



OAuth2 Konfiguration 23.4

in Moodle 3.10/4.1

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

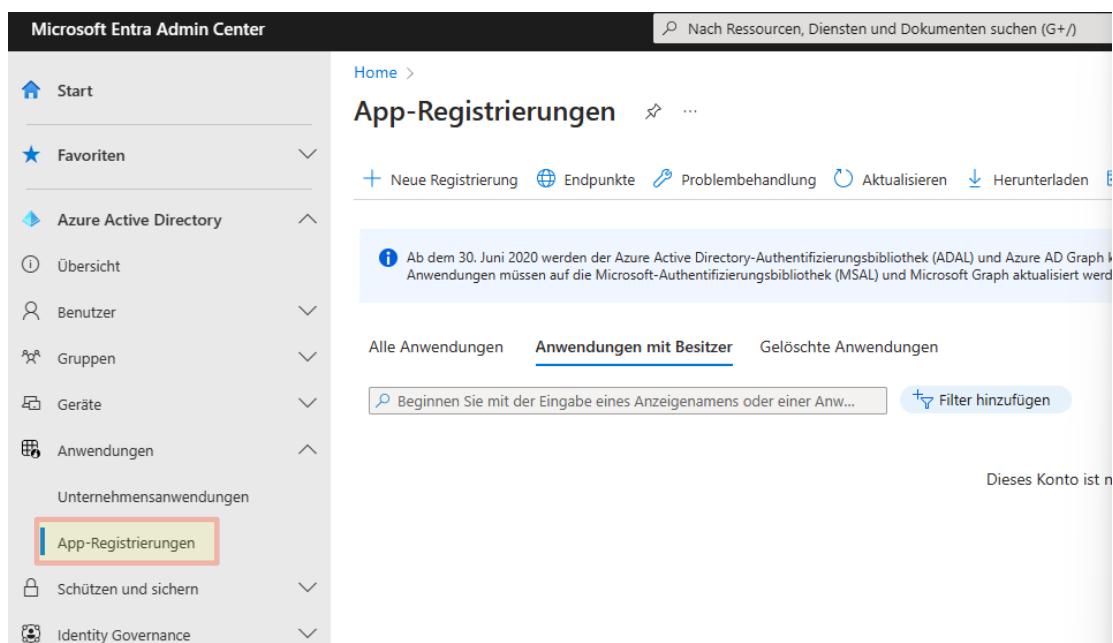
Das OAuth 2 Authentifizierungs-Plugin ermöglicht es Benutzern, sich mit ihrem Google-, Microsoft- und/oder Facebook-Konto über Schaltflächen auf der Anmeldeseite anzumelden. Dies ist ein Standard Moodle Plugin. Damit die Oauth2 Authentifizierung in Moodle funktioniert, müssen zuerst Einstellungen im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

