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

Inhalt

1. Vorbemerkung

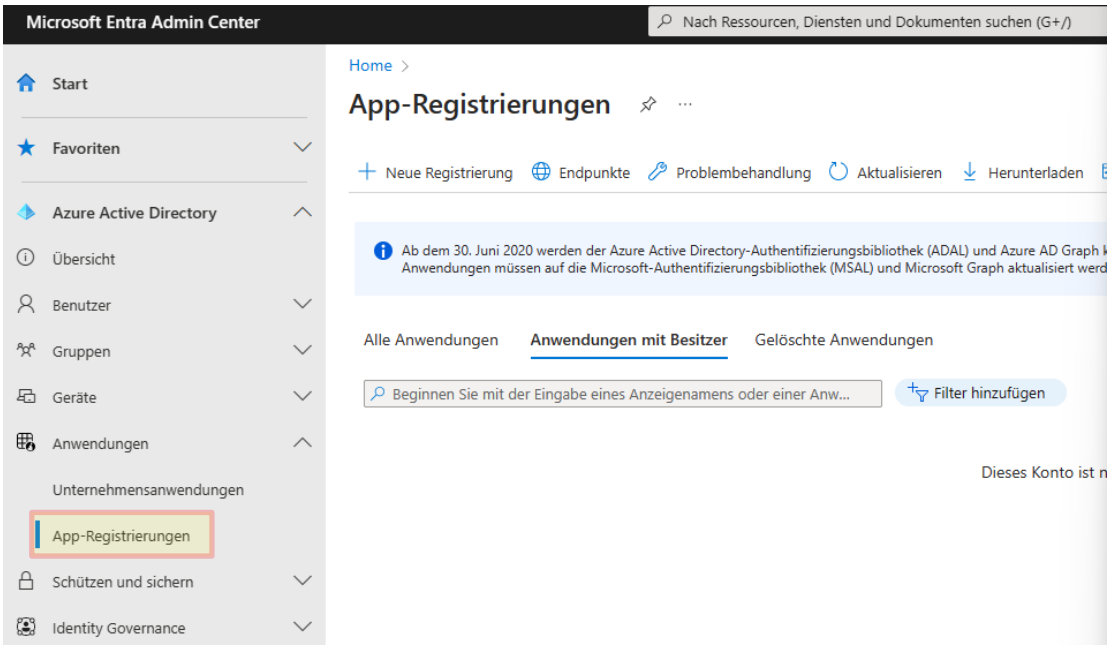
Das OAuth 2 Authentifizierungs-Plugin ermöglicht es Benutzern, sich mit ihrem Google-, Microsoft- und/oder Facebook-Konto über Schaltflächen auf der Anmeldeseite anzumelden. Dies ist ein Standard Moodle Plugin. Damit die Oauth2 Authentifizierung in Moodle funktioniert, müssen zuerst Einstellungen im 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“.

