

MICROSOFT ENTRA · EINRICHTUNG

Workplify mit Microsoft verbinden.

Zentrale IT-Freigabe · Anmeldung · Benutzerbereitstellung

Sie benötigen einen eingerichteten Workplify-Firmenbereich, einen berechtigten Microsoft-Administrator und ein reguläres Testkonto. Ihr lokaler Firmenadmin mit Authenticator bleibt als Notfallzugang erhalten. Den Firmenbereich und das Microsoft-Verzeichnis verbindet der Workplify-Support mit Ihrer IT.

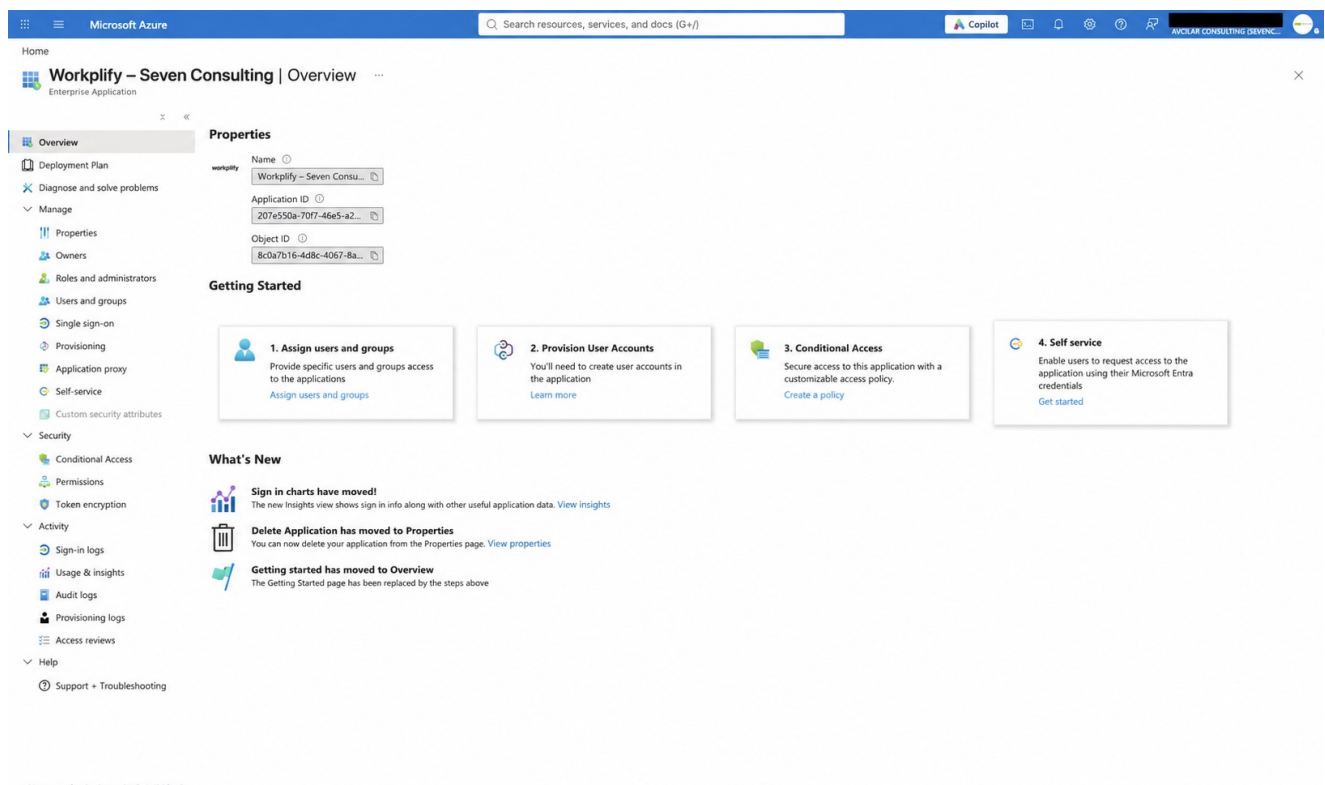
01 · Unternehmensanwendung

Die Workplify-Anwendung öffnen.