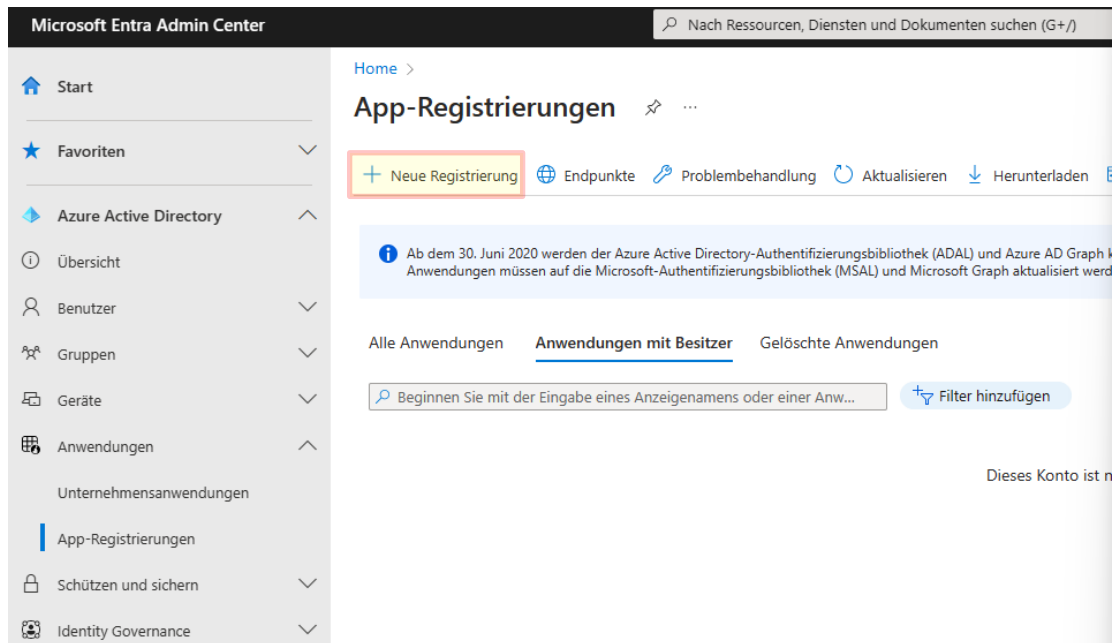
2. Vorbereitung Azure Active Directory

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

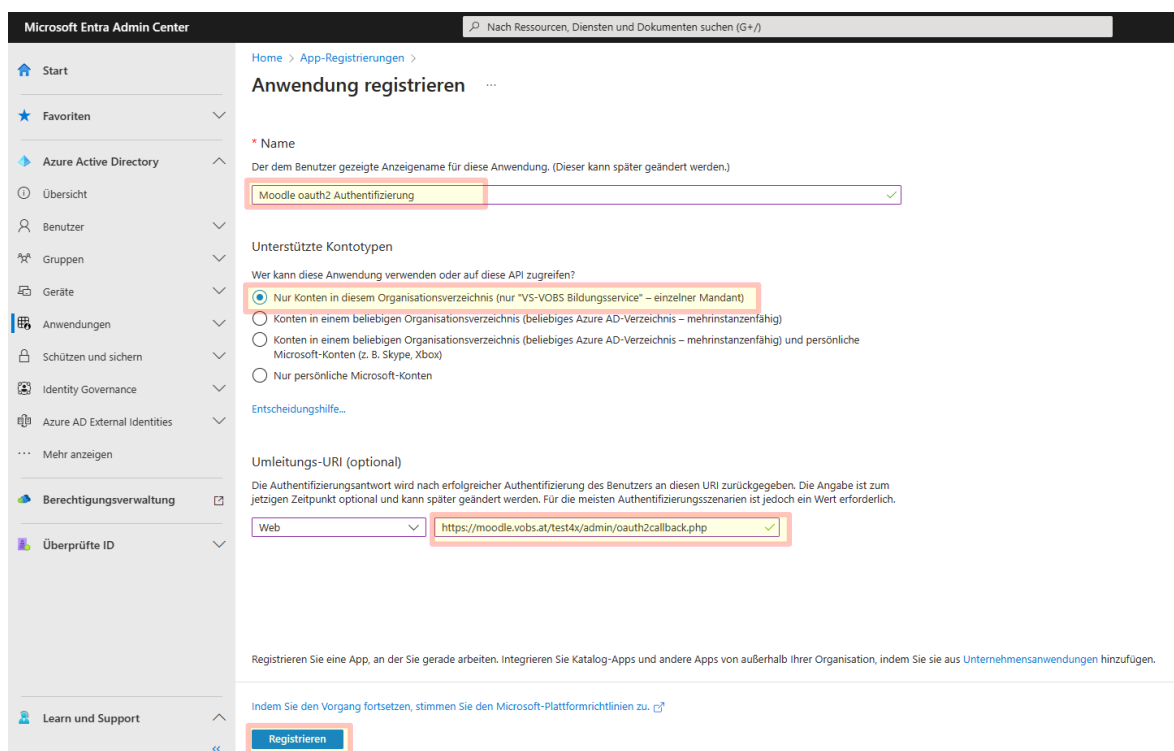
Azure Active Directory → Anwendungen → App-Registrierungen



→ Neue Registrierung



Folgende Werte eintragen:



Name: sinnvolle Bezeichnung der Registrierung

Kontotypen: Nur Konten in diesem Organisationsverzeichnis

Umleitungen – 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

Microsoft Entra Admin Center

Nach Ressourcen, Diensten und Dokumenten suchen (G+/)

Home > App-Registrierungen > Moodle oauth2 Authentifizierung

Suche

Löschen Endpunkte Vorschaufeatures

Übersicht

Schnellstart

Integrations-Assistent

Verwalten

Branding und Eigenschaften

Authentifizierung

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

Rollen und Administratoren

Manifest

Support + Problembehandlung

Problembehandlung

Zusammenfassung

Anzeigename : Moodle oauth2 Authentifizierung

Anwendungs-ID (Client) : 970aa4c4-6956-469a-9ac8-a902561...

Objekt-ID : a96fe801-e26d-4474-90a6-ef20db7...

Verzeichnis-ID (Mandant) : 282d83c5-1aaf-4206-9194-320e97b...

Unterstützte Kontotypen : Nur meine Organisation

Clientanmeldeinformationen : Ein Zertifikat oder Geheimnis hinzufügen...

Umleitungs-URIs : 1 vom Typ "Web", 0 vom Typ "SPA", ...

Anwendungs-ID-URI : Anwendungs-ID-URI hinzufügen

Verwaltete Anwendung in lokalem Verze... : Moodle oauth2 Authentifizierung

Willkommen bei der neuen und verbesserten Funktion für App-Registrierungen. Möchten Sie wissen, was sich gegenüber den bisherigen App-Registrierungen (Legacy) geändert hat? [Weitere Informationen](#)

Ab dem 30. Juni 2020 werden der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Azure AD Graph keine neuen Features mehr hinzugefügt. Wir stellen weiterhin technischen Support und Sicherheitsupdates bereit, bieten aber keine weiteren Featureupdates an. Anwendungen müssen auf die Microsoft-Authentifizierungsbibliothek (MSAL) und Microsoft Graph aktualisiert werden. [Weitere Informationen](#)

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

Folgende Punkte Kontrollieren:

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

Moodle oauth2 Authentifizierung | Authentifizierung

Suche

Haben Sie Feedback für uns?

Übersicht

Schnellstart

Integrations-Assistent

Verwalten

Branding und Eigenschaften

Authentifizierung

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

URL für Front-Channel-Abmeldung

An diese Adresse wird eine Anforderung gesendet, um die Sitzungsdaten des Benutzers von der Anwendung löschen zu lassen. Dies ist erforderlich, damit das einmalige Abmelden ordnungsgemäß funktioniert.

Beispiel:

Implizite Genehmigung und Hybridflows

Fordern Sie ein Token direkt vom Autorisierungsendpunkt an. Wenn die Anwendung eine Single-Page-Architektur (SPA) aufweist und keinen Autorisierungscodeflow nutzt, oder wenn die Anwendung eine Web-API über JavaScript aufruft, wählen Sie sowohl Zugriffstoken als auch ID-Token aus. Wählen Sie für ASP.NET Core-Web-Apps und andere Web-Apps mit Verwendung der Hybridauthentifizierung nur ID-Token aus. [Erfahren Sie mehr über Token.](#)

Wählen Sie die Token aus, die vom Autorisierungsendpunkt ausgegeben werden sollen:

Zugriffstoken (werden für implizite Flows verwendet)

ID-Token (werden für implizite und Hybridflows verwendet)

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

Authentifizierung
 Zertifikate & Geheimnisse
 Tokenkonfiguration
API-Berechtigungen
 Eine API verfügbar machen
 App-Rollen
 Besitzer
 Rollen und Administratoren

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen und Zustimmung](#)

+ Berechtigung hinzufügen ✓ Administratorzustimmung für "VS-VOBS Bildungsservice" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administr...
Microsoft Graph (1)			
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein

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

Verwalten

Branding und Eigenschaften
 Authentifizierung
Zertifikate & Geheimnisse
 Tokenkonfiguration
 API-Berechtigungen
 Eine API verfügbar machen
 App-Rollen

Anwendungsregistrierungszertifikate, Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.

