# Sentry SSO with OneLogin

## Contents



## Introduction

This article explains how to integrate the One Login Web portal with Auth Control Sentry. This article does not cover the initial setting-up of Sentry and assumes that you have generated the required keys etc. These steps are covered in other articles , eg Sentry_SSO_with_Salesforce

The following article maybe a useful reference.

https://support.onelogin.com/hc/en-us/articles/201173344-Trusted-IdP-Relying-Party-Trust-

**NOTE** OneLogin requires http://www.w3.org/2001/10/xml-exc-c14n# canonicalisation. Check your version supports this

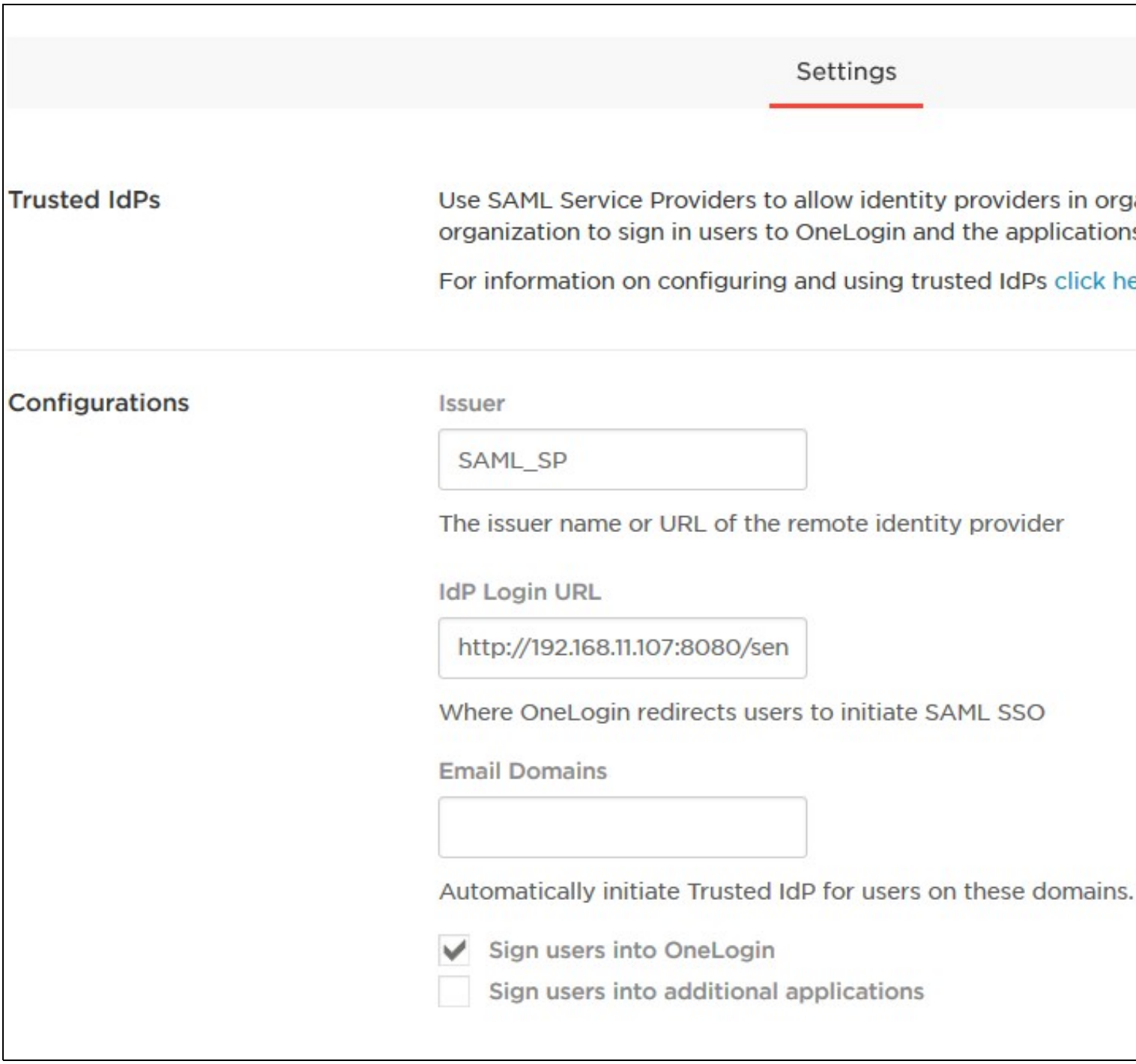
## OneLogin Setup

In order to set-up your Onelogin domain to use Auth Control Sentry as its Identity Provider you first need to log into the OneLogin Admin Console.

