

管理者コンソール > ユーザー管理 >

Microsoft Entra ID SCIM統合

ヘルプセンターで表示:

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

Microsoft Entra ID SCIM統合

クロスドメインID管理 (SCIM) システムは、Bitwarden組織内のメンバーやグループを自動的にプロビジョニングおよびデプロビジョニングするために使用できます。

Note

SCIMインテグレーションは、**エンタープライズ組織**で利用可能です。SCIM互換のIDプロバイダーを使用していないチーム組織、または顧客は、プロビジョニングの代替手段としてディレクトリコネクタの使用を検討することがあります。

この記事は、AzureとのSCIM統合を設定するのに役立ちます。設定は、Bitwardenのウェブ保管庫とAzure Portalを同時に操作することを含みます。進行するにあたり、両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

SCIM を有効にする

Note

あなたは自己ホスト型のBitwardenを使用していますか？それなら、進む前にサーバーでSCIMを有効にするためのこれらの手順を完了してください。

SCIM統合を開始するには、管理者コンソールを開き、**設定** → **SCIMプロビジョニング**に移動します。

The screenshot shows the Bitwarden Admin Console interface. On the left is a navigation sidebar with 'Settings' expanded to 'SCIM provisioning'. The main content area is titled 'SCIM provisioning' and contains the following elements:

- Header: 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning'
- Checkbox: 'Enable SCIM' (checked)
- Text: 'Set up your preferred identity provider by configuring the URL and SCIM API Key'
- Form: 'SCIM URL' field with a masked value and a copy icon.
- Form: 'SCIM API key' field with a masked value, an eye icon, a refresh icon, and a copy icon.
- Text: 'This API key has access to manage users within your organization. It should be kept secret.'
- Button: 'Save'

SCIM プロビジョニング

SCIMを有効にするチェックボックスを選択し、SCIM URLとSCIM APIキーをメモしてください。後のステップで両方の値を使用する必要があります。

エンタープライズアプリケーションを作成する



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

Azure Portalで、Microsoft Entra ID に移動し、ナビゲーションメニューからエンタープライズアプリケーションを選択します。

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	[Redacted]	Users
Tenant ID	[Redacted]	Groups
Primary domain	[Redacted]	Applications
License	[Redacted]	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

+ 新しいアプリケーション ボタンを選択してください。

Home > Enterprise applications

Enterprise applications | All applications ...

+ 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

Microsoft Entra IDギャラリー画面で、+ あなた自身のアプリケーションを作成するボタンを選択してください:

[+ 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](#)

あなた自身のアプリケーションを作成する画面で、アプリケーションにはユニークで、Bitwarden特有の名前を付けてください。
ギャラリー以外のオプションを選択し、次に**作成**ボタンを選択してください。

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?

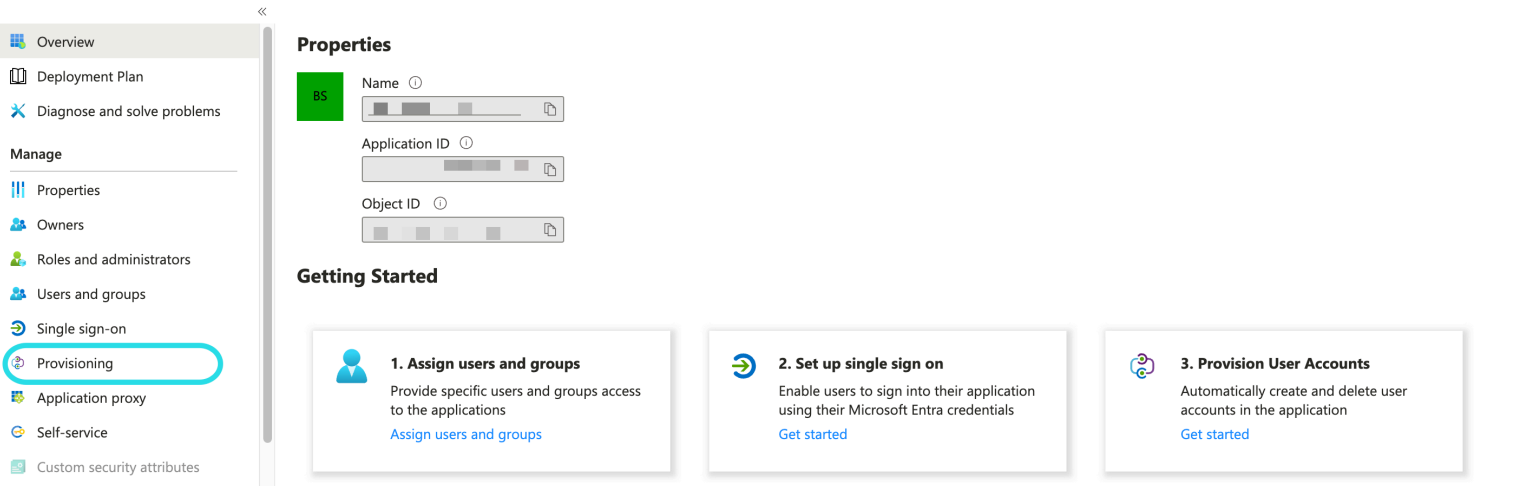
What are you looking to do with your application?

