

管理者コンソール > SSOでログイン >

ADFS OIDC 実装

ヘルプセンターで表示: https://bitwarden.com/help/adfs-oidc-implementation/

ADFS OIDC 実装

この記事には、OpenID Connect (OIDC) を介したSSOでのログインを設定するためのActive Directory Federation Services (AD FS) 固有のヘルプが含まれています。別のOIDC IdPでのSSOを使用したログインの設定、またはSAML 2.0を介したAD FSの設定のヘルプについては、 OIDC設定またはADFS SAML実装を参照してください。

設定は、BitwardenウェブアプリとAD FSサーバー管理マネージャー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。

ウェブ保管庫でSSOを開く

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

D Password Manager	All vaults			New ~	BW
🗇 Vaults			Nome	Quarter 1	
🖉 Send			Name	Owner	:
$ m \ll$ Tools \sim	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults		Personal Legin		
🕸 Settings 🛛 🗸 🗸	∠ My vault ∅ My Organiz :		myusername	Me	:
	+ New organization		Secure Note	Me	:
	 ✓ All items ☆ Favorites ④ Login ⊡ Card Identity ↓ Secure note 		Shared Login sharedusername	My Organiz	:
 ☐ Password Manager ☐ Secrets Manager Æ Admin Console Ă Toggle Width 	 Folders No folder Collections Default colle Default colle Trash 				

製品-スイッチャー

ナビゲーションから**設定 → シングルサインオン**を選択してください。

D bit warden	Single sign-on 🗰	0
	Use the require single sign-on authentication policy to require all members to log in with SSO.	
Collections 은 Members 略 Groups	 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)	
₩ Reporting	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification	
🗄 Billing 🗸 🗸	Member decryption options	
\otimes Settings \land	Master password	
Organization info Policies	Orrusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, a account recovery administration policy with automatic enrollment will turn on when this option is used.	ind
Two-step login	OpenID Connect	~
Export vault	OpenID connect configuration	
Single sign-on	Callback path	
Device approvals	Cigned out collhook with	
SCIM provisioning		

OIDC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**を作成してください。それ以外の場合、 この画面でまだ何も編集する必要はありませんが、簡単に参照できるように開いたままにしておいてください。



アプリケーショングループを作成する

サーバーマネージャーで、AD FS 管理に移動し、新しいアプリケーショングループを作成します。

1. コンソールツリーで、**アプリケーショングループ**を選択し、アクションリストから**アプリケーショングループを追加**を選択します。

2. ウィザードのウェルカム画面で、**サーバーアプリケーションがWeb APIにアクセス**テンプレートを選択してください。

翰 Add Application Group Wizard

Welcome

 \times

Steps	Name:
Welcome	BitwardenCloud
Server application	Description
 Configure Application Credentials 	
Configure Web API	
Apply Access Control Policy	Template:
 Configure Application Permissions 	Client-Server applications
Summary	Native application accessing a web API
Complete	Server application accessing a web API
	Web browser accessing a web application Standalone applications Image: Native application Image: Server application
	Web API More information

AD FS Add Application Group

3. サーバーアプリケーション画面上で:

🛯 훾 Add Application Group Wizard

ς.	
``	
1	`
•	

Server application		
Steps	Name:	
Welcome	BitwardenCloud - Server application	
Server application	Client Identifier	
 Configure Application Credentials 	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	
Configure Web API	Redirect URI:	
Apply Access Control Policy	Example: https://Contoso.com	Add
 Configure Application Permissions 	https://sso.bitwarden.com/oidc-signin	Remove
Summary		
Complete		
	Description:	
	< Previous Next >	Cancel

AD FS Server Application screen

- サーバーアプリケーションに**名前**を付けてください。
- クライアント識別子をメモしてください。この値は次のステップで必要になります。
- リダイレクトURIを指定してください。クラウドホストのお客様の場合、これはhttps://sso.bitwarden.com/oidc-signinまたはhtt ps://sso.bitwarden.eu/oidc-signinです。自己ホスト型のインスタンスの場合、 これは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/oidc-signinのような形式です。

4. アプリケーション資格情報の設定画面で、クライアントシークレットをメモしてください。この値は次のステップで必要になります。

5. Web API設定画面で:

翰 Add Application Group Wi	zard	×
Configure Web API		'n
Steps Velcome	Name: BitwardenCloud - Web API	
 Server application Configure Application Credentials 	Identifier: Example: https://Contoso.com	Add
 Configure Web API Apply Access Control Policy Configure Application Permissions 	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d https://sso.bitwarden.com/	Remove
 Summary Complete 	Description:	
	< Previous Next >	Cancel

AD FS Configure Web API screen

- Web APIに**名前**を付けてください。
- クライアント識別子とリダイレクトURIを識別子リストに追加してください(ステップ2B.& C.を参照)。

6.「アクセス制御ポリシーの適用」画面で、アプリケーショングループに適切なアクセス制御ポリシーを設定します。

7. アプリケーション権限の設定画面で、スコープallatclaimsとopenidを許可します。

Madd Application Group W	izard Permissions	×
Steps • Welcome • Server application • Configure Application Credentials • Configure Web API • Apply Access Control Policy • Configure Application	Configure permissions to enable client applications to access this Web API. Client application (caller): Name Description BitwardenCloud - Server application	
 Permissions Summary Complete 	Add	Remove
	Scope Name Description Image: allatclaims Requests the access token claims in the identity token. Image: aza Scope allows broker client to request primary refresh token. Image: email Request the email claim for the signed in user. Image: logon_cert The logon_cert scope allows an application to request logo Image: openid Request use of the OpenID Connect authorization protocol. Image: profile Request profile related claims for the signed in user. Image: user_imperso Request permission for the application to access the resour Image: vpn cert The vpn cert scope allows an application to request VPN	New scope
	< Previous Next >	Cancel

AD FS Configure Application Permissions screen

8. アプリケーショングループウィザードを完了します。

変換クレームルールを追加します

サーバーマネージャーで、AD FS 管理に移動し、作成されたアプリケーショングループを編集します:

1. コンソールツリーで、**アプリケーショングループ**を選択します。

2. アプリケーショングループリストで、作成したアプリケーショングループを右クリックし、プロパティを選択します。

3. アプリケーションセクションで、Web APIを選択し、編集... を選択します。

4. 発行変換ルールタブに移動し、ルールを追加...ボタンを選択します。

5. ルールタイプ選択画面で、LDAP属性をクレームとしてSendするを選択します。

6. 「クレームルール設定」画面で:

🏟 Add Transform Claim Rule	Wizard			×
Configure Rule				
Steps Choose Rule Type Configure Claim Rule	You ca to extra from the Claim ru email Rule te Attribute Mappin	n configure this rule to send the values of L ct LDAP attributes. Specify how the attribut a rule. Ile name: mplate: Send LDAP Attributes as Claims e store: Directory g of LDAP attributes to outgoing claim type: LDAP Attribute (Select or type to add more) E-Mail-Addresses ~	DAP attributes as claims. Select an attribute sto tes will map to the outgoing claim types that will ss: Outgoing Claim Type (Select or type to add n E-Mail Address 2	nore)
			< Previous Finish	Cancel

AD FS Configure Claim Rule screen

- ルールには**請求ルール名**を付けてