Sentry SSO with PulseSecure

Contents

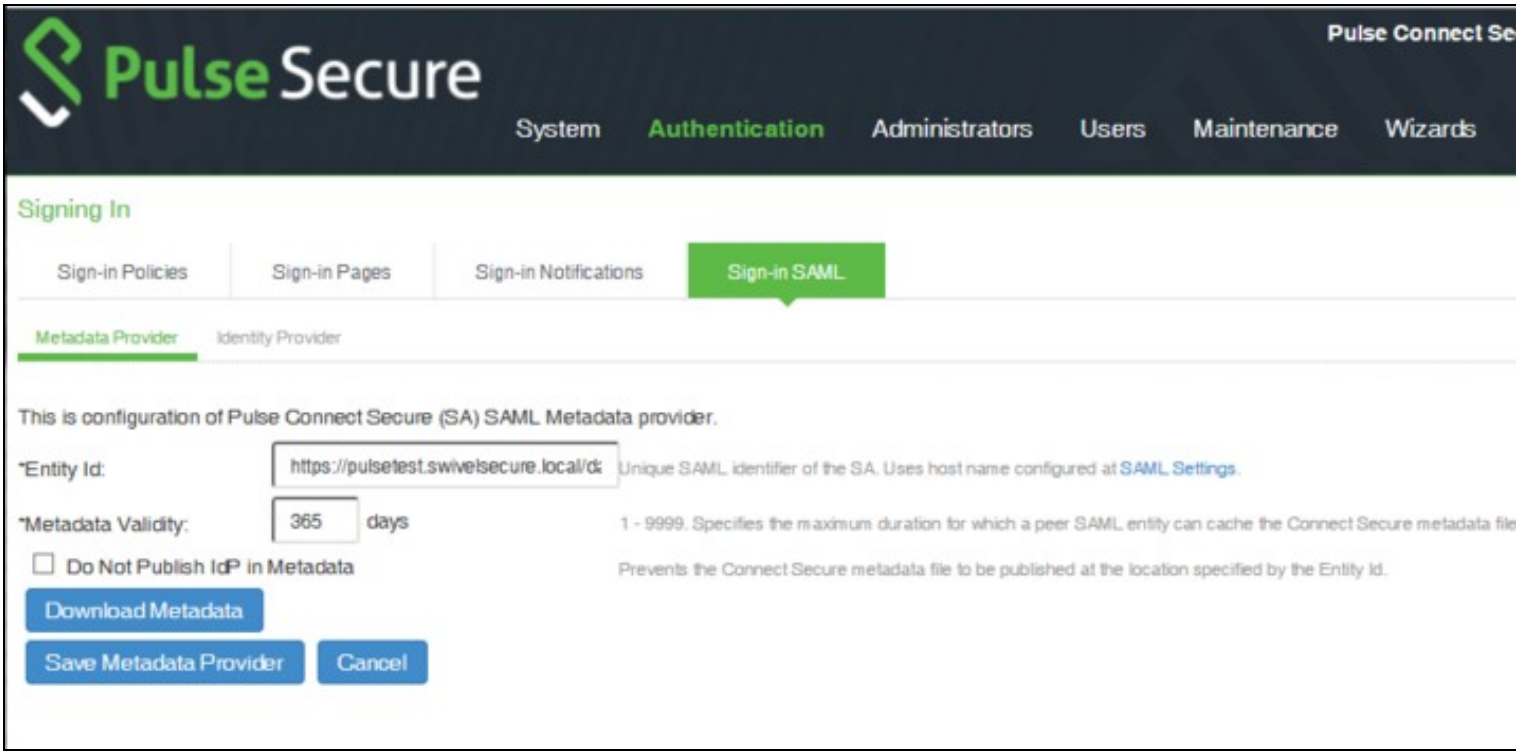
Introduction

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

