● bitwarden ヘルプセンターの記事

管理者コンソール > SSOでログイン >

Duo SAML 実装

ヘルプセンターで表示: https://bitwarden.com/help/saml-duo/

U bitwarden

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.

Jownload 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(闘)を使用して管理者コンソールを開きます。

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。

D bit warden	Single sign-on 🖩 🗧
g My Organization $~~ \lor~~$	Use the require single sign-on authentication policy to require all members to log in with SSO.
	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
绺 Groups	SSO identifier (required) unique-organization-identifier
agreen Equation = 1	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
\mathbb{B} Billing \checkmark	Member decryption options
\otimes Settings \land	Master password
Organization info	○ Trusted devices
Policies	Once authenticated, members will decrypt vauit 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.
Two-step login	C Type
Import data	SAML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization
SCIM provisioning	
	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、 組电IDがSPエンティティID値から削除されますが、ほとんどの場合では、このオプションをオンにしておくことをお勧めします。

∂ Tip

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		Dashboard > Applications > Protect an Application			
Device Insight	~	Protect an Application			
Policies Applications 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 Documentation: Getting Started C Choose an application below to get started.	the only one that will see it, until you decide to add others.		
Authentication	Proxy				
Single Sign-On	~	Bitwarden			
Users	~	Application	Protection Type		
Groups	\sim				
Endpoints	\sim	bitwarden Bitwarden	2FA	Documentation 🗗	Protect
2FA Devices	\sim				
Administrators	~	bitwarden Bitwarden	2FA with SSO hosted by Duo (Single Sign-On)	Documentation 🗗	Configure
Trusted Endpoints					

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		Dashboard > Single Sign-On	
Device Insight	\sim	Single Sign-On	
Policies	\sim	Simplify access to the applications your users rely on. With Duo's cloud- hosted SSO, protecting your applications while reducing user friction has	
Applications	\sim	never been easier. Learn how it works ⊡	
Single Sign-On	^	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	
Duo Central		encrypted when passed to your Authentication Proxy server(s) C. Duo caches the AD password and SAML assertions only long enough to complete the authentication. Learn more C.	
Passwordless		✓ I have read and understand these Duo-hosted SSO updates, the Privacy Statement C [*] and Duo's Privacy Data Sheet C [*]	
Users	\sim	Activate and Start Setup	
Groups	\sim		
Endpoints	\sim		
2FA Devices	\sim		
		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		← Back to Single Sign-On SAML Identity		Status: Enabled Disable Source
Device Insight	\checkmark		des te excluide acience estheritientien fer Due Single Sign On hu fellowing the postions below	
Policies	\sim	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 다		
Applications	\sim	1. Configure the SAML Identity Provider		
Single Sign-On	^	Provide this information about y	our Duo Single Sign-On account to your SAML identity provider.	
Duo Central Passwordless		Entity ID	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
Users	\checkmark	Assertion Consumer	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs	Сору
Groups	~	Service URL		
Endpoints	~	Audience Restriction	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
2FA Devices	~	Metadata URL	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Copy
Administrators	\sim			
Trusted Endpoints		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	Сору
Single Sign-On URL	https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/sso	Сору

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
エンティティロ	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。
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。

フィールド	説明
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https://vault.bitwarden.com/#/sso または https://v ault.bitwarden.eu/#/ssoです。自己ホスト型のインスタンスの場合、 これはあなたの設定されたサーバーURLによって決定されます。例えば、https://your.domain.com/#/ ssoなどです。

SAMLレスポンス

フィールド	説明
NamelD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。
NamelD属性	このフィールドを設定し、応答のNamelD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のメールアドレス属性をメール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	
	<pre>« <email address=""></email></pre>	Email]⊕
	Map the values of an IdP attribute to a	nother attribute name to be included in	the SAML response
	(e.g. Username to User.Username). En	ter in an IdP attribute or select one of I	Duo's preconfigured
	attributes that automatically chooses t	he SAML response attribute based on	the IdP. There are five
	preconfigured attributes: <email addre<="" th=""><th>ess>, <username>, <first name="">, <las< th=""><th>st Name> and</th></las<></first></username></th></email>	ess>, <username>, <first name="">, <las< th=""><th>st Name> and</th></las<></first></username>	st Name> and
	<display name="">. Consult your service</display>	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、 <mark>rsa-sha256</mark> 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。
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。

フィールド	説明	
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。 BEGIN CERTIFICATE そして 証明書の終わり 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 。	
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。	
 ONOTE 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!

(i) 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。