Passle SSO (Single Sign-On) Integrations

v1.4

Contents

1. Introduction **3**

2. SAML 2.0 Integration **4**

SAML Configuration 4

Configuration data from you 4

Configuration data from Passle 4

Account authentication 4

Security & Signing 5

Enabling and testing the integration 5

3. SAML 2.0 *Multi-Tenant* Integration **6**

Multi-Tenant SAML Configuration 6

Configuration data from you 6

Configuration data from Passle 6

Account authentication 6

Security & Signing 7

Enabling and testing the integration 7

4. JWT Integration with Shared Secret or Certificate **8**

Updating your Secret Key/Certificate 9

1. Introduction

Single Sign-On (SSO) mitigates compliance and security risks for organisations by giving businesses control over user authentication and user revocation via corporate mandated tools.

The purpose of this document is to describe the SSO capabilities Passle supports, and the steps necessary to integrate an Identity Provider (IdP) with Passle. This document is created for those with knowledge regarding the technicalities of SSO integration.

Please note that all of our SSO integrations are used for authentication only, not authorization. A Passle user's permissions are managed by your Passle Administrator via their Passle account.

If you have any questions or feedback, please contact support@passle.net.

2. SAML 2.0 Integration

In order to integrate with Passle, your IdP (Identity Provider) must support SAML 2.0.

SAML Configuration

Configuration data from you

In order to configure SSO, you will need to provide the following details:

1. SSO Service URL: IdP URL where login requests will be directed (GET)
2. Entity ID / Issuer
3. Single logout URL (optional): where to send users after single logout
4. Public x509 Certificate
5. Signature Algorithm used (either RSA-SHA1, RSA-SHA256, RSA-SHA384 or RSA-SHA512)

These details are often provided by your IdP via an XML file. If your IdP provides this XML via an externally available URL, then please just provide the URL and we can load the data directly from there.

Configuration data from Passle

Passle provides our metadata via the following URL:

```
https://www.passle.net/saml/[Your client shortcode]/metadata
```

If you're not sure what your client shortcode is, please ask your contact at Passle or email support@passle.net.

Account authentication

In order to log a user in, Passle needs to match the email address of the user we have in our application with the email address found in the SAML packet.

Passle looks for the email address in the Name Identifier or an Email Assertion, so you must populate at least one of those fields with the user's email address.

Security & Signing

By default, SAML responses must be signed. We do not need the assertions to be signed.

If you need additional security capabilities, please contact support@passle.net.

Enabling and testing the integration

Once you have configured your IdP, please contact support@passle.net with the required information described above and our team will do the configuration required for your IdP on the Passle application. Once this is complete, we will enable SSO for your users and work with you to test and ensure that it is working correctly.

3. SAML 2.0 *Multi-Tenant* Integration

In order to integrate with Passle, your IdP (Identity Providers) must support SAML 2.0.

Multi-Tenant SAML Configuration

Configuration data from you

In order to configure SSO, you will need to provide the following details for each domain:

1. SSO Service URL: IdP URL where login requests will be directed (GET)
2. Entity ID / Issuer
3. Single logout URL (optional): where to send users after single logout
4. Public x509 Certificate
5. Signature Algorithm used (either RSA-SHA1, RSA-SHA256, RSA-SHA384 or RSA-SHA512)

These details are often provided by the IdPs, via XML files. If your IdPs provides this XML via externally available URLs, please just provide us with the URLs for each domain and we can load the configuration data directly, from each of the urls.

Configuration data from Passle

Passle provides separate metadata, for each of your tenants, via the following URL format:

```
https://www.passle.net/saml/[Your client shortcode]/[domain identifier]/metadata
```

Please liaise with your client success contact or the Passle Support team (email support@passle.net) to confirm the metadata, for each tenant/instance.

Account authentication

In order to log in a Passle user, we check that the email address of the user we have in our application, matches the email address in the SAML token.

When a user attempts to log in, the Passle application determines their organization (usually via their email domain/custom tenant URL) and securely directs authentication to the appropriate directory.

Passle looks for the email address in the Name Identifier or an Email Assertion, so you must populate at least one of those fields with the user's email address.

Security & Signing

By default, SAML responses must be signed. We do not need the assertions to be signed.

If you need additional security capabilities, please contact support@passle.net.

Enabling and testing the integration

Once you have configured your IdP, please contact support@passle.net with the required information described above and our team will complete the configuration required for your IdP(s) on the Passle application. Once this is complete, we will enable SSO for users and work with you, to test and ensure that it is working correctly for each tenant.

3. JWT Integration with Shared Secret or Certificate

To enable JWT integration using a Shared Secret or Certificate, you will need to provide the following information:

1. An X.509 certificate, or if using a Shared Secret Key, Passle will provide a Base64 encoded 128bit key to be used
2. The URL on your application, which we should redirect to for logging a user in

The login URL that you provide should redirect to `https://www.passle.localhost/SSO/Login/[your client shortcode]` along with the JWT security token as the "token" query string parameter.

If you are not sure what your client shortcode is, please email support@passle.net.

Attribute	Required	Description
iat	Yes	Issued At. The time the token was generated, this is used to help ensure that a given token gets used shortly after it's generated. The value must be the number of seconds since UNIX Epoch.
iss	Yes	Issuer. Please set this to be the root of your authentication URL. Eg. if your URL is `https://www.example.com/jwtlogin` then the issuer should be set to `https://www.example.com/`.
jti	Yes	JSON Web Token ID. A unique ID for the token, used to prevent token replay attacks.
sub	Yes	Email of the user being signed in. Used to uniquely identify the user. Alternatively, the email attribute can be used. One or the other must contain the user's email address.
aud	Yes	The audience the jwt is intended for. Please set this to `https://www.passle.net/`.
email	No	This should be populated with the user's email address, if the sub attribute is not populated.

Updating your Secret Key/Certificate

It is good practice to change your Secret Key or Certificate on a fairly regular basis. In order to update it, please contact support@passle.net. We will be able to work with you to ensure that the Secret Key/Certificate is updated at both ends at the same time to ensure a seamless transition.