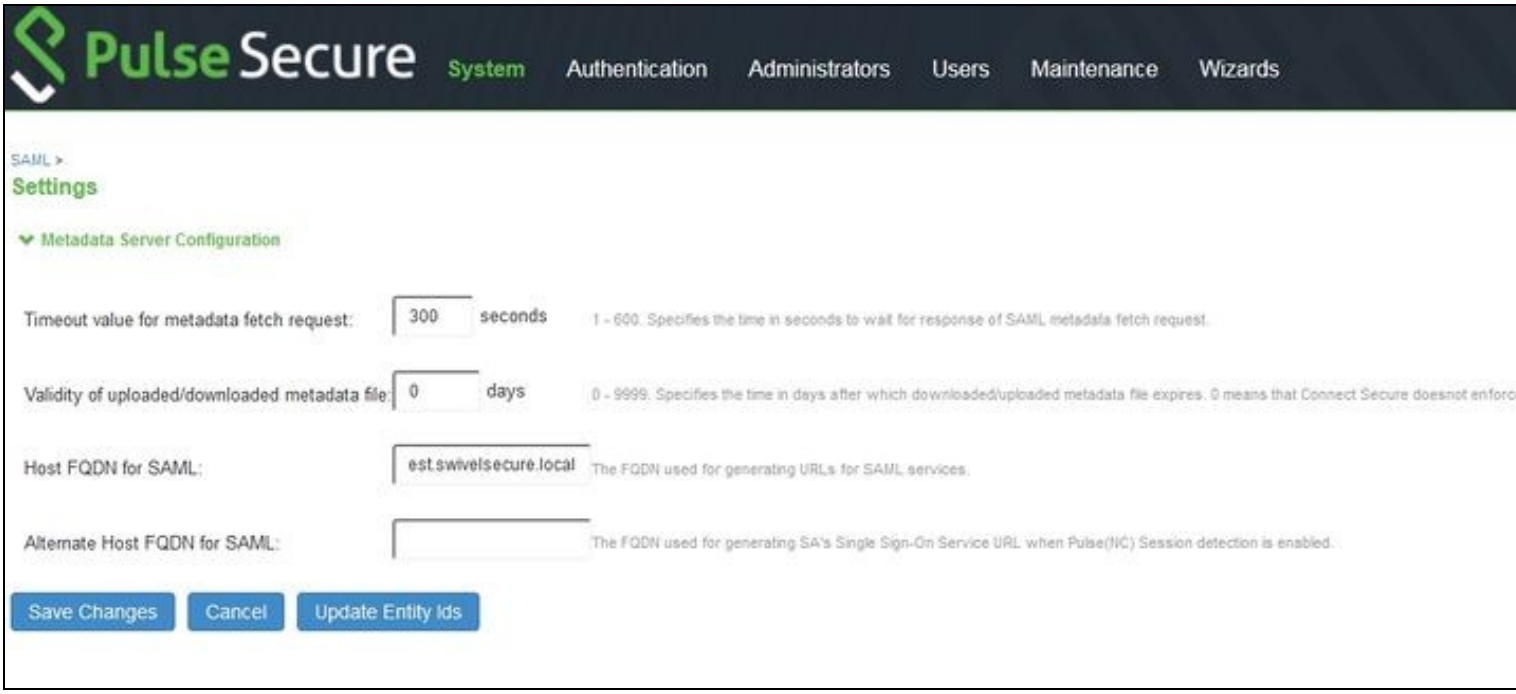
Configuring the PulseSecure VPN

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**.



