

OAuth2 Konfiguration 23.4

in Moodle 3.10/4.1

Vorarlberger Standardschulinstallation Autor: Martin Schnetzer Besuchen Sie uns im Internet http://www.vobs.at/rb © 2023 IT-Regionalbetreuer Vorarlberg 6900 Bregenz , Römerstraße 14 Alle Rechte vorbehalten

Inhalt

1.	Vorbemerkung	3
2.	Vorbereitung Azure Active Directory	3
3.	Eigene Moodle-Instanz	8
3.1.	- Website-Administration	8
3.2.	Aktivieren der Authentifizierung	9



1. Vorbemerkung

Das OAuth 2 Authentifizierungs-Plugin ermöglicht es Benutzern, sich mit ihrem Google-, Microsoftund/oder Facebook-Konto über Schaltflächen auf der Anmeldeseite anzumelden. Dies ist ein Standard Moodle Plugin. Damit die Oauth2 Authentifizierung in Moodle funktioniert, müssen zuerst Einstellungen im Azure Active Directory (Entra Admin Center) gemacht werden.

Damit alle benötigten Werte und Schlüssel zu Hand und gespeichert sind, erstelle ein Dokument "Moodle Microsoft SSO.txt".

2. Vorbereitung Azure Active Directory

Um einen OAuth 2.0-Client bei Microsoft einzurichten, müssen Sie zunächst eine neue Anwendung mithilfe von App-Registrierungen im Entra Admin Center registrieren.

Azure Active Directory \rightarrow Anwendungen \rightarrow App-Registrierungen

М	icrosoft Entra Admin Center		${\cal P}$ Nach Ressourcen, Diensten und Dokumenten suchen (G+/)
^	Start		Home⇒ App-Registrierungen 🖈 …
*	Favoriten	\sim	+ Neue Registrierung 🌐 Endpunkte 🖉 Problembehandlung 🖒 Aktualisieren 🞍 Herunterladen 🗄
٠	Azure Active Directory	^	
í	Übersicht		Ab dem 30. Juni 2020 werden der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Azure AD Graph I Anwendungen müssen auf die Microsoft-Authentifizierungsbibliothek (MSAL) und Microsoft Graph aktualisiert werd
8	Benutzer	\sim	
የጽቶ	Gruppen	\sim	Alle Anwendungen Anwendungen mit Besitzer Gelöschte Anwendungen
Ð	Geräte	\sim	P Beginnen Sie mit der Eingabe eines Anzeigenamens oder einer Anw
₿	Anwendungen	\sim	
	Unternehmensanwendungen		Dieses Konto ist n
Į	App-Registrierungen		
≙	Schützen und sichern	\sim	
٢	Identity Governance	\sim	

→ Neue Registrierung

М	icrosoft Entra Admin Center					ssourcen, Die	nsten und Dokum	enten suchen (G+/)	
	Start		Home >						
<u> </u>	Stalt		App-Registrie	rungen	\$				
*	Favoriten	\sim	+ Neue Registrierung	🕀 Endpunkte	🤌 Problemb	ehandlung	🕐 Aktualisieren	↓ Herunterlader	n E
٠	Azure Active Directory	^							
i	Übersicht		Ab dem 30. Juni 20 Anwendungen müs	120 werden der Azure ssen auf die Microso	e Active Directory ft-Authentifizieru	y-Authentifizie Ingsbibliothek	rungsbibliothek (Al (MSAL) und Micro	DAL) und Azure AD Gra soft Graph aktualisiert	aph k werd
8	Benutzer	\sim							
^A X ^A	Gruppen	\sim	Alle Anwendungen	Anwendungen	mit Besitzer	Gelöschte	Anwendungen		
Ð	Geräte	\sim		er Eingabe eines Ai	nzeigenamens (oder einer An	w + F	ilter hinzufügen	
₿	Anwendungen	^							
	Unternehmensanwendungen							Dieses Konto	ist n
1	App-Registrierungen								
≙	Schützen und sichern	\sim							
۲	Identity Governance	\sim							

Folgende Werte eintragen:

Μ	icrosoft Entra Admin Center	,○ Nach Ressourcen, Diensten und Dokumenten suchen (G+/)
\$	Start	Home > App-Registrierungen > Anwendung registrieren
*	Favoriten	× · · · · · · · · · · · · · · · · · · ·
•	Azure Active Directory	* Name Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)
()	Übersicht	Moodle oauth2 Authentifizierung
Я **	Benutzer Gruppen	Unterstützte Kontotypen
R	Gorāto	Wer kann diese Anwendung verwenden oder auf diese API zugreifen?
	Gerate	Nur Konten in diesem Organisationsverzeichnis (nur "VS-VOBS Bildungsservice" – einzelner Mandant) Konten in einem heliebinen Organisationsverzeichnis (heliebiner Anure AD-Verzeichnis – mehrinstanzenfähin)
# 8	Anwendungen	Konter in einem beliebigen Organisationsverzeichnis (beliebiges zure AD-Verzeichnis – mehrinstatizentialing) Konten in einem beliebigen Organisationsverzeichnis (beliebiges zure AD-Verzeichnis – mehrinstatizentialing)
8	Schützen und sichern	Microsoft-Konten (z. B. Skype, Xbox)
۲	Identity Governance	V Nur personliche Microsoft-Konten
Ę	Azure AD External Identities	Entscheidungshilfe
	Mehr anzeigen	Umleitungs-URI (optional)
4	Berechtigungsverwaltung	Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.
1	Überprüfte ID	Web Inttps://moodle.vobs.at/test4x/admin/oauth2callback.php
		Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus Unternehmensanwendungen hinzufügen.
2	Learn und Support	Indem Sie den Vorgang fortsetzen, stimmen Sie den Microsoft-Plattformrichtlinien zu. C [*] Kegistrieren

Name: sinnvolle Bezeichnung der Registrierung

Kontotypen: Nur Konten in diesem Organisationsverzeichnis

Umleitungs – URI: z.B. https://moodle.vobs.at/moodleinstanz/admin/oauth2callback.php

Die URL setzt sich aus der Adresse der eigenen Moodle-Instanz und der Ergänzung "/admin/oauth2callback.php" zusammen

 \rightarrow Registrieren





Die Anwendungs-ID in "Moodle Microsoft SSO.txt" kopieren (wird später benötigt).

Folgende Punkte Kontrollieren:



◆ API-Berechtigungen → Microsoft Graph (1) → User.Read enthalten

3	Authentifizierung	Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozess									
1	Zertifikate & Geheimnisse	Bere Bere	Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. Weitere								
- 11	Tokenkonfiguration	Infor	Informationen zu Berechtigungen und Zustimmung								
	API-Berechtigungen	+	Berechtigung	hinzufüger	n 🧹 Admir	nistratorzustimmung für "VS-VOBS Bildungsservic	e" erteilen				
	Eine API verfügbar machen	AP	I/Berechtigung	Jsname	Тур	Beschreibung	Administ				
	App-Rollen	\sim	Microsoft Graph	(1)							
- 24	Besitzer		User.Read		Delegiert	Anmelden und Benutzerprofil lesen	Nein				
2,	Rollen und Administratoren	•					Þ				

📍 ^{Zertifikate & Geheimnisse} → Beschreibung: Moodle mit einer Gültigkeit von 24 Monaten.



Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.



Unbedingt den Wert des Schlüssels in das Dokument "Moodle Microsoft SSO.txt" kopieren.

Wird der "Geheime Clientschlüssel" zu einem späteren Zeitpunkt geöffnet, kann dieser nicht mehr angezeigt werden. Sollte es dennoch passieren, dass der Schlüssel nicht mehr angezeigt wird, muss ein zweiter neuer Schlüssel erstellt werden.

