Table of Contents

Table of Contents

1 Juniper ChangePIN

2 Introduction

This document outlines how to integrate the Swivel ChangePIN with Juniper. See also RADIUS ChangePIN and ChangePIN How to Guide

3 Prerequisites

Swivel Server

Juniper SSL VPN version 6 or 7 OS.

Modified Changepin page for version 6

Modified Changepin page for version 7

4 Baseline

Juniper SA 2000 JunOS 6 or 7.

Swivel 3.8

5 Architecture

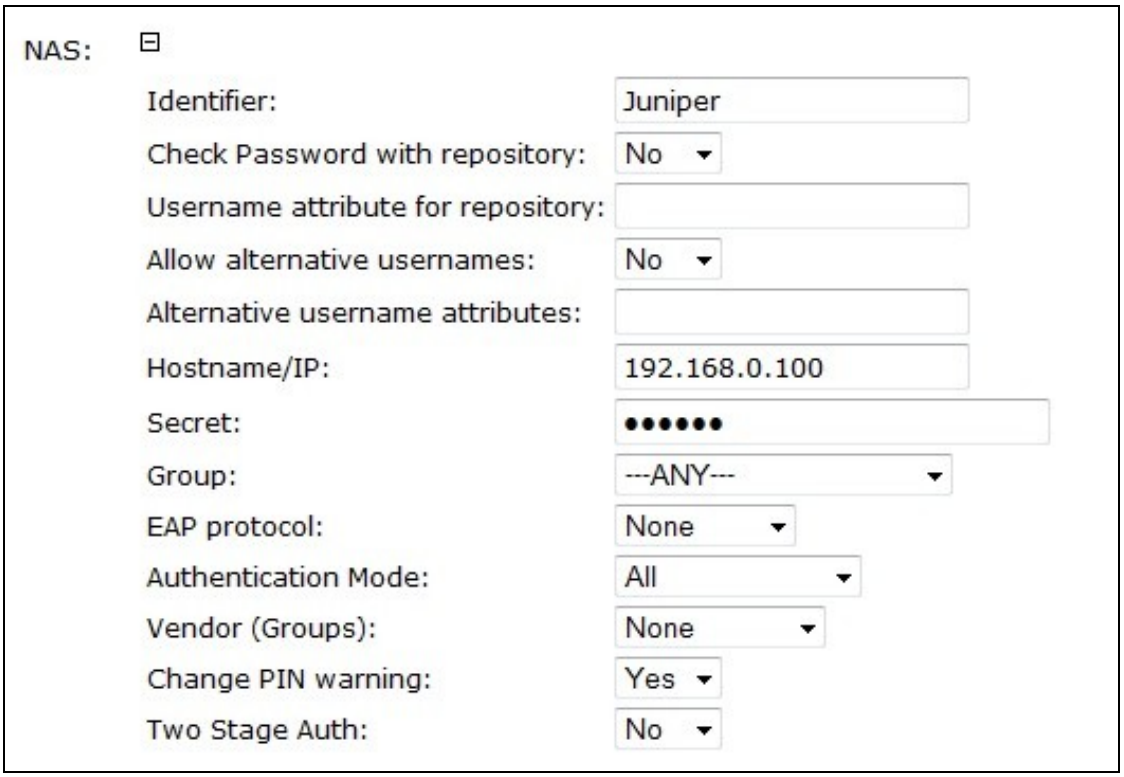
A user authenticates against the Juniper server, which passes the RADIUS authentication to the Swivel server. If the user is required to Change their PIN the Swivel server responds with a RADIUS Challenge, and the user is redirected to a change PIN page.

6 Installation

Configure the Swivel and Juniper so that they are fully working together, see Juniper SA 6.x Integration or Juniper SA 7.x Integration or Juniper SA 8.x Integration

6.1 Swivel Integration Configuration

On the Swivel Administration Console select RADIUS then NAS and edit the required Juniper NAS entry Change PIN Warning to Yes, then apply the settings.



6.2 Juniper ChangePIN Integration

Download the login page and add the modified ChangePIN page given above under prerequisites, rename and edit as appropriate, add to the zip file and upload to the Juniper server.

6.2.1 Juniper ChangePIN page options

Edit the following options:

```
var OTC_OPTION = "image"; // button, image, disable
```

image When the user tabs down from the username field, the TURing will automatically show, used for Single Channel access

button The login page will present a TURing button. Click the button to display the TURing, used for Single or Dual Channel access

disable The TURing image will not be shown, used for Dual Channel access.

TURingImage: Is the URL used to generate a TURing image. This should point to the internal IP address of the appliance

var TURingImage = "https://turing.swivelsecure.com/proxy/SCImage?username=";

6.2.2 Juniper RADIUS Custom rules

On the Juniper Administration console select the Swivel RADIUS server and create a Custom RADIUS rule with the following settings:

Name: ChangePIN

Response Packet Type: Access Challenge

Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand Matches the expression

Value: changepin

Action: use the appropriately modified page; *Show Next Token page* or *show New Pin Page*

	Name	Response Packet Type	Attribute criteria
	ChangePIN	**Access Challenge**	(Reply-Message matches the expression "change

6.3 Additional Installation Options

6.3.1 Combining Swivel and RSA RADIUS changePIN

Where Swivel is acting as a proxy RADIUS server for RSA authentication, Swivel can proxy the RADIUS request.

Configure the Swivel RADIUS proxy so that it will authenticate RSA users, see RADIUS Proxy How to guide.

On the Juniper edit the Swivel RADIUS authentication setting to add an additional custom rule with the following settings:

Name: RSAChangePIN

Response Packet Type: Access Challenge

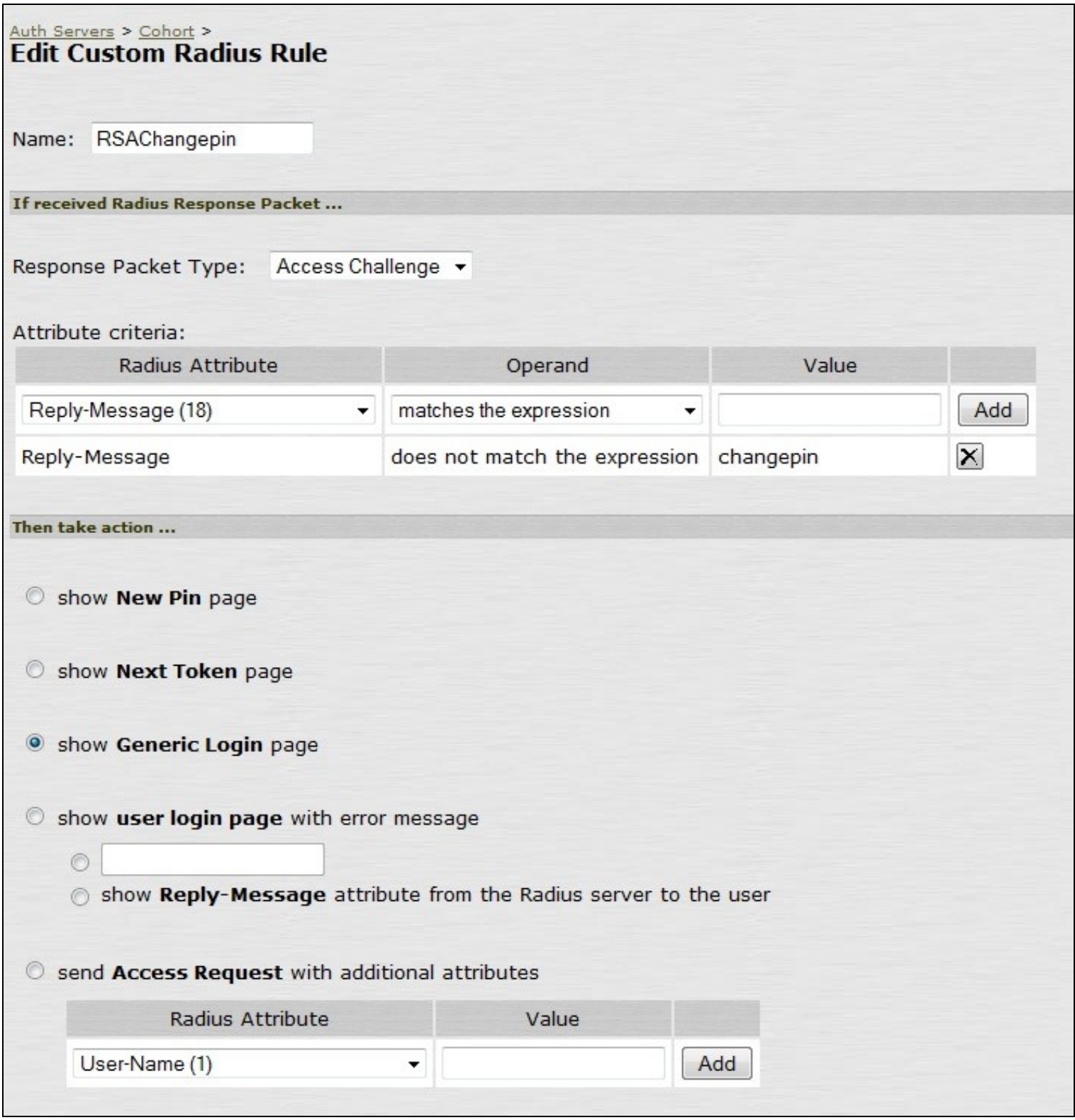
Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand does not match the expression

Value: changepin

Action: show Generic Login page

Apply the settings



Note: The Juniper displays the Generic login page as *show **Defender** page*

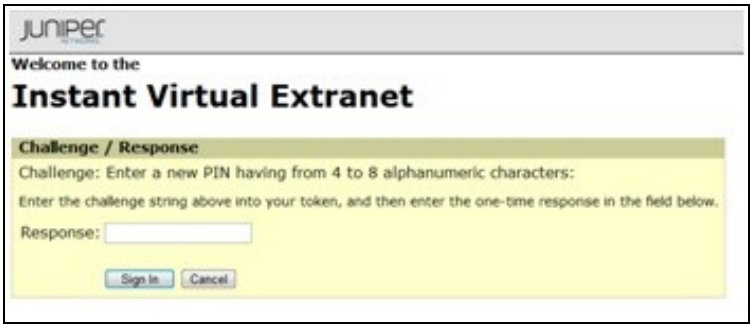
	Name	Response Packet Type	Attribute criteria
☐	ChangePIN	**Access Challenge**	(Reply-Message matches the expression "change
☐	RSAChangepin	**Access Challenge**	(Reply-Message does not match the expression "

7 Verifying the Installation

Login as a Swivel user.

Set the user to be required to change their PIN, the user should be redirected to the ChangePIN page. The user will be required to enter their old OTC, and a new OTC based on what they want their PIN to be. This OTC could be from the TURing, SMS message or mobile app. Remember to never enter the Swivel PIN.

Where RSA authentication is being used, require the user to change their PIN, and they should be redirected to a RSA Change PIN page. The the first time a user accesses the system with a new token the user will be required to enter a new PIN. If the user wanted a PIN of 1234 the would enter 1234 in the box.



The RSA server then send a challenge asking for the PIN to be re-entered to confirm the user has not miss-typed it. The user would again enter 1234.

Once the user has successfully changed their PIN the RSA server asks them to login again with their new PIN plus token code. The user would enter 1234XXXXXX where XXXXXX is the code displayed on the token.

If the RSA server sees the token go out of sync it will ask the user to enter their next token code. The user would now enter XXXXXX where XXXXXX is the next code displayed on the token after the code the user used to authenticate. They do not type their PIN at this stage.

8 Uninstalling the Swivel Integration

Remove the modified login pages and RADIUS customisation.

9 Troubleshooting

Check the Swivel logs for authentication, proxy and ChangePIN requests.

10 Known Issues and Limitations

Where Swivel and RSA change PIN is being used and the user is a Swivel and a RSA user, and dual channel authentication is being used, then the Change PIN will fail for RSA users. for single channel users not using dual channel authentication, the proxy server can be used to detect the presence of a single channel session being started.

11 Additional Information

12 Juniper SA 5.x Integration

12.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 5.x Basic Integration Guide

Juniper SA 5.x files for modified login page

Juniper SA 5.x Enhanced Integration Guide

13 Juniper SA 6.x Integration

13.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 6.x Integration Guide

13.2 Troubleshooting

INFO RADIUS: <69> Access-Request(1) LEN=147 192.168.1.1:13145 Access-Request by ADMIN\graham Failed: AccessRejectException: AGENT_ERROR_NO_USER_DATA

INFO 192.168.1.1 Juniper:Login failed for user: ADMIN\graham, error: No data for the user was found.

Authentication has failed as the User Ream has been configured with <USER> instead of <USERNAME>

14 Juniper SA 7.x Integration

15 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 8.x integration guide see Juniper SA 8.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

16 Prerequisites

Juniper 7.x

Swivel 3.x

Modified login pages can be downloaded from here: PINsafe modified pages also requires sample pages from Juniper appliance.

It is possible to access Juniper SSL VPN from mobile devices such as iPhone, Blackberry, Windows Mobile and Andriod devices.

To support this, additional pages needs to be modified to support Swivel.

Mobile login pages can be downloaded from here: Swivel Mobile login pages, and should be included if the Single channel images are required on mobile devices.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. A valid certificate is required on the Swivel server.

17 Baseline

Juniper 7.2

Swivel 3.7

18 Architecture

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

19 Installation

19.1 Swivel Configuration

19.1.1 Configuring the RADIUS server

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

19.1.2 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.

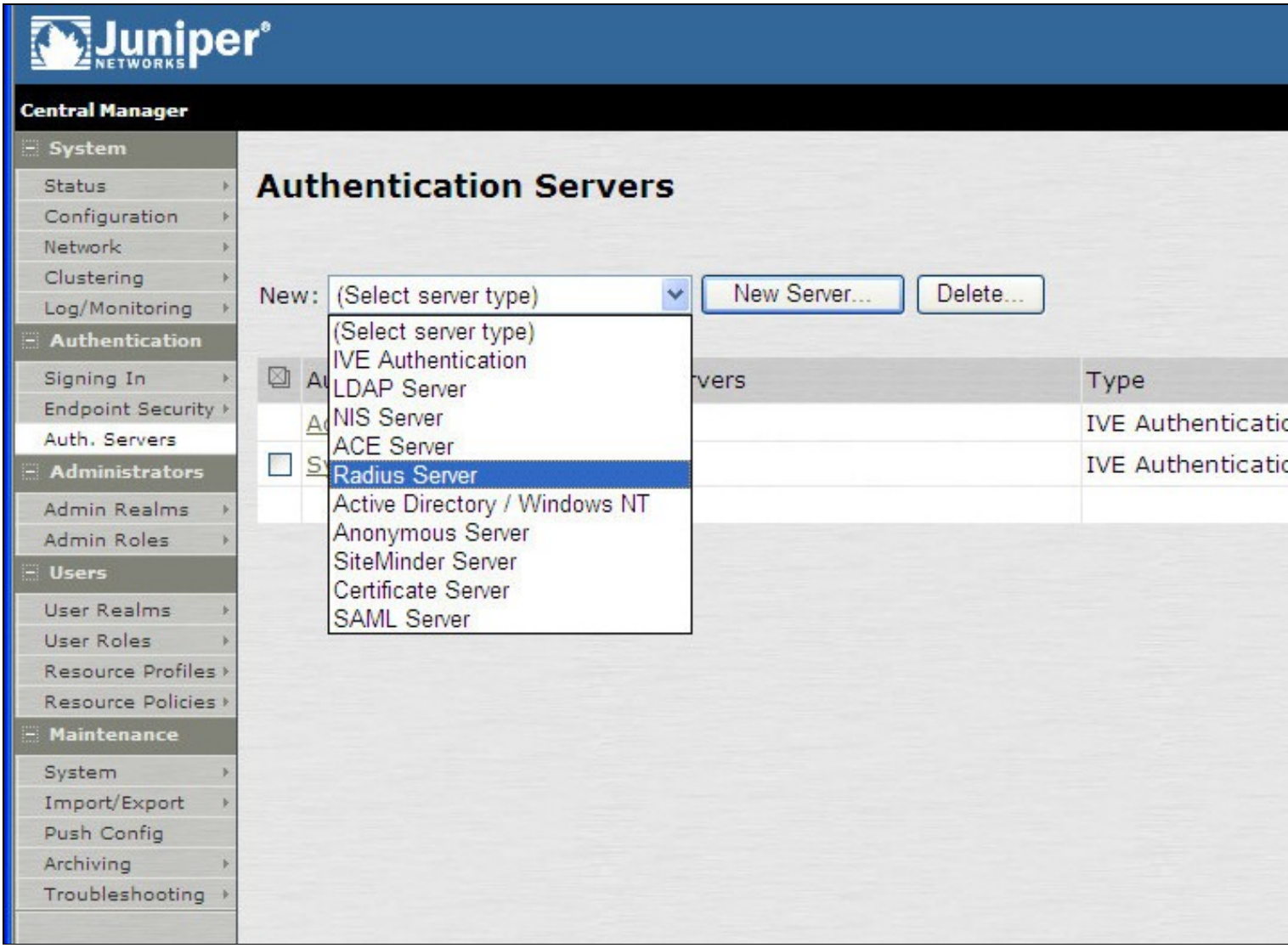
19.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

19.3 Juniper Integration

19.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.



The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

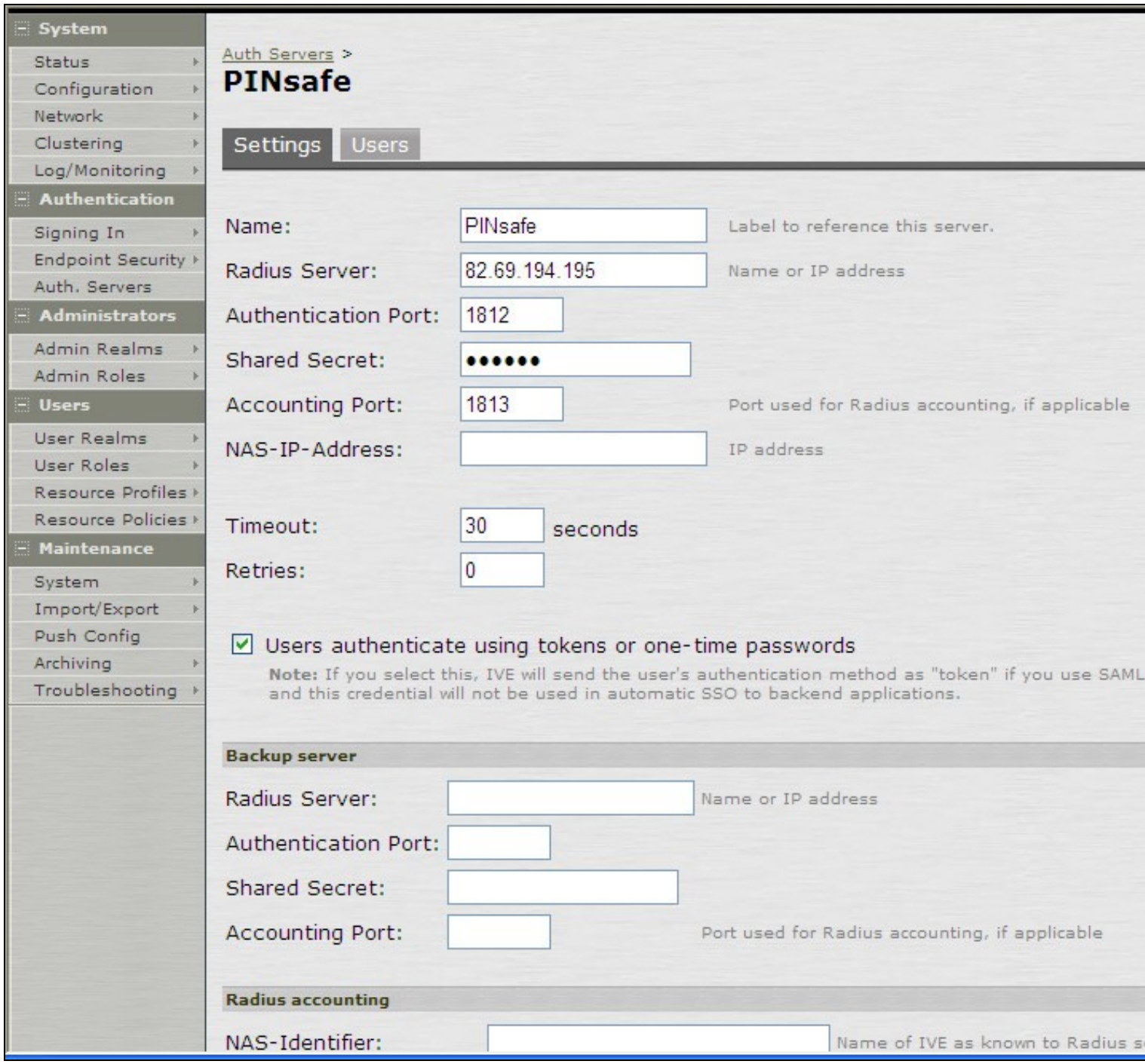
Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

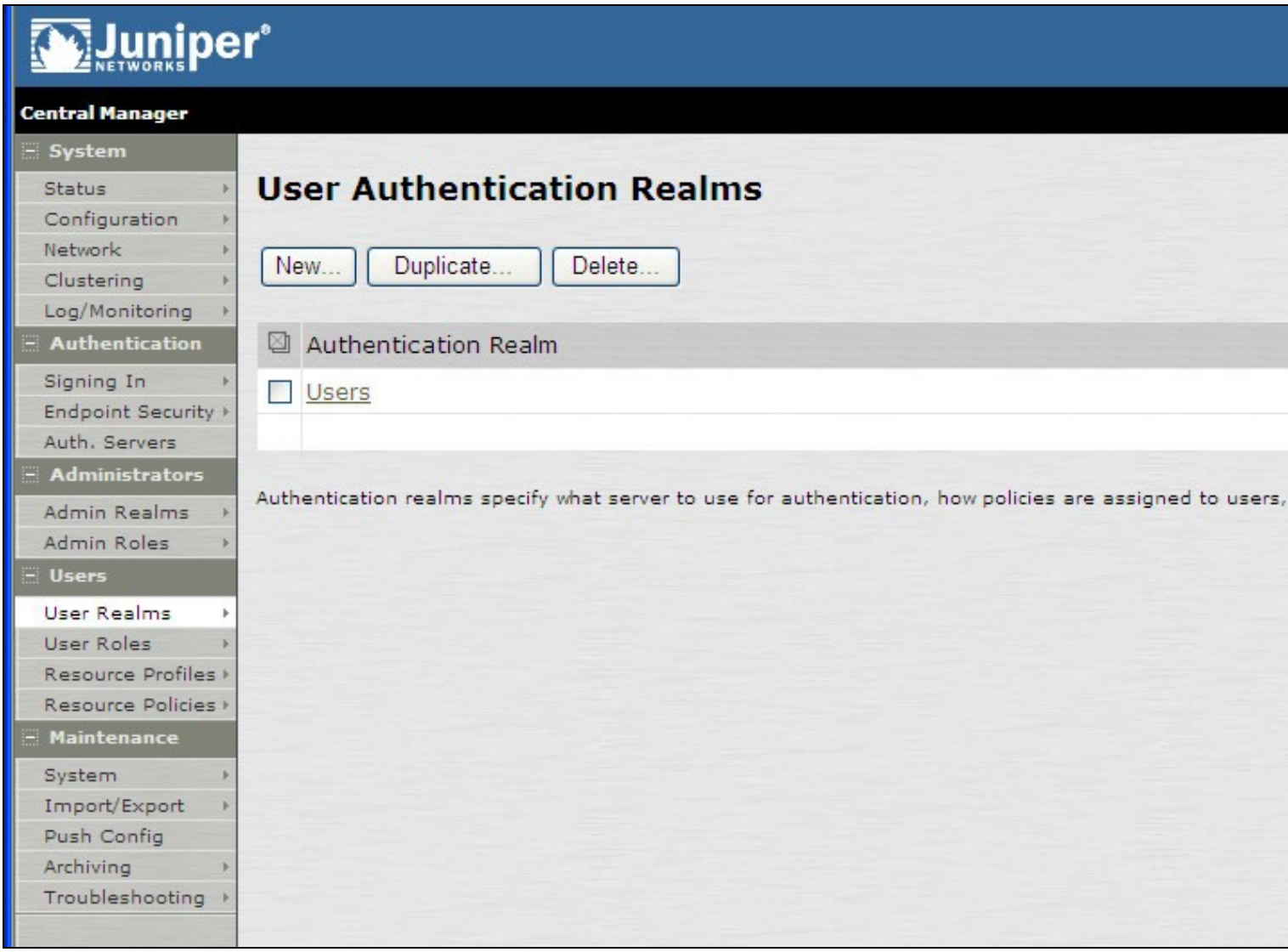
Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.



19.3.2 Authentication Realm Configuration

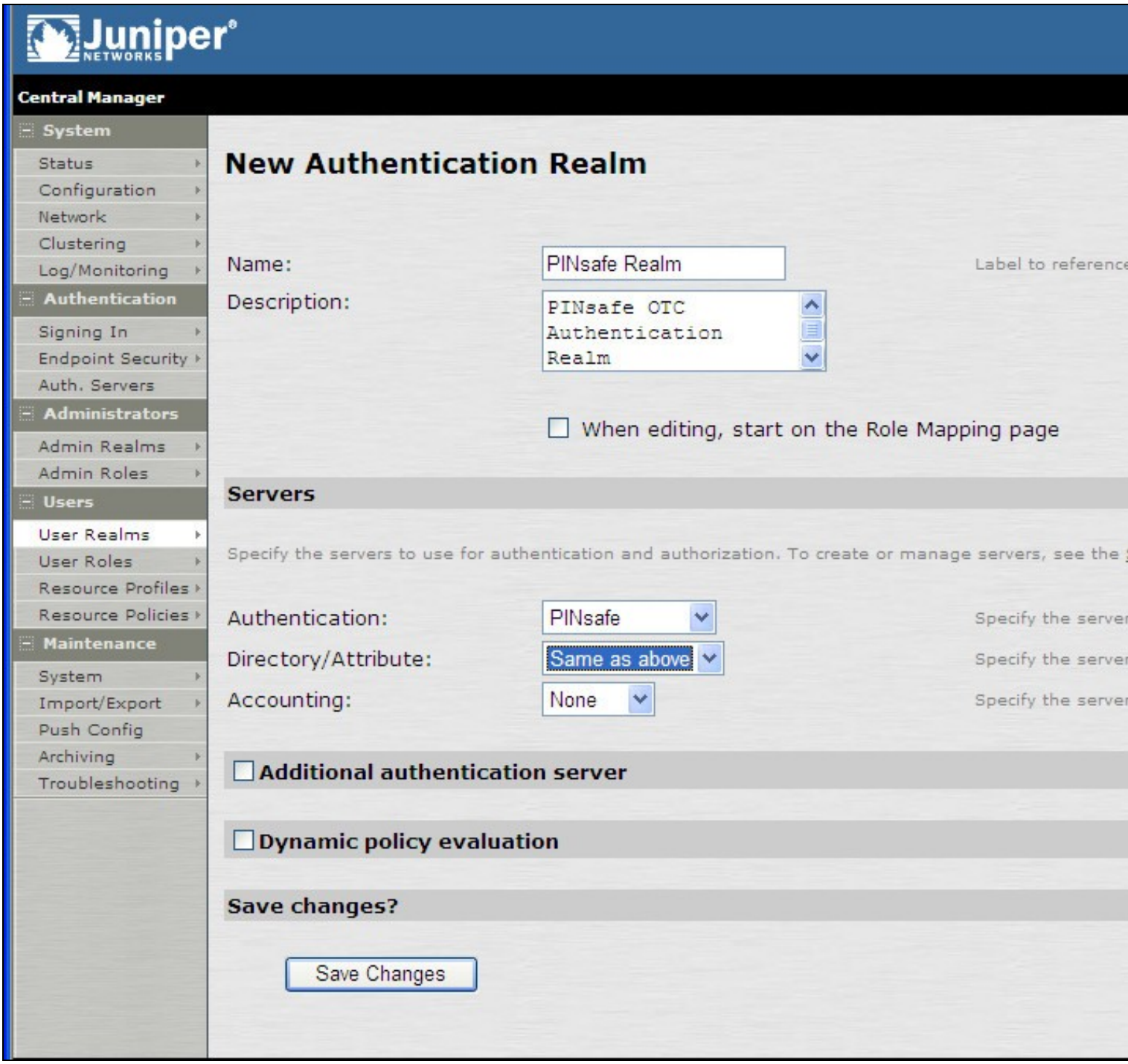
Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.



19.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

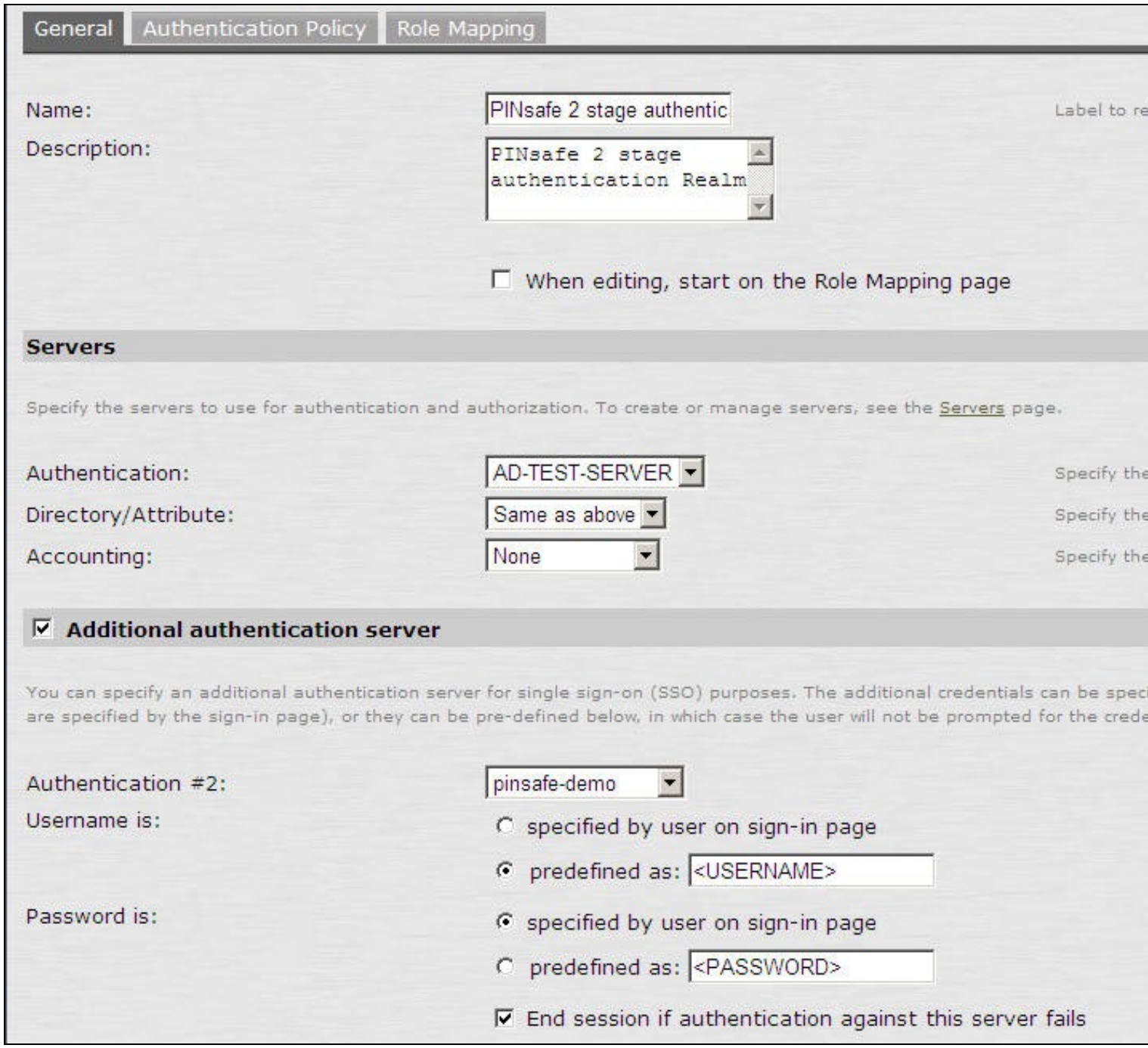
To configure Swivel as the server select the Swivel server as the first listed Authentication Server.



19.3.4 Swivel as the Secondary Authentication Server

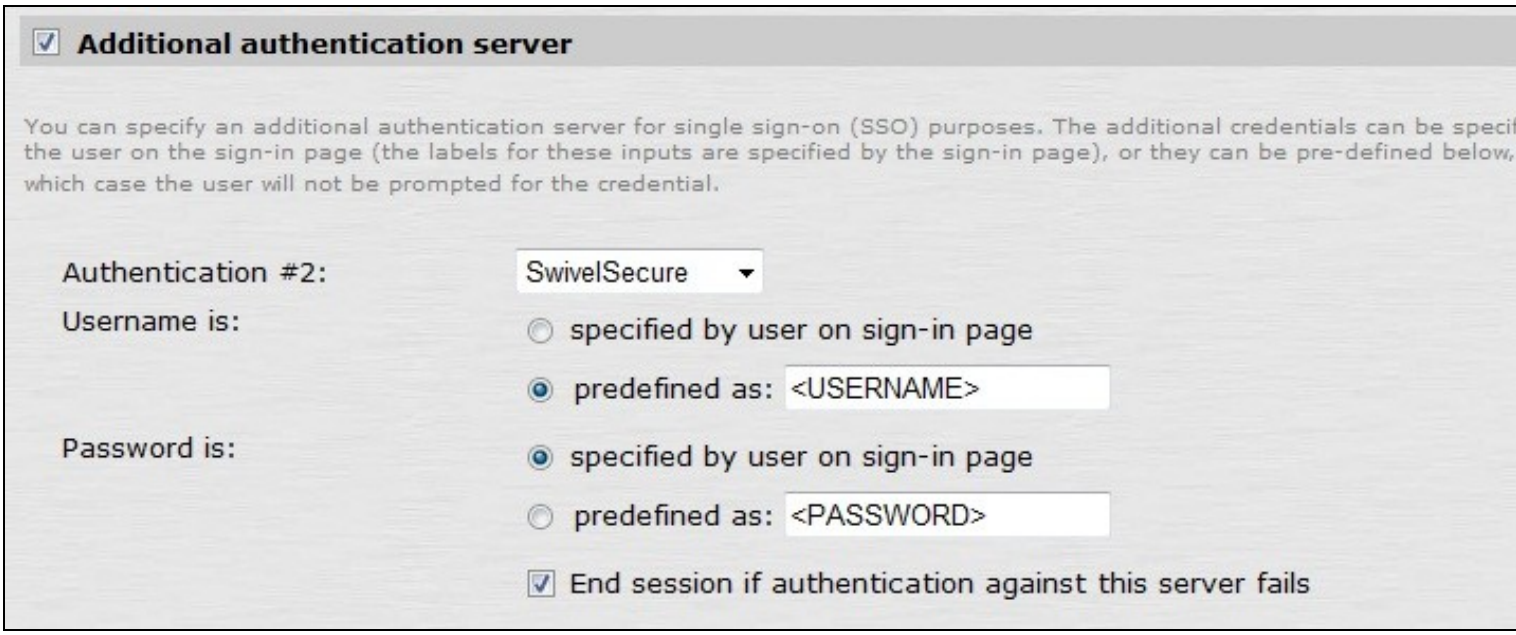
Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box **Additional authentication server**

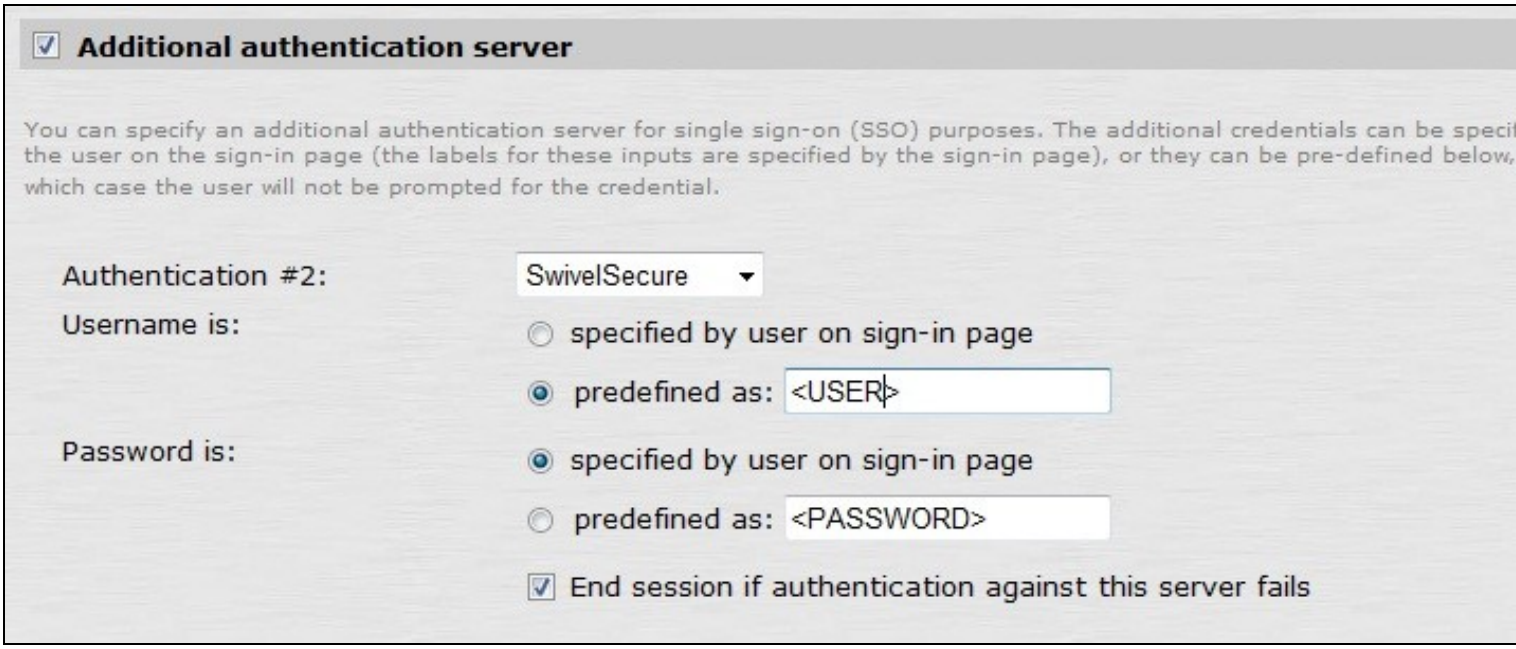


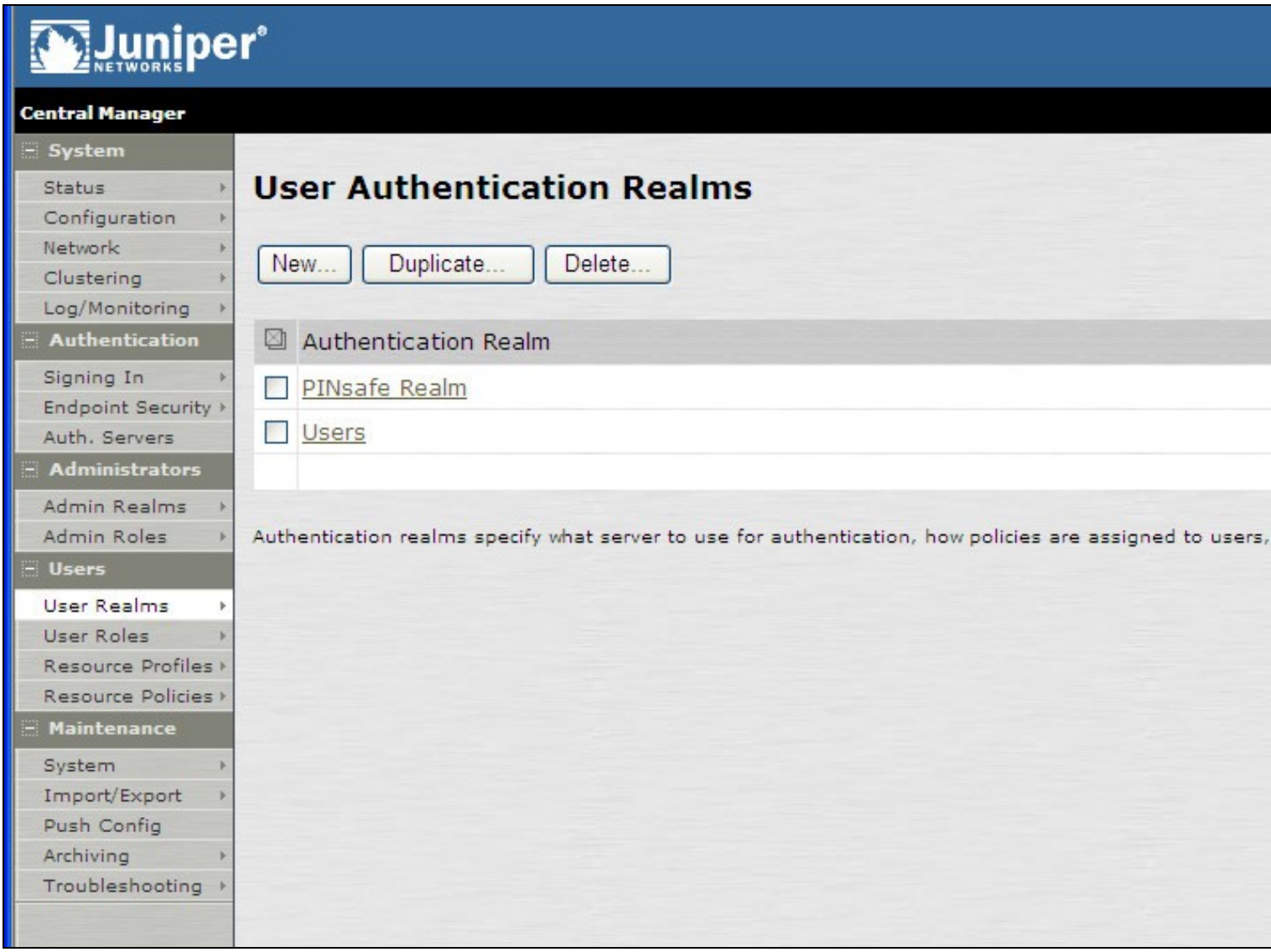
NOTE: when <USERNAME> is used then just the Username is sent to the Juniper, without a Domain prefix/suffix. When <USER> is used then the Domain Name may be added in the authentication request to the Swivel instance in the form domain\username.

USERNAME


Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USERNAME>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails

USER

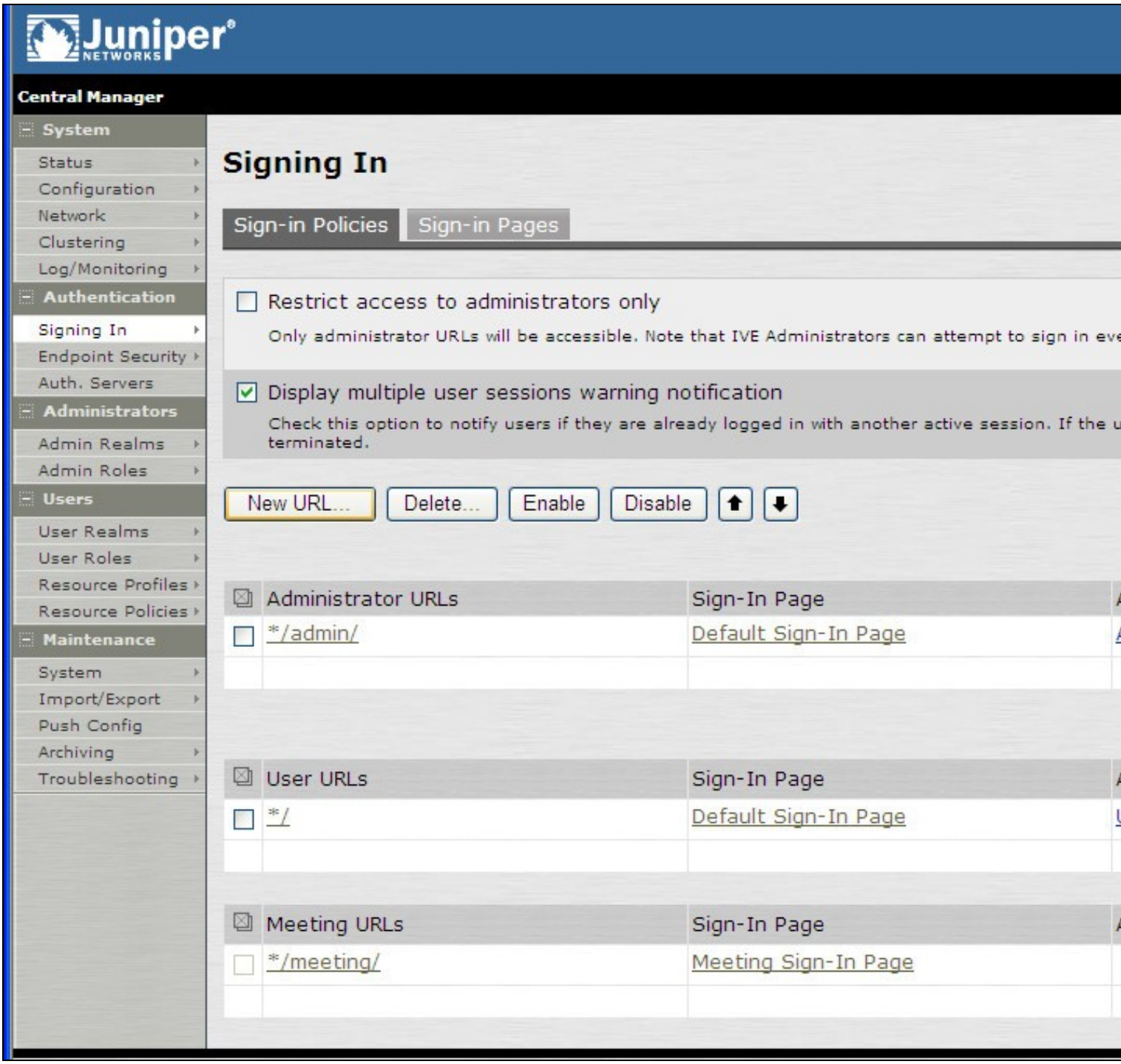

Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USER>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails



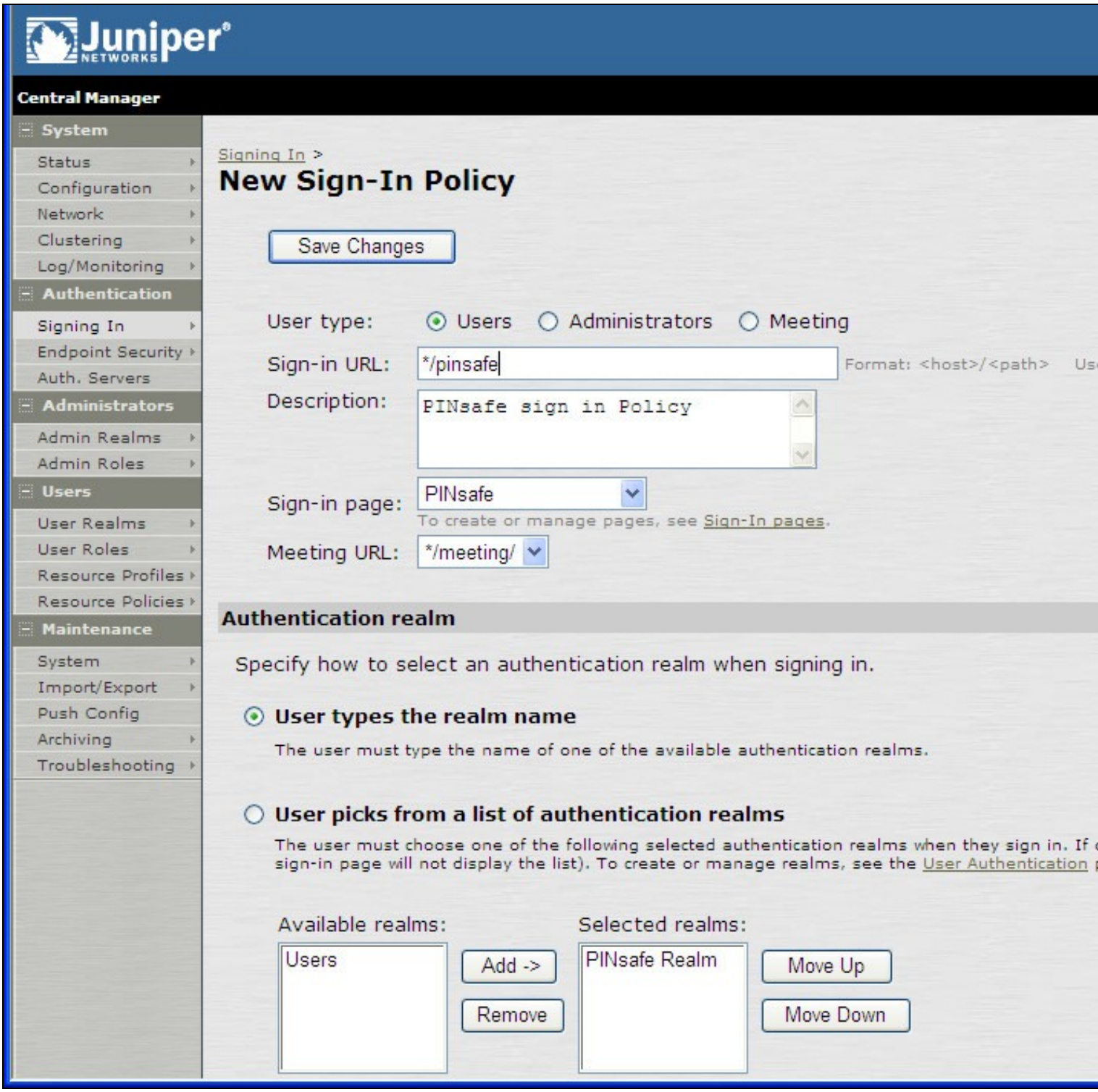
19.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.



Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.



When complete the new Swivel policy should be listed.


Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
Restrict access to administrators only
Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve
Display multiple user sessions warning notification
Check this option to notify users if they are already logged in with another active session. If the u
terminated.
New URL...
Delete...
Enable
Disable
Administrator URLs
Sign-In Page
*/admin/
Default Sign-In Page
User URLs
Sign-In Page
*/
Default Sign-In Page
*/pinsafe/
PINsafe
Meeting URLs
Sign-In Page
*/meeting/
Meeting Sign-In Page

20 Additional Installation Options

Swivel can provide additional authentication options including:

Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

20.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

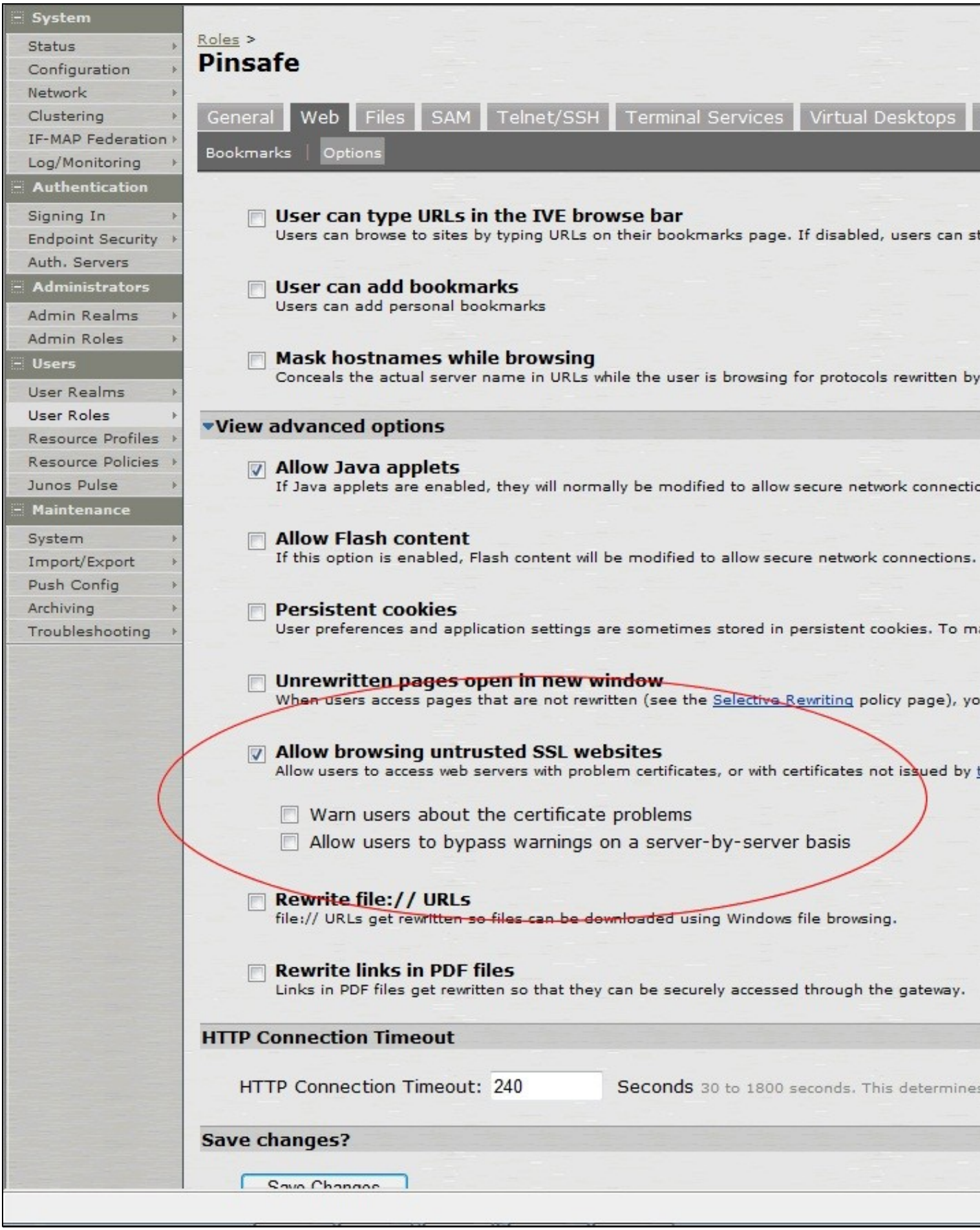
Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

20.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.


System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
Pinsafe
General
Web
Files
SAM
Telnet/SSH
Terminal Services
Virtual Desktops
Bookmarks
Options
User can type URLs in the IVE browse bar
Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can st
User can add bookmarks
Users can add personal bookmarks
Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
View advanced options
Allow Java applets
If Java applets are enabled, they will normally be modified to allow secure network connectio
Allow Flash content
If this option is enabled, Flash content will be modified to allow secure network connections.
Persistent cookies
User preferences and application settings are sometimes stored in persistent cookies. To ma
Unrewritten pages open in new window
When users access pages that are not rewritten (see the Selective Rewriting policy page), yo
Allow browsing untrusted SSL websites
Allow users to access web servers with problem certificates, or with certificates not issued by t
Warn users about the certificate problems
Allow users to bypass warnings on a server-by-server basis
Rewrite file:// URLs
file:// URLs get rewritten so files can be downloaded using Windows file browsing.
Rewrite links in PDF files
Links in PDF files get rewritten so that they can be securely accessed through the gateway.
HTTP Connection Timeout
HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determines
Save changes?
Save Changes

20.1.2 Creating an ACL for the Virtual hostname role

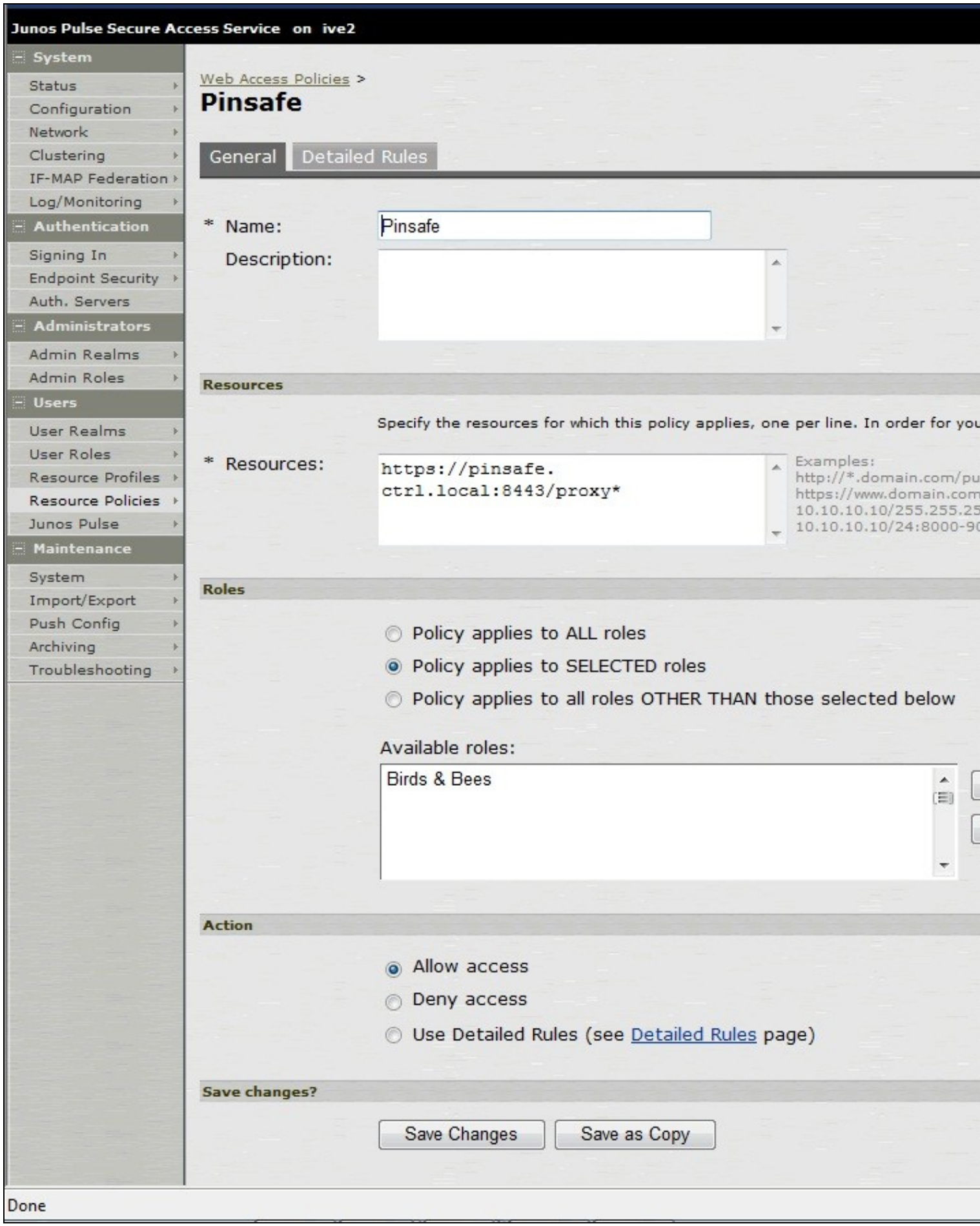
An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.


Junos Pulse Secure Access Service on ive2
System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Web Access Policies >
Pinsafe
General
Detailed Rules
* Name:
Pinsafe
Description:
Resources
Specify the resources for which this policy applies, one per line. In order for you
* Resources:
https://pinsafe.
ctrl.local:8443/proxy*
Examples:
http://*.domain.com/pu
https://www.domain.com
10.10.10.10/255.255.25
10.10.10.10/24:8000-90
Roles
Policy applies to ALL roles
Policy applies to SELECTED roles
Policy applies to all roles OTHER THAN those selected below
Available roles:
Birds & Bees
Action
Allow access
Deny access
Use Detailed Rules (see Detailed Rules page)
Save changes?
Save Changes
Save as Copy
Done

20.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New Page. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

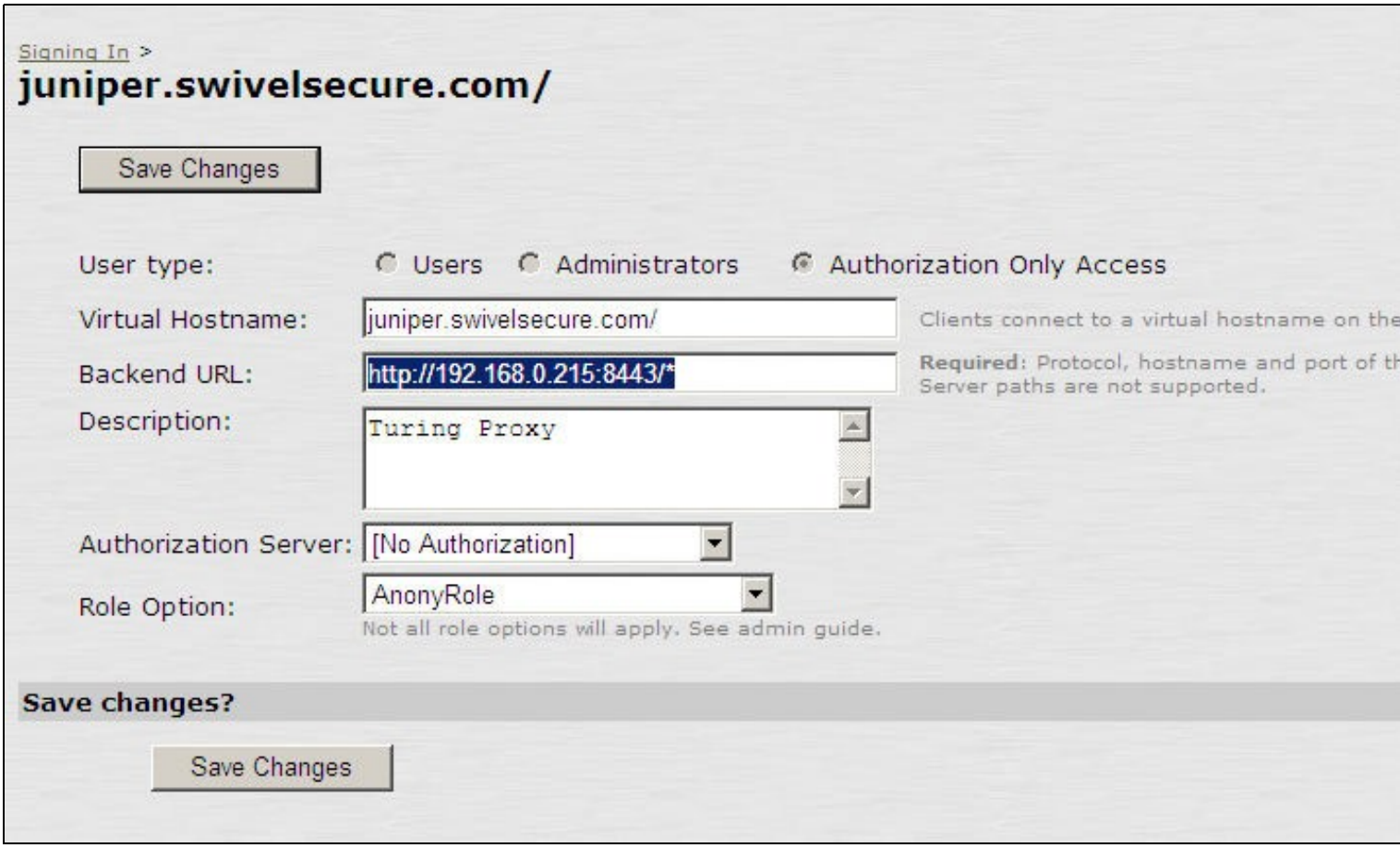
Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

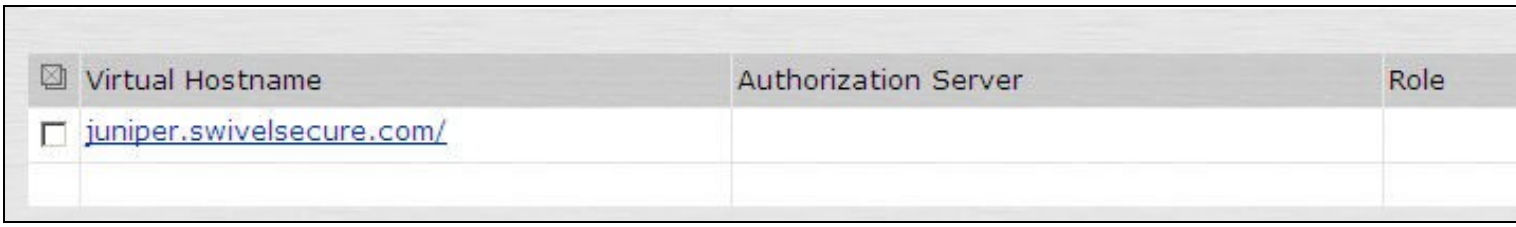
For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes





20.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

https://<turing.mycompany.com>/proxy/SCImage?username=test

Software Install

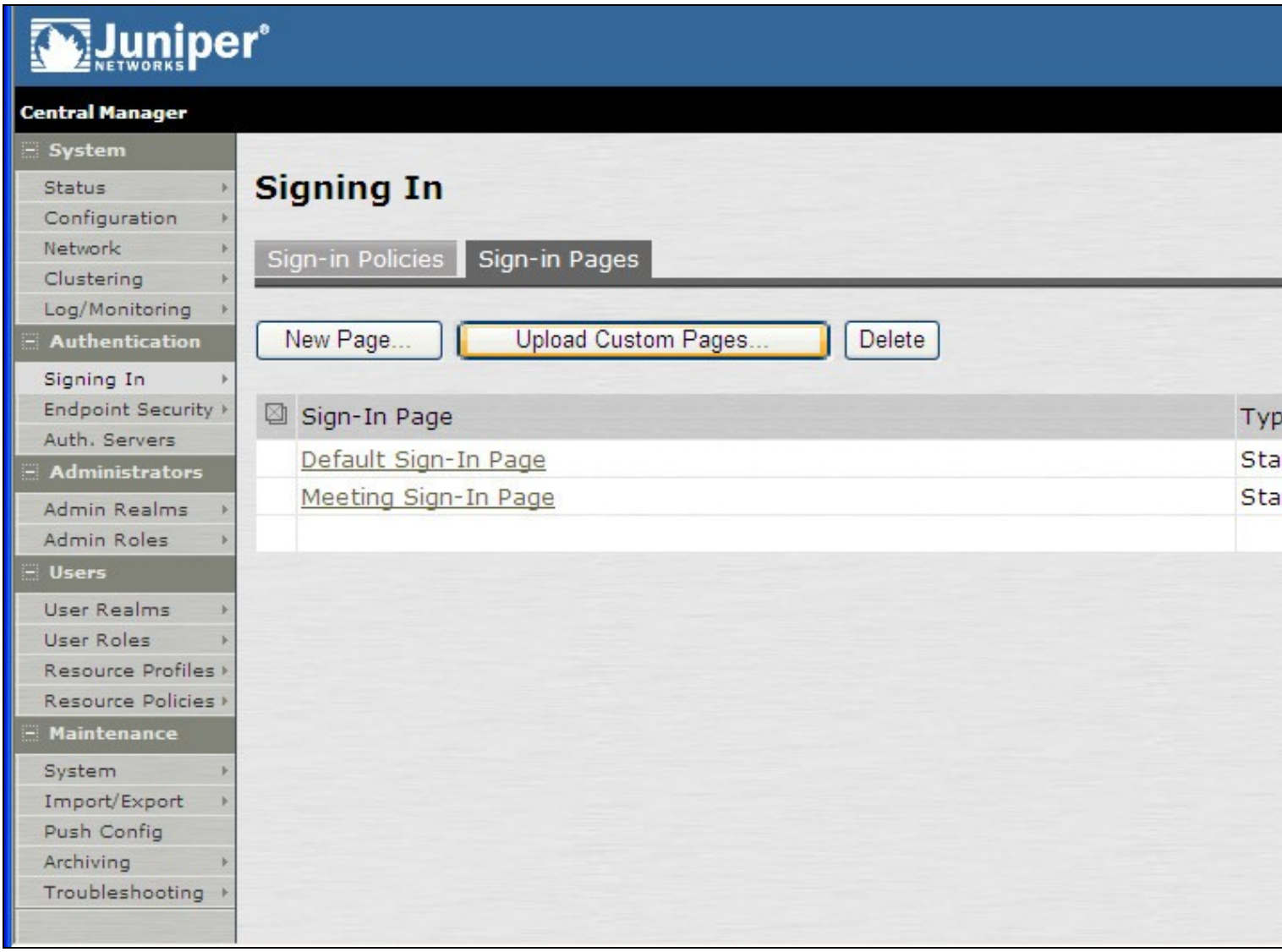
For a software only install see Software Only Installation

Then verify the external access using

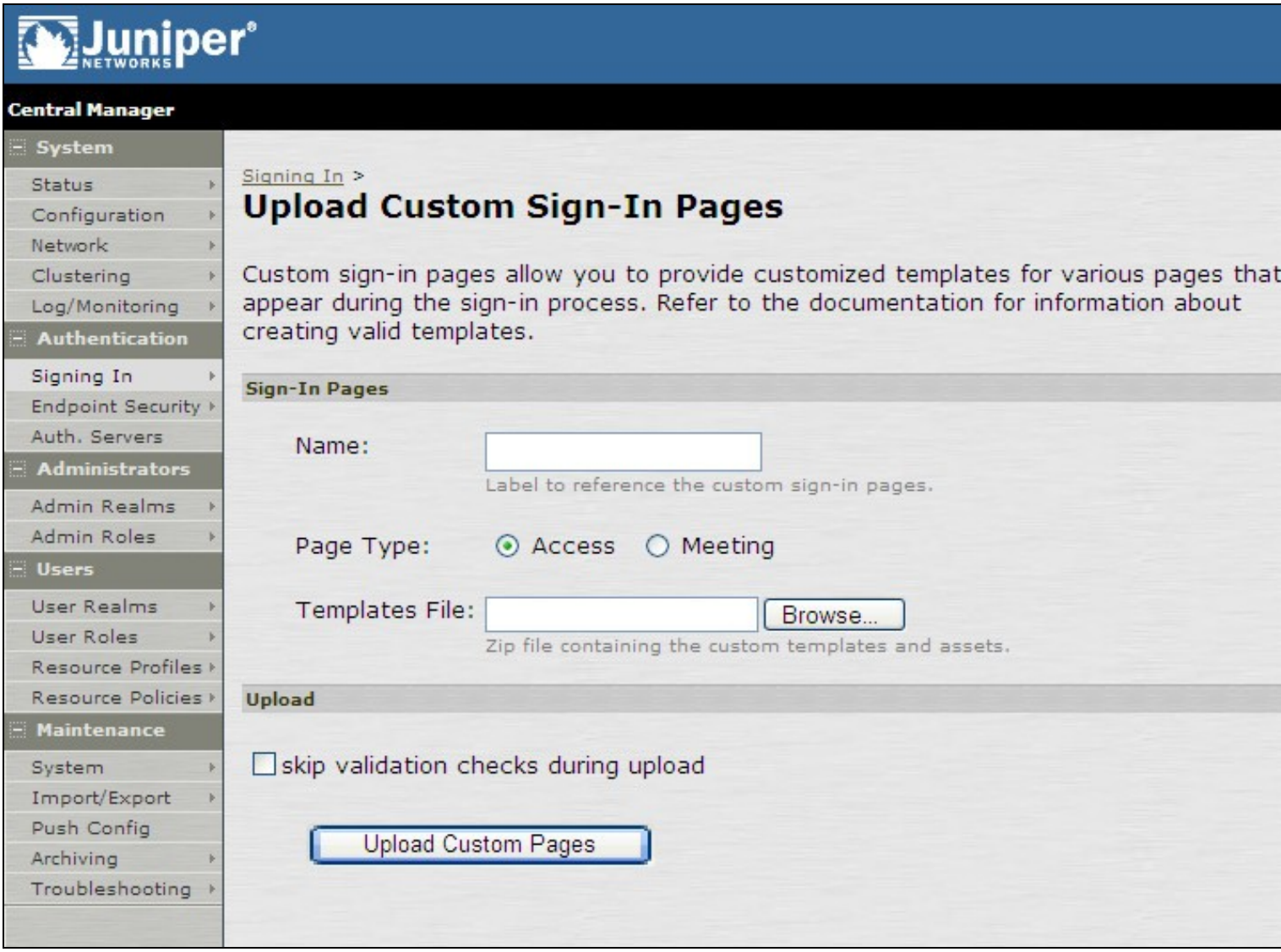
https://<turing.mycompany.com>/pinsafe/SCImage?username=test

20.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.



Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.



Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within **LoginPage.thtml** should be edited to suit your environment as the below modifications.

20.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/SCImage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/SCImage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/SCImage?username=";
```

Software install

```
http://hostname:8080/pinsafe/SCImage?username=";
```

20.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

20.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/DCMessage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/DCMessage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

20.2.4 Modifying the login button text

The login page button and link to *Get Another Image* may be modified.

To modify the login button text locate the text *value='Turing'* and replace the Turing with the required text.

To modify the *Get another image?* URL, locate the two instances of *Get another image?* and change the text as required.

20.2.5 Modifying the login for PINpad

The custom page for Pinpad, is available from here.

Follow the same instructions as above, but note the following:

- The zip file contains 3 additional images that need to go into the *imgs* folder of the Juniper custom login.
- **OTC_OPTION** needs to be set to **"pinpad"**, which it already is in the attached file.

- You need to set the value for *PinpadImage*, rather than *TURingImage* to match your own Swivel instance.

Example

```
var PinpadImage = "https://hostname:8443/pinsafe/SCImage?username=";
```

to

```
var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";
```

20.2.6 Modifying the Login pages for Mobile Devices

Download the mobile modified pages that can be uploaded with any other modified pages to add Swivel authentication to the login.

Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above.

var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

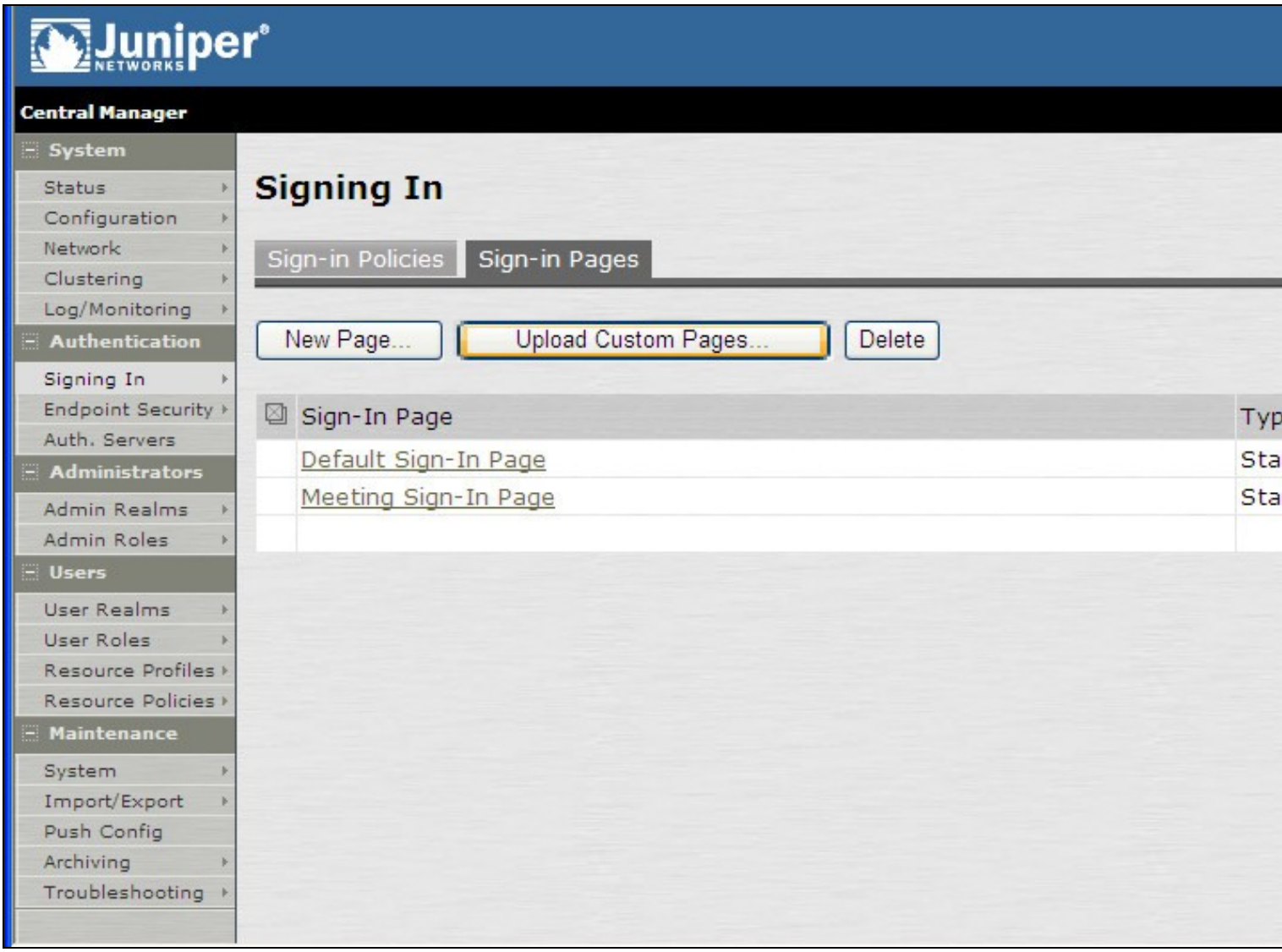
20.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

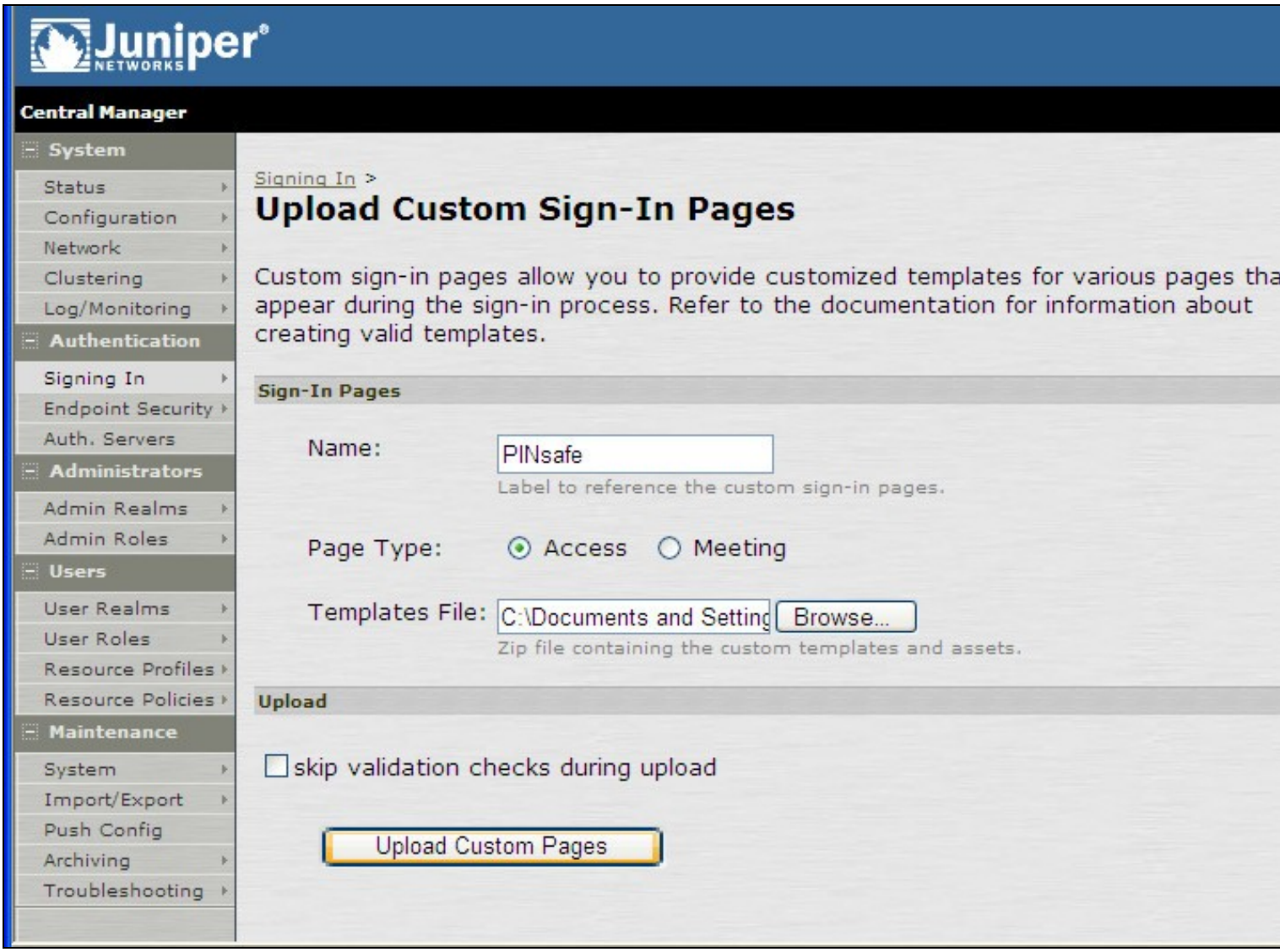
Juniper Network Connect with TURing

20.2.8 Uploading the Modified Page

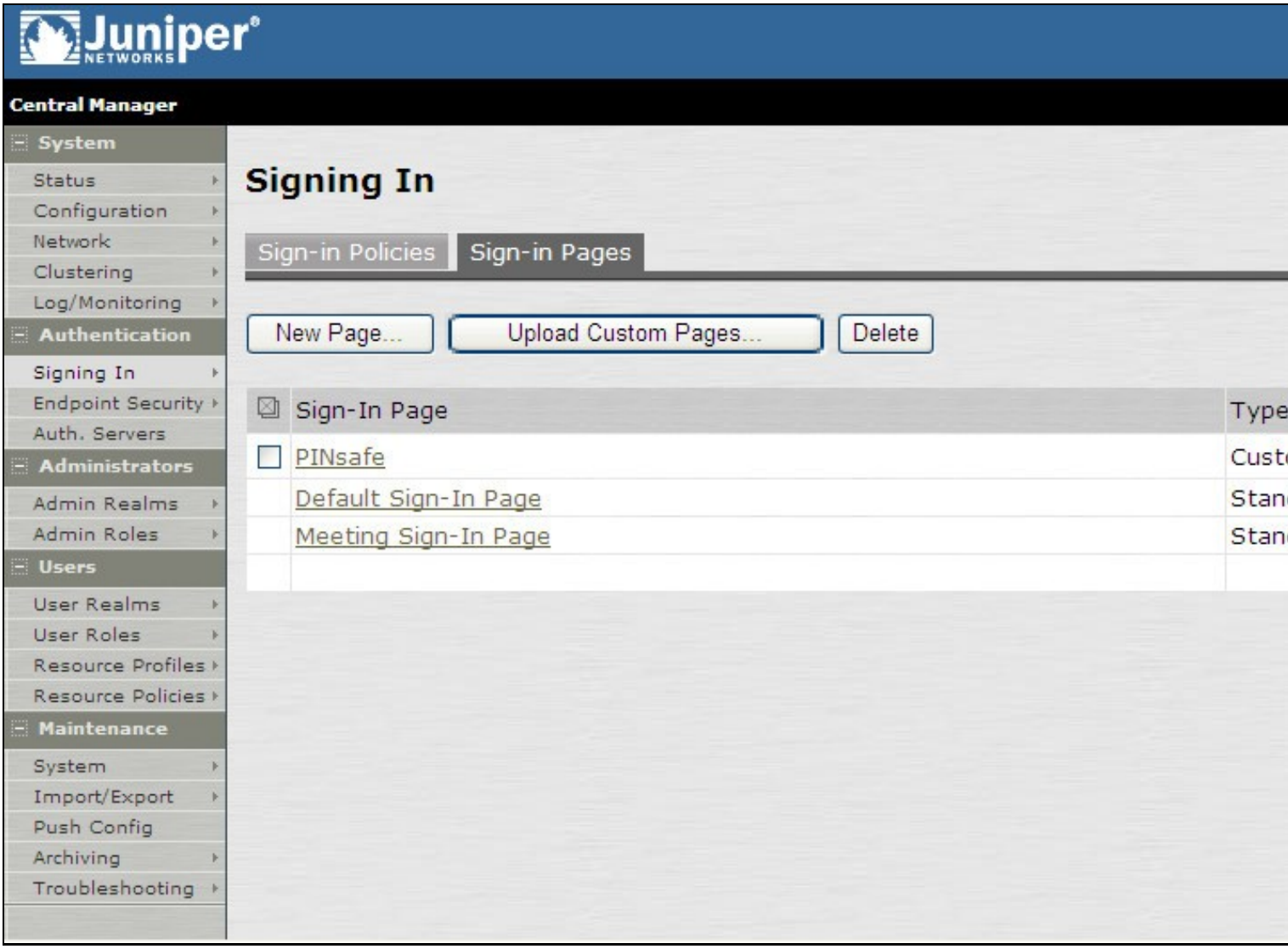
Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.



Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.



The new signing in page should be listed.

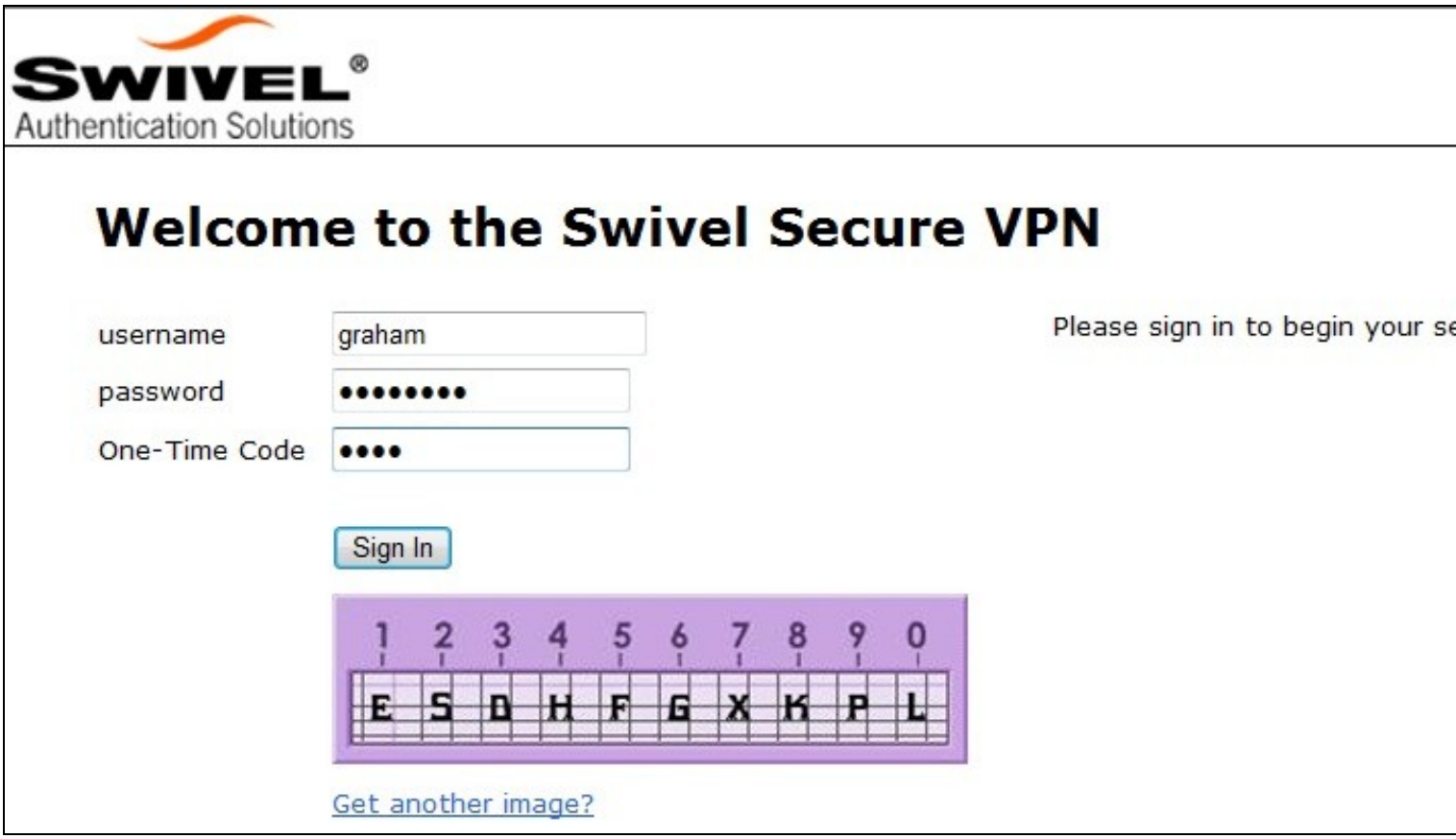

Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
New Page...
Upload Custom Pages...
Delete
Sign-In Page
Type
PINsafe
Default Sign-In Page
Meeting Sign-In Page

21 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

Dual Channel Authentication

Single Channel Authentication



22 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

23 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Internal Certificate Authorities

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username. When USERNAME is used then just the username is sent to the Juniper.

24 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

24.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