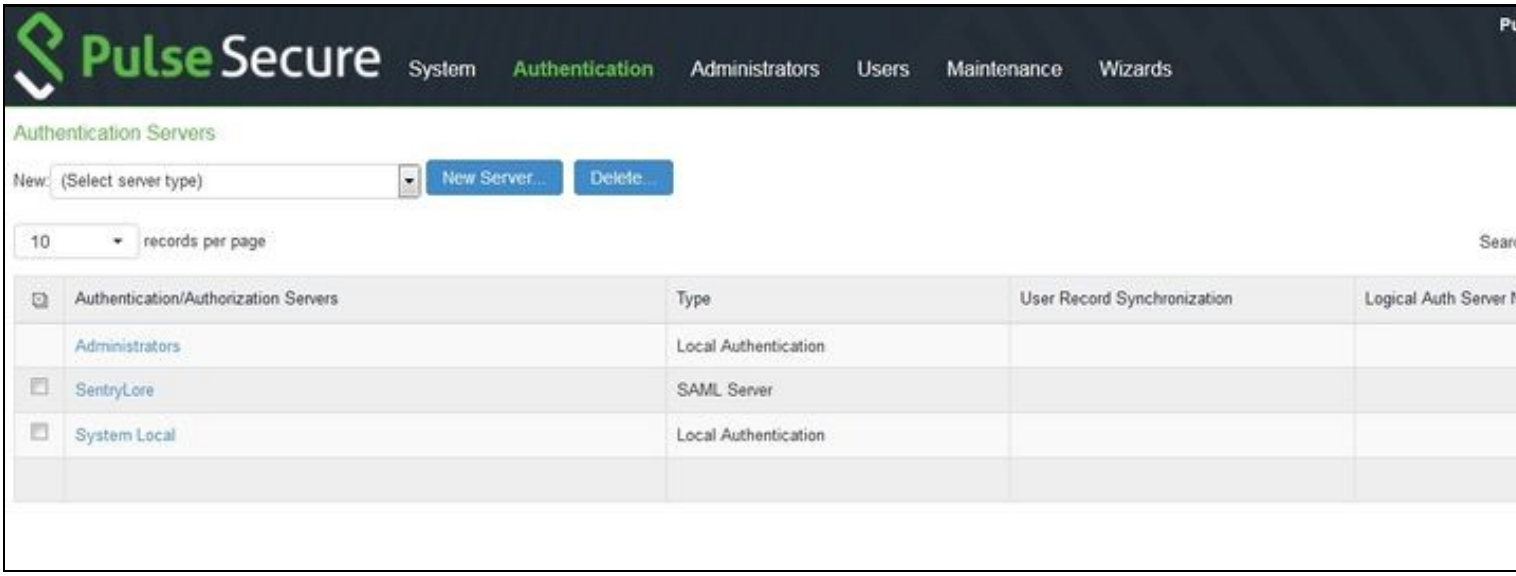
Click the link for **SAML Settings**, at the end of the line for **Entity Id**.



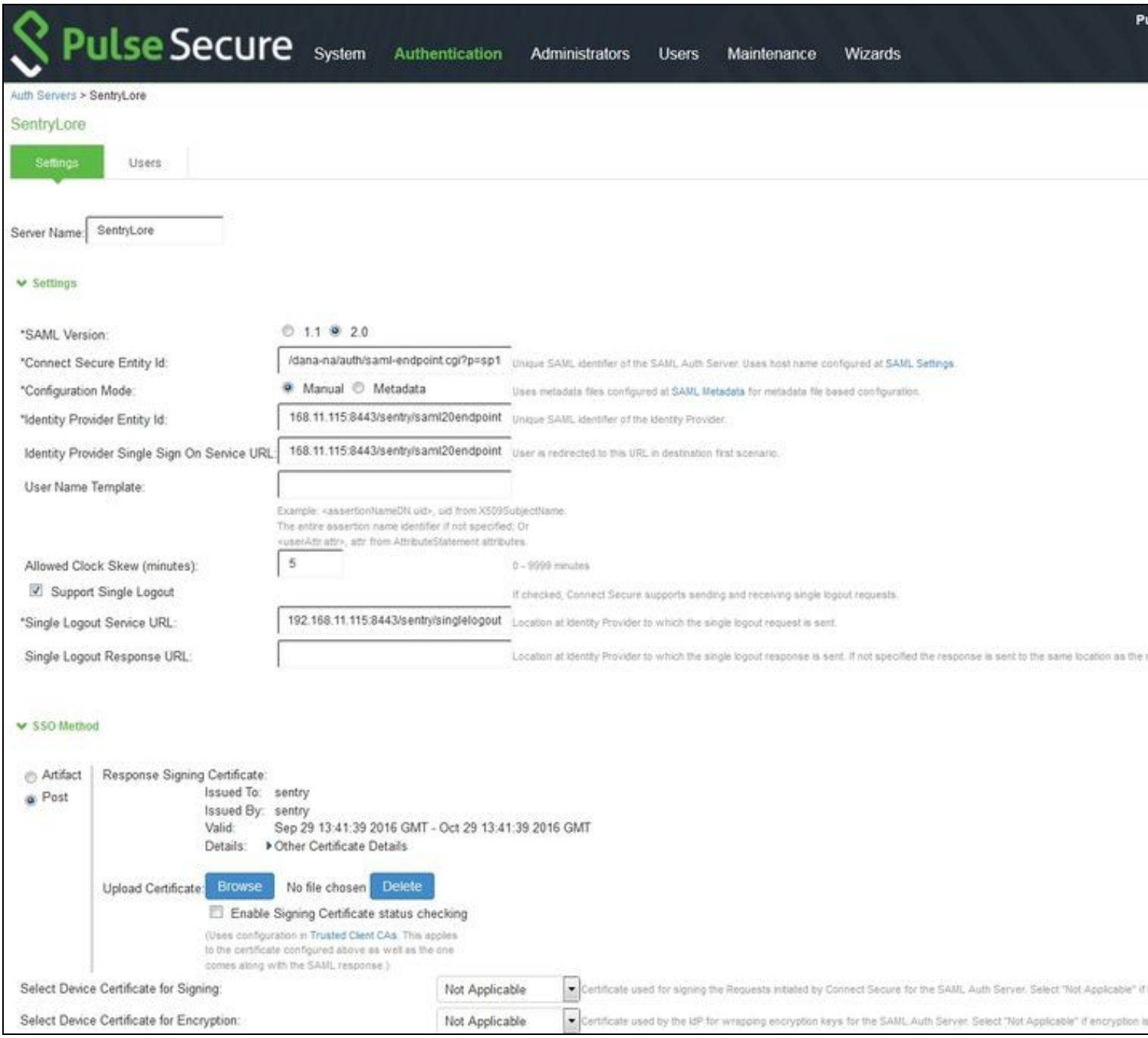
Enter the public host name of your PulseSecure server under **Host FQDN for SAML**, and click **Save Changes**.

