Juniper SA 8.x Integration

Contents

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.

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.

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.

Baseline

Juniper 8

Swivel 3.9.7

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.

Installation

Swivel Configuration

Configuring the RADIUS server

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

Enabling Session creation with username

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

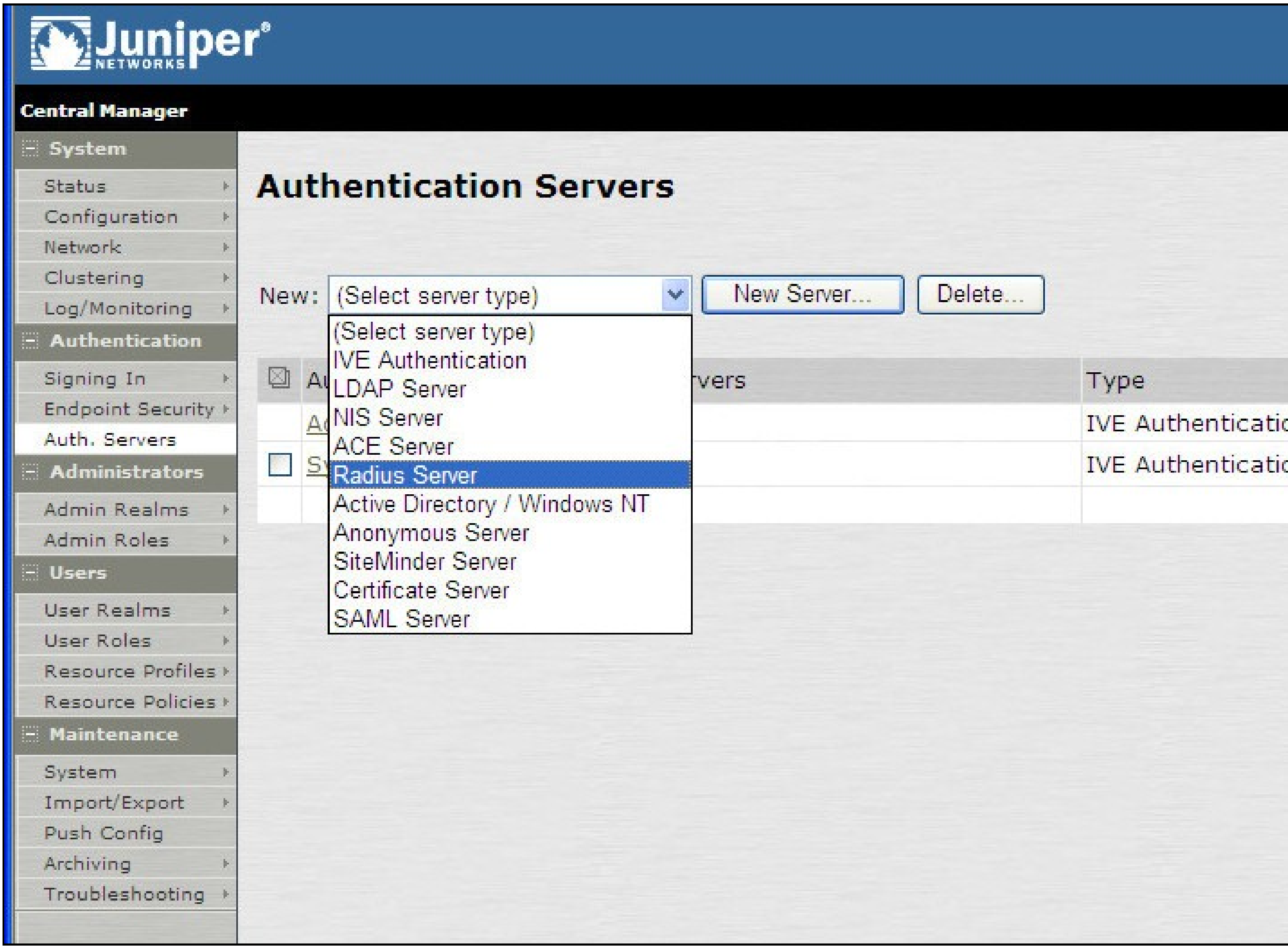
Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

Juniper Integration

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

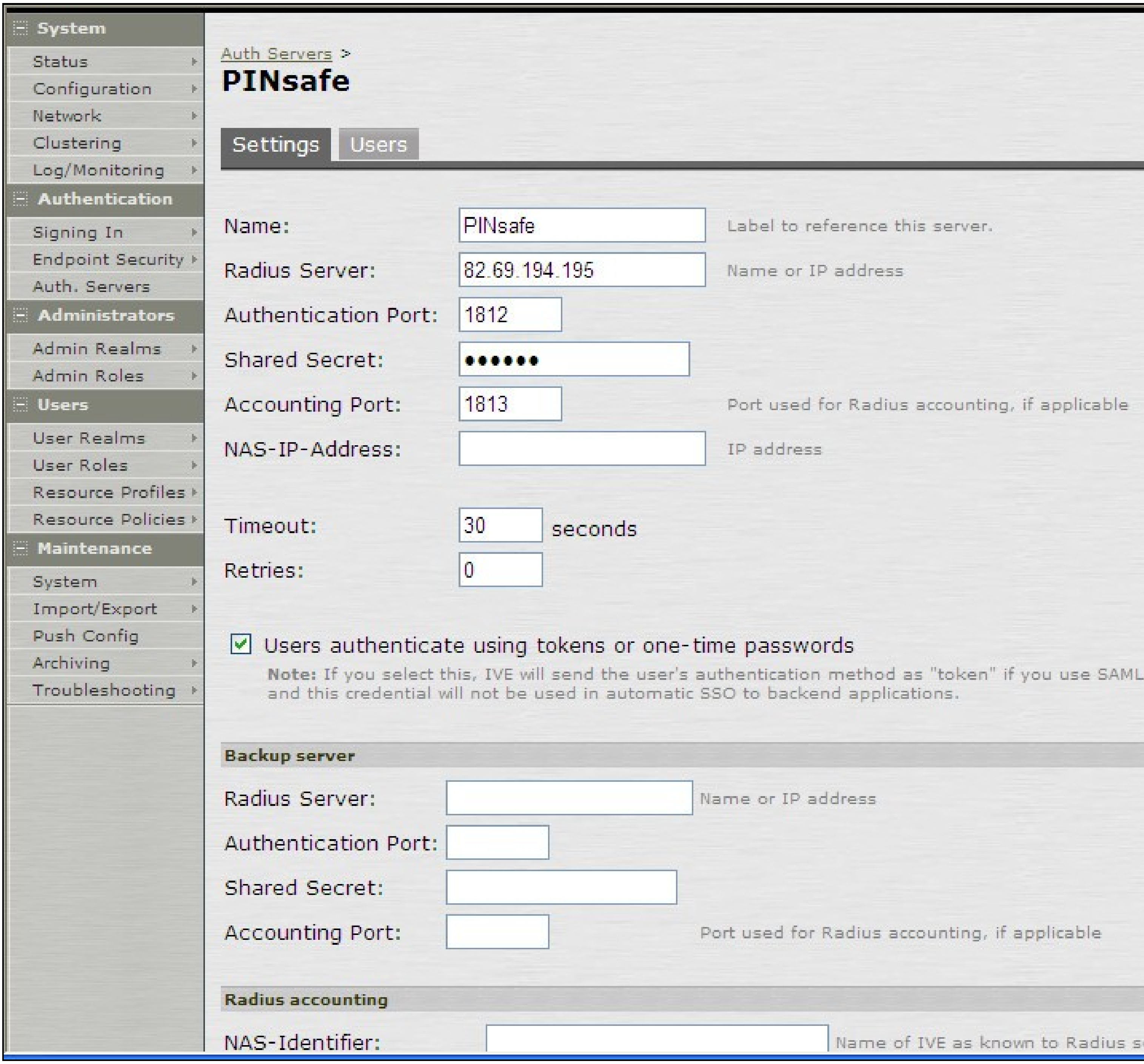
Shared Secret: The shared secret that has been entered on the Swivel server

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.



Auth Servers >

PINsafe

Name:	PINsafe	Label to reference this server.
Radius Server:	82.69.194.195	Name or IP address
Authentication Port:	1812	
Shared Secret:	••••••	
Accounting Port:	1813	Port used for Radius accounting, if applicable
NAS-IP-Address:		IP address
Timeout:	30 seconds	
Retries:	0	

☑ Users authenticate using tokens or one-time passwords

Note: If you select this, IVE will send the user's authentication method as "token" if you use SAML and this credential will not be used in automatic SSO to backend applications.

Backup server

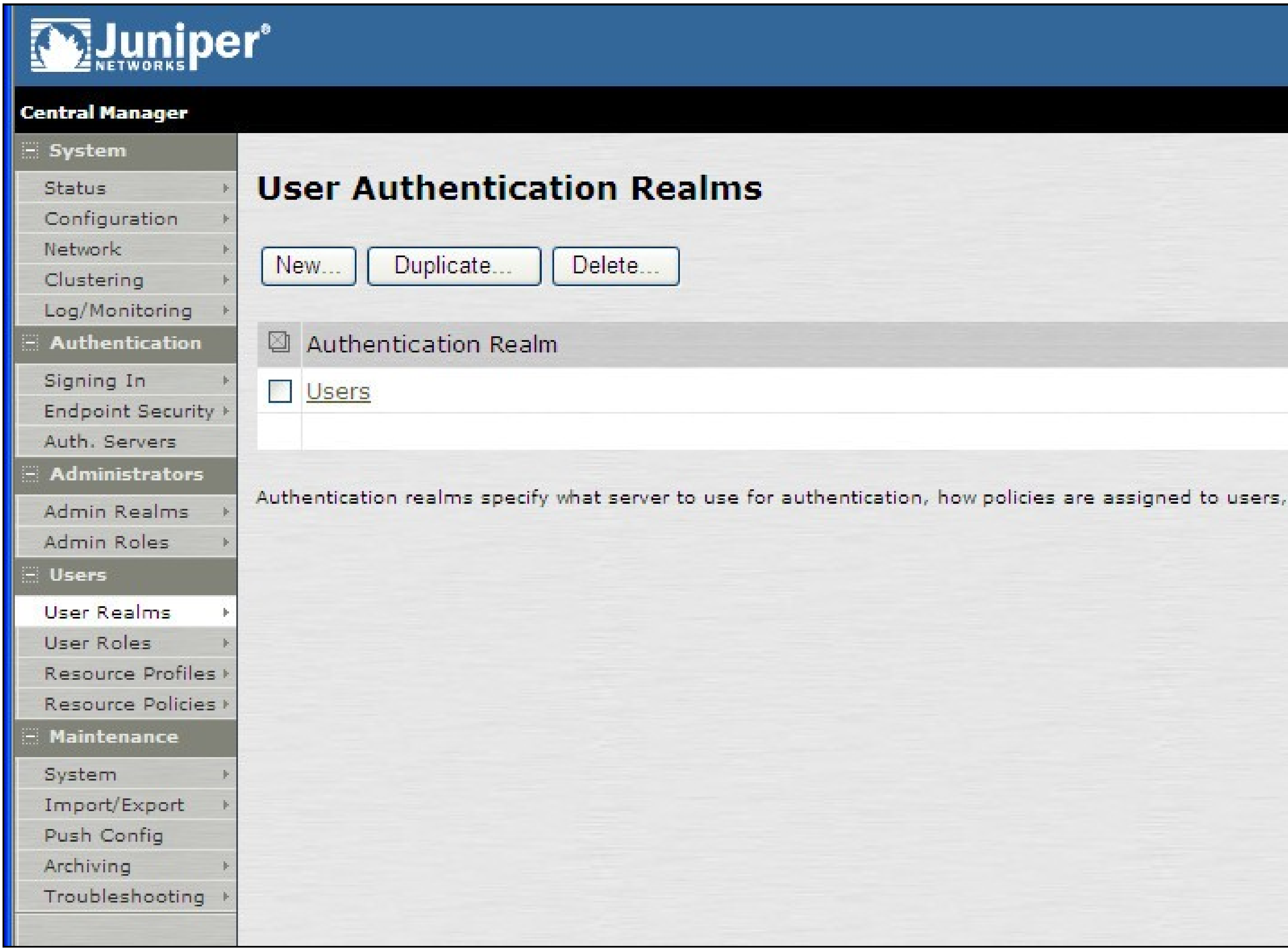
Radius Server:		Name or IP address
Authentication Port:		
Shared Secret:		
Accounting Port:		Port used for Radius accounting, if applicable

Radius accounting

NAS-Identifier:		Name of IVE as known to Radius s

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.