Zertifikate (0) **Geheime Clientschlüssel (0)** Verbundanmeldeinformationen (0)

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

+ Neuer geheimer Clientschlüssel

Microsoft Entra Admin Center

Nach Ressourcen, Diensten und Dokumenten suchen (G+/)

Home > App-Registrierungen > Moodle oauth2

Moodle oauth2 Authentifizierung

Suche

Übersicht
 Schnellstart
 Integrations-Assistent

Verwalten

Branding und Eigenschaften
 Authentifizierung
Zertifikate & Geheimnisse
 Tokenkonfiguration

Geheimen Clientschlüssel hinzufügen

Beschreibung: Moodle

Gültig bis: 730 Tage (24 Monate)

Anhang
 Authentifizierungsadresse (anste...

Zertifikate (0) **Geheime Clientschlüssel (1)** Verbundanmeldeinformationen (0)

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

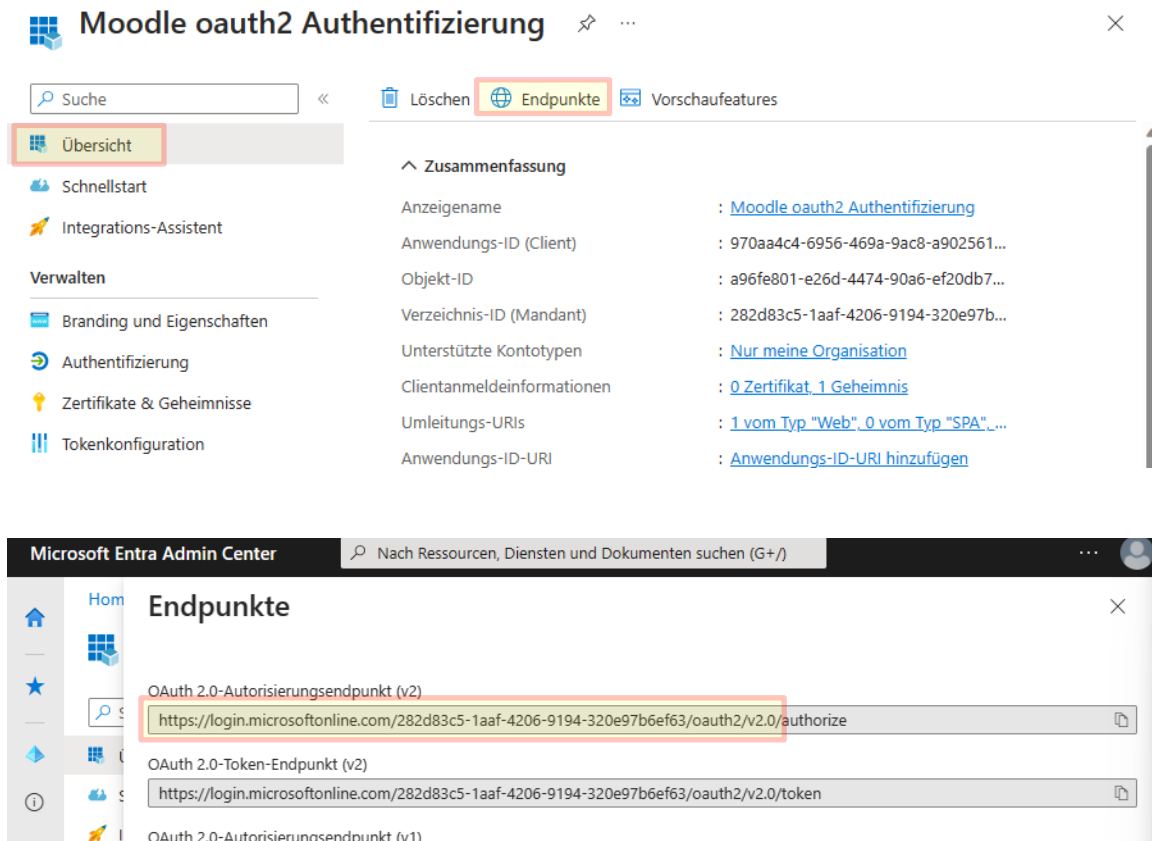
+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	Geheime ID
Moodle	19.4.2025	Lmt8Q~v4nRMG...	1093b861-fb8b-4...

