One and One Reference Shopping
NetScaler with Unified Gateway
Please log on to continue.
Refresh
Log On

Username: user

Password:

OTC:

88 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.

89 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.

89.1 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 preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

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

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

After making the changes, reboot the system to login.

90 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

91 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

92 Citrix Netscaler Gateway 12

93 Introduction

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

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

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

93.1 Integration Architecture

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

94 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.

94.1 Rewrite Rules

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

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

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

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

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

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

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

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

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

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

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

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

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

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

94.1.1 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.

94.2 Green Bubble Theme

Use the following rules for the Green Bubble theme.

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

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

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

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

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

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

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

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

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

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

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

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

94.3 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

94.4 X1

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

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

add rewrite action Act_Sentry_ModX1 insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=$(\"<div></div>\").addClass('field')

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

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

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

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

add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModX1

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

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

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

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

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

95 Pinpad Integration

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

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

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

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

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

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

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

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

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

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

96 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.

97 Adjust Buttons at the login page

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

97.1 Edit Password to OTC

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

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

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

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

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

98 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

99 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 ...
```

100 nFactor ? Customizing UI to Display Images

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

101 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

102 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

103 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.

104 Prerequisites

Swivel HA solution

Netscaler 10.x

105 Baseline

Swivel 3.10.3

Netscaler 10.5

106 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.

107 Netscaler Configuration

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

107.1 Create a Swivel Radius Monitor

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

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

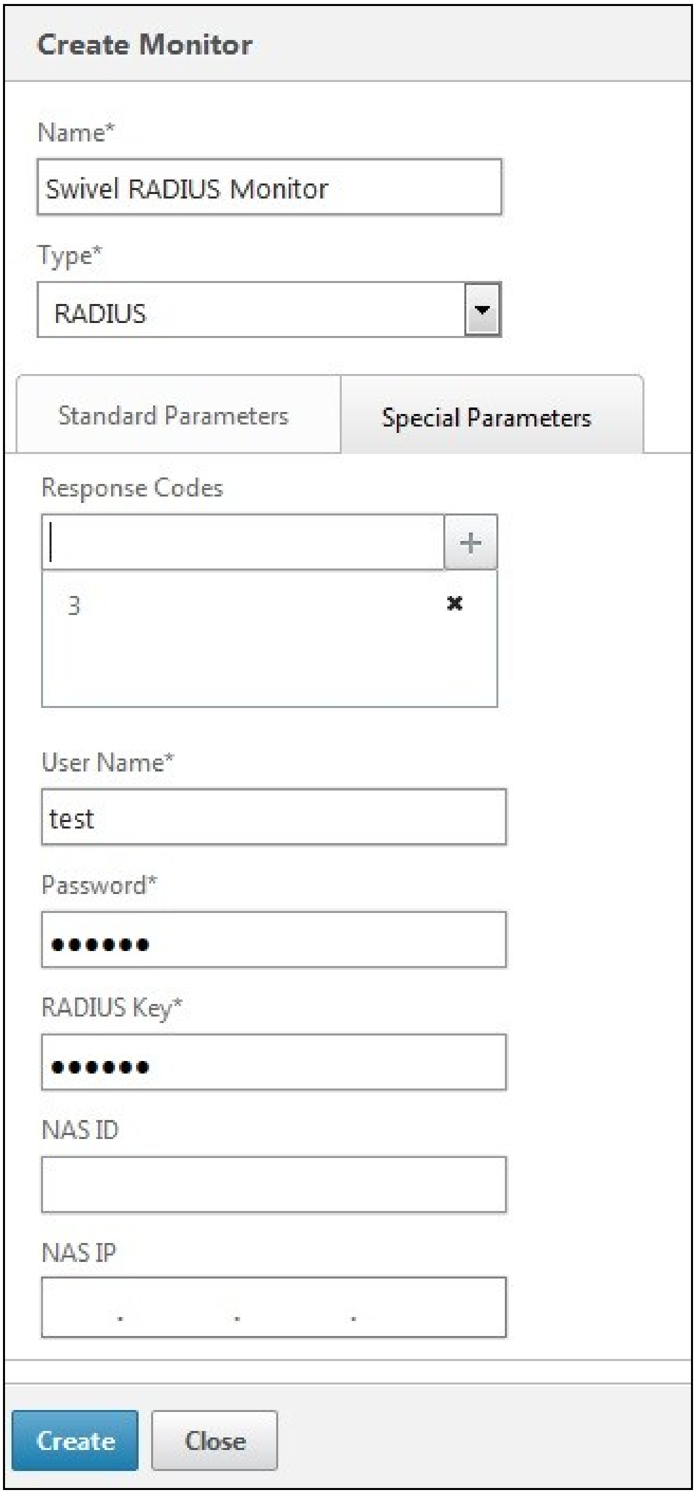
Set **Username** to an appropriate test user

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

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

Leave other settings as default

Click Create to create the Monitor



Create Monitor

Name*: Swivel RADIUS Monitor

Type*: RADIUS

Response Codes: 3

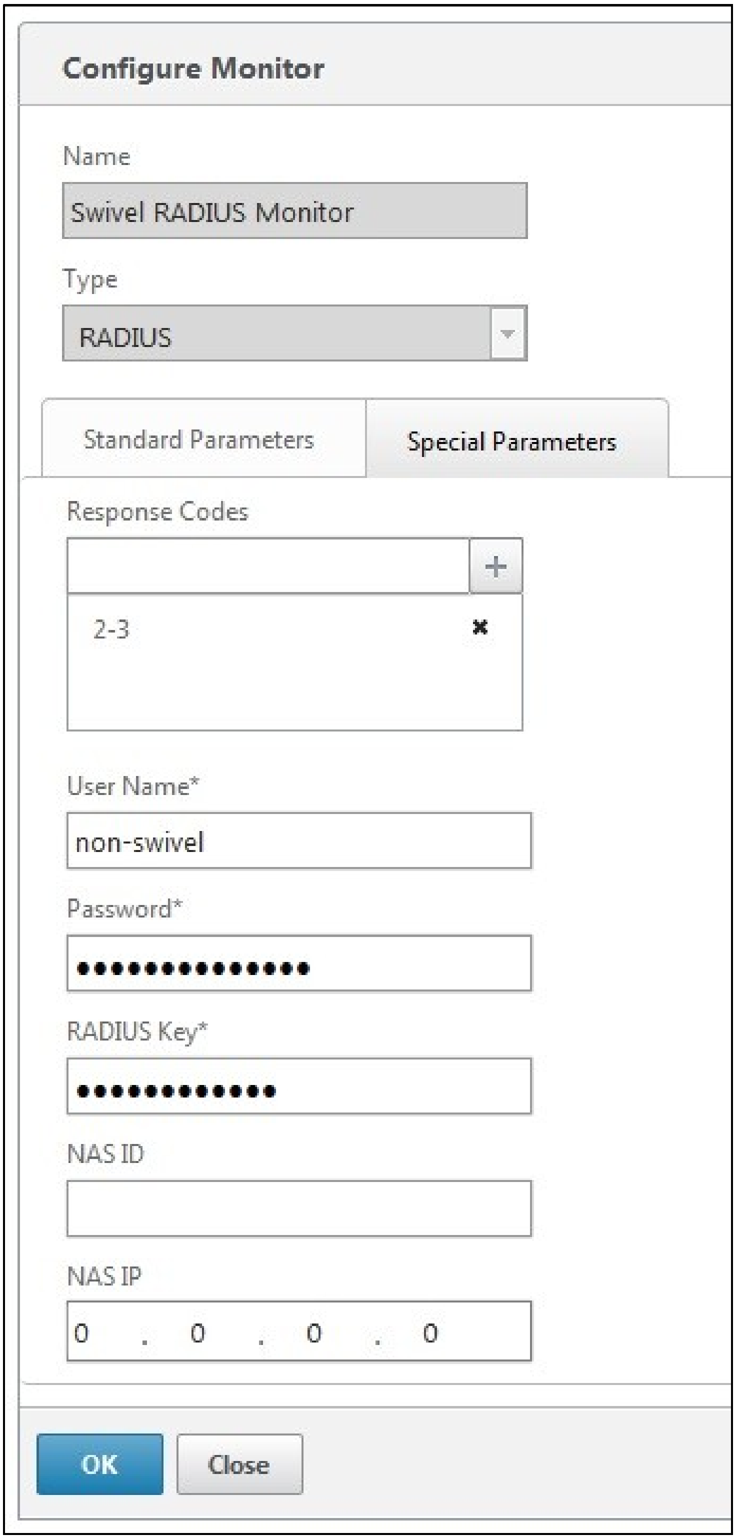
User Name*: test

Password*: ●●●●●●

RADIUS Key*: ●●●●●●

NAS ID:

NAS IP: . . .



Configure Monitor

Name: Swivel RADIUS Monitor

Type: RADIUS

Response Codes: 2-3

User Name*: non-swivel

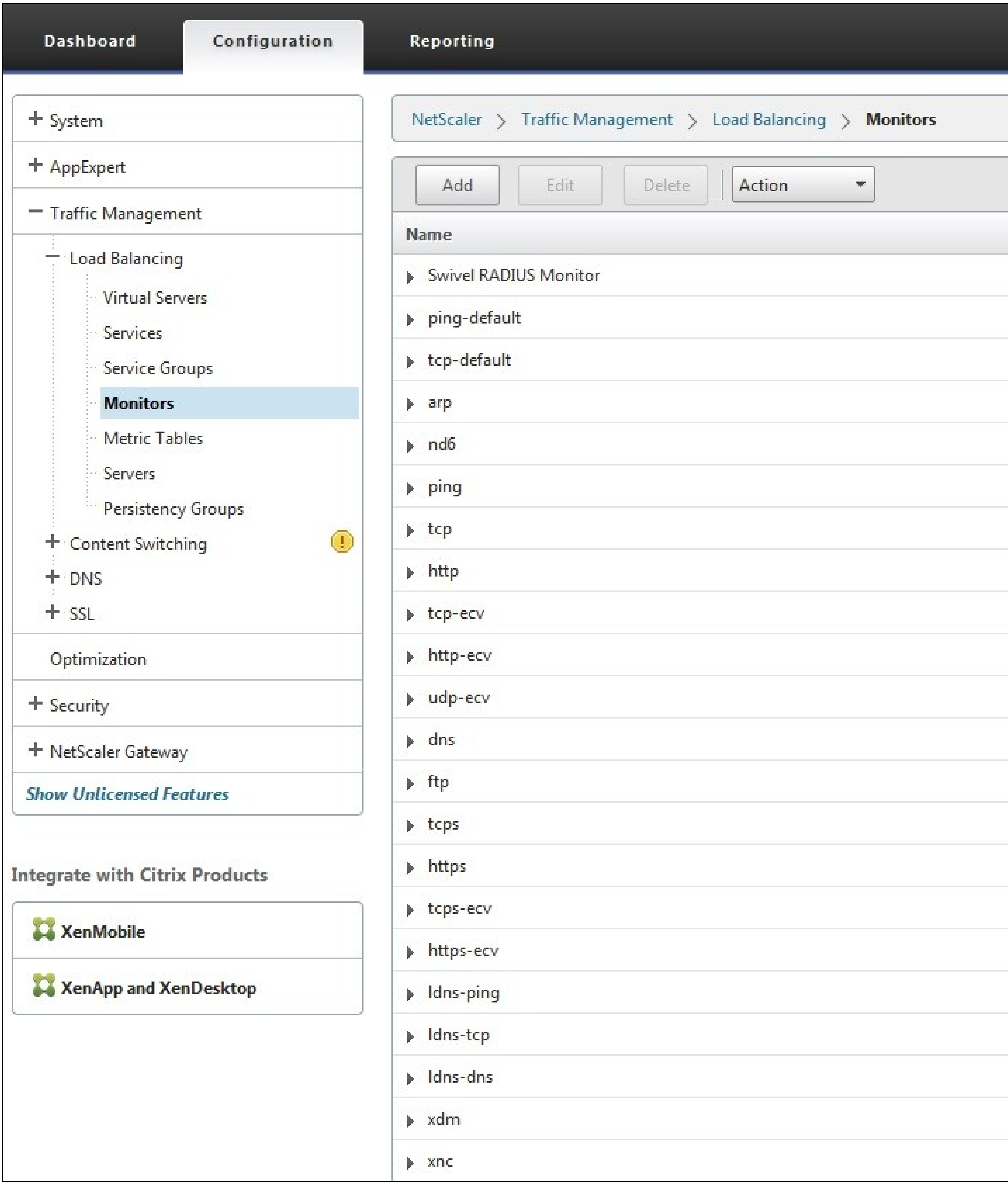
Password*: ●●●●●●●●●●●●●●

RADIUS Key*: ●●●●●●●●●●●●

NAS ID:

NAS IP: 0 . 0 . 0 . 0

The Monitor should appear in the list.

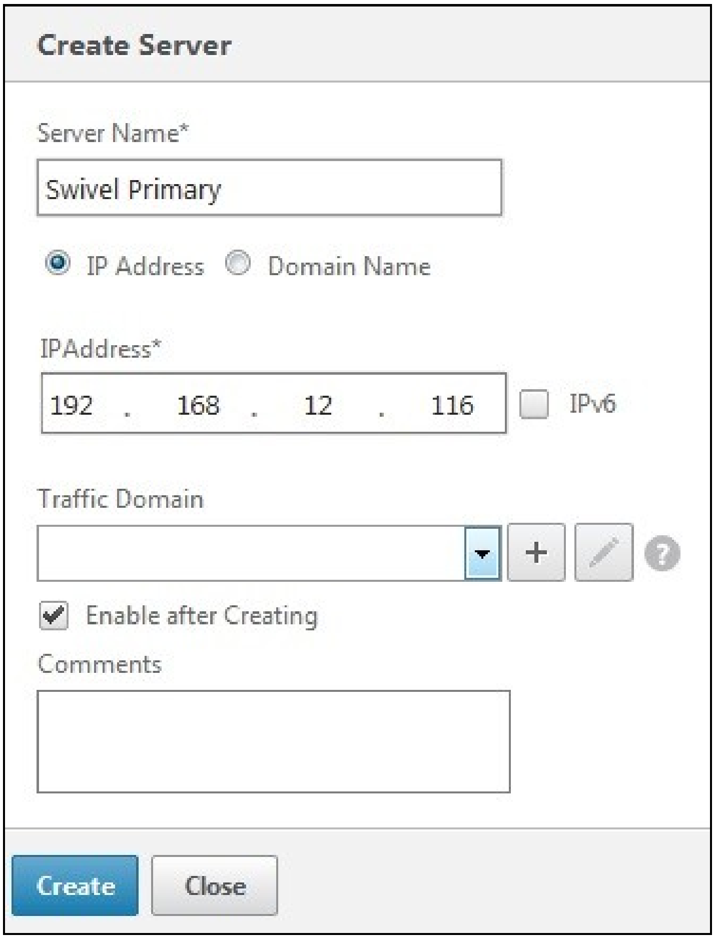


Name
Swivel RADIUS Monitor
ping-default
tcp-default
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
xdm
xnc

107.2 Create Entries for the Swivel RADIUS Servers

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

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



Create Server

Server Name*: Swivel Primary

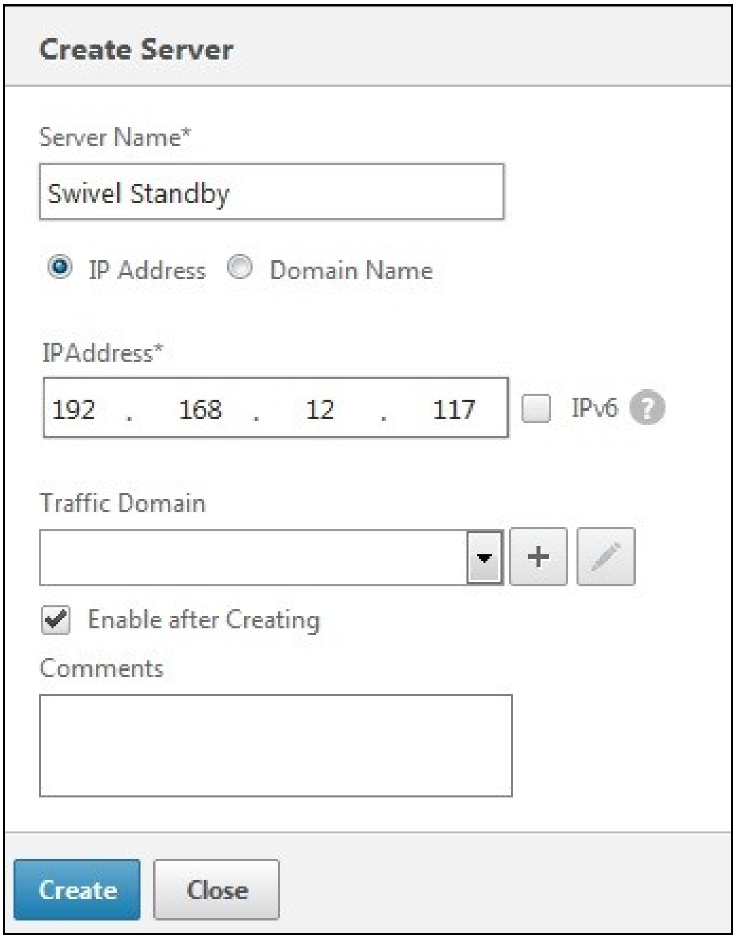
● IP Address ○ Domain Name

IPAddress*: 192 . 168 . 12 . 116 □ IPv6

Traffic Domain:

☑ Enable after Creating

Comments:



Create Server

Server Name*

Swivel Standby

● IP Address ○ Domain Name

IPAddress*

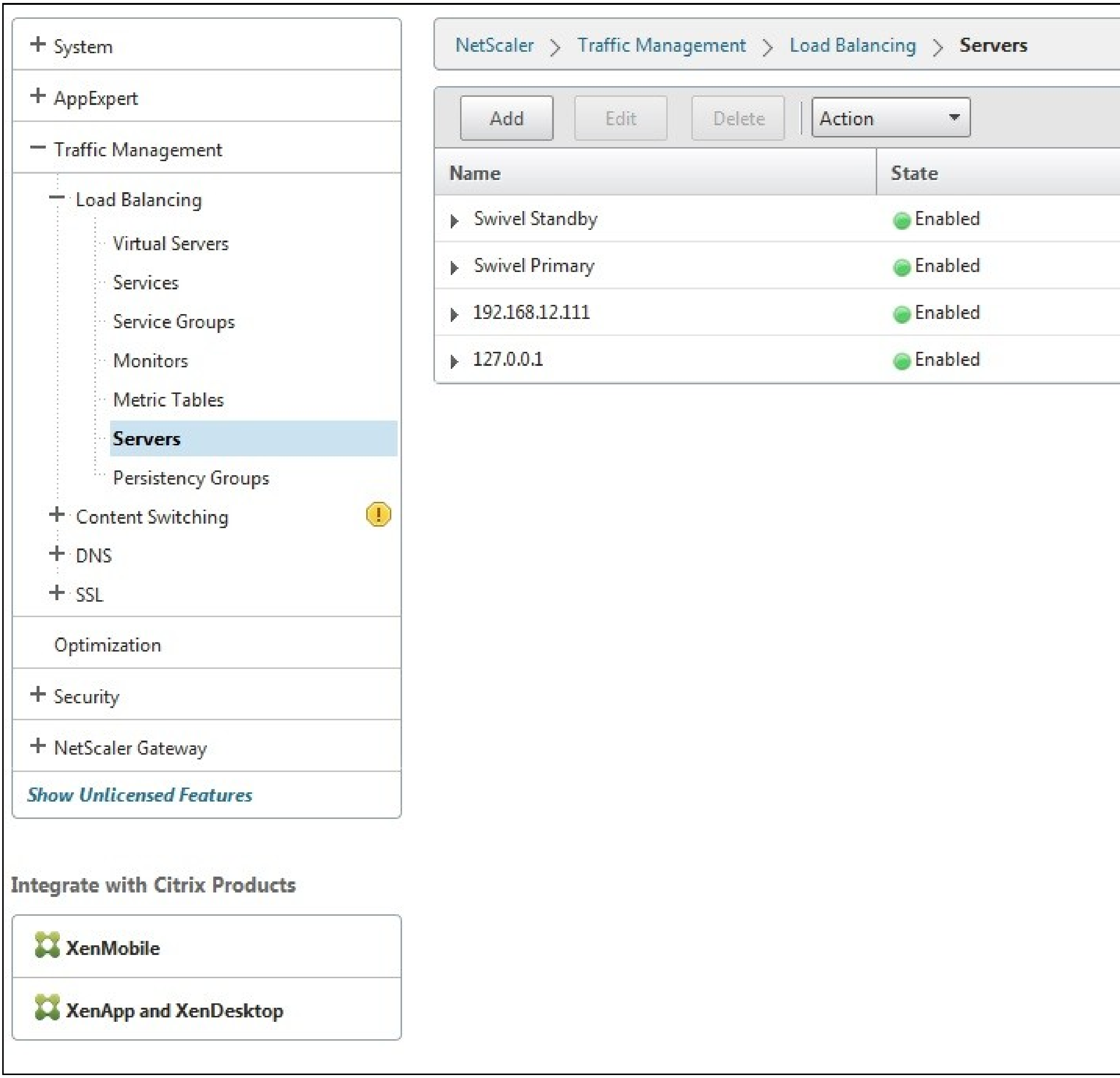
192 . 168 . 12 . 117 □ IPv6

Traffic Domain

☑ Enable after Creating

Comments

Click Create to create the Server

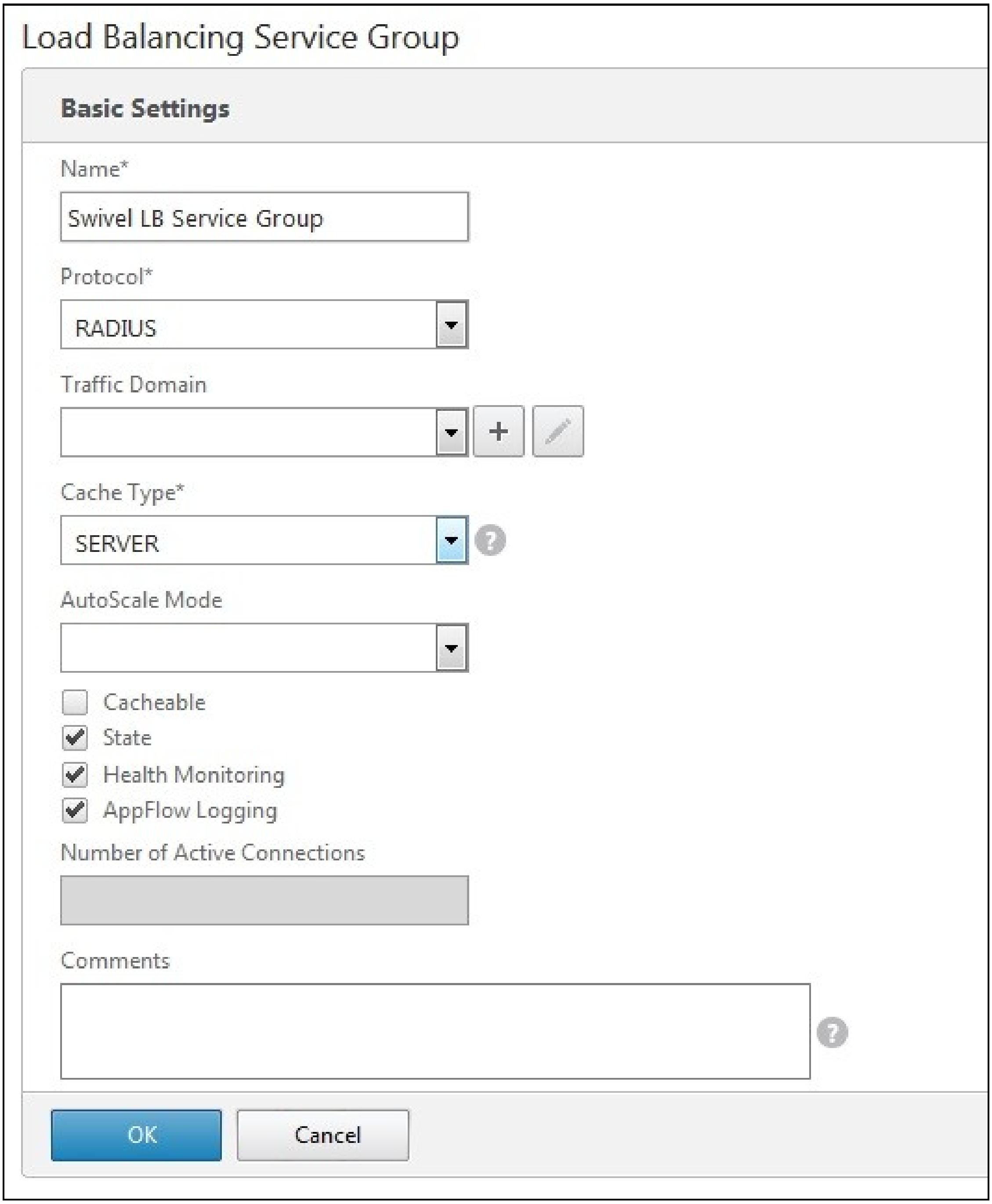


Name	State
Swivel Standby	● Enabled
Swivel Primary	● Enabled
192.168.12.111	● Enabled
127.0.0.1	● Enabled

107.3 Create a Swivel Load Balance Service Group

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

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



Load Balancing Service Group

Basic Settings

Name*: Swivel LB Service Group

Protocol*: RADIUS

Traffic Domain:

Cache Type*: SERVER

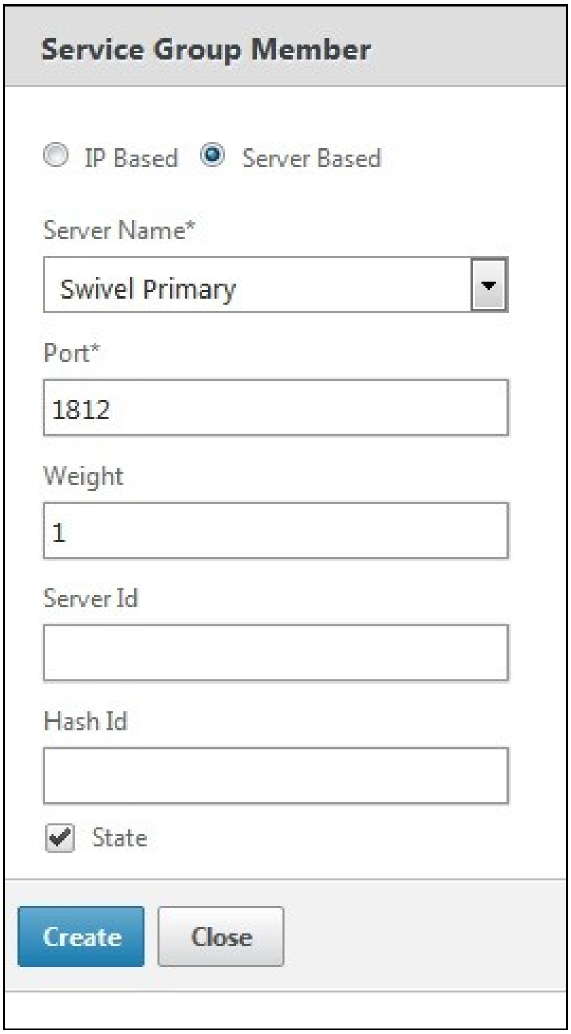
AutoScale Mode:

☐ Cacheable
☑ State
☑ Health Monitoring
☑ AppFlow Logging

Number of Active Connections:

Comments:

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

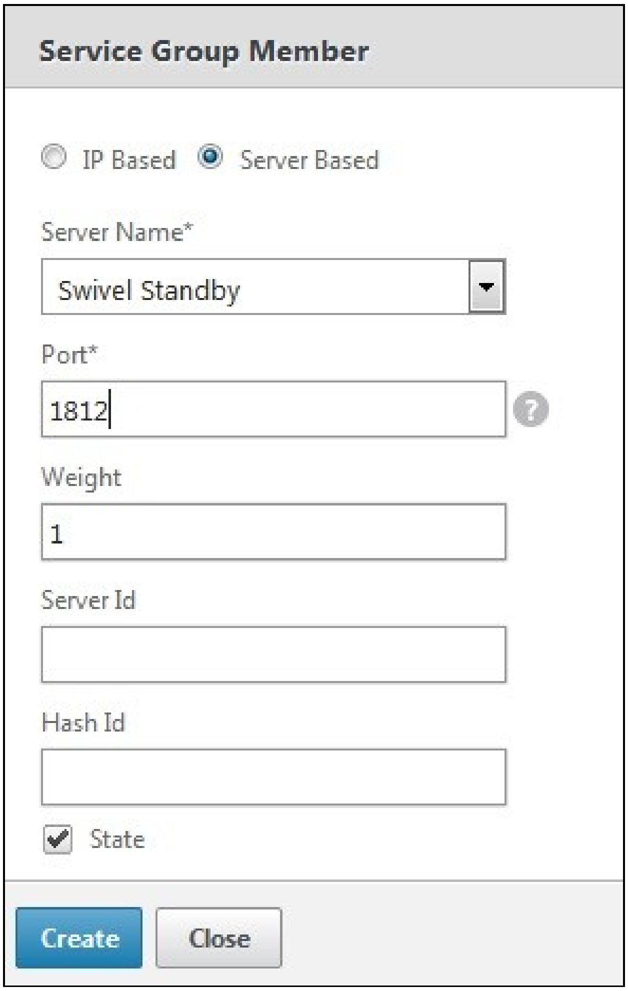
Port*: 1812

Weight: 1

Server Id:

Hash Id:

☑ State



Service Group Member

○ IP Based ● Server Based

Server Name*: Swivel Standby

Port*: 1812

Weight: 1

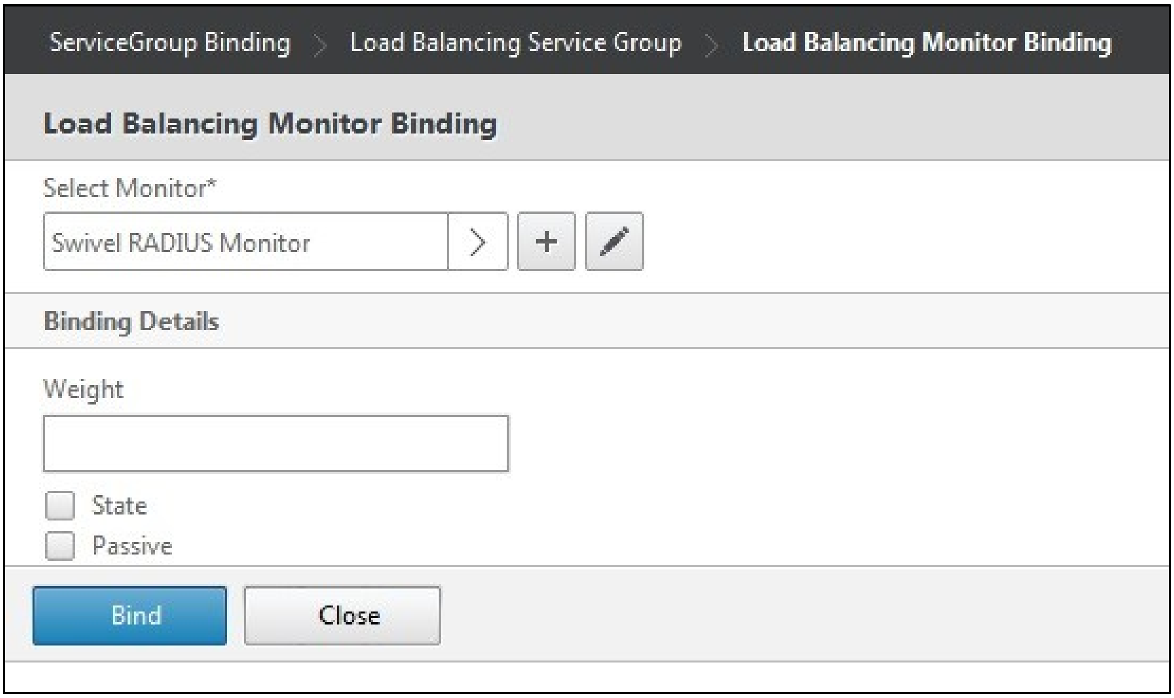
Server Id:

Hash Id:

☑ State

107.3.1 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:

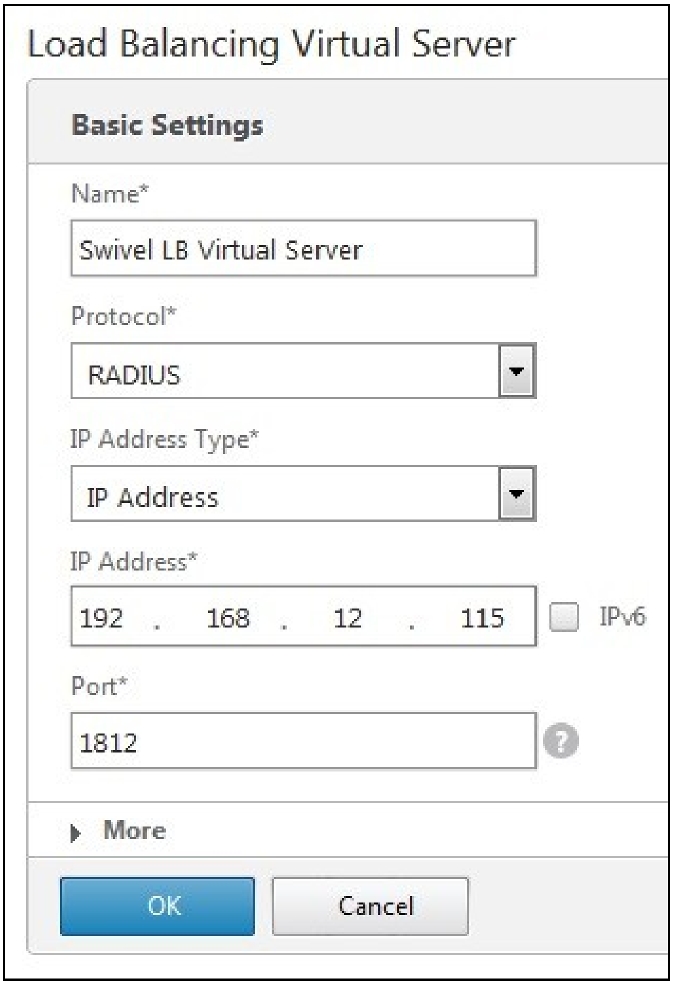
□ State

□ Passive

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

107.4 Create A Virtual Server

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



Load Balancing Virtual Server

Basic Settings

Name*: Swivel LB Virtual Server

Protocol*: RADIUS

IP Address Type*: IP Address

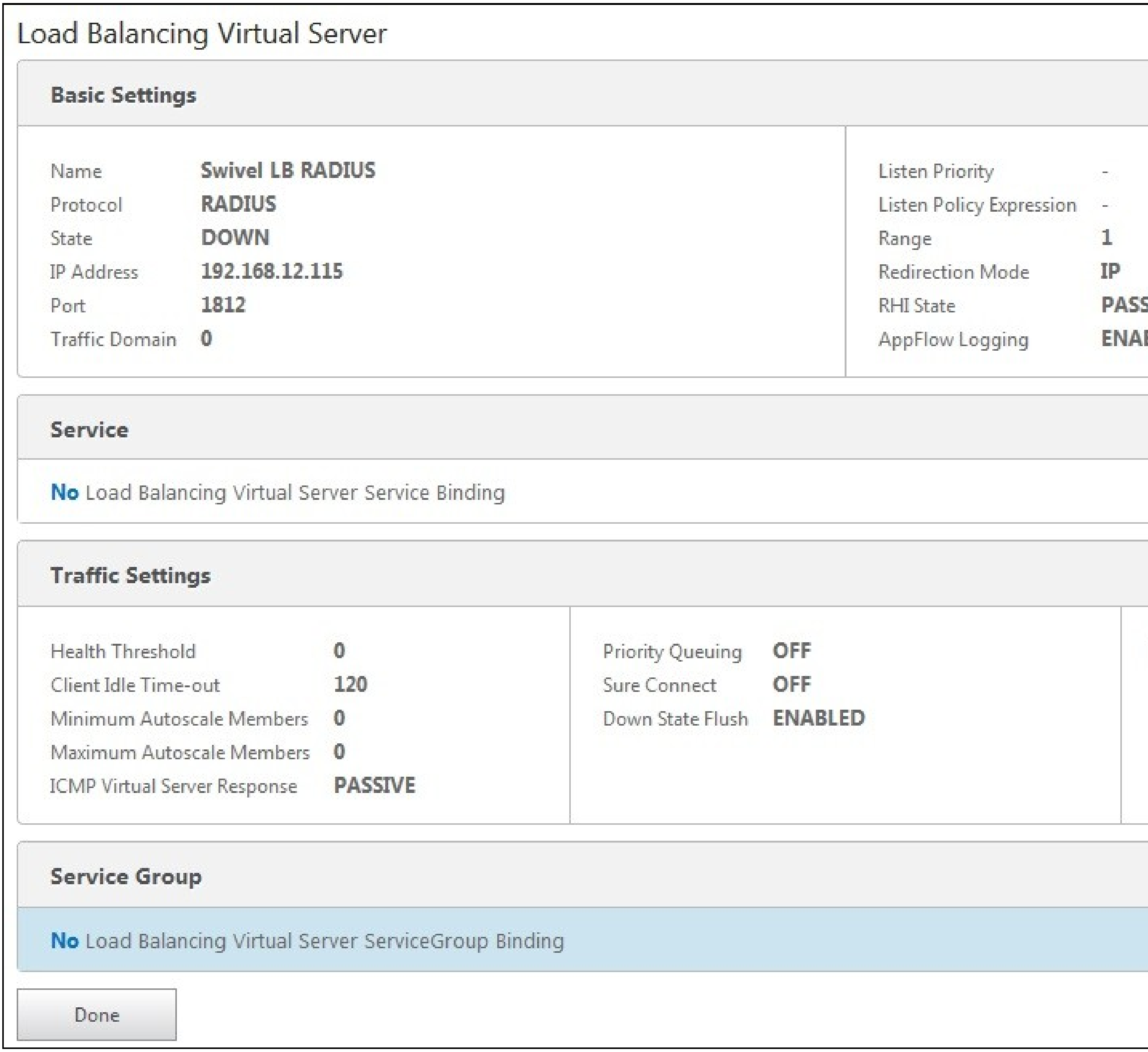
IP Address*: 192 . 168 . 12 . 115 □ IPv6

Port*: 1812

Click OK to create the entry

107.4.1 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	ENAI

Service

No Load Balancing Virtual Server Service Binding

Traffic Settings

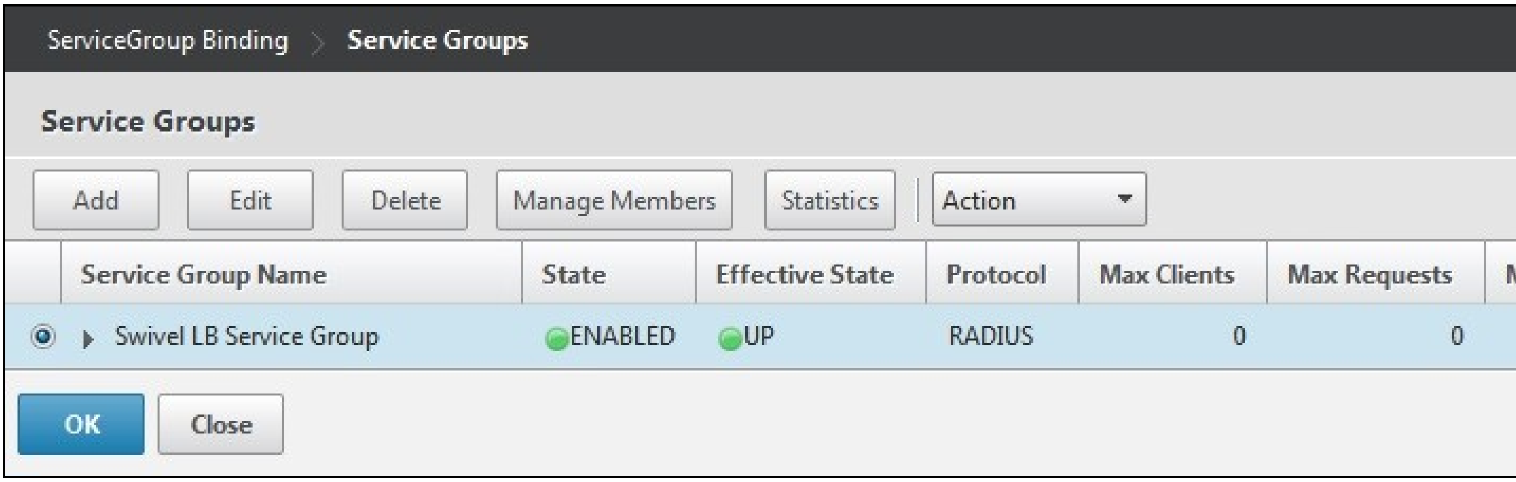
Health Threshold	0
Client Idle Time-out	120
Minimum Autoscale Members	0
Maximum Autoscale Members	0
ICMP Virtual Server Response	PASSIVE

Priority Queuing	OFF
Sure Connect	OFF
Down State Flush	ENABLED

Service Group

No Load Balancing Virtual Server ServiceGroup Binding

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



ServiceGroup Binding > Service Groups

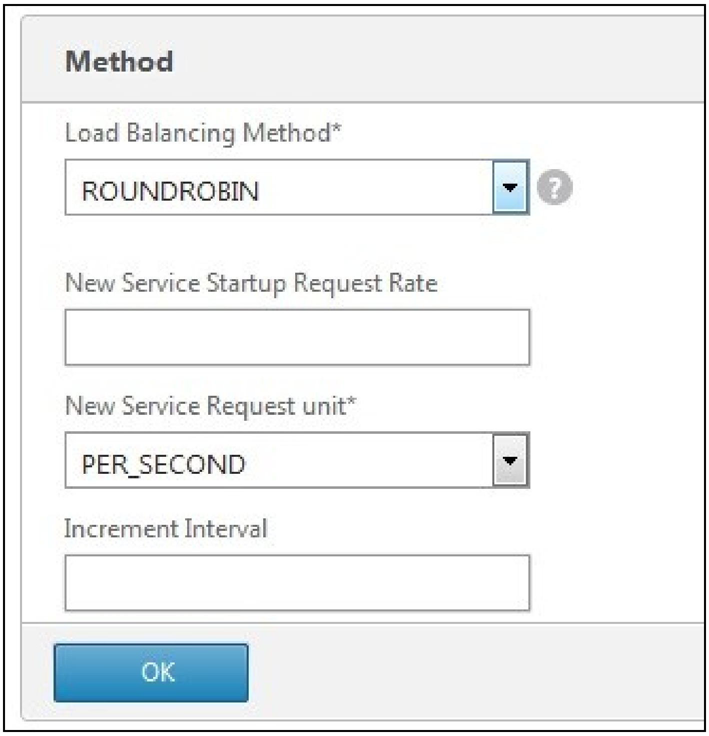
Service Groups

	Service Group Name	State	Effective State	Protocol	Max Clients	Max Requests
●	Swivel LB Service Group	ENABLED	UP	RADIUS	0	0

Then click **Bind**

107.4.2 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

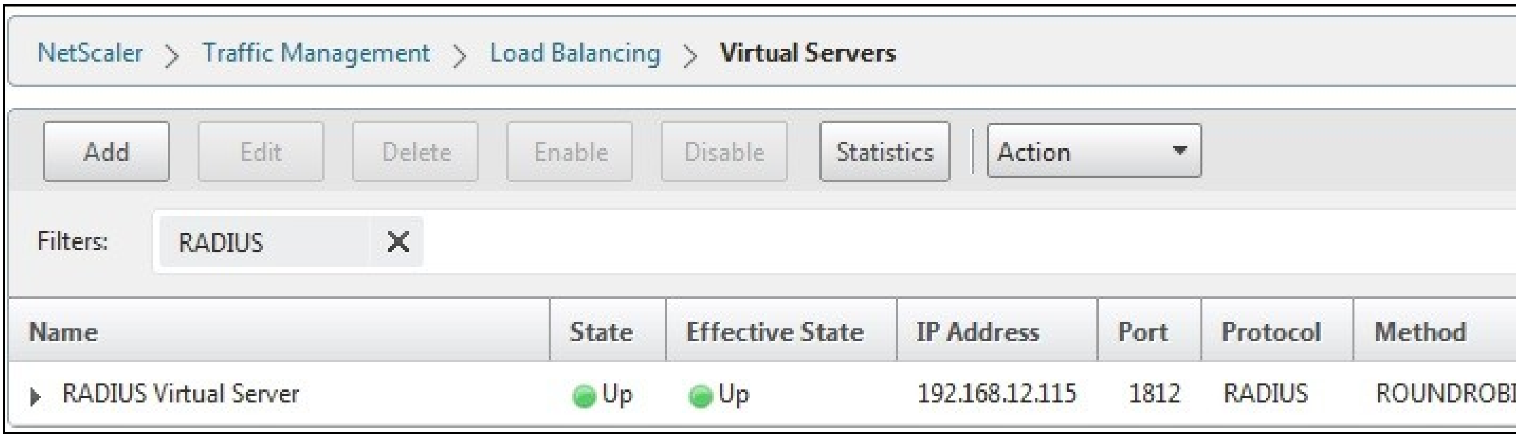
Load Balancing Method*: ROUNDROBIN

New Service Startup Request Rate:

New Service Request unit*: PER_SECOND

Increment Interval:

Click Done and the Virtual server should be created.



NetScaler > Traffic Management > Load Balancing > Virtual Servers
Add
Edit
Delete
Enable
Disable
Statistics
Action

Filters: RADIUS ✕

Name	State	Effective State	IP Address	Port	Protocol	Method
▸ RADIUS Virtual Server	● Up	● Up	192.168.12.115	1812	RADIUS	ROUNDROBI

107.5 Netscaler RADIUS configuration

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

108 Testing

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

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

109 Known Issues

The load balancing can produce a large number of logs.

110 Troubleshooting

111 Category:Netscaler

112 Citrix Receiver

[[Category:android|A]]

113 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 configuring Netscaler and Receiver to work with multiple authentication servers see Citrix Netscaler configuration for Receiver

114 Prerequisites

Citrix receiver Client

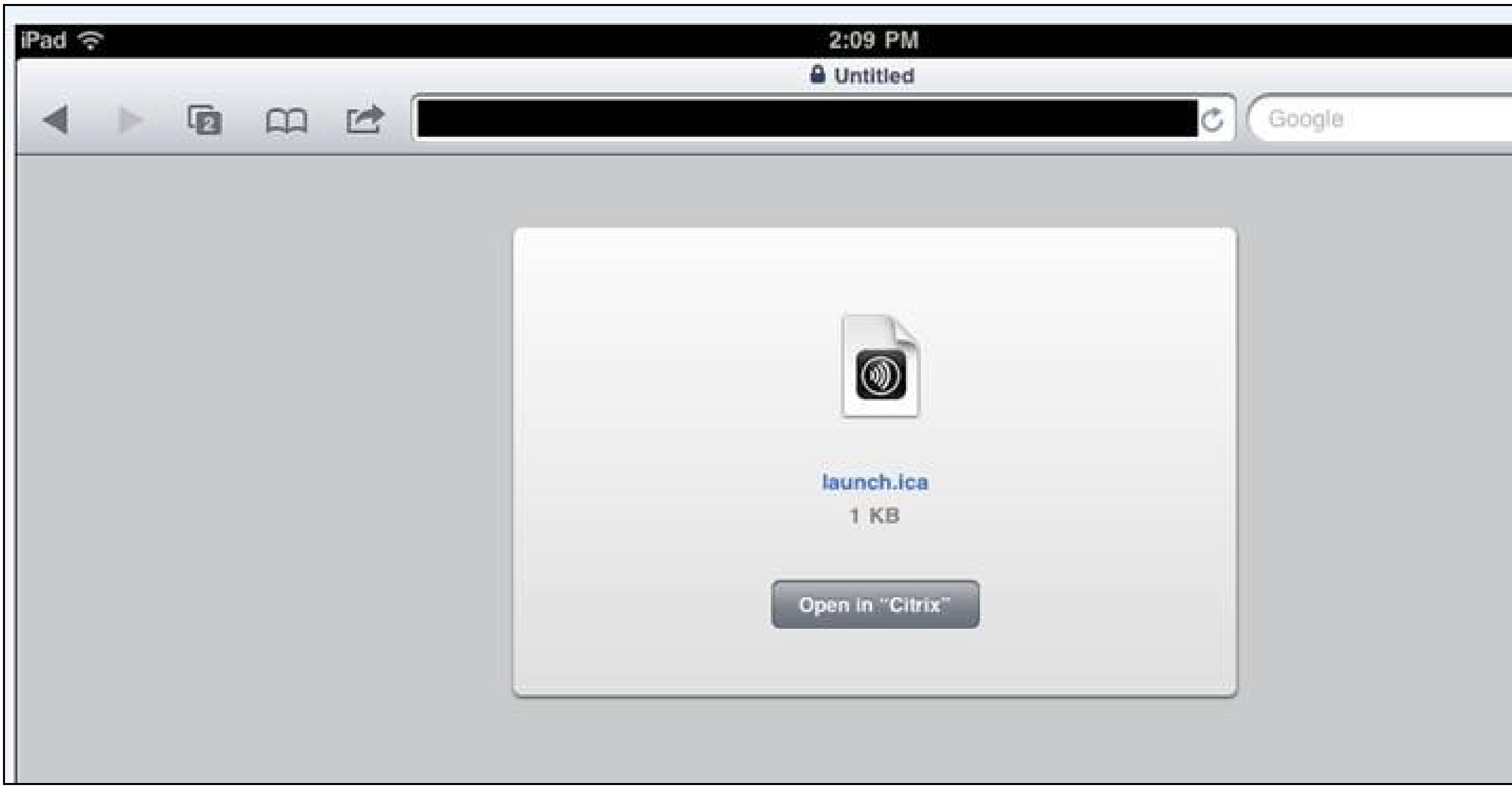
Swivel Appliance or Server

Citrix Gateway integrated with Swivel

115 iPhone / Android Citrix receiver

1. Open the **Safari** web browser on the iPad / **Mozilla Firefox** on Android Please see Known Issues and Limitations
2. Browse to the login page of the Citrix gateway
3. Enter username, password, and Swivel security string (Using TURing or SMS). Click login button.
4. Once the user is logged in go to the Citrix gateway, click on the Citrix application they want to launch (eg, the published desktop)
5. Here?s where things are a little different from a PC. Instead of just launching the Citrix plug-in directly, the user will see the screen shot in the attachment. The user then clicks on the ?Open in Citrix? button.
6. The Citrix receiver app will launch and allow the user to access the selected Citrix app

The latest version of the Citrix Receiver supports ?Third-Party Authentication support? for the iOS and Android platform allowing the configuration data to be retrieved from a Citrix gateway URL, so there is no Swivel configuration required on the directly within the Receiver app.



116 Citrix Netscaler RADIUS authentication for Receiver

For configuring Netscaler and Receiver to work with multiple authentication servers see Citrix Netscaler configuration for Receiver

117 Citrix Access Standard Edition Gateway RADIUS authentication for Receiver

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

118 Citrix Access Advanced Edition Gateway RADIUS authentication for receiver

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

119 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)

120 Citrix Web Interface 4 with Presentation Server 4

120.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix Presentation Server 4 web interface. This also works with Citrix Secure Gateway v3.0. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

120.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 45083 of the Citrix web interface and have been tested with versions 4.0 and 4.2, for later versions please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.cs ? Customised login logic constants.
- login.cs ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here: File:Citrix_PS_4.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

120.3 Baseline

PINsafe 3.x

Citrix Web Interface build 3.x, 4.0, 4.2

120.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

120.5 PINsafe Configuration

120.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

120.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet.

On the PINsafe server:

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

Click Apply to save settings.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

120.6 Citrix Web Interface Configuration

120.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.cs and login.cs to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

120.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

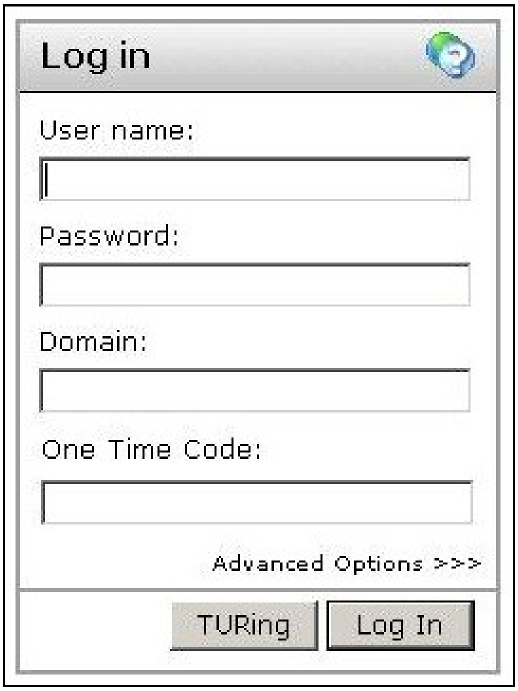
```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

