

Microsoft Entra Integration

Service Description
imc Learning Suite

July 31, 202<mark>4</mark>

Preface and Goals

This document describes the **Microsoft Entra Integration** service provided by the imc project team for the Learning Management System (LMS) imc Learning Suite. The imc Learning Suite is a standard product (standard software) which is constantly being extended with further functions & features (Innovation Packages). In addition, the LMS offers several standard integration options, and this document describes the services to integrate the LMS with Microsoft Entra in terms of **User Provisioning** and **User Authentication**.

The procedure for integration with Microsoft Entra describes the imc recommendation that uses **SCIM** for user provisioning and **SAML2** for user authentication via SSO. There might be alternatives such as Open ID Connect or CSV user import, and extension such as user provisioning via SSO but this service description focuses on the imc recommended integration with Microsoft Entra and describes the relevant step. For this reason, the document contains the procedures considering the following aspects:

- **Description of the services to be provided** by the imc project team in the context of implementing a customisation.
- **Description of the competences and responsibilities**, which lie partly on the part of imc and partly on the part of the customer.
- **Description of the procedure, the process and time dependencies** for the implementation of the customisations, so that a transparent view of the individual steps is possible for all involved people.

User Provisioning via SCIM

User Provisioning via SCIM needs to exchange details between Microsoft Entra and the LMS.

Configuration in imc Learning Suite

User Provisioning via SCIM needs SCIM to be activated in the *Configuration* area of the LMS. The following screenshot illustrates that SCIM is activated (see tab **Description**) and the *User identifier* used for SCIM integration (scim_admin).

	Edit System setup 60 saved: 21-Feb-2024 Context: GLOBAL					
Descripti	on Mapping					
	Created	Last update	Object ID			
	System	21-Feb-2024 02:05 (imc SCIM)	60			
	Active					
	Return multi-value attributes always as a list	st even when only one value is available (i)				
	User identifier (100 characters max.)					
	scim_admin					

The tab **Mapping** allows to define the field mapping that means the fields provided by Microsoft Entra (source fields) are mapped to user attributes (target fields) in the LMS. The following screenshot shows the recommended mapping of **firstname**, **lastname**, **login**, **mail**, **id**, and **manager information**.

	Edit System setup 60 saved: 08-Jul-2024 Context: GLOBAL	
Descript	ion Mapping	
		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

As the manager information (SCIM-ID of the manager) is stored in a temporary user attribute of type *text field*, this field must be created manually (*Microsoft Entra Superior*).

8	Global	Personal a	attributes
	My saved searches All contents	Search term Microsoft Entra Superior	2 2
	■ Name		▼ Display name
×	SUPERIOR		Microsoft Entra Superior
	Hite ass assas	14 d Page 1 of	
	nits per page.		
	Details		
	Microsoft Entra Sup	erior (126050)	
	Attribute name	SUPERIOR	
	Form element	Text field	
	Required field	No	

In addition, the **profile data source** must be configured (in the Configuration area of the LMS) for SCIM with EXT_ID_SCIM as profile identifier attribute.

For user authentication, a user must be created in the LMS (SCIM user). Recommendation is to use *scim_admin* as *Login name* (LOGIN) and *External SCIM ID* (EXT_ID_SCIM). The following screenshot illustrates the user. This completes the configuration in the LMS.

4	Global	· Users							
<u>,</u>	My saved searches All contents	scim	Q Q						
1.	E Login name	▼ E-mail			 Authentication status 	 External SCIM ID 	 Microsoft Entra Superior 	♥ Update	
×	scim_admin	scim@im-c.de	imc	SCIM	Active	scim_admin		08-Jul-2024 08:58	Active
# •									
*									

Configuration in Microsoft Entra

To configure SCIM and LMS integration in Microsoft Entra, as a first step, a **JSON Web Token** (JWT) must be created for the defined scim user. This will be provided by imc technical specialist. Using this token, the SCIM providing can be configured in Microsoft Entra. This assume that an Enterprise Application was created in Microsoft Entra by the IT specialist on customer side. The following screen illustrates where the token needs to be stored.

