

Microsoft Entra Integration

Service-Beschreibung

imc Learning Suite

31. Juli 2024

Vorwort und Zielsetzung

Dieses Dokument beschreibt die **Integration mit Microsoft Entra**, die vom imc Projektteam für das Learning Management System (LMS) imc Learning Suite bereitgestellt wird. Die imc Learning Suite ist ein Standardprodukt (Standardsoftware), das ständig um weitere Funktionen & Features (Innovation Packages) erweitert wird. Darüber hinaus bietet das LMS mehrere Integrationsmöglichkeiten im Standardumfang und dieses Dokument beschreibt die Dienste zur Integration des LMS mit Microsoft Entra in Bezug auf **Nutzerbereitstellung / User Provisioning** und **Nutzerauthentifizierung / User Authentication**.

Das Verfahren zur Integration mit Microsoft Entra beschreibt die imc-Empfehlung, die **SCIM** für die Nutzerbereitstellung und **SAML2** für die Nutzerauthentifizierung über SSO verwendet. Es gibt zwar auch Alternativen wie Open ID Connect oder CSV-Nutzerimport und Erweiterungen wie die Nutzerbereitstellung (Account Provisioning) über SSO, aber diese Service-Beschreibung konzentriert sich auf die von imc empfohlene Integration mit Microsoft Entra und beschreibt die entsprechenden Schritte. Aus diesem Grund enthält das Dokument die Vorgehensweisen unter Berücksichtigung der folgenden Aspekte:

- **Beschreibung der vom imc Projektteam zu erbringenden Leistungen** im Rahmen der Umsetzung einer Anpassung.
- **Beschreibung der Zuständigkeiten und Verantwortlichkeiten**, die teilweise auf Seiten von imc und teilweise auf Seiten des Kunden liegen.
- **Beschreibung der Vorgehensweise, der Prozess- und Zeitabhängigkeiten** bei der Umsetzung der Anpassungen, so dass eine transparente Darstellung der einzelnen Schritte für alle Beteiligten möglich ist.

Nutzerbereitstellung (User Provisioning) via SCIM

Die Nutzerbereitstellung über SCIM muss Details zwischen Microsoft Entra und dem LMS austauschen.

Konfiguration in der imc Learning Suite

Für die Bereitstellung von Nutzern über SCIM muss SCIM im **Konfigurationsbereich** des LMS aktiviert werden. Der folgende Screenshot zeigt, dass SCIM aktiviert ist (siehe Registerkarte **Beschreibung**) und den für SCIM verwendete **User Identifier** (scim_admin).

SCIM
Edit System setup 60 saved: 21-Feb-2024 Context: GLOBAL

Description Mapping

Created	Last update	Object ID
System	21-Feb-2024 02:05 (imc SCIM)	60

☒ Active

☒ Return multi-value attributes always as a list even when only one value is available ⓘ

User identifier (100 characters max.) ⓘ

scim_admin

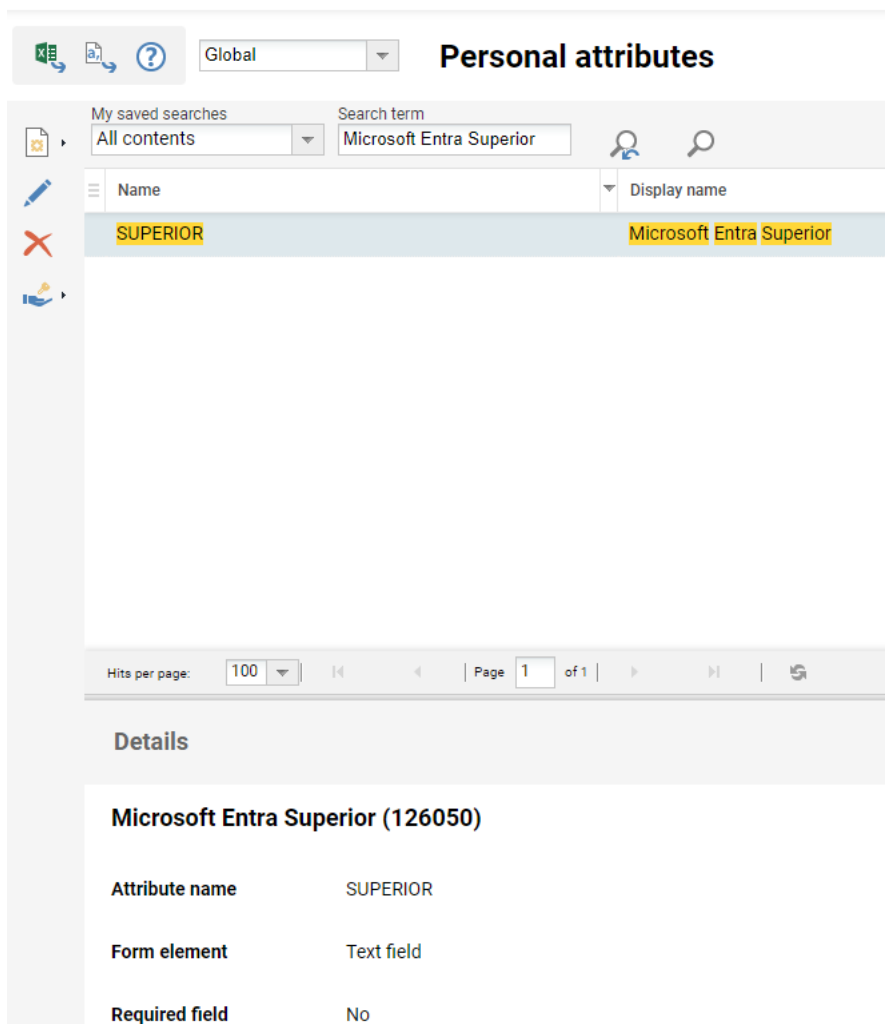
Auf der Registerkarte **Mapping** kann die Feldzuordnung definiert werden, d. h. die von Microsoft Entra bereitgestellten Felder (Quellfelder) werden den Benutzerattributen (Zielfeldern) im LMS zugeordnet. Der folgende Screenshot zeigt die empfohlene Zuordnung von: **Vorname, Nachname, Login, Mail, ID** und **Manager-Informationen**.