120.7 Additional Configuration Options

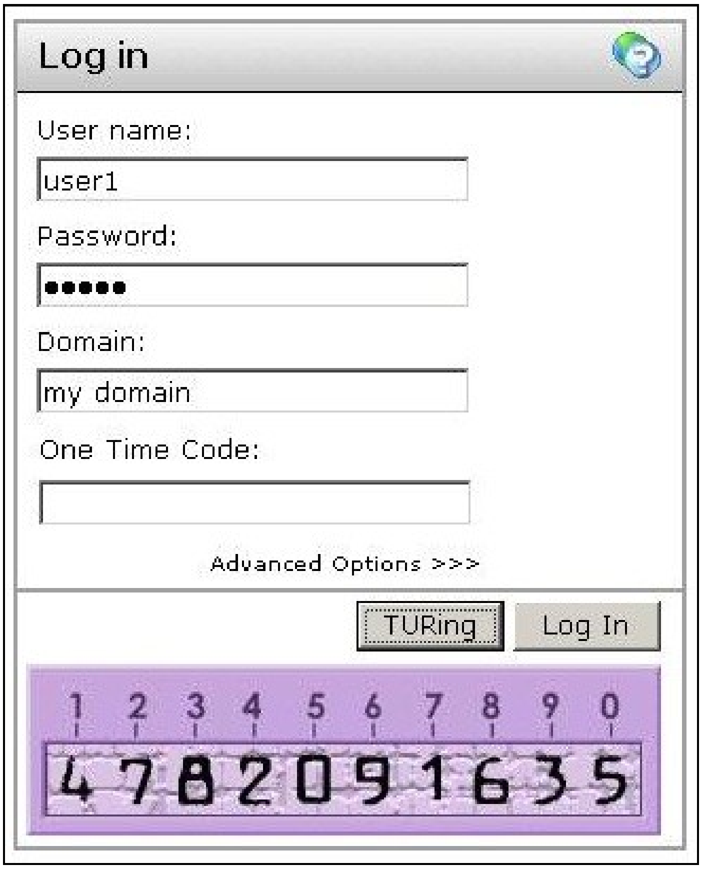
120.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface login with SMS (Do not click on the Turing Button)



Citrix Web Interface login with Turing



User name: user1

Password: •••••

Domain: my domain

120.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

120.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

120.11 Known Issues and Limitations

Self signed certificates are not supported with this version of the integration, either use a valid certificate, or non SSL communications or upgrade the Web Interface version.

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

120.12 Additional Information

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

121 Citrix Web Interface 4.5 Integration

121.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.5 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

121.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.5.1.8215 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.aspxf ? Customised login logic constants.
- login.aspxf ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\MetaFrame

121.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.5.1.8215

121.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

121.5 PINsafe Configuration

121.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

121.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCIMage servlet.

On the PINsafe server:

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

Click Apply to save settings.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

121.6 Citrix Web Interface Configuration

121.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

121.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

121.7 Additional Configuration Options

121.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

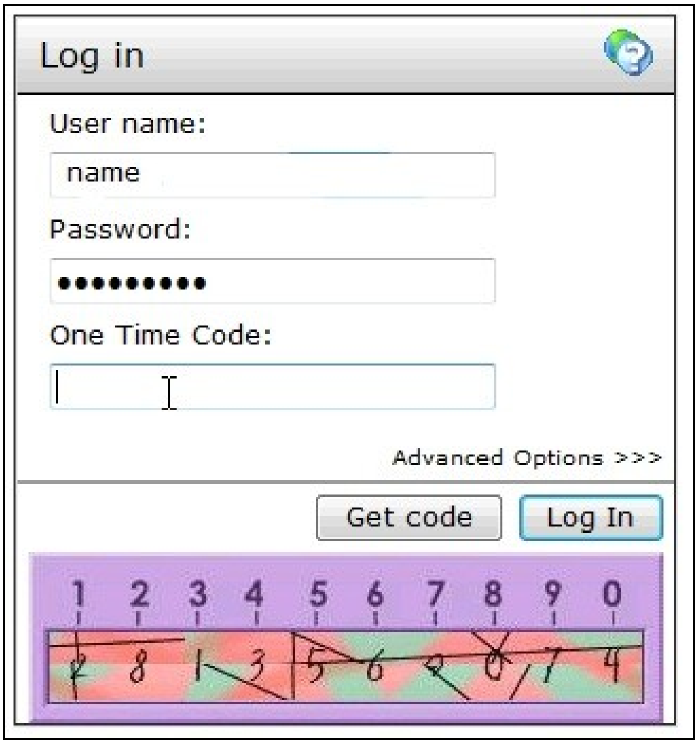
to

if (!pc.Login(user,password, otc))

121.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with TURing image (For SMS do not click on Get Code button)



121.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

121.9.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

121.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

121.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

121.12 Additional Information

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

122 Citrix Web Interface 4.6 Integration

122.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.6 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

122.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.6.0.18291 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.aspxf ? Customised login logic constants.
- login.aspxf ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

122.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.6.0.18291

122.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

122.5 PINsafe Configuration

122.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

122.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet.

On the PINsafe server:

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

Click Apply to save settings.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

122.6 Citrix Web Interface Configuration

122.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

122.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

122.7 Additional Configuration Options

122.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

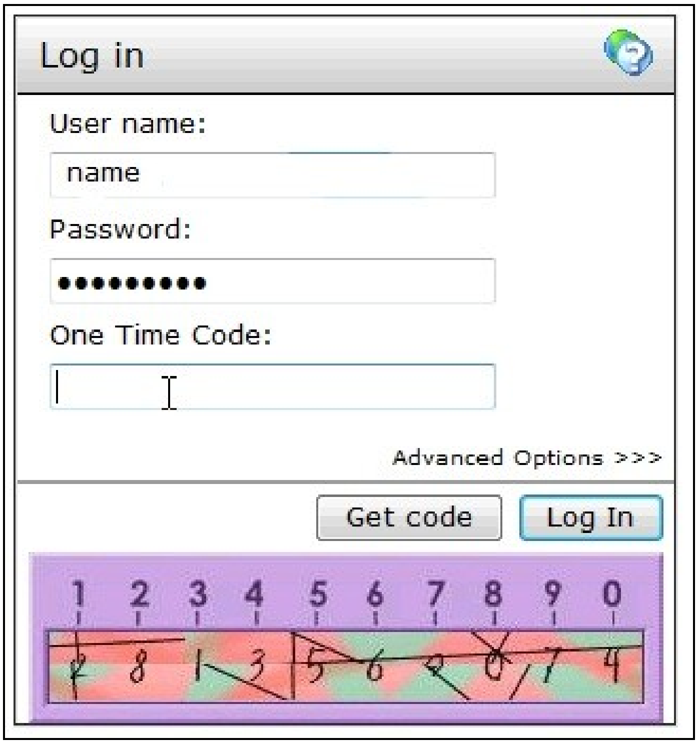
to

if (!pc.Login(user,password, otc))

122.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with Turing image (For SMS do not click on Get Code button)



Log in

User name:

name

Password:

●●●●●●●●●

One Time Code:

122.9 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

122.10 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

122.10.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

122.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

122.12 Additional Information

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

123 Citrix Web Interface 5.0 Integration

123.1 Introduction

This document outlines the necessary steps to integrate Swivel authentication into the Citrix 5.0 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the Swivel server as the Image is proxied through the Web Interface server.

123.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.0.1.29110 of the Citrix web interface, if you have a later version please contact your Swivel reseller for an update. Your Swivel server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? Swivel authentication client library.
- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from Swivel to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for Swivel integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

123.3 Baseline

Swivel 3.5

Citrix Web Interface build 5.0.1.29110

123.4 Architecture

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

124 Swivel Configuration

124.1 Configuring the RADIUS server

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

124.2 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.

124.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

124.3 Citrix Web Interface Configuration

124.3.1 Copy accros the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

124.3.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the Swivel server.

124.3.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your Swivel installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />
```

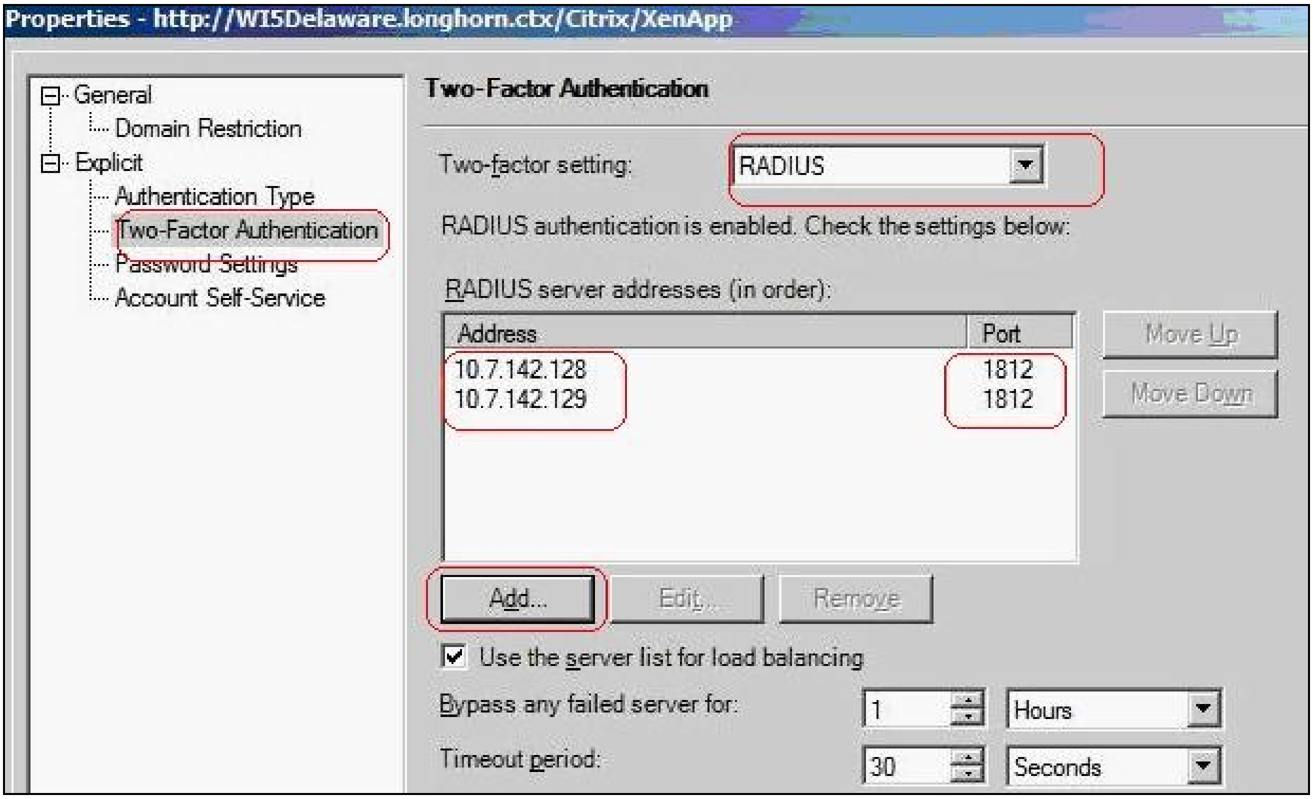
```
<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />
```

124.3.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, the select Radius from the dropdown list.



Properties - http://WI5Delaware.longhorn.ctx/Citrix/XenApp

Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

124.4 Additional Configuration Options

see Citrix Web Interface 5.X additional login page options

124.5 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Citrix credentials should the user be logged in.

124.6 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the Swivel RADIUS entries.

124.7 Troubleshooting

Check the Swivel logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the Swivel server or for testing the client can accept the certificate (load Image URL into browser)
- Swivel server not accessible, check networking and firewalls. Check the Swivel server logs for a session started message.
- Incorrect Swivel URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

124.7.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the Swivel NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

124.8 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the Swivel settings and files so the Swivel integration may need to be applied again.

124.9 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

125 Citrix Web Interface 5.1 Dual Channel button

125.1 Citrix Web Interface Dual Chanel Integration Notes

This outlines how to replace the Single Channel Image request button with a Dual Channel button. This is a supplement to the Citrix Web Interface 5.1 Integration guide.

125.2 Log-in page Customisation

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
       href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
       onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
       onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
       tabIndex="<%=Constants.TAB_INDEX_FORM%>"
       id="dcmessage"
       name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

125.3 Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

126 Citrix Web Interface 5.1 Integration

127 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.1 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

128 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.1.1 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.1_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

129 Baseline

PINsafe 3.5

Citrix Web Interface build 5.1.1

130 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

131 Swivel Configuration

131.1 Configuring the RADIUS server

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

131.2 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.

131.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

132 Citrix Web Interface Configuration

132.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

132.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

132.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />
```

