

管理者コンソール > SSOでログイン >

Microsoft Entra ID SAML 実装

ヘルプセンターで表示:

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

Microsoft Entra ID SAML 実装

この記事には、SAML 2.0を介したSSOでのログインを設定するための**Azure特有のヘルプ**が含まれています。別のIdPでSSOを使用したログインの設定についてのヘルプは、[SAML 2.0設定](#)を参照してください。

設定は、Bitwardenウェブアプリと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。

Tip

すでにSSOの専門家ですか？この記事の指示をスキップして、自分の設定と比較するためのサンプル設定のスクリーンショットをダウンロードしてください。

📄 タイプ：アセット-ハイパーリンク ID: 7CKe4TX98FPF86eAimKgak

ウェブアプリでSSOを開く

Bitwardenウェブアプリにログインし、製品スイッチャー (☰) を使用して管理者コンソールを開きます。

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

製品-スイッチャー

あなたの組織の設定 → シングルサインオン画面を開きます：

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

Default Directory - Microsoft Entra ID

Overview: Overview, Diagnose and solve problems

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

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](#).

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ます:

Home > Default Directory | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra ID Gallery

+ 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](#).

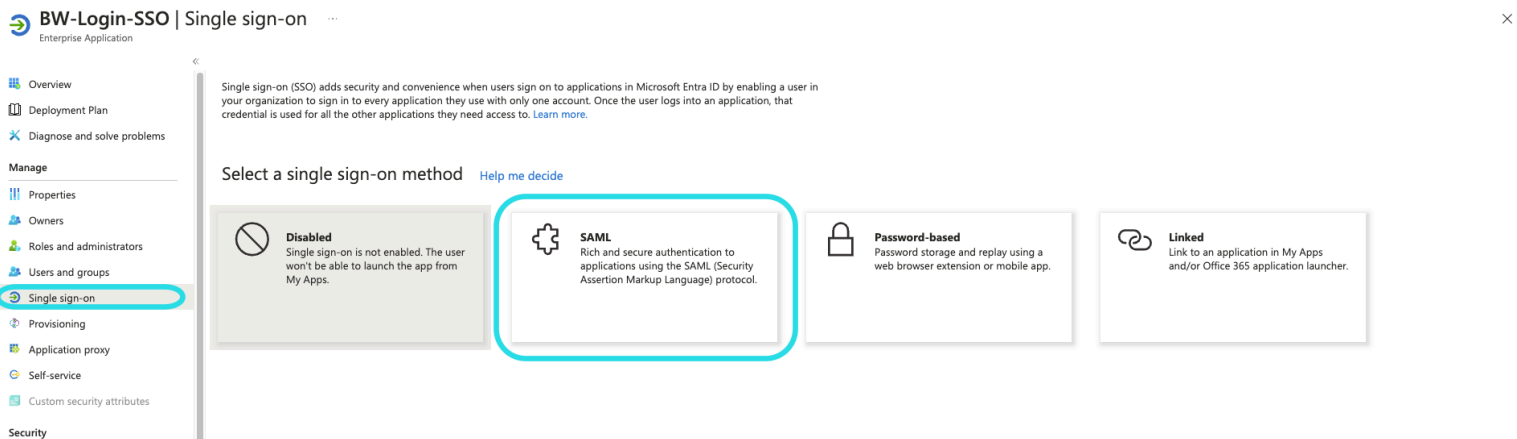
Search application Single Sign-on: All User Account Management: All Categories: All

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ユニークでBitwarden特有の名前を付け、(ギャラリー以外)のオプションを選択してください。終了したら、作成ボタンをクリックしてください。

シングルサインオンを有効にする

アプリケーション概要画面から、ナビゲーションからシングルサインオンを選択してください。



Configure Single sign-on

シングルサインオン画面で、**SAML**を選択してください。

SAML設定

基本的なSAML設定

編集ボタンを選択し、次のフィールドを設定してください：

フィールド	説明
識別子 (エンティティID)	このフィールドを事前に生成された SPエンティティID に設定します。 この自動生成された値は、組織の設定 → シングルサインオン画面からコピーでき、設定により異なります。
返信URL (アサーション消費者サービスURL)	このフィールドを事前に生成された Assertion Consumer Service (ACS) URL に設定します。 この自動生成された値は、組織の設定 → シングルサインオン画面からコピーでき、設定により異なります。
URLにサインイン	このフィールドを、ユーザーがBitwardenにアクセスするためのログインURLに設定してください。 クラウドホストのお客様の場合、これは https://vault.bitwarden.com/#/sso または https://vault.bitwarden.eu/#/sso です。自己ホスト型のインスタンスの場合、これはあなたが設定したサーバーURLによって決まります。例えば、 https://your-domain.com/#/sso などです。

ユーザー属性&クレーム

Azureによって構築されるデフォルトのクレームは、SSOでのログインで動作しますが、必要に応じてこのセクションを使用して、AzureがSAMLレスポンスで使用するNameIDフォーマットを設定することができます。

編集ボタンを選択し、**ユニークユーザー識別子 (名前ID)** エントリを選択してNameIDクレームを編集します：

Attributes & Claims ...