SCIM
Edit System setup 60 saved: 08-Jul-2024 Context: GLOBAL

Description **Mapping**

Source field	Target field
emails work value	EMAIL
externalId	EXT_ID_SCIM
id	EXT_ID_SCIM
name familyName	LASTNAME
name givenName	FIRSTNAME
userName	LOGIN
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User manager value	SUPERIOR

Da die Managerinformation (SCIM-ID des Managers) in einem temporären Nutzerattribut vom Typ *Textfeld* gespeichert wird, muss dieses Feld manuell erstellt werden (*Microsoft Entra Superior*).



Personal attributes

Global

My saved searches: All contents | Search term: Microsoft Entra Superior

Name	Display name
SUPERIOR	Microsoft Entra Superior

Hits per page: 100 | Page 1 of 1

Details

Microsoft Entra Superior (126050)

Attribute name	SUPERIOR
Form element	Text field
Required field	No

Außerdem muss die **Profildatenquelle** (im Konfigurationsbereich des LMS) für SCIM mit EXT_ID_SCIM als **profile identifier attribute** konfiguriert sein.

Für die Nutzerauthentifizierung muss ein Nutzer im LMS angelegt werden (SCIM-Nutzer). Es wird empfohlen, scim_admin als **Anmeldenamen** (LOGIN) und **Externe SCIM-ID** (EXT_ID_SCIM) zu verwenden. Der folgende Screenshot veranschaulicht den Nutzer. Damit ist die Konfiguration im LMS abgeschlossen.

Global

Users

My saved searches

All contents

Search term

scim

</

Konfiguration in Microsoft Entra

Um die SCIM- und LMS-Integration in Microsoft Entra zu konfigurieren, muss in einem ersten Schritt ein JSON Web Token (JWT) für den definierten scim-Nutzer erstellt werden. Dieses wird von imc Technical Specialist bereitgestellt. Mit diesem Token kann das SCIM-Providing in

Microsoft Entra konfiguriert werden. Dies setzt voraus, dass eine Enterprise Application in Microsoft Entra vom IT-Spezialisten auf Kundenseite erstellt wurde. Der folgende Bildschirm veranschaulicht, wo das Token gespeichert werden muss.

Darüber hinaus muss die Tenant URL definiert werden: **<LMS-URL>/ils/restapi/lms/scim**

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation pane with categories like Home, Favorites, Identity, and Applications. The main area is titled 'Provisioning' and shows the configuration for an application named 'imssandbox'. The 'Provisioning Mode' is set to 'Automatic'. Below this, the 'Admin Credentials' section is expanded, showing the 'Tenant URL' field with the value 'https://sandbox.lms-saas.com/ils/restapi/lms/scim/' and a 'Secret Token' field. A warning message from Microsoft recommends using a pre-integrated application from the gallery. At the bottom, there is a 'Test Connection' button and a 'Settings' section.

Dann muss der Microsoft Entra-Spezialist auf Kundenseite definieren, welche Nutzer und Nutzergruppen für die SCIM-Synchronisation in Frage kommen.

Hinweis: Wenn der Kunde auch nicht-produktive Umgebungen wie Test oder Stage nutzt, empfiehlt die imc, die SCIM-Integration auch für diese Umgebungen mit separaten Enterprise Application in Microsoft Entra einzurichten.

