Sentry SSO with PulseSecure

Contents

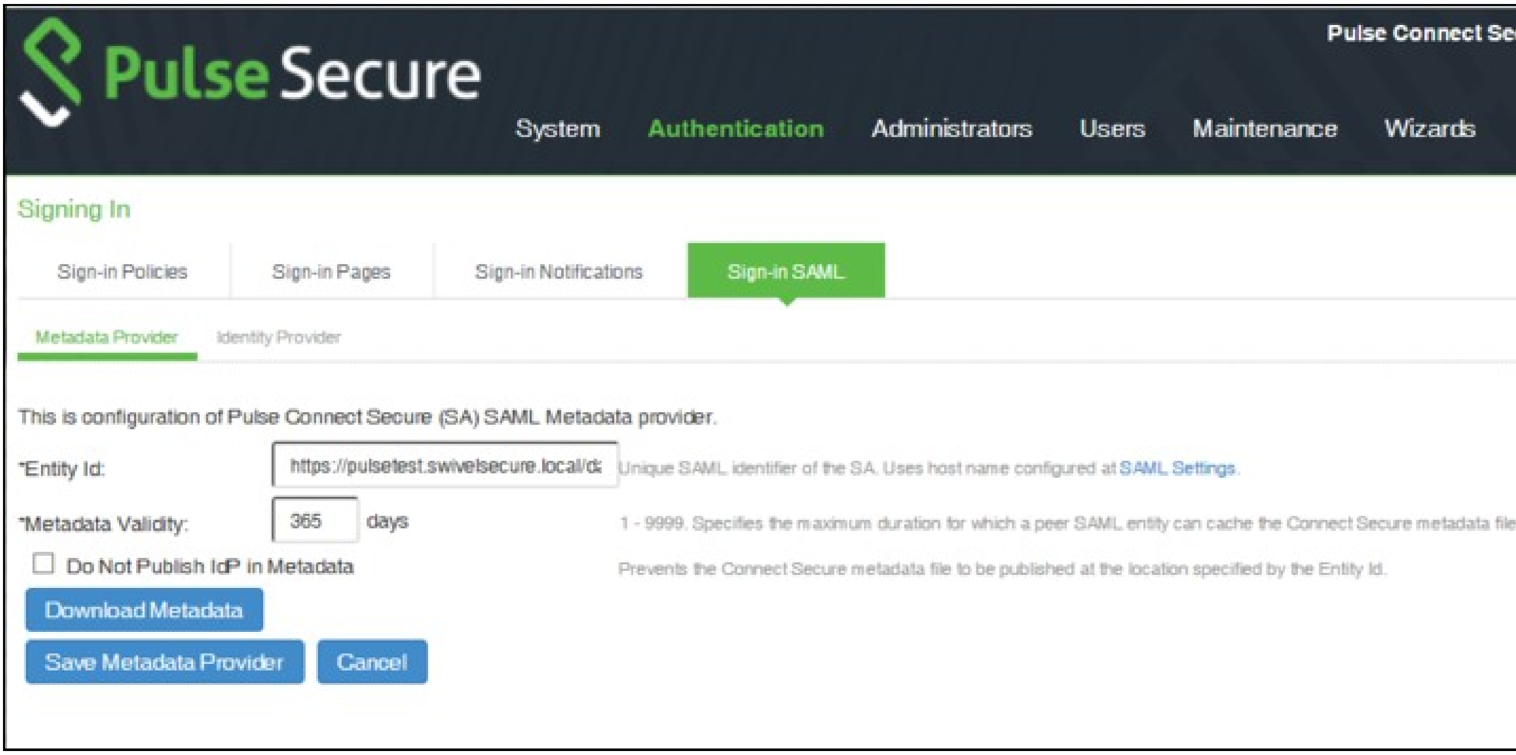
Introduction

This article explains how to integrate a PulseSecure SSL VPN with Sentry.

Configuring the PulseSecure VPN

NOTE: It is assumed that your PulseSecure already has a basic, working configuration.

Log into the PulseSecure administration console. From the menu, select **Authentication**, then **Signing In** and **Sign-in SAML**.



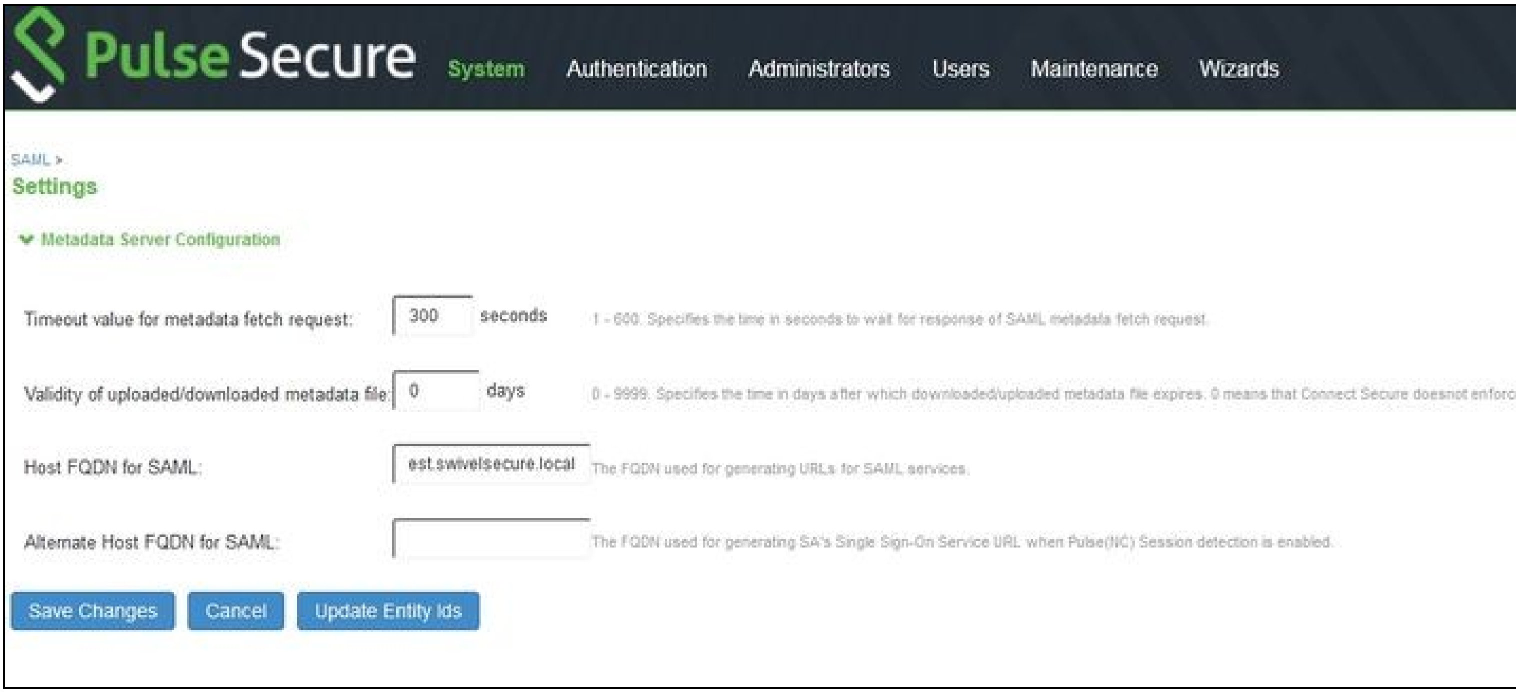
This is configuration of Pulse Connect Secure (SA) SAML Metadata provider.