1. Im [Microsoft Entra Admin Center](#) als Administrator anmelden und das richtige Firmenverzeichnis auswählen.
2. **Entra ID > Unternehmensanwendungen > Alle Anwendungen** öffnen. Nach **Workplify - Seven Consulting** suchen; gegebenenfalls den Filter „Anwendungstyp“ auf alle Anwendungen setzen.
3. Die Anwendung öffnen und die **Anwendungs-ID** mit der unten angegebenen ID vergleichen.

207e550a-70f7-46e5-a2e5-3e4cafdd0bc2

Verwenden Sie die bereitgestellte Workplify-App mit dieser ID. Eine neue eigene App-Registrierung mit einer anderen Client-ID ist für diesen Anmeldeweg nicht erforderlich.



Unternehmensanwendung öffnen und Anwendungs-ID vergleichen. Links folgen Benutzerzuweisung und Berechtigungen.
[Große Ansicht](#)

02 · Zentrale Freigabe

Anmelderechte für das Unternehmen genehmigen.

1. In der Workplify-Unternehmensanwendung links **Sicherheit > Berechtigungen (Security > Permissions)** öffnen.
2. **Administratorzustimmung für [Ihr Unternehmen] erteilen (Grant admin consent)** auswählen. Die IT prüft und bestätigt die angeforderten Rechte für das eigene Unternehmen.
3. Unter **Administratorzustimmung (Admin consent)** kontrollieren, dass openid und profile als **Delegated / Admin consent** erscheinen.

openid ermöglicht die Anmeldung. profile liefert grundlegende Profilangaben zur Zuordnung des Kontos. Workplify benötigt für diesen Anmeldeweg keine Postfach-, SharePoint- oder umfassenden Verzeichnisrechte.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with categories like Overview, Deployment Plan, Manage, Security, Activity, and Help. The 'Permissions' page is selected under the 'Security' category. The main content area shows the 'Permissions' section for the 'Workplify - Seven Consulting' application. It includes a 'Grant admin consent for Aviclar Consulting' button and a table of permissions.

API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (2)					
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator

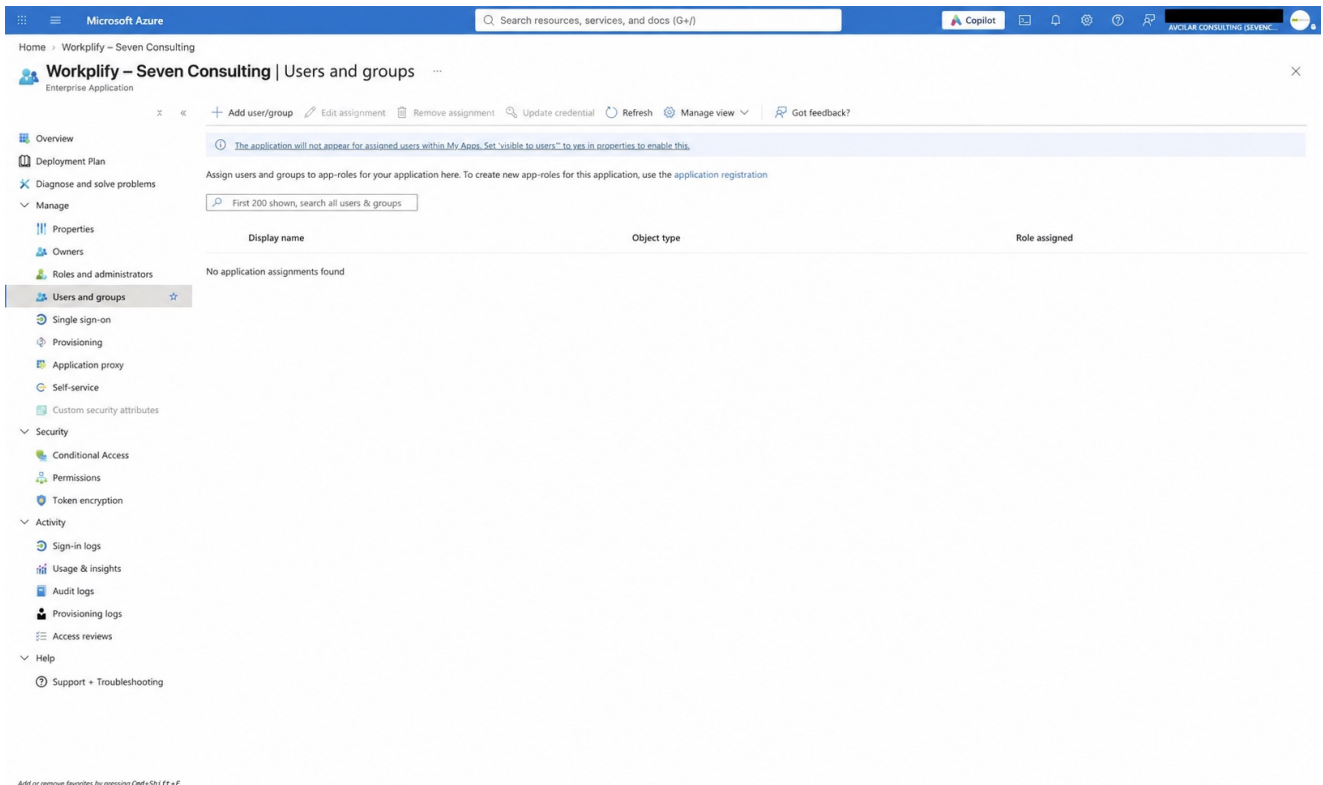
Unter „Admin consent“ sind beide Rechte durch einen Administrator freigegeben. Diese Prüfung erfolgt vor dem Mitarbeiterlogin.
Große Ansicht

Ergebnis: Mitarbeiter bestätigen diese bereits freigegebenen Rechte beim normalen Login nicht einzeln. Anmeldung, MFA und firmeneigene Zugriffsregeln gelten weiterhin. Jede Kundenorganisation erteilt die Freigabe selbst; Herausgeberverifizierung und Katalogeintrag ersetzen diesen Schritt nicht.

03 · Benutzer zuweisen

Mit einem regulären Testkonto starten.

1. **Benutzer und Gruppen (Users and groups)** öffnen.
2. **Benutzer/Gruppe hinzufügen (Add user/group)** wählen, das vorgesehene Testkonto auswählen und mit **Zuweisen (Assign)** bestätigen.
3. Wenn ausschließlich zugewiesene Konten zugreifen sollen, unter **Eigenschaften > Zuweisung erforderlich? (Properties > Assignment required?) Ja** wählen und speichern. Zuerst die benötigten Test- und Administrationskonten zuweisen.



Über „Add user/group“ beginnt die Zuweisung. Die abgebildete Liste zeigt den Ausgangszustand vor der ersten Zuweisung.
Große Ansicht

Die Zuweisung verwaltet den Zugriff in Microsoft. Der Benutzer benötigt zusätzlich ein aktives Konto im richtigen Workplify-Firmenbereich. Falls SCIM eingesetzt wird, erfolgt die Bereitstellung im folgenden Schritt.

04 · Benutzerbereitstellung mit SCIM

Konten aus Microsoft übernehmen.

Die Benutzerbereitstellung wird in einer eigenen Unternehmensanwendung **Workplify - Benutzerbereitstellung** verwaltet. Die Freigabe der Anmelderechte bleibt in der Workplify-Anmeldeanwendung aus Schritt 2.