You then need to go to Settings->Security->Trusted IdPs

This will take you to a page where you can add an IdP by clicking the NEW TRUST button.

Create a new Trust called Swivel (or something of your own choosing) and complete the following settings




**Issuer**

This is the issuer of the SAML assertion. This is set within settings.properties (refer to Sentry Manual ) So this entry needs to match that set with settings.properties.

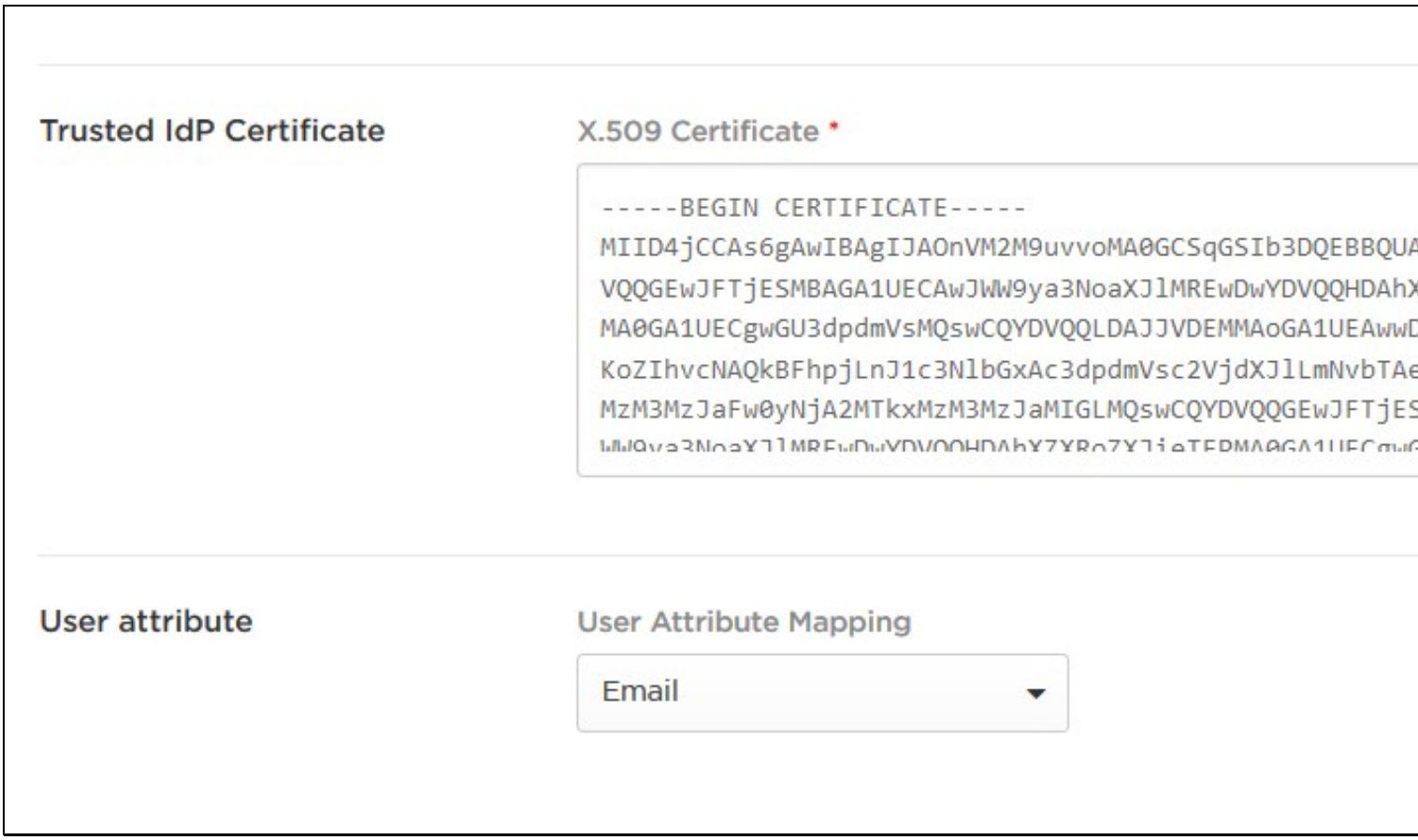
**IdP Login Url**

This will be the external URL of your Sentry login page. For example if the public hostname of your Sentry server is sentry.domain.com this value would be https://sentry.domain.com:8443/sentry/saml20endpoint

This can also be an IP address and need not be https, but for production hostname and https are recommended.

**Email Domains** If your one-login account covers multiple domains you can list the domains here that you want to use this IdP. If you only have one domain this field can be left blank.

**Sign Users into ..** You can configure this IdP to log users into their OneLogin account only or into this account and any applications that have been added to this account.




