

SSO / OAuth / OpenID Connect

Benutzerverwaltung mittels SSO, OAuth und OpenID Connect.

- [Login mit Microsoft](#)

Login mit Microsoft

Mit der Squeeze Version 2.20 besteht die Möglichkeit des einfachen Logins mit Hilfe von Microsoft Entra ID auch bekannt als Azure AD.

Auf dieser Seite wird beschrieben wie sie vorgehen können, um einen Login Button auf der Anmeldeseite von Squeeze anzeigen zu lassen. Nach Abschluss der Konfiguration sieht die Anmeldeseite wie folgt aus:



SQUEEZE Extract

private.squeeze.one

deutsch



Benutzer

Passwort

Login

Login with Microsoft / SSO

[Passwort vergessen?](#)

Konfiguration in Microsoft Entra ID

Erstellen Sie ein Microsoft Entra App für ihr Unternehmen

Die Redirect URL ist die URL Ihres Squeeze Tenants mit der zusätzlichen Pfadangabe /sso/
In diesen Beispiel ist es <https://private.squeeze.one/sso/>

Anwendung registrieren ...

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

Squeeze Microsoft Login ✓

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- Nur Konten in diesem Organisationsverzeichnis (nur **private.squeeze.one** – einzelner Mandant)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- Nur persönliche Microsoft-Konten

[Entscheidungshilfe...](#)

Umleitungs-URI (optional)

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.

Web ✓ ✓

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.

Indem Sie den Vorgang fortsetzen, stimmen Sie den [Microsoft-Plattformrichtlinien](#) zu. [↗](#)

[Registrieren](#)

Secret für die App erstellen

Dokumentation Login mit Microsoft | Zertifikate & Geheimnisse

Suche

Haben Sie Feedback für uns?

- Übersicht
- Schnellstart
- Integrations-Assistent
- Diagnose und Problembehandlung

Verwalten

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

Support + Problembehandlung

- Neue Supportanfrage

Anhand von Anmeldeinformationen können vertrauliche Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) verwenden.

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

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	Geheime ID
--------------	------------	------	------------

Für diese Anwendung wurden keine Clientgeheimnisse erstellt.

Geheimen Clientschlüssel hinzufügen

Beschreibung

Gültig bis

Hinzufügen Abbrechen

Kopieren Sie das Secret.

Beachten Sie, dass das Secret später nicht mehr eingesehen/kopiert werden kann.

Dokumentation Login mit Microsoft | Zertifikate & Geheimnisse

Suche

Haben Sie Feedback für uns?

- Übersicht
- Schnellstart
- Integrations-Assistent
- Diagnose und Problembehandlung

Verwalten

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

Support + Problembehandlung

- Neue Supportanfrage

Haben Sie einen Moment, um uns Feedback zu geben? →

Anhand von Anmeldeinformationen können vertrauliche Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an einem adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) als Anmeldeinformation zu verwenden.

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

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
Dokumentation	18.9.2025	[Secret]	5e3ca94c-3d65-46e4-a7b5-0d3da80ef56a

API-Berechtigungen festlegen

Suche Aktualisieren Haben Sie Feedback für uns?

- Übersicht
- Schnellstart
- Integrations-Assistent
- Diagnose und Problembehandlung
- Verwalten
 - Branding und Eigenschaften
 - Authentifizierung
 - Zertifikate & Geheimnisse
 - Tokenkonfiguration
 - API-Berechtigungen**
 - Eine API verfügbar machen
 - App-Rollen
 - Besitzer
 - Rollen und Administratoren
 - Manifest
- Support + Problembehandlung
 - Neue Supportanfrage

Durch das Erteilen einer mandantenweiten Einwilligung können Berechtigungen widerrufen werden, die bereits mandantenweit für diese Anwendung erteilt wurden. Berechtigungen, die Benutzer bereits in ihrem eigenen Namen erteilt haben, sind davon nicht betroffen. [Weitere Informationen](#)

In der Spalte "Administratoreinwilligung erforderlich," wird der Standardwert für eine Organisation angezeigt. Die Benutzereinwilligung kann jedoch pro Berechtigung, Benutzer oder App angepasst werden. Diese Spalte zeigt möglicherweise nicht den Wert für Ihre Organisation oder für Organisationen, in denen diese App verwendet wird. [Weitere Informationen](#)

Konfigurierte Berechtigungen

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 "DEXPRO Solutions GmbH" erteilen

API/Berechtigungsnamen	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (1)				
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	✓ Gewährt für "DEXPRO S...

Um die genehmigten Berechtigungen für einzelne Apps sowie die Einwilligungseinstellungen Ihres Mandanten anzuzeigen und zu verwalten, testen Sie [Unternehmensanwendung](#).

Client App-Id und Secret in Squeeze hinterlegen

Das Secret ist nach dem Speichern nicht mehr einsehbar.

System

Version: 2.20.0
Mandant: private.squeeze.one
Mandantenname: private.squeeze.one

System Information

Microsoft-Authentifizierung

App-Id: a1234b5c-d678-90e1-fg23-hi45j678k90l
Secret:

Speichern