

Sentry SSO with PulseSecure

Contents

- 1 Introduction
- 2 Configuring the PulseSecure VPN
- 3 Configuring the Sentry Application
- 4 Testing authentication to PulseSecure via Swivel AuthControl Sentry

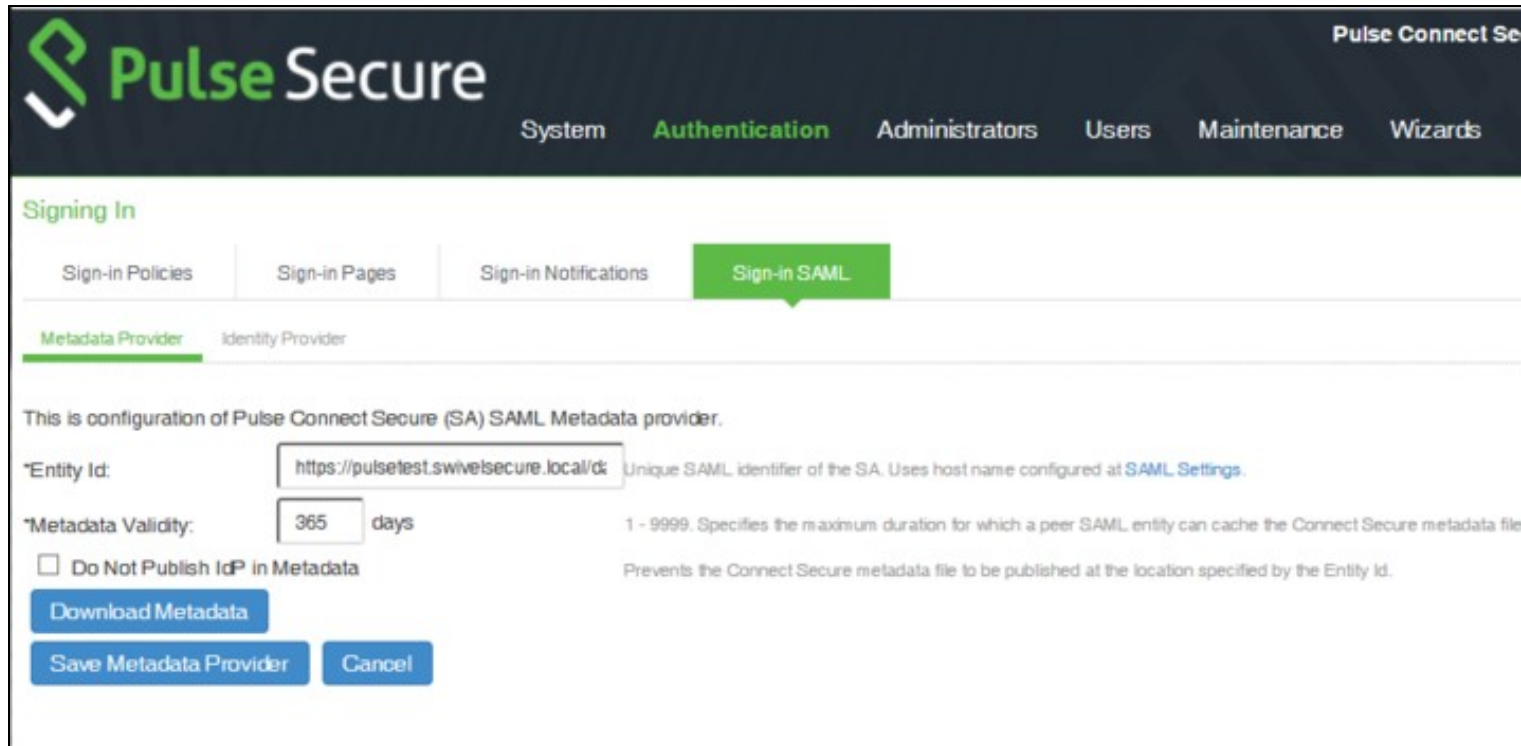
