Single Sign-On - mashme.io Integration Guide V1

Content

Introduction

The Single Sign-On feature will allow your organization member to login using your corporate credentials, avoiding the need for extra user names and passwords, therefore reducing the time and friction required by a user to access the platform.

This document will guide you to set up your mashme organization in order to prepare for the Single Sign-On integration.

Some information required in this process needs to be provided by your organization prior to the setup. More information is available in this document.

Prerequisites

mashme Single Sign-On (SSO) is based on the standard SAML 2.0, please check that your corporate Identity Provider is compatible with this standard.

mashme has tested the Single Sign-On integration with Identity Providers such as Google, Shibboleth and other SAML-compatible providers. Depending on your specific Identity Provider, we may need to test and adjust our system prior to the integration.

The Single Sign-On integration will turn mashme into a Service Provider able to exchange information with your Identity Provider. The method to initiate authentication in this scheme will be SP-Initiated.

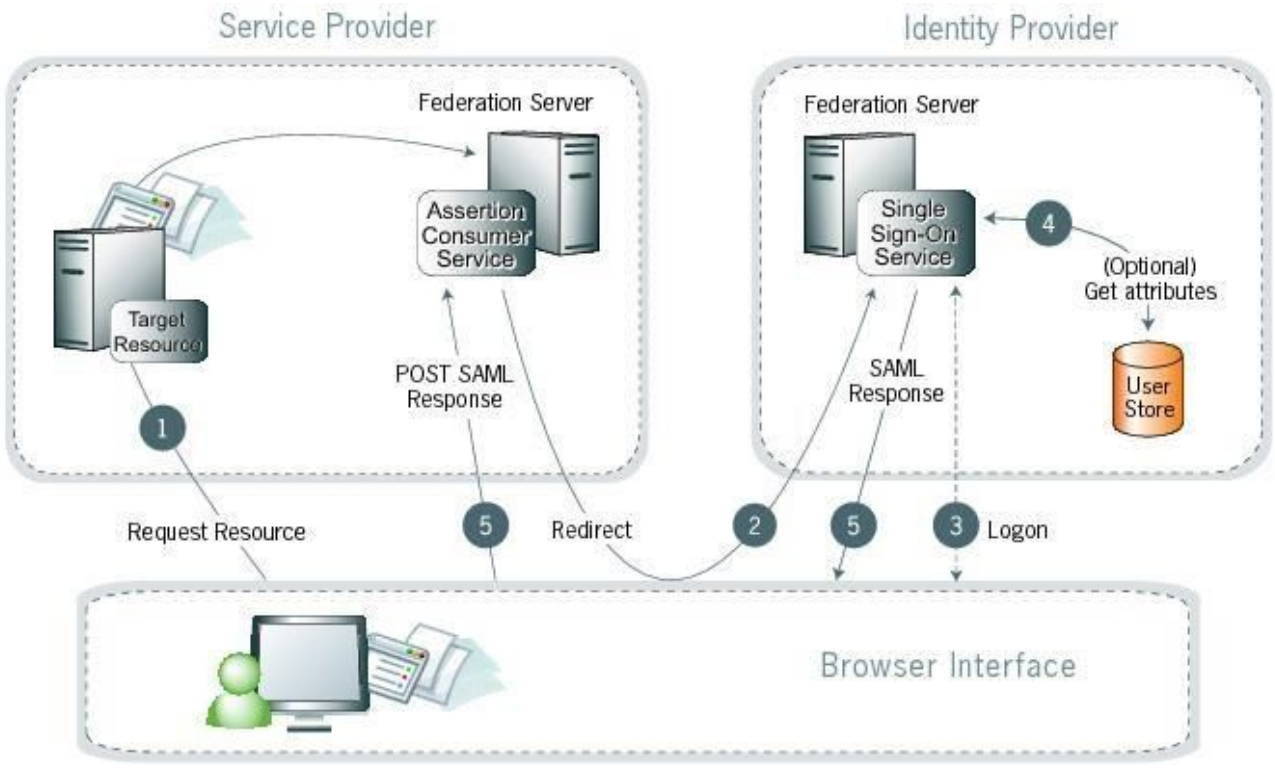
Known limitations

- Single Log-Out
  - SLO is not available at this moment.
  - The log-out action in mashme will only close the application session
- Authentication request signed by SP
  - Not supported at this time

Supported SSO Methods

SP-Initiated SSO: POST/POST (SAML 2.0)

In this scenario, a user attempts to access a protected resource directly on an SP Website without being logged on. The user does not have an account on the SP site but does have a federated account managed by a third-party IDP. The SP sends an authentication request to the IDP. Both the request and the returned SAML assertion are sent through the user's browser via HTTP POST.