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**



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



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: 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 Applicat

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

Add ->
Remove

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.

Download Metadata

User Record Synchronization

Enable User Record Synchronization

Logical Auth Server Name:

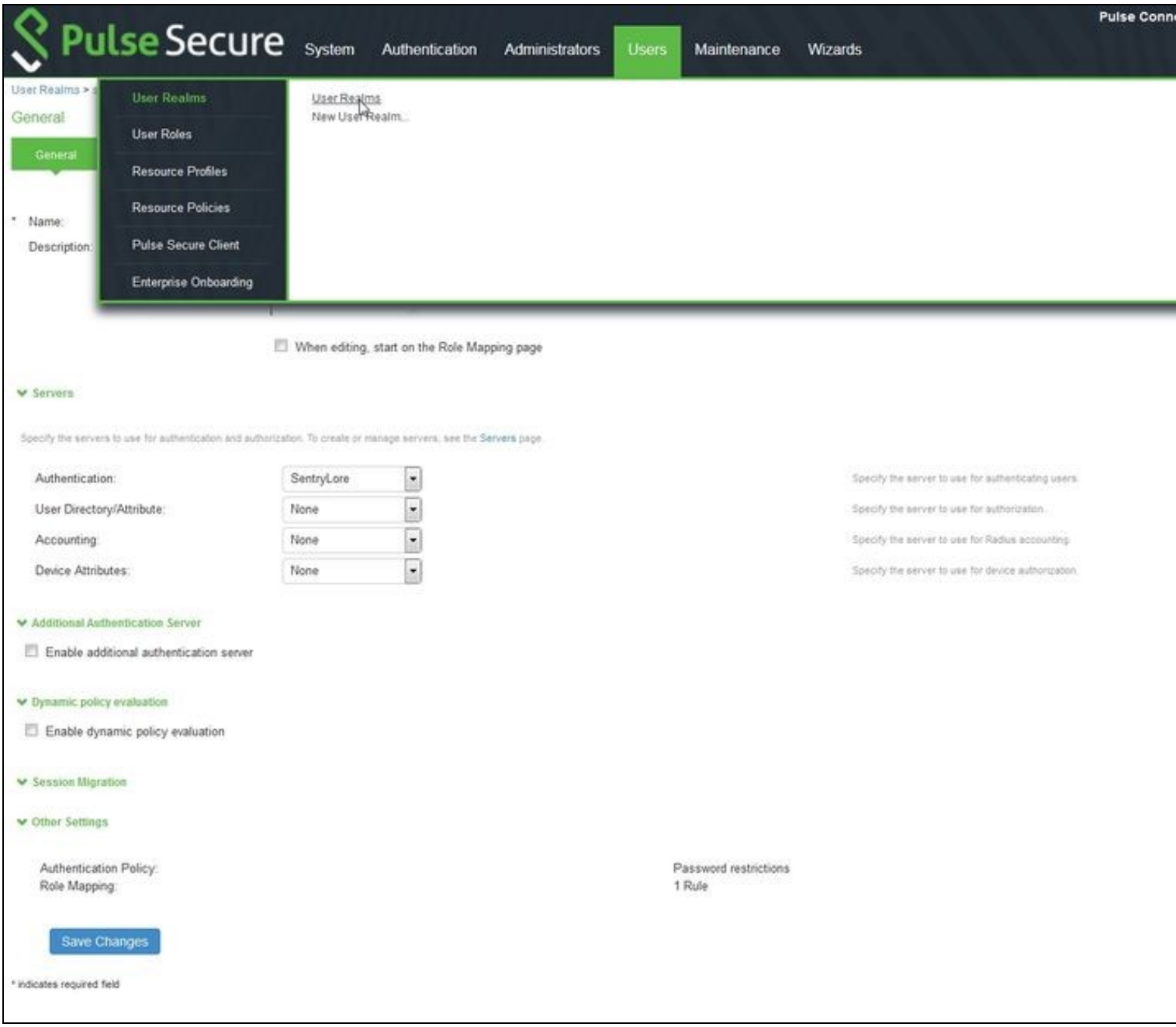
Save Changes

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**.