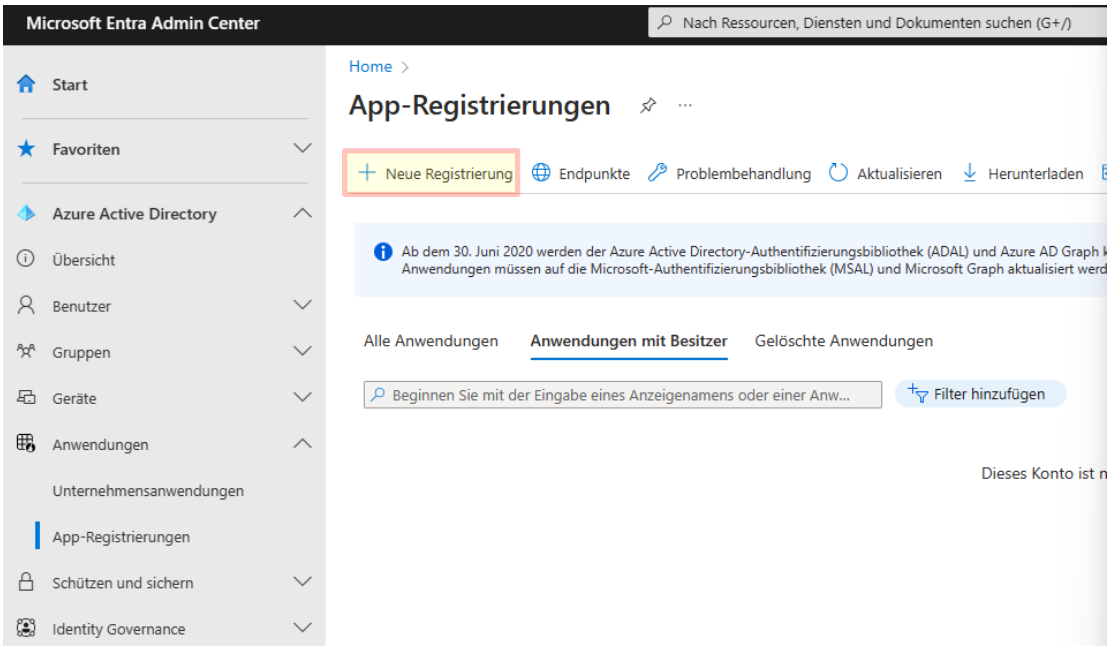
2. Vorbereitung Azure Active Directory

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

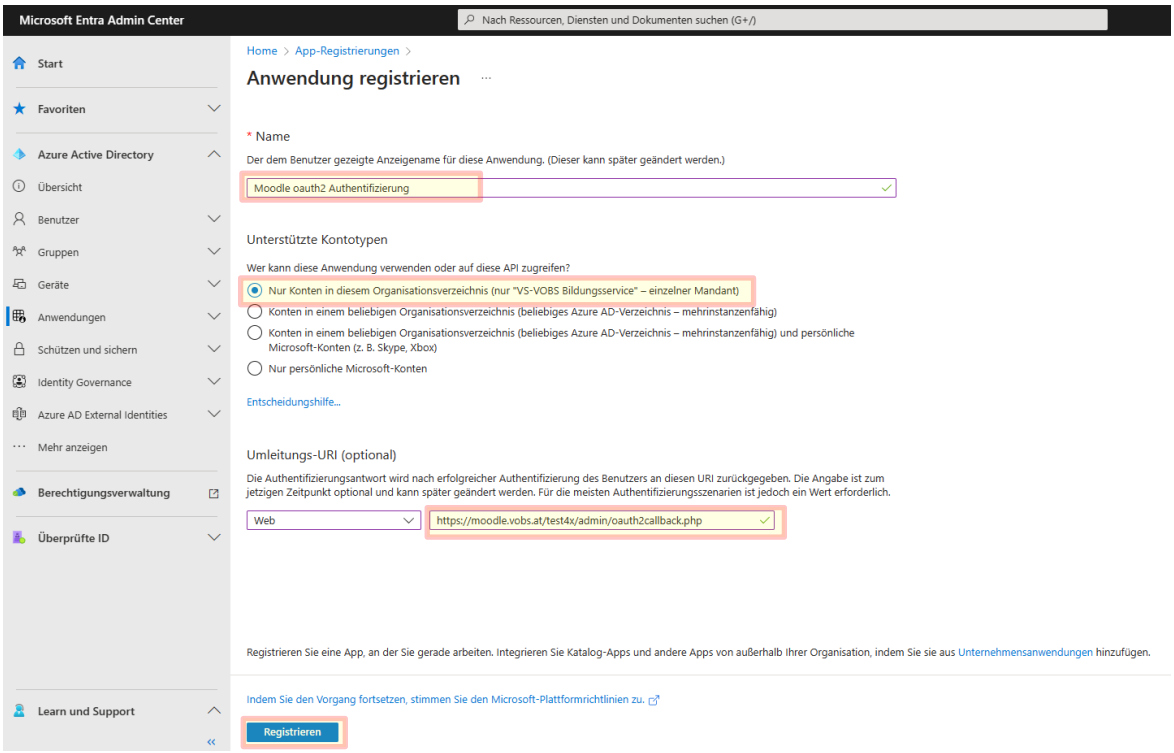
Azure Active Directory → Anwendungen → App-Registrierungen



