

# Handbuch - Add-ons - MS Azure AD über OAuth

Brainformatik GmbH

2024-04-05

<b>1 Einführung MS Azure AD über OAuth</b>	<b>1</b>
<b>2 Aktivierung und Konfiguration</b>	<b>2</b>
2.1 Aktivierung . . . . .	2
2.2 Konfiguration in MS Azure AD . . . . .	3
2.3 Konfiguration in CRM+ . . . . .	3
<b>3 Login-Prozess</b>	<b>6</b>
<b>4 Fehlerbehandlung</b>	<b>12</b>

---

## Einführung MS Azure AD über OAuth

---

Das CRM+ Add-on „MS Azure AD über OAuth“ ermöglicht die OAuth Anmeldung an das CRM mittels eines Office365 Kontos.

Bei OAuth handelt es sich um ein offenes Sicherheitsprotokoll für die tokenbasierte Autorisierung und Authentifizierung im Internet.

Die Anmeldedaten - insbesondere das Passwort - werden dabei nicht in der Datenbank von CRM+ gespeichert.

---

### **Definition**

Microsoft Azure ist eine Cloud-Computing-Plattform von Microsoft, welche Anwendungen und Datenbanken zur Verfügung stellt, die netzbasiert genutzt werden können.

Der Enterprise-Identitätsdienst Azure Active Directory (Azure AD) bietet Single Sign-On (SSO) und mehrstufige Authentifizierung (Multi-Factor Authentication).

---

Das Add-on „MS Azure AD“ gehört nicht zum Standardumfang von CRM+, kann jedoch separat erworben werden.

Für weitere Informationen hierzu besuchen Sie bitte unsere Webseite unter [brainformatik.com](http://brainformatik.com) oder kontaktieren uns per E-Mail/Telefon.

### 2.1 Aktivierung

---

**Bemerkung:** Add-ons werden nach dem Erwerb i.d.R. von der Brainformatik GmbH aktiviert.

---

Grundsätzlich können Add-ons aber auch durch Kunden aktiviert werden.

Damit Sie selbst ein Add-on aktivieren können, benötigen Sie einen passenden Aktivierungscode. Nach dem Erwerb des Add-ons erhalten Sie einen Aktivierungscode, welcher zur Aktivierung in den Globalen Einstellungen im Punkt Add-on Manager benötigt wird.

The screenshot shows the 'Add-on Manager' settings page in CRM+. The left sidebar contains a search bar and a list of settings categories. The main content area displays a table of installed add-ons:

Add-on Name	Status	Configuration
Anbindung externe Zeiterfassung	✓	⚙️
Besuchsbericht	✓	
DATEV Buchungsdatenservice	✓	⚙️
DATEV Rechnungsdatenservice 1.0	✓	⚙️
Digitaler Assistent powered by ChatGPT		Aktivieren
DocuSign		Aktivieren
DS-GVO (weiterführende Informationen)		Aktivieren
E-Mail-Marketing: Brevo		Aktivieren
E-Mail-Marketing: CleverReach	✓	
Kontingente	✓	
Lieferscheine	✓	
Microsoft Teams	✓	
MS Azure AD über OAuth	✓	
Multimandantenfähigkeit	✓	
PDF-Vorlagen Plus	✓	
SalesViewer		Aktivieren
snapADDY	✓	⚙️
Softphone Connector	✓	
Umkreissuche	✓	
Variable Pflichtfelder	✓	
ZUGFeRD		Aktivieren

## 2.2 Konfiguration in MS Azure AD

Das OAuth 2.0 Anmeldeverfahren muss im Microsoft Azure Active Directory Server konfiguriert sein. Weitere Einstellungen in MS Azure AD müssen ansonsten nicht vorgenommen werden.