**Trusted IdP Certificate** This is the certificate that Sentry will use to sign the SAML assertion. You can get this information by logging onto to the Sentry admin console and using the view certificates option or view metadata option. You need to cut and past the certificate information, inlcuding the begin and end certificae header and footer by ensuring that no whitespace is added.

**User Attribute** This is an optional field to be used if, for example, users are logging in with attributes other than their email address.

## Sentry Configuration

You need to add the OneLogin application to the Sentry admin console. If you have the option to add "OneLogin" as an application type use this option. If not then select the SwivelServiceProvider option.

# SAML Application

Note: The Endpoint URL is used only if the ACS
SAML (Security Assertion Markup Language) r

| | |
|---|---|
| Name | OneLogin |
| Image | OneLogin.png |
| Points | 0 |
| Portal URL | https://yourdomain.onelog |
| Endpoint URL | https://yourdomain.onelog |
| Entity ID | https://yourdomain.onelog |
| Federated Id | email |

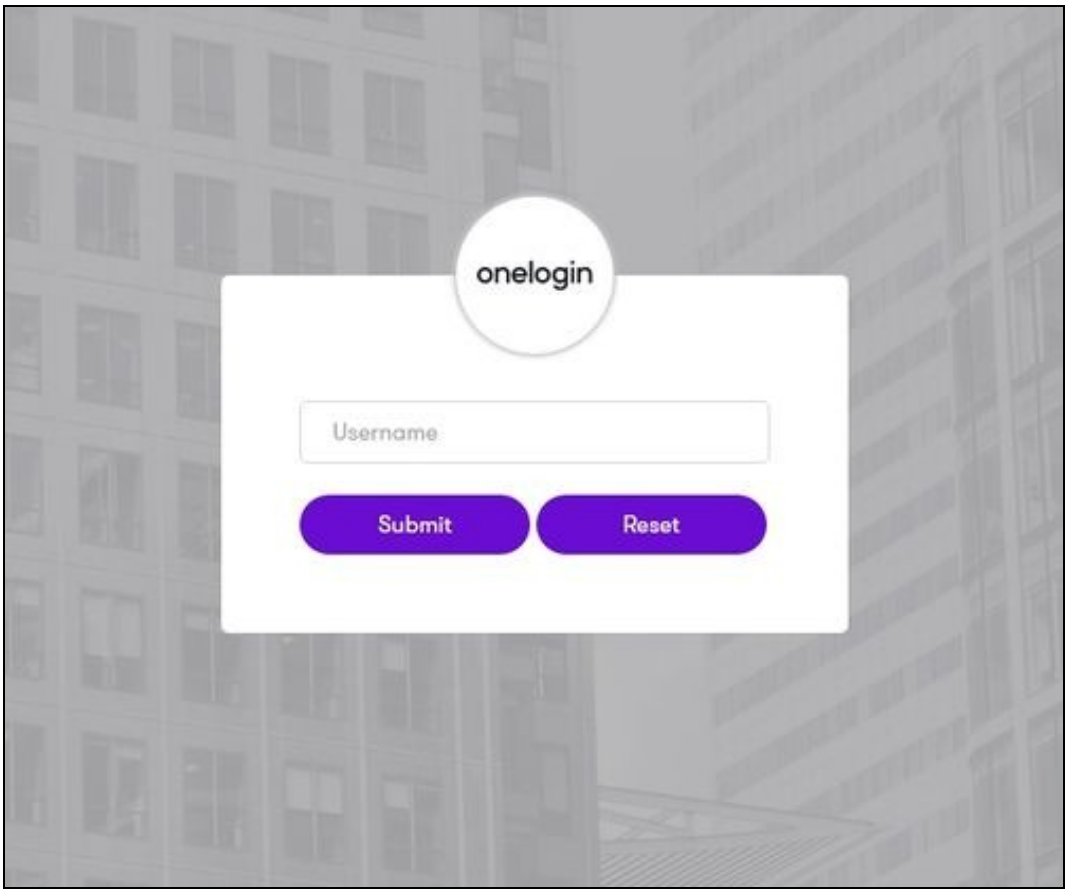
You need to specify

- **Name:** OneLogin
- **Image:** OneLogin.png (Selected by default)
- **Points:** The number of points required to access this service
- **Portal URL:** https://yourdomain.onelogin.com
- **Endpoint URL** This is the URL to which the Sentry server will redirect the user with their SAML assertion after authentication. This will be in the format of yourdomain.onelogin.com/sessions/saml. In this case domain is the domain you have registered with OneLogin.
- **Entity ID** This will be in the format of https://yourdomain.onelogin.com
- **Federated Id** email

