

管理者コンソール > SSOでログイン > 実装ガイド

Duo SAML 実装

Duo 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**Duo特有のヘルプ**が含まれています。別のIdPのSSOでのログインを設定するためのヘルプは、[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Duo管理者ポータル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

Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

ウェブアプリでSSOを開く



Warning

This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see [Duo's documentation](#) for details.

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。

Password Manager

Vaults

Send

Tools

Reports

Settings

Password Manager

Secrets Manager

Admin Console

Toggle Width

All vaults

FILTERS

Search vaults

All vaults

My vault

My Organiz... :
Teams Org... :
+ New organization

All items

Favorites

Login

Card

Identity

Secure note

Folders

No folder

Collections

Default colle...

Default colle...

Trash

New

BW

All

Name

Owner

Company Credit Card

Visa, *4242

My Organiz...

Personal Login

myusername

Me

Secure Note

Me

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。



My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Organization info

Policies

Two-step login

Import data

Export vault

Domain verification

Single sign-on

Device approvals

SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

☒ Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

☒ Master password

☐ Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

SAML 2.0

SAML service provider configuration

☒ Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

SAML 2.0 metadata URL

SAML 2.0設定

まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成し、**タイプ**のドロップダウンから**SAML**を選択してください。この画面を開いたままにして、簡単に参照できるようにしてください。

この段階で、必要に応じて**ユニークなSPエンティティIDを設定する**オプションをオフにすることができます。これを行うと、組電IDがSPエンティティID値から削除されますが、ほとんどの場合は、このオプションをオンにしておくことをお勧めします。



代替の**メンバー復号化オプション**があります。信頼できるデバイスでのSSOの使い方またはキーコネクターの使い方を学びましょう。

アプリケーションを保護する

続行する前に、[Duoのドキュメンテーション](#)を参照して、Duo Single Sign-OnがあなたのSAML IDプロバイダーと認証のために設定されていることを確認してください。

Duo管理者ポータルで、**アプリケーション画面**に移動し、**アプリケーションを保護する**を選択します。検索バーに**Bitwarden**を入力し、**DuoがホストするBitwarden 二要素認証とSSOアプリケーションの設定**を選択します：

Dashboard
Device Insight
Policies
Applications
Protect an Application
Authentication Proxy
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Trusted Endpoints

Dashboard > Applications > Protect an Application

Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: [Getting Started](#)

Choose an application below to get started.

Application	Protection Type	
Bitwarden	2FA	Documentation Protect
Bitwarden	2FA with SSO hosted by Duo (Single Sign-On)	Documentation Configure

Duo Bitwarden Application

新しく作成されたアプリケーションに対してアクティベートしてセットアップを開始を選択します。

Dashboard
Device Insight
Policies
Applications
Single Sign-On
Duo Central
Passwordless
Users
Groups
Endpoints
2FA Devices

Dashboard > Single Sign-On

Single Sign-On

Simplify access to the applications your users rely on. With Duo's cloud-hosted SSO, protecting your applications while reducing user friction has never been easier. [Learn how it works](#)

Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your [Authentication Proxy server\(s\)](#). Duo caches the AD password and SAML assertions only long enough to complete the authentication. [Learn more](#)

☒ I have read and understand these Duo-hosted SSO updates, the [Privacy Statement](#) and Duo's [Privacy Data Sheet](#)

Activate and Start Setup

Duo Activation and Setup

次の手順と設定をアプリケーション設定画面で完了してください。これらの一部は、Bitwardenシングルサインオン画面から取得する必要があります：

- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On
- Duo Central
- Passwordless
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints

← [Back to Single Sign-On](#)

SAML Identity Provider Configuration

✓ Enabled

Status: Enabled [Disable Source](#)

Configure a SAML Identity Provider to provide primary authentication for Duo Single Sign-On by following the sections below.
[Learn more about configuring the SAML Identity Provider with Duo Single Sign-On](#)

1. Configure the SAML Identity Provider

Provide this information about your Duo Single Sign-On account to your SAML identity provider.