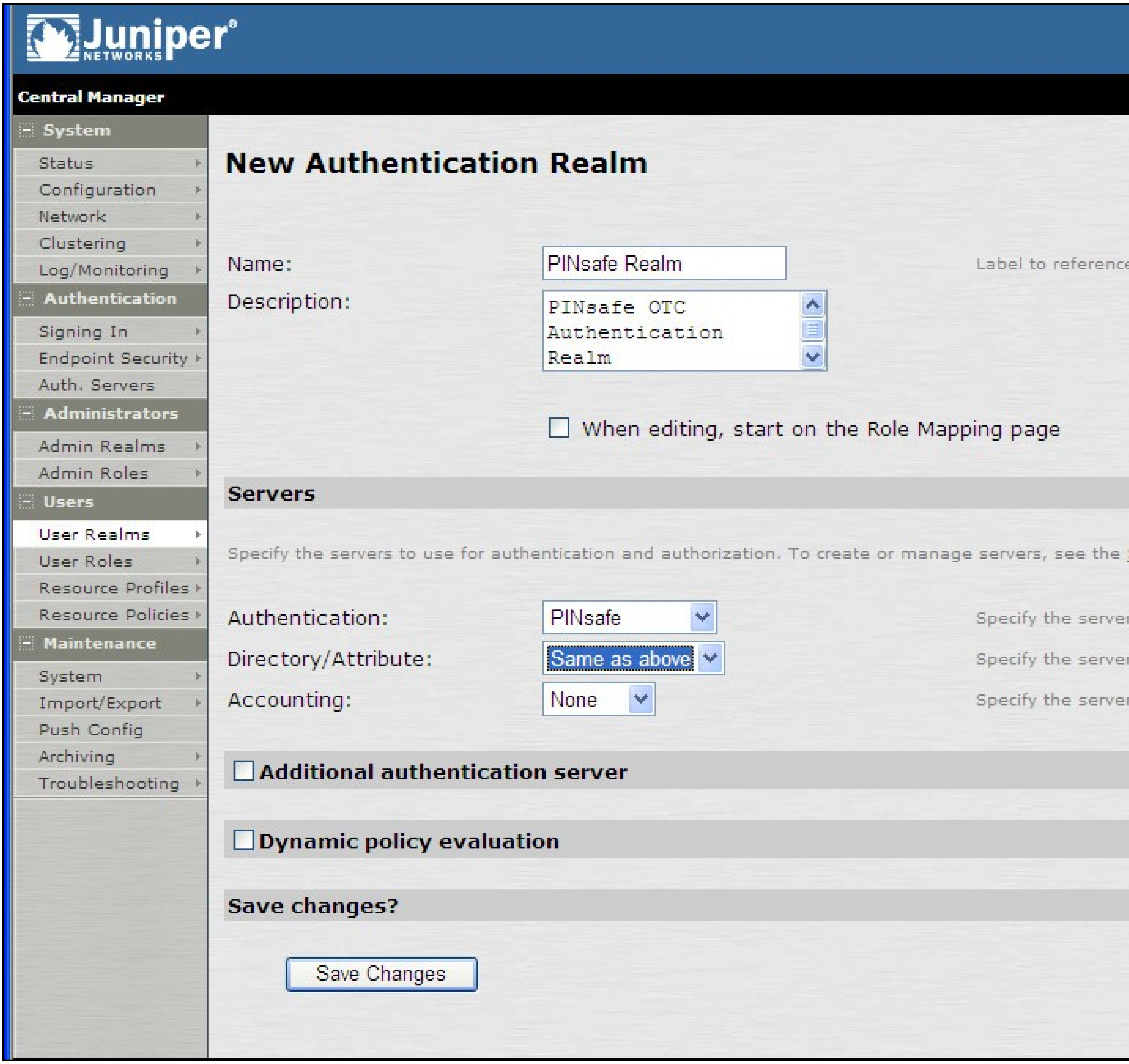
☒	Authentication Realm
□	Users

Authentication realms specify what server to use for authentication, how policies are assigned to users,

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.



New Authentication Realm

Name: PINsafe Realm

Label to referenc

Description: PINsafe OTC Authentication Realm

□ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the

Authentication: PINsafe

Specify the serve

Directory/Attribute: Same as above

Specify the serve

Accounting: None

Specify the serve

□ Additional authentication server

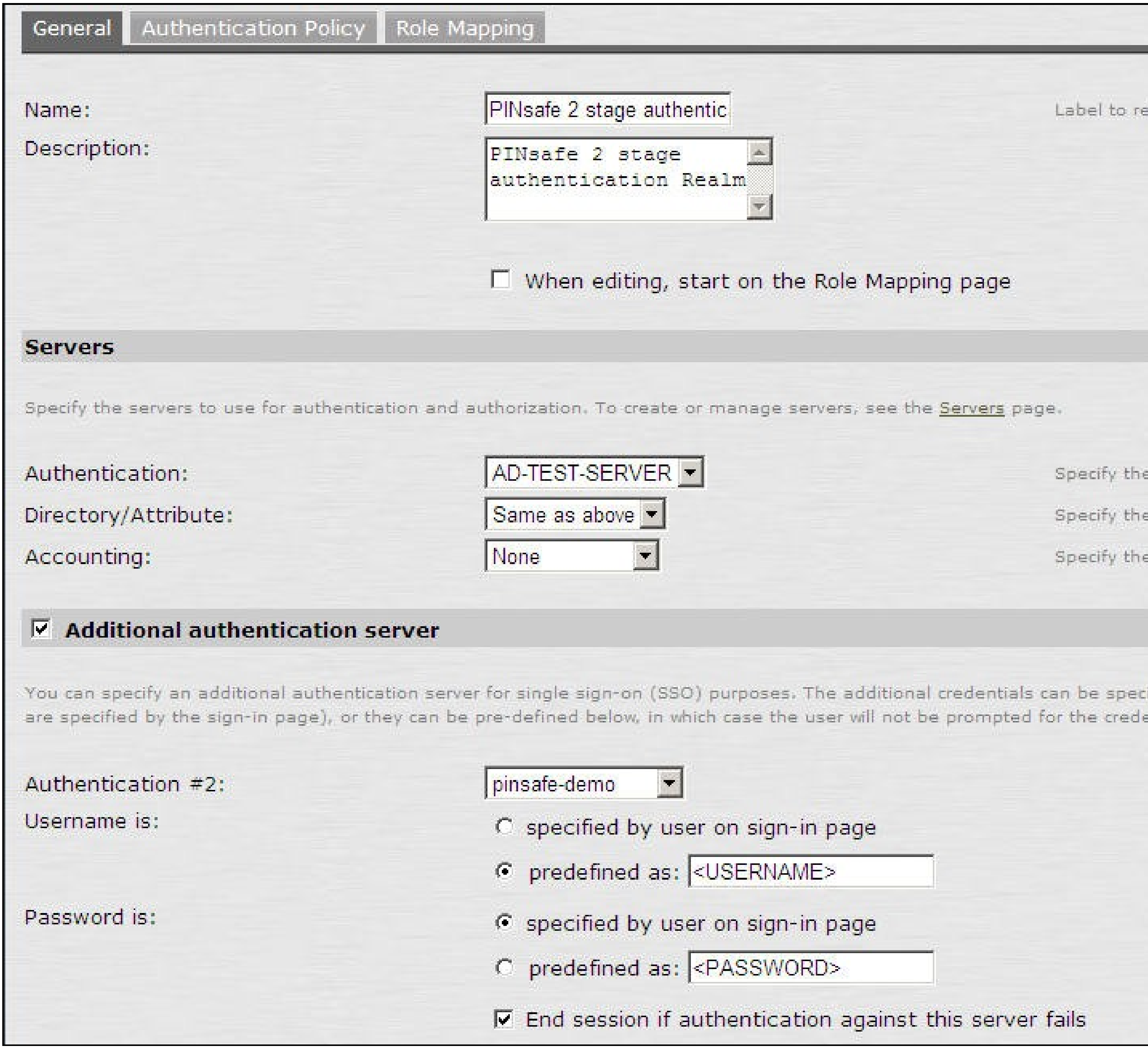
□ Dynamic policy evaluation

Save changes?

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**



General | Authentication Policy | Role Mapping

Name: PINsafe 2 stage authentic

Label to re

Description: PINsafe 2 stage authentication Realm

☐ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication: AD-TEST-SERVER

Specify the

Directory/Attribute: Same as above

Specify the

Accounting: None

Specify the

☑ **Additional authentication server**

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be spec
are specified by the sign-in page), or they can be pre-defined below, in which case the user will not be prompted for the crede

Authentication #2: pinsafe-demo

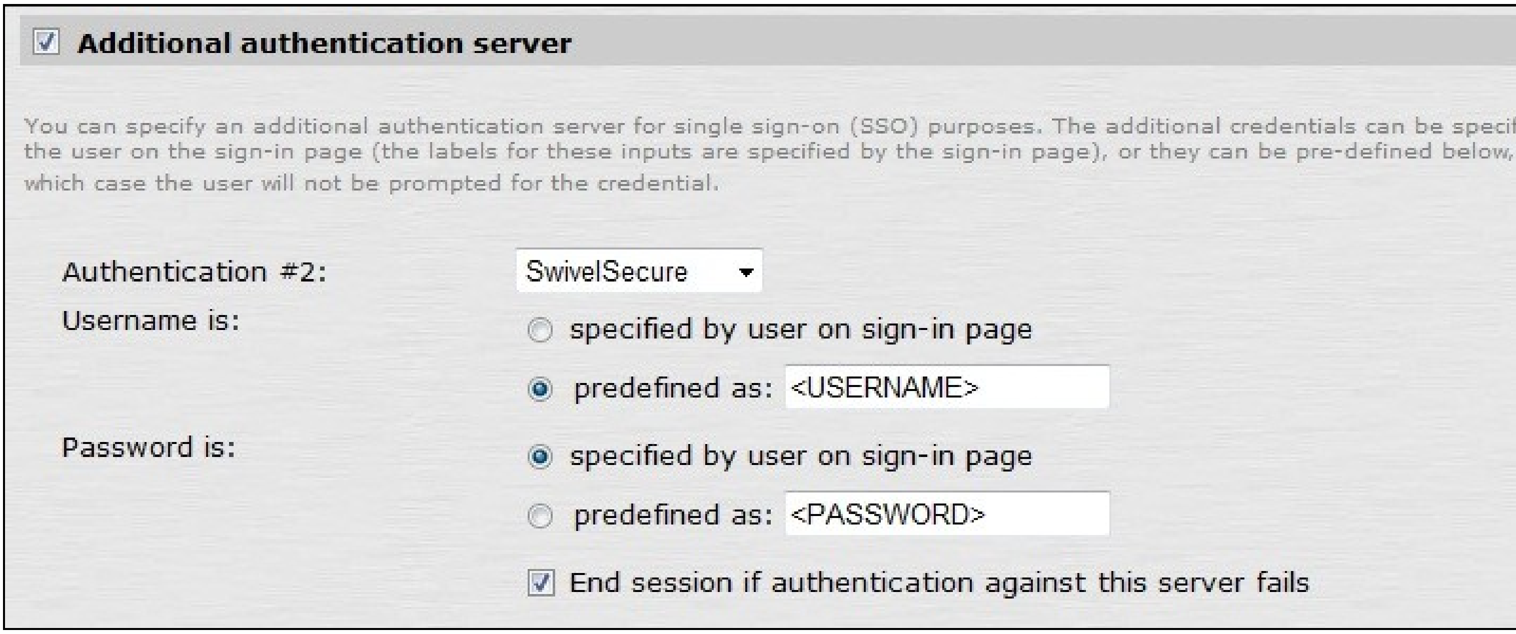
Username is:
○ specified by user on sign-in page
● predefined as: <USERNAME>

Password is:
● specified by user on sign-in page
○ predefined as: <PASSWORD>

☑ End session if authentication against this server fails

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.