*Entity Id: https://pulsetest.swivelsecure.local/da Unique SAML identifier of the SA. Uses host name configured at SAML Settings.

*Metadata Validity: 365 days 1 - 9999. Specifies the maximum duration for which a peer SAML entity can cache the Connect Secure metadata file

☐ Do Not Publish IdP in Metadata Prevents the Connect Secure metadata file to be published at the location specified by the Entity Id.

Click the link for **SAML Settings**, at the end of the line for **Entity Id**.



Timeout value for metadata fetch request: 300 seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: 0 days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure doesnot enforc

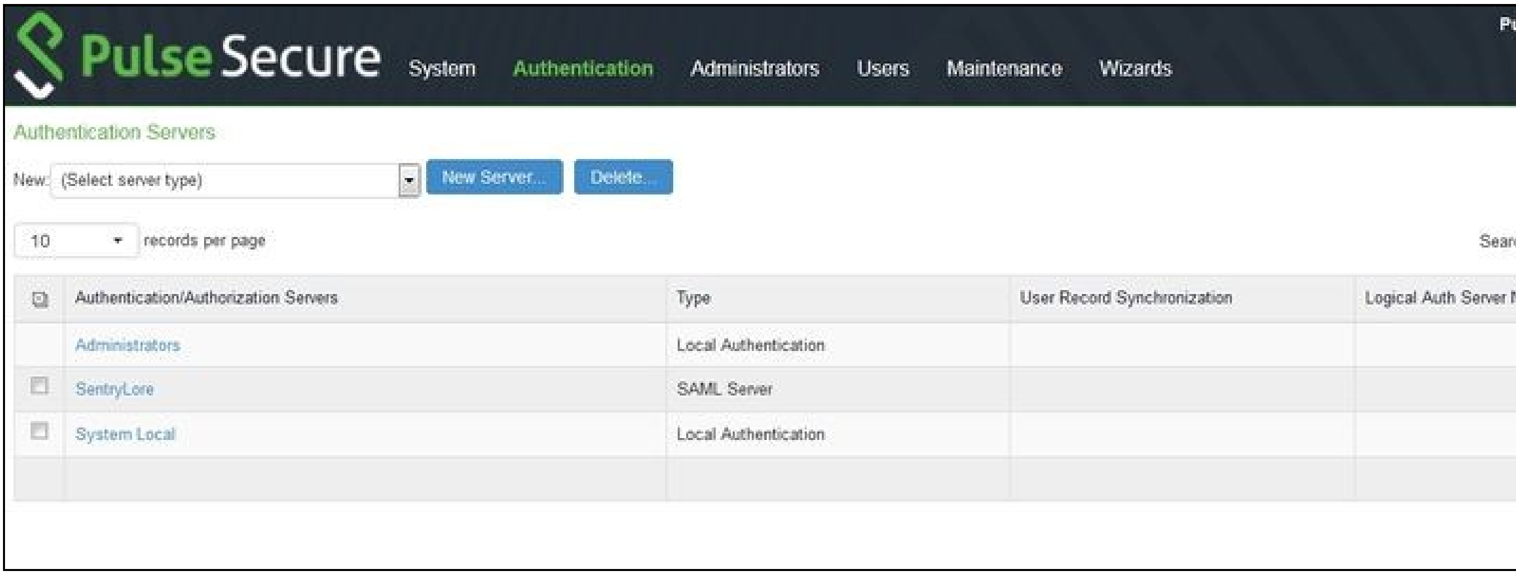
Host FQDN for SAML: est.swivelsecure.local The FQDN used for generating URLs for SAML services.

Alternate Host FQDN for SAML: The FQDN used for generating SA's Single Sign-On Service URL when Pulse(NC) Session detection is enabled.

Enter the public host name of your PulseSecure server under **Host FQDN for SAML**, and click **Save Changes**.