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

General

General | Authentication Policy | Role Mapping

* 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

Save Changes

* 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**.

User Realms > sentryLoreRealm > Role Mapping

Role Mapping

General | Authentication Policy | Role Mapping

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.

New Rule... | Duplicate | Delete

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

When more than one role is assigned to a user:

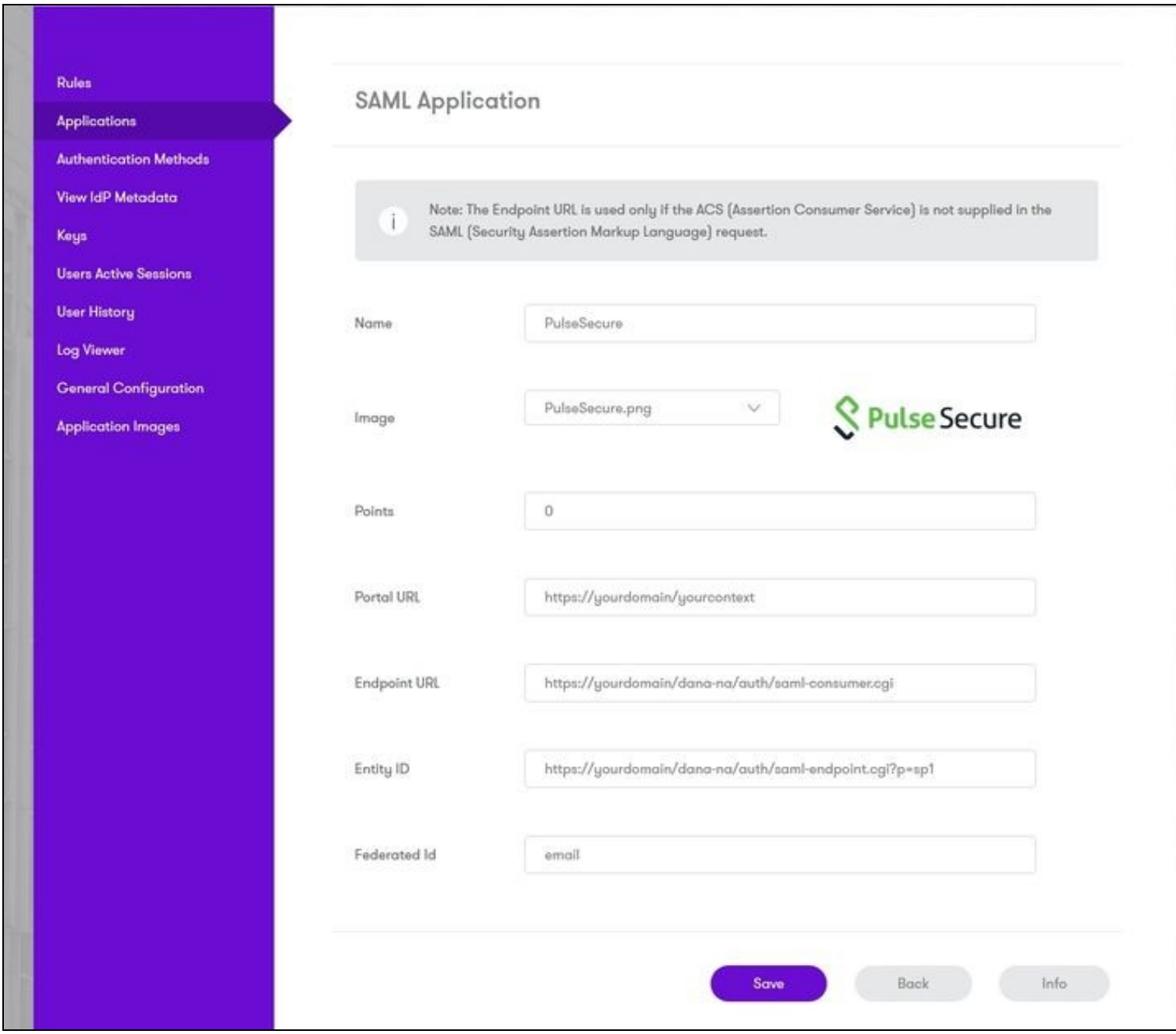
- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