Introduction

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

Configuring the PulseSecure VPN

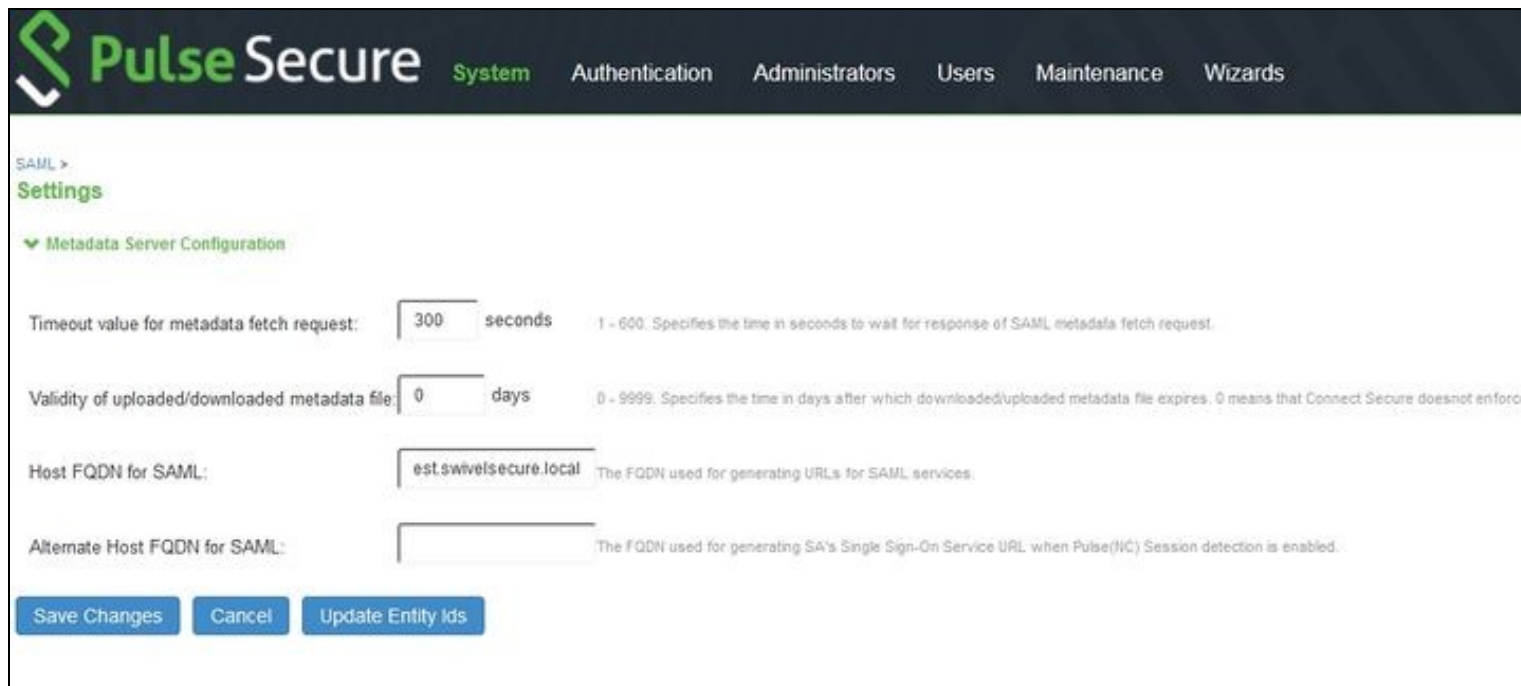
NOTE: It is assumed that your PulseSecure already has a basic, working configuration.