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

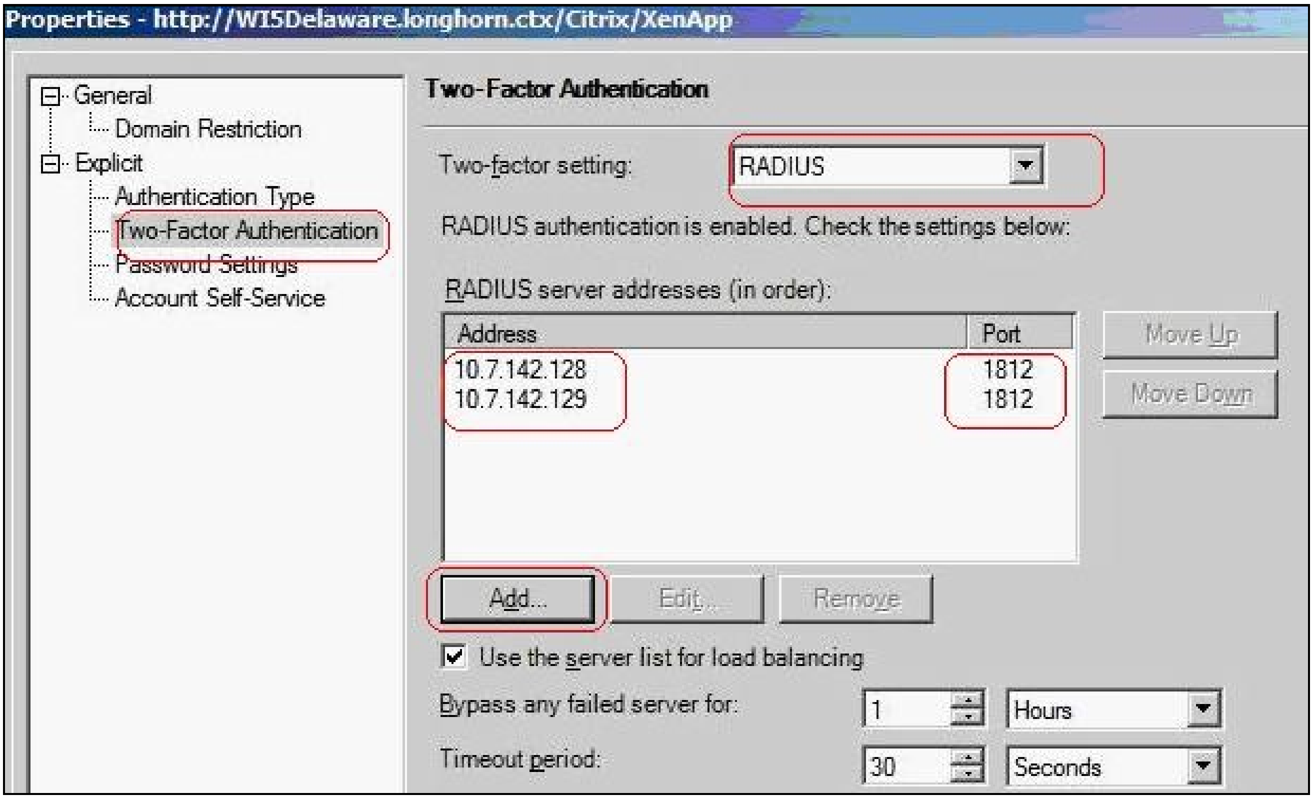
```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="true" />
```

132.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list.



Properties - http://WI5Delaware.longhorn.ctx/Citrix/XenApp

Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

133 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

133.1 Self Reset

This outlines how to add the self reset option to the Citrix Web Interface.

The Citrix Web Interface 5.1 self reset files can be downloaded here: File:Citrix_WI_5.1_SelfReset.zip

Download PINsafeClient.dll and copy to the bin folder overwriting the existing file installed above. Copy reset.aspx and reset.aspx.cs into the auth folder.

Add reset.aspx to the list of unprotected pages in web.config. Locate key="AUTH:UNPROTECTED_PAGES", and at the end of the value field, insert ",./reset.aspx".

Insert a link on the Citrix login page to open the reset page.

Edit app_data\include\loginMainForm.inc, and insert the following line after the login button row, immediately before the </table> tag.

<tr><td><a href="./reset.aspx" target="_blank">Forgotten my PIN</a></td></tr>

134 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

135 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the PINsafe RADIUS entries.

136 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

136.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

137 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

138 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

139 Citrix Web Interface 5.2 Integration

140 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.2 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

141 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.2 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- include.aspxf ? Customised include file.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.2_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

142 Baseline

PINsafe 3.5

Citrix Web Interface build 5.2

143 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

144 Swivel Configuration

144.1 Configuring the RADIUS server

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

144.2 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.

144.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

145 Citrix Web Interface Configuration

145.1 Copy across the Web Interface Files

The The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

145.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

145.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />
```

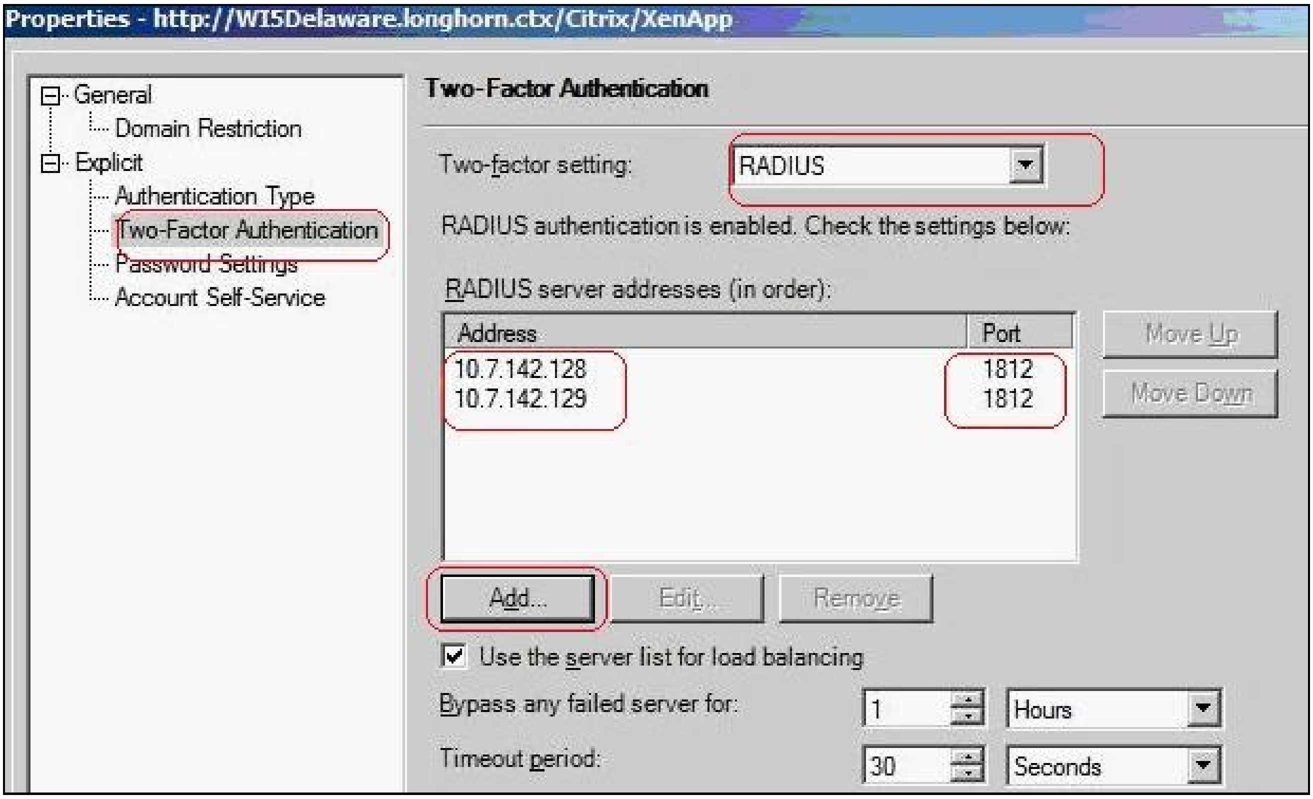
```
<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />
```

145.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

Configure the PINsafe server as RADIUS server. If you have more than 1 PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

146 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

147 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

148 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

149 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

149.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

150 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

151 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

152 Citrix Web Interface 5.3 Integration

153 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.3 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

154 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.3 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependant on the OS being 32 bit or 64 bit.

155 Baseline

PINsafe 3.5

Citrix Web Interface build 5.3

156 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

157 Swivel Configuration

157.1 Configuring the RADIUS server

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

157.2 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.

157.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

158 Citrix Web Interface Configuration

158.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

158.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

158.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Note: The setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be set to <add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />
```

The settings for a software install of PINsafe are:

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />
```

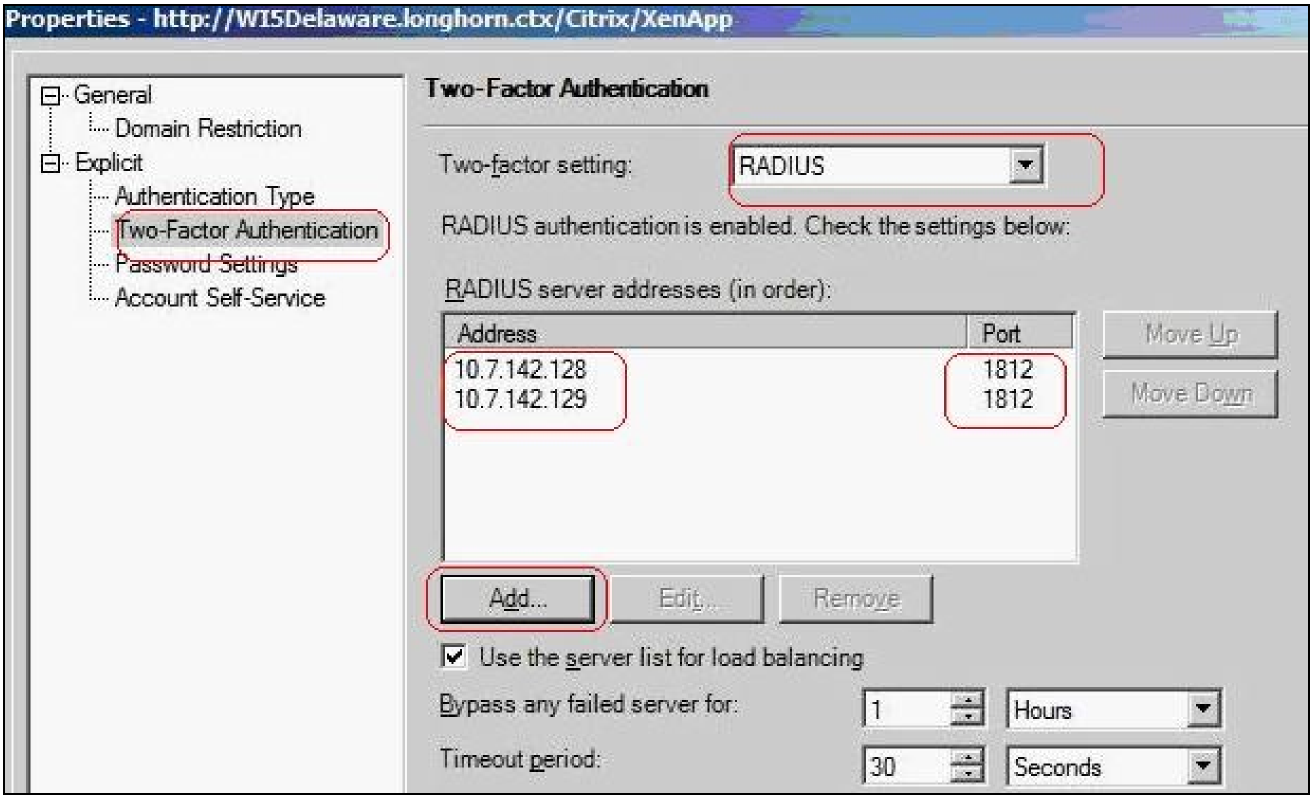
```
<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="false" />
```

158.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Properties - http://WI5Delaware.longhorn.ctx/Citrix/XenApp

Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

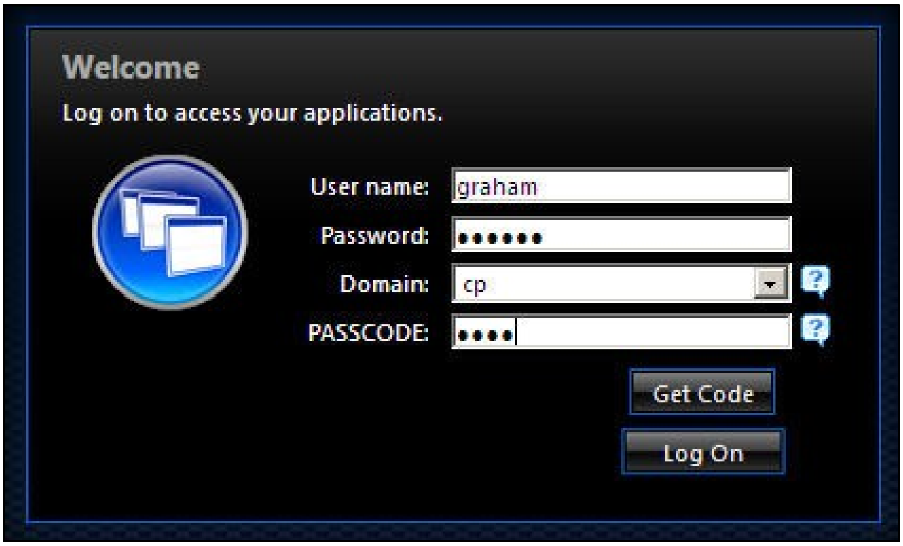
159 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

160 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication



Welcome

Log on to access your applications.

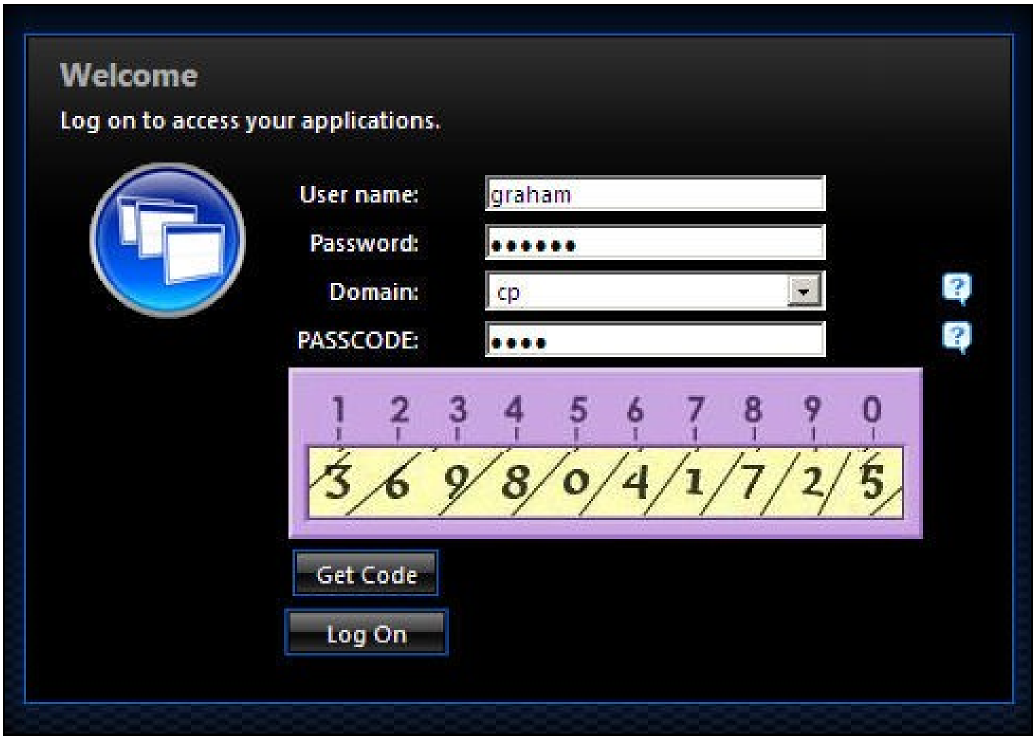
User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

Login Using Single Channel Graphical Turing Image



Welcome

Log on to access your applications.

User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

1	2	3	4	5	6	7	8	9	0
3	6	9	8	0	4	1	7	2	5

161 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

162 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a PINsafe virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

162.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

163 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

164 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

165 Citrix Web Interface 5.4 Integration

166 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.4 web interface/Xen App. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

A statement from Citrix: *All 7.x versions of XenApp and XenDesktop now support the use of Web Interface 5.4. Citrix has extended support of Web Interface for XenApp 7.5, XenDesktop 7.5, XenDesktop 7.1 and XenDesktop 7.0 to allow more time for planning and transition to StoreFront. Note, no new features will be added to Web Interface and its end-of-life remains August 2016.*

167 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.4 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation and need to be edited as required (see below):

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js.add ? Customised login page client script.
- loginStyle.inc.add ? Customised login form style.
- loginMainForm.inc.add ? Customised login form.
- web.config.add ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here.

An alternative solution, which includes buttons for TURing image and message request, can be found here. This solution includes two additional files: pinsafe_message.aspx and pinsafe_ping.aspx.

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependent on the OS being 32 bit or 64 bit.

NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

NOTE: the files with the extension ".add" cannot simply be copied into the appropriate directories. They are text files containing notes as to how you should modify the corresponding files to implement PINsafe customisation. See the notes below for more details.

168 Baseline

PINsafe 3.7

Citrix Web Interface build 5.4

169 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

170 Swivel Configuration

170.1 Configuring the RADIUS server

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

170.2 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.

170.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

171 Citrix Web Interface Configuration

171.1 Edit the radius_secret.txt

On the Citrix Web Interface server

Edit the conf/radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server. A copy of this file is included in the zip archive.

171.2 Edit the web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Note: the setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be changed to

```
 <add key="RADIUS_NAS_IDENTIFIER" value="citrix_wi" />
```

Note: It is recommended that you use the same value as the identifier in the NAS entry in the PINsafe admin console.

If the Web Interface server has multiple network interfaces, the value of RADIUS_NAS_IP_ADDRESS may need to be set to the IP address used by the NAS. This is the IP address of the Web Interface server, NOT the PINsafe server.

Make sure that the following entry is included, if it is not there already:

```
 <add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />
```

To allow access to the TURing image from the login page, locate the following line:

```
 <add key="AUTH:UNPROTECTED_PAGES" ...
```

The value attribute on this entry is a list of URLs that can be accessed without authentication. Add the following to the end of this list (before the closing quote):

```
 ,/auth/pinsafe_image.aspx
```

If you are using the alternative integration, you will need to include the other files:

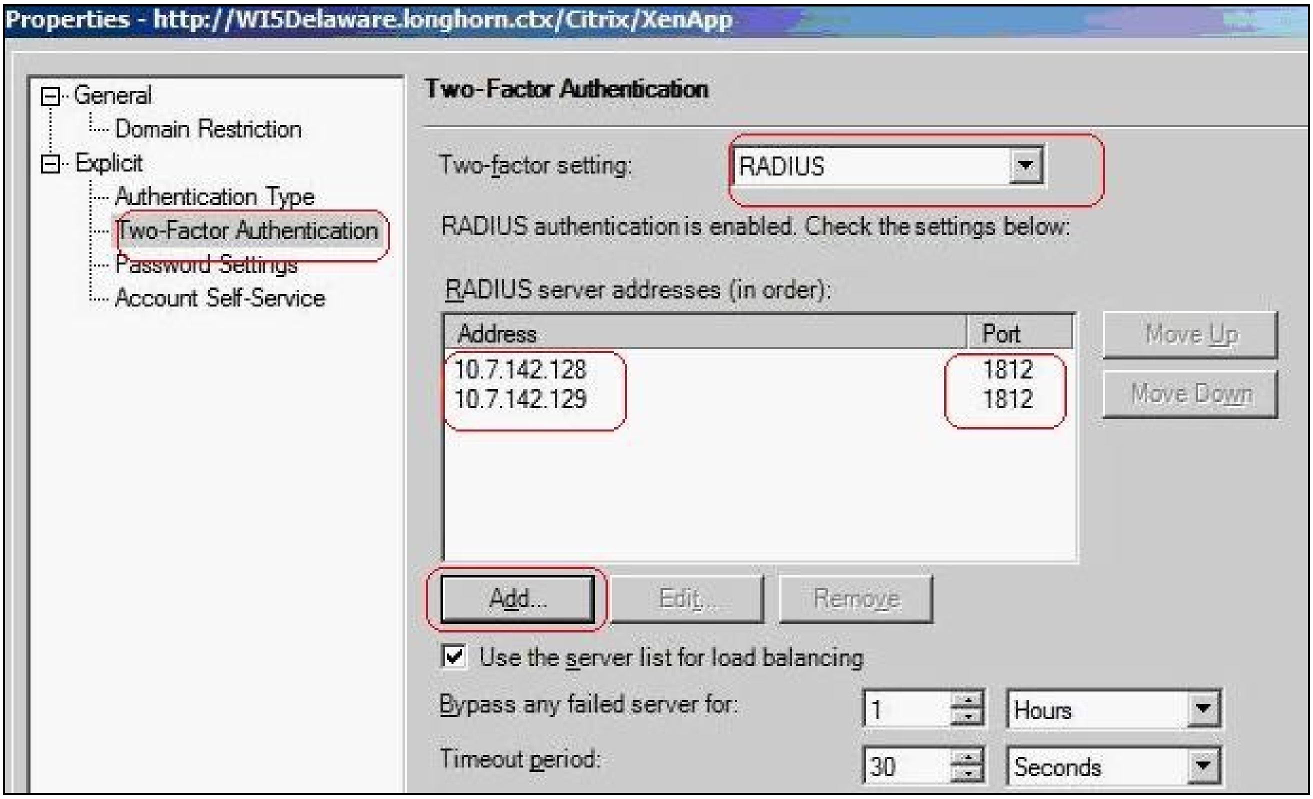
```
,/auth/pinsafe_image.aspx,/auth/pinsafe_message.aspx,/auth/pinsafe_ping.aspx
```

171.3 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.



Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

172 Additional Configuration Options

The above modifications will allow authentication to the Web Interface using some of the PINsafe authentication mechanisms such as SMS, mobile Phone applet, and Taskbar. Additional configuration options including the single channel TURing image are listed below.

see also Citrix Web Interface 5.X additional login page options

172.1 Changing the OTC label

To change the label for the PINsafe one-time code field from the default of ?PASSCODE:?, locate the file C:\Program Files\Citrix\Web Interface\5.4.0\Languages\accessplatform_strings.properties. (If the language is not English, locate the appropriate file for the appropriate language, if it exists). Edit this file, and locate the line containing ?Passcode=PASSCODE:?. Replace the second word PASSCODE with OTC, or an appropriate text.

172.2 Configuring Single Channel: Modifying the Web Interface Files

The required files (see prerequisites) are of two types: those NOT ending in ".add" need to be copied to the following locations below the root of the Citrix web interface site. Those ending in ".add" contain instructions describing how to modify the corresponding file without the ".add" extension. Where an existing file is being replaced or modified, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory. The below files contained within the zip file should extract to the relevant locations.

The majority of the files included in the integration are modifications to existing files. This are stored with the same name as the file they are intended to modify, but with the additional extension of .add. Each file contains instructions as to how the original files should be added. More details are given below:

1. Copy pinsafe_image.aspx to /auth. This is a new file, not a modification to an existing one.

2. Edit login.js in /auth/clientscripts. Insert the contents of login.js.add at the start of this file, below the header, as indicated in the file itself.

3. Edit loginMainForm.inc in /app_data/include. Insert the contents of loginMainForm.inc.add as indicated in this file: locate a particular section of the file and insert a line.

4. Edit loginstyle.inc in /app_data/include. Insert the contents of loginstyle.inc.add at the bottom of this file, before the footer text, as indicated in the file.

5. Ensure file permissions are set correctly on the copied files, Authenticated users need read permissions.

172.3 Configuring Single Channel: Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

The web.config.add file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />
```

The settings for a software install of PINsafe are:

```
<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />
```

```
<add key="PINsafe_AcceptSelfSigned" value="false" />
```

172.4 Challenge and Response Authentication with Count Down Timer

Citrix Web Interface can be configured to use Challenge and Response whereby a user enters a username and password, and if that is correct the user is sent an SMS message and will be prompted to enter an OTC. By default the OTC sent is valid for two minutes only, so a count down timer is provided to show how long the user has left.

For information on configuring the PINsafe RADIUS Challenge and response see Challenge and Response How to Guide.

The required files can be downloaded here: Challenge and Response with count down files

Extract the files ensuring their correct locations

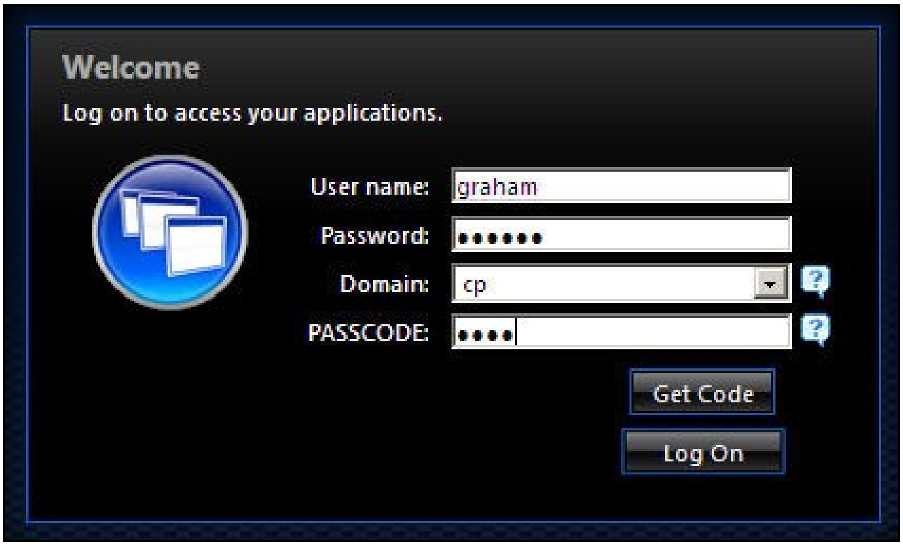
challenge.inc is copied to app_data/include

challenge.js to auth/clientscripts

173 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication



Welcome

Log on to access your applications.