Processing Steps:

1. The user requests access to a protected SP resource. The request is redirected to the federation server to handle authentication.

2. The federation server sends an HTML form back to the browser with a SAML request for authentication from the IDP. The HTML form is automatically posted to the IDP's SSO service.

3. If the user is not already logged on to the IDP site or if re-authentication is required, the IDP asks for credentials (e.g., ID and password) and the user logs on.

4. Additional information about the user may be retrieved from the user data store for inclusion in the SAML response.

5. The IDP's SSO service returns an HTML form to the browser with a SAML response containing the authentication assertion and any additional attributes. The browser automatically posts the HTML form back to the SP.

Supported Federation Criteria

Request Signing

The standard specification requires signing for compliance. The IDP certificate will be used for signing the request.

Response Signing

The standard specification requires signing for compliance. The IDP certificate will be used for signing the response.

Response Encryption

Not supported.

Digital Signature Exchange

Digital Signature – used in electronic documents (requests, responses, and assertions) to verify that a person or entity is who they say they are.

Based on mutually agreed-upon digital signature requirements, IDP should provide the following:

- The SAML response signing certificate which has the public key.
- All applicable cert chain(s) of signing certificate (for self-signed certificates only).

Identity Mapping

Identity Mapping is the process in which users authenticated by IDP are associated with user accounts local to the SP.

Based on that, the SSO integration will use the following field mapping:

FIELD	MANDATORY	COMMENTS
EMAIL	YES	This is the unique identifier for a user in mashme
SURNAME	YES	
GIVEN NAME	NO	

Supported Attribute Designations

The following data elements should be used when configuring an IDP connection with SP

Definitions

Entity ID: An entity ID is a globally unique name given to a SAML entity, either an Identity Provider (IDP) or a Service Provider (SP).

Attribute Contract: A list of attributes, agreed to by the partners in an identity federation, representing information about a user (SAML Subject). The attributes are sent from IDP to SP during SSO. Please refer to the below section for a list of required and optional attributes.

Assertion Consumer Service (ACS): The location where the SP receives and consumes assertions. SAML 2.0 defines the Assertion Consumer URL for the POST method.

Target URL (TargetResource or RelayState): The URL for the protected resource that the Identity Provider is trying to access at SP.

SSO SAML Integration Implementation Timeline

IDP – Your organization

SP – mashme.io

Implementation timeline

1. Requirements gathering and definition of scope
    a. Initial call to discuss business requirements and implementation if needed by mashme team
    b. Technical requirements gathering
    c. IDP and SP to exchange SSO related documentation
    d. IDP and SP to exchange SSO Metadata files for preproduction and production environments
    e. IDP and SP to agree and confirm attributes
2. Implementation and deployment (**Minimum of 2-3 weeks to implement, depending on your IDP)**
    a. SP to set up, test and integrate SSO in Preproduction
    b. SP to deploy SSO implementation to Production
    c. SP to test and approve IDP SSO in Production
    d. Application goes live with SAML SSO in PRD

SSO Information provided by Mashme as SP

SSO Workflow

- SP-initiated

Common information for all environments

Assertion Digital Signing (Y/N)	N
Name identifier to be configured	email
Attributes to be sent in SAML assertion	email (urn:oid:0.9.2342.19200300.100.1.3) surname (urn:oid:2.5.4.4) givenName (urn:oid:2.5.4.42)
Certificate if SP signs Authentication request	Not supported

SP Preproduction Environment (sample)

EntityID	`https://yourorganization.syncrtc.io`
Assertion Consumer Service (ACS)	`https://api.syncrtc.io/auth/saml/yourorganization`
SP Metadata	<?xml version="1.0"?> <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://yourorganization.syncrtc.io" ID="https___yourorganization_syncrtc_io"> <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat> <AssertionConsumerService index="1" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://api.syncrtc.io/auth/saml/yourorganization"/>

SP Production Environment (sample)

EntityID	`https://yourorganization.mashme.io`
Assertion Consumer Service (ACS)	`https://api.mashme.io/auth/saml/yourorganization`
SP Metadata	<?xml version="1.0"?> <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://yourorganization.mashme.io" ID="https___yourorganization_mashme_io"> <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat> <AssertionConsumerService index="1" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-PO

SSO Information to be provided by IDP to SP

Fill this information for preproduction and production environments

IDP Environment

Metadata	Certificate (s)

Basic URLs

EntityID	
SSO service URL	
Assertion Digital Signing (Y/N)	YES (signed with IdP public certificate)

Corporate domains under SSO

A set of corporate domains that are included in the SSO authentication flow.