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



The screenshot shows the Pulse Secure administration console interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Maintenance', and 'Wizards'. The 'Authentication' section is expanded, showing 'Signing In' with sub-tabs: 'Sign-in Policies', 'Sign-in Pages', 'Sign-in Notifications', and 'Sign-in SAML'. The 'Sign-in SAML' tab is active. Below the tabs, there are two sub-sections: 'Metadata Provider' and 'Identity Provider'. The 'Metadata Provider' section is selected, showing the configuration for the Pulse Connect Secure (SA) SAML Metadata provider. The 'Entity Id' field is set to 'https://pulsestest.swivelsecure.local/ds'. The 'Metadata Validity' is set to '365 days'. There is a checkbox for 'Do Not Publish IdP in Metadata' which is unchecked. At the bottom, there are buttons for 'Download Metadata', 'Save Metadata Provider', and 'Cancel'.

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




The screenshot shows the Pulse Secure administration console interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Maintenance', and 'Wizards'. The 'Authentication' section is expanded, showing 'SAML > Settings'. The 'Metadata Server Configuration' section is expanded, showing the following fields: 'Timeout value for metadata fetch request' set to '300 seconds', 'Validity of uploaded/downloaded metadata file' set to '0 days', 'Host FQDN for SAML' set to 'est.swivelsecure.local', and 'Alternate Host FQDN for SAML' which is empty. At the bottom, there are buttons for 'Save Changes', 'Cancel', and 'Update Entity Ids'.

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**



[System](#) [Authentication](#) [Administrators](#) [Users](#) [Maintenance](#) [Wizards](#)

Authentication Servers

New:


(Select server type)

New Server...


Delete...

10 records per page

Search

	Authentication/Authorization Servers	Type	User Record Synchronization	Logical Auth Server
	Administrators	Local Authentication		
<input type="checkbox"/>	SentryLore	SAML Server		
<input type="checkbox"/>	System Local	Local Authentication		

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


System **Authentication** Administrators Users Maintenance Wizards

Auth Servers > SentryLore

SentryLore

Settings Users

Server Name:

Settings

*SAML Version:

☐ 1.1 ☒ 2.0

*Connect Secure Entity Id:

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:

Unique SAML identifier of the Identity Provider.

Identity Provider Single Sign On Service URL:

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):

0 - 9999 minutes

☒ Support Single Logout

If checked, Connect Secure supports sending and receiving single logout requests.

*Single Logout Service URL:

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 request.

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:

Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if not applicable.

Select Device Certificate for Encryption:

Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

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: Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

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

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

Available:

- InternetProtocol
- InternetProtocolPassword
- Kerberos
- MobileOneFactorUnregistered
- MobileTwoFactorUnregistered

Selected: (none)

Comparison Method for Authentication Classes:

▼ Service Provider Metadata Settings

Metadata Validity: 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 the metadata.

☐ 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**.

PulseSecure

SystemAuthenticationAdministrators**Users**MaintenanceWizards

User Realms > General

General

User Realms

User Roles

Resource Profiles

Resource Policies

Pulse Secure Client

Enterprise Onboarding

Name:

Description:

User Realms

New User 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:

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:

Role Mapping

Save Changes

Password restrictions

1 Rule

* indicates required field

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

General

General Authentication Policy Role Mapping

* Name: 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: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: 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
<input checked="" type="checkbox"/> 1.	username is "any"	→ Users

When more than one role is assigned to a user:

☒ Merge settings for all assigned roles

☐ User must select from among assigned roles

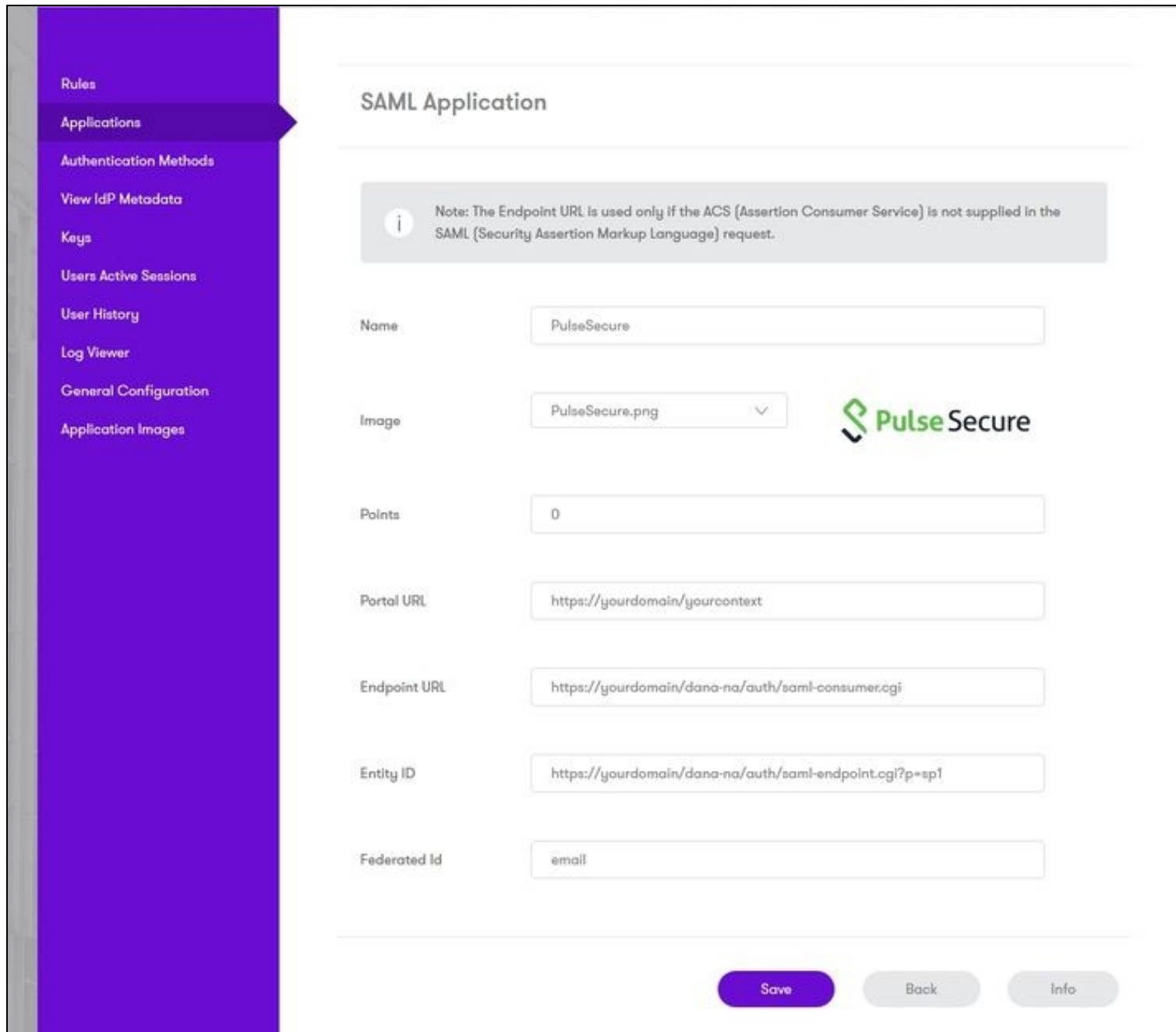
☐ User must select the sets of merged roles assigned by each rule

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**



The screenshot shows the Sentry Administration Console interface. On the left is a purple sidebar with navigation links: Rules, Applications (highlighted), Authentication Methods, View IdP Metadata, Keys, Users Active Sessions, User History, Log Viewer, General Configuration, and Application Images. The main content area is titled 'SAML Application'. Below the title is a note: 'Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.' The configuration form includes fields for Name (PulseSecure), Image (PulseSecure.png with a dropdown arrow), 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), and Federated Id (email). To the right of the Image field is the PulseSecure logo. At the bottom right are three buttons: Save (purple), Back (grey), and Info (grey).