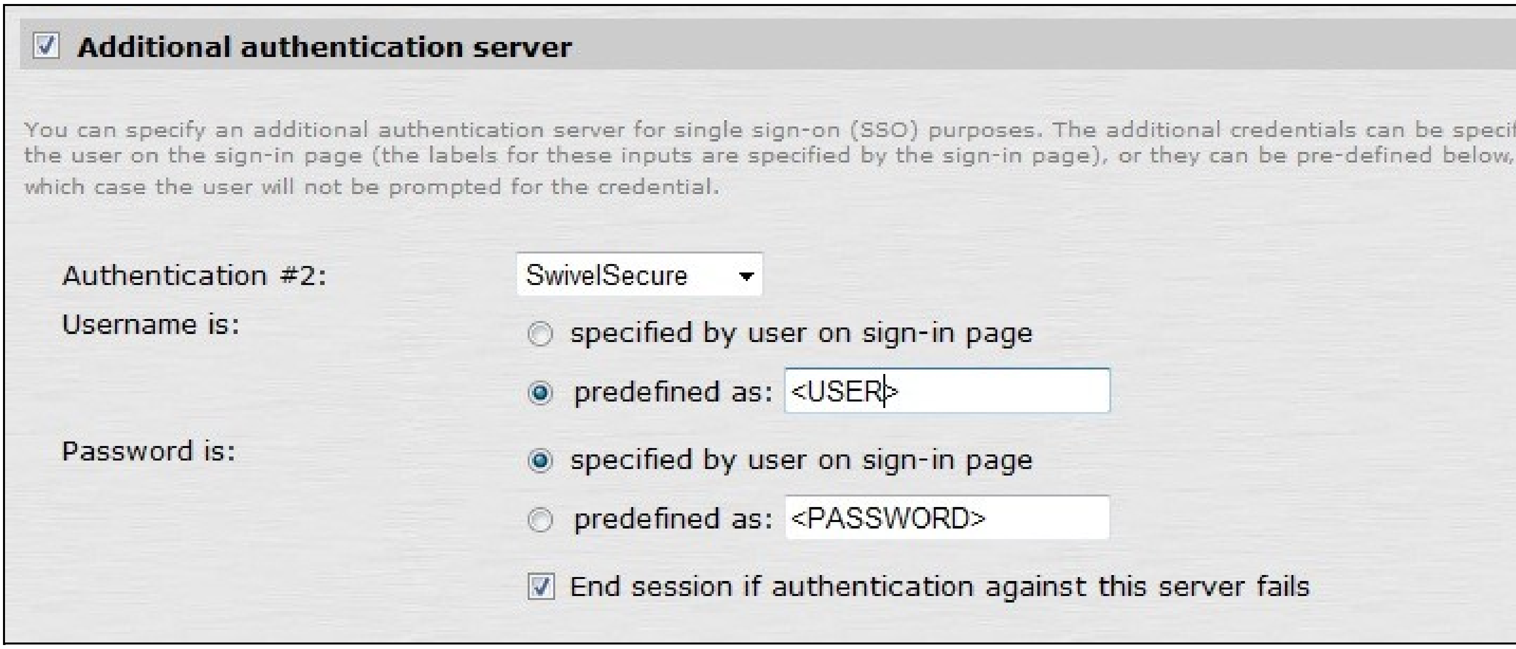
Authentication #2: SwivelSecure

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**

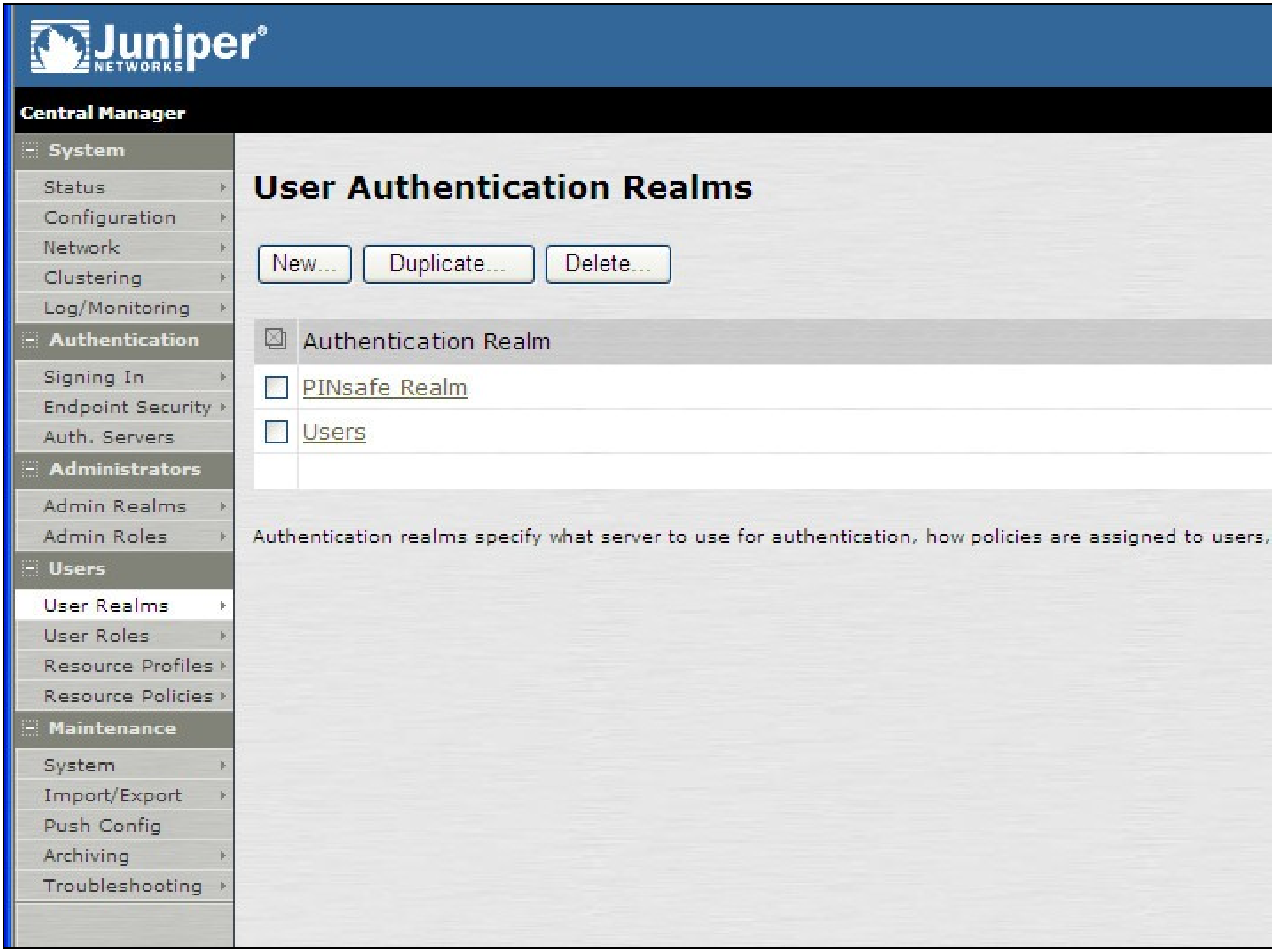
You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specif the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below, which case the user will not be prompted for 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



User Authentication Realms

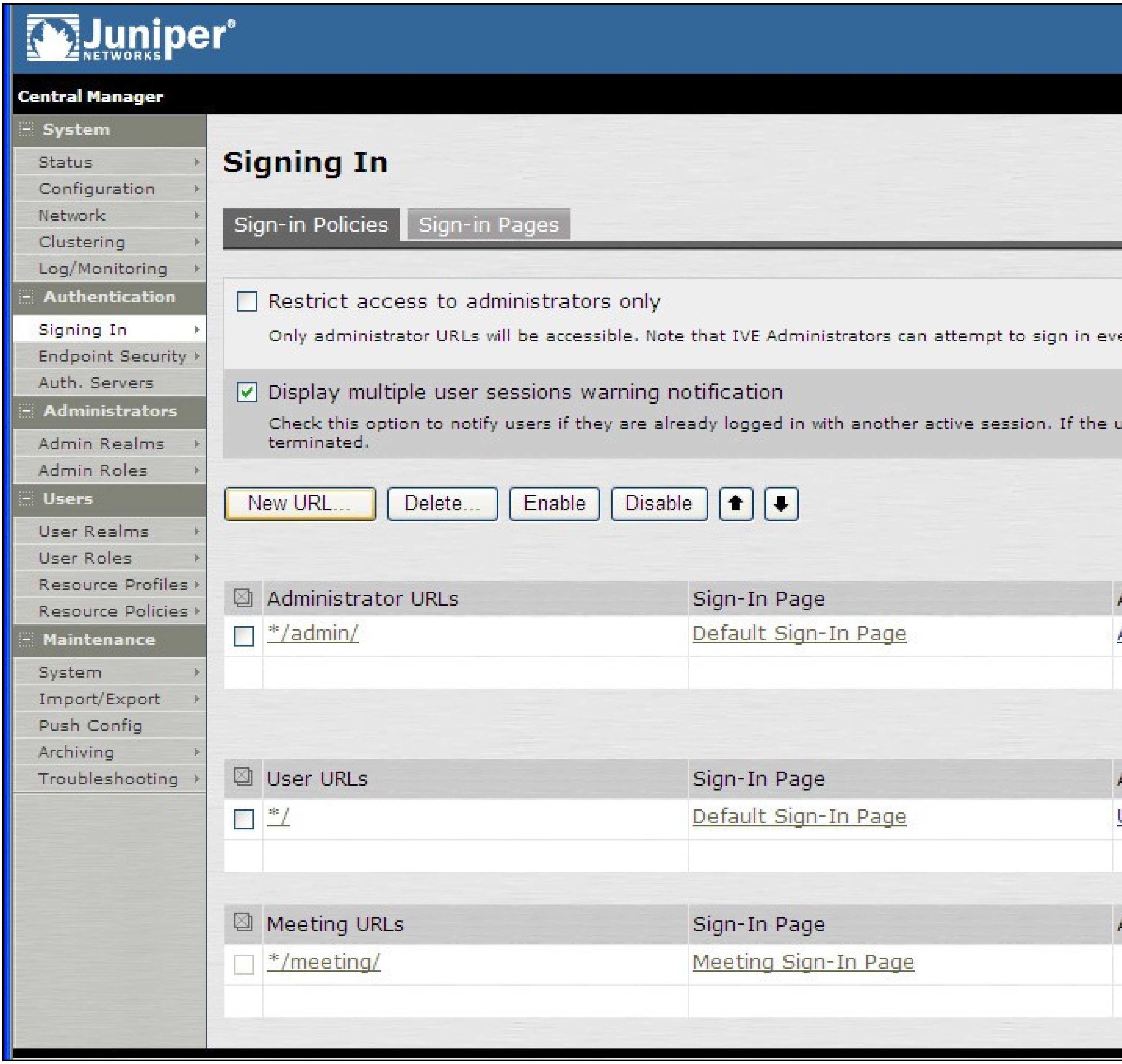
☒	Authentication Realm
□	PINsafe Realm
□	Users

Authentication realms specify what server to use for authentication, how policies are assigned to users,

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.



Signing In

□ 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

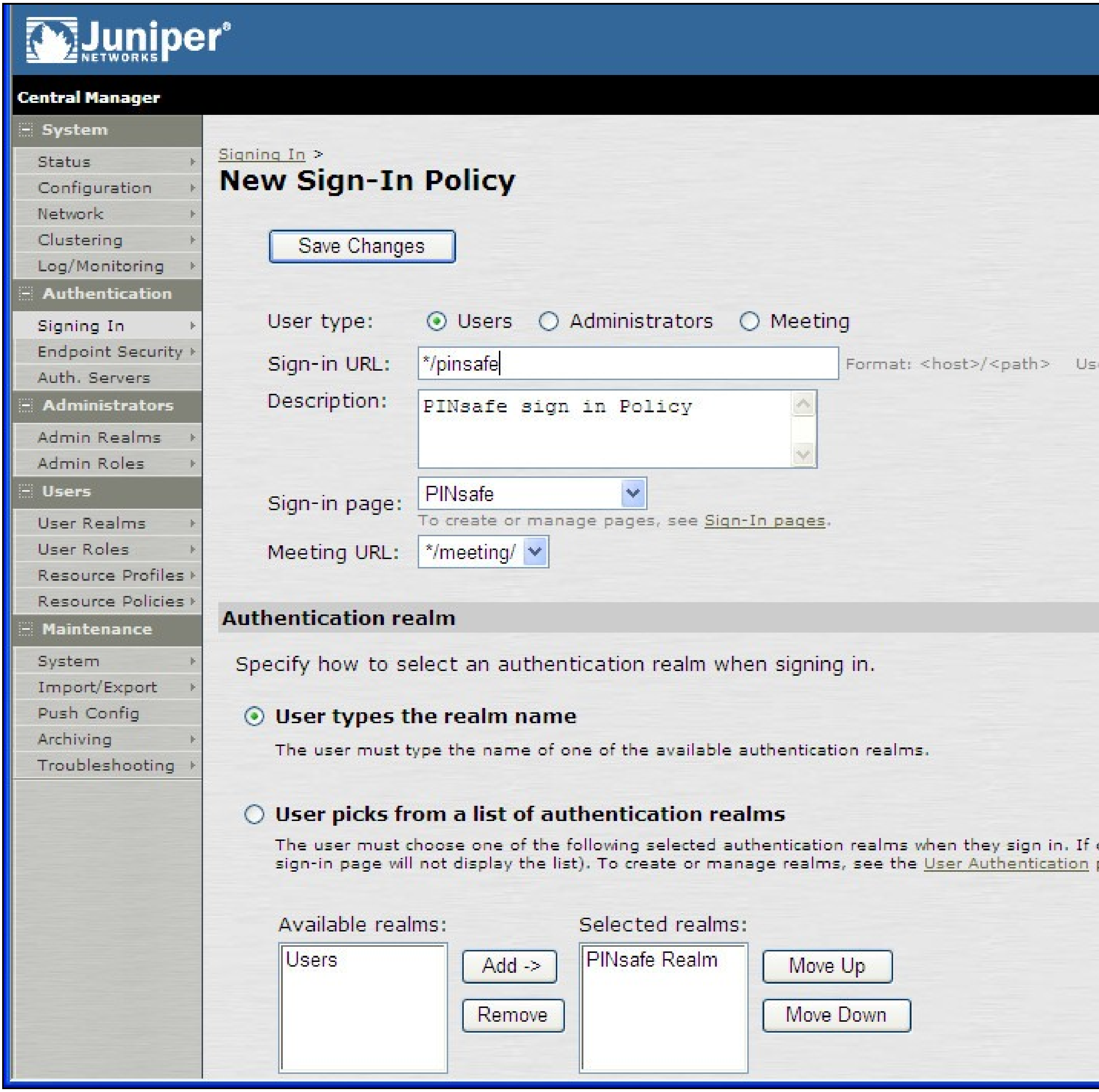
Check this option to notify users if they are already logged in with another active session. If the u terminated.

☒	Administrator URLs	Sign-In Page
□	*/admin/	Default Sign-In Page

☒	User URLs	Sign-In Page
□	*/	Default Sign-In Page

☒	Meeting URLs	Sign-In Page
□	*/meeting/	Meeting Sign-In Page

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.



New Sign-In Policy

User type: ● Users ○ Administrators ○ Meeting

Sign-in URL: */pinsafe Format: <host>/<path> Us

Description: PINsafe sign in Policy

Sign-in page: PINsafe

To create or manage pages, see Sign-In pages.

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

● User types the realm name

The user must type the name of one of the available authentication realms.

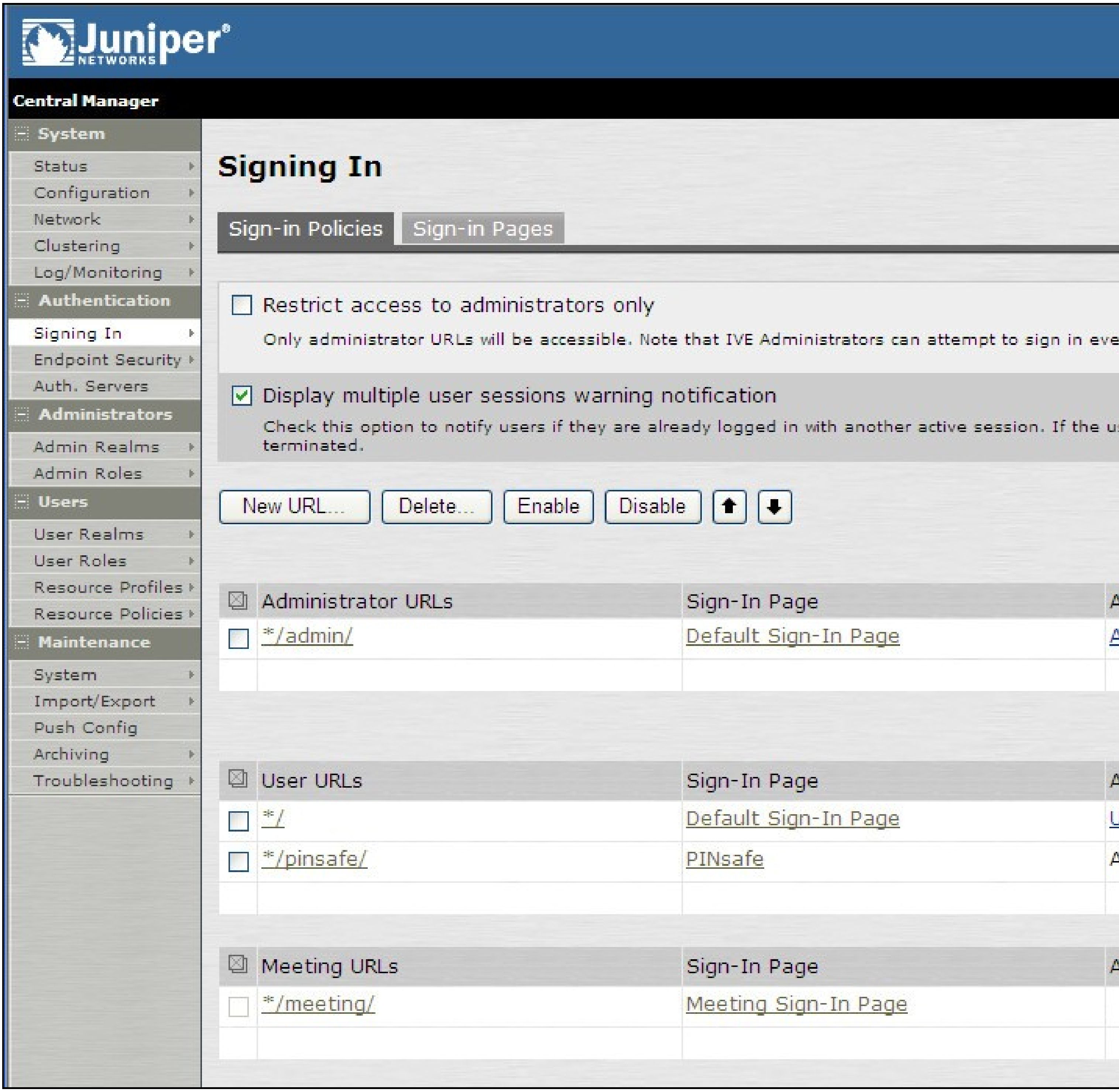
○ User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If
sign-in page will not display the list). To create or manage realms, see the User Authentication

Available realms: Users

Selected realms: PINsafe Realm

When complete the new Swivel policy should be listed.



Signing In

☐ 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.

☒	Administrator URLs	Sign-In Page	A
☐	*/admin/	Default Sign-In Page	A

☒	User URLs	Sign-In Page	A
☐	*/	Default Sign-In Page	U
☐	*/pinsafe/	PINsafe	A

☒	Meeting URLs	Sign-In Page	A
☐	*/meeting/	Meeting Sign-In Page	

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

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:

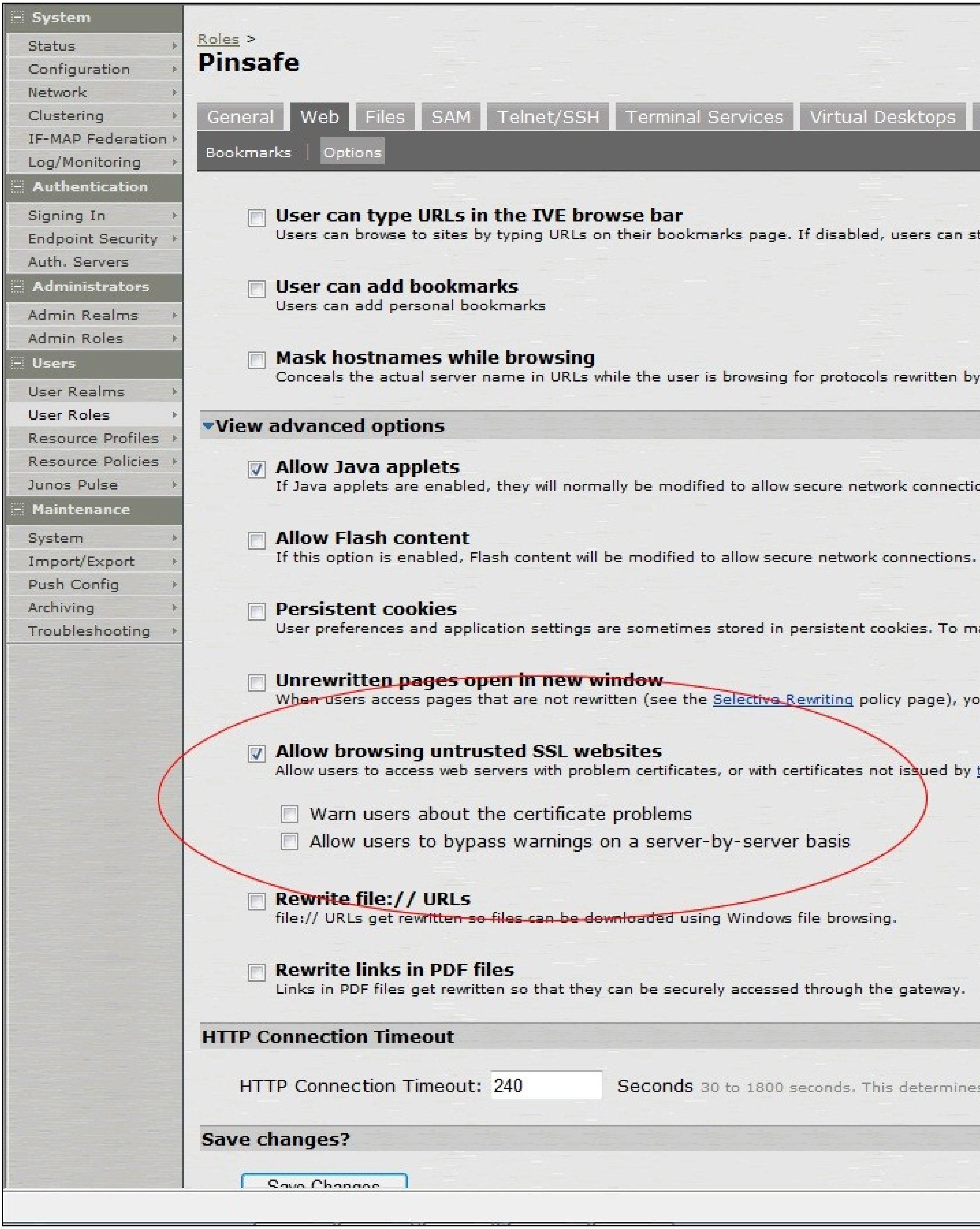
Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

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

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*.



Pinsafe

□ **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 connectic

□ **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 m

□ **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?