→ Neue Registrierung



Folgende Werte eintragen:



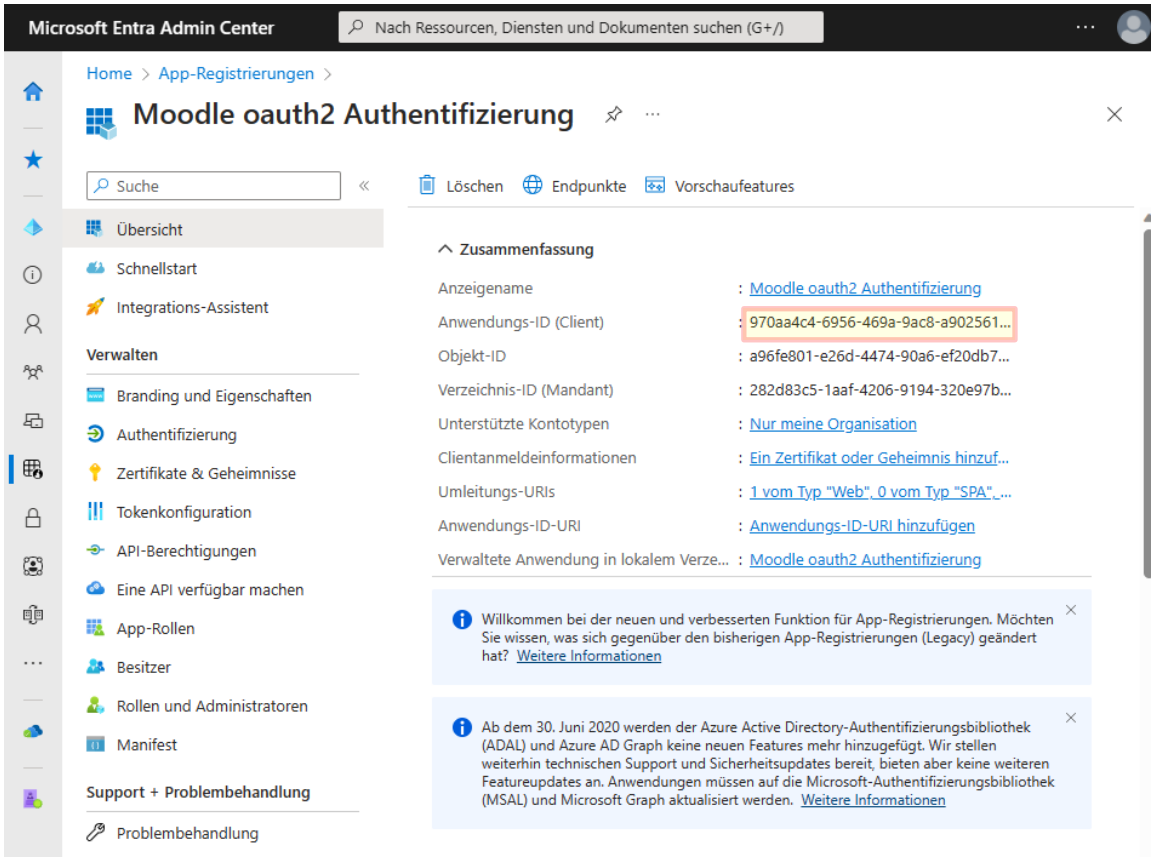
Name: sinnvolle Bezeichnung der Registrierung

