Scheer IMC

SSO SAML2

Servicebeschreibung

imc Learning Suite | Consulting Department | 26 August 2025

Inhalt

Scheer IMC
information multimedia communication AG

Scheer Tower, Uni-Campus Nord
66123 Saarbrücken
Deutschland

Tel. +49 681 9476-0
Fax +49 681 9476-530
info@im-c.de
scheer-imc.de

1 Vorwort

Eine Servicebeschreibung sorgt für Klarheit und Kommunikation, indem sie klar definiert, wasder Service ist, welchen Umfang und welche Grenzen er hat, und so ein gemeinsamesVerständnis aller Beteiligten sicherstellt. Sie gibt die Servicelevel und Qualitätsmetriken an undlegt Erwartungen an Leistung und Zuverlässigkeit fest. Darüber hinaus beschreibt sie detailliertdie Abhängigkeiten und Interaktionen mit anderen Services und skizziert notwendigeIntegrationen. Die Rollen und Verantwortlichkeiten sowohl des Serviceanbieters als auch des Kunden sind klar definiert, wodurch Verantwortlichkeit gewährleistet wird.

2 Kontext

Diese Servicebeschreibung gilt für die Implementierung von Single Sign-On (SSO) mit Security Assertion Markup Language 2.0 (SAML 2.0) für die imc Learning Suite. SSO ermöglicht es Benutzern, sich einmal zu authentifizieren und auf mehrere Anwendungen zuzugreifen, ohne sich bei jeder einzeln anmelden zu müssen. SAML 2.0 ist ein weit verbreitetes Protokoll zur Implementierung von SSO und bietet sicheres, föderiertes Identitätsmanagement über verschiedene Systeme hinweg.

Dieses Dokument führt Sie durch den Prozess der Einrichtung von SSO mit SAML 2.0 und der imc Learning Suite, einschließlich der erforderlichen Rollen und Verantwortlichkeiten, um eine erfolgreiche Integration sicherzustellen.

3 Beschreibung des Dienstes

Bei der SSO SAML2-Implementierung für die imc Learning Suite wird die Learning Suite so konfiguriert, dass Benutzer über einen Identity Provider (IdP) eines Drittanbieters unter Verwendung des SAML 2.0-Protokolls authentifiziert werden. Diese Integration ermöglicht einen nahtlosen Zugriff auf die Learning Suite mit vorhandenen Anmeldeinformationen aus dem Authentifizierungssystem des Kunden.

3.1 Voraussetzungen

Identity Provider (IdP): Ein funktionierender IdP, der SAML 2.0 unterstützt (z. B. Okta, Entra / Azure AD, ADFS).

Metadatenaustausch: Austausch von Metadatendateien zwischen IdP und Service Provider (imc Learning Suite).

SSL-Zertifikat: Gültiges SSL-Zertifikat für sichere Kommunikation.

3.2 Rollen und Verantwortlichkeiten

Kunde: Überwacht das SSO-Implementierungsprojekt und koordiniert zwischen internen Teams und imc.IT-Administrator: Stellt die IdP- Föderationsmetadaten bereit, konfiguriert den IdP mit den Service Provider (SP)-Metadaten.

imc -Projektmanager: Verwaltet das Projekt von imc-Seite aus und stellt sicher, dass Zeitpläne und Leistungen eingehalten werden. Technische Dienste: Hilft bei der Konfiguration der Learning Suite, stellt SP-Metadaten bereit und unterstützt das IT-Team des Kunden während der Integration. Support: Bietet fortlaufenden Support und Fehlerbehebung bei Projektaktivitäten nach der Implementierung.

4 Einrichtungsprozess

Der Einrichtungsprozess für Single Sign-On (SSO) mit Security Assertion Markup Language 2.0 (SAML 2.0) in der imc Learning Suite ist umfassend und umfasst mehrere wichtige Schritte, um eine sichere und nahtlose Integration zu gewährleisten.

Der Prozess beginnt damit, dass der Kunde dem imc-Team die erforderlichen Föderationsmetadaten als URL oder Datei zur Verfügung stellt. Dazu gehören alle Föderationsmetadaten für alle Systeme, wie in den anspruchsvollsten Szenarien Produktions-, Staging- und Entwicklungssysteme. Die Föderationsmetadatendatei ist von entscheidender Bedeutung, da sie Informationen über den Identitätsanbieter (IdP) enthält, wie z. B. seine Endpunkte und Zertifikate, die zum Aufbau einer Vertrauensbeziehung zwischen dem IdP und dem Dienstanbieter (SP) erforderlich sind. Zusätzlich zu den Föderationsmetadaten benötigt imc auch die Informationen, welcher Betreff oder welche eindeutige Kennung vom IDP zusammen mit der SAML-Antwort gesendet wird, um den Benutzer zu identifizieren und zu authentifizieren. Dies kann die E-Mail-Adresse, ein Benutzername oder ein anderes Attribut sein, das für einen Benutzer eindeutig ist. Zusätzlich zu den Föderationsmetadaten und dem Betreff/der eindeutigen Kennung erhält imc im Idealfall ein Testbenutzerkonto vom Kunden, damit imc Tests unabhängig von der Beteiligung des Kunden durchführen kann. Nach der Bereitstellung aller oben genannten Informationen stellt das imc-Team dem Kunden im nächsten Schritt die Datei ServiceProvider.xml zur Verfügung. Diese Datei enthält die erforderlichen Metadaten für den Service Provider (SP), einschließlich seiner Endpunkte und Zertifikate, die der IdP des Kunden benötigt, um den SP zu erkennen und ihm zu vertrauen.

