Scheer IMC

Microsoft Entra Integration

Servicebeschreibung

imc Learning Suite | Consulting Department | 20. 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

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:

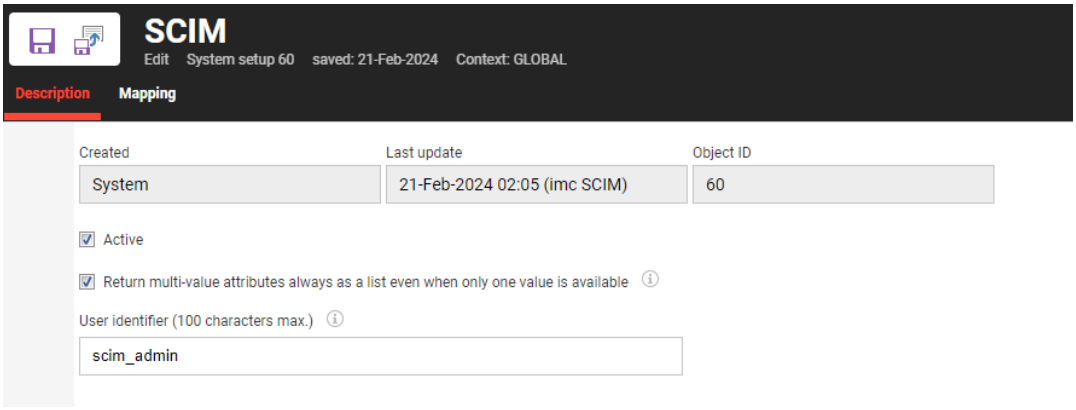
- Beschreibung der vom imc Projektteam zu erbringenden Leistungen im Rahmen der Umsetzung einer Anpassung.
- Beschreibung der Zuständigkeiten und Verantwortlichkeiten, die teilweise auf Seiten von imc und teilweise auf Seiten des Kunden liegen.
- Beschreibung der Vorgehensweise, der Prozess- und Zeitabhängigkeiten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

2 Nutzerbereitstellung (User Provisioning) via SCIM

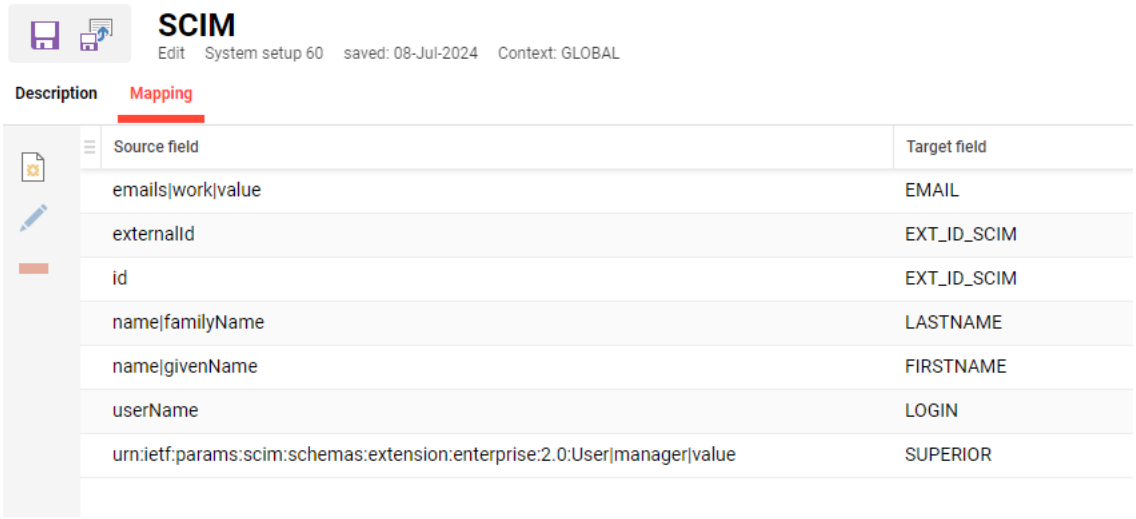
Die Nutzerbereitstellung über SCIM muss Details zwischen Microsoft Entra und dem LMS austauschen.