## 2.3 Konfiguration in CRM+

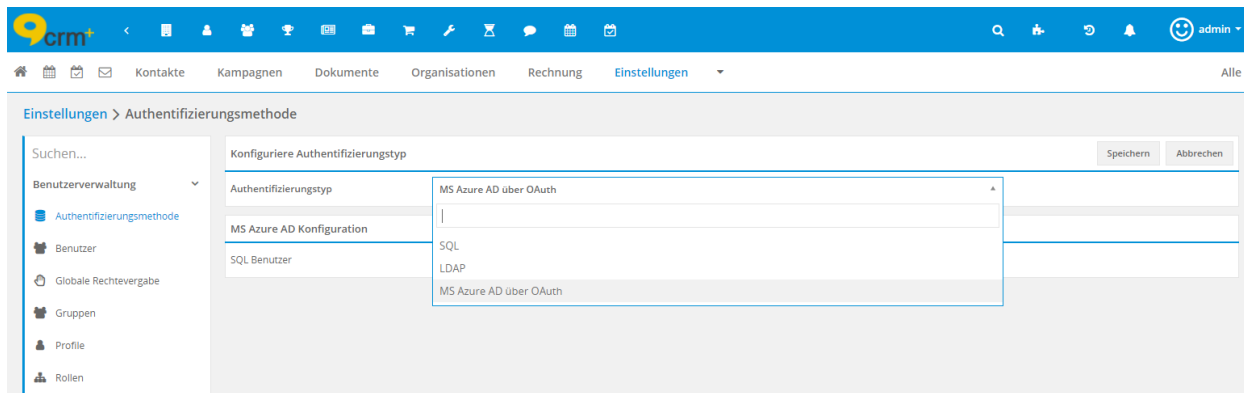
Nach Aktivierung des Add-ons muss lediglich die Authentifizierungsart über die Globalen Einstellungen auf Azure AD geändert und bei den Benutzern die E-Mail Adressen für den Azure AD hinterlegt werden.

Der Einstellungspunkt „Authentifizierungsart“ befindet sich im Bereich „Benutzerverwaltung“:

The screenshot shows the 'Benutzerverwaltung' (User Management) settings page in CRM+. The page is divided into several sections:

- Authentifizierungsmethode**: Verwalten Sie den Authentifizierungstyp von CRM+
- Benutzer**: Erstellen, bearbeiten oder löschen Sie CRM Benutzer
- Globale Rechtevergabe**: Definieren Sie die unternehmensweit gültigen Zugangsrechte für alle aktiven Module
- Gruppen**: Definieren Sie Gruppen auf Basis von Rollen, Benutzern oder bereits vorhandenen anderen Gruppen
- Profile**: Definieren Sie Profile für Benutzer, um die Zugriffsrechte für Module, Felder und diversen Aktionen bestimmen zu können
- Rollen**: Definieren Sie die Hierarchie von Benutzer-Rollen, um den Zugriff auf Datensätze regeln zu können

Der Einstellungspunkt „Authentifizierungsart“ stellt sich wie folgt dar:



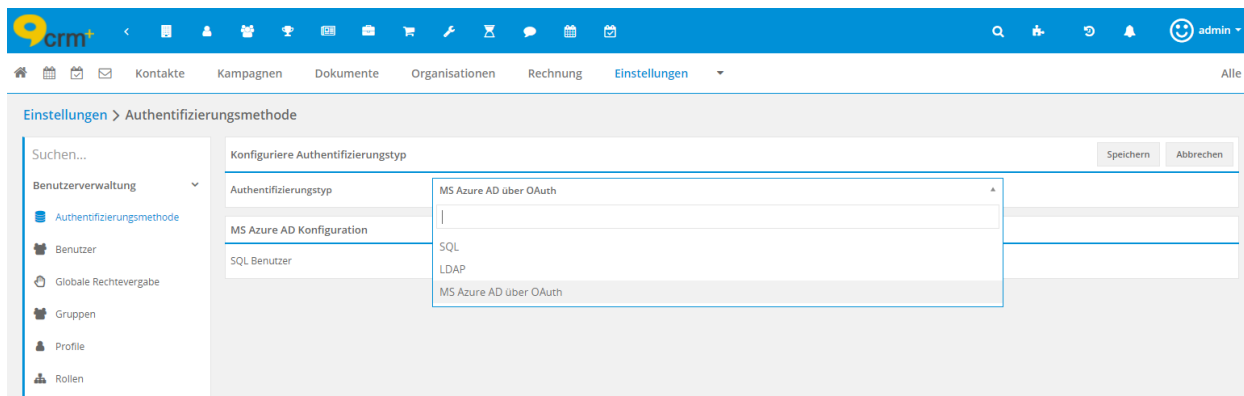
Es sind hier zwei Einstellungsbereiche verfügbar:

- Konfiguriere Authentifizierungstyp
- MS Azure AD Konfiguration

### Konfiguriere Authentifizierungstyp

Bei aktiviertem Add-on „MS Azure AD über OAuth“ sind in der Auswahlliste „Authentifizierungstyp“ drei Werte verfügbar:

- SQL - Für den Login wird der Benutzername und das Passwort (verschlüsselt) in der CRM Datenbank gespeichert.
- LDAP - Benutzerauthentifizierung über ein LDAP-Verzeichnis. Siehe hierzu Abschnitt LDAP im Handbuch.
- MS Azure AD über OAuth - Anmeldung an CRM+ mittels eines Office365 Kontos.



### MS Azure AD Konfiguration

In diesem Einstellungspunkt werden die CRM Benutzer festgelegt, welche sich weiterhin über den Authentifizierungstyp „SQL“ anmelden sollen.

Siehe hierzu auch den Abschnitt *Login ohne MS Azure AD über OAuth* im Handbuch.

**Bemerkung:** Für den Benutzer „admin“ ist der Authentifizierungstyp „SQL“ fest hinterlegt und kann auch

nicht geändert werden.

### 2.3.1 Benutzereinstellungen

Bei aktiviertem Add-on „MS Azure AD über OAuth“ ist in den Benutzereinstellungen das Feld „Azure AD E-Mail“ verfügbar, in welchem die E-Mail Adresse hinterlegt werden muss, welche zur Anmeldung genutzt wird:

The screenshot shows the user settings for 'Peter' in the CRM+ system. The interface includes a navigation menu on the left and a main content area with tabs for 'Benutzer', 'Grundeinstellungen', 'Weitere Einstellungen', 'Schnittstellen', 'Tag Einstellungen', 'Kalender', and 'Meine Gruppen'. The 'Benutzer' tab is selected, displaying a list of user attributes and their values. Two fields are highlighted with orange boxes: 'Passwort' (set to 'MS Azure AD Anmeldeprozess') and 'Azure AD E-Mail' (set to 'peter.mueller@localhost.xy').

Attribut	Wert
Nutzername	Peter
Rolle	CEO
Nachname	Müller
Status	Aktiv
Weitere E-Mail	
Funktion	Geschäftsführer
Abteilung	
Mobil	
Vorgesetzter	
Azure AD E-Mail	peter.mueller@localhost.xy
Benutzerbild	
Passwort	MS Azure AD Anmeldeprozess
Vorname	Peter
E-Mail	peter.mueller@localhost.xy
Telefon Büro	
Weiteres Telefon	
Sprache	Deutsch
Rechtmanagement	CustomerAdmin
Beschreibung	

**Warnung:** Die beim Benutzer hinterlegte E-Mail Adresse im Feld „Azure AD E-Mail“ muss für dieses Feld systemweit einzigartig sein.

Ist für einen Benutzer der Authentifizierungstyp „MS Azure AD über OAuth“ konfiguriert, wird beim Feld „Passwort“ der Wert „MS Azure AD Anmeldeprozess“ angezeigt. Der Button „Passwort ändern“ steht nicht mehr zur Verfügung.

Bei aktiviertem Add-on „MS Azure AD über OAuth“ stellt sich die Loginseite wie folgt dar:

CRM+MS Azure AD Login

*Login wechseln*

CRM+

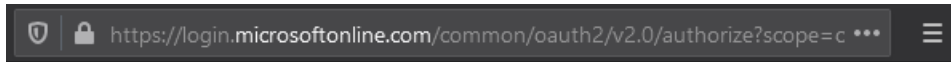
Powered by Brainformatik GmbH | [Impressum](#) | [App öffnen](#)

### **Erstmaliger Login**

Beim ersten Login wird nach dem Anklicken des Buttons „MS Azure AD Login“ autom. ein weiteres Browserfenster geöffnet, in welchem die Anmeldedaten (E-Mail Adresse und Passwort) des Microsoft-Kontos eingetragen werden müssen.

Eingabe der E-Mail Adresse:





## Anmelden

E-Mail, Telefon oder Skype

Kein Konto? [Erstellen Sie jetzt eins!](#)

[Sie können nicht auf Ihr Konto zugreifen?](#)

Zurück

Weiter



Anmeldeoptionen

[Nutzungsbedingungen](#) [Datenschutz & Cookies](#) ...