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**



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*.

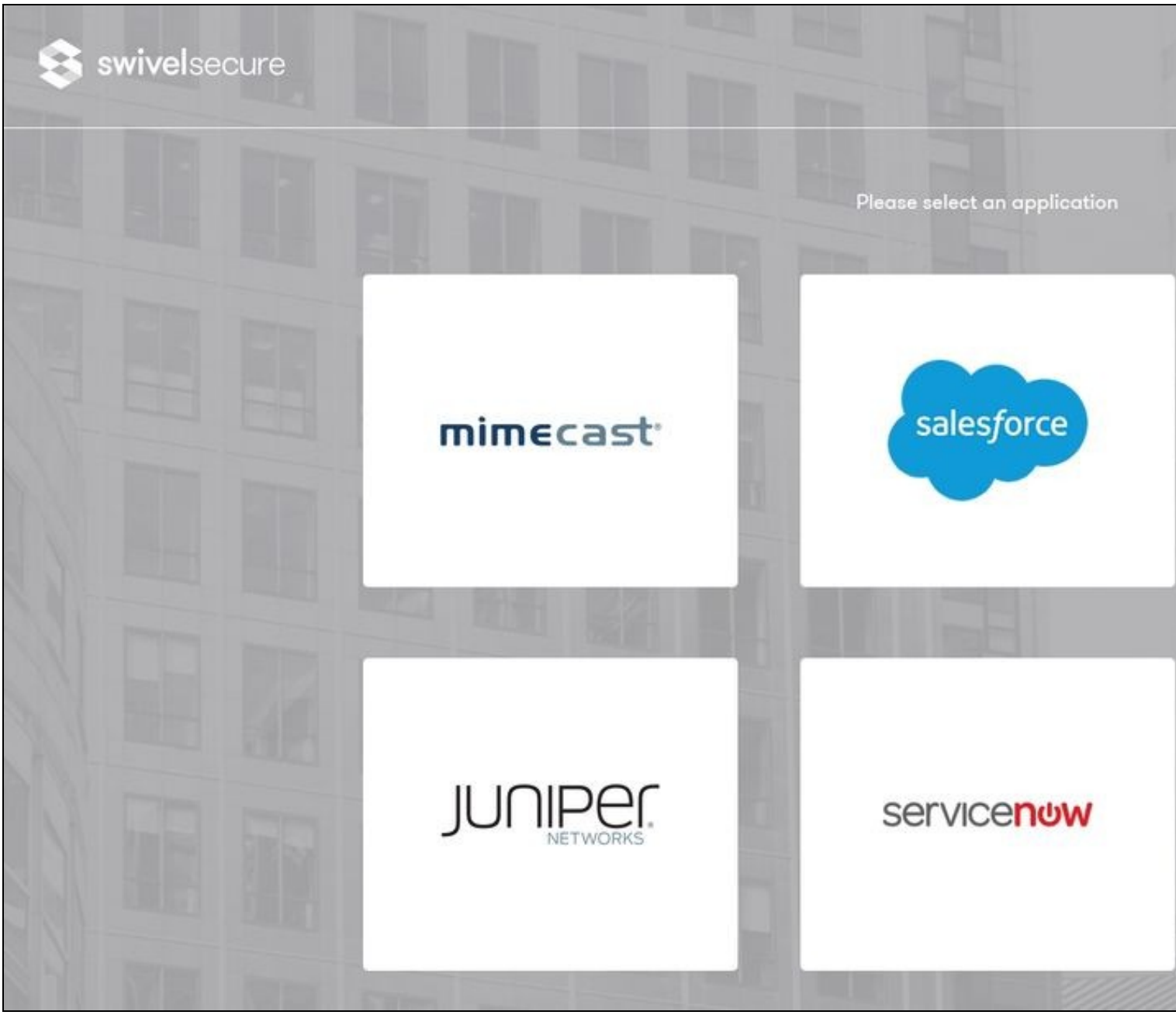
Under **Entity ID**, enter the unique Entity ID you recorded from the PulseSecure authentication server.