2.1 Konfiguration in der imc Learning Suite

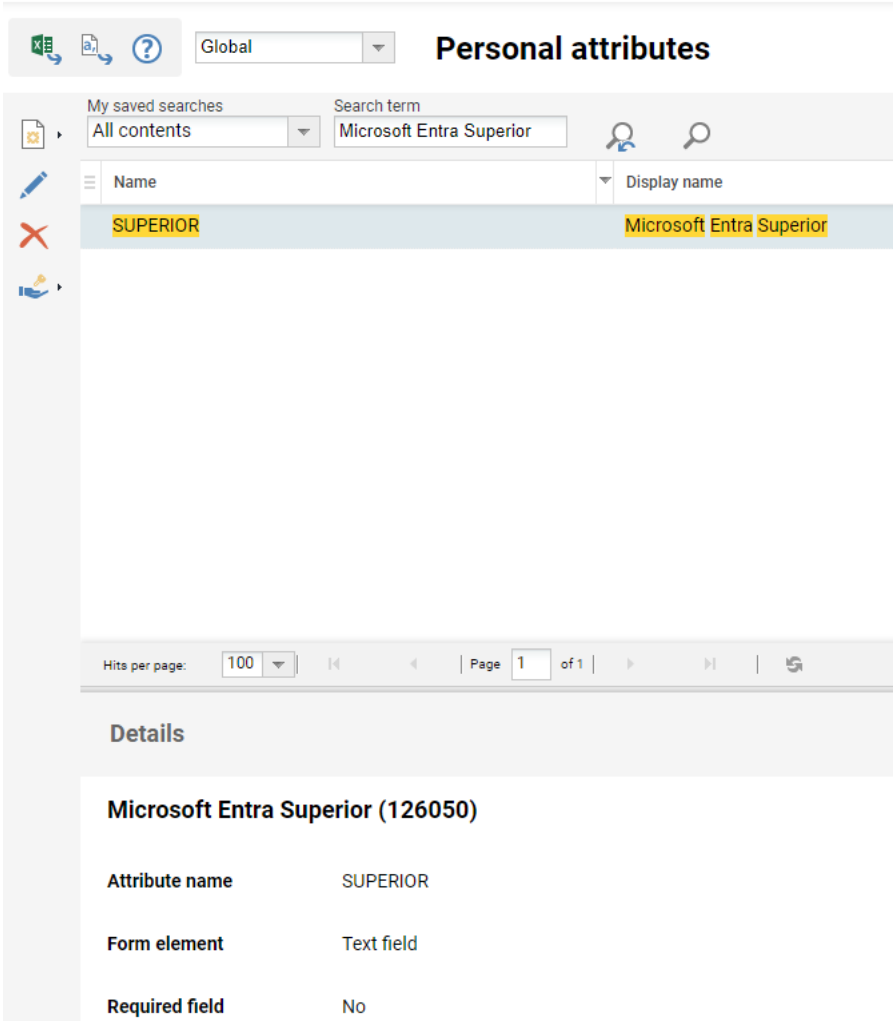
Für die Bereitstellung von Nutzern über SCIM muss SCIM im **Konfigurationsbereich** des LMS aktiviert werden. Der folgende Screenshot zeigt, dass SCIM aktiviert ist (siehe Registerkarte **Beschreibung**) und den für SCIM verwendete **User Identifier** (scim_admin).



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**.

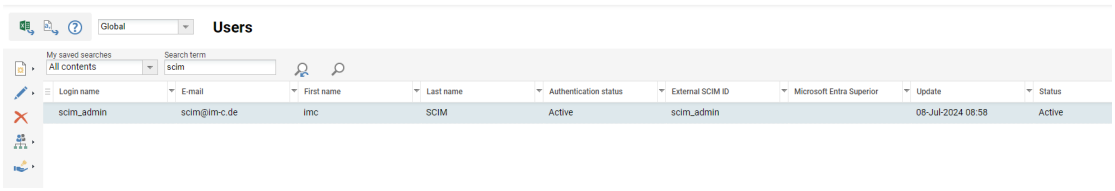


Da die Managerinformation (SCIM-ID des Managers) in einem temporären Nutzerattribut vom Typ *Textfeld* gespeichert wird, muss dieses Feld manuell erstellt werden (*Microsoft Entra Superior*).