In einem letzten Schritt wird das **SCIM-Mapping** definiert. Dabei muss das Mapping in Microsoft Entra mit dem im LMS definierten Mapping identisch sein.

Home > Enterprise applications | All applications > Imssandbox | Overview > Provisioning >

Attribute Mapping

Save Discard

Yes No

Source Object

User

Source Object Scope

All records

Target Object

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Target Object Actions

☒ Create

☒ Update

☒ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Microsoft Entra ID and customappsso

customappsso Attribute	Microsoft Entra ID Attribute	Matching precedence	Edit	Remove
userName	userPrincipalName	1	Edit	Delete
emails[type eq "work"].value	mail		Edit	Delete
name.givenName	givenName		Edit	Delete
name.familyName	surname		Edit	Delete
externalid	objectId		Edit	Delete
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	manager		Edit	Delete

[Add New Mapping](#)

☐ Show advanced options

Mit der Fertigstellung des Mappings ist die Einrichtung der SCIM-Nutzerbereitstellung abgeschlossen und kann in Microsoft Entra aktiviert werden.

Hinweis: Microsoft Entra bietet eine On-Demand-Synchronisierung und eine automatische Verarbeitung, bei der Microsoft immer dann synchronisiert, wenn Nutzer aktualisiert werden.

Als Ergebnis dieser SCIM-Einrichtung werden alle dem Synchronisierungsprozess zugewiesenen Nutzer im LMS angelegt.

Nutzerauthentifizierung (User Authentication) via SAML2

Für die Nutzerauthentifizierung über SAML2 müssen Details zwischen Microsoft Entra und dem LMS ausgetauscht werden. Im Folgenden wird die EntityID *lms-sandbox* als Beispiel verwendet.

Konfiguration in Microsoft Entra

Zunächst muss in Microsoft Entra eine neue Enterprise Application („new Application“ und „create your own application“) für das LMS angelegt werden. Das Beispiel hier verwendet den Namen *LMS Sandbox*. Wichtig ist, dass dies vom Microsoft Entra Spezialisten auf Kundenseite durchgeführt werden muss und der Prozess direkt die Konfiguration für eine zusätzliche nicht-produktive LMS-Umgebung (z.B. Test- oder Stage-Umgebung) berücksichtigen sollte. Es wird empfohlen, dies im Namen der zusätzlichen Enterprise Application anzugeben (z.B. *LMS Test Sandbox*).

In einem zweiten Schritt muss Single Sign On im Abschnitt SAML2 der neuen Applikation konfiguriert werden. Hier wird die **SAML entityID** (*lms-sandbox*) sowie die **Reply-URL** **<LMS-URL>/idm/saml/SSO/alias/lms-sandbox** verwendet.

Microsoft Entra erlaubt es nun, die **Federation-Metadaten-URL** zu extrahieren (über „Get App Federation Metadata URL“). Die URL sieht wie folgt aus:

<https://login.microsoftonline.com/308c5dac-2481-4467-8487-f122d91c7f24/federationmetadata/2007-06/federationmetadata.xml?appid=d89e8c21-b9bb-4f76-9fda-cef532a7d0a9>

Der Microsoft Entra Spezialist muss sicherstellen, dass der Abschnitt **Attributes & Claims** korrekt konfiguriert ist. Hier wird das Attribut **user.userprincipalname** (in der Regel die Mailadresse der Nutzer) als Unique User Identifier (**Name ID**) verwendet.

In einem letzten Schritt müssen in Microsoft Entra die Nutzergruppen und einzelnen Nutzer hinzugefügt werden, die die neue Application oder den neuen Service nutzen dürfen. Damit ist die Konfiguration in Microsoft Entra abgeschlossen, die Anwendung ist erstellt, Single Sign On ist konfiguriert und die Nutzer sind berechtigt, die Anwendung zu nutzen.

Konfiguration in imc Learning Suite

Als nächstes muss das Single Sign On über SAML2 im LMS konfiguriert werden. Über den Abschnitt **Konfiguration** und den Punkt **Saml-Authentifizierung** kann die Verbindung zu Microsoft Entra eingerichtet werden. Die folgenden beiden Abbildungen zeigen die relevanten Einträge:

- Auf der Registerkarte **Description** müssen die Felder *Ignore validation* und *Send Saml request* angekreuzt sein. In das Feld *SP meta data file path* kann ein beliebiger Wert eingegeben werden. Der Abschnitt Mapping wird nicht ausgefüllt, da in diesem Szenario kein Account Provisioning verwendet wird. Dies bedeutet auch, dass die Registerkarte **Mapping entries** leer bleibt.

Saml Authentication
Edit System setup 16 saved: 14-Jun-2024 Context: GLOBAL

Description Identity provider Mapping entries

Created	Last update	Object ID
System	14-Jun-2024 09:47 (imc Super)	16

Note: Mandatory fields are marked with an asterisk (*).

