imc
part of Scheer

SS0 SAML2

Service Description

imc Learning Suite

08.10.2024

im-c.com

Preface

A service description provides clarity and communication by clearly defining what the service is, its scope, and boundaries, ensuring a common understanding among all stakeholders. It specifies the service levels and quality metrics, setting expectations for performance and reliability. Additionally, it details the dependencies and interactions with other services, outlining necessary integrations. The roles and responsibilities of both the service provider and the customer are clearly defined, ensuring accountability.

Context

This service description applies to the implementation of Single Sign-On (SSO) using Security Assertion Markup Language 2.0 (SAML 2.0) for the imc Learning Suite. SSO allows users to authenticate once and gain access to multiple applications without having to log in separately to each one. SAML 2.0 is a widely-adopted protocol for implementing SSO, providing secure, federated identity management across various systems.

This document will guide you through the process of setting up SSO with SAML 2.0 and the imc Learning Suite, including the necessary roles and responsibilities to ensure a successful integration.

Description of the Service

The SSO SAML2 implementation for the imc Learning Suite involves configuring the Learning Suite to authenticate users via a third-party Identity Provider (IdP) using the SAML 2.0 protocol. This integration enables seamless access to the Learning Suite with existing credentials from the customer's authentication system.

Prerequisites:

Identity Provider (IdP): A functioning IdP that supports SAML 2.0 (e.g., Okta, Entra / Azure AD, ADFS).
Metadata Exchange: Exchange of metadata files between the IdP and Service Provider (imc Learning Suite).
SSL Certificate: Valid SSL certificate for secure communication.

Roles and Responsibilities:

Customer
Project Manager: Oversees the SSO implementation project, coordinating between internal teams and imc.
IT Administrator: Provides the IdP federation metadata, configures the IdP with the Service Provider (SP) metadata.

imc
Project Manager: Manages the project from imc's side, ensuring timelines and deliverables are met.
Technical Services: Assists with the configuration of the Learning Suite, provides SP metadata, and supports the customer's IT team during integration.
Support: Offers ongoing support and troubleshooting post-implementation project activities.

Setup process

The setup process for Single Sign-On (SSO) using Security Assertion Markup Language 2.0 (SAML 2.0) in the imc Learning Suite is comprehensive and involves several critical steps to ensure a secure and seamless integration.
The process begins with the customer providing the necessary federation metadata as URL or file to the imc team. This includes all federation metadata for all systems, as in the most sophisticated scenario production, staging and development systems. The federation metadata file is crucial as it contains information about the Identity Provider (IdP), such as its endpoints and certificates, which are necessary for establishing a trust relationship between the IdP and the Service Provider (SP). Additionally to the federation metadata, imc also requires the information which subject or unique identifier will be send from the IDP along with the SAML response to identify and authenticate the user. This could be the email address, a username or any other attribute that is unique for a user. On top of federation metadata and subject/unique identifier, ideally imc receives a test user account from the customer so that imc is able to do testing independent from customer involvement.

Following the provision of all the above information, imc team as a next step provides the ServiceProvider.xml file to the customer. This file contains the required metadata for the Service Provider (SP), including its endpoints and certificates, which the customer's IdP needs to recognize and trust the SP. By exchanging these metadata files, both systems can securely communicate, ensuring that the authentication assertions sent from the IdP are trusted and accepted by the SP. This secure communication is fundamental to the integrity of the SSO setup.

Once the metadata exchange is complete, the next step is to validate the SSO configuration through testing. If imc was provided with a test user, imc can test independent the SSO configuration. If no test user was provided, customer team needs to test and report to imc the result. This testing is critical as it verifies that the SSO integration is functioning correctly, allowing a user to authenticate via the IdP and gain access to the imc Learning Suite without having to log in separately. This testing phase involves checking various aspects of the authentication process, such as the redirection to the IdP, the handling of authentication assertions, and successful login to the Learning Suite.

The successful completion of these tests confirms that the SSO setup is correctly configured and ready for activation to a wider target group.

Best Practice Approach

To achieve an optimal SSO implementation, it is highly recommended that the customer provides a test user account to the imc team at the beginning of the implementation. This test account is essential for independent testing and verification of the SSO configuration. By using a test account, the imc team can simulate the user authentication process and identify any potential issues or misconfigurations without impacting actual user accounts. This proactive approach ensures that any problems are resolved early in the implementation phase, leading to a smoother and more efficient setup.

Engaging with key stakeholders from both the customer's and imc's teams is also crucial. Clear and continuous communication throughout the implementation helps in aligning expectations, clarifying requirements, and addressing any concerns that may arise. Stakeholders should be involved in regular updates and discussions to ensure that the project stays on track and any adjustments needed are made promptly.

Furthermore, it is essential to document all configurations, steps, and findings during the implementation process. This documentation serves as a valuable reference for future troubleshooting and maintenance. It also helps in ensuring that all team members are informed about the setup details and can contribute effectively to the implementation’s success.

By adhering to these best practices, the SSO implementation is more likely to be successful, providing users with a seamless and secure authentication experience while accessing the imc Learning Suite.

Overview of tasks & responsible parties

Tasks	Responsible Party
Configuration of the Identity Provider	Customer
Provide FederationMetadata.xml for all systems and subject / unique identifier attribute	Customer
Provide test account for SSO testing to imc	Customer
Provide ServiceProvider.xml	imc
Test SSO with provided test user account from customer	imc
Test SSO with several user accounts	Customer