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.

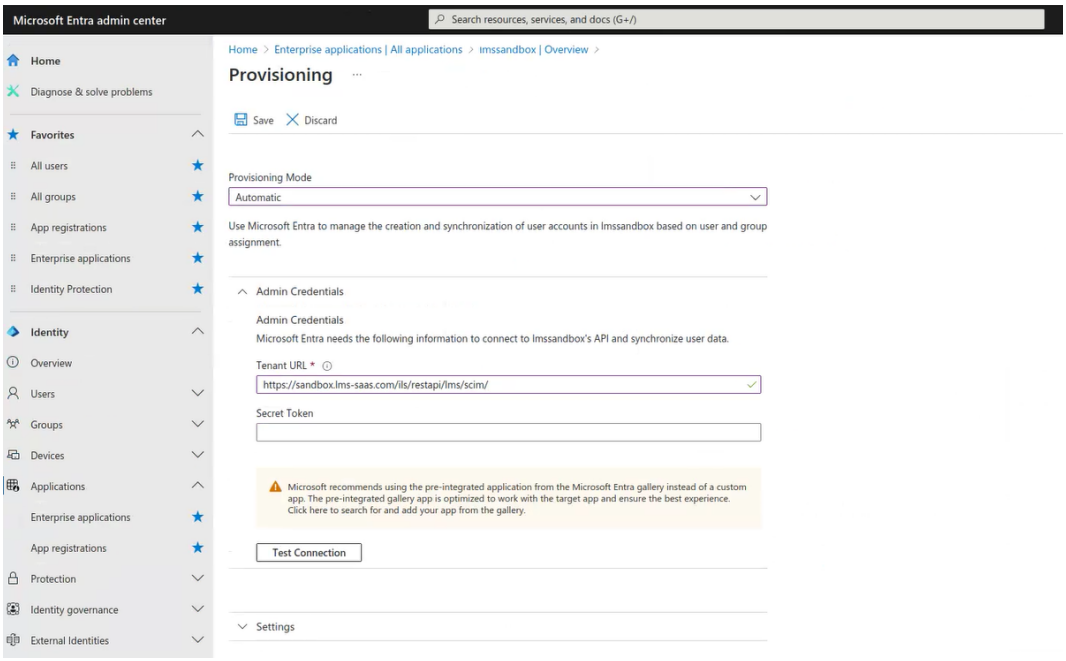


2.2 Konfiguration in Microsoft Entra

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.