Eingabe des Kennworts:



← [redacted]@ [redacted].com

## Kennwort eingeben

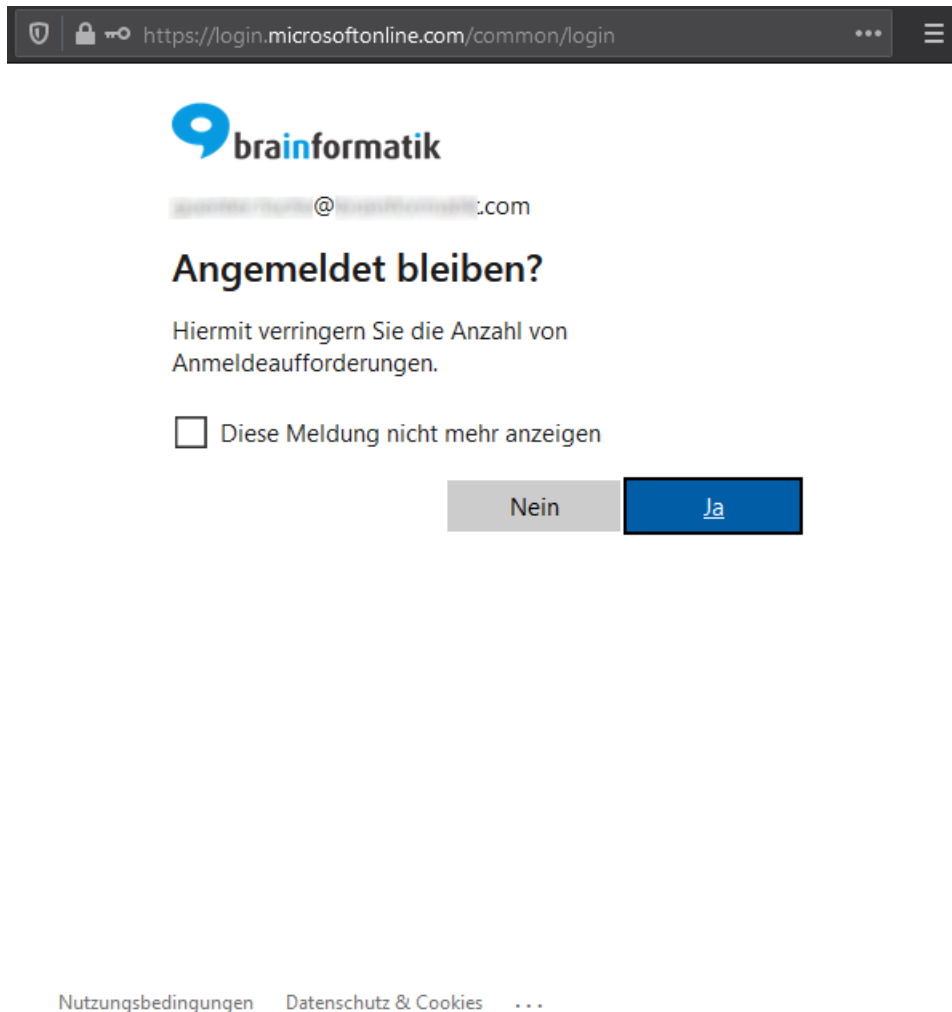
.....|

[Kennwort vergessen](#)

Anmelden

[Nutzungsbedingungen](#) [Datenschutz & Cookies](#) ...

Abfrage „Angemeldet bleiben?“:



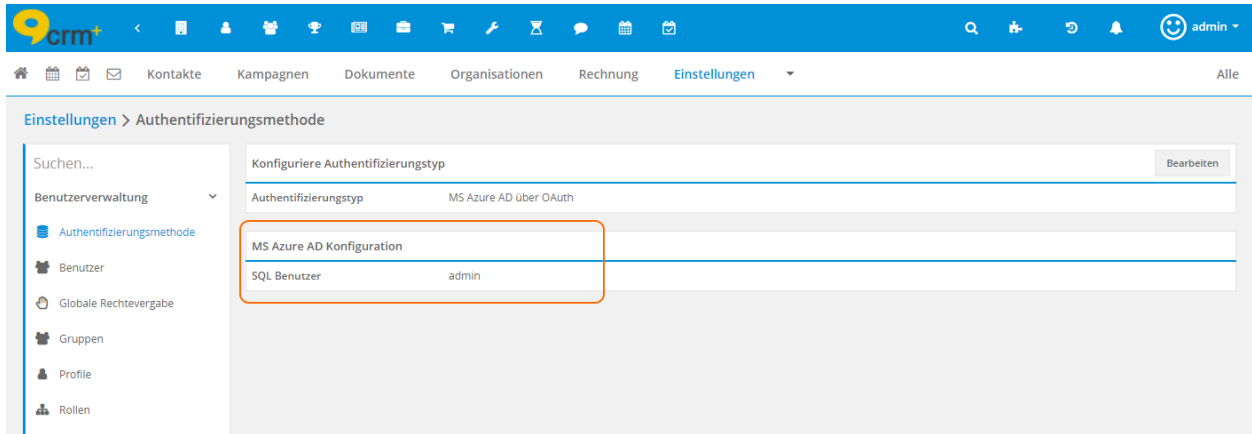
Nach der abschließenden Bestätigung wird der Login in CRM+ ausgeführt.

### **Künftige Logins**

Solange die OAuth Authentifizierung gültig ist, muss der Benutzer für künftige Logins lediglich den Button „MS Azure AD Login“ anklicken, ohne nochmals die Anmeldedaten (E-Mail Adresse und Passwort) des Microsoft-Kontos eintragen zu müssen.

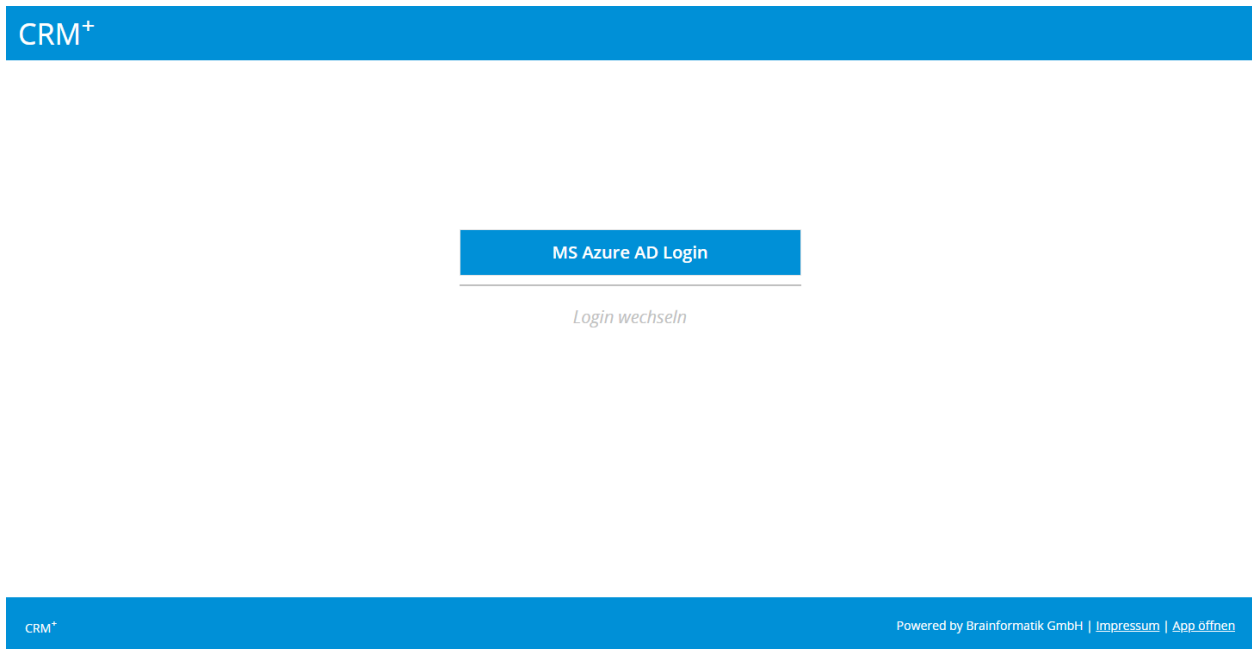
### **Login ohne MS Azure AD über OAuth**

In Globale Einstellungen - Authentifizierungsmethode können beim Einstellungspunkt „MS Azure AD Konfiguration“ CRM Benutzer festgelegt werden, welche sich weiterhin über den Authentifizierungstyp „SQL“ anmelden sollen.