```
<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si
```

A modified login page is available here: iPad modified login page

24.2 Junos Pulse usability issue

Junos Pulse for SSL VPN: How to resolve usability issue (very small fonts and field size) with the VPN login screen on iPhone running iOS 7

24.3 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

25 Additional Information

Custom sign-in pages for Pinpad can be found here.

26 Juniper SA 8.x Integration

27 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 7.x integration guide see Juniper SA 7.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

28 Prerequisites

Juniper 8.x

Swivel 3.x

Modified login pages can be downloaded below. Note that you don't need the included image files unless you are using Pinpad.

It is possible to access Juniper SSL VPN from all mobile devices, however additional pages need to be modified to support Swivel integration.

Mobile login pages can be downloaded below, and should be included if the Single channel images are required on mobile devices. NOTE: These have not been tested on version 8.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. Since the Juniper will be supporting at least two different host names, the SSL certificate on the Juniper must either be a wildcard certificate, or must include SANs (Subject Alternative Names) for all host names used.

29 File Downloads

PINsafe modified pages

Swivel Mobile login pages

Modified pages for both PC and tablets. These files have been tested internally only, and do not currently work with PINpad on tablets. The main advantage is that you only need edit one file - swivel-header.thtml - to set the image URL for all devices.

30 Baseline

Juniper 8

Swivel 3.9.7

31 Architecture

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

32 Installation

32.1 Swivel Configuration

32.1.1 Configuring the RADIUS server

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

32.1.2 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.

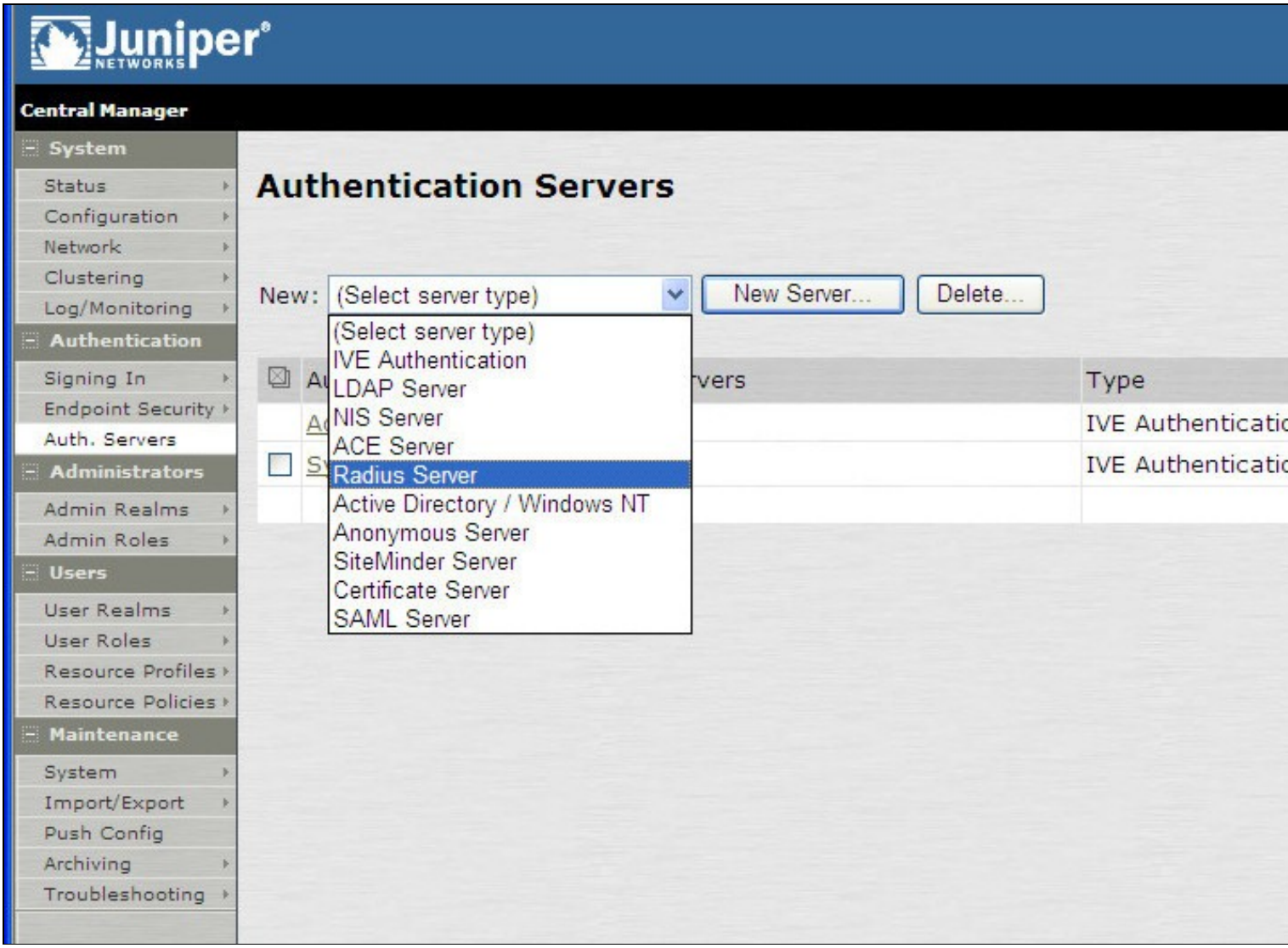
32.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

32.3 Juniper Integration

32.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.



The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

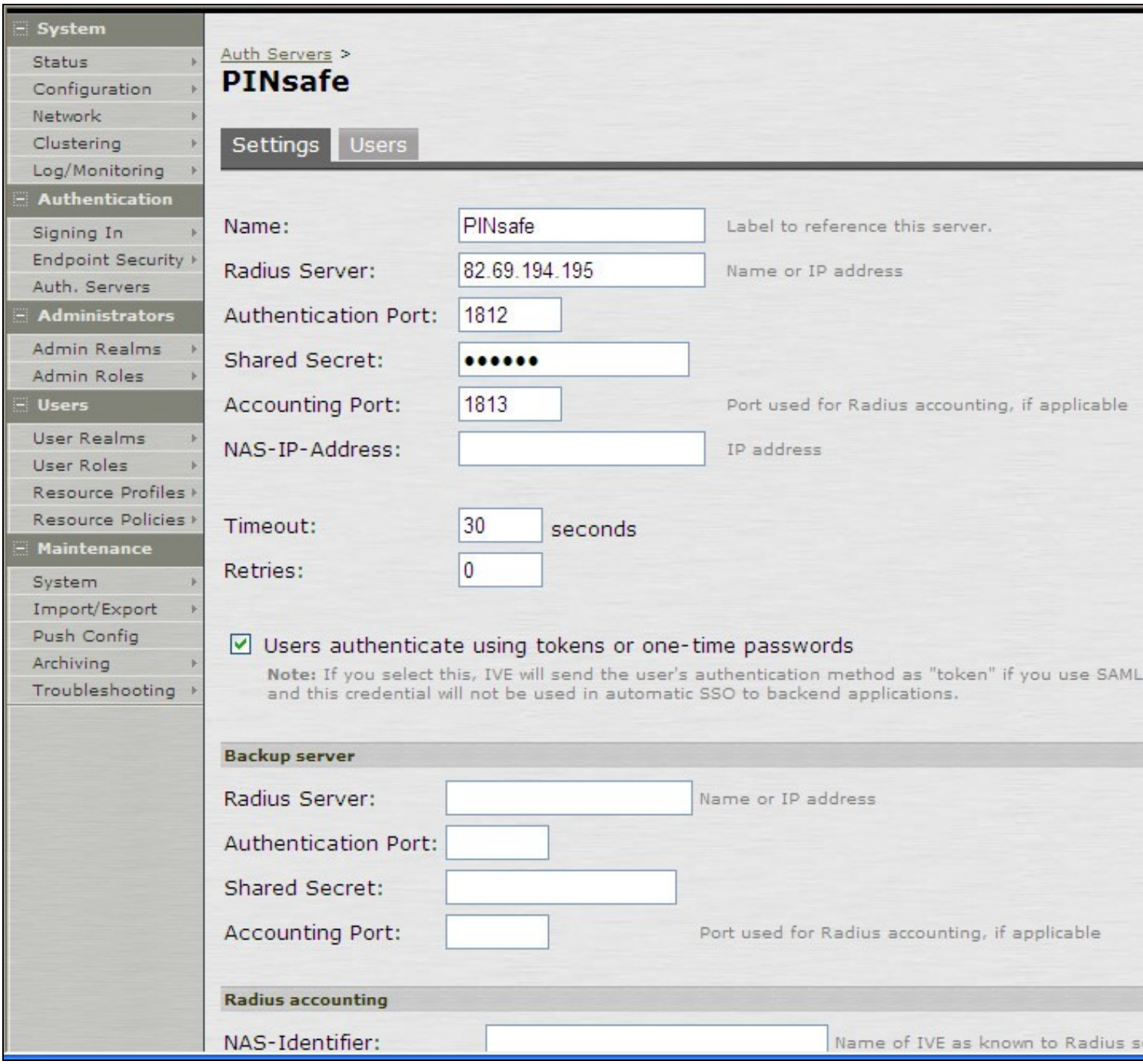
Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

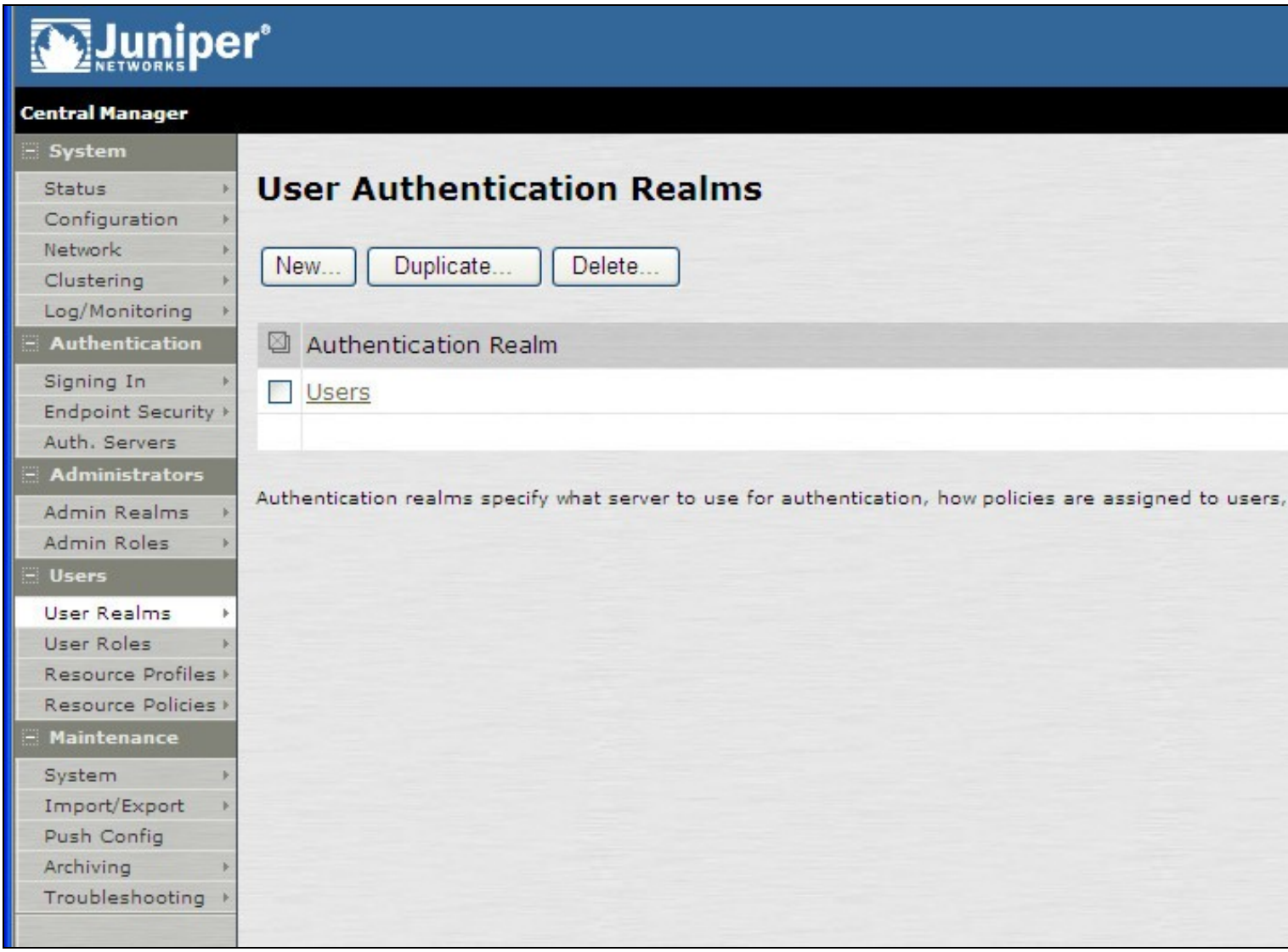
Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.



32.3.2 Authentication Realm Configuration

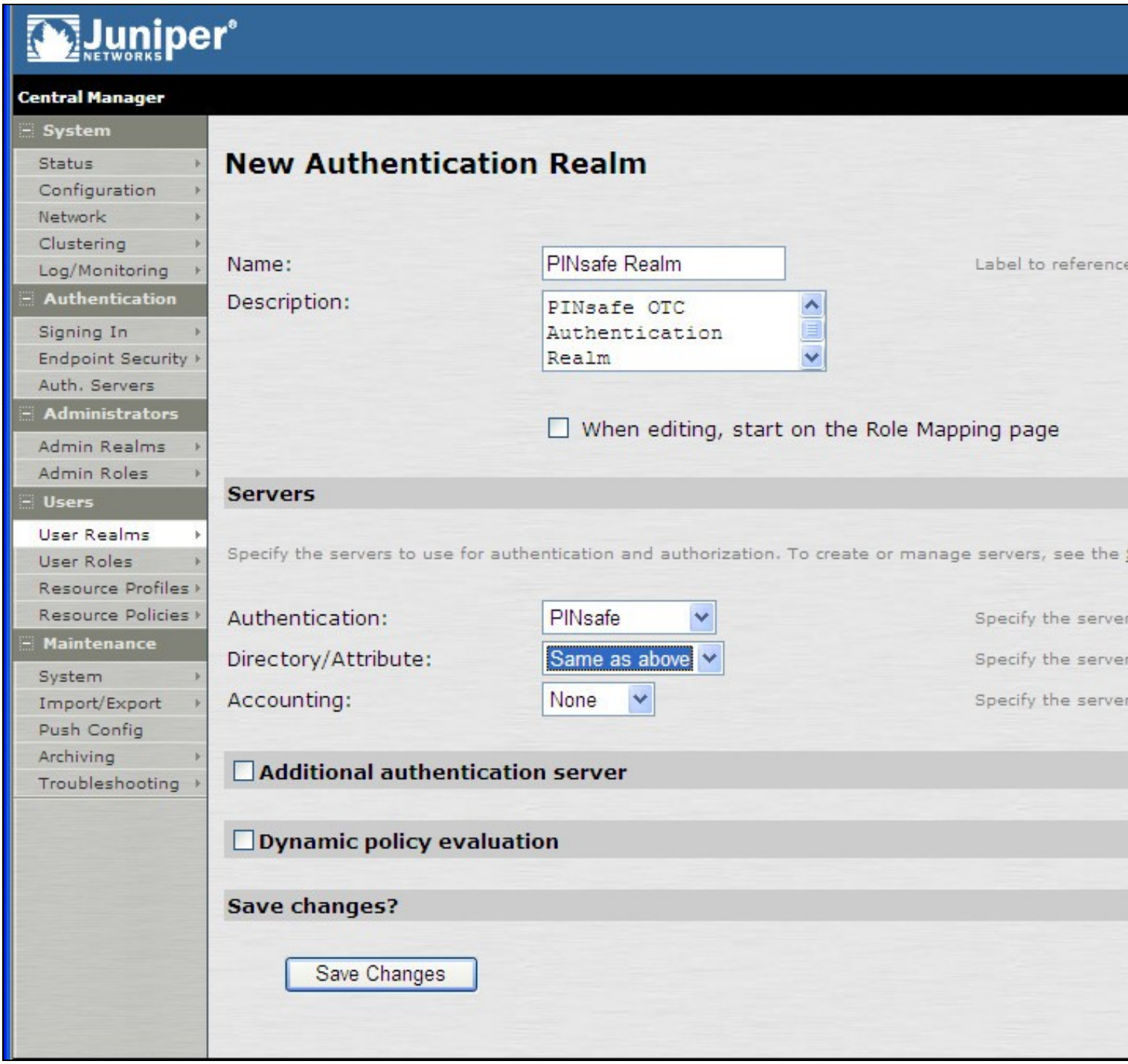
Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.



32.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

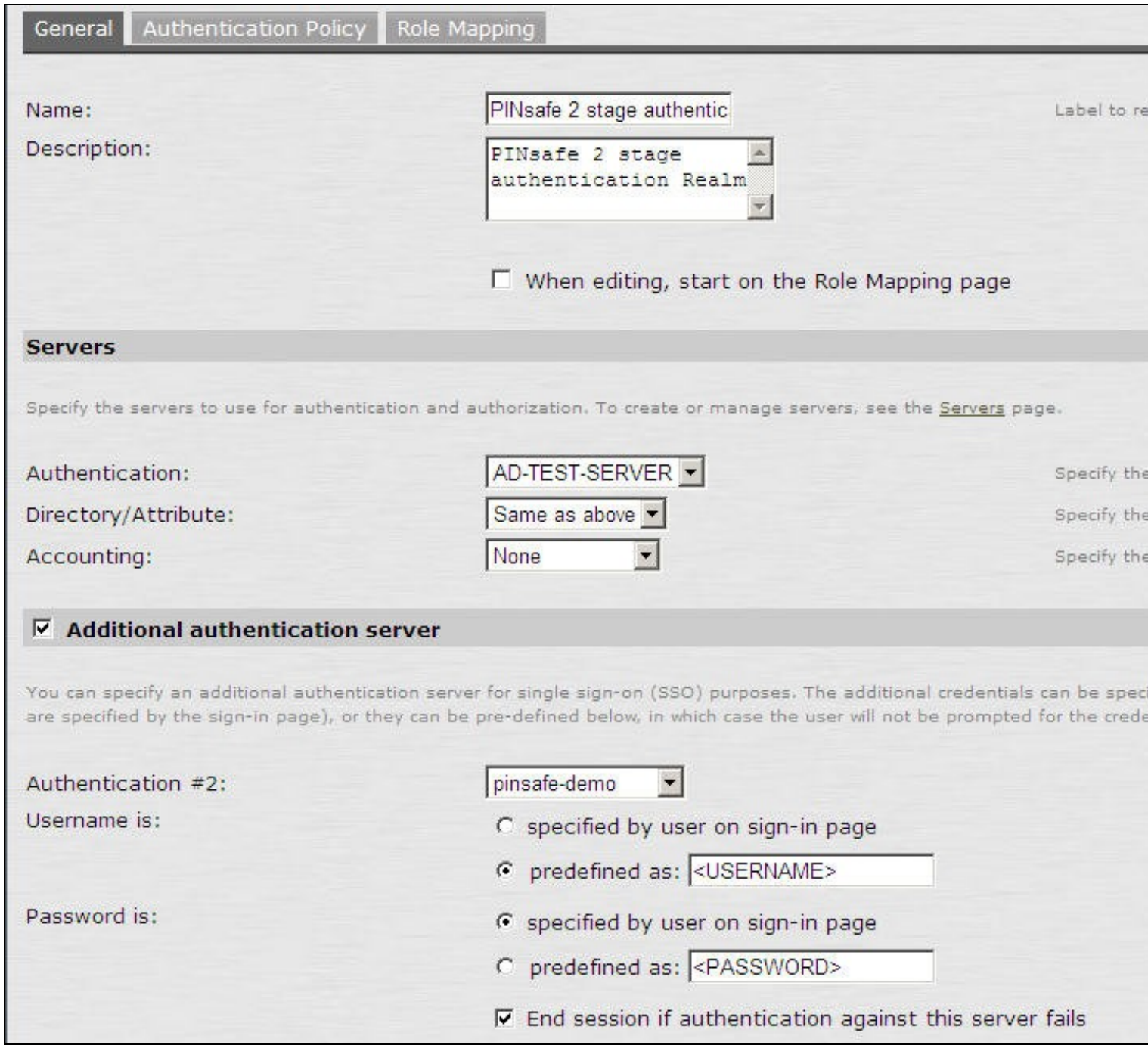
To configure Swivel as the server select the Swivel server as the first listed Authentication Server.



32.3.4 Swivel as the Secondary Authentication Server

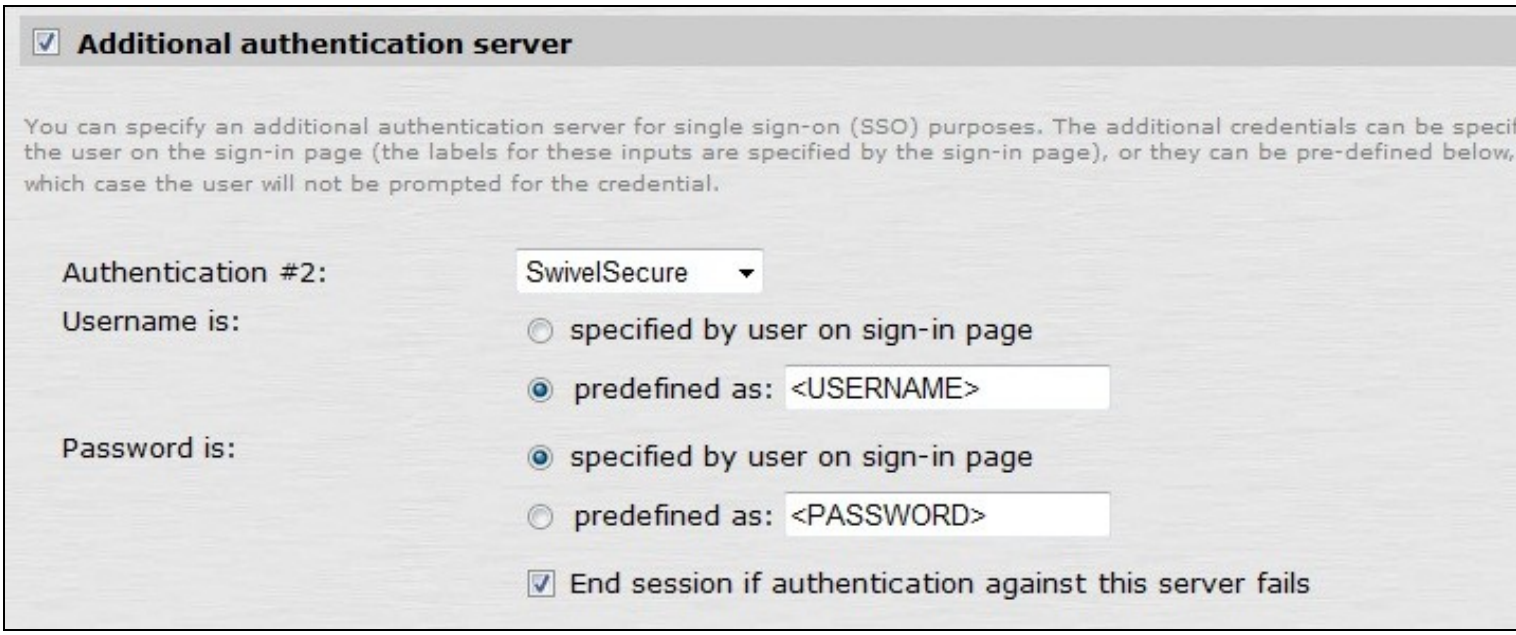
Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box **Additional authentication server**

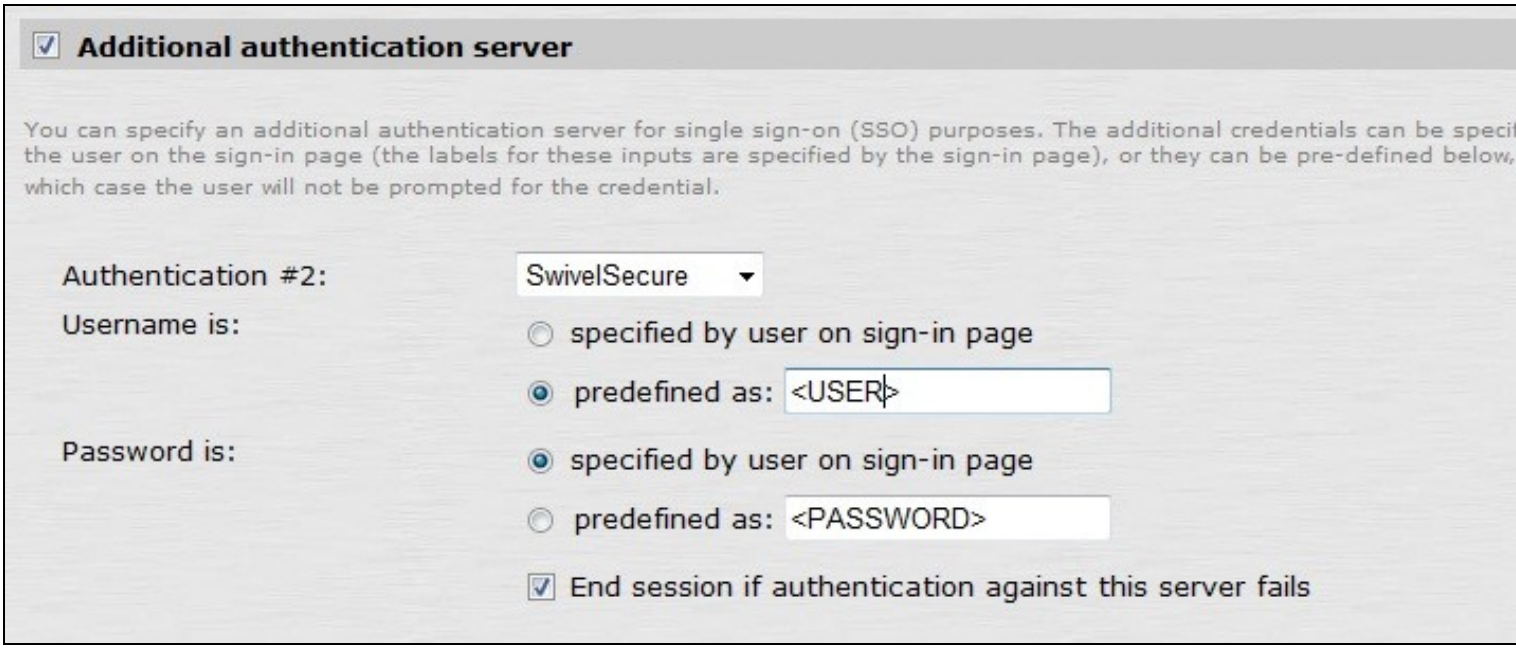


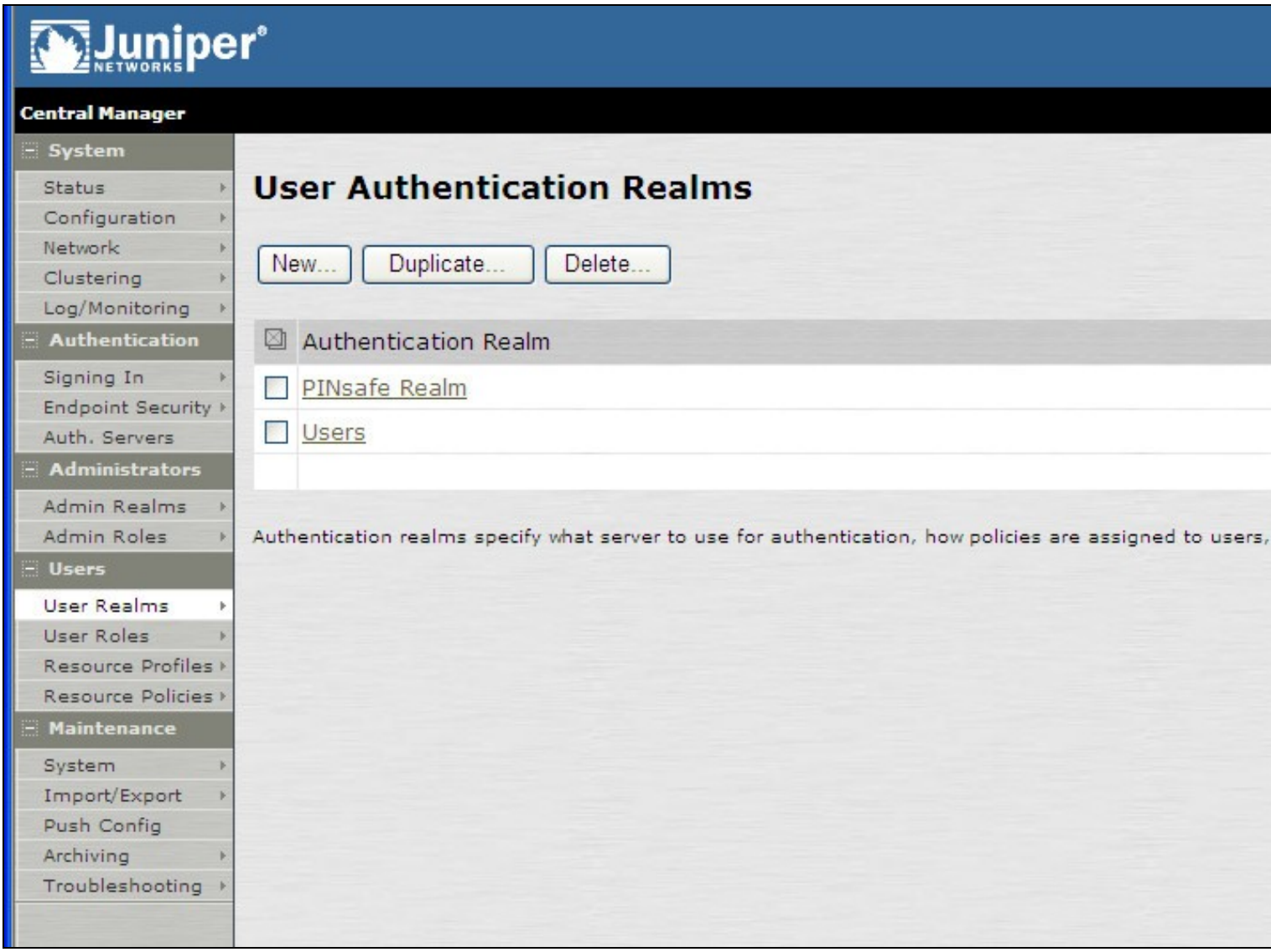
Note when USERNAME is used then just the username is sent to the Juniper. When USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username.

USERNAME


Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USERNAME>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails

USER

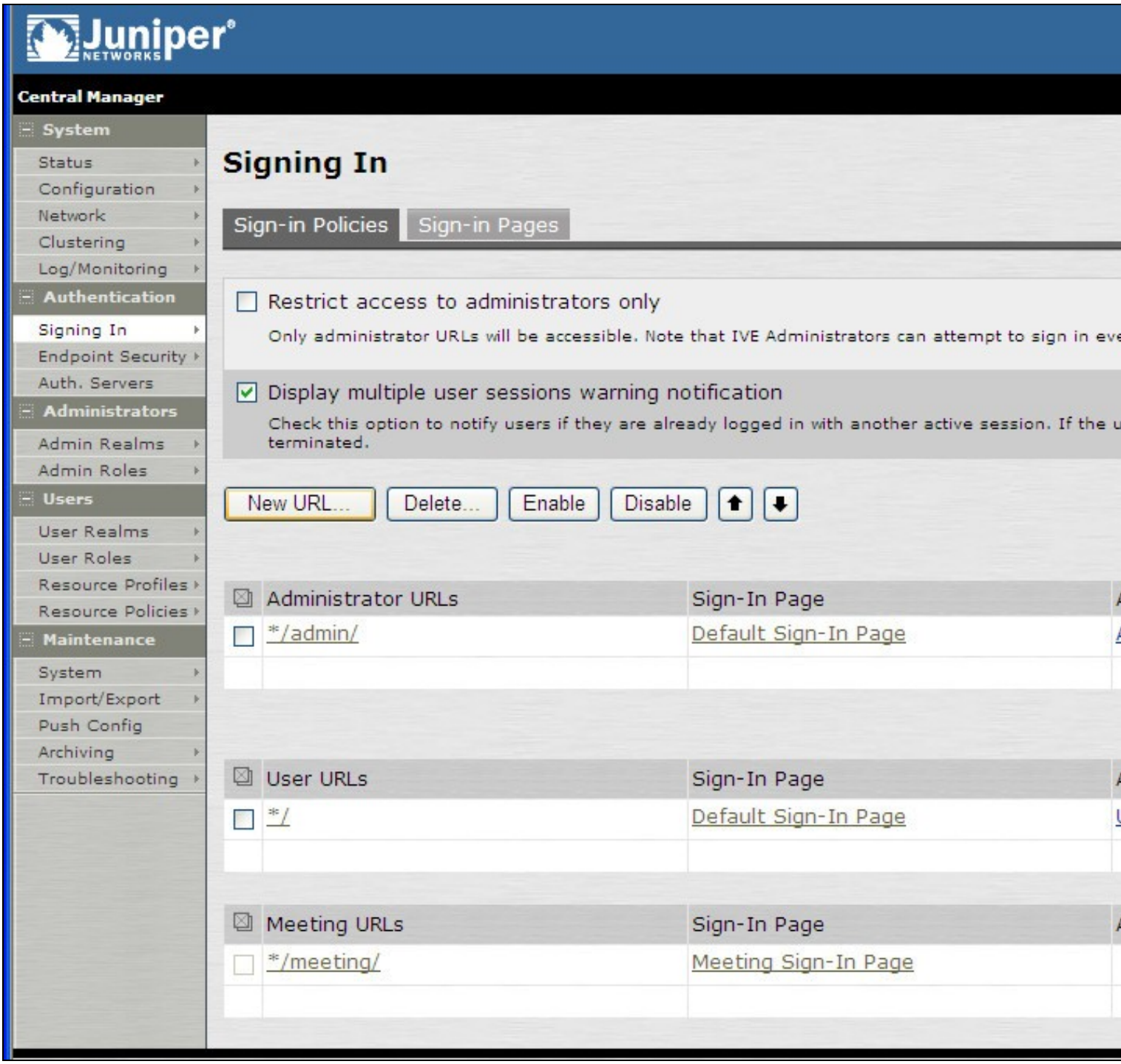

Additional authentication server
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif
the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below,
which case the user will not be prompted for the credential.
Authentication #2:
SwivelSecure
Username is:
specified by user on sign-in page
predefined as: <USER>
Password is:
specified by user on sign-in page
predefined as: <PASSWORD>
End session if authentication against this server fails



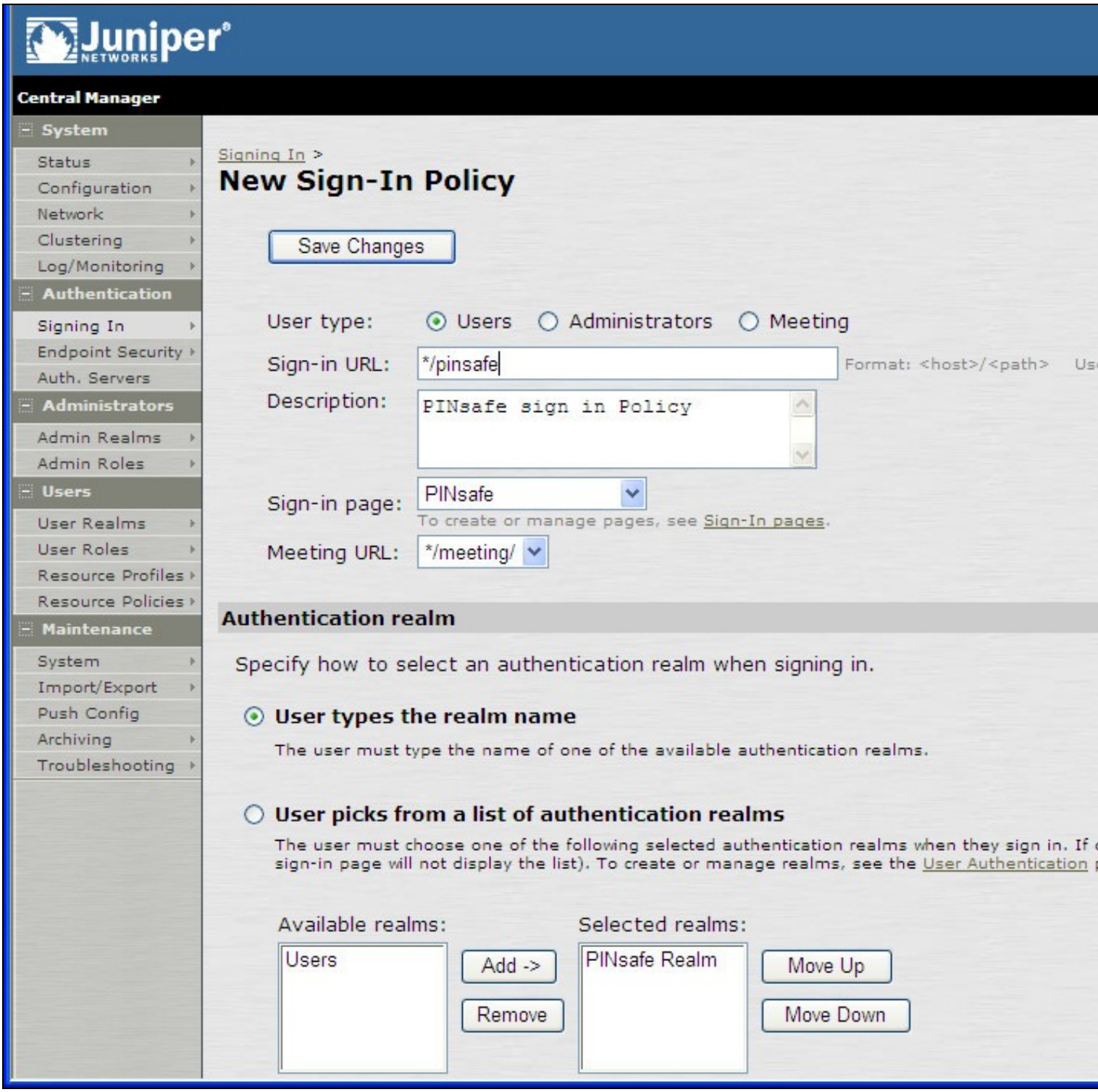
32.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.



Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.



When complete the new Swivel policy should be listed.


Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
Restrict access to administrators only
Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve
Display multiple user sessions warning notification
Check this option to notify users if they are already logged in with another active session. If the u