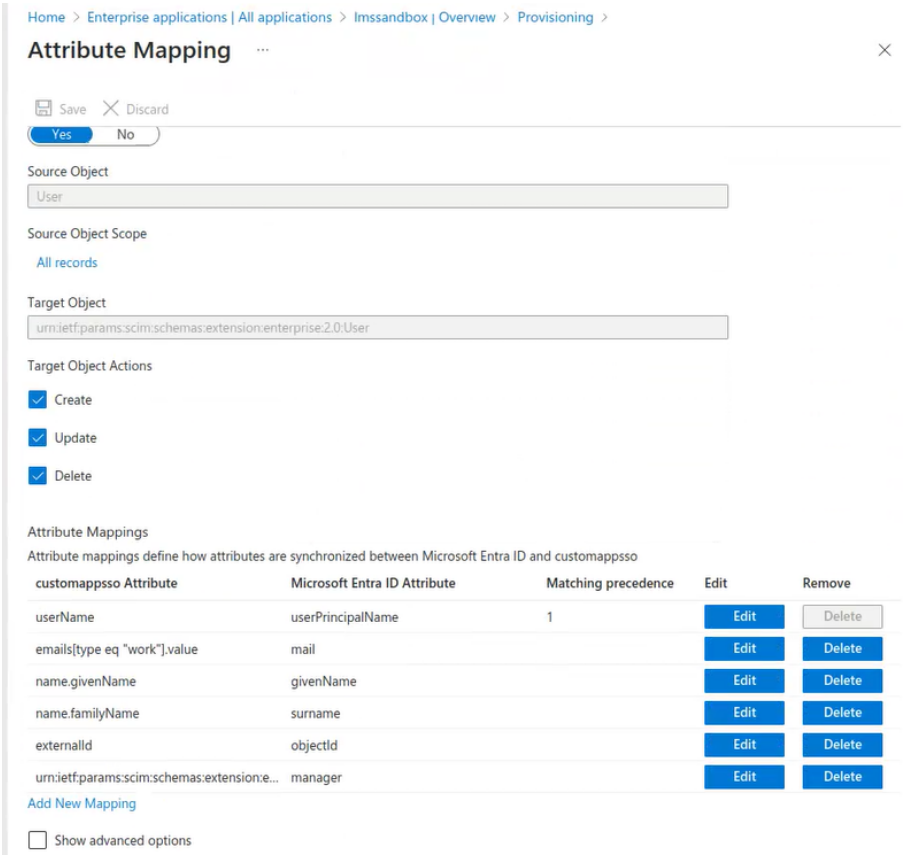
Darüber hinaus muss die Tenant URL definiert werden: **<LMS-URL>/ils/restapi/lms/scim**



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.



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.

3 Nutzerathentifizierung (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.

3.1 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

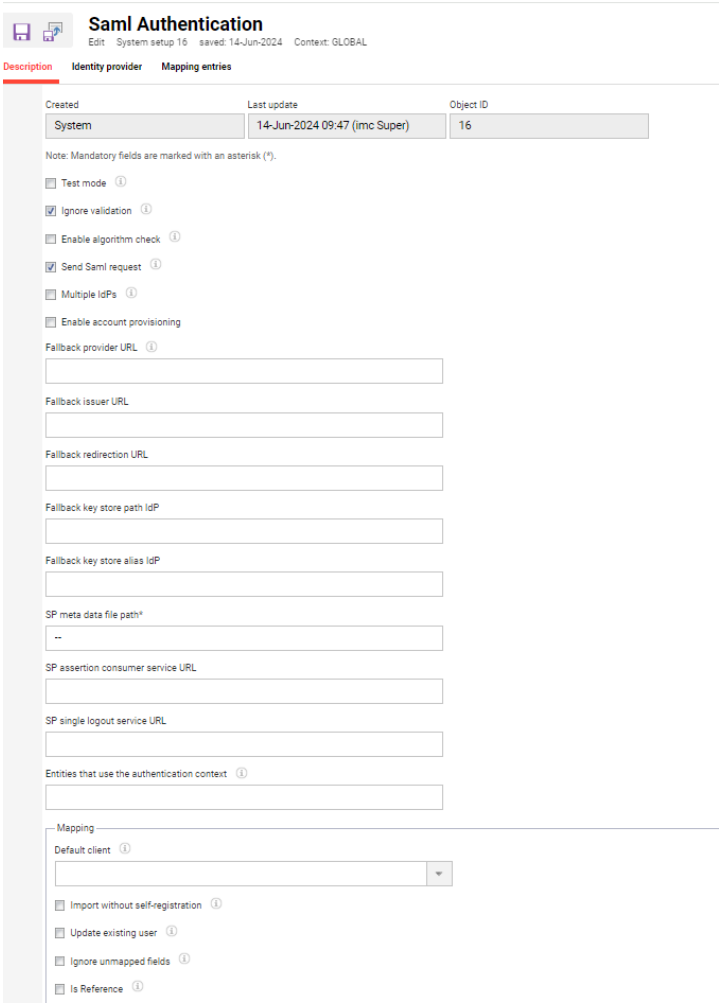
Der Microsoft Entra Spezialist muss sicherstellen, dass der Abschnitt Attributes & Claims korrekt konfiguriert ist. Hier wird das Attribut user.userprinciplename (in der Regel die Mailadresse der Nutzer) als Unique User Identifier (Name ID) verwendet.