🔣 Moodle oauth2 Au	ithentifizierung 🖈 …		\times
₽ Suche «	🗴 Löschen 🕀 Endpunkte 💀 Vo	prschaufeatures	
 Übersicht Schnellstart Integrations-Assistent Verwalten 	 Zusammenfassung Anzeigename Anwendungs-ID (Client) Objekt-ID 	: <u>Moodle oauth2 Authentifizierung</u> : 970aa4c4-6956-469a-9ac8-a902561 : a96fe801-e26d-4474-90a6-ef20db7	
 Branding und Eigenschaften Authentifizierung Zertifikate & Geheimnisse Tokenkonfiguration 	Verzeichnis-ID (Mandant) Unterstützte Kontotypen Clientanmeldeinformationen Umleitungs-URIs Anwendungs-ID-URI	: 282d83c5-1aaf-4206-9194-320e97b : <u>Nur meine Organisation</u> : <u>0 Zertifikat, 1 Geheimnis</u> : <u>1 vom Typ "Web", 0 vom Typ "SPA",</u> : <u>Anwendungs-ID-URI hinzufügen</u>	
Microsoft Entra Admin Center	$ \mathcal{P} $ Nach Ressourcen, Diensten und Dokumer	ten suchen (G+/)	(×
OAuth 2.0-Autorisierungse	ndpunkt (v2) line.com/282d83c5-1aaf-4206-9194-320e97b6e t (v2)	<mark>f63/oauth2/v2.0/a</mark> uthorize	Ū
i i https://login.microsofton i OAuth 2.0-Autorisierunase	ndpunkt (v1)	f63/oauth2/v2.0/token	D

In der Übersicht wird nun der benötige Endpunkt nachgeschaut.

Kopiere nun den Endpunkt bis einschließlich ".../oauth2/v2.0/" (dieser Link wird insgesamt dreimal benötigt)

Nun sollten folgende Werte im Dokument "Moodle Microsoft SSO.txt" vorhanden sein:

Anwendungs-ID (Client): 970aa4c4-6956-469a-9ac8-a90...

Wert des Schlüssels: Lmt8Q~~v4nRMGellw4vH8VvY1GsJNWU...

Endpunkt: https://login.microsoftonline.com/282d83c5-1aaf-4206-9194-320e97b6ef63/oauth2/v2.0/

3. Eigene Moodle-Instanz

3.1. Website-Administration

We hsle in die Website-Administration \rightarrow Server \rightarrow Oauth 2-Services

≡ VOBS-Moodle test2x ▲	Meine Kurse 👻 Deutsch (de)	•							
🚳 Dashboard									
# Startseite	Website-Administration	Nutzer/innen	Kurse	Bewertungen	Plugins	Darstellung	Server	Berichte	Entwicklung
🛗 Kalender		Server			Systempfade Supportanfrag	en			
C Meine Dateien					Sitzungsinforr HTTP	nation			
✓ Inhaltsspeicher					Aufräumarbei	us ten			
✔ Website-Administration					PHP Info	ing			
				_	Aktualisierung	snachrichten			
				. [OAuth 2-Servi	ces			
		Tasks			Task-Verarbeit	ung			

Klicke auf die Schaltfläche "Neuen Microsoft-Service anlegen"

OAuth 2 C	Convisos							
OAuth 2-3	services							
Anleitung für di	ie Einrichtung von Se	ervice-Providern						
Name	Anmeldung	Auf der Anmelde	eite anzeigen als	Inter	rne Services	Erkennung 💡	Systemaccount verbunden 💡	Bearbeiten
Neuen Service anle	gen: Google	Microsoft Facebook	Nextcloud Ope	en Badges	LinkedIn	Clever Nutzerdefin	niert	
			Neuen Service	anlege	n: Micros	oft		
			🖉 Detaillierte Anleitung zur Ko Name	ntiguration de	Microsoft	Microsoft		
			Client-ID	00	970aa4c4-6956-4	69a-9ac8-		
			Client-Secret	0 0	Lmt8Q~~v4nRM0	Sellw4vH8		
					Authentifizierung	stoken-Anforderungen über H	TP-Header 💡	
			Service-Basis-URL	0	https://login.micr	osoftonlin		
			Logo-URL	0	https://www.micr	osoft.com,		
			Dieser Service wird verwendet.	0	Anmeldeseite und	l interne Services \$		
			Angezeigter Name auf der Anmeldeseite	0				
			Scopes, die bei einer Anmeldeanforderung angeforde werden.	e rt	openid profile em	ail user.re		
			Scopes in einer Anmeldeanford für einen Offline-Zugriff	erung 💡	openid profile em	ail user.re		

für einen Offline-Zugriff		
Zusätzliche Parameter für die Login- Anforderung	0	
Zusätzliche Parameter, die in einer Login-Anforderung für den Offline- Zugriff enthalten sind.	0	
Login-Domains	0	
		E-Mail-Bestätigung notwendig
		Ich weiß, dass die Deaktivierung der E-Mail-Bestätigung ein Sicherheitspr
		Änderungen speicherm Abbrechen
notwandia		

Trage die Werte aus "Moodle Microsoft SSO.txt" in die Felder **Client-ID** (= Anwendungs-ID), **Client-Secret** (= Geheime Schlüssel) und die **Service-Basis-URL** (= Endpunkt) ein.