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 benötigte 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...

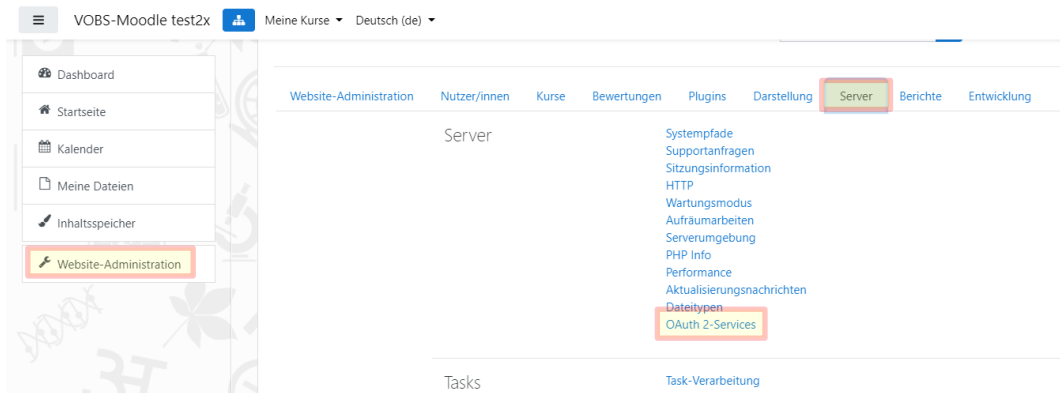
Wert des Schlüssels: Lmt8Q~~v4nRMGellw4vH8VvY1GsJNWU...

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

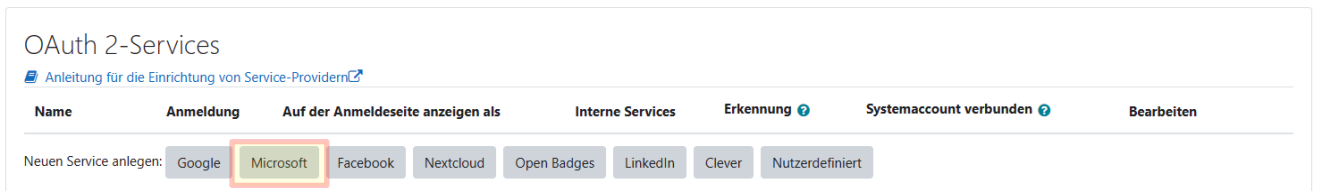
3. Eigene Moodle-Instanz

3.1. Website-Administration

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



Klicke auf die Schaltfläche „Neuen Microsoft-Service anlegen“



Neuen Service anlegen: Microsoft

[Detaillierte Anleitung zur Konfiguration des OAuth 2-Providers Microsoft](#)

Name	Microsoft
Client-ID	970aa4c4-6956-460a-9ac8-
Client-Secret	Lmt8Q~--v4nRMGellw4vH8
Service-Basis-URL	https://login.microsoftonline
Logo-URL	https://www.microsoft.com
Dieser Service wird verwendet.	Anmeldeseite und interne Services
Angezeigter Name auf der Anmeldeseite	
Scopes, die bei einer Anmeldeanforderung angefordert werden.	openid profile email user.re
Scopes in einer Anmeldeanforderung für einen Offline-Zugriff	openid profile email user.re
Zusätzliche Parameter für die Login-Anforderung	
Zusätzliche Parameter, die in einer Login-Anforderung für den Offline-Zugriff enthalten sind.	
Login-Domains	