Microsoft Entra admin cente	${\cal P}$ Search resources, services, and docs (G+/)
Home	Home > Enterprise applications All applications > Imssandbox Overview >
Ciagnose & solve problems	Provisioning
Favorites	Save X Discard
All users	* Provisioning Mode
i All groups	★ Automatic ✓
App registrations	★ Use Microsoft Entra to manage the creation and synchronization of user accounts in Imssandbox based on user and group
Enterprise applications	assignment. ★
Identity Protection	★ ∧ Admin Credentials
Identity	Admin Credentials Microsoft Entra needs the following information to connect to imssandbox's API and synchronize user data.
Overview	Tenant URL * 💿
کر Users	https://sandbox.lms-saas.com/ils/restapi/lms/scim/
ස් Groups	V Secret Token
Devices	
Applications	Microsoft recommends using the pre-integrated application from the Microsoft Entra galley instead of a custom and The residuentation of a subscription of the work with the tarent and and unsize the best expression.
Enterprise applications	Click here to search for and add your app from the gallery.
App registrations	★ Test Connection
Protection	
Identity governance	
External Identities	V Settings

In addition, the Tenant URL must be defined: <LMS-URL>/ils/restapi/lms/scim

Then, the Microsoft Entra specialist on customer side must define which **users and user groups** should be considered for SCIM synchronization.

Hint: If the customer also uses non-productive environments such as Test or Stage, imc recommends to setup SCIM integration also for these environments with separate Enterprise Applications in Microsoft Entra.

As a last step, the **SCIM mapping** gets defined. Here the mapping in Microsoft Entra must be identical to the mapping defined in the LMS.

Attribute Mapping				
🗟 Save 🗙 Discard				
Yes No				
ource Object				
User				
ource Object Scope				
All records				
arget Object				
urnietf:params:scim:schemas:extension.ent	terprise:2.0:User			
arget Object Actions				
Create				
Update				
V Delete				
Attribute Mappings Attribute mappings define how attributes ar	e synchronized between Microsoft Ent	ra ID and customappeso		
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
	objectId		Edit	Delete
externalld			2003200	
externalld urn:ietf:params:scim:schemas:extension:e	manager		Edit	Delete

With completing the mapping, the SCIM user provisioning setup is completed and can be activated in Microsoft Entra.

Hint: Microsoft Entra offers on-demand synchronization and some automatic processing where Microsoft synchronizes whenever users are updated.

As a result of this SCIM setup, all users assigned to the synchronization process are created in the LMS.

User Authentication via SAML2 needs to exchange details between Microsoft Entra and the LMS. In the following, the entityID *Ims-sandbox* is used as example.

Configuration in Microsoft Entra

First, a new Enterprise Application ("new Application" and "create your own application") must be created in Microsoft Entra for the LMS. The example here uses the name *LMS Sandbox*. Important to note is that this needs to be done by the Microsoft Entra specialist on customer side and the process should directly consider the configuration for any additional non-productive LMS environment (i.e., Test or Stage environment). The recommendation is to specify this in the name of the additional Enterprise Application (e.g., *LMS Test Sandbox*).

In a second step, Single Sign On must be configured in the section SAML2 of the new Application. Here the *SAML entityID* (*Ims-sandbox*) as well as the reply-URL **<LMS-***URL>/idm/saml/SSO/alias/Ims-sandbox* is used.

Microsoft Entra allows now to extract the federation metadata URL (via "Get App Federation Metadata URL"). The URL looks like this:

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

The Microsoft Entra specialist must ensure that the *Attributes & Claims* section is correctly configured. Here, the attribute user.userprinciplename (which is usually the mail address of the users) is used as *Unique User identifier* (*Name ID*).

As a last step in Microsoft Entra, the user groups and individual users must be added that are allowed to use the new application or service. This completes the configuration in Microsoft Entra as the application is created, Single Sign On is configured, and users are allowed to use the application.

Configuration in imc Learning Suite

Next, the Single Sign On via Saml2 needs to be configured in the LMS. Using the Configuration section and item Saml Authentication allows to setup the connection to Microsoft Entra. The following two figures show the relevant entries:

- On the **Description** tab *Ignore validation* and *Send Saml request* must be ticked. The field *SP* meta data file path can be entered with any arbitrary value. The *Mapping* section is not filled as account provisioning is not used in this scenario. This also means that the tab **Mapping** entries stays empty.