All users with emails containing that domain will have SSO authentication enabled by default.

- Example:
  - SSO domains
    - acme.com
    - other.com
  - User emails
    - john.doe@acme.com
      - SSO authentication activated when registered

- john.black@other.com
  - SSO authentication activated when registered
- john.white@gmail.com
  - Regular authentication (email and password) activated when registered

SSO DOMAIN

Glossary

SAML v2

SAML (Secure Assertion Markup Language) is an open standard for Web SSO, single logout (SLO), and the cross-domain transfer of user attributes. It specifies a set of XML formats and transport mechanisms designed to enable secure, decentralized identity management over the Internet.

In many cases, SAML is the foundation of current identity federation activity. SAML defines a security token format (called an “assertion”) and profiles that define methods for using these assertions to provide Web SSO. In addition, SAML defines a SOAP protocol through which assertions may be served. SAML has gone through three releases (none of which is compatible with the others): 1.0, 1.1, and 2.0. SAML 2.0 is seen as a point of convergence between Liberty and SAML because it incorporates all of Liberty’s early ID-FF 1.1 and 1.2 functionality.

SAML 2.0 is the protocol of choice for most new federations, due to the convergence of the use cases from the previous protocols.

Single Sign-On (SSO)

Single Sign-On (SSO) is a method of leveraging security tokens to indicate authentication between multiple domains, rather than requiring each member of a security domain to re-verify authentication credentials. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Identity Provider (IdP)

An entity that makes various claims about an entity (ex. End User) to SPs. SPs take these claims and make a decision about whether to act on them as true. With SSO, these claims are meant to provide the service with enough information to consider a user authenticated.

Service Provider (SP/Third PartyApplication)

An SP is a consumer of claims from an Identity Provider. Based on the evaluation of the claims as well as any pre-existing relationship between the service and the Identity Provider, the information conveyed can be used for authentication, authorization, and to provide the claims as additional data into other business processes. Within the definitions of SAML, an SP is merely an entity providing a service to others, while an Identity Provider is the “SAML authority,” is a system entity that authenticates a user, or “SAML subject,” and transmits referential identity information based on that authentication.

Assertion/Token

Assertions are XML documents sent from an IDP to an SP. Each assertion contains identifying information about a user who has initiated a SSO request. Three types of statements can be conveyed in SAML assertions:

- A piece of data produced by a SAML authority regarding an act of authentication performed on a subject
- Attribute information about the subject
- Authorization data applying to the subject with respect to a specified resource

Attribute/Claim

Attributes are distinct characteristics of an object (in SAML, of a subject). An object’s attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, etc.

1 Attributes are often represented as pairs of "attribute name" and "attribute value(s). Often, these are referred to as "attribute value pairs". Note that identifiers are essentially "distinguished attributes". Claims are statements about various attributes/characteristics of an entity.

Bindings

A SAML binding describes the way messages are exchanged using transport protocols. Some common SAML 2.0 bindings are:

- HTTP POST – Describes how SAML messages are transported in HTML form-control content, which uses a base-64 format.
- HTTP Artifact – Describes how to use an artifact to represent a SAML message. The artifact can be transported via an HTML form control or a query string in the URL.
- HTTP Redirect – Describes how SAML messages are transported using HTTP 302 status-code response messages.
- SOAP – Describes how SAML messages are to be transferred across the backchannel.

Most common SAML bindings are:

- HTTP POST – Describes how SAML messages are transported in HTML form-control content, which uses a base-64 format.

- HTTP Artifact – Describes how to use an artifact to represent a SAML message. The artifact can be transported via an HTML form control or a query string in the URL.

Profiles

Profiles describe processes and message flows combining assertions, request/response message specifications, and bindings to achieve a specific desired functionality or use case. SAML 2.0 is the most commonly used profile currently in the industry.

Metadata

SAML 2.0 defines an XML schema to standardize metadata to facilitate the exchange of configuration information among federation partners. This information includes, for example, profile and binding support, connection endpoints, and certificate information. Exchanging metadata files as “Best Practices” is common in the industry.