Creating an ACL for the Virtual hostname role

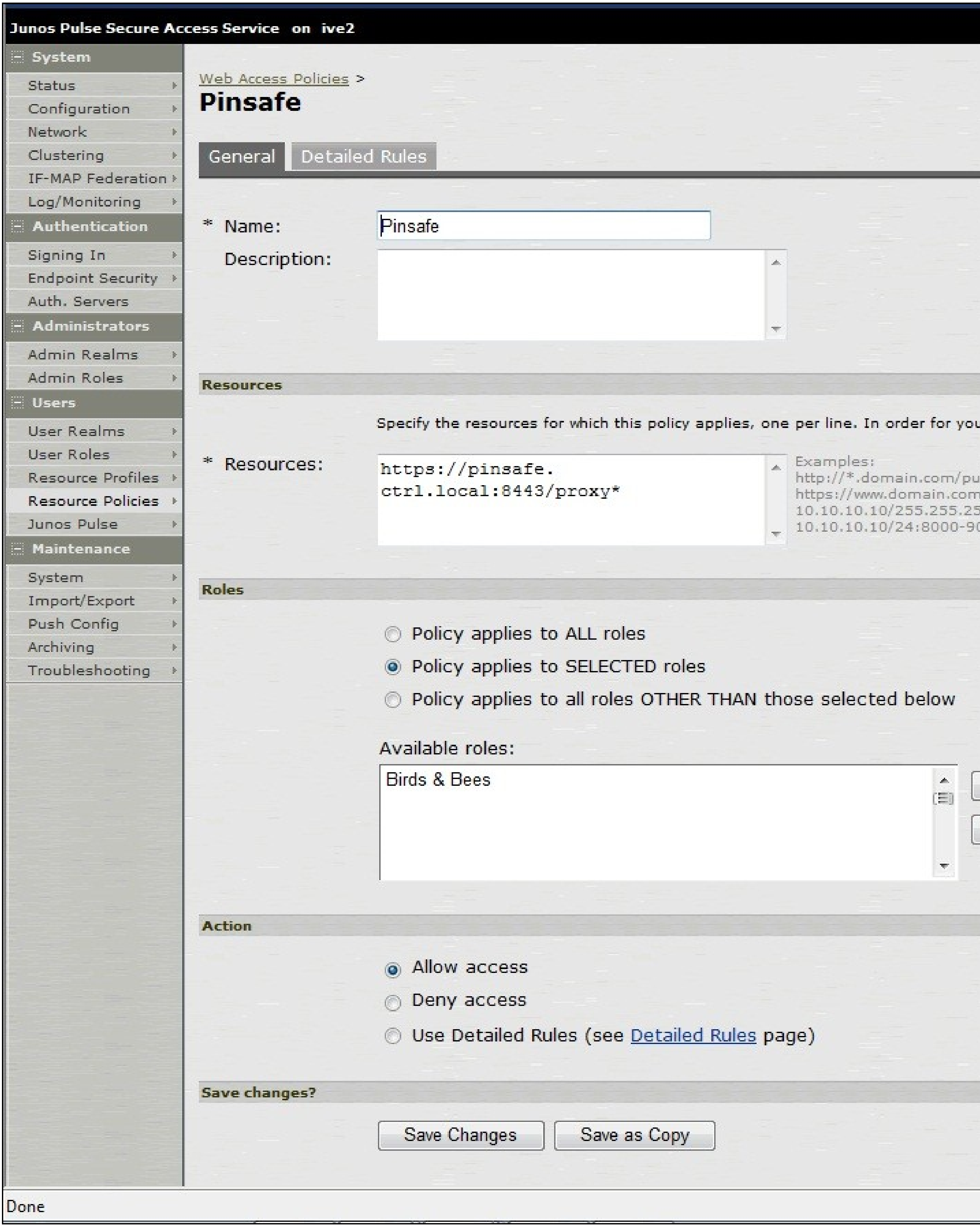
An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

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.



Pinsafe

* 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?

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

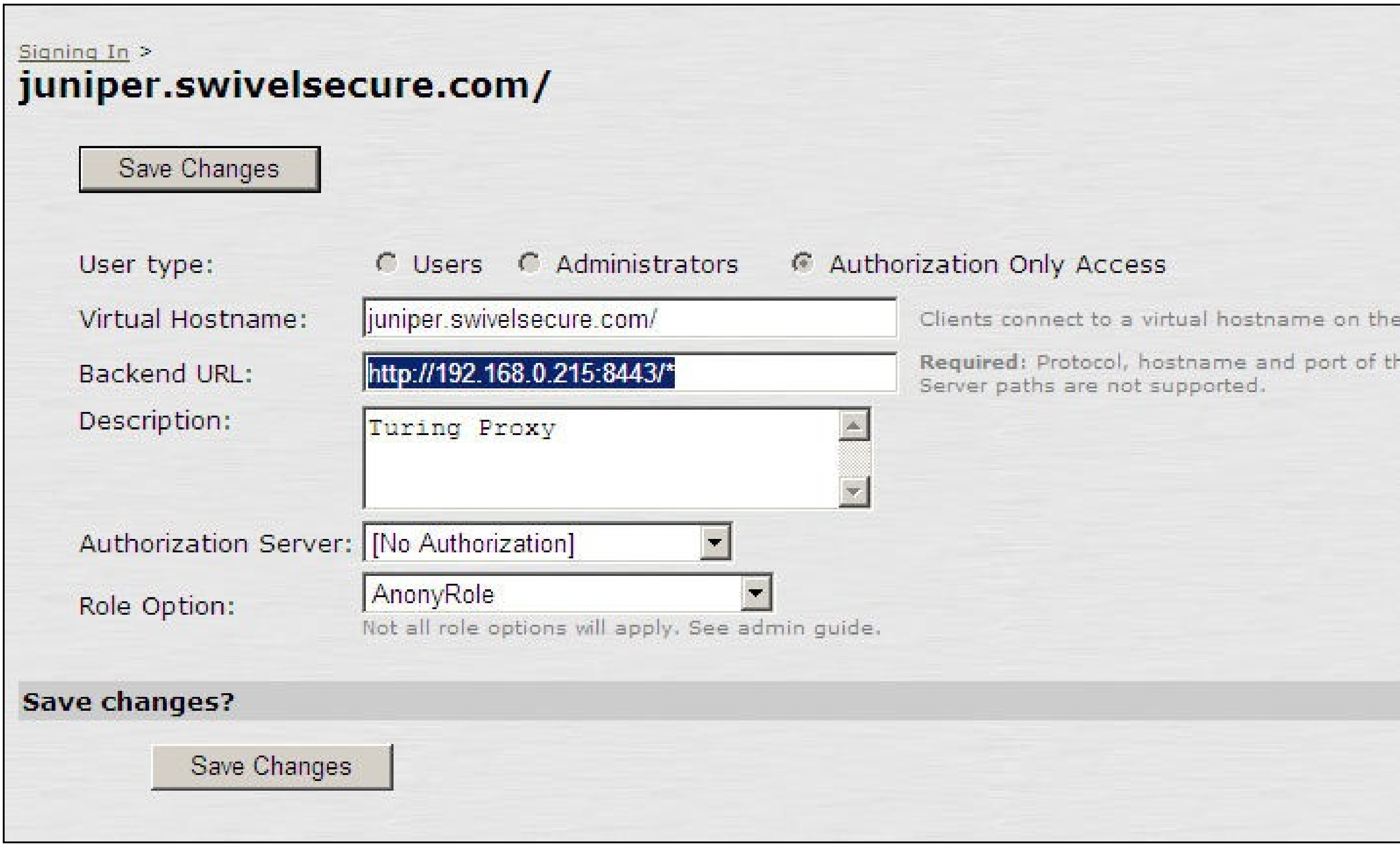
Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes



Signing In >

juniper.swivelsecure.com/

Save Changes

User type: ○ Users ○ Administrators ● Authorization Only Access

Virtual Hostname: juniper.swivelsecure.com/ Clients connect to a virtual hostname on the

Backend URL: http://192.168.0.215:8443/* **Required:** Protocol, hostname and port of th Server paths are not supported.

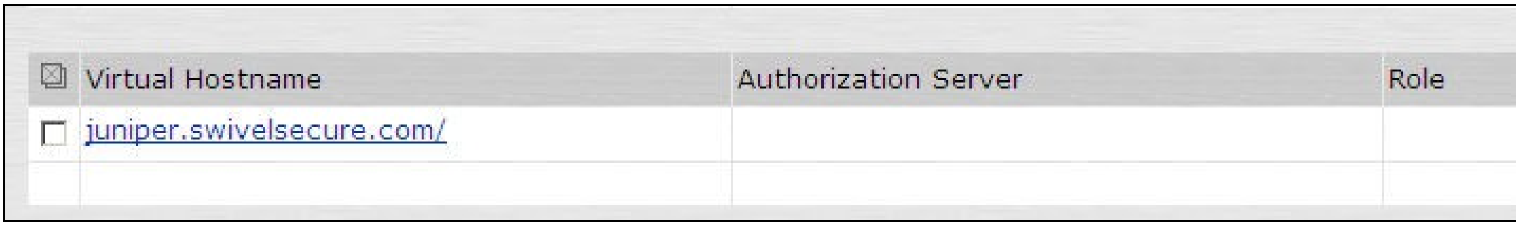
Description: Turing Proxy

Authorization Server: [No Authorization]

Role Option: AnonyRole Not all role options will apply. See admin guide.

Save changes?

Save Changes



☒	Virtual Hostname	Authorization Server	Role
□	juniper.swivelsecure.com/		

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

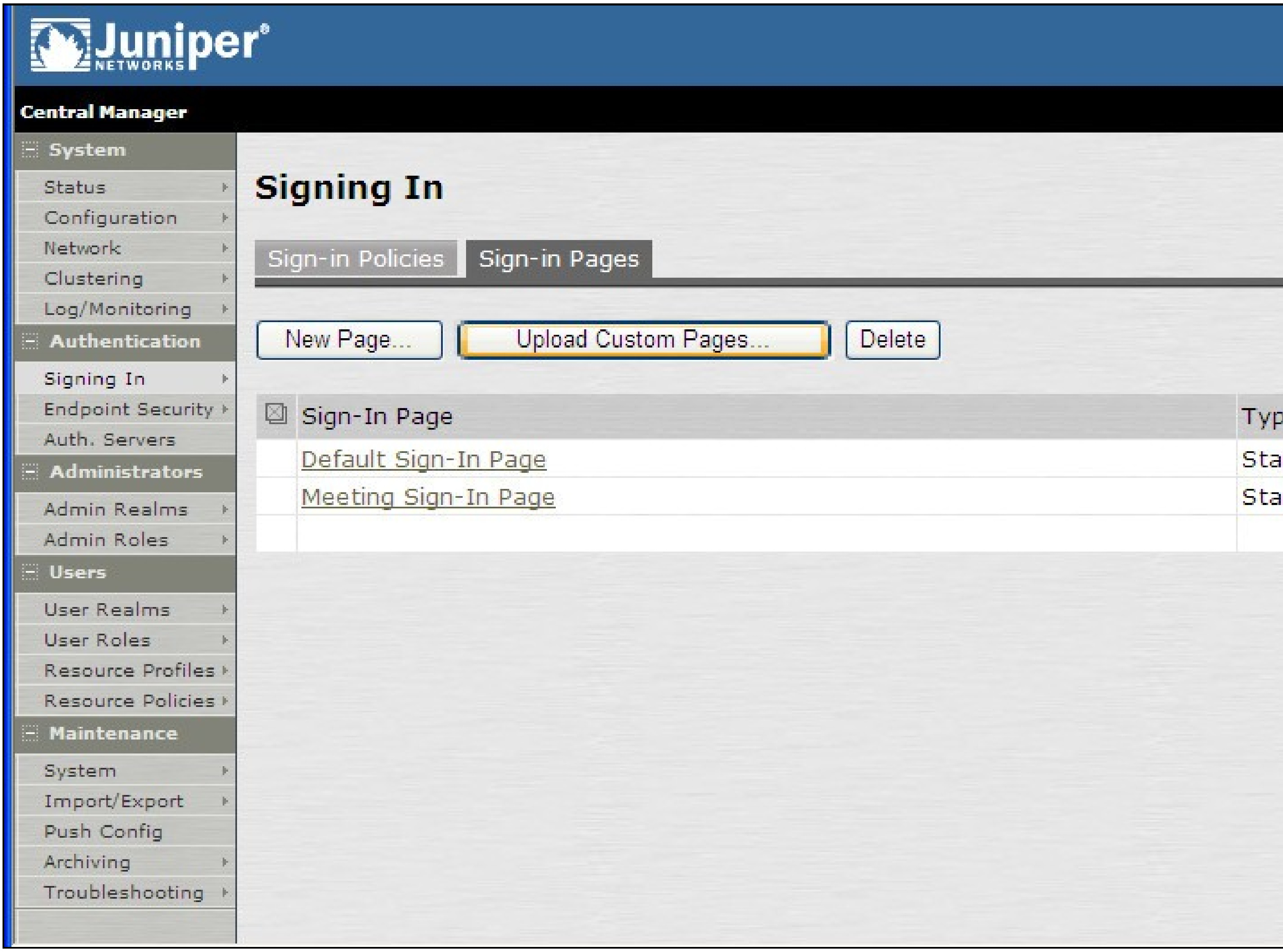
For a software only install see Software Only Installation

