

ADMINISTRATOR KONSOLE > BENUTZERVERWALTUNG >

Microsoft Entra ID SCIM Integration

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/microsoft-entra-id-scim-integration/>

Microsoft Entra ID SCIM Integration

System für Identitätsmanagement über Domänen hinweg (SCIM) kann verwendet werden, um Mitglieder und Gruppen in Ihrer Bitwarden Organisation automatisch bereitzustellen und zu deaktivieren.

Note

SCIM-Integrationen sind verfügbar für **Enterprise-Organisationen**. Teams Organisationen oder Kunden, die keinen SCIM-kompatiblen Identitätsanbieter verwenden, sollten in Betracht ziehen, [Directory Connector](#) als alternative Methode zur Bereitstellung zu verwenden.

Dieser Artikel wird Ihnen helfen, eine SCIM-Integration mit Azure zu konfigurieren. Die Konfiguration beinhaltet die gleichzeitige Arbeit mit dem Bitwarden Web-Tresor und dem Azure Portal. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

SCIM aktivieren

Note

Hosten Sie Bitwarden selbst? Falls ja, führen Sie [diese Schritte zur Aktivierung von SCIM für Ihren Server](#) durch, bevor Sie fortfahren.

Um Ihre SCIM-Integration zu starten, öffnen Sie die Admin-Konsole und navigieren Sie zu **Einstellungen** → **SCIM-Provisioning**:

The screenshot shows the Bitwarden Admin Console interface. On the left is a navigation sidebar with the following items: My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The Settings section is expanded, showing options like Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on, Device approvals, and SCIM provisioning (which is highlighted). The main content area is titled 'SCIM provisioning' and contains the following elements: a sub-header 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning', a checked checkbox for 'Enable SCIM', a text prompt 'Set up your preferred identity provider by configuring the URL and SCIM API Key', a text input field for 'SCIM URL' containing a long alphanumeric string, a text input field for 'SCIM API key' containing a masked string, a warning note 'This API key has access to manage users within your organization. It should be kept secret.', and a blue 'Save' button.

SCIM-Bereitstellung

Wählen Sie das **SCIM aktivieren** Kontrollkästchen aus und machen Sie eine Notiz von Ihrer **SCIM URL** und Ihrem **SCIM API Schlüssel**. Sie müssen beide Werte in einem späteren Schritt verwenden.

Erstellen Sie eine Enterprise-Anwendung



If you are already using this IdP for Login with SSO, open that existing enterprise application and [skip to this step](#). Otherwise, proceed with this section to create a new application

Im Azure Portal navigieren Sie zu **Microsoft Entra ID** und wählen Sie **Enterprise-Anwendungen** aus dem Navigationsmenü:

Home > **Default Directory | Overview** ...
Microsoft Entra ID

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

| | | |
|----------------|--|--------------|
| Name | | Users |
| Tenant ID | | Groups |
| Primary domain | | Applications |
| License | | Devices |

Alerts

- Microsoft Entra Connect v1 Retirement**
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.
[Learn more](#)
- Azure AD is now Microsoft Entra ID**
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
[Learn more](#)

Enterprise applications

Wählen Sie die **+ Neue Anwendung** Schaltfläche:

Home > Enterprise applications

Enterprise applications | All applications ...
Default Directory - Microsoft Entra ID

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.
The list of applications that are maintained by your organization are in [application registrations](#).

Manage

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

Create new application

Auf dem Bildschirm **Microsoft Entra ID** Galerie auswählen, wählen Sie die **+ Erstellen Sie Ihre eigene Anwendung** Schaltfläche:

[+ Create your own application](#) [Got feedback?](#)

The Microsoft Entra ID App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra ID Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#).

Single Sign-on : **All**User Account Management : **All**Categories : **All**[Create your own application](#)

Auf dem Bildschirm "Erstellen Sie Ihre eigene Anwendung" geben Sie der Anwendung einen einzigartigen, Bitwarden-spezifischen Namen. Wählen Sie die **Nicht-Galerie** Option und klicken Sie dann auf den **Erstellen** Knopf.

Create your own application

[Got feedback?](#)