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

Testing authentication to PulseSecure via Swivel AuthControl Sentry

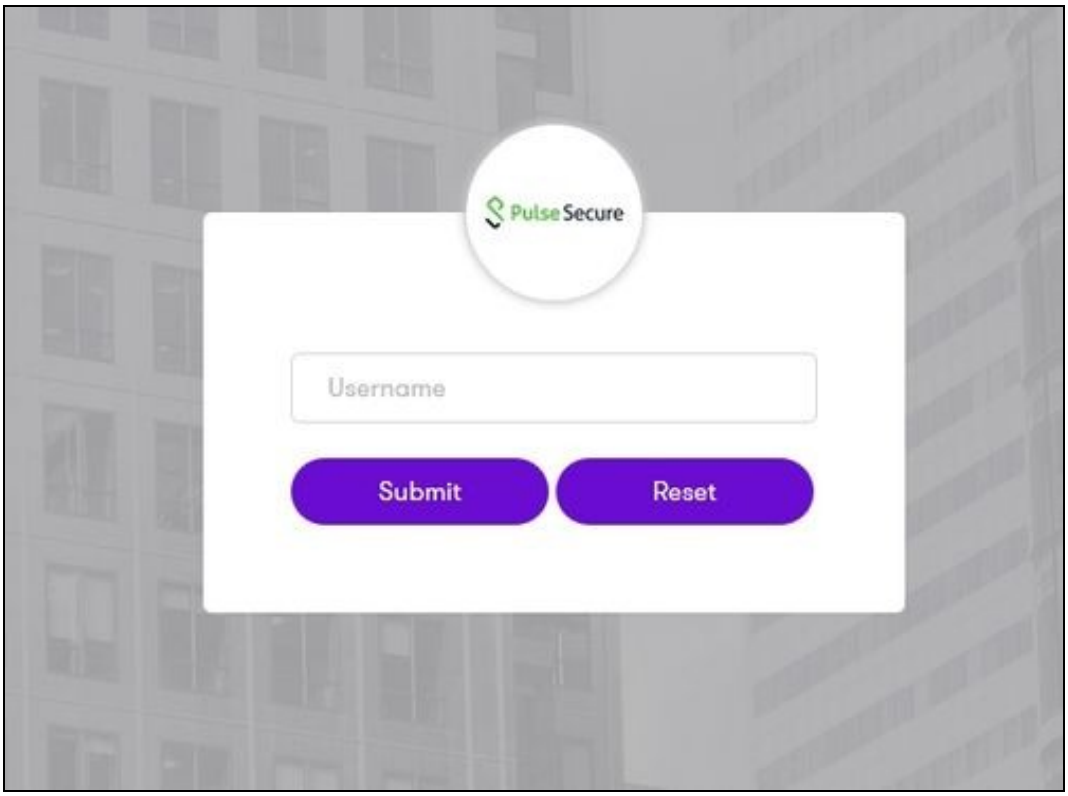
This should be the final step after all previous elements have been configured.