Then verify the external access using

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

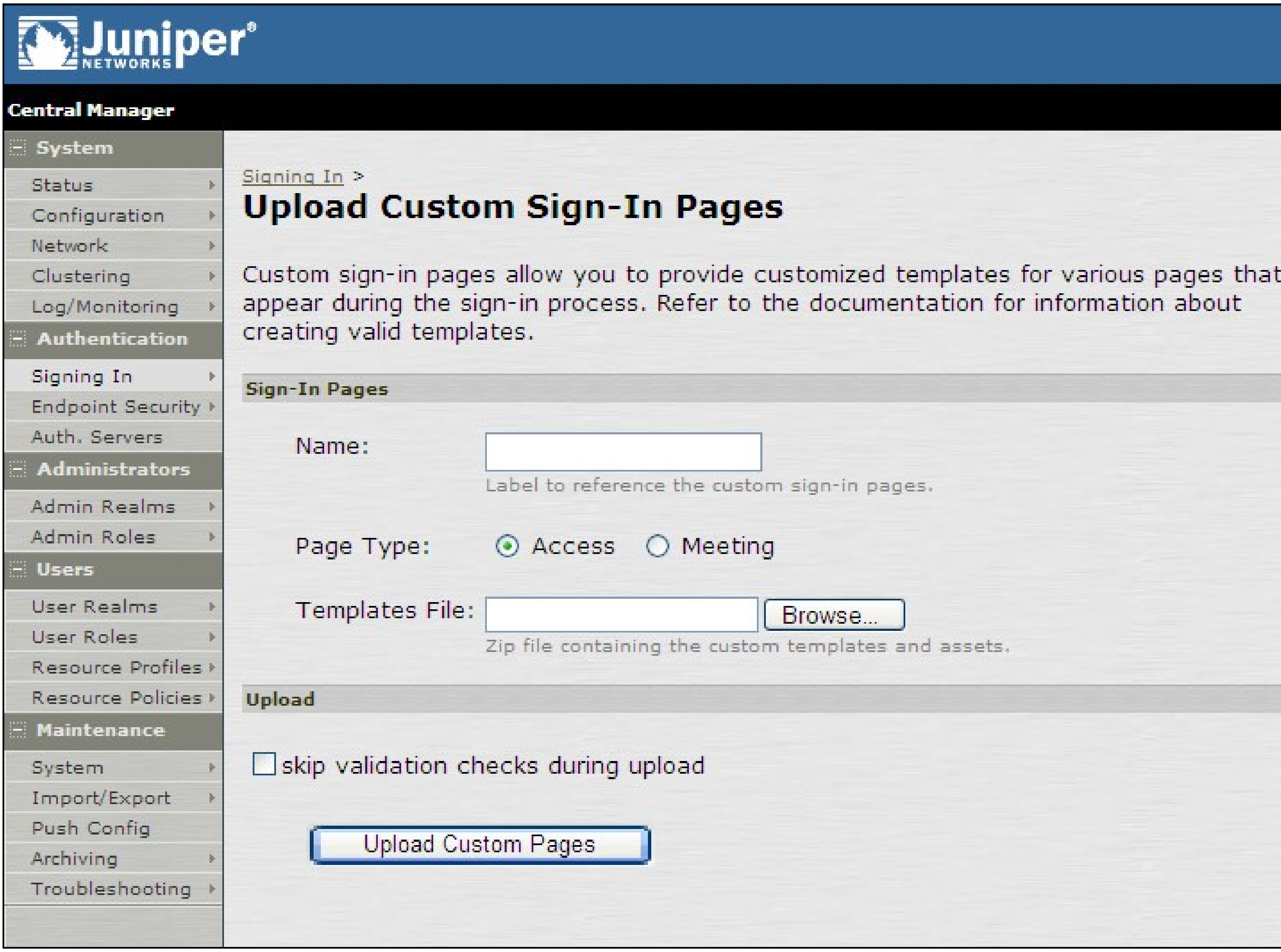
Login Page Modifications for Single Channel Authentication and SMS On Demand

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.



☒	Sign-In Page	Typ
	Default Sign-In Page	Sta
	Meeting Sign-In Page	Sta

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.



Signing In >

Upload Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-In Pages

Name:

Label to reference the custom sign-in pages.

Page Type: ● Access ○ Meeting

Templates File: Browse...

Zip file containing the custom templates and assets.

Upload

□ skip validation checks during upload

Upload Custom Pages

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.

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

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"

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

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.

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

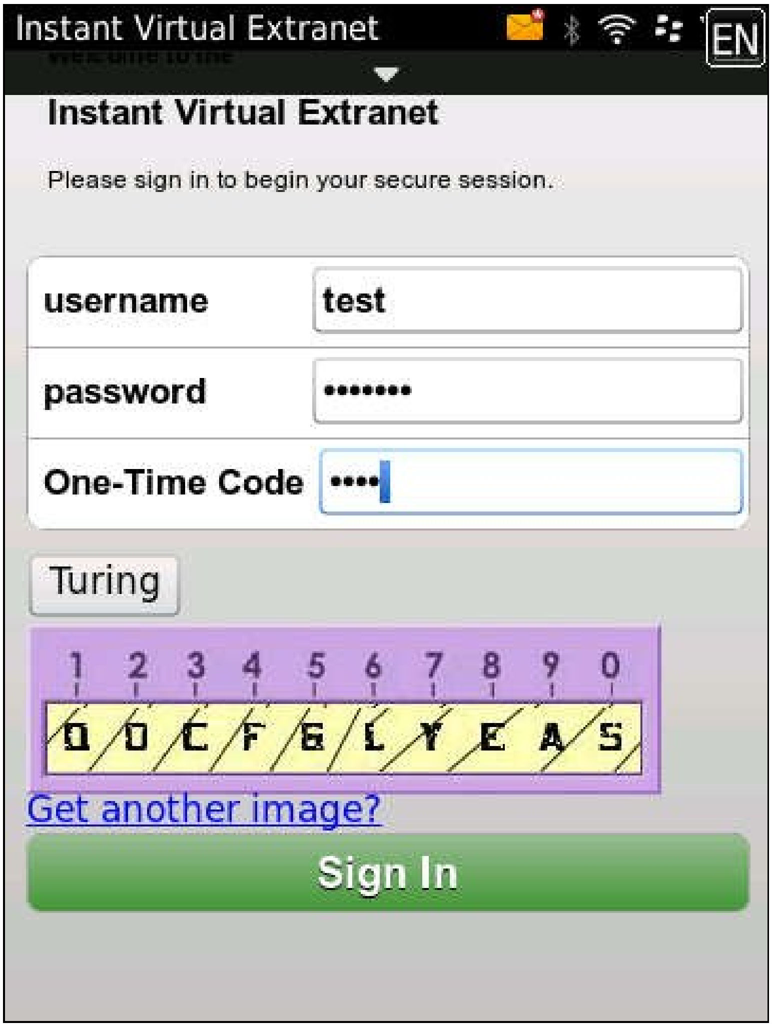
```
var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";
```

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=";



Instant Virtual Extranet

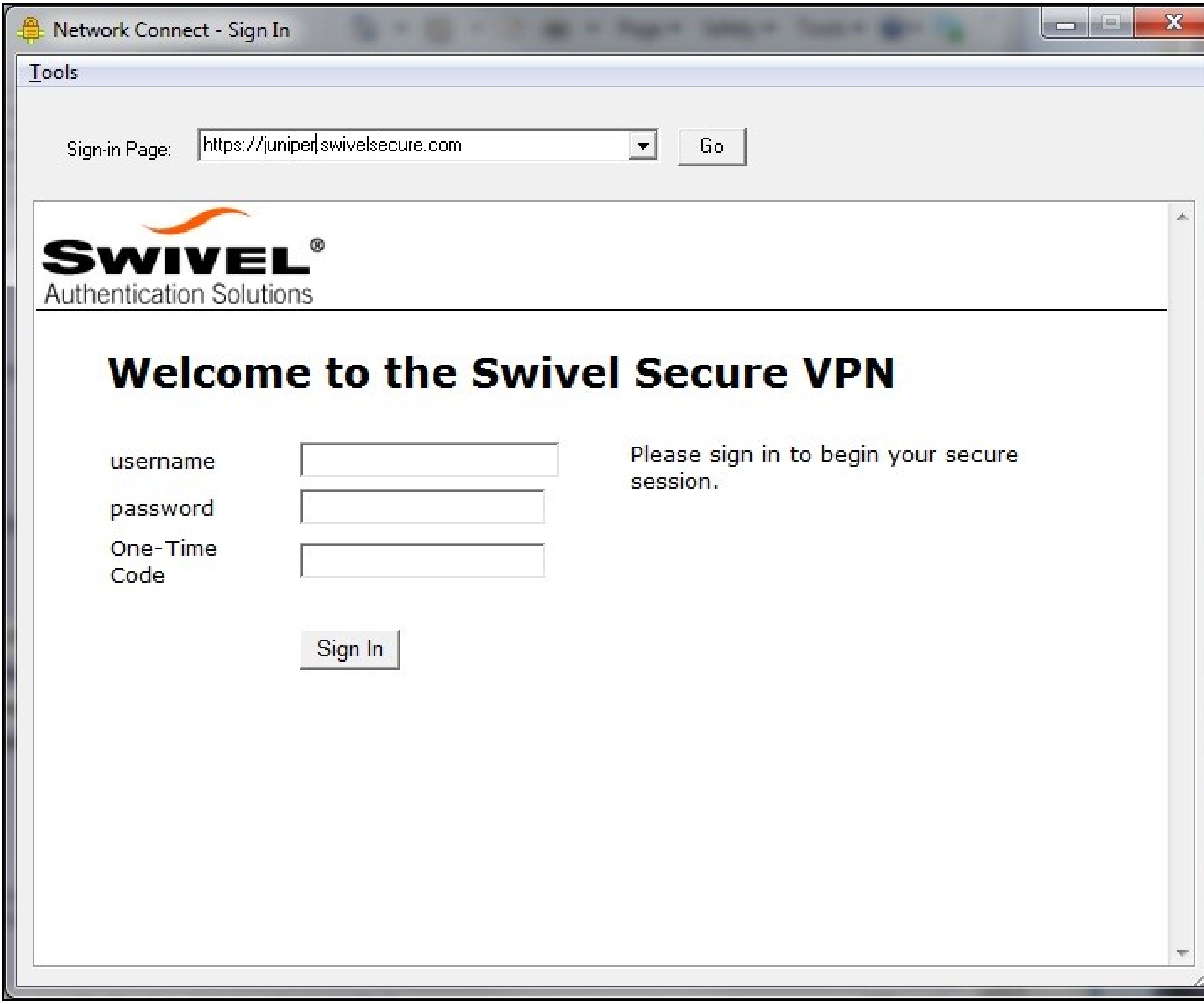
Please sign in to begin your secure session.

username	test
password	••••••••
One-Time Code	••••

1	2	3	4	5	6	7	8	9	0
Q	D	C	F	G	L	Y	E	A	S

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



https://juniper.swivelsecure.com

Welcome to the Swivel Secure VPN

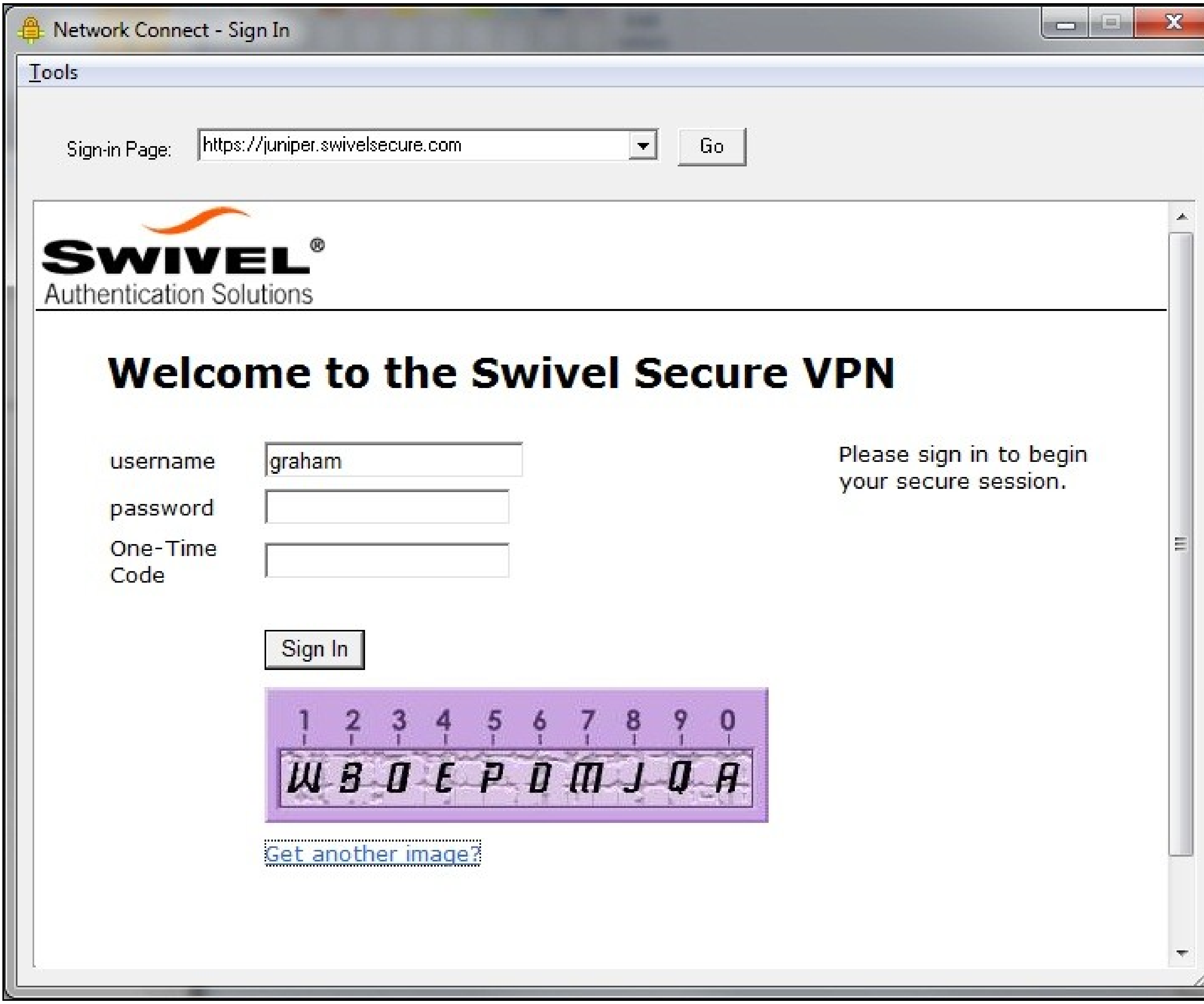
username

password

One-Time Code

Please sign in to begin your secure session.