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

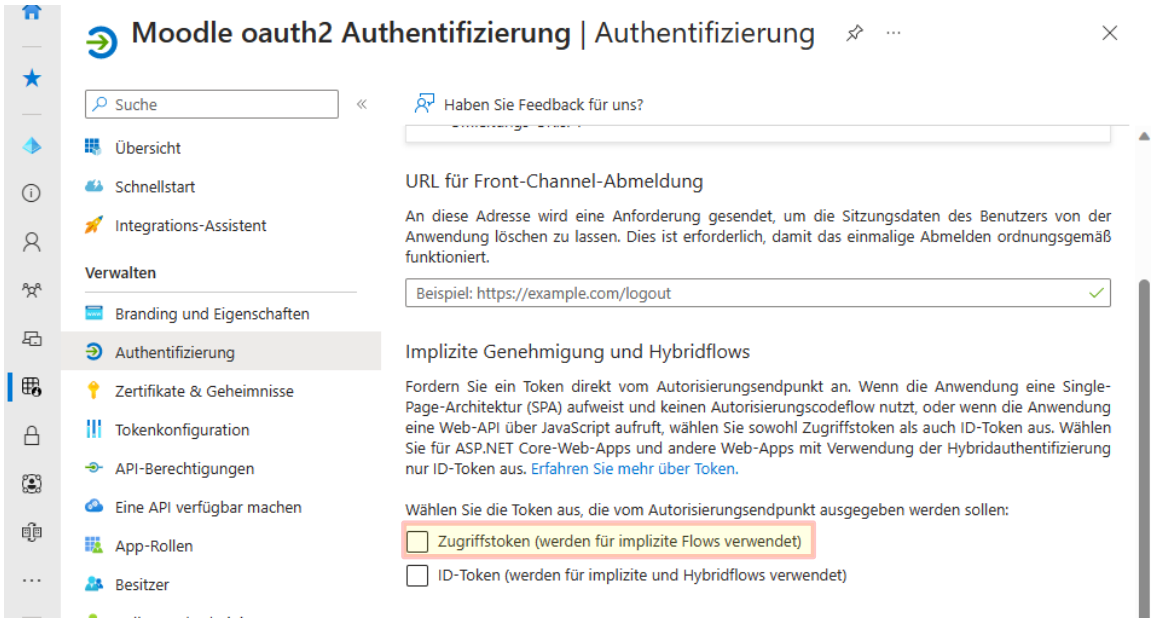
→ Registrieren



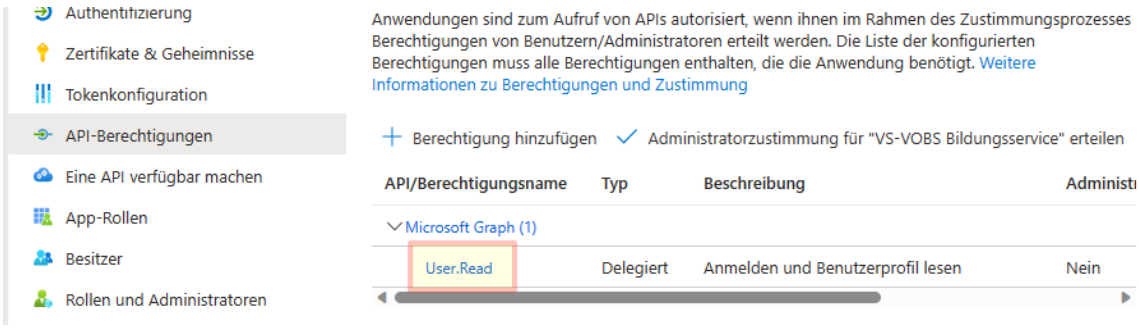
Die Anwendungs-ID in „Moodle Microsoft SSO.txt“ kopieren (wird später benötigt).

Folgende Punkte Kontrollieren:

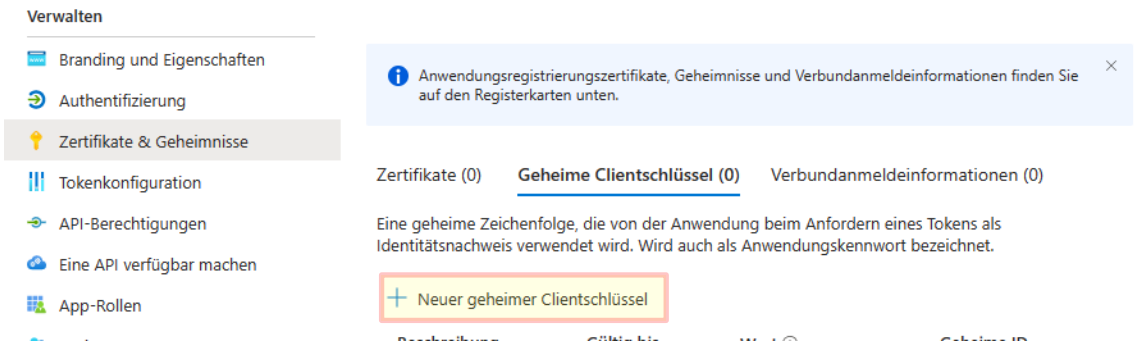
Authentifizierung → Zugrifftoken (werden für implizite Flows verwendet) → **deaktiviert**