- 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](#)

プロビジョニングを有効にする

ナビゲーションから**プロビジョニング**を選択し、次の手順を完了してください：



Select Provisioning

1. **開始** ボタンを選択してください。
2. **自動** を **プロビジョニングモード** のドロップダウンメニューから選択します。
3. あなたのSCIM URL ([詳細を学ぶ](#)) を **テナントURL** フィールドに入力してください。
4. あなたのSCIM APIキー ([もっと詳しく](#)) を **シークレットトークン** フィールドに入力してください。
5. **接続をテスト** ボタンを選択します。
6. あなたの接続テストが成功した場合、**保存** ボタンを選択してください。

マッピング

Bitwardenは標準的なSCIM v2属性名を使用しますが、これらはMicrosoft Entra ID属性名と異なる場合があります。デフォルトのマッピングは機能しますが、必要に応じてこのセクションを使用して変更を加えることができます。Bitwardenは、ユーザーとグループに以下のプロパティを使用します：

ユーザーマッピング

Bitwarden属性	デフォルトのAAD属性
アクティブ	Switch([IsSoftDeleted], , "False", "True", "True", "False")
メールアドレスまたはユーザー名	メールまたはuserPrincipalName
表示名	表示名

Bitwarden属性	デフォルトのAAD属性
外部ID	メールニックネーム

- SCIMはユーザーがオブジェクトの配列として複数のメールアドレスを持つことを可能にするため、Bitwardenはオブジェクトの値を使用します。そのオブジェクトには"**primary**": trueが含まれています。

グループマッピング

Bitwarden属性	デフォルトのAAD属性
表示名	表示名
メンバーたち	メンバーたち
外部ID	オブジェクトID

設定

設定 ドロップダウンから、選択してください：

- 障害が発生した場合にメール通知を送るかどうか、そして送る場合はどのメールアドレスに送るか（推奨）。
- 割り当てられたユーザーとグループのみを同期するか、すべてのユーザーとグループを同期するか。
すべてのユーザーとグループを同期することを選択した場合、次のステップをスキップしてください。

ユーザーとグループを割り当てる

このステップを完了してください。

あなたがプロビジョニングの設定から割り当てられたユーザーとグループのみを同期するように選択した場合。ナビゲーションからユーザーとグループを選択してください。

Microsoft Azure | Search resources, services, and docs (G+)

Home > Default Directory > Enterprise applications > Bitwarden SCIM

Bitwarden SCIM | Users and groups

Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes (preview)

Actions: Add user/group, Edit, Remove, Update Credentials, Columns, Got feedback?

Info: The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

Search: First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		

Enterprise application users and groups

SCIMアプリケーションへのユーザーまたはグループレベルでのアクセスを割り当てるには、**＋ユーザー/グループを追加** ボタンを選択してください。次のセクションでは、Azureでユーザーとグループを変更すると、それがBitwardenの対応する部分にどのような影響を与えるかについて説明します:

ユーザー

- Azureで新しいユーザーが割り当てられると、そのユーザーはあなたのBitwarden組織に招待されます。
- あなたの組織のメンバーであるユーザーがAzureに割り当てられると、Bitwardenのユーザーはその**ユーザー名**の値を通じてAzureのユーザーにリンクされます。
 - このようにリンクされたユーザーは、このリストの他のワークフローに依然として対象となりますが、**displayName**や**externalId/mailNickname**のような値はBitwardenで自動的に変更されません。
- Azureで指定されたユーザーが停止されると、そのユーザーは組電へのアクセスが**取り消されます**。
- Azureで指定されたユーザーが削除されると、そのユーザーは組織から削除されます。
- Azureのグループから割り当てられたユーザーが削除されると、そのユーザーはBitwardenのそのグループから削除されますが、組織のメンバーとして残ります。

グループ

- Azureで新しいグループが割り当てられると、そのグループはBitwardenで作成されます。
 - あなたのBitwarden組織のメンバーであるグループメンバーは、グループに追加されます。
 - あなたのBitwarden組織のメンバーでないグループメンバーは、参加するために招待されています。
- あなたのBitwarden組織にすでに存在するグループがAzureに割り当てられると、Bitwardenグループは**displayName**および**externalId/objectId**の値を通じてAzureにリンクされます。

- このようにリンクされたグループは、Azureからそのメンバーが同期されます。
- Azureでグループの名前が変更されると、初期の同期が行われている限り、Bitwardenでも更新されます。
 - Bitwardenでグループの名前が変更されると、それはAzureでの名前に戻されます。常にAzure側でグループ名を変更します。

プロビジョニングを開始します

アプリケーションが完全に設定されたら、エンタープライズアプリケーションの▷[プロビジョニングページ](#)で **プロビジョニングを開始** ボタンを選択してプロビジョニングを開始します:

The screenshot shows the Bitwarden provisioning interface. At the top, there is a navigation bar with a back arrow and several action buttons: **Start provisioning** (highlighted with a red circle), Stop provisioning, Restart provisioning, Edit provisioning, Provision on demand, Refresh, and Got feedback?. Below this is a sidebar menu with sections: Overview, Provision on demand, Manage (Provisioning, Users and groups, Expression builder), Monitor (Provisioning logs, Audit logs, Insights), and Troubleshoot (New support request). The main content area is divided into three columns. The first column, 'Current cycle status', shows 'Initial cycle not run.' and a progress bar at '0% complete'. The second column, 'Statistics to date', has expandable options for 'View provisioning details' and 'View technical information'. The third column, 'Manage provisioning', includes links for 'Update credentials', 'Edit attribute mappings', 'Add scoping filters', and 'Provision on demand'. At the bottom of the main content area, there is a 'View provisioning logs' link and a 'Start provisioning' button.

[Start provisioning](#)

ユーザーオンボーディングを完了する

あなたのユーザーが準備されたので、彼らは組織に参加するための招待を受け取ります。ユーザーに招待を受け入れるよう指示し、それが完了したら、[彼らを組織に確認してください](#)。

Note

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