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

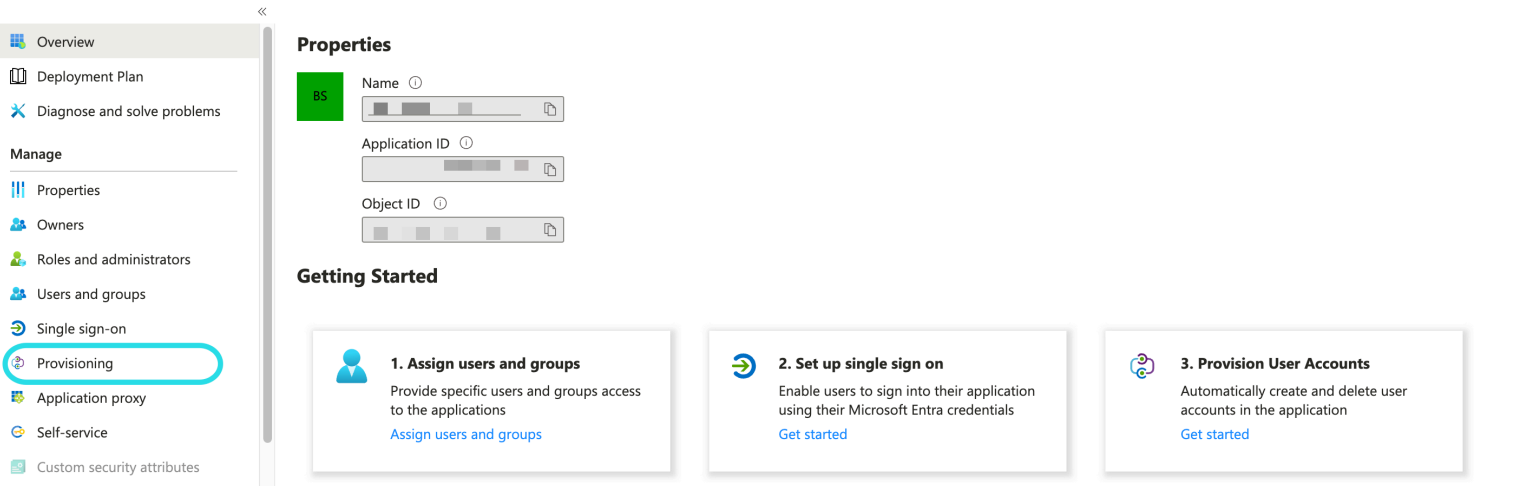
What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

[Create Entra ID app](#)

Provisionierung aktivieren

Wählen Sie **Bereitstellung** aus der Navigation aus und führen Sie die folgenden Schritte aus:



Select Provisioning

1. Wählen Sie die Schaltfläche **Starten**.
2. Wählen Sie **Automatisch** aus dem **Bereitstellungsmodus** Dropdown-Menü.
3. Geben Sie Ihre SCIM-URL ([mehr erfahren](#)) in das Feld **Mieter-URL** ein.
4. Geben Sie Ihren SCIM-API-Schlüssel ([mehr erfahren](#)) in das Feld **Geheimes Token** ein.
5. Wählen Sie die Schaltfläche **Verbindung testen**.
6. Wenn Ihr Verbindungstest erfolgreich ist, wählen Sie die **Speichern** Schaltfläche.

Zuordnungen

Bitwarden verwendet standardmäßige SCIM v2 Attributnamen, obwohl diese sich von den Attributnamen von Microsoft Entra ID unterscheiden können. Die Standardzuordnungen funktionieren, aber Sie können diesen Abschnitt verwenden, um Änderungen vorzunehmen, wenn Sie möchten. Bitwarden wird die folgenden Eigenschaften für Benutzer und Gruppen verwenden:

Benutzermapping

| Bitwarden Attribut | Standard AAD Attribut |
|--|--|
| aktiv | Wechsel([IstSoftGelöscht], , "Falsch", "Wahr", "Wahr", "Falsch") |
| E-Mails ^a oder Benutzername | Post oder userPrincipalName |
| Anzeigename | Anzeigename |

| Bitwarden Attribut | Standard AAD Attribut |
|--------------------|-----------------------|
| ExterneId | E-Mail-Spitzname |

- Da SCIM es Benutzern ermöglicht, mehrere E-Mail-Adressen als ein Array von Objekten auszudrücken, wird Bitwarden den Wert des Objekts verwenden, das "primary": true enthält.

Gruppenzuordnung

| Bitwarden Attribut | Standard AAD Attribut |
|--------------------|-----------------------|
| Anzeigename | Anzeigename |
| Mitglieder | Mitglieder |
| ExterneId | ObjektId |

Einstellungen

Unter dem Dropdown-Menü **Einstellungen** wählen Sie:

- Ob eine E-Mail-Benachrichtigung gesendet werden soll, wenn ein Fehler auftritt, und wenn ja, an welche Adresse sie gesendet werden soll (empfohlen).
- Ob nur **zugewiesene Benutzer und Gruppen synchronisiert** werden sollen oder **alle Benutzer und Gruppen synchronisiert** werden sollen. Wenn Sie sich dafür entscheiden, alle Benutzer und Gruppen zu synchronisieren, überspringen Sie [den nächsten Schritt](#).