☐ Test mode ⓘ
☒ Ignore validation ⓘ
☐ Enable algorithm check ⓘ
☒ Send Saml request ⓘ
☐ Multiple IdPs ⓘ
☐ Enable account provisioning

Fallback provider URL ⓘ

Fallback issuer URL

Fallback redirection URL

Fallback key store path IdP

Fallback key store alias IdP

SP meta data file path*

SP assertion consumer service URL

SP single logout service URL

Entities that use the authentication context ⓘ

Mapping

Default client ⓘ

☐ Import without self-registration ⓘ
☐ Update existing user ⓘ
☐ Ignore unmapped fields ⓘ
☐ Is Reference ⓘ

- Auf der Registerkarte **Identity Provider** muss der Microsoft Entra IDP konfiguriert werden. Hier muss die **SAML Entity ID** (*lms-sandbox*) als URL zum LMS Identity Manager Service (IDM-Service) eingetragen werden: **<LMS-URL>/idm**. Das Feld *IDP metadata URL* benötigt den Link zur *federation metadata URL* aus Microsoft Entra und der Typ des Signaturalgorithmus wird auf RSA-SHA256 gesetzt.

Saml Authentication
Edit System setup 16 saved: 14-Jun-2024 Context: GLOBAL

Identity provider Mapping entries

Entity entity ID	Issuer URL	Provider URL	Redirection URL	Use for LMS
lms-sandbox	https://sandbox.lms.scheer.com/idm	https://sandbox.lms.scheer.com/idm	https://sandbox.lms.scheer.com/idm	Yes

Edit

SAML entity ID* (2000 characters max.)
 SAML entity alias (2000 characters max.)
 SAML display name (30 characters max.)
 User attribute in SAML response (20 characters max.)
 User attribute A.S (20 characters max.)
 Issuer URL* (2000 characters max.)
 Provider URL* (2000 characters max.)
 Redirection URL* (2000 characters max.)
 IDP metadata URL* (2000 characters max.)
☒ Use for LMS
☐ Key store password encrypted
☐ Enable account provisioning
 Signature algorithm type
 RSA-SHA256
 Key store path IdP* (2000 characters max.)
 Key store path SP* (2000 characters max.)
 Key store alias IdP* (2000 characters max.)
 Key store alias SP* (2000 characters max.)
 Key store password IdP* (2000 characters max.)
 Key store password SP* (2000 characters max.)
 Relay state (2000 characters max.)

Nach einigen Minuten (der IDM aktualisiert die Konfiguration regelmäßig alle 5 bis 10 Minuten) ist der Zugriff auf die **Service Provider Metadaten** über den folgenden Link möglich:
<LMS-URL>/idm/saml/metadata/alias/lms-sandbox

Als letzter Schritt muss die **SAML-Entity-ID** zur Konfiguration des Mandanten hinzugefügt werden, der vor der Anmeldung auf der öffentlichen Portalseite des LMS verwendet wird. Der folgende Bildschirm zeigt, dass das Anmeldeformular und die SAML-Authentifizierung mit der SAML-Entity-ID *lms-sandbox* aktiviert sind.

Customer
Edit Client 1 saved: 08-Jul-2024

Description E-mail addresses Languages Settings **Access and security** Import source settings

Created	Last update	Object ID
01-Jul-2023 00:00 (imc Super)	08-Jul-2024 08:48 (imc Super)	1

Authentication

- ☒ Username and password login form ⓘ
- ☒ SAML authentication ⓘ

SAML entity ID (100 characters max.) ⓘ

lms-sandbox

Als Ergebnis der LMS-Konfiguration zeigt der Anmeldebildschirm des LMS die SAML2-Anmelde-schaltfläche oberhalb des lokalen Anmeldeformulars.

Login

Login with external identity provider

or

Login

Password

Login

Hinweis: Wenn nur SAML2 als Authentifizierungsmodul aktiviert ist, löst der Anmeldebildschirm automatisch die Saml-Anfrage aus und leitet den Nutzer zur Authentifizierung an Microsoft Entra weiter.

Schließlich ermöglicht die Integration von Microsoft Entra und die Single Sign On-Authentifizierung über SAML2 eine einfache Authentifizierung mit imc Nutzern. Der Microsoft Entra-Spezialist muss imc keine Testbenutzer für Testzwecke zur Verfügung stellen. Microsoft Entra ermöglicht den Zugriff auf die neue Application (*LMS Sandbox*), indem einfach bestehende Microsoft-Nutzer von imc zur Anwendung / zum Dienst hinzugefügt werden. Dies ist für Testzwecke sehr empfehlenswert, da dies einen vollständigen End-to-End-Test durch imc ermöglicht.