Juniper Network Connect with TURing



Sign-in Page: https://juniper.swivelsecure.com

Welcome to the Swivel Secure VPN

username: graham

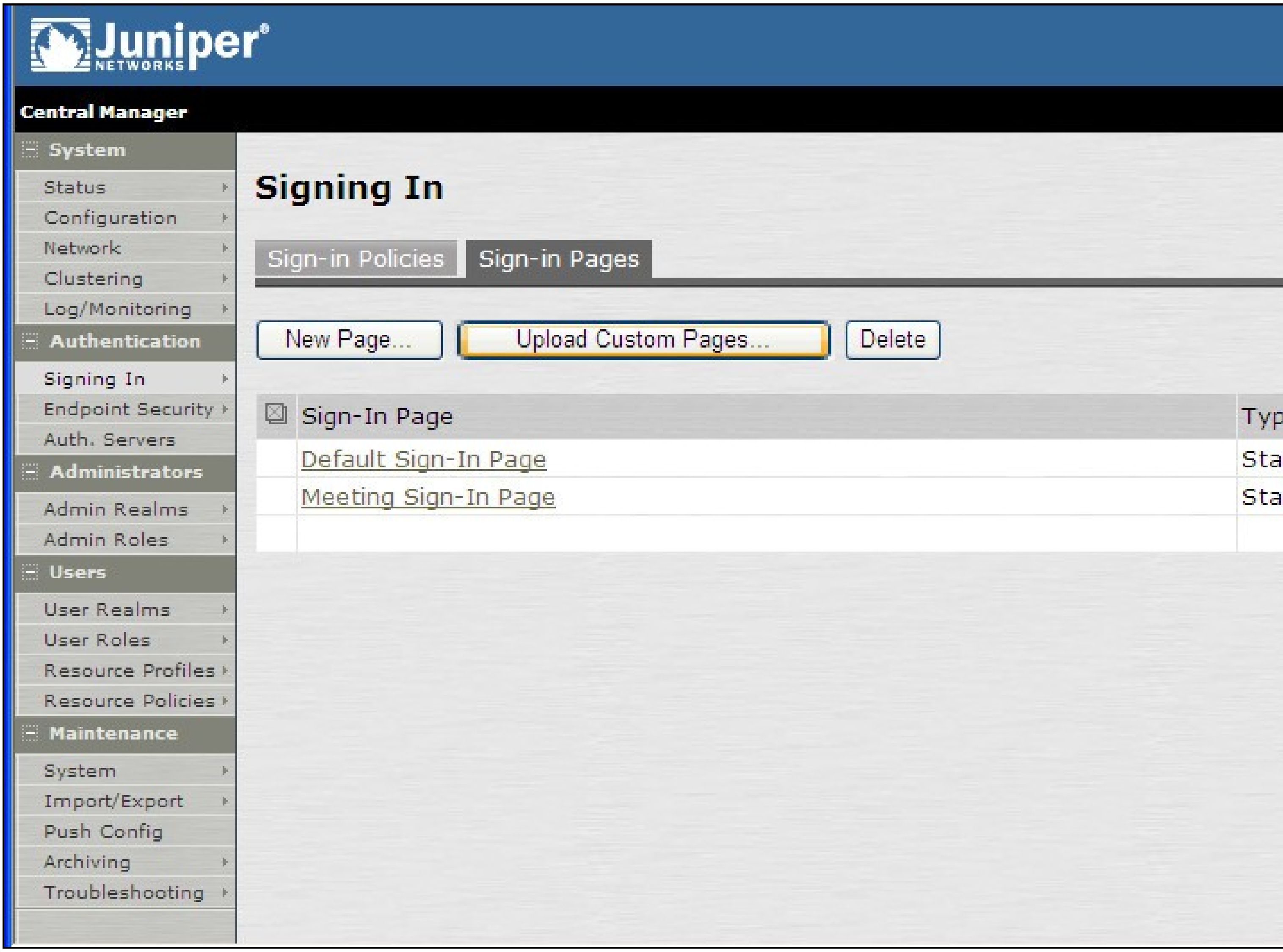
password:

One-Time Code:

Please sign in to begin your secure session.

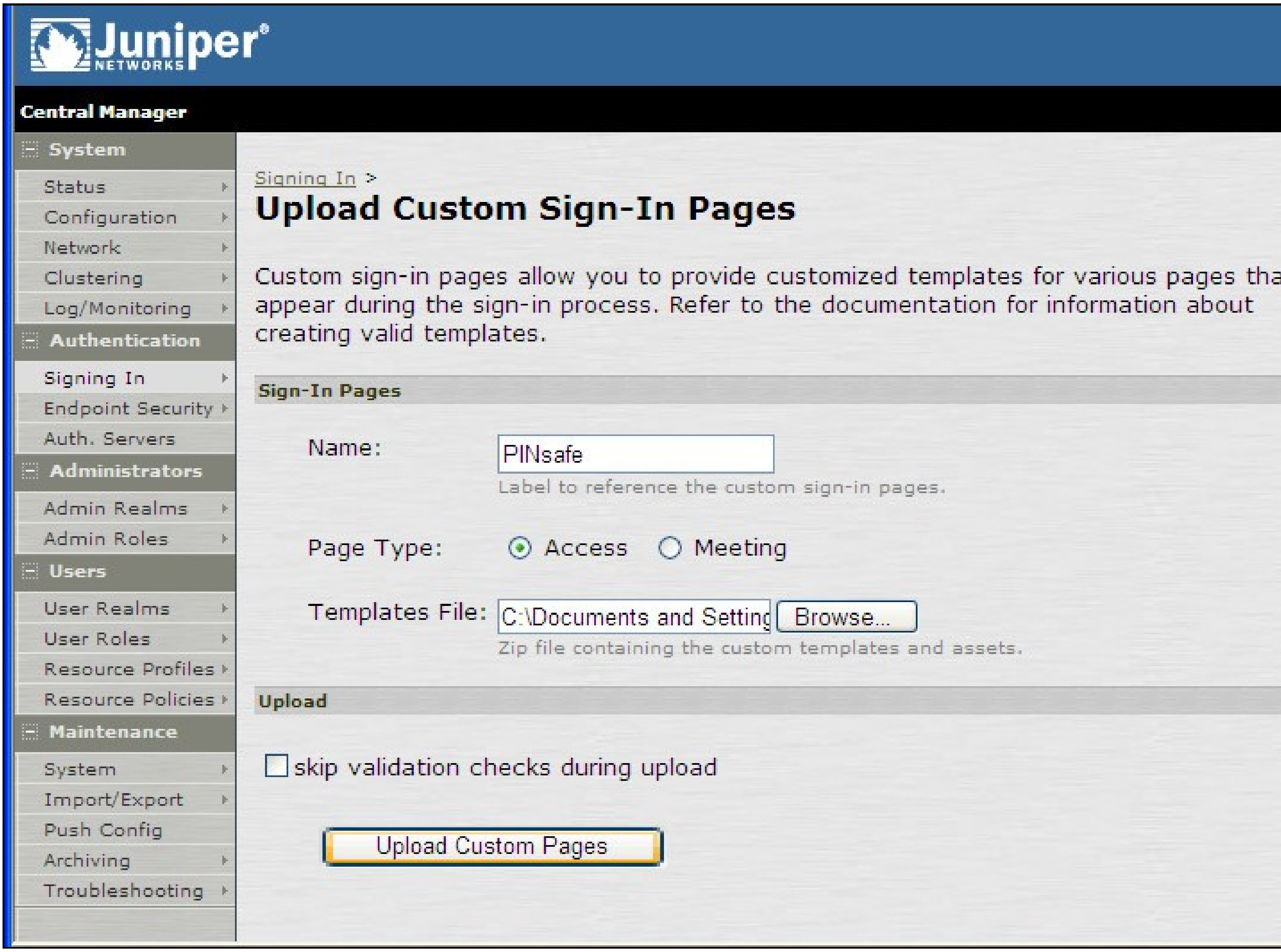
Uploading the Modified Page

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.



☒	Sign-In Page	Typ
	Default Sign-In Page	Sta
	Meeting Sign-In Page	Sta

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.



Signing In >

Upload Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages tha
appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-In Pages

Name: PINsafe
Label to reference the custom sign-in pages.

Page Type: ● Access ○ Meeting

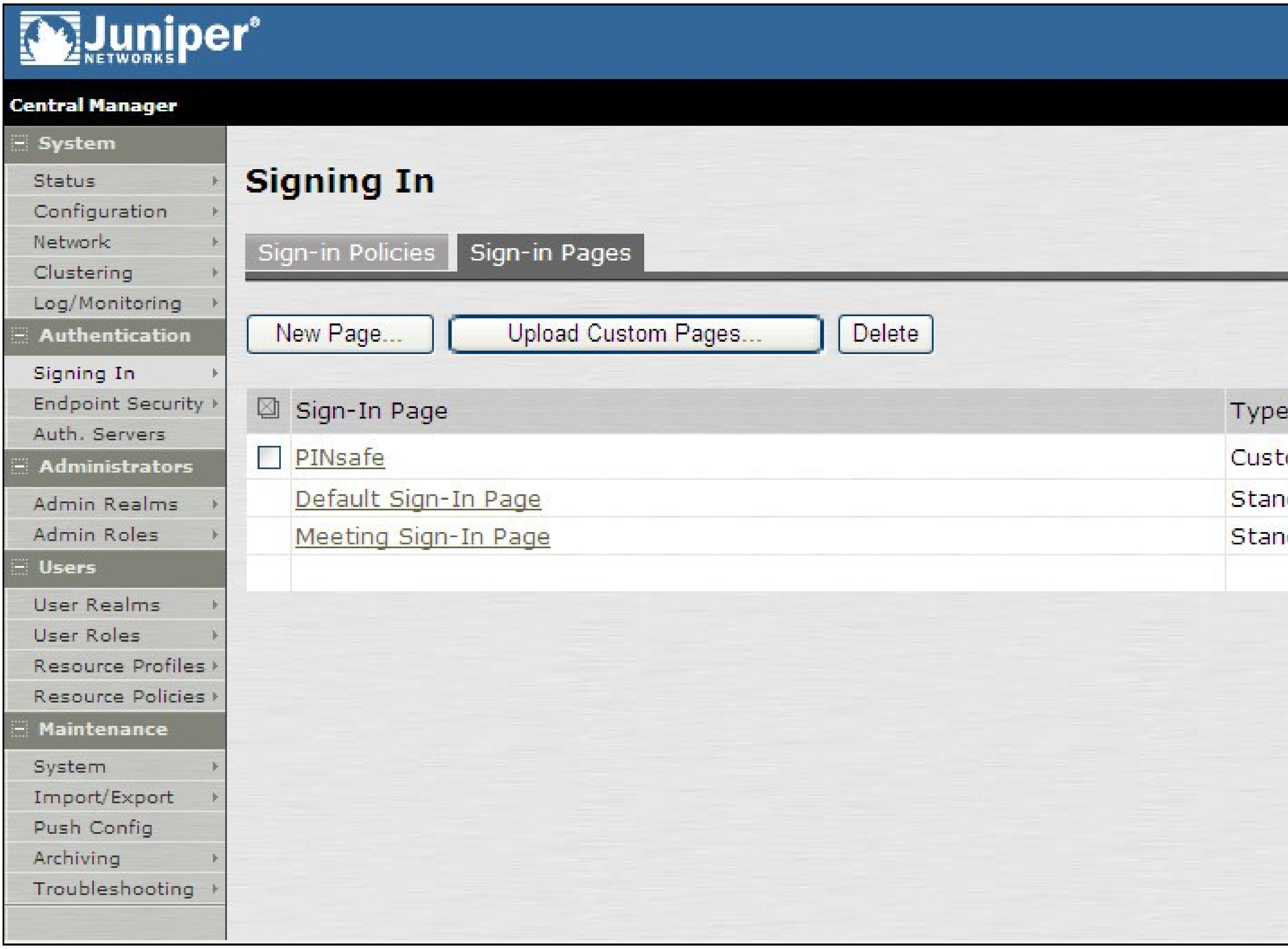
Templates File: C:\Documents and Setting [Browse...]
Zip file containing the custom templates and assets.