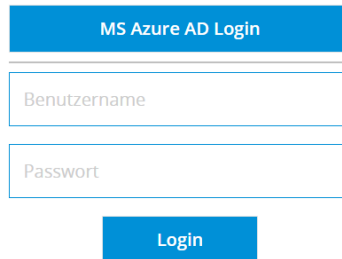
**Bemerkung:** Für den Benutzer „admin“ ist der Authentifizierungstyp „SQL“ fest hinterlegt und kann nicht geändert werden.

Alle CRM Benutzer, welche sich weiterhin über den Authentifizierungstyp „SQL“ anmelden, müssen auf der Loginseite den Button „Login wechseln“ anklicken:



Nach dem Anklicken werden die Eingabefelder für Benutzername und Passwort eingeblendet:

CRM+



The image shows a login form for MS Azure AD. It consists of a blue header bar with the text "MS Azure AD Login". Below the header are two input fields: "Benutzername" (Username) and "Passwort" (Password). At the bottom of the form is a blue button labeled "Login".

CRM+

Powered by Brainformatik GmbH | [Impressum](#) | [App öffnen](#)

Nach der Eingabe des CRM+ Benutzernamens sowie des CRM+ Passworts und dem Anklicken des Buttons „Login“ wird der Login in CRM+ ausgeführt.

**Warnung:** Die Nutzung der Mobile App für CRM Benutzer, für die der Authentifizierungstyp „MS Azure AD über OAuth“ eingestellt ist, ist in Verbindung mit „MS Azure AD“ leider nicht möglich. Es können lediglich Benutzer die Mobile App nutzen, bei der die Authentifizierung als sog. „SQL-Benutzer“ hinterlegt ist.

In Ausnahmefällen kann es zu einem Fehler während des Anmeldeverfahrens kommen. Die Ursache kann hier seitens des Microsoft Azure Active Directory Servers oder am CRM+ Loginprozess liegen.

### **Ursache Microsoft Azure Active Directory**

Bei einem Fehler während des Authentifizierungsprozesses am Microsoft Azure Active Directory Server wird die Fehlermeldung direkt vom Active Directory Server zurückgegeben.

Wenden Sie sich bitte in diesem Fall an Ihren CRM+ Administrator, bzw. den Verantwortlichen des Microsoft Azure Active Directory Servers.

### **Ursache CRM+ Loginprozess**

Könnte der Login Prozess am Microsoft Azure Active Directory Server erfolgreich abgeschlossen werden, kann es innerhalb des CRM+ Loginprozesses ebenfalls zu Fehlern kommen.

Für die Fehler, die innerhalb des CRM+ Loginprozesses auftreten ist ein Logging integriert, über welches der Administrator des CRM+ Systems Detailinformationen abrufen kann. Alle Fehlermeldungen werden in der Datei „azure\_ad.log“ protokolliert.

Benutzer mit administrativen Rechten können diese Logdatei in Globale Einstellungen - Logs verwalten einsehen.

Folgende Fehler werden in der Logdatei protokolliert:

- Fehlercode: 1597335037  
Beschreibung: Die Azure AD E-Mail in der Microsoft Azure Active Directory Server Genehmigung ist bei keinem CRM+ Benutzer hinterlegt.
- Fehlercode: 1597335049  
Beschreibung: Die Azure AD E-Mail in der Microsoft Azure Active Directory Server Genehmigung ist mehr als einem Benutzer CRM+ Benutzer zugewiesen.

- Fehlercode: 1597335055  
Beschreibung: Der Benutzer mit der Azure AD E-Mail in der Microsoft Azure Active Directory Server Genehmigung ist nicht für diesen Prozess aktiviert.
- Fehlercode: 1597335061  
Beschreibung: Die Azure AD E-Mail in der Microsoft Azure Active Directory Server Genehmigung gehört zu einem Benutzer, dessen Status „Inaktiv“ ist.