1. In Workplify **Anbindungen > Microsoft-Anmeldung > Benutzerbereitstellung mit Microsoft (SCIM)** öffnen. Die Verbindung für Ihren Microsoft-Mandanten einrichten und die angezeigte SCIM-Adresse sowie den Einrichtungsschlüssel bereithalten.
2. In Entra **Unternehmensanwendungen > Neue Anwendung > Eigene Anwendung erstellen** wählen. Als Namen **Workplify - Benutzerbereitstellung** eingeben und die Option zur Integration einer anderen, nicht im Katalog aufgeführten Anwendung wählen. Eine vorhandene SCIM-Anwendung weiterverwenden.
3. In dieser Anwendung **Bereitstellung > Neue Konfiguration (Provisioning > New configuration)** öffnen. Bei einer vorhandenen Konfiguration **Connectivity** wählen. Bei der Authentifizierung **Bearer authentication** auswählen. Die Workplify-Adresse in **Tenant URL** und den Einrichtungsschlüssel in **Secret token** eintragen.
4. **Test connection** ausführen und die Konfiguration nach erfolgreichem Test speichern beziehungsweise mit **Create** anlegen.

The screenshot displays the 'Connectivity' configuration page in the Microsoft Entra portal for the application 'Workplify - Benutzerbereitstellung'. The page includes a left-hand navigation pane with options such as Overview, Provision on demand, Manage, Monitor, and Troubleshoot. The main content area shows a configuration form for the 'Connectivity' section. It includes a message about a new version of the provisioning user experience, a 'Test connection' button, and fields for 'Select authentication method' (set to 'Bearer authentication (Active)'), 'Tenant URL' (set to 'https://www.sevenconsulting.de/app/hr-api/scim.php/v2'), and 'Secret token' (masked with a dot). A footer note indicates that favorites can be added or removed by pressing Ctrl+Shift+F.

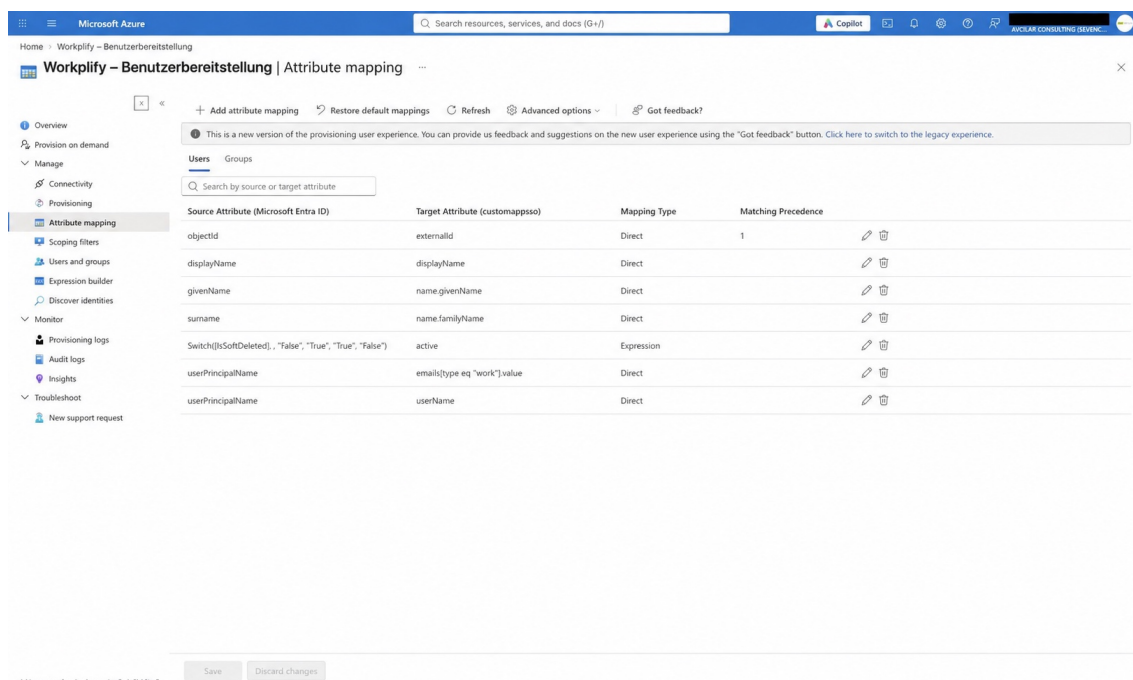
Die Verbindungsadresse und der Schlüssel stammen aus Ihrem geschützten Workplify-Firmenbereich. Der Schlüssel gehört ausschließlich in „Secret token“. [Große Ansicht](#)