Entity ID

<https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata>

[Copy](#)

Assertion Consumer
Service URL

<https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs>

[Copy](#)

Audience Restriction

<https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata>

[Copy](#)

Metadata URL

<https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata>

[Copy](#)

XML File

[Download Metadata XML](#)

DUO SAML Identity Provider Configuration

メタデータ

メタデータのセクションでは何も編集する必要はありませんが、後でこれらの値を使用する必要があります。

Metadata

Entity ID

<https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/metadata>

[Copy](#)

Single Sign-On URL

<https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/sso>

[Copy](#)

URLs for Configuration

ダウンロード

証明書をダウンロードボタンを選択して、X.509証明書をダウンロードしてください。これは設定の後半で使用する必要があります。

サービスプロバイダー

フィールド

説明

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。

フィールド	説明
アサーションコンシューマーサービス (ACS) 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。
サービスプロバイダーログインURL	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に設定します。 クラウドホストのお客様のために、これは <code>https://vault.bitwarden.com/#/sso</code> または <code>https://vault.bitwarden.eu/#/sso</code>です。自己ホスト型のインスタンスの場合、これはあなたの設定されたサーバーURLによって決定されます。例えば、<code>https://your.domain.com/#/sso</code> などです。

SAMLレスポンス

フィールド	説明
NameID形式	このフィールドを SAML NameID形式 に設定し、DuoがSAMLレスポンスでSendするようにします。
NameID属性	このフィールドを設定し、応答のNameIDを生成するDuo属性にします。
署名アルゴリズム	このフィールドをSAMLアサーションとレスポンスに使用する暗号化アルゴリズムに設定します。
署名オプション	署名応答 を選択するか、 署名主張 を選択するか、または両方を選択してください。
地図の属性	これらのフィールドを使用して、IdP属性をSAMLレスポンス属性にマッピングします。あなたが設定したNameID属性に関係なく、IdPの <code>メールアドレス</code> 属性を <code>メール</code> にマッピングします。以下のスクリーンショットのように：

Map attributes

IdP Attribute

SAML Response Attribute

✖ <Email Address>	Email	+
-------------------	-------	---

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the SAML response attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>. Consult your service provider for more information on their attribute names.

Required Attribute Mapping

これらのフィールドの設定が完了したら、**保存**して変更を保存してください。

ウェブアプリに戻る

この時点で、Duoポータル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、設定を二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フォーマットを決定します。

サービスプロバイダーの設定

次のフィールドを、Duo管理者ポータルで[アプリケーション設定中](#)に選択した選択肢に従って設定してください：

フィールド	説明
名前ID形式	NameID形式 をSAMLリクエストで使用する（ NameIDPolicy ）。このフィールドを 選択されたNameID形式 に設定してください。
アウトバウンド署名アルゴリズム	デフォルトでSAMLリクエストに署名するために使用されるアルゴリズムは、 rsa-sha256 です。
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。デフォルトでは、Duoはリクエストの署名を必要としません。
最小入力署名アルゴリズム	BitwardenがSAMLレスポンスで受け入れる最小の署名アルゴリズム。デフォルトでは、Duoは rsa-sha256 で署名するので、 別のオプションを選択 していない限り、そのオプションをドロップダウンから選択してください。

フィールド	説明
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を求めるかどうか。このボックスをチェックしてください、もしあなたが署名確認の署名オプションを選択した場合。
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 with SSO dockerイメージ内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Duo管理者ポータル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	あなたのDuoアプリケーションのエンティティIDの値を入力してください。これはDuoアプリのメタデータセクションから取得できます。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	このフィールドをHTTP Postに設定してください。
シングルサインオンサービスURL	DuoアプリケーションのシングルサインオンURLの値を入力してください。これはDuoアプリのメタデータセクションから取得できます。
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、あなたのDuoアプリケーションのシングルログアウトURLの値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、削除してください。 <pre>-----BEGIN CERTIFICATE-----</pre> そして <pre>-----証明書の終わり-----</pre> 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認証の検証に失敗する原因となります。

フィールド	説明
アウトバウンド署名アルゴリズム	このフィールドを 選択されたSAMLレスポンス署名アルゴリズム に設定します。
アウトバウンドログアウトリクエストを無効にする	SSOでのログインは現在、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。
認証リクエストに署名が必要です	DuoがSAMLリクエストに署名を期待するかどうか。

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、**続ける**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 to Bitwarden

Email address (required)

☒ Remember email

Continue

or

 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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、あなたはソースIdPのログイン画面にリダイレクトされます。

あなたのIdPログインとDuo二要素で認証した後、Bitwarden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！

Note

Bitwardenは勝手の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。