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

NameID 請求の編集

オプションには、デフォルト、メールアドレス、永続的、未指定、およびWindowsの資格付けられたドメイン名が含まれます。詳細については、[Microsoft Azureのドキュメンテーション](#)を参照してください。

SAML署名証明書

後のステップで使用するために、Base64証明書をダウンロードしてください。後のステップで。

あなたのアプリケーションを設定してください。

このセクションのログインURLとMicrosoft Entra ID識別子をコピーまたはメモして、後のステップで使用してください：

4

Set up BW-Login-SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	<input type="text"/>
Microsoft Entra ID Identifier	<input type="text"/>
Logout URL	<input type="text"/>

Azure URLs

Note

If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

ユーザーとグループ

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。

The screenshot shows the Azure portal interface for configuring Bitwarden Login with SSO. The breadcrumb path is: Home > Default Directory > Enterprise applications > Bitwarden Login with SSO. The main heading is "Bitwarden Login with SSO | Users and groups". A left-hand navigation menu includes: Overview, Deployment Plan, Manage (Properties, Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service). The main content area has a toolbar with: Add user/group, Edit, Remove, Update Credentials, Columns, and Got feedback?. A message states: "The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this." Below this is a search bar: "First 100 shown, to search all users & groups, enter a display name." A table with columns "Display Name", "Object Type", and "Role assigned" is shown, containing the text "No application assignments found". A link "Assign users or groups" is at the bottom.

ユーザーまたはグループレベルでSSOアプリケーションへのログイン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。

ウェブアプリに戻る

この時点で、Azure Portalのコンテキスト内で必要なすべてを設定しました。設定を完了するためにBitwardenウェブアプリに戻ってください。

シングルサインオン画面は、設定を2つのセクションに分けています：

- **SAML サービス プロバイダーの構成によって**、SAML リクエストの形式が決まります。
- **SAML IDプロバイダーの設定は**、SAMLのレスポンスで期待する形式を決定します。

サービスプロバイダーの設定

次のフィールドを設定してください:

フィールド	説明
名前ID形式	デフォルトでは、Azureはメールアドレスを使用します。あなたがこの設定を変更した場合、対応する値を選択してください。それ以外の場合は、このフィールドを 未指定 または メールアドレス に設定します。

フィールド	説明
アウトバウンド署名アルゴリズム	BitwardenがSAMLリクエストに署名するために使用するアルゴリズム。
署名行動	SAMLリクエストが署名されるかどうか/いつ署名されるか。
最小入力署名アルゴリズム	デフォルトでは、AzureはRSA SHA-256で署名します。ドロップダウンから rsa-sha256 を選択してください。
署名されたアサーションが欲しい	BitwardenがSAMLアサーションに署名が必要かどうか。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼性のある有効な証明書を使用するときは、このボックスをチェックしてください。自己署名証明書は、適切な信頼チェーンがBitwardenログインのSSO Dockerイメージと一緒に設定されていない限り、失敗する可能性があります。

サービスプロバイダーの設定が完了したら、作業を**保存**してください。

IDプロバイダーの設定

IDプロバイダーの設定では、アプリケーションの値を取得するために、しばしばAzure Portalを参照する必要があります。

フィールド	説明
エンティティID	Azure Portalの アプリケーションの設定 セクションから取得した、あなたの Microsoft Entra ID 識別子を入力してください。このフィールドは大文字と小文字を区別します。
バインディングタイプ	HTTP POST または リダイレクト に設定します。
シングルサインオンサービスURL	Azure Portalの アプリケーションの設定 セクションから取得した ログインURL を入力してください。
シングルログアウトサービスURL	現在、SSOでのログインはSLOを サポートしていません 。 このオプションは将来の開発のために計画されていますが、ご希望であれば ログアウトURL で事前に設定することができます。
X509公開証明書	ダウンロードした 証明書 を貼り付け、削除します -----BEGIN CERTIFICATE----- そして

フィールド	説明
	<p>-----証明書終了-----</p> <p>証明書の値は大文字と小文字を区別し、余分なスペース、キャリッジリターン、その他の余分な文字は証明書の検証に失敗する原因となります。</p>
アウトバウンド署名アルゴリズム	<p>デフォルトでは、AzureはRSA SHA-256で署名します。ドロップダウンから rsa-sha256 を選択してください。</p>
アウトバウンドログアウトリクエストを無効にする	<p>現在、SSOでのログインはSLOをサポートしていません。このオプションは将来の開発のために計画されています。</p>
認証リクエストに署名が必要です	<p>AzureがSAMLリクエストの署名を期待しているかどうか。</p>

① Note

X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、証明書を更新する必要があります。証明書が期限切れになった場合でも、管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

IDプロバイダーの設定が完了したら、**保存**してください。

💡 Tip

シングルサインオン認証ポリシーを有効にすることで、ユーザーにSSOでログインすることを要求することができます。メモしてください、これは単一の組織ポリシーも同時に活性化する必要があります。[もっと学ぶ](#)

設定をテストする

設定が完了したら、<https://vault.bitwarden.com>に移動して、メールアドレスを入力し、**続行**を選択し、**エンタープライズシングルオン**ボタンを選択してテストしてください。



Log in

Master password (required)

⊗ Input is required.