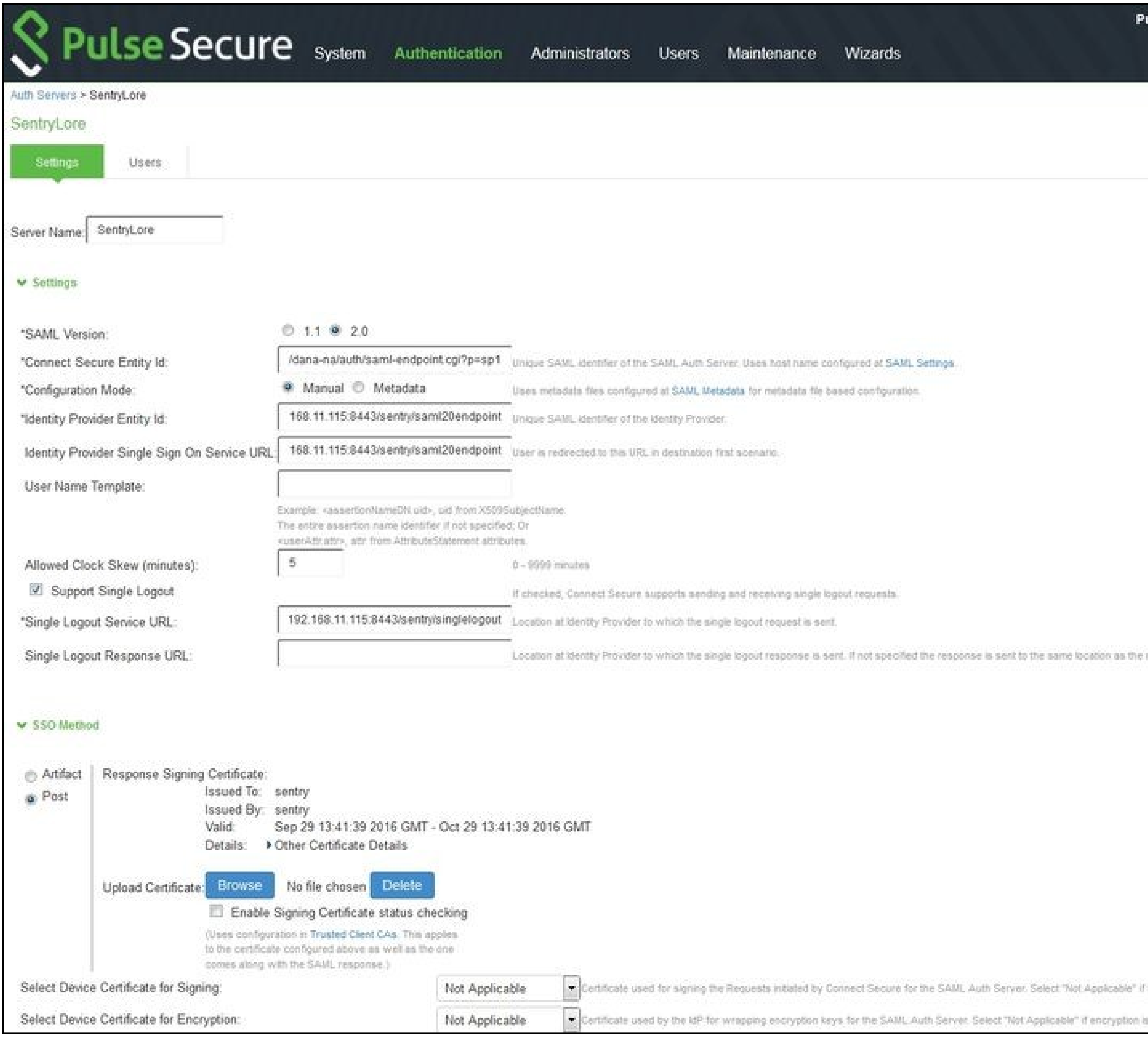
Go back to the **Sign-in SAML** page, and ensure that the Entity Id is *https://<pulse_server>/dana-na/auth/saml-endpoint.cgi* - i.e. it should be exactly the same as the Entity ID you put on the Sentry application settings, except for *?p=sp1*.

Now go to **Authentication**, **Auth. Servers**



☐	Authentication/Authorization Servers	Type	User Record Synchronization	Logical Auth Server N
	Administrators	Local Authentication		
☐	SentryLore	SAML Server		
☐	System Local	Local Authentication		

Select **SAML Server** from the drop-down, then click **New Server...**.



Server Name: SentryLore

Settings

*SAML Version: ○ 1.1 ● 2.0

*Connect Secure Entity Id: /dana-na/auth/saml-endpoint.cgi?p=sp1 — Unique SAML identifier of the SAML Auth Server. Uses host name configured at SAML Settings.

*Configuration Mode: ● Manual ○ Metadata — Uses metadata files configured at SAML Metadata for metadata file based configuration.

*Identity Provider Entity Id: 168.11.115:8443/sentry/saml20endpoint — Unique SAML identifier of the Identity Provider.

Identity Provider Single Sign On Service URL: 168.11.115:8443/sentry/saml20endpoint — User is redirected to this URL in destination first scenario.

User Name Template:

Example: <assertionNameDN.uid>, uid from X509SubjectName.
The entire assertion name identifier if not specified; Or
<userAttr.attr>, attr from AttributeStatement attributes.

Allowed Clock Skew (minutes): 5 — 0 - 9999 minutes

☑ Support Single Logout — If checked, Connect Secure supports sending and receiving single logout requests.

*Single Logout Service URL: 192.168.11.115:8443/sentry/singlelogout — Location at Identity Provider to which the single logout request is sent.

Single Logout Response URL: — Location at Identity Provider to which the single logout response is sent. If not specified the response is sent to the same location as the

SSO Method

○ Artifact
● Post

Response Signing Certificate:
Issued To: sentry
Issued By: sentry
Valid: Sep 29 13:41:39 2016 GMT - Oct 29 13:41:39 2016 GMT
Details: ▸ Other Certificate Details

Upload Certificate: Browse No file chosen Delete

□ Enable Signing Certificate status checking

(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing: Not Applicable — Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if

Select Device Certificate for Encryption: Not Applicable — Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is