04 · SCIM — Attribute und Testlauf

Attribute und Umfang festlegen

Unter **Attribute mappings** die Benutzerbereitstellung einschalten und die Gruppenbereitstellung ausschalten. Nur die folgenden sieben Benutzerattribute übertragen; zusätzliche Standardzuordnungen entfernen.

Microsoft-Attribut	Workplify / SCIM	Einstellung
objectId	externalId	Abgleichpriorität 1
userPrincipalName	userName	Firmen-Anmeldename
Microsoft-Ausdruck zur Deaktivierung	active	Vorhandene Deaktivierungslogik erhalten
displayName	displayName	Anzeigename
userPrincipalName	emails[type eq "work"].value	Geschäftliche Adresse; UPN muss der Firmenadresse entsprechen
givenName	name.givenName	Vorname
surname	name.familyName	Nachname



Die sieben Zuordnungen verbinden die unveränderliche Microsoft-Objekt-ID mit dem Workplify-Konto. Gruppen, Rollen und Personaldokumente werden nicht übertragen. [Große Ansicht](#)

- In den Bereitstellungseinstellungen den Umfang **Nur zugewiesene Benutzer und Gruppen synchronisieren (Sync only assigned users and groups)** wählen. Die Gruppenbereitstellung bleibt dabei ausgeschaltet.
 - Unter **Benutzer und Gruppen** dieser SCIM-Anwendung dasselbe Testkonto zuweisen. Über **Bei Bedarf bereitstellen (Provision on demand)** ausführen und das Ergebnis im Bereitstellungsprotokoll sowie in Workplify prüfen.
 - Nach dem erfolgreichen Anmelde- und Entzugstest den regelmäßigen Bereitstellungslauf einschalten.
- Übertragen werden Benutzerkennung, Name, Firmenadresse und Aktivstatus. Personalunterlagen und Gehaltsdaten gehören nicht dazu. Ein Entzug wirkt nach der nächsten erfolgreichen Synchronisierung.

05 · Anmeldetest

Ohne Einzelzustimmung anmelden.

1. In Workplify das bereitgestellte Testkonto prüfen. Unter **Anbindungen > Microsoft-Anmeldung** die Verbindung prüfen, den lokalen Notfalladmin benennen und **Microsoft-Anmeldung für diese Firma** auf **An** setzen und **Microsoft-Anmeldung einschalten** wählen.
2. Für den Test eine neue Sitzung mit dem regulären Testkonto öffnen. Ein bereits offenes altes Berechtigungsfenster schließen und erneut über den [Workplify-Zugang](#) starten.
3. **Mit Microsoft anmelden** auswählen. Das Firmenkonto verwenden und eine gegebenenfalls geforderte MFA bestätigen. Für die zentral freigegebenen Rechte soll kein Berechtigungsdialog erscheinen.
4. Prüfen, dass anschließend der richtige Workplify-Firmenbereich und die vorgesehenen Benutzerrechte angezeigt werden.
5. Nach dem Einschalten genügt im Workplify-Zugang die Firmen-E-Mail-Adresse und **Weiter**: Workplify leitet zu Microsoft. Reguläre Firmenkonto können sich nicht mehr mit ihrem lokalen Passwort anmelden. Der benannte lokale Notfalladmin bleibt ausgenommen.
6. Bei SCIM die Testzuweisung in der Bereitstellungsanwendung entziehen. Nach erfolgreicher Synchronisierung kontrollieren, dass der Workplify-Zugang deaktiviert ist. Erst nach diesen Prüfungen weitere Mitarbeiter aufnehmen.