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)

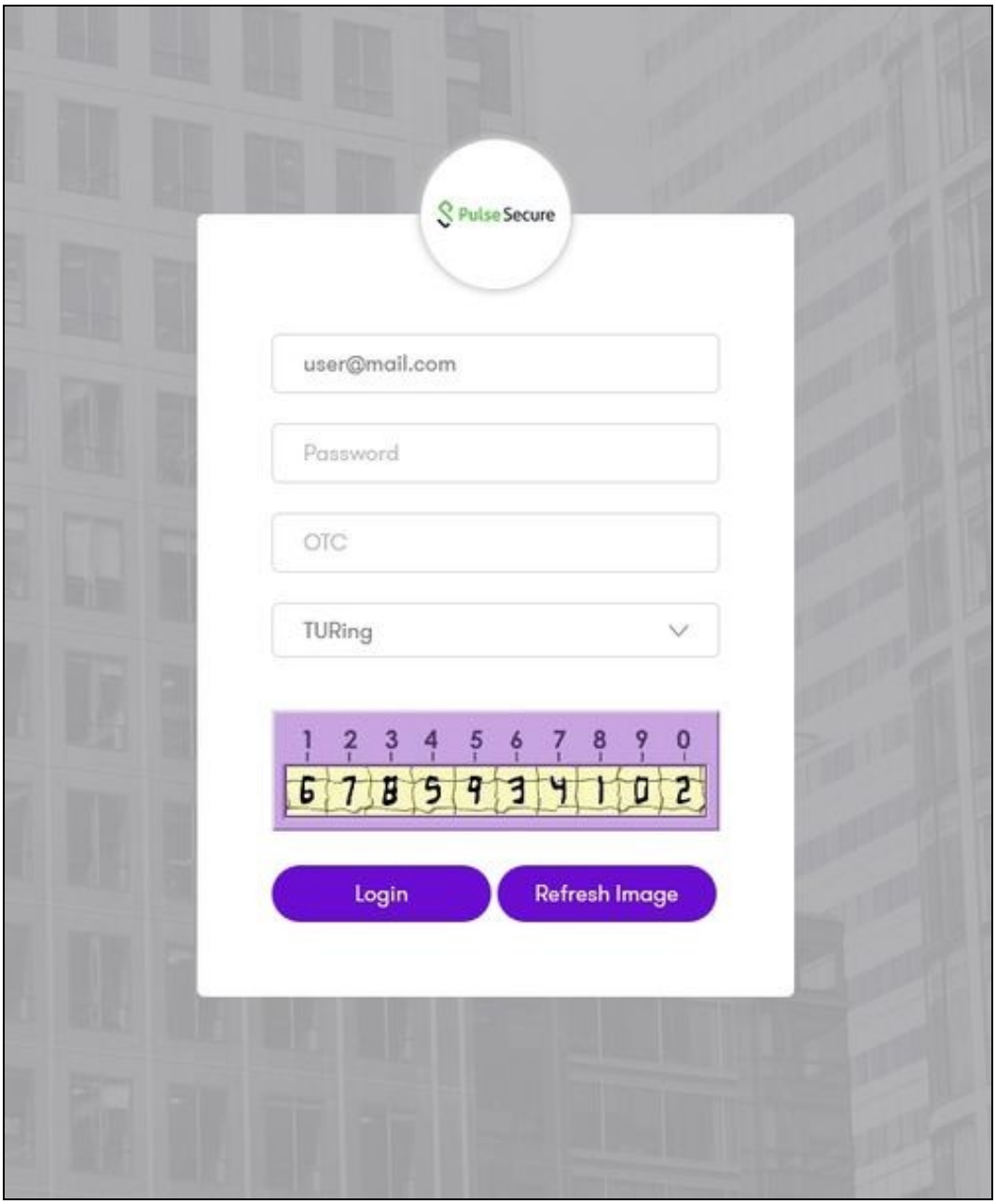


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the PulseSecure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