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.

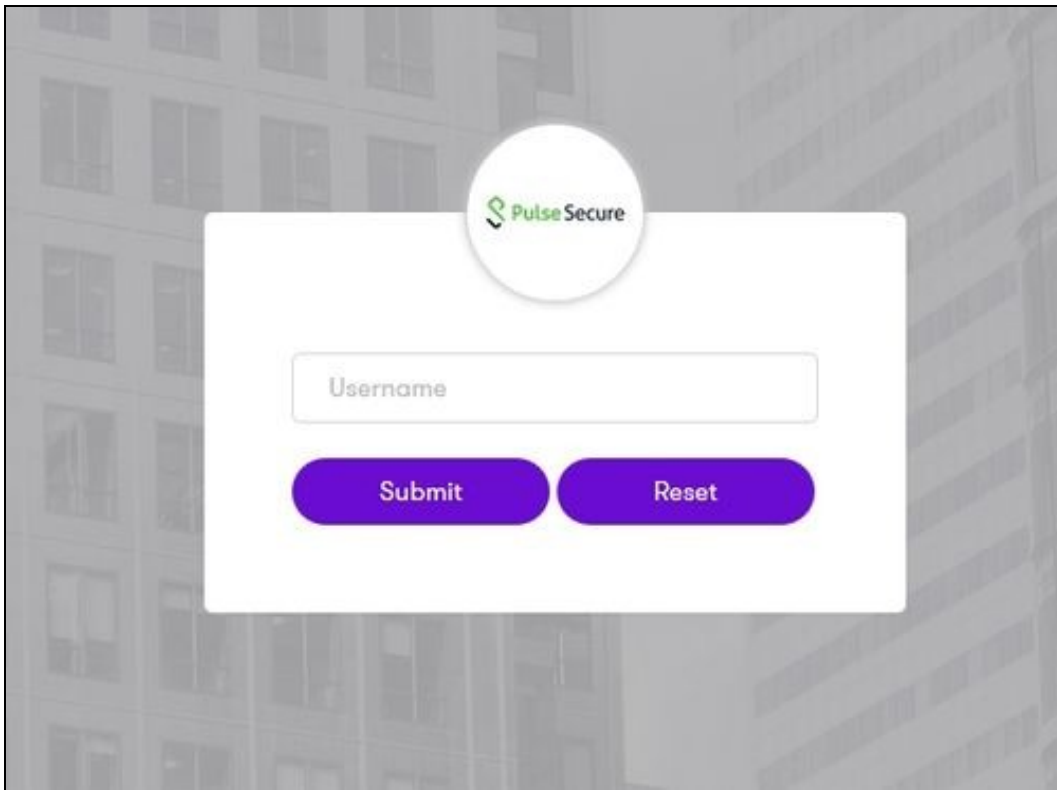
https://mycompanysentrydomain/sentry/startPage On a Start Page you will be able to see a new PulseSecure Icon on which you can click and proceed with authentication (as you would by going straight to the PulseSecure page)