terminated.
New URL...
Delete...
Enable
Disable
Administrator URLs
Sign-In Page
*/admin/
Default Sign-In Page
User URLs
Sign-In Page
*/
Default Sign-In Page
*/pinsafe/
PINsafe
Meeting URLs
Sign-In Page
*/meeting/
Meeting Sign-In Page

33 Additional Installation Options

Swivel can provide additional authentication options including:

Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

33.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

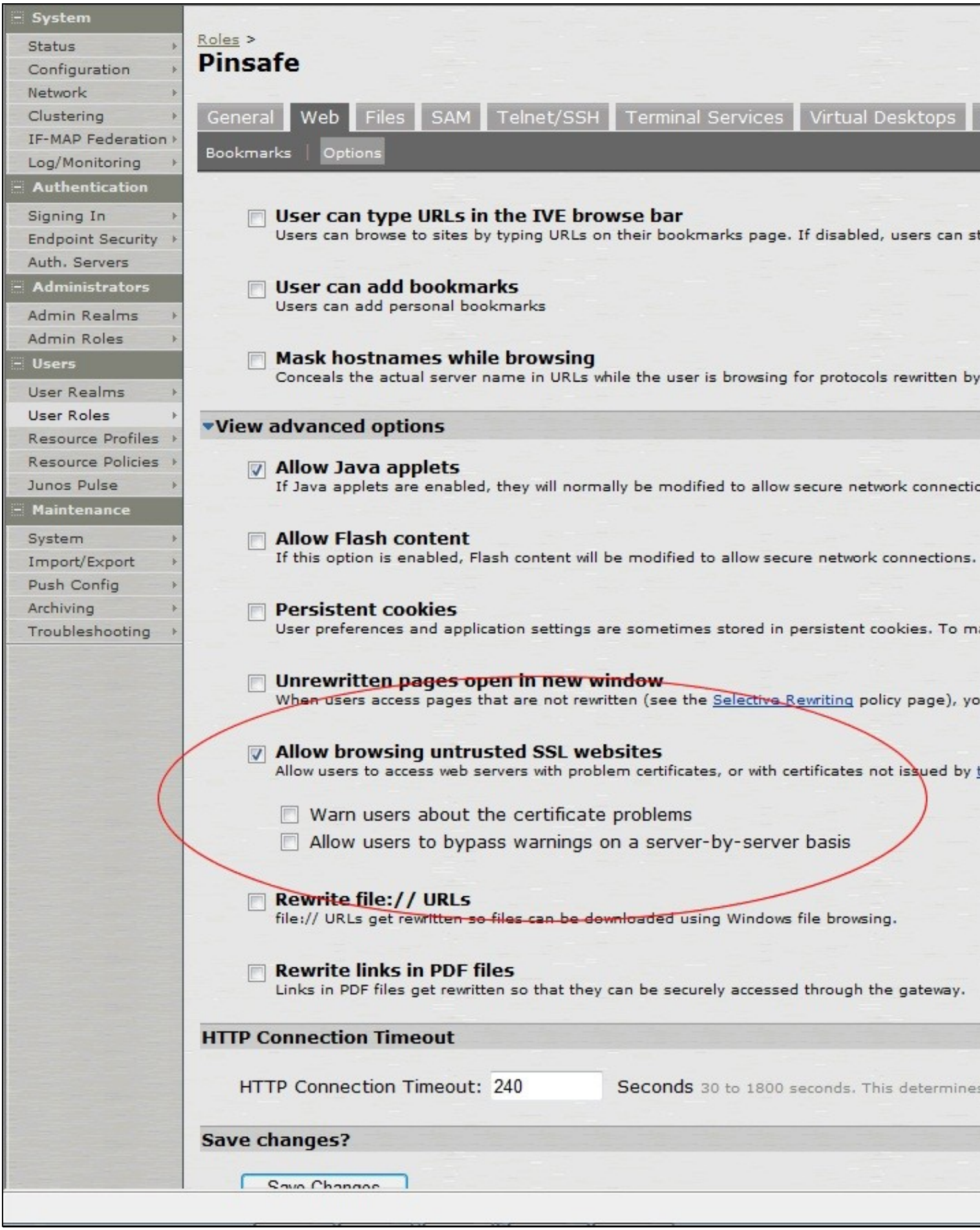
Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

33.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.


System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
Pinsafe
General
Web
Files
SAM
Telnet/SSH
Terminal Services
Virtual Desktops
Bookmarks
Options
User can type URLs in the IVE browse bar
Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can st
User can add bookmarks
Users can add personal bookmarks
Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
View advanced options
Allow Java applets
If Java applets are enabled, they will normally be modified to allow secure network connectio
Allow Flash content
If this option is enabled, Flash content will be modified to allow secure network connections.
Persistent cookies
User preferences and application settings are sometimes stored in persistent cookies. To ma
Unrewritten pages open in new window
When users access pages that are not rewritten (see the Selective Rewriting policy page), yo
Allow browsing untrusted SSL websites
Allow users to access web servers with problem certificates, or with certificates not issued by t
Warn users about the certificate problems
Allow users to bypass warnings on a server-by-server basis
Rewrite file:// URLs
file:// URLs get rewritten so files can be downloaded using Windows file browsing.
Rewrite links in PDF files
Links in PDF files get rewritten so that they can be securely accessed through the gateway.
HTTP Connection Timeout
HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determines
Save changes?
Save Changes

33.1.2 Creating an ACL for the Virtual hostname role

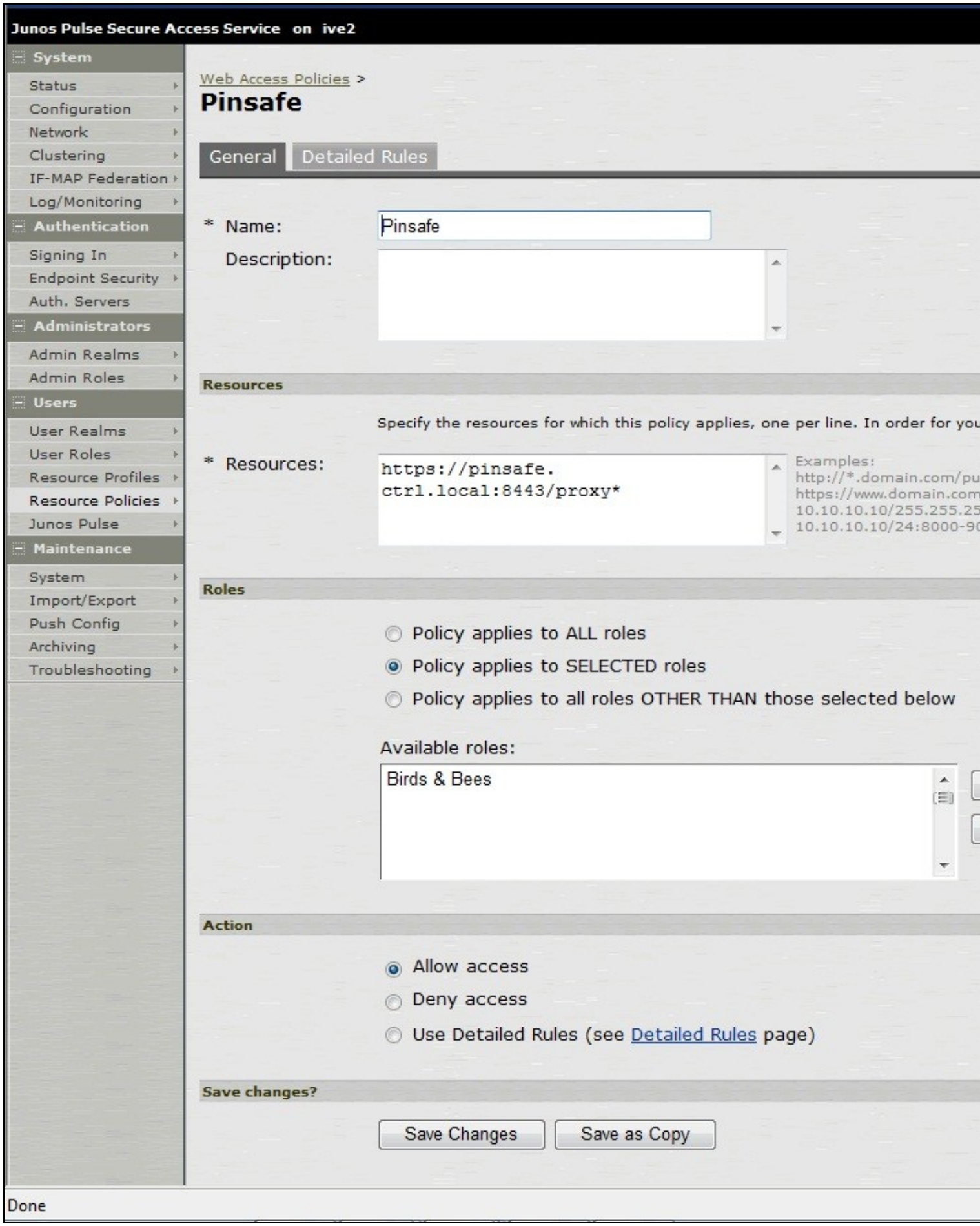
An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.


Junos Pulse Secure Access Service on ive2
System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Web Access Policies >
Pinsafe
General
Detailed Rules
* Name:
Pinsafe
Description:
Resources
Specify the resources for which this policy applies, one per line. In order for you
* Resources:
https://pinsafe.
ctrl.local:8443/proxy*
Examples:
http://*.domain.com/pu
https://www.domain.com
10.10.10.10/255.255.25
10.10.10.10/24:8000-90
Roles
Policy applies to ALL roles
Policy applies to SELECTED roles
Policy applies to all roles OTHER THAN those selected below
Available roles:
Birds & Bees
Action
Allow access
Deny access
Use Detailed Rules (see Detailed Rules page)
Save changes?
Save Changes
Save as Copy
Done

33.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New URL. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

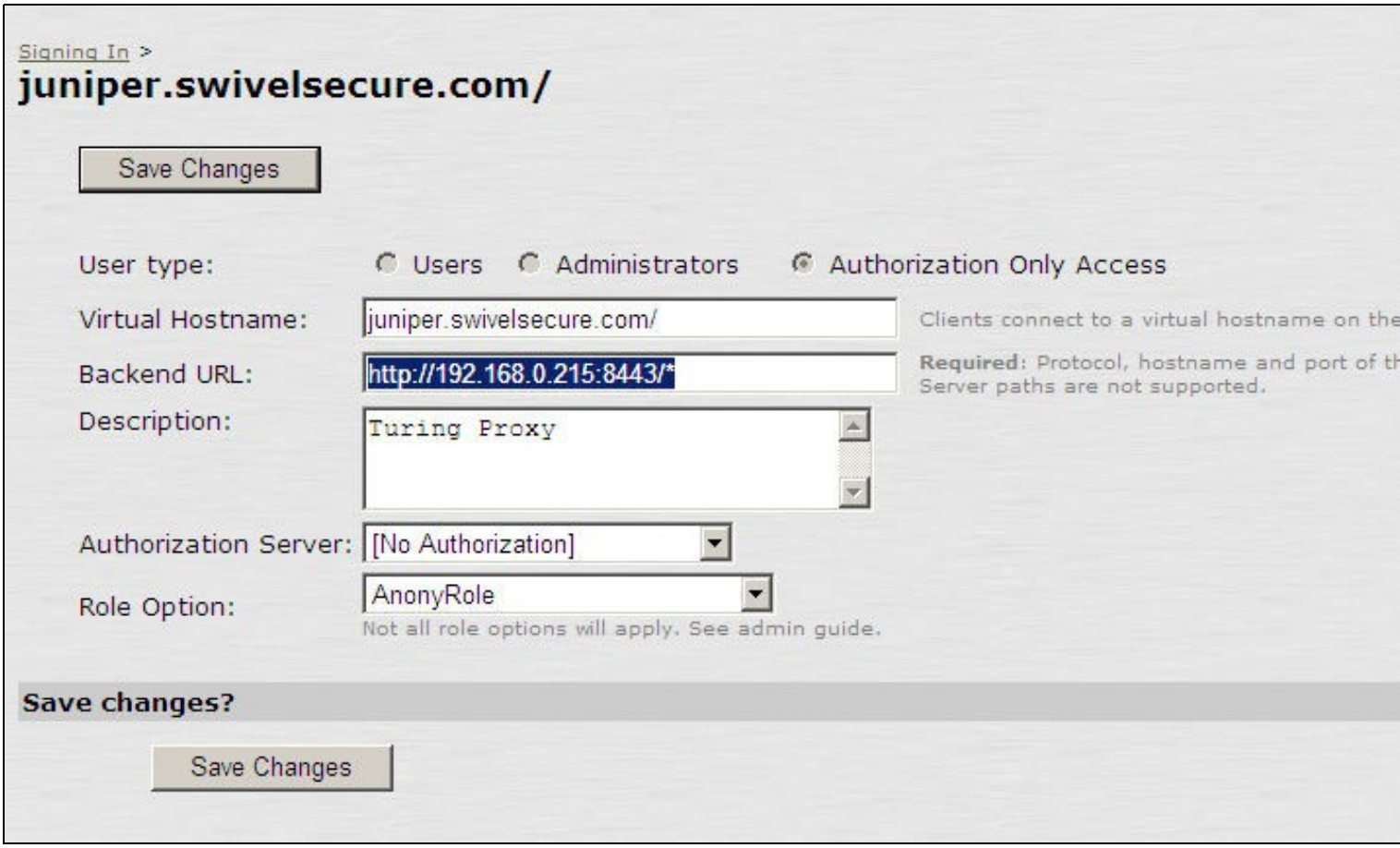
Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

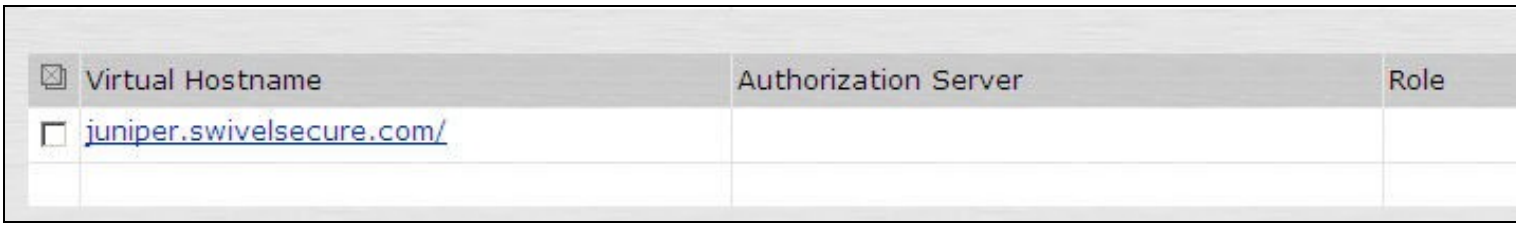
For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes





33.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

https://<turing.mycompany.com>/proxy/SCImage?username=test

Software Install

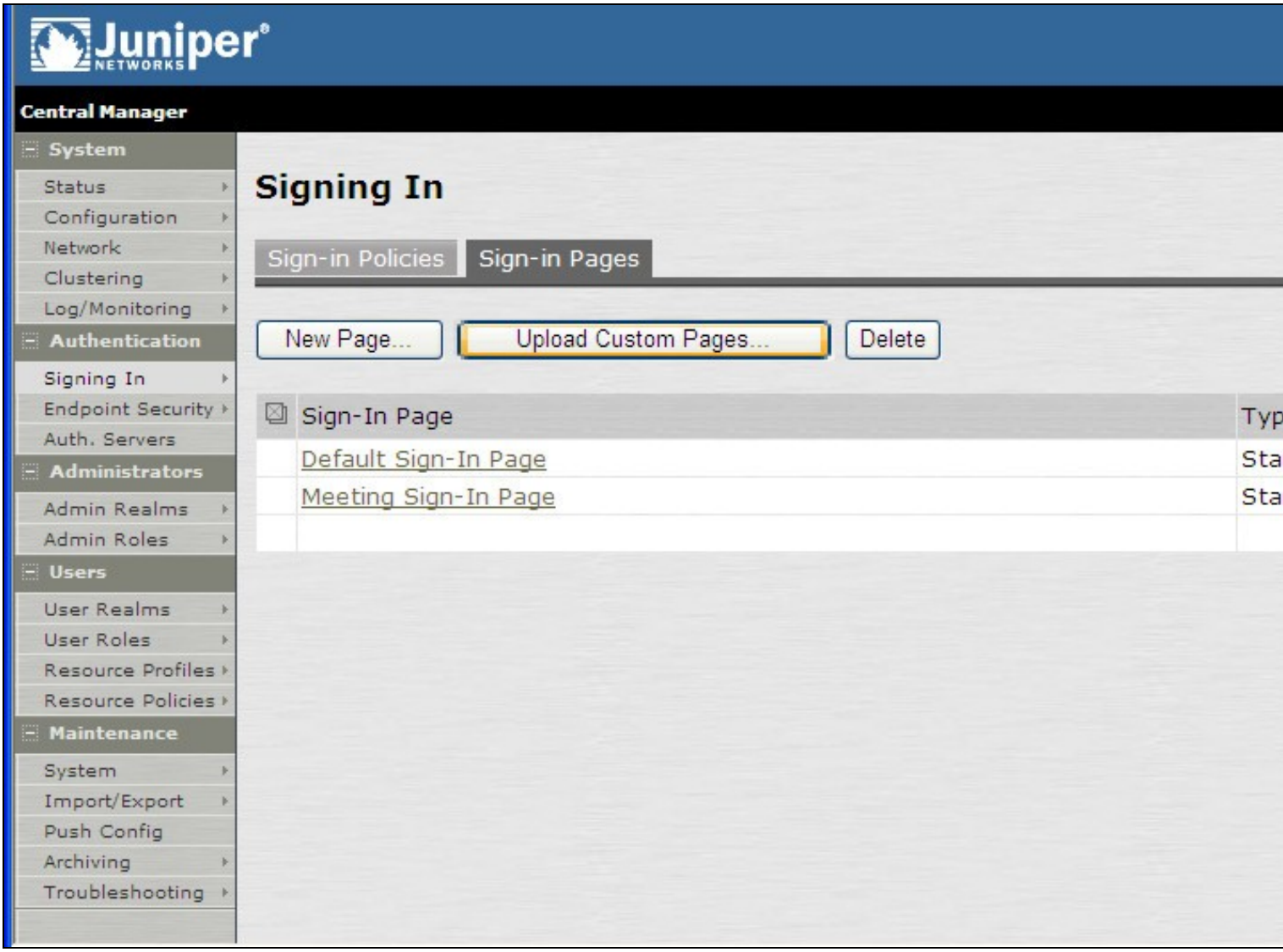
For a software only install see Software Only Installation

Then verify the external access using

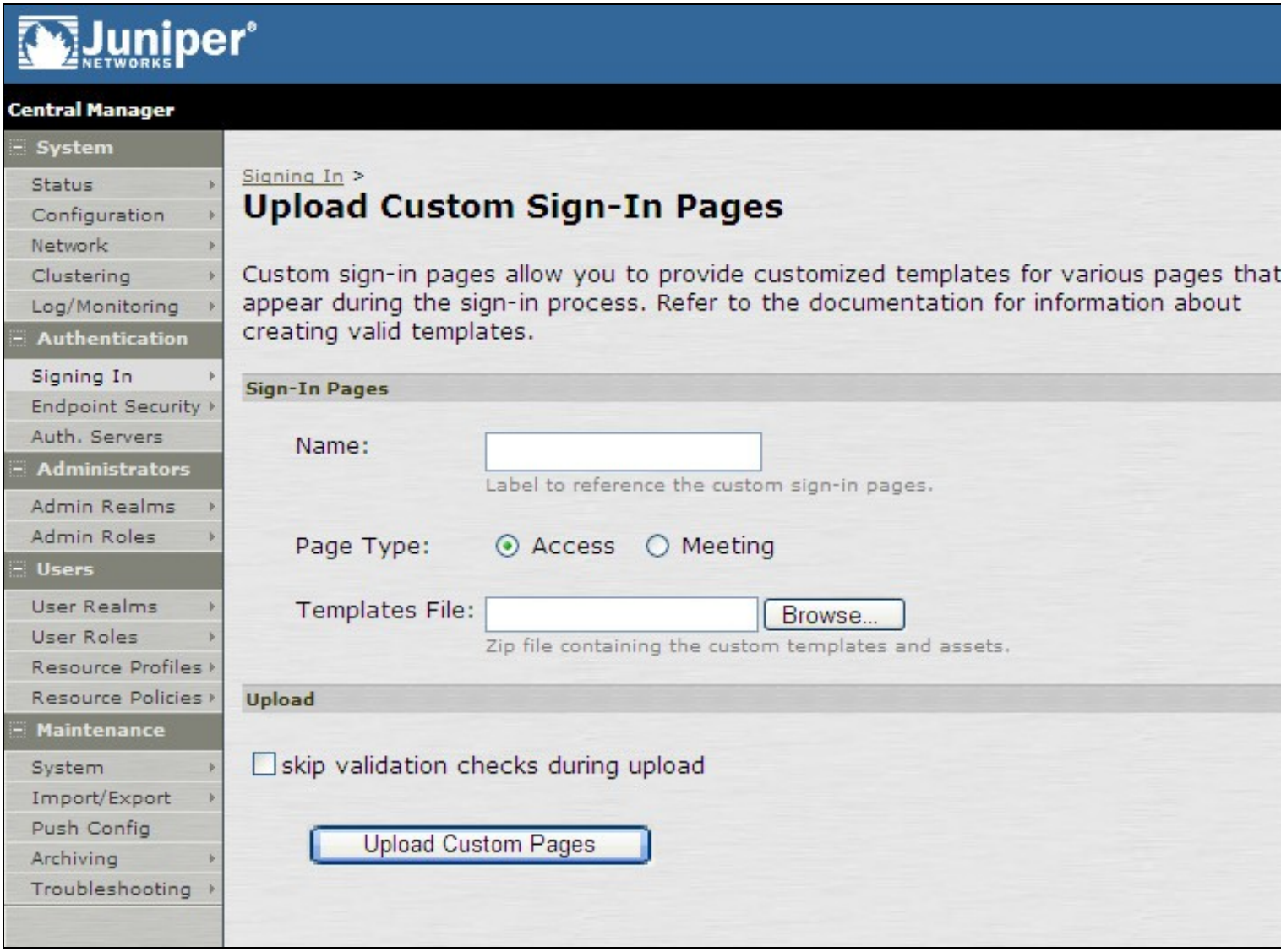
https://<turing.mycompany.com>/pinsafe/SCImage?username=test

33.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.



Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.



Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within **LoginPage.thtml** should be edited to suit your environment as the below modifications.

If you are using the combined PC and tablet version, you should make these changes to swivel-header.thtml.

33.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/SCImage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/SCImage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

33.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

33.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

- Using Virtual DNS

Swivel appliance