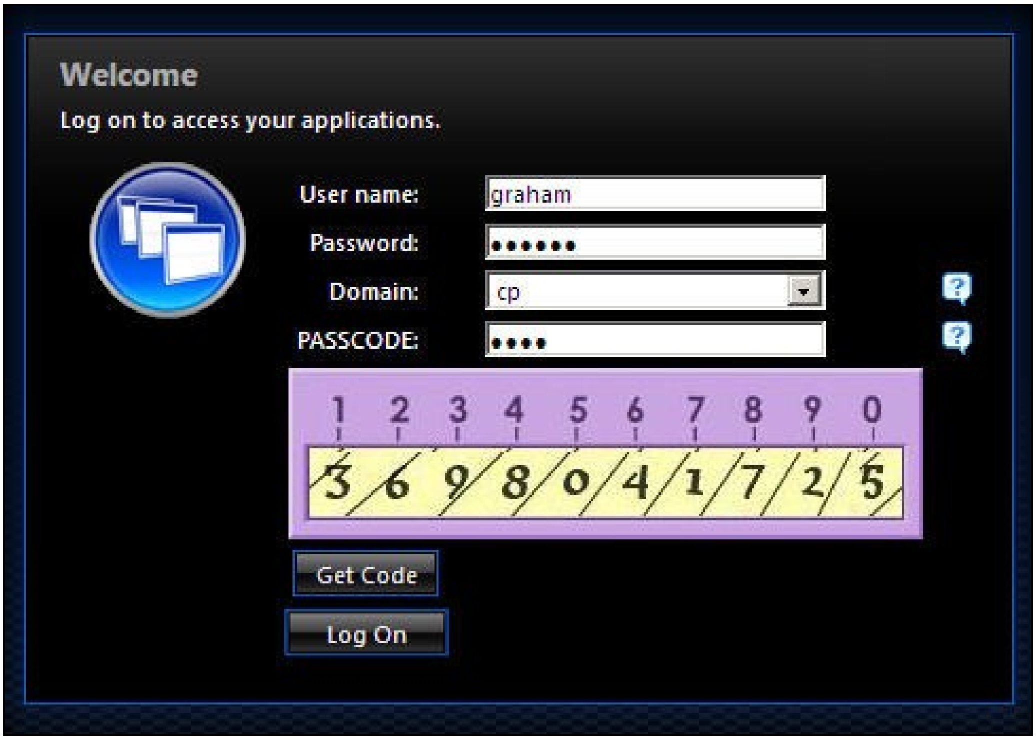
User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

Login Using Single Channel Graphical Turing Image



Welcome

Log on to access your applications.

User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

1	2	3	4	5	6	7	8	9	0
3	6	9	8	0	4	1	7	2	5

174 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

175 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate, you need to add the following entry to web.config:

```
<add key="PINsafe_AcceptSelfSigned" value="true" />
```

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

175.1 Error Messages

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

176 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

If you need to use userPrincipalName to authenticate to Swivel, you may find that the domain name is removed before sending the username to Swivel. To avoid this, make the following changes:

Locate and edit the file app_code\PagesJava\com\citrix\wi\pageutils\TwoFactorAuth.java

Find the following method:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
  if (fullyQualified) {
    return token.getShortDomain() + "\\" + token.getShortUserName();
  } else {
    return token.getShortUserName();
  }
}
```

Replace it with the following:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
  return token.getUserIdentity();
}
```

177 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

178 Citrix Web Interface 5.X additional login page options

178.1 Citrix Web Interface 5.x additional login page options

This outlines how to further customise the Citrix login page. This is a supplement to the Citrix Web Interface 5.x Integration guides.

178.2 Removing the Single Channel Button

To remove the *refresh image*, delete the following text:

```
"<a class='leftDoor' href='javascript:onTuringButtonClick();'>" +
                                 "Refresh Image" +
                                 "</a>
```

178.3 Replacing the Single Channel Button with a Dual Channel Button

178.3.1 Replacing TURing image with a Dual Channel (SMS) request

Edit the file pinsafe_image.aspx

find the following line:

```
url.AppendFormat("{0}:{1}/{2}/SCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

Replace with:

```
url.AppendFormat("{0}:{1}/{2}/DCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

178.3.2 Compatibility

This has been tested on Citrix Web Interface 5.1

178.3.3 Dual Channel Button modification

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
       href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
       onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
       onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
       tabIndex="<%=Constants.TAB_INDEX_FORM%>"
       id="dcmessage"
       name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

To change the Refresh Image button modify the file under auth\clientscripts\login.js.add and search for the line Refresh Image and change to the required text, such as Request Code or Request SMS.

```
"<span class='rightDoor'>Refresh Image</span>" +"
```

178.3.4 Dual Channel Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

178.4 Single Channel Button with an automated Single Channel Image

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to automatically show the Turing image without the need for pressing the button when the user enters into the required field.

178.4.1 Compatibility

This has been tested on Citrix Web Interface 5.1 using the Single Channel Turing Image

178.4.2 Single Channel Button to automated Single Channel Image modification

Edit the loginMainForm.inc file on the Citrix server. Locate the username field - look for the following:

```
<input type='text' name='<%=Constants.ID_USER%>' ...
```

insert the following line after that one:

```
onblur='onTuringButtonClick()'
```

This causes the turing image JavaScript function to be called when the user leaves the username field.

178.4.3 Automated Single Channel Image Testing

Test the image from the login page. Check the Swivel logs for the single channel image requests.

178.5 Turing, Dual channel and Display Index buttons

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to add additional buttons of Show Turing Image, Send Dual Channel Security String and Display Index number. See also Multiple Security Strings How To Guide

178.5.1 Compatibility

This has been tested on Citrix Web Interface 5.3

178.5.2 Required Files

The following files are required and should be used for installation: [1]

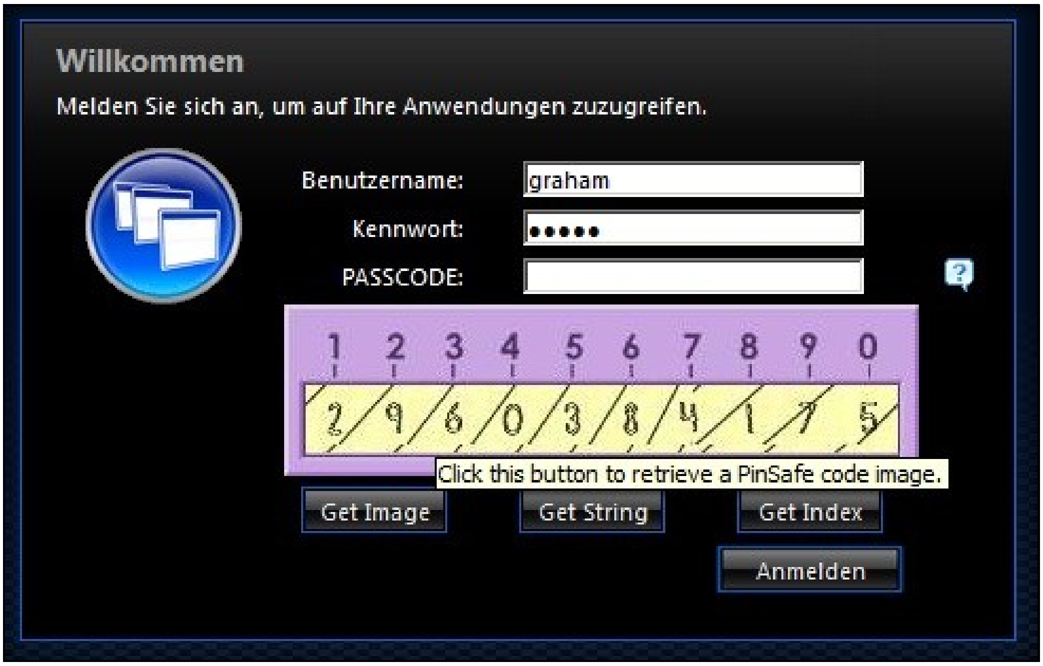
178.5.3 Installation Instructions

Follow the installation instructions for the relevant Citrix version.

178.5.4 Testing

Verify that three buttons are displayed and that they show the expected results when selected.

The following screen shots show the different buttons in use



Willkommen

Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

Benutzername: graham

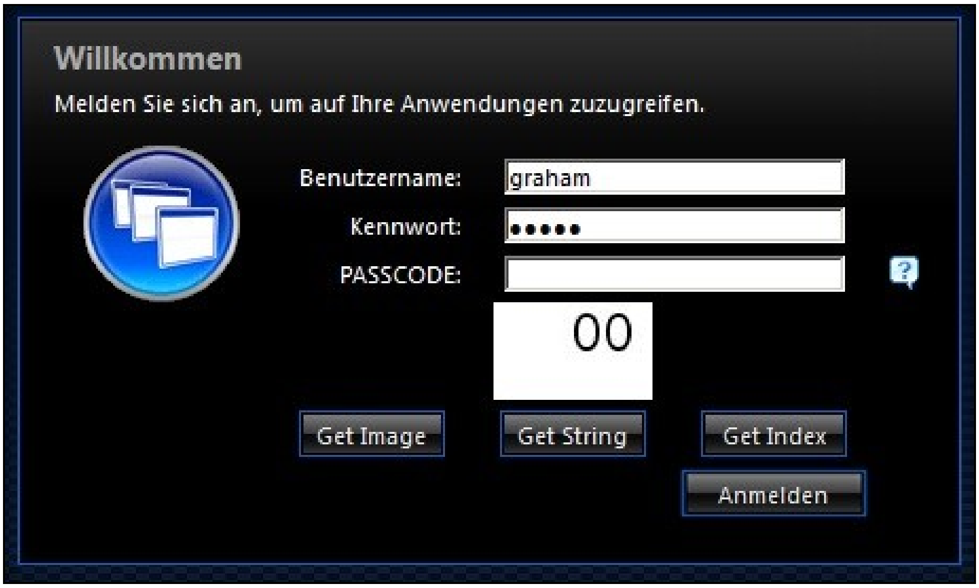
Kennwort: •••••

PASSCODE:

1	2	3	4	5	6	7	8	9	0
2	9	6	0	3	8	4	1	7	5

Click this button to retrieve a PinSafe code image.

Single Channel TURing Image request



Willkommen

Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

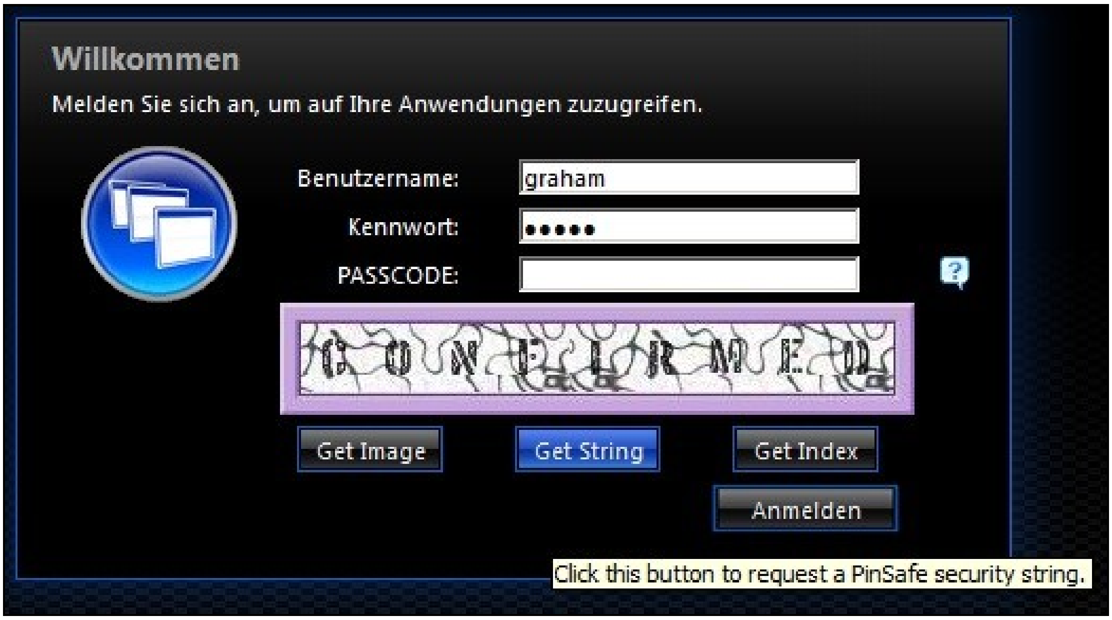
Benutzername: graham

Kennwort: •••••

PASSCODE:

00

Multiple Security String Message index number telling user which security string to use for authentication



Willkommen

Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

Benutzername: graham

Kennwort: ●●●●●

PASSCODE:

CONFIRMED

Click this button to request a PinSafe security string.

Securiy String On Demand Confirmation message of sending the user a Security String

179 Category:Web Interface

180 Category:XenApp

Citrix XenApp (formerly Citrix WinFrame Server, Citrix MetaFrame Server and Citrix Presentation Server) ships with Citrix Web Interface with which Swivel authentication can be used.

Please refer to the documentation on the listed links.

For XenApp 6.x use the Web Interface 5.4 guide