Please select an application

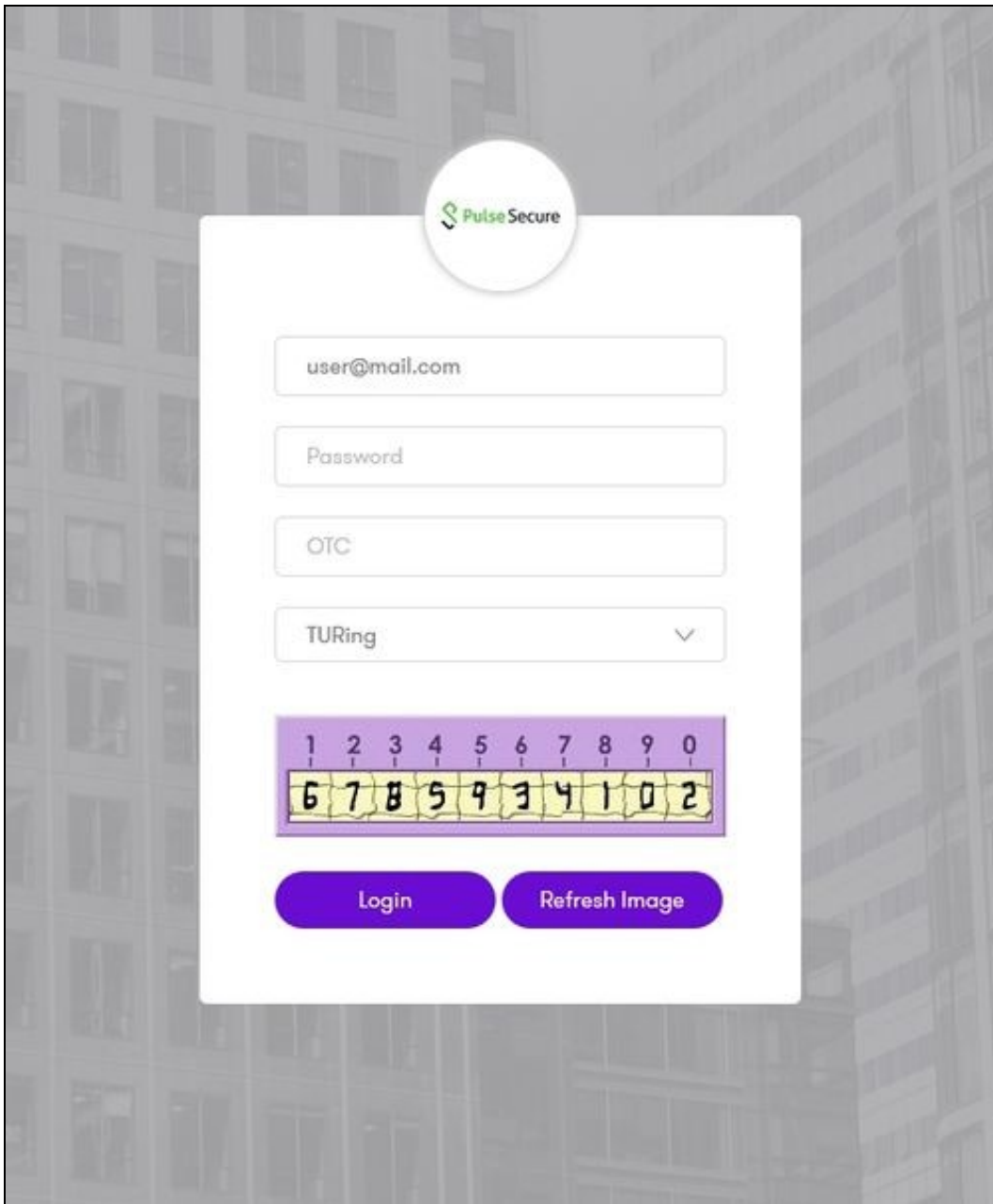


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the PulseSecure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



The image shows a PulseSecure login interface overlaid on a blurred background of a modern building. The interface is a white rectangular box with rounded corners. At the top center is the PulseSecure logo, which consists of a green circular icon with a white 'S' and the text 'PulseSecure' in green. Below the logo are four input fields: a text field containing 'user@mail.com', a text field labeled 'Password', a text field labeled 'OTC', and a dropdown menu labeled 'TURing' with a downward arrow. Below these fields is a 10-digit numeric keypad. The keypad has a purple border and a yellow background. The digits are arranged in two rows: the top row contains 1 through 9 and 0, and the bottom row contains 6, 7, 8, 5, 9, 3, 4, 1, 0, 2. Below the keypad are two purple buttons with white text: 'Login' and 'Refresh Image'.

PulseSecure

user@mail.com

Password

OTC

TURing ▼

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

Login Refresh Image

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