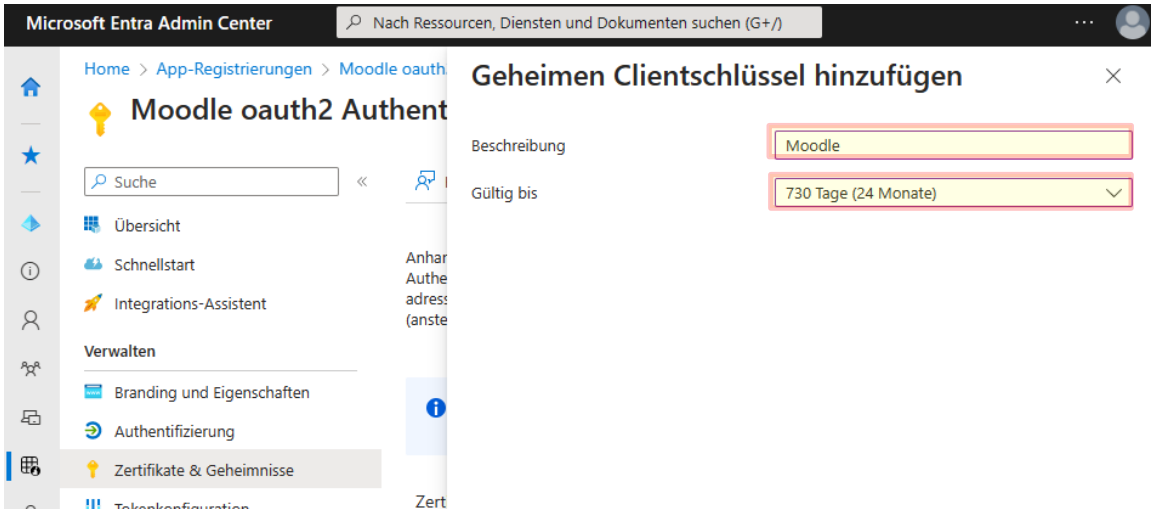


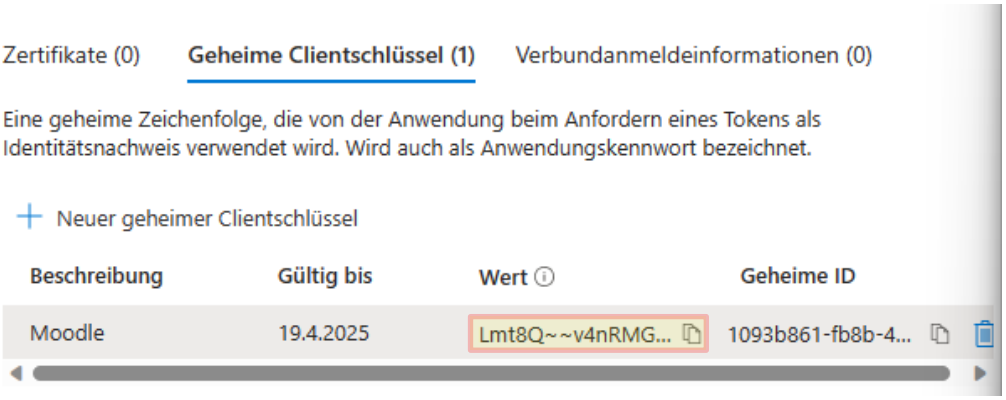
API-Berechtigungen → Microsoft Graph (1) → User.Read enthalten



Zertifikate & Geheimnisse → Beschreibung: Moodle mit einer Gültigkeit von 24 Monaten.