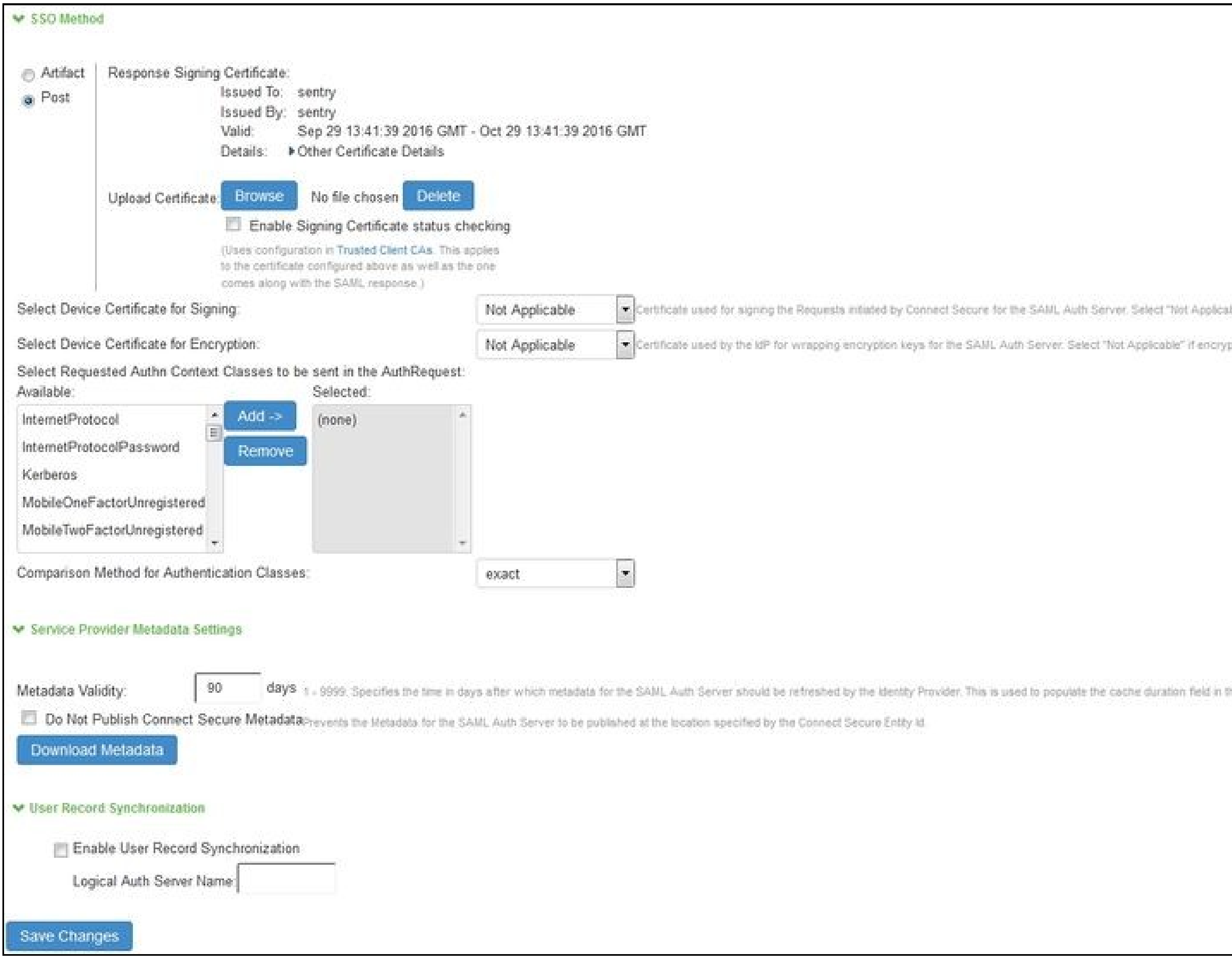
Set a name for the server. Ensure that **SAML Version** is set to 2.0.

Connect Secure Entity Id will be set as the unique entity ID for this server. Make a note of it, as you will be entering it in the Sentry configuration page.

For **Identity Provider Entity Id** and **Identity Provider Single Sign On Service URL**, enter *https://<swivel_server>/sentry/saml20endpoint*. Here, *<swivel_server>* is the public URL of the Swivel sentry server.

Check **Support Single Logout**, and enter *https://<swivel_server>/sentry/singlelogout* as the **Single Logout Server URL**. The **Single Logout Response URL** is the same, so can be left blank.

NOTE: for the next part, you will need a copy of the metadata from the Swivel Sentry server. If you do not already have one, open your browser to ***https://<swivel_server>/sentry/metadata/generatedMetadata.xml****. When the metadata is displayed in your browser, save it to disk.*



SSO Method

○ Artifact
● Post

Response Signing Certificate:
Issued To: sentry
Issued By: sentry
Valid: Sep 29 13:41:39 2016 GMT - Oct 29 13:41:39 2016 GMT
Details: ▸Other Certificate Details

Upload Certificate: No file chosen

□ Enable Signing Certificate status checking

(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing: Not Applicable Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applical

Select Device Certificate for Encryption: Not Applicable Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryp

Select Requested Authn Context Classes to be sent in the AuthRequest:

Available:
InternetProtocol
InternetProtocolPassword
Kerberos
MobileOneFactorUnregistered
MobileTwoFactorUnregistered

Selected:
(none)

Comparison Method for Authentication Classes: exact

Service Provider Metadata Settings

Metadata Validity: 90 days 1 - 9999. Specifies the time in days after which metadata for the SAML Auth Server should be refreshed by the Identity Provider. This is used to populate the cache duration field in th

□ Do Not Publish Connect Secure Metadata Prevents the Metadata for the SAML Auth Server to be published at the location specified by the Connect Secure Entity Id.

User Record Synchronization

□ Enable User Record Synchronization

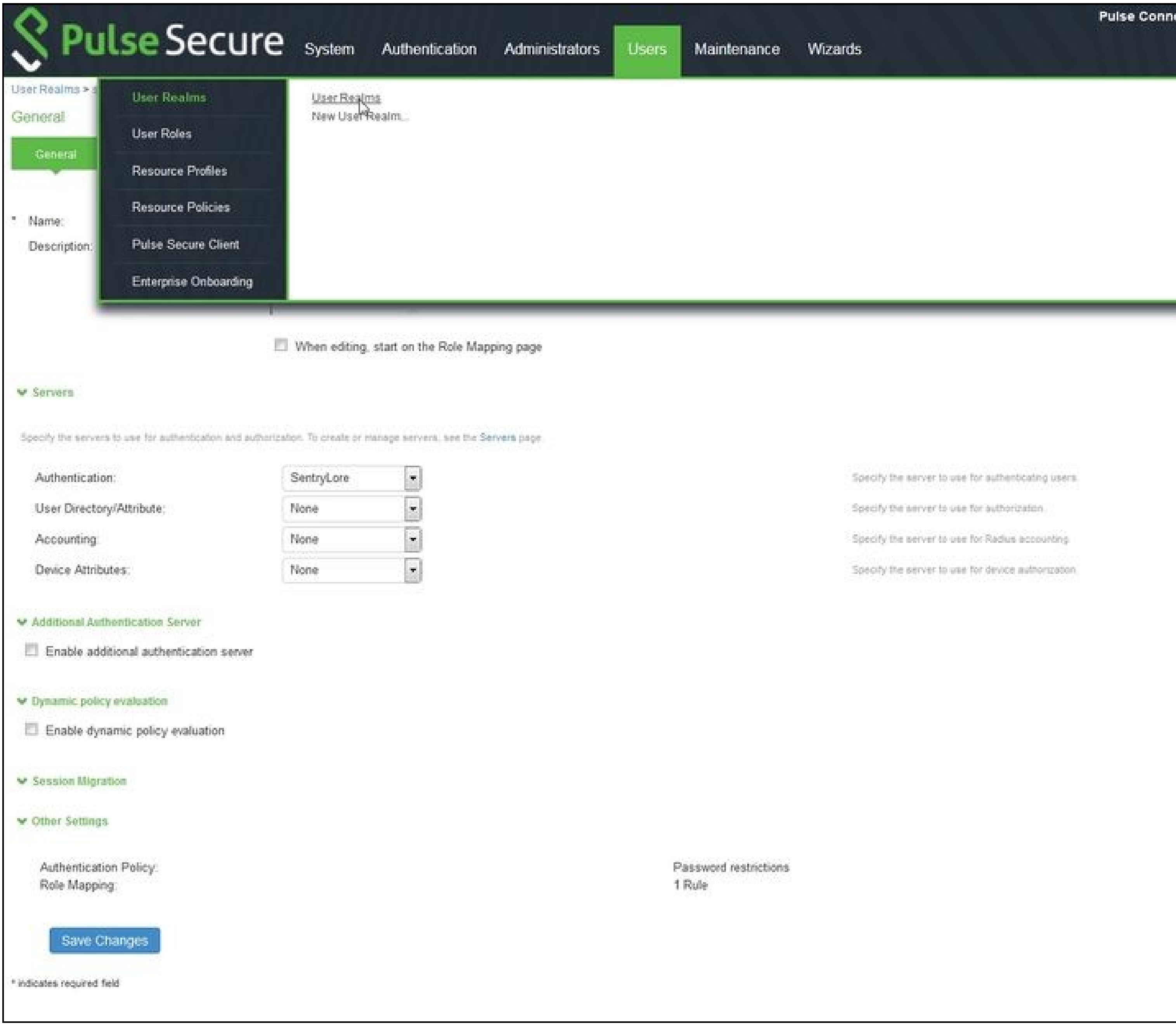
Logical Auth Server Name:

Ensure that **Post** is selected as the **SSO Method**. Click **Browse** next to **Upload Certificate** and select the metadata file you downloaded earlier.

Set a valid value for **Metadata Validity**.

Click **Save Changes**.

Now Select **Users**, then **User Realms**.



* Name:

Description:

□ 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:	SentryLore	Specify the server to use for authenticating users
User Directory/Attribute:	None	Specify the server to use for authorization
Accounting:	None	Specify the server to use for Radius accounting
Device Attributes:	None	Specify the server to use for device authorization

Additional Authentication Server

□ Enable additional authentication server

Dynamic policy evaluation

□ Enable dynamic policy evaluation

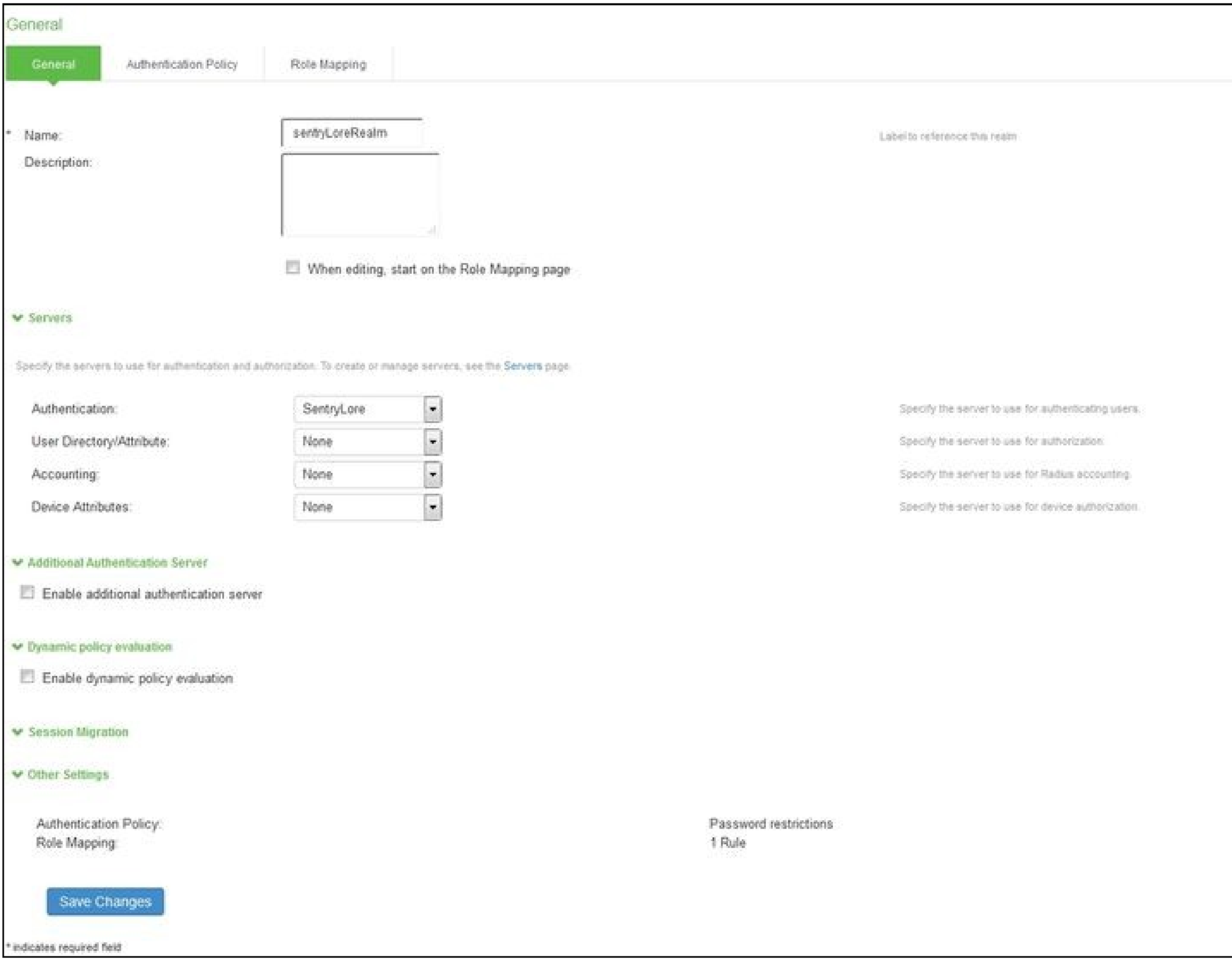
Session Migration

Other Settings

Authentication Policy:	Password restrictions
Role Mapping:	1 Rule

* indicates required field

Click **New** to create a new user realm.



* Name: sentryLoreRealm — Label to reference this realm

Description:

□ 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: SentryLore — Specify the server to use for authenticating users.

User Directory/Attribute: None — Specify the server to use for authorization.

Accounting: None — Specify the server to use for Radius accounting.

Device Attributes: None — Specify the server to use for device authorization.