Ist die E-Mail-Bestätigung aktiviert, muss das Konto noch bestätigt werden. Da jedoch nur Konten aus der eigenen Organisation zulässig sind, ist das nicht notwendig.

OAuth 2-Ser	vices					
Dashboard Vebsite-A	dministration 💙 Server	OAuth 2-Services				
OAuth 2-Service	S					
Anleitung f ür die Einrichtung	g von Service-Providern					
Name	Konfiguriert	Login erlauben	Erkennung 📀	Systemaccount verbunden	Bearbeiten	
Microsoft	√	✓	-	★ ⊡	• • •	
Neuen Google-Service anlege	en Neuen Microsoft-S	Service anlegen Neuen Facebook	Service anlegen Neuen Next	cloud-Service anlegen Create new LinkedIn	service Neuen eigenen Service anlegen	

Nach dem Speichern kontrollieren wir in der Übersicht, ob alles richtig eingetragen wurde.

Endpoint für den Service/Identitätsaussteller: Microsoft									
Name	URL	Bearbeiten							
authorization_endpoint	https://login.microsoftonline.com/282d83c5-1aaf-4206-9194-320e97b6ef63/oauth2/v2.0/authorize	o 0							
token_endpoint	https://login.microsoftonline.com/282d83c5-1aaf-4206-9194-320e97b6ef63/oauth2/v2.0/token	o 0							
userinfo_endpoint	https://graph.microsoft.com/v1.0/me/	¢ û							

Bei authorization_endpoint und beim token_endpoint muss die ID enthalten sein.

Sollte "https://login.microsoftonline.com/common/oauth2/v2.0/authorize" bzw. ".../token" eingetragen sein, kopiere aus dem Azure AD die betreffenden Endpunkte ins Moodle. Ändern des Endpunktes mit dem Zahnrad. Diese Endpunkte befinden sich in der App-Registrierungen.

3.2. Aktivieren der Authentifizierung

Als letzten Punkt muss noch die Authentifizierung aktiviert werden.

Website-Administration \rightarrow Plugins \rightarrow Authentifizierung \rightarrow Übersicht



Aktiviere das "OAuth 2" Plugin mit dem "Auge"-Symbol.

Dashboard / Website-Administration / Plugin	ashboard / Website-Administration / Plugins / Authentificierung / Übersicht										
Navigation V Dashboard Startseite V Website Mine Kurna	Übersicht Verfügbare Plugins zur Authentifizierun	9									
> Kurse	Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Einstellungen prüfen	Deinstallieren				
Administration	Manuelle Konten	3			Einstellungen						
Website-Administration	Kein Login	0									
Systemnachrichten Registriegung	OAuth 2	1	۲	*	Einstellungen	Einstellungen prüfen					
Moodle Services Section 1	E-Mail-basierte Selbstregistrierung	0	۲	^	Einstellungen		Deinstallieren				
reedback-cinstellungen Zusatzoptionen	CAS-Server (SSO)	0	Ø		Einstellungen	Einstellungen prüfen	Deinstallieren				
Nutzer/innen Kurse	Externe Datenbank	0	Ø		Einstellungen	Einstellungen prüfen	Deinstallieren				

Nun ist die Konfiguration abgeschlossen und auf der Login-Seite ist nun die Möglichkeit der Microsoft Authentifizierung.

9/10

Anneidenan	ne
Kennwort	
Login	
Kennwort vergesse	in?
Verwenden S	ie Ihr Nutzerkonto bei
	Microsoft

Hinweis:

Ist ein User mit der Microsoft Adresse vorhanden, so wird dieser User mit dem Microsoft Konto verknüpft. Die Verknüpfung des Kontos nicht mehr rückgängig gemacht werden.

Eine Anmeldung ist nun über den Microsoft Button (nicht über den Anmeldenamen und Kennwort) möglich.