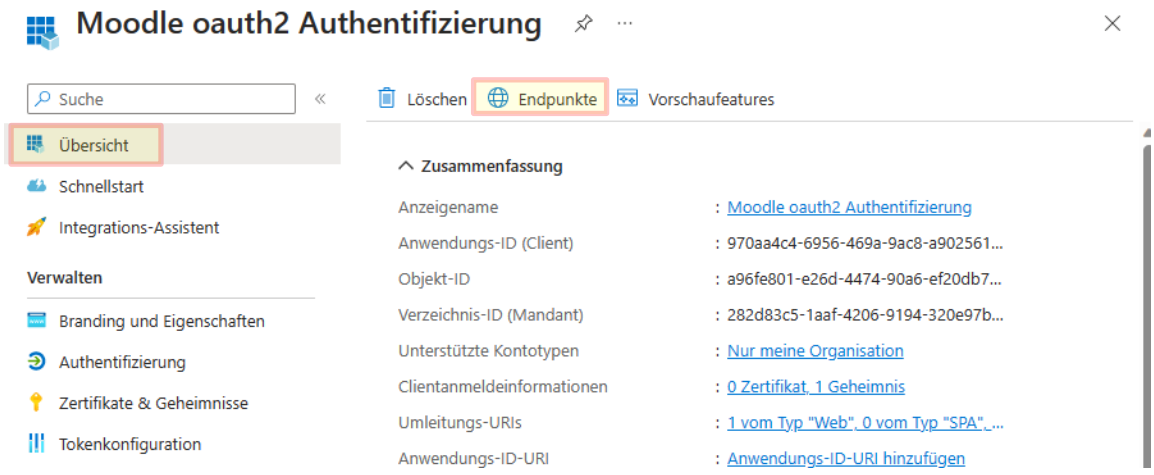


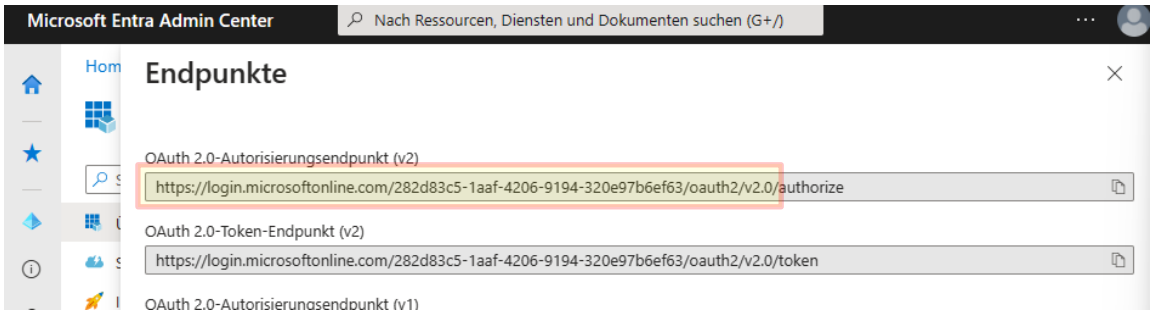


Unbedingt den Wert des Schlüssels in das Dokument „Moodle Microsoft SSO.txt“ kopieren.

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.

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…

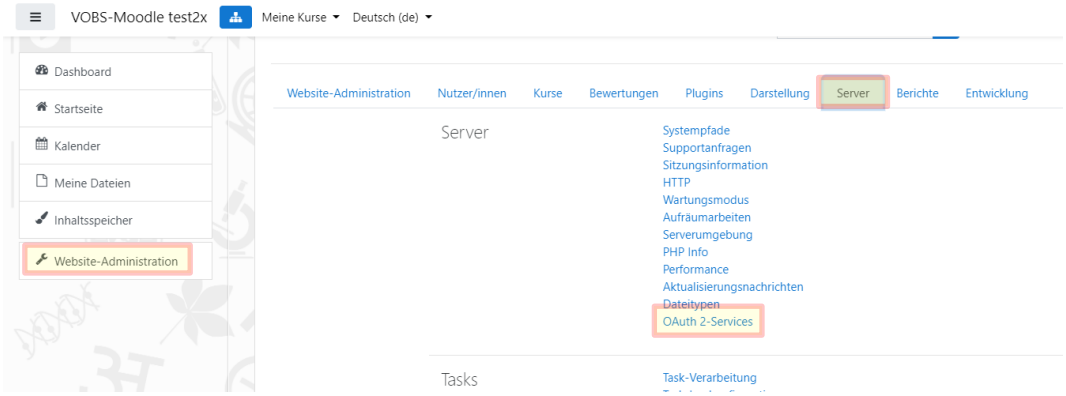
Wert des Schlüssels: Lmt8Q~~v4nRMGeIlw4vH8VvY1GsJNWU…