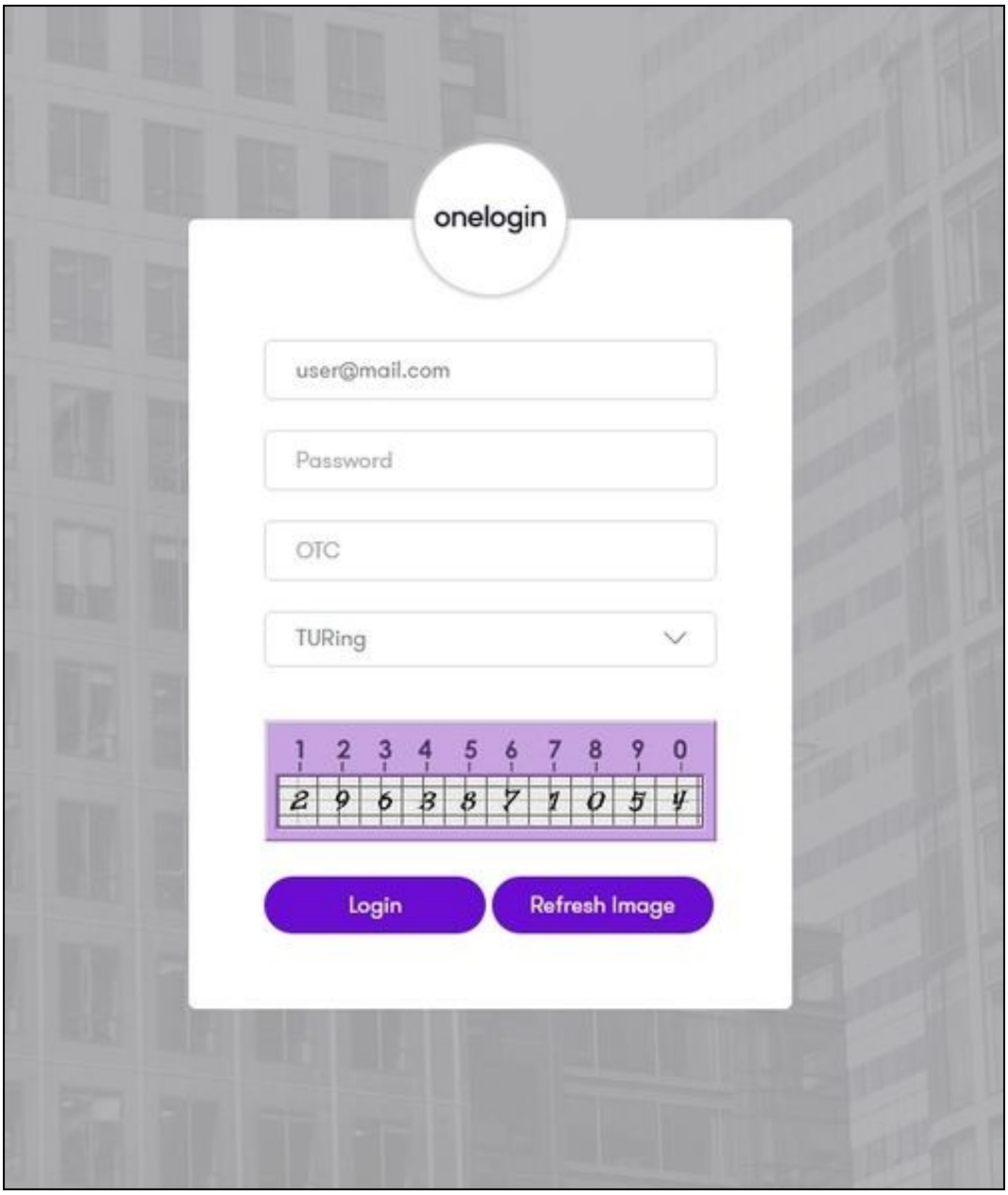
## Testing

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 OneLogin Icon on which you can click and proceed with authentication (as you would by going straight to the OneLogin page)


You should be redirected to the Sentry Login Page.




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




After you enter your authentication credentials you successfully will see the OneLogin account that you tried to access.

## Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from OneLogin

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

```
* Certificate or decryption issues;
    * Can AuthControl Sentry find the Certificate locally, is it the correct one?
    * Has the correct Metadata been uploaded to the OneLogin?
    * Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core
```

Most common issues are likely to be related to the SAML response and whether the OneLogin portal will accept it. To see the SAML response that Sentry is generating you can use a Firefox Plug-in called SAML Tracer https://addons.mozilla.org/en-GB/firefox/addon/saml-tracer/ There are also some on-line tools you can use to validate the SAML assertion https://www.samltool.com/