Upload

□ skip validation checks during upload

[Upload Custom Pages]

The new signing in page should be listed.

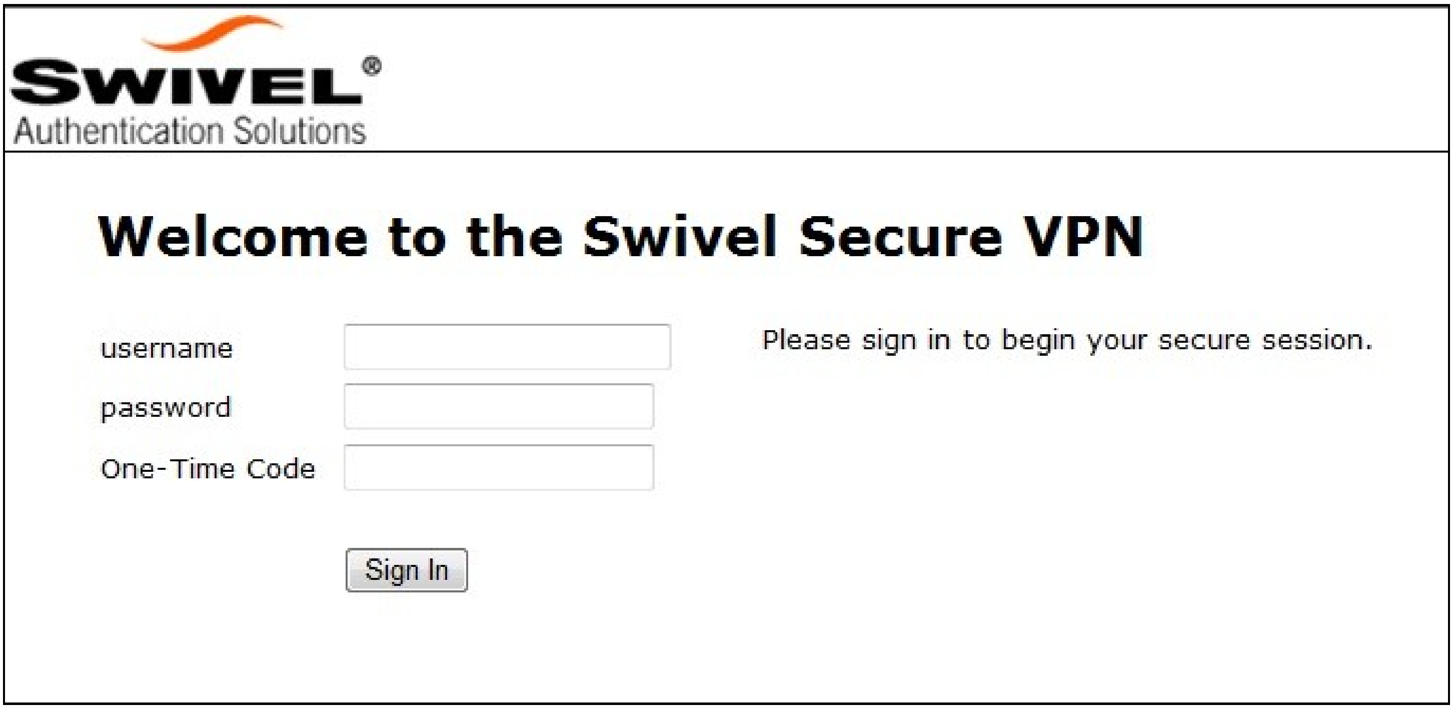


☒	Sign-In Page	Type
□	PINsafe	Custo
	Default Sign-In Page	Stan
	Meeting Sign-In Page	Stan

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



Welcome to the Swivel Secure VPN

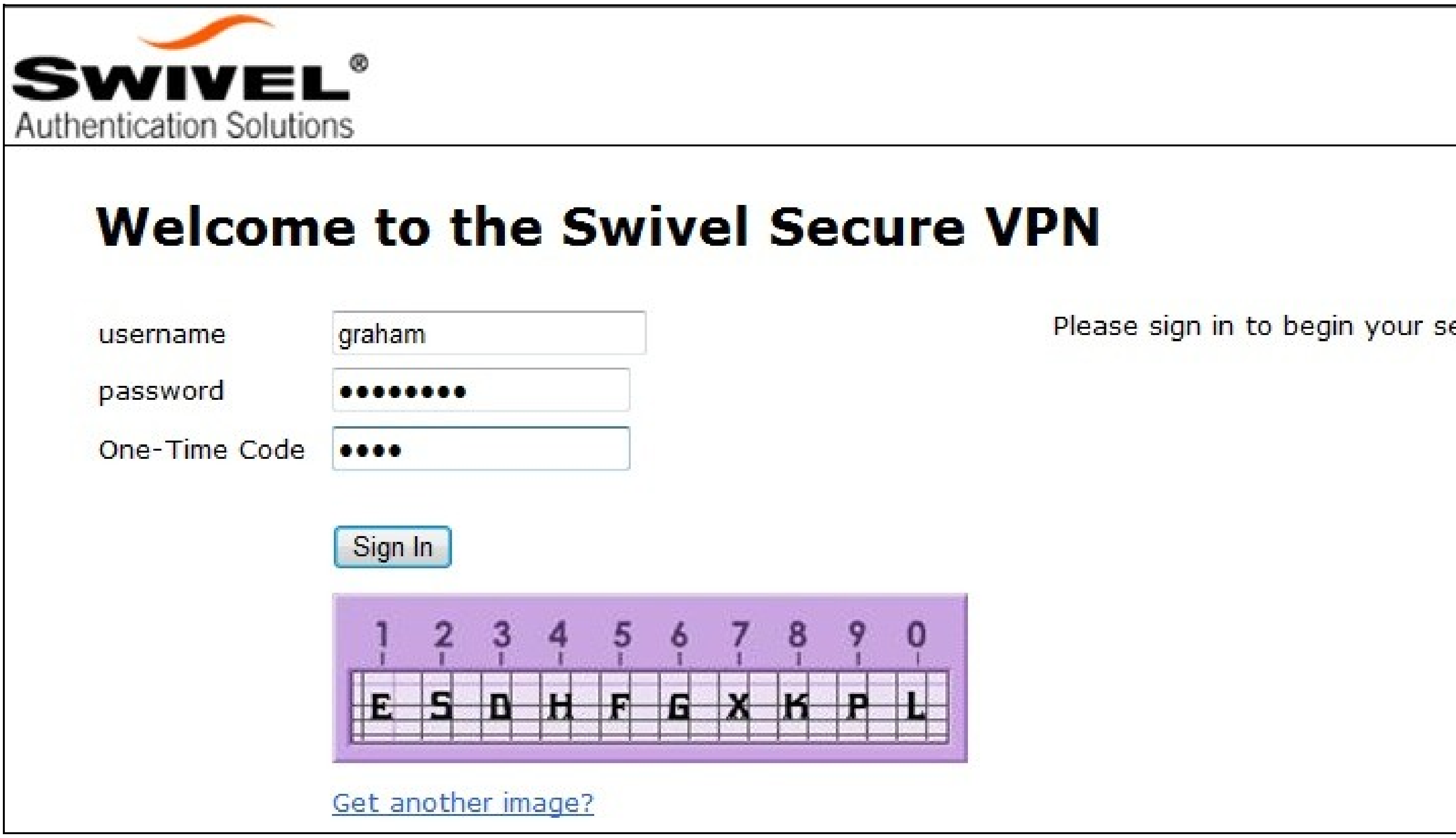
username

password

One-Time Code

Please sign in to begin your secure session.

Single Channel Authentication



Welcome to the Swivel Secure VPN

username graham

password ●●●●●●●●●

One-Time Code ●●●●

Please sign in to begin your se

1	2	3	4	5	6	7	8	9	0
E	S	D	H	F	G	X	K	P	L

Uninstalling the Swivel Integration

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

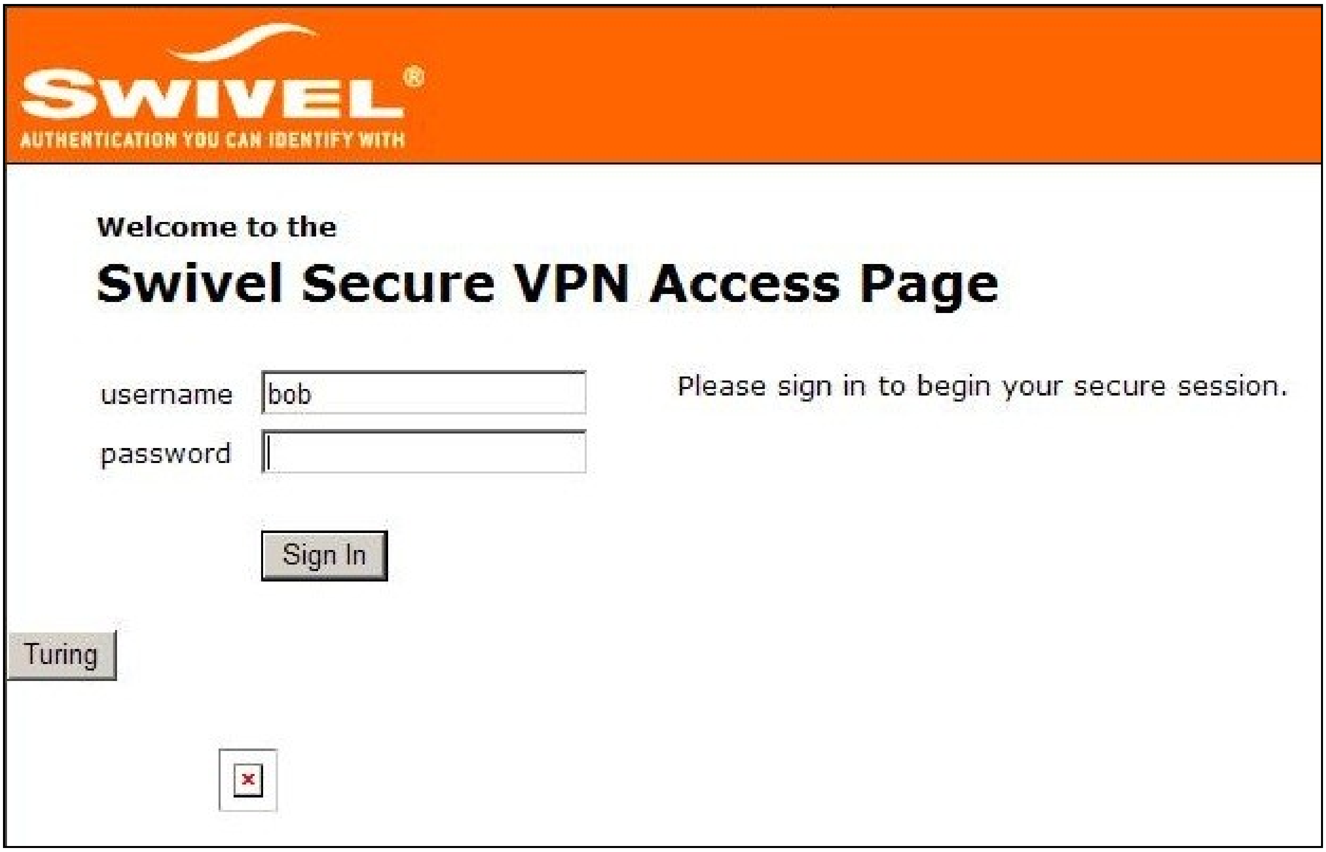
Troubleshooting

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.



Welcome to the

Swivel Secure VPN Access Page

username bob

password

Please sign in to begin your secure session.

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.

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

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

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".

Additional Information

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