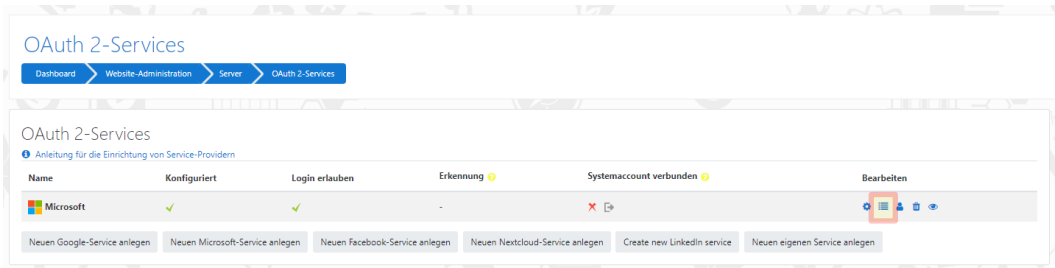
E-Mail-Bestätigung notwendig

Ich weiß, dass die Deaktivierung der E-Mail-Bestätigung ein Sicherheitspr

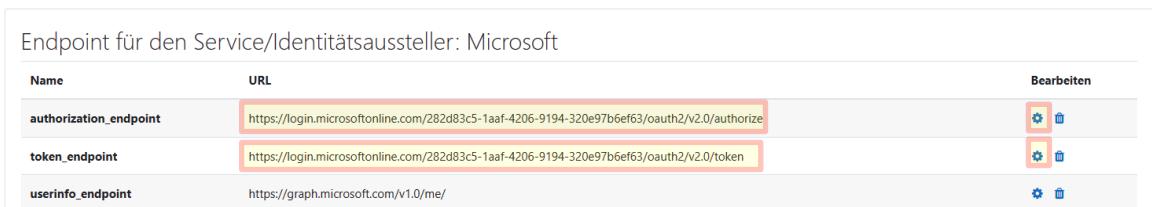
Änderungen speichern Abbrechen

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.

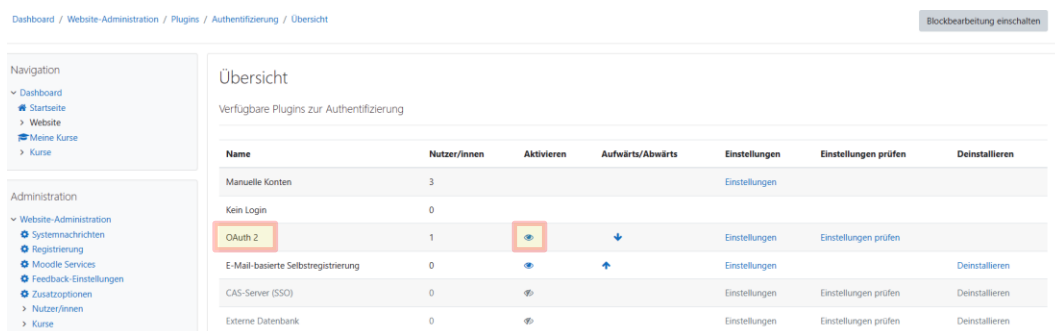
3.2. Aktivieren der Authentifizierung

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.

The screenshot shows a login interface with the following elements:

- Title: Login bei 'Testseite'
- Input field: Anmeldenname
- Input field: Kennwort
- Button: Login (blue)
- Text: Kennwort vergessen?
- Text: Verwenden Sie Ihr Nutzerkonto bei
- Input field: Microsoft (with Microsoft logo)
- Text: Deutsch (de) ▾
- Button: Cookie-Hinweis

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.