```
https://virtual_hostname/proxy/DCMessage?username=";
```

Software install

```
http://virtual_hostname/pinsafe/DCMessage?username=";
```

- For a NAT or Public IP address

Swivel appliance

```
https://hostname:8443/proxy/DCMessage?username=";
```

For a software only install see Software Only Installation

33.2.4 Modifying the login button text

The login page button and link to *Get Another Image* may be modified.

To modify the login button text locate the text *value='Turing'* and replace the Turing with the required text.

To modify the *Get another image?* URL, locate the two instances of *Get another image?* and change the text as required.

33.2.5 Modifying the login for PINpad

Customising for Pinpad can be done using the same custom pages as above. Follow the same instructions as above, except the following:

- The zip file contains 3 additional images that need to go into the *imgs* folder of the Juniper custom login.
- **OTC_OPTION** needs to be set to **"pinpad"**.
- You need to set the value for *PinpadImage*, rather than *TURingImage* to match your own Swivel instance.

Example

```
var PinpadImage = "https://hostname:8443/pinsafe/SCImage?username=";
```

to

```
var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";
```

33.2.6 Modifying the Login pages for Mobile Devices

The prerequisites section contains the mobile modified pages that can be uploaded with any other modified pages to ad wivel authentication to the login.

Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above.

var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

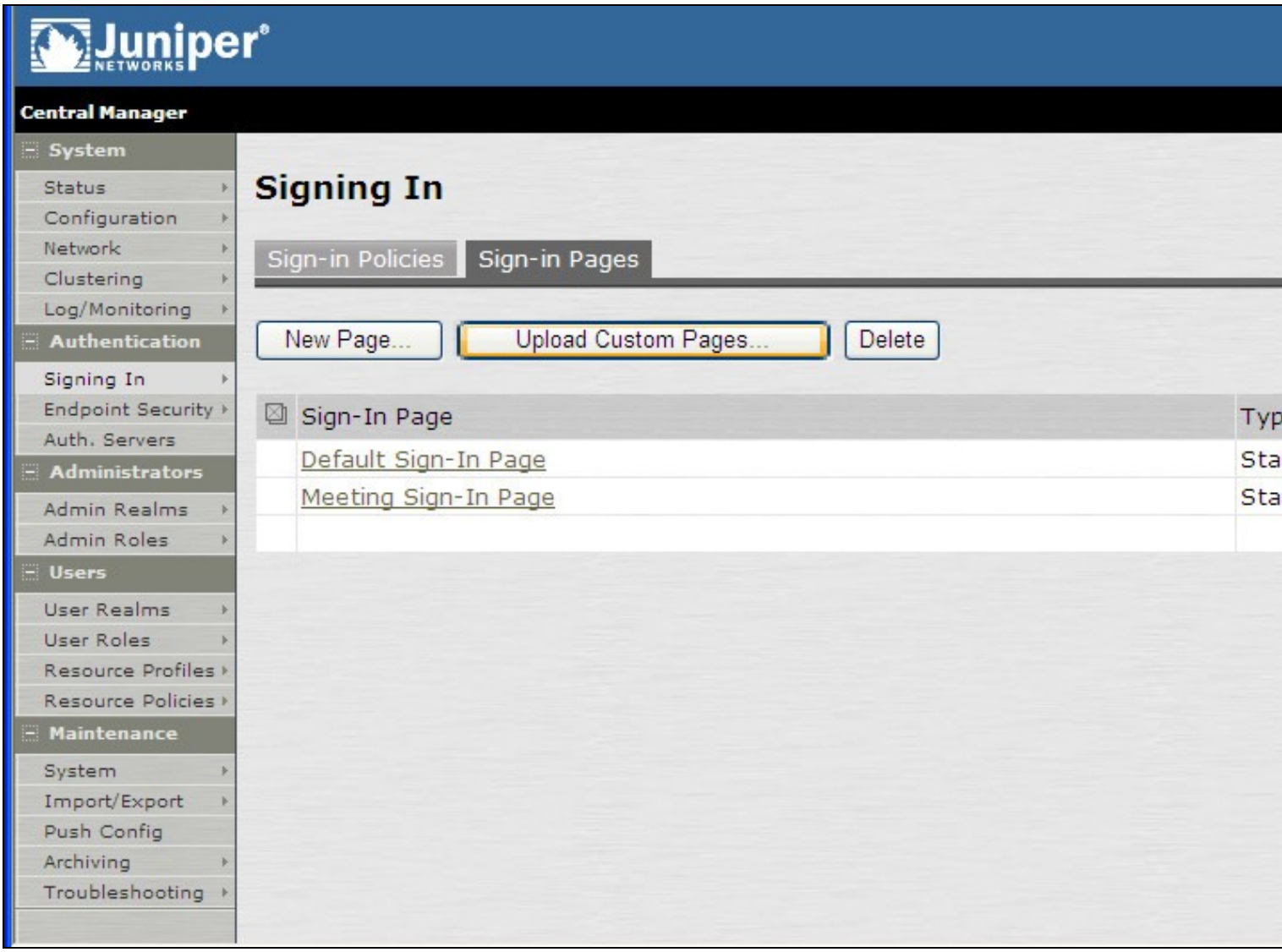
33.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

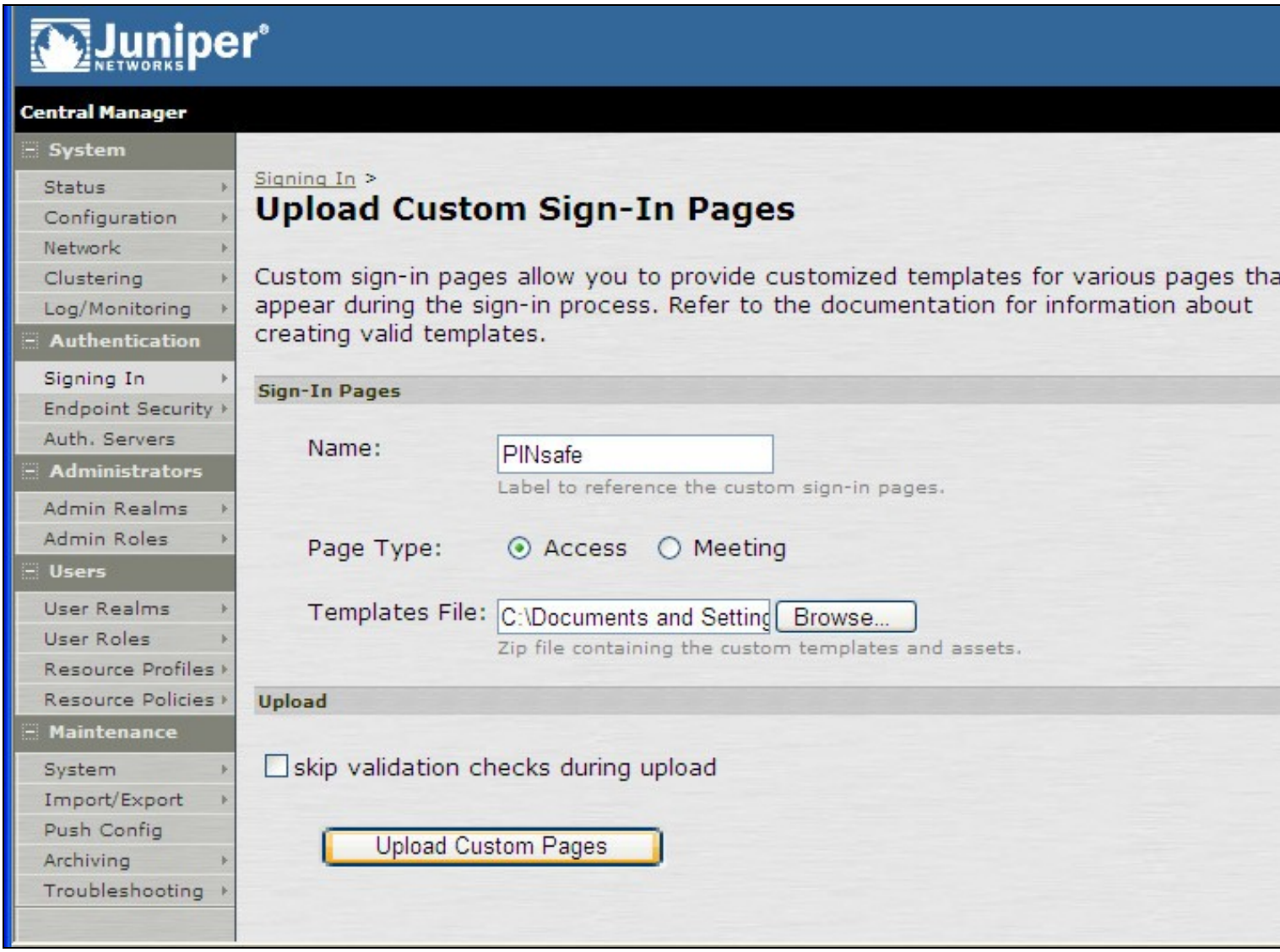
Juniper Network Connect with TURing

33.2.8 Uploading the Modified Page

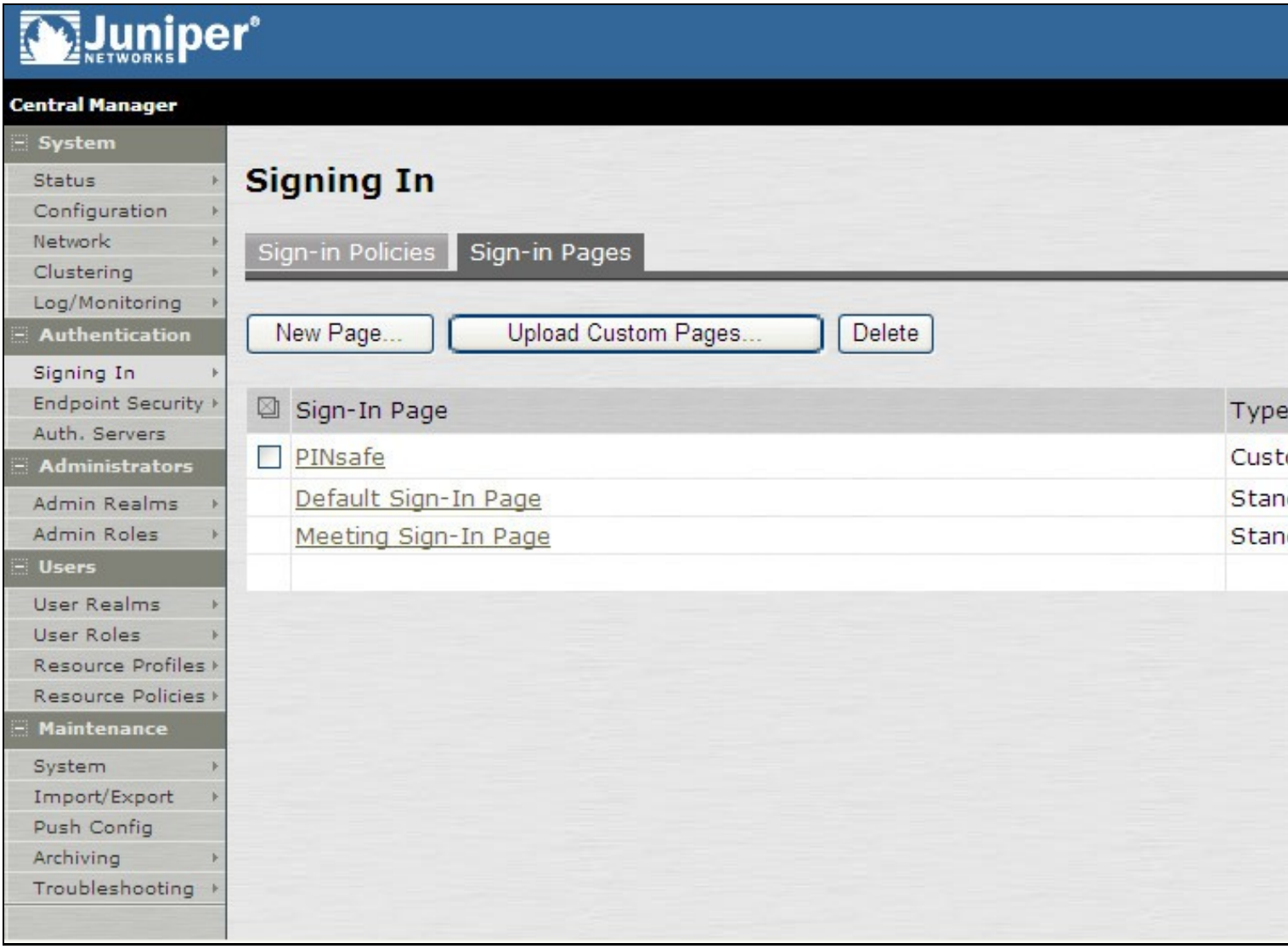
Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.



Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.



The new signing in page should be listed.

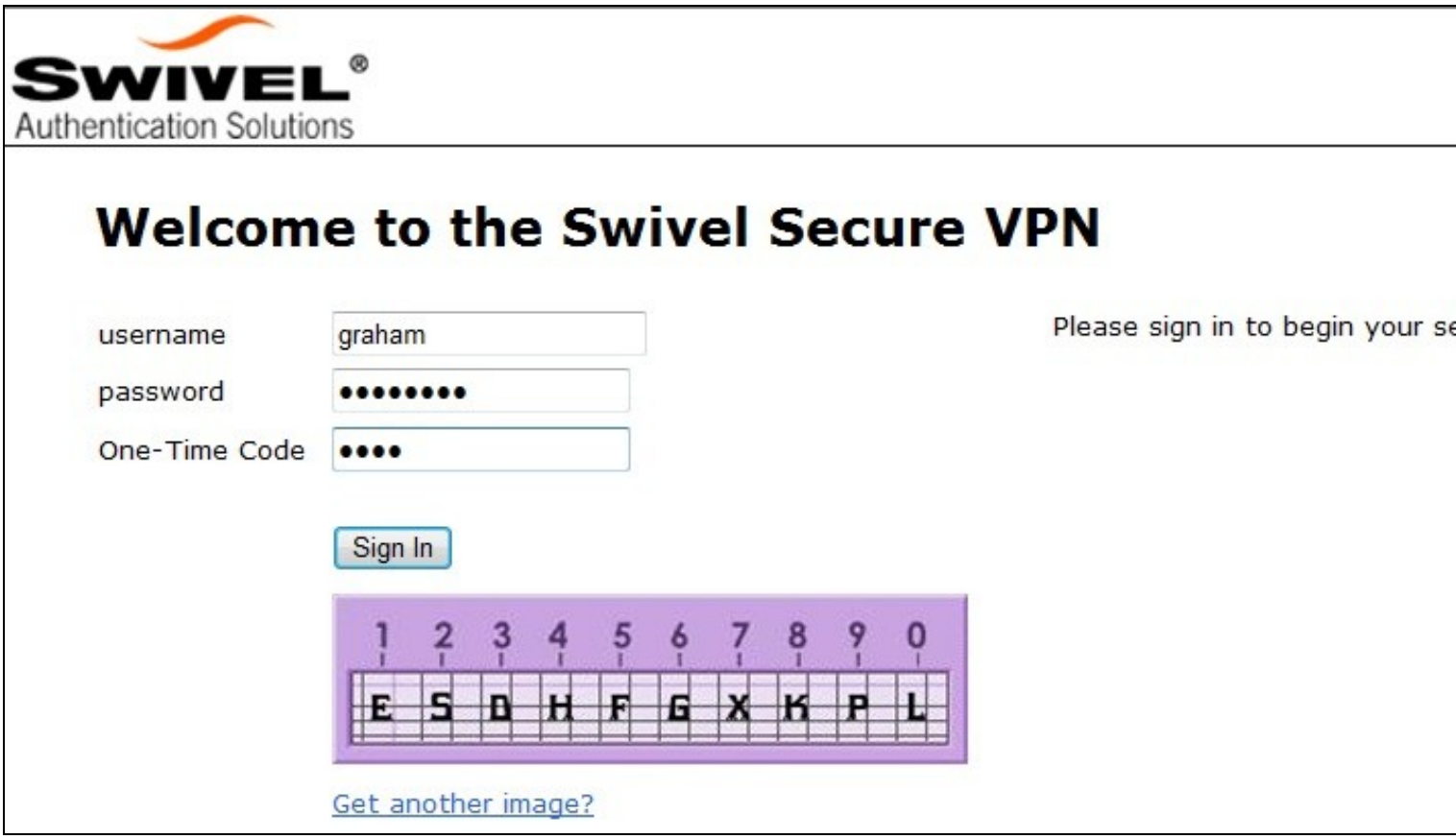

Juniper NETWORKS
Central Manager
System
Status
Configuration
Network
Clustering
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Signing In
Sign-in Policies
Sign-in Pages
New Page...
Upload Custom Pages...
Delete
Sign-In Page
Type
PINsafe
Default Sign-In Page
Meeting Sign-In Page

34 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

Dual Channel Authentication

Single Channel Authentication



35 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

36 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Internal Certificate Authorities

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain\username. When USERNAME is used then just the username is sent to the Juniper.

37 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

37.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