Additional Authentication Server

□ Enable additional authentication server

Dynamic policy evaluation

□ Enable dynamic policy evaluation

Session Migration

Other Settings

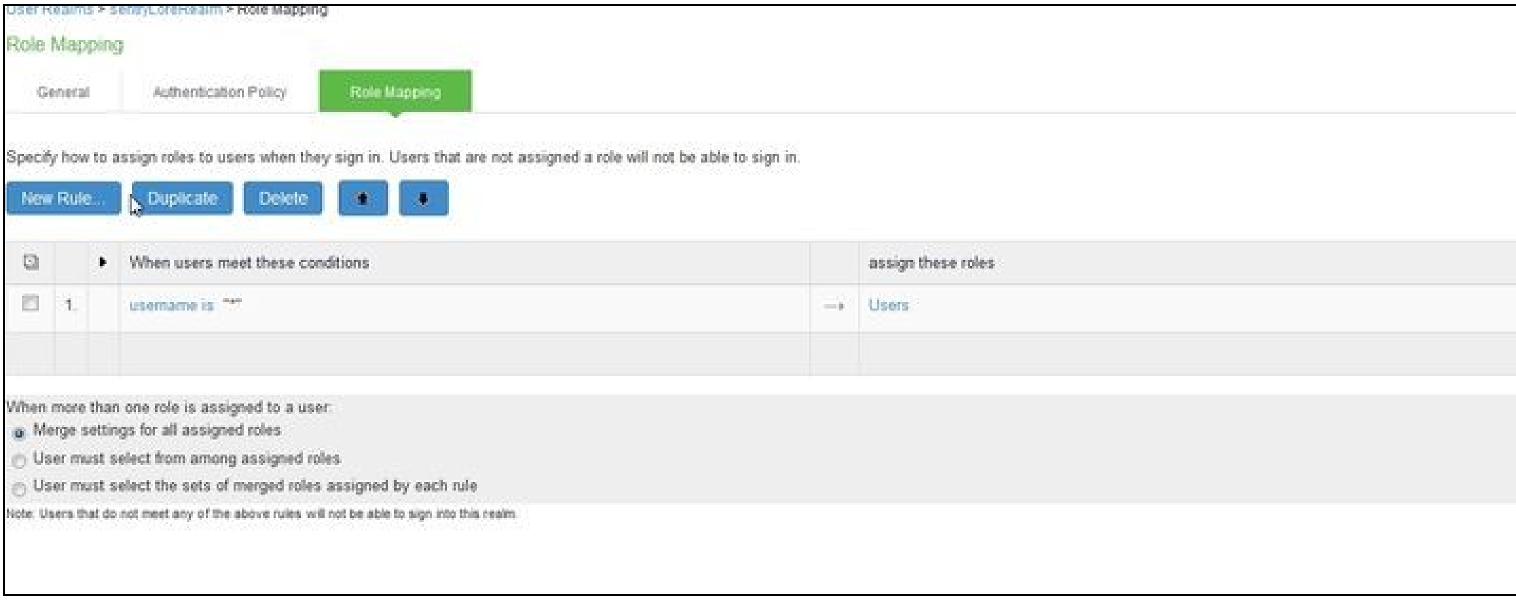
Authentication Policy: Password restrictions

Role Mapping: 1 Rule

* indicates required field

Add a name, then under **Authentication**, select your new authentication server. Click **Save Changes**.

Now under **Role Mapping**, select the role(s) that users will be assigned. For example, in the following role mapping, all users are assigned to the Role **Users**.



Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

□			When users meet these conditions		assign these roles
□	1.		username is "*"	→	Users

When more than one role is assigned to a user:

● Merge settings for all assigned roles

○ User must select from among assigned roles

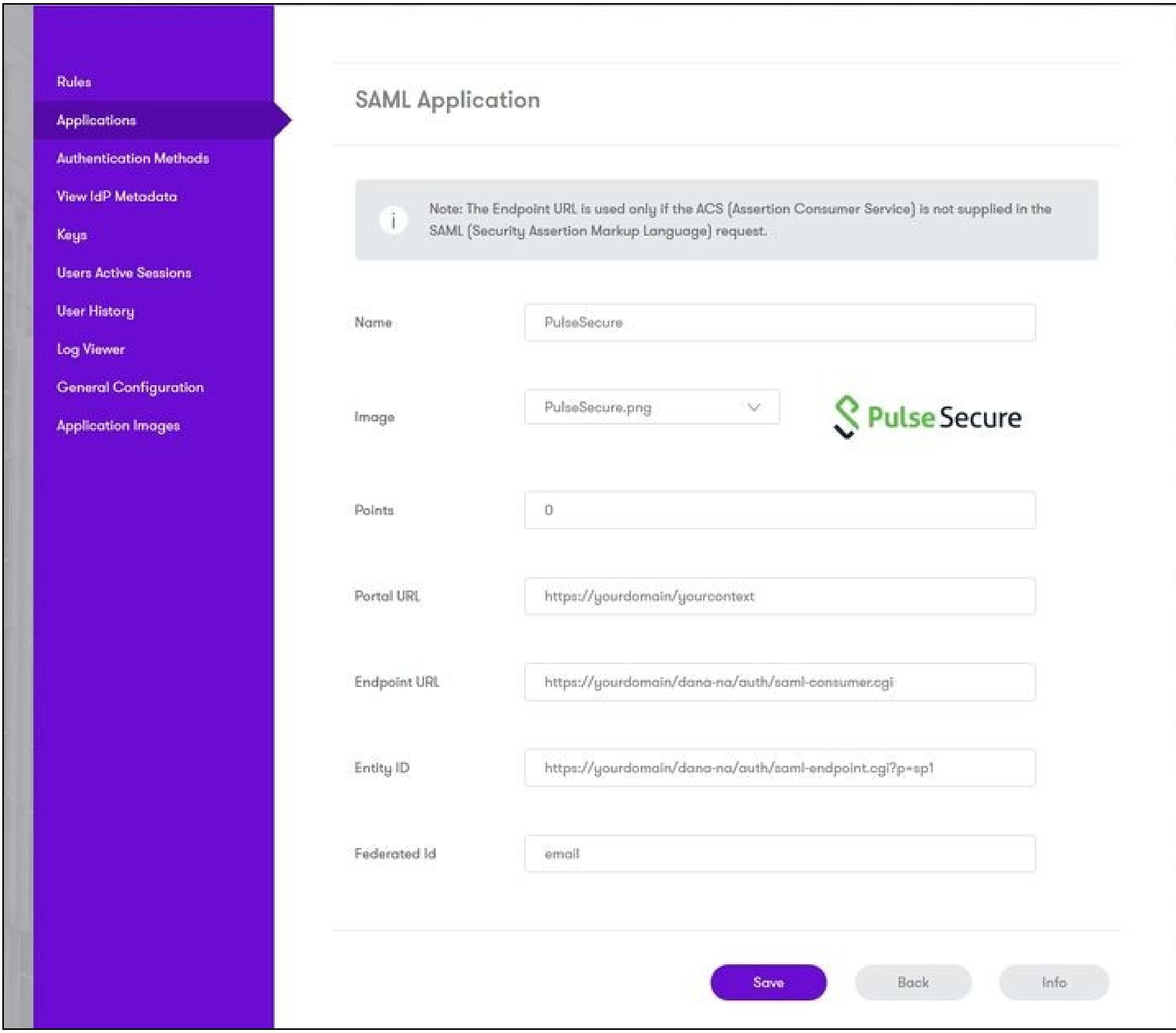
○ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Finally, go to **Authentication**, **Signing In**, **Sign-in Policies**. Click **New URL...**. Enter the **Sign-in URL**, then select **User picks from a list of authentication realms** and add the user realm created above. Click **Save Changes**.