Durch den Austausch dieser Metadatendateien können beide Systeme sicher kommunizieren und sicherstellen, dass die vom IdP gesendeten Authentifizierungsbehauptungen vom SP als vertrauenswürdig eingestuft und akzeptiert werden. Diese sichere Kommunikation ist für die Integrität des SSO-Setups von grundlegender Bedeutung. Sobald der Metadatenaustausch abgeschlossen ist, besteht der nächste Schritt darin, die SSO-Konfiguration durch Tests zu validieren. Wenn imc ein Testbenutzer zur Verfügung gestellt wurde, kann imc die SSO-Konfiguration unabhängig testen. Wenn kein Testbenutzer bereitgestellt wurde, muss das Kundenteam den Test durchführen und imc das Ergebnis mitteilen. Dieser Test ist von entscheidender Bedeutung, da er überprüft, ob die SSO-Integrationordnungsgemäß funktioniert und ein Benutzer sich über den IdP authentifizieren und auf die imc Learning Suite zugreifen kann, ohne sich separat anmelden zu müssen. In dieser Testphase werden verschiedene Aspekte des Authentifizierungsprozesses überprüft, z. B. die Umleitung zum IdP, die Handhabung von Authentifizierungsbehauptungen und die erfolgreiche Anmeldung bei der Learning Suite.

Der erfolgreiche Abschluss dieser Tests bestätigt, dass das SSO-Setup korrekt konfiguriert und für die Aktivierung einer breiteren Zielgruppe bereit ist.

5 Best Practice-Ansatz

Um eine optimale SSO-Implementierung zu erreichen, wird dringend empfohlen, dass der Kunde dem imc-Team zu Beginn der Implementierung ein Testbenutzerkonto zur Verfügung stellt. Dieses Testkonto ist für das unabhängige Testen und Überprüfen der SSO-Konfiguration unerlässlich. Durch die Verwendung eines Testkontos kann das imc-Team den Benutzerauthentifizierungsprozess simulieren und potenzielle Probleme oder Fehlkonfigurationen identifizieren, ohne tatsächliche Benutzerkonten zu beeinträchtigen. Dieser proaktive Ansatz stellt sicher, dass alle Probleme früh in der Implementierungsphase gelöst werden, was zu einer reibungsloseren und effizienteren Einrichtung führt. Auch die Einbindung wichtiger Stakeholder aus den Teams des Kunden und von imc ist von entscheidender Bedeutung. Eine klare und kontinuierliche Kommunikation während der gesamten Implementierung hilft dabei, Erwartungen abzustimmen, Anforderungen zu klären und eventuell auftretende Bedenken auszuräumen. Stakeholder sollten in regelmäßige Updates und Diskussionen einbezogen werden, um sicherzustellen, dass das Projekt im Zeitplan bleibt und alle erforderlichen Anpassungen umgehend vorgenommen werden. Darüber hinaus ist es wichtig, alle Konfigurationen, Schritte und Ergebnisse während des Implementierungsprozesses zu dokumentieren. Diese Dokumentation dient als wertvolle Referenz für zukünftige Fehlerbehebungen und Wartungsarbeiten. Sie trägt auch dazu bei, sicherzustellen, dass alle Teammitglieder über die Einrichtungsdetails informiert sind und effektiv zum Erfolg der Implementierung beitragen können.

Durch die Einhaltung dieser Best Practices ist die SSO-Implementierung mit größerer Wahrscheinlichkeit erfolgreich und bietet Benutzern eine nahtlose und sichere Authentifizierung beim Zugriff auf die imc Learning Suite.

6 Übersicht Aufgaben & Verantwortliche

Aufgaben	Veanworlicher
Konfiguration des Identity Providers	Kunde
Stellen Sie FederationMetadata.xml für alle Systeme und das Betreff-/eindeutige Identifikationsattribut bereit	Kunde
Testaccount für SSO-Tests an imc übermitteln	Kunde
Stellen Sie ServiceProvider.xml bereit	imc
Testen Sie SSO mit dem vom Kunden bereitgestellten Testbenutzerkonto	imc
SSO mit mehreren Benutzerkonten testen	Kunde