The screenshot shows the Workplify login interface. At the top left is the 'workplify' logo with the tagline 'Personal und Onboarding'. At the top right is the text 'Ihr Workplify-Zugang'. The main heading is 'Willkommen bei Workplify.' followed by instructions: 'Hier finden Sie Ihre Aufgaben, Anträge und freigegebenen Unterlagen. Melden Sie sich mit der E-Mail-Adresse an, für die Ihr Unternehmen einen Zugang eingerichtet hat.' Below this is a link: 'Neu bei Workplify? Folgen Sie der Einladung Ihres Unternehmens, um Ihren Zugang zu aktivieren.' The login form is titled 'Anmelden' and asks the user to 'Geben Sie Ihre Firmen-E-Mail-Adresse ein.' It features an 'E-Mail-Adresse' input field, a green 'Weiter →' button, a 'Passwort vergessen?' link, an 'oder' separator, and a 'Mit Microsoft anmelden' button with the Microsoft logo. The footer contains the 'workplify' logo, 'Eine Anwendung von Seven Consulting®', and links for 'Workplify-Support', 'Datenschutz', and 'Impressum'.

Bei Microsoft-Pflicht führen Firmen-E-Mail-Adresse und „Weiter“ direkt zu Microsoft. Alternativ bleibt „Mit Microsoft anmelden“ verfügbar. [Große Ansicht](#)

Hilfe

Die Einrichtung gezielt prüfen.

Berechtigungsdialog beim Mitarbeiter: Die IT vergleicht Anwendungs-ID, Microsoft-Verzeichnis und die Einträge unter „Admin consent“. Benutzerzuweisung allein erteilt keine Zustimmung. Auch neu angeforderte Rechte müssen zentral geprüft werden.

Anmeldung bei Microsoft erfolgreich, Workplify-Zugang fehlt: Firmenzuordnung, aktiven Kontostatus, SCIM-Bereitstellung und Workplify-Anmelderegel kontrollieren.

Erneute Anmeldung: Die Workplify-Sitzung erlaubt 60 Minuten Inaktivität und höchstens zwölf Stunden. Die Bestätigung für Microsoft- und SCIM-Einstellungen gilt innerhalb dieser aktiven Sitzung. Abmeldung, Ablauf oder geänderte Sicherheitsdaten erfordern eine neue Anmeldung.

[Workplify-Support](#) · [Datenschutz](#) · [Nutzungsbedingungen](#)

Für die Unterstützung genügen der betroffene Schritt und die Fehlermeldung. Keine Passwörter, Schlüssel oder Wiederherstellungscodes senden.

Microsoft-Dokumentation: [Zentrale Administratorzustimmung](#) · [Unerwartete Zustimmungsabfragen](#).

Workplify ist noch nicht in diesem Firmenverzeichnis vorhanden

Die IT kann die bestehende mandantenfähige Workplify-App über Microsoft Graph PowerShell hinzufügen. Dazu mit einem berechtigten Administrator im gewünschten Mandanten anmelden. Ersetzen Sie IHRE-MANDANTEN-ID durch die ID Ihres Unternehmens.

```
Connect-MgGraph -TenantId "IHRE-MANDANTEN-ID" -Scopes "Application.ReadWrite.All"  
New-MgServicePrincipal -AppId "207e550a-70f7-46e5-a2e5-3e4cafd0bc2"  
Disconnect-MgGraph
```

Der Verwaltungszugriff gilt für Microsoft Graph PowerShell. Workplify erhält dadurch keine Verzeichnis-Schreibrechte. Anschließend die Liste der Unternehmensanwendungen aktualisieren. Eine vorhandene Anwendung nicht erneut anlegen.

[Microsoft-Anleitung zum Hinzufügen einer bestehenden App](#)