[Get master password hint](#)

[Log in with master password](#)

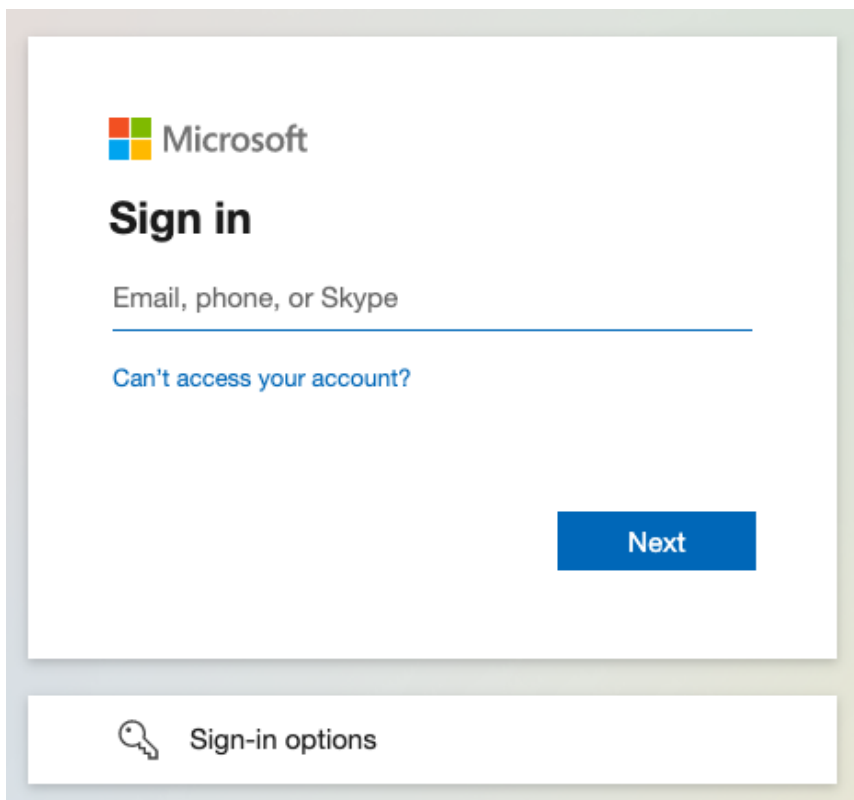
[Enterprise single sign-on](#)

Logging in as myemailaddress@bitwarden.com

[Not you?](#)

エンタープライズシングルサインオンとマスターパスワード

設定された組織識別子を入力し、**ログイン**を選択してください。あなたの実装が正常に設定されている場合、Microsoftのログイン画面にリダイレクトされます。



Azure login screen

あなたのAzureの認証情報で認証した後、Bitwardenのマスターパスワードを入力して保管庫を復号化してください！

① Note

Bitwardenは勝手なレスポンスをサポートしていませんので、あなたのIdPからログインを開始するとエラーが発生します。SSOログインフローはBitwardenから開始されなければなりません。Azure SAML管理者は、ユーザーがBitwardenウェブ保管庫ログインページに誘導されるように[アプリ登録](#)を設定することができます。

1. 既存のBitwardenボタンを無効にするには、**すべてのアプリケーション**ページで現在のBitwardenエンタープライズアプリケーションに移動し、プロパティを選択し、**ユーザーに表示オプション**を**いいえ**に設定します。
2. **アプリ登録**に移動して、**新規登録**を選択することでアプリ登録を作成します。
3. アプリケーションに名前を付けてください。例えば、**Bitwarden SSO**など。リダイレクトURLを指定しないでください。フォーラムを完了するには、**登録**を選択してください。
4. アプリが作成されたら、ナビゲーションメニューにある**ブランディング&プロパティ**に移動します。
5. 次の設定をアプリケーションに追加してください：
 1. エンドユーザーの認識のためにロゴをアップロードしてください。Bitwardenのロゴは[ここ](#)から取得できます。
 2. **ホームページのURL**をあなたのBitwardenクライアントログインページ、例えば<https://vault.bitwarden.com/#/login>またはyour-self-hostedURL.comに設定します。

このプロセスが完了すると、指定されたユーザーはBitwardenアプリケーションを持つことになり、それによりユーザーは直接Bitwardenのウェブ保管庫ログインページにリンクされます。