```
<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si
```

A modified login page is available here: iPad modified login page

37.2 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

38 Additional Information

Custom sign-in pages for Pinpad can be found here.

39 Juniper Two Stage Challenge and Response

39.1 Juniper Two Stage and Challenge and Response Authentication

39.2 Introduction

Juniper supports the use of a challenge and response whereby a password is used prior to entering a One Time Code. In addition the Challenge and Response mechanism allows an SMS to be sent upon successful entry of a password.

39.3 Prerequisites

PINsafe 3.7

Juniper 6.x

Dual Channel authentication

Two stage authentication requires the use of either a PINsafe password, or that Check password with repository is enabled.

39.4 Baseline

PINsafe 3.7

Juniper 6.4

39.5 Architecture

Juniper using RADIUS authentication to the PINsafe server, with security strings sent to the user using an SMS gateway.

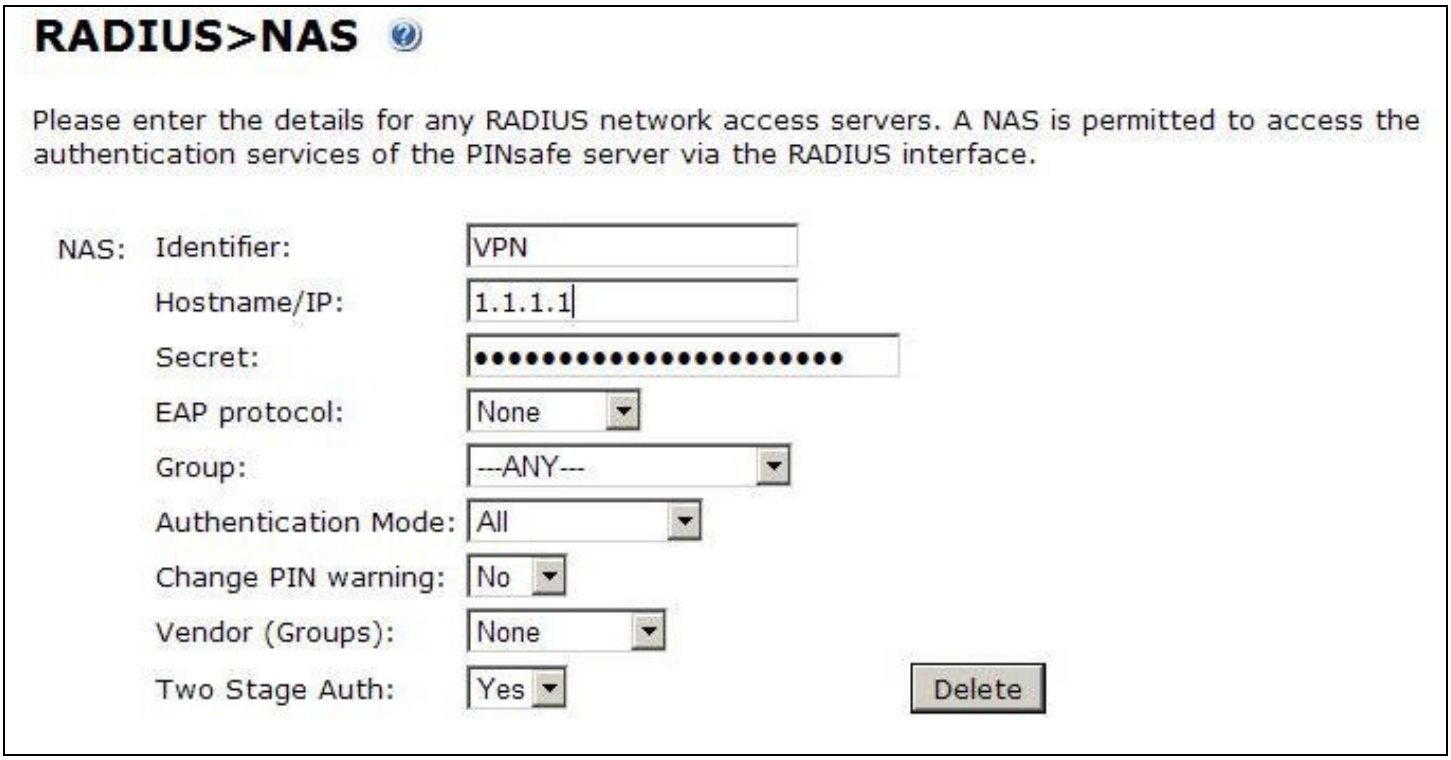
39.6 Installation

Configure the PINsafe server and Juniper appliance for Dual Channel Authentication. Ensure either the user has a PINsafe password, or that Check password with repository is enabled.

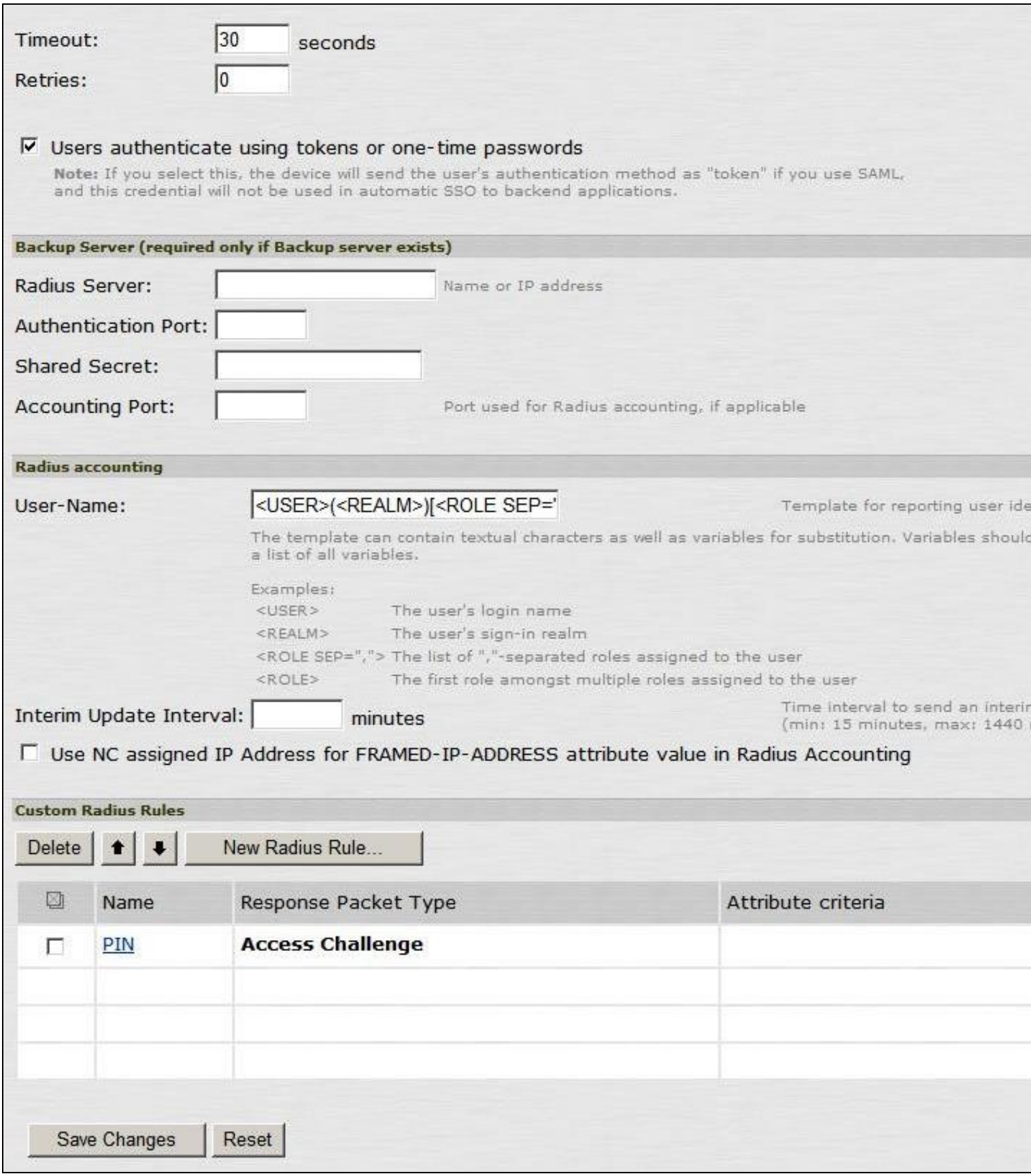
39.7 Adding Two Stage Authentication

See also: Two Stage Authentication How to Guide

On the PINsafe Administration Console server select RADIUS/NAS and the Access device which two stage authentication is required. Set the Two stage Auth to Yes and Apply.



On the Juniper Administration Console, browse to the Authentication/Auth Servers menu, and select the PINsafe RADIUS authentication server. Under Custom RADIUS Rules click on the New RADIUS Rule button.

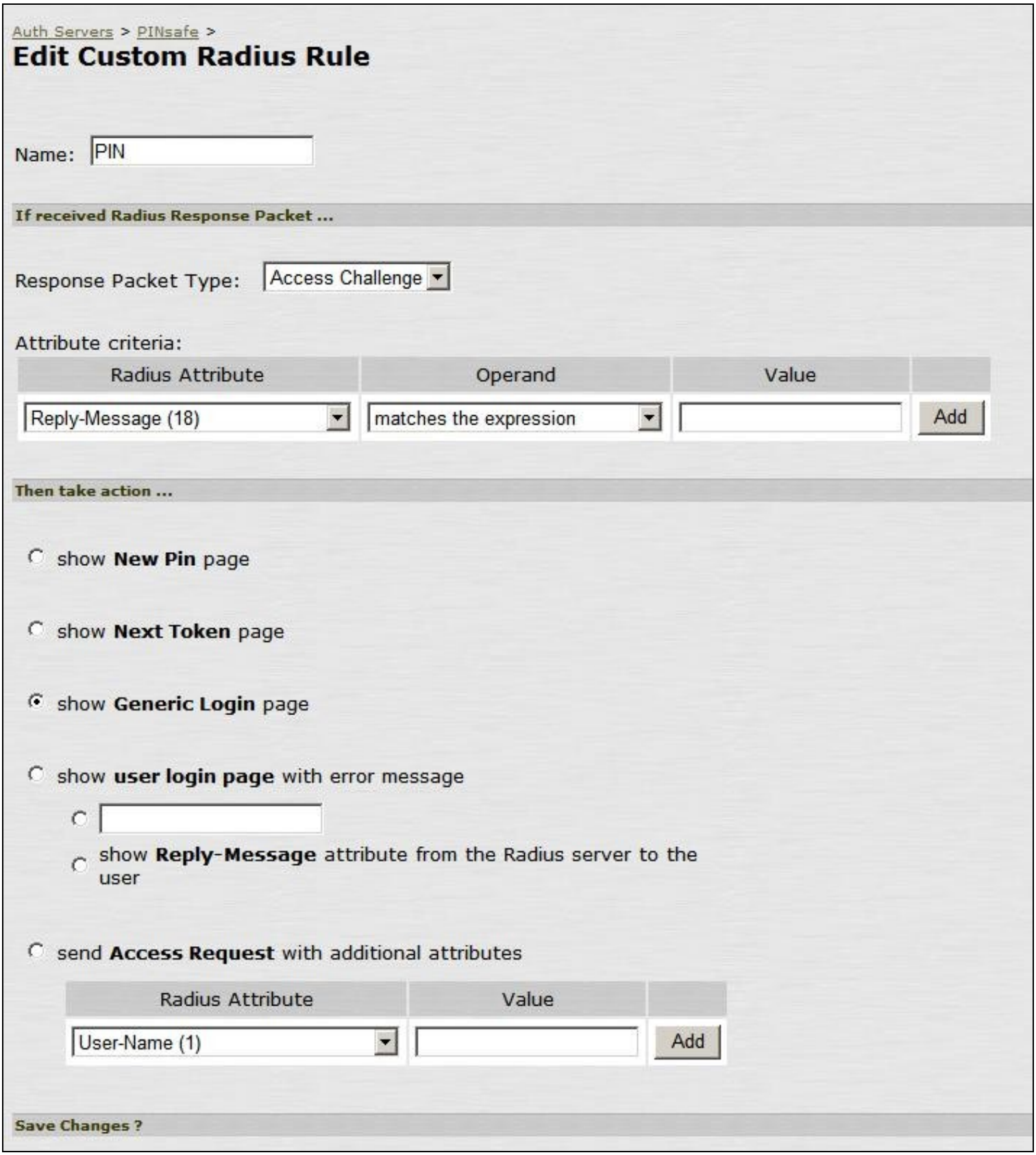


Enter a name for the Rule and ensure Response Packet Type is set to Access Challenge.

Under Attribute Criteria ensure RADIUS Attribute is set to Reply Message (18), with the Operand matches the expression, leave the value setting blank.

Ensure that the radio button for ?Show Generic Login Page? is selected.

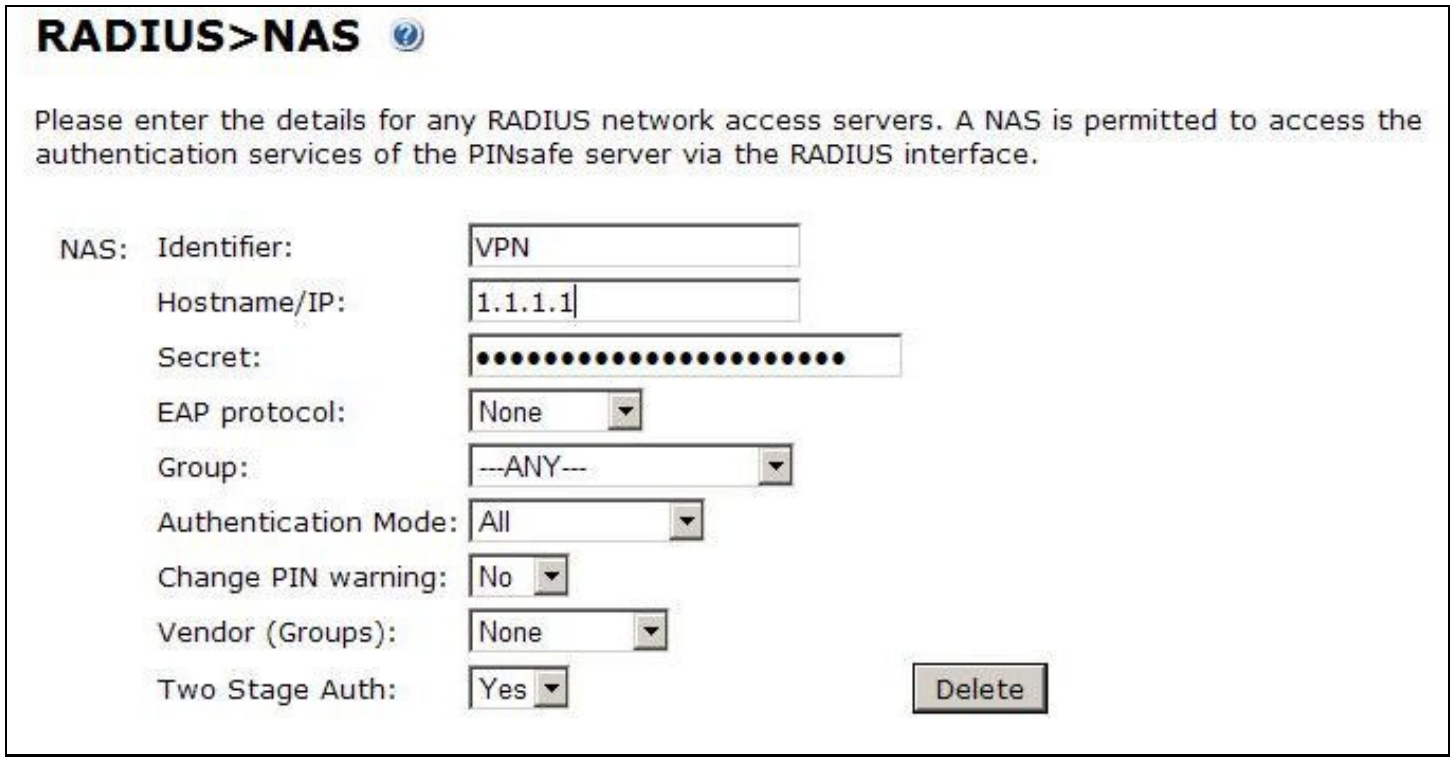
Click on Save Changes.



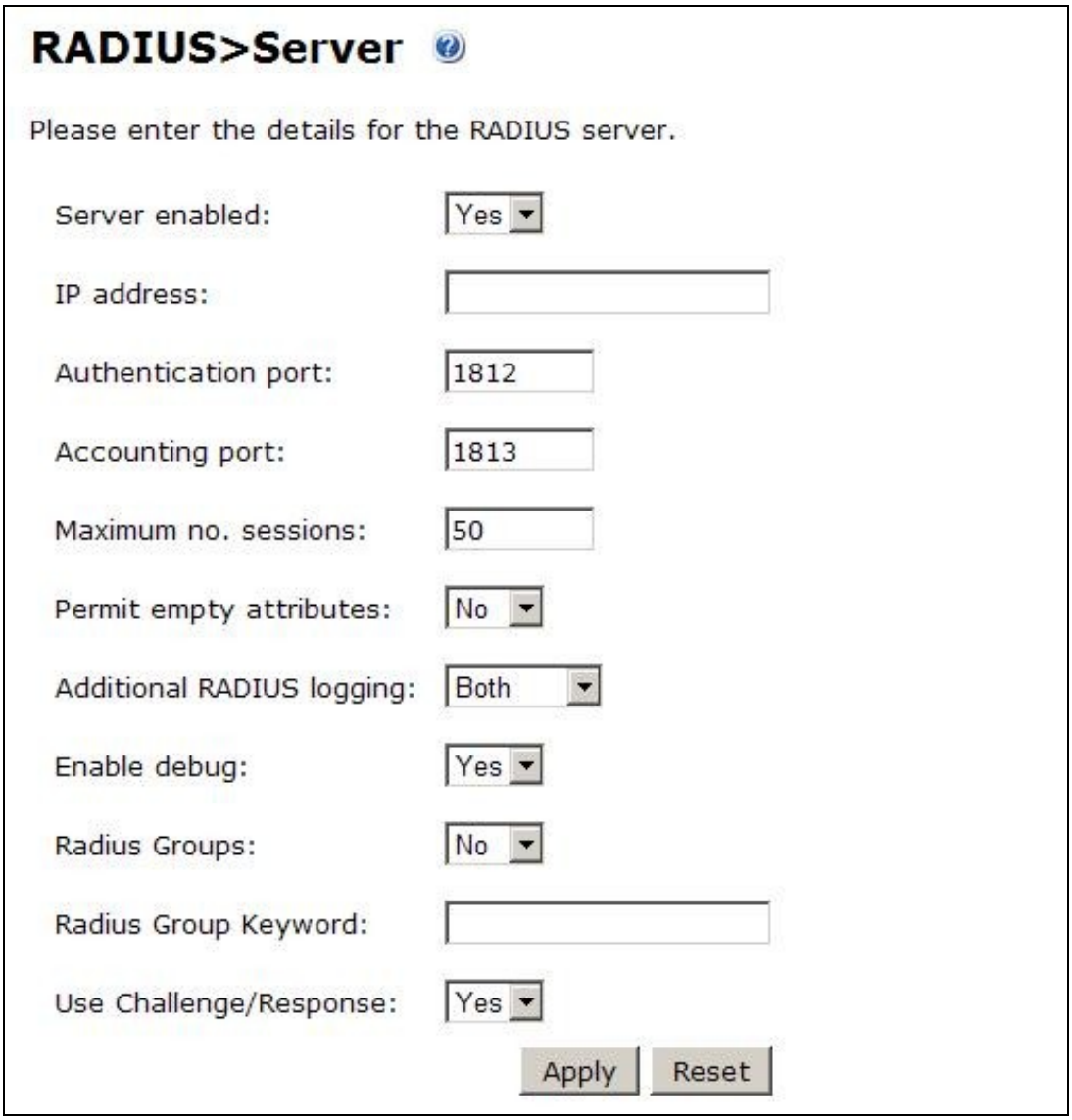
39.8 Adding Challenge and response Authentication

See also: Challenge and Response How to Guide

For PINsafe 3.7 and later, on the PINsafe Administration Console server select RADIUS/NAS and ensure the Two Stage Auth is set to Yes, then click on Apply.



For PINsafe 3.6 and earlier, on the PINsafe Administration Console server select RADIUS/Server and ensure the Use Challenge/Response is set to Yes, then click on Apply.



On the PINsafe Administration Console server select Server/Dual Channel. For delivery of a new security string upon entering a correct password, ensure On-Demand Authentication is set to Yes, then click on Apply.

39.9 Combining Juniper and PINsafe Two Stage Authentication

Using the Juniper AD authentication is useful for single Sign On (SSO) features, so it may be of use to combine the Juniper Two Stage login with that of the PINsafe Two Stage authentication in order to send the user a security string or OTC when the AD password is entered. To configure this:

Enable Two Stage Authentication on the Juniper

Enable two Stage Authentication on the PINsafe Administration Console

Enable Check Password with Repository on the PINsafe Administration Console, See Check Password With Repository

On the Juniper select the User Realm relating to the required Authentication Realm and change the **set Password is:** to the value **Predefined as <PASSWORD>**

When an authentication is made, the AD password is used for the Juniper and the PINsafe Two Stage Authentication so it does not need to be entered twice.

39.10 Verifying the Installation

Check the PINsafe logs

Check the Juniper logs

39.11 Troubleshooting

View the users security string to ensure the correct security string is being used.

Ensure authentication is working with standard authentication.

39.12 Known Issues and Limitations

PINsafe 3.7 Beta required the use of Multiple Authentications per string to be enabled for dual/single channel located on the PINsafe Administration console under Server/Single Channel or Server/Dual Channel.

39.13 Additional Information

Juniper can also be configured for Constrained Delegation where a PINsafe One Time Code is entered and this signs the user into their AD applications without the use of an AD password in the login process. See the following documentation: http://www.juniper.net/techpubs/software/ive/6.x/6.4/

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