Identity provider Mapp	ing entries	
reated	Last update	Object ID
System	14-Jun-2024 09:47 (imc Super)	16
lote: Mandatory fields are marke	d with an asterisk (*).	
] Test mode 🕕		
Ignore validation (1)		
Enable algorithm check 🔅		
Send Saml request 🕕		
Multiple IdPs		
Enable account provisioning		
allback provider URL ①		
allback issuer URL		
allback redirection URL		
allback key store path IdP		
allback key store alias IdP		
P meta data file path*		
P assertion consumer service U	RL	
P single logout service URL		
ntities that use the authenticatio	in context (3)	
Mapping		
Default client		
		Ψ
Import without self-registra	tion (i)	

 On the Identity Provider tab, the Microsoft Entra IDP needs to be configured. Here, the SAML entity ID (*Ims-sandbox*) must be entered as the URL to the LMS Identity Manager Service (IDM Service): <LMS-URL>/idm. The field *IDP metadata URL* needs the link to the federation metadata URL taken from Microsoft Entra and the *Signature algorithm type* is set to RSA-SHA256.

L with D	htar iffs	Franke 18.	- Berlander UR.	One Part 1
sendoox	Http://sandbox.impises.com/idm	Https://saketbox.ine-sage.com/sam.	https://secdoucline-sees.com/idm	Yes
		SAML entry 67 (2000 characters max.)	i.	
		SAM write also (2000 characters may)		
		Instantiox		
		SAML display name (50 characters max)		
		User attribute in SAML response (20 characters max.)		
		User attribute ILS (20 characters max.)		
		Issuer URL* (2000 characters max.)		
		Enclose LET (2000) characteris may \		
		https://sandbox.imu-saas.com/ibm		
		Redirection URL* (2000 characters max.) https://sandbox.ims-saas.com/idm		
		EP metadata URL* (2000 characters max.) https://login.microsoftonline.com/308c5dac-2481-4467-8487-F122091c7f24/fede		
		g Use for LMS		
		Key store password crypted		
		Enable account provisioning		
		Signature algorithm type RSA SH4256 ♥		
		Key store path (dP* (2000 characters max.)		
		note		
		Key store path S8* (2000 characters max.)		
		none		
		Key store alias IdP* (2000 characters max.)		
		nove		
		Key store alias SP* (2000 characters max.)		
		POM		
		Key store password SP* (2000 characters max.)		
		note		
		Refay state (2000 characters max.)		

After some minutes (the IDM refreshes the configuration on a regular basis every 5 to 10 minutes), the access to the Service Provider Metadata is possible via the following link: *<LMS-URL>/idm/saml/metadata/alias/lms-sandbox*

As a last step, the SAML entity ID must be added to the client configuration of the client that is used on the public dashboard page before login. The following screen shows that login form and SAML authentication with SAML entity ID Ims-sandbox are activated.

	Customer Edit Client 1 saved: 08-Jul-2024						
Description	E-mail addresses	Languages	Settings	Access and security	Import source	ce settings	
c	reated		Last up	date		Object ID	
	01-Jul-2023 00:00 (ir	mc Super)	08-J	ul-2024 08:48 (imc Su	iper)	1	
	Authentication						
	Username and pass	word login form					
	SAML authentication	n (i)					
	SAML entity ID (100 cha	racters max.)	D				
	lms-sandbox						

As a result of the LMS configuration, the login screen of the LMS shows the SAML2 login button above the local login form.

Login with exter	rnal identity provider	
	or	
Login		
Password		
assword		

<u>Hint</u>: If only SAML2 is activated as authentication mode, the login screen is automatically triggering the Saml request and forwarding to Microsoft Entra for authentication.

Finally, Microsoft Entra integration and Single Sign On authentication via SAML2 allows to easily perform authentication with imc users. The Microsoft Entra specialist does not need to provide test users to imc for testing purposes. Microsoft Entra allow to provide access to the new Enterprise (*LMS Sandbox*) just by adding existing Microsoft users from imc to the application / service. It is highly recommended for testing purposes as this allows to do a full end-to-end testing by imc.