Configuring the Sentry Application

Log into the Sentry administration console. Select **Applications**. Then Click **Add Application** and select **SAML - PulseSecure**



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name: PulseSecure

Image: PulseSecure.png

Points: 0

Portal URL: https://yourdomain/yourcontext

Endpoint URL: https://yourdomain/dana-na/auth/saml-consumer.cgi

Entity ID: https://yourdomain/dana-na/auth/saml-endpoint.cgi?p=sp1

Federated Id: email

NOTE: for all the following, replace *<pulse_server>* with the public host name for your Pulse server.

Under **Portal URL**, enter the URL for the PulseSecure portal that will be authenticated using Sentry, for example *https://<pulse_server>/saml*.

Under **Endpoint URL**, enter *https://<pulse_server>/dana-na/auth/saml-consumer.cgi*.

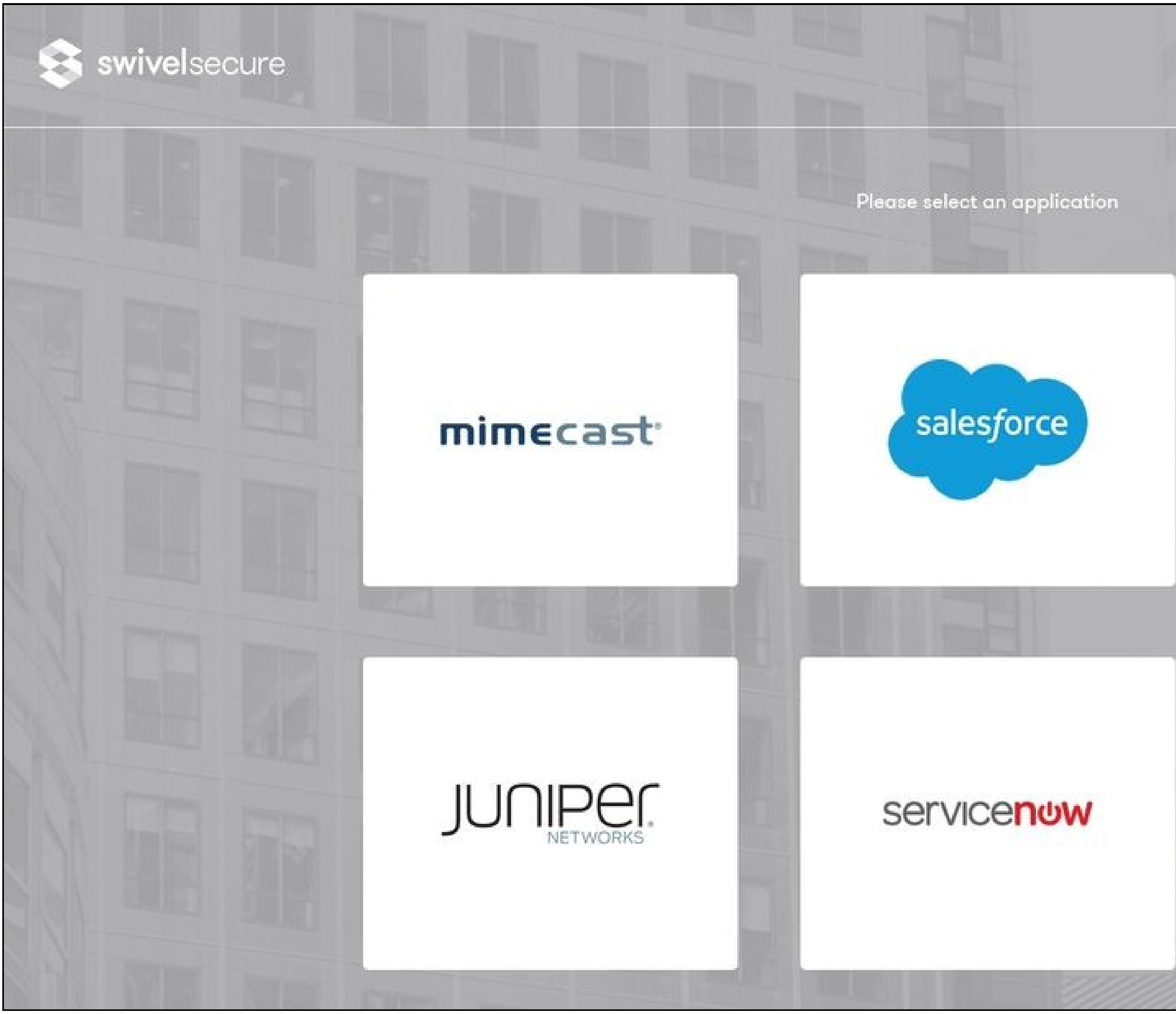
Under **Entity ID**, enter the unique Entity ID you recorded from the PulseSecure authentication server.

Under **Federated Id**, enter *email*.

