Single Sign-On - mashme.io administrator Guide V1

Contents

Introduction

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

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

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 Identity Provider is compatible with this standard.

mashme has tested the SSO 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 SSO integration will turn mashme.io 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

- Autoprovision users
    - Limitation:
        - It is not possible to auto-provision users in mashme

        - A user must be registered in mashme in order to access the platform, even if the user has been authenticated by the Identity Provider.
- It is not possible to change the authentication strategy for registered users
    - Limitation:
        - The current SSO integration will assign an authentication strategy to new users based on the list of domains configured for SSO in your organization (more information see - Assigning the right authentication method to new users).
        - The organization can not change the authentication strategy for a specific user at this time.
    - Workaround:
        - If your organization requires a change to the authentication strategy for a user, contact the mashme support team and your request will be managed directly by them.
- It is not possible to change the domains configured for SSO in your organization (more information see - Enabling SSO authentication in your organization)
    - Limitation:
        - The current SSO integration will have a set of domains used to assign the right authentication strategy when a new user is registered.
        - The organization can not change the set of domains for your organization at this time.
    - Workaround:
        - If your organization requires to change the set of SSO domains, contact the mashme support team and your request will be managed directly by them.

SSO as a new authentication method

When SSO is activated for your organization, mashme.io will present two different authentication methods for all users:

- Regular login: using the user's email and password
- SSO login: using the corporate identity provider

Each user will have a unique authentication method thus only one option will allow the user to access the platform. Please, contact your organization's support team if you have any questions regarding what authentication method has been assigned to you.

The organizations will have both authentication methods available in order to onboard users that do not belong to the organization and SSO corporate authentication.

Depending on the authentication method, the platform will generate a different output related to:

- Email notification templates
    - The user onboarding email template will not have a password with SSO authentication

- Login
    - A user with SSO authentication will be warned when attempting to use the regular login
- Forgot password
    - A user with SSO authentication will be warned when using the ‘forgot password’ action
- Reset password
    - A user with SSO authentication will not have the ‘reset password’ link in the user profile

Enabling the SSO authentication in your organization

In order to enable or disable the SAML-SSO authentication in your organization, you need to contact the mashme support team.

Besides the requisites described in the SSO integration guide, from the administration point of view the most important aspect to configure is the list of corporate domains that coexist in the Identity Provider.

Those domains will be used by the platform to assign the right authentication strategy for new users, as explained in the next section.

In order to change the list of domains configured in your organization, you need to contact the support team.

Authorizing new users to access mashme

It is mandatory to be a registered user in mashme in order to access the platform. This is also mandatory for SSO users.

If any user tries to access mashme through the SSO feature without being registered, an error code (M207) will be displayed to let the user know the reason.

Given that, a user can be authenticated by your Identity Provider but not authorized to access mashme if the user has not been registered previously.

Assigning the right authentication method to new users

As explained in the previous section, your organization needs to provide a set of domains that are covered by your Identity Provider.

The platform will use that set of domains to assign the SSO authentication method for those users whose email address contains a domain in that list.

In order to change the authentication method for any user, you need to contact the mashme support team.

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