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

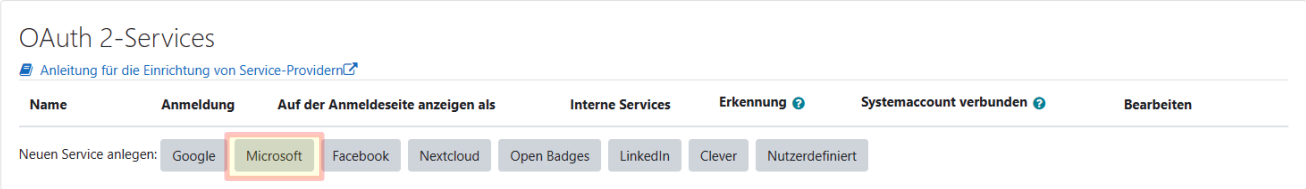
3. Eigene Moodle-Instanz

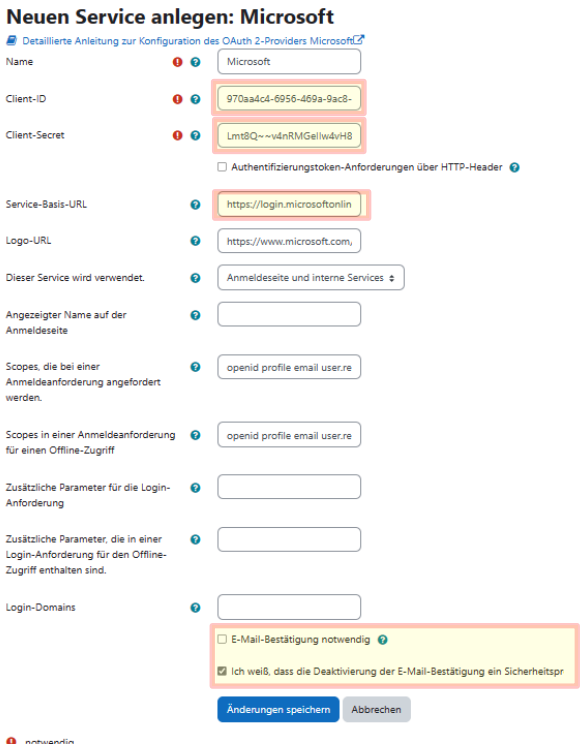
3.1. Website-Administration

Wechsle in die Website-Administration → Server → Oauth 2-Services



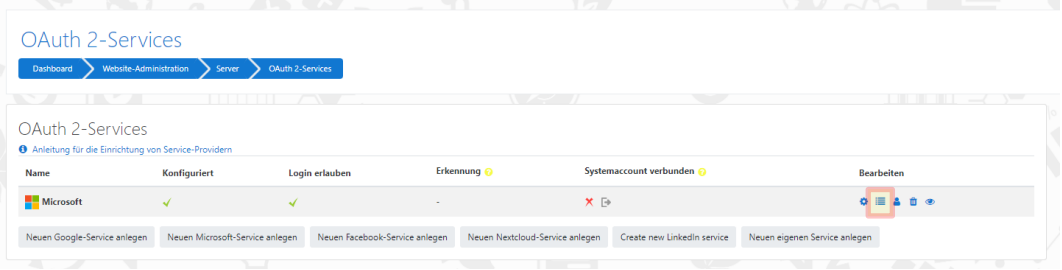
Klicke auf die Schaltfläche „Neuen Microsoft-Service anlegen“