Testing authentication to PulseSecure via Swivel AuthControl Sentry

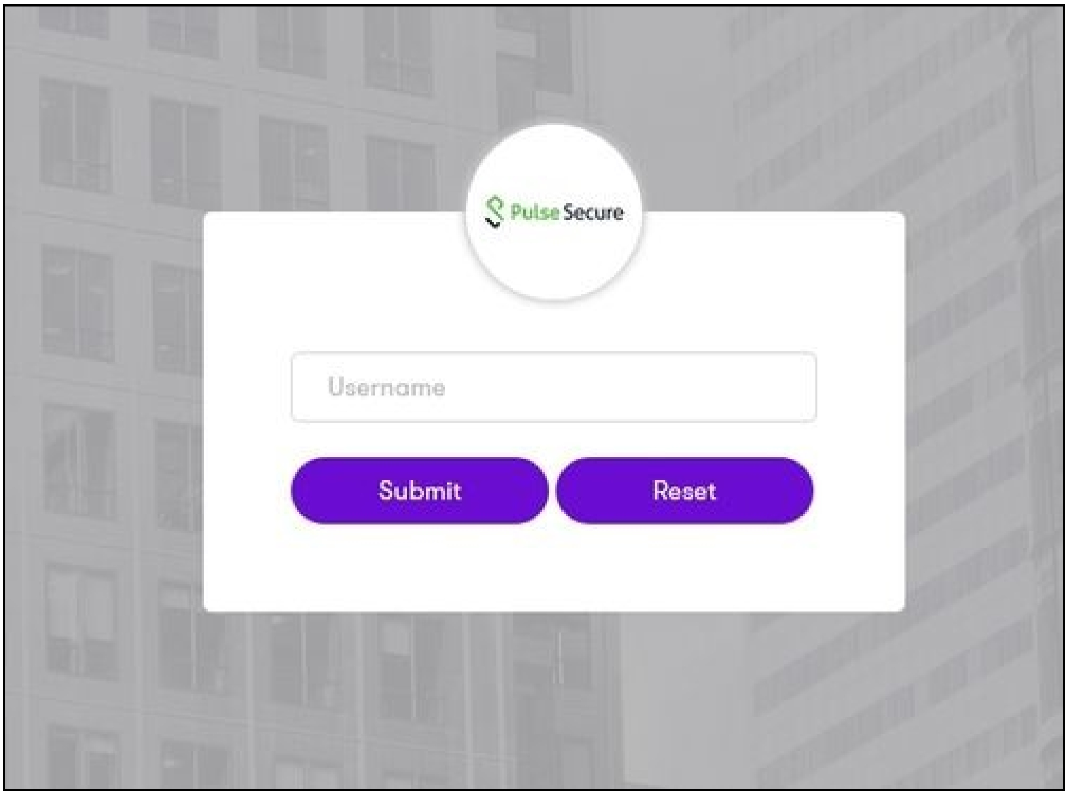
This should be the final step after all previous elements have been configured.

Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. **https://mycompanysentrydomain/sentry/startPage** On a Start Page you will be able to see a new PulseSecure Icon on which you can click and proceed with authentication (as you would by going straight to the PulseSecure page)

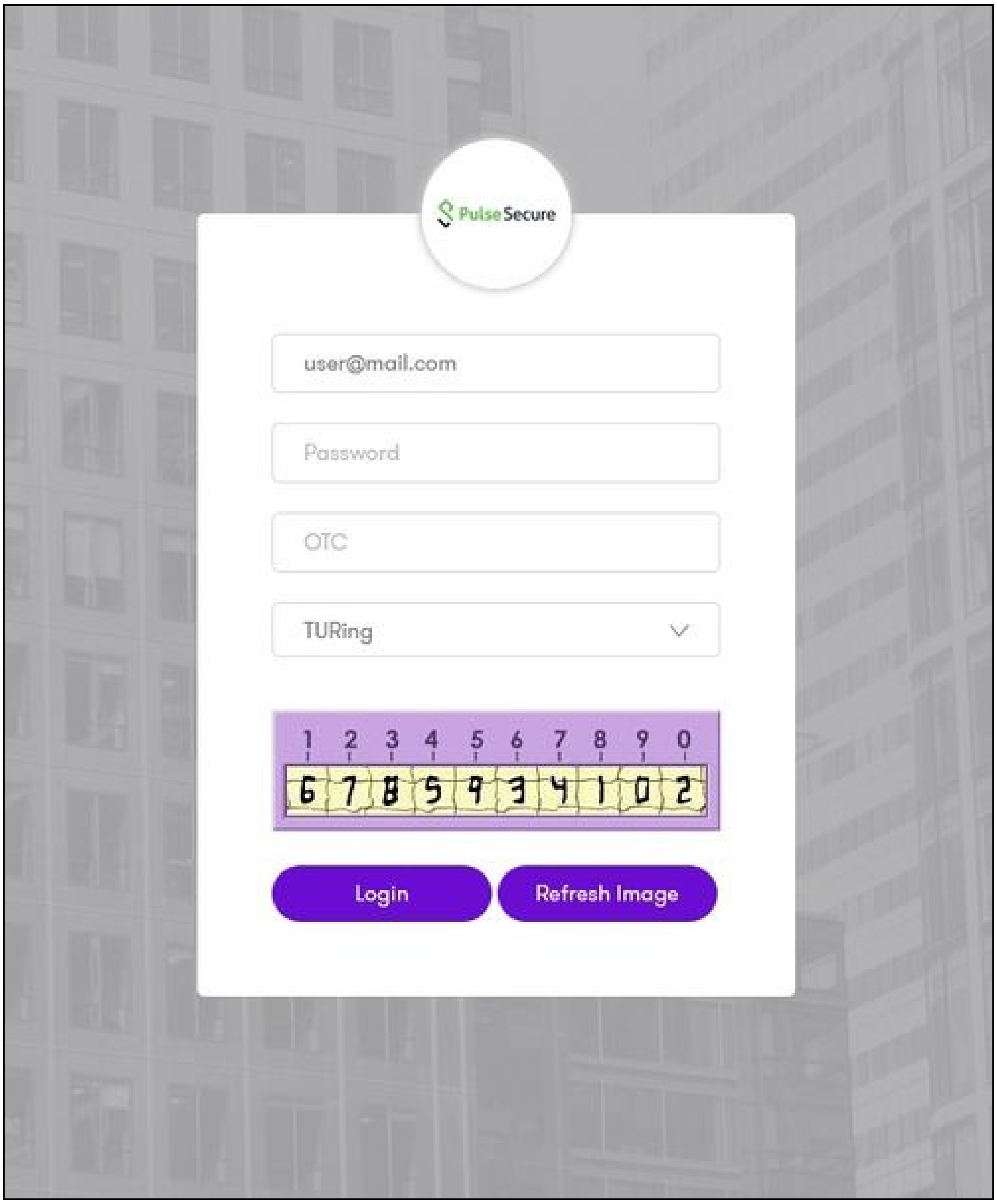


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the PulseSecure Application definition.

In this login example we are using the email as a username



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the PulseSecure that we tried to access.