SAML2 and SSO Overview

Version 1.0

Abstract

The LiveSafe platform supports SSO in two areas, in the traditional sense for the Command Dashboard and as a checkpoint for joining an organization from within the mobile application.

Goal

This document will explain both the use of SAML 2.0 assertions and SSO in the LiveSafe platform as well as the needed information and process used to setup and validate the SSO configuration between a client organization and LiveSafe. We support a Service Provider (SP) initiated flow via PingFederate for SAML/SSO processing, but any standards-based SAML 2.0 Identity Provider (IdP) should be supported.

Platform Functionality

Command Dashboard SSO

The Command Dashboard supports the option to use SSO instead of the the built in authentication mechanism provided by the platform. Once configured, the organization administrators will be provided a custom login URL. This URL will begin a standard SSO flow where the user is taken to the client's login page. Once the user logs in successfully, the SAML 2.0 assertion is passed back to the LiveSafe identity server where the assertion is validated and information (including email address) is extracted via our application servers. The user is the logged into the command dashboard and has privileges as assigned within the LiveSafe platform.

Mobile Application SAML Integration

If so configured, the same SSO exchange can be leveraged from within the mobile application to act as a checkpoint for joining the organization. In this configuration, mobile users first select the organization (or start via a deep-link) and are then presented with the same SAML flow as described above. The client's identity provider login screen is presented and the user logs in. Upon successful login, the user is then granted access to the organization. This only happens when initially joining the organization and will not be presented again unless the user is removed from the organization and then attempts re-join.

Configuration

To setup the SAML exchange, we follow a standard process of exchanging metadata about both the client's identity provider and that of the LiveSafe identity servers. We do this first in our staging environment, connecting to our client's staging system. We then verify the exchange of data and that we have the required fields needed in the assertion.

The fields that should be included in the SAML metadata and that are exchanged in the assertion are:

- SAML_SUBJECT (required) - this should be the unique identity for the user on the client's systems. It can be an email or a userid
- Email address (required) - email address for the user
- First name (required) - user's first name
- Last name (required) - user's last name
- Mobile phone (optional) - user's mobile phone number

NOTE: To avoid delays in the integration, please make sure that the assertion attributes, claim types, etc. for the aforementioned fields are included in the metadata. As a general recommendation, the phone number provided should be the mobile (cell phone) number for the user. If you do not have this information, you do not need to include it in the assertion (e.g. do not include office number).

Once verified in staging, we will do the same exchange of metadata information for the production servers and then can go live based on the client's desired launch date.

Summary

Federation Method: SP Initiated
SAML Services Used: Ping Identity
SAML Version: 2.0
SAML Transport Method: Post, Redirect
Environment: UAT, Production
Assertion Consumer Service End Point URL (#### - org specific)
    Stage URL: https://devstg-idp.livesafemobile.com:####
    Prod URL: https://idp.livesafemobile.com:####
SP Entity ID: Stage, Production
SAML NameID Format: Unspecified

Environment: UAT, Production
Assertion Consumer Service Endpoint URL (#### - org specific)
    Stage URL: https://devstg-idp.livesafemobile.com:####
    Prod URL: https://idp.livesafemobile.com:####
SP Entity ID: Stage, Production
    Livesafe
    Idp.livesafemobile
SAML_SUBJECT Value: UID (should be persistent, revocable, and non-reassignable)
Application Header: UID, Email, First Name, Last Name, Other (Mobile phone – Optional)

References

- https://en.wikipedia.org/wiki/SAML_2.0
- https://documentation.pingidentity.com/display/PF66/SP-Initiated+SSO--Redirect-POST

Revision History

Date	Version	Description
2016-11-29	1.0	First release.
2017-1-27	1.1	Added summary.
2018-7-18	1.2	Added clarification to assertion attributes under configuration Added clarification on SAML_SUBJECT UID Added SAML NameID Format