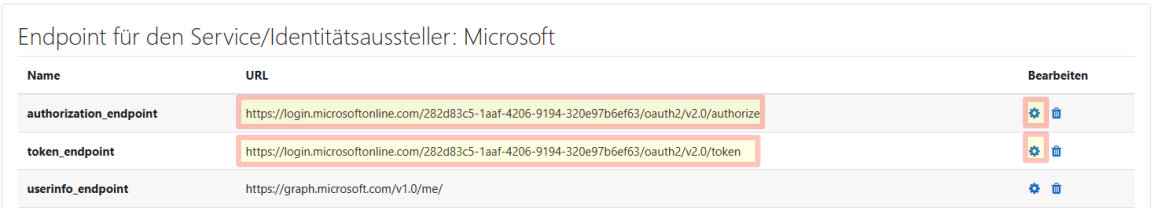


Trage die Werte aus „Moodle Microsoft SSO.txt“ in die Felder **Client-ID** (= Anwendungs-ID), **Client-Secret** (= Geheime Schlüssel) und die **Service-Basis-URL** (= Endpunkt) ein.

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.



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

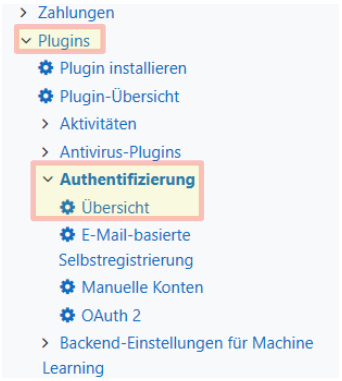


Bei **authorization_endpoint** und beim **token_endpoint** muss die **ID** enthalten sein.
Sollte „https://login.microsoftonline.com/common/oauth2/v2.0/authorize“ bzw. „…/token“ eingetragen sein, kopiere aus dem Azure AD die betreffenden Endpunkte ins Moodle. Ändern des Endpunktes mit dem Zahnrad. Diese Endpunkte befinden sich in der App-Registrierungen.

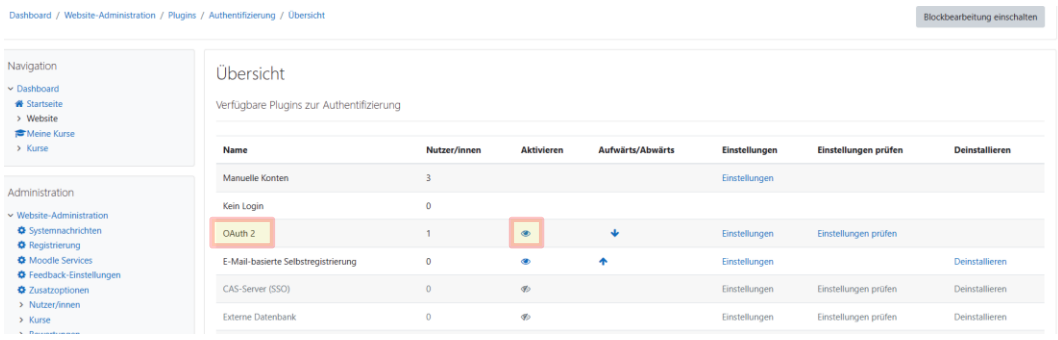
3.2. Aktivieren der Authentifizierung

Als letzten Punkt muss noch die Authentifizierung aktiviert werden.

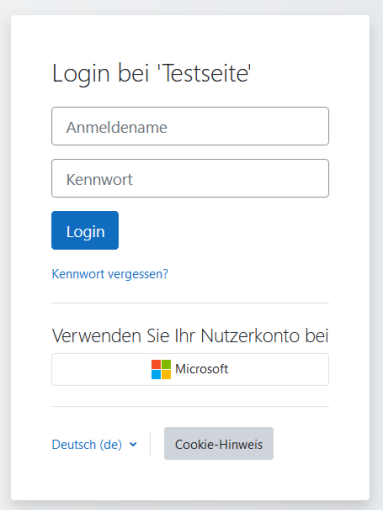
Website-Administration → Plugins → Authentifizierung → Übersicht



Aktiviere das „OAuth 2“ Plugin mit dem „Auge“-Symbol.



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



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.