Benutzer und Gruppen zuweisen

Führen Sie diesen Schritt aus, wenn Sie ausgewählt haben, nur **zugewiesene Benutzer und Gruppen zu synchronisieren** aus den Bereitstellungseinstellungen. Wählen Sie **Benutzer und Gruppen** aus der Navigation aus:

The screenshot shows the Azure portal interface for the Bitwarden SCIM application. The breadcrumb navigation is: Home > Default Directory > Enterprise applications > Bitwarden SCIM. The page title is "Bitwarden SCIM | Users and groups". On the left, there is a navigation menu with options like Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators, Users and groups (selected), Single sign-on, Provisioning, Application proxy, Self-service, and Custom security attributes (preview). The main content area has a toolbar with "Add user/group", "Edit", "Remove", "Update Credentials", "Columns", and "Got feedback?". Below the toolbar is a blue information banner: "The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →". Underneath is a text box with the placeholder "First 200 shown, to search all users & groups, enter a display name." Below that is a table with columns "Display Name", "Object Type", and "Role assigned". The table content is "No application assignments found".

Enterprise application users and groups

Wählen Sie die Schaltfläche **+ Benutzer/Gruppe hinzufügen**, um den Zugriff auf die SCIM-Anwendung auf Benutzer- oder Gruppenebene zu gewähren. Die folgenden Abschnitte beschreiben, wie Änderungen an Benutzern und Gruppen in Azure ihre Entsprechungen in Bitwarden beeinflussen:

Benutzer

- Wenn einem neuen Benutzer in Azure zugewiesen wird, wird der Benutzer eingeladen, Ihrer Bitwarden Organisation beizutreten.
- Wenn ein Benutzer, der bereits ein Mitglied Ihrer Organisation ist, in Azure zugewiesen wird, wird der Bitwarden-Benutzer über ihren **Benutzername**-Wert mit dem Azure-Benutzer verknüpft.
 - Benutzer, die auf diese Weise verknüpft sind, unterliegen immer noch den anderen Workflows in dieser Liste, jedoch werden Werte wie **displayName** und **externalId/mailNickname** nicht automatisch in Bitwarden geändert.
- Wenn ein zugewiesener Benutzer in Azure gesperrt wird, wird dem Benutzer der Zugang zur Organisation **entzogen**.
- Wenn ein zugewiesener Benutzer in Azure gelöscht wird, wird der Benutzer aus der Organisation entfernt.
- Wenn ein zugewiesener Benutzer aus einer Gruppe in Azure entfernt wird, wird der Benutzer aus dieser Gruppe in Bitwarden entfernt, bleibt aber ein Mitglied der Organisation.

Gruppen

- Wenn in Azure eine neue Gruppe zugewiesen wird, wird die Gruppe in Bitwarden erstellt.
 - Gruppenmitglieder, die bereits Mitglieder Ihrer Bitwarden Organisation sind, werden der Gruppe hinzugefügt.
 - Gruppenmitglieder, die noch nicht Mitglieder Ihrer Bitwarden Organisation sind, werden eingeladen beizutreten.
- Wenn eine Gruppe, die bereits in Ihrer Bitwarden Organisation existiert, in Azure zugewiesen wird, wird die Bitwarden Gruppe über die **displayName** und **externalId/objectId** Werte mit Azure verknüpft.

- Gruppen, die auf diese Weise verknüpft sind, werden ihre Mitglieder aus Azure synchronisieren.
- Wenn eine Gruppe in Azure umbenannt wird, wird sie in Bitwarden aktualisiert, solange die erste Synchronisation durchgeführt wurde.
- Wenn eine Gruppe in Bitwarden umbenannt wird, wird sie wieder auf den Namen zurückgesetzt, den sie in Azure hat. Ändern Sie immer Gruppennamen auf der Azure-Seite.

Beginnen Sie mit der Bereitstellung

Sobald die Anwendung vollständig konfiguriert ist, starten Sie die Bereitstellung, indem Sie die **Bereitstellung starten** Schaltfläche auf der **Bereitstellungs** Seite der Enterprise-Anwendung auswählen:

« **Start provisioning** Stop provisioning Restart provisioning Edit provisioning Provision on demand | Refresh | Got feedback?

Overview

Provision on demand

Manage

Provisioning

Users and groups

Expression builder

Monitor

Provisioning logs

Audit logs

Insights

Troubleshoot

New support request

Current cycle status

Initial cycle not run.

0% complete

[View provisioning logs](#)

Statistics to date

View provisioning details

View technical information

Manage provisioning

[Update credentials](#)

[Edit attribute mappings](#)

[Add scoping filters](#)

[Provision on demand](#)

Start provisioning

Benutzer-Onboarding abschließen

Jetzt, wo Ihre Benutzer bereitgestellt wurden, werden sie Einladungen erhalten, der Organisation beizutreten. Weisen Sie Ihre Benutzer an, die [Einladung anzunehmen](#) und, sobald sie dies getan haben, [bestätigen Sie sie für die Organisation](#).

Note

The Invite → Accept → Confirm workflow facilitates the decryption key handshake that allows users to securely access organization vault data.