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.

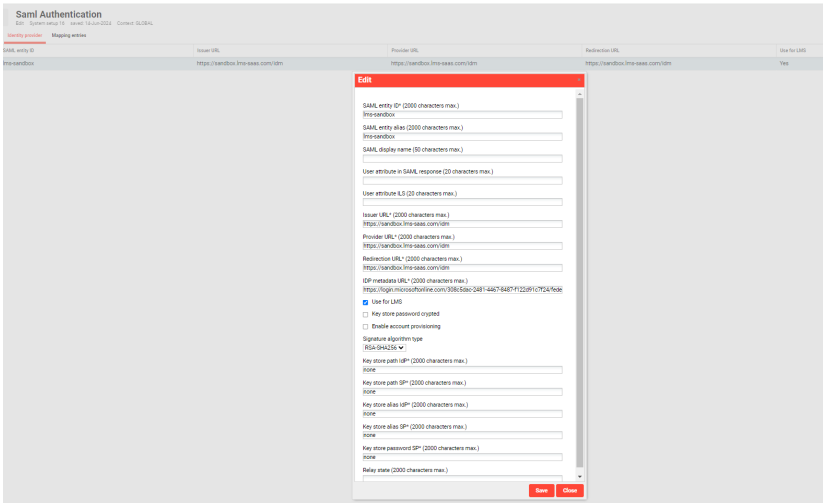
3.2 Konfiguration in Learning Suite

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.



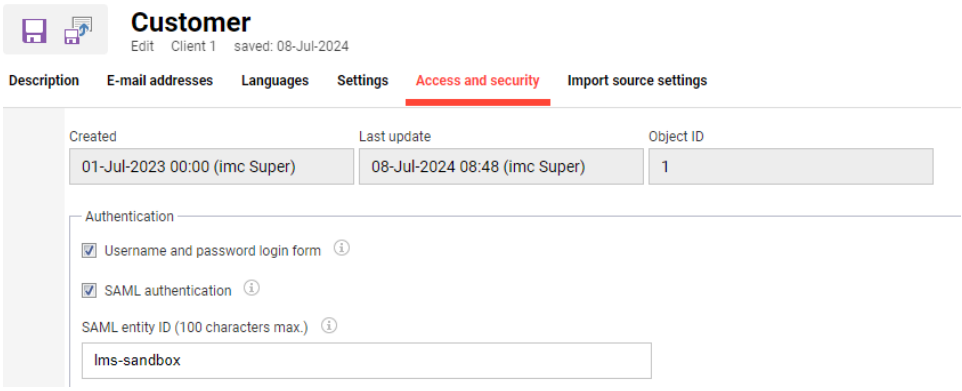
– Auf der Registerkarte **Identity Provider** muss der Microsoft Entra IDP konfiguriert werden. Hier muss die **SAML Entity ID** (*lms-sandbox*) als URL zum LMS Identity Manager Service (IDM-Service) eingetragen werden**:<LMS-URL>/idm**. Das Feld *IDP metadata URL* benötigt den Link zur *federation metadata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



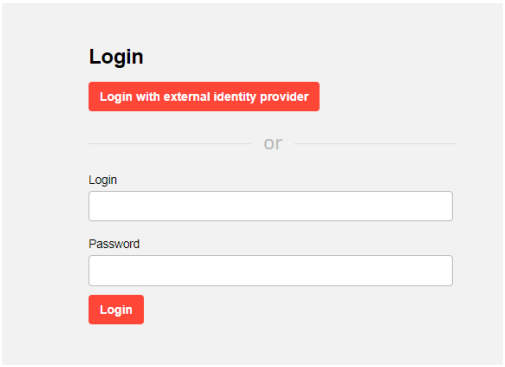
Nach einigen Minuten (der IDM aktualisiert die Konfiguration regelmäßig alle 5 bis 10 Minuten) ist der Zugriff auf die **Service Provider Metadaten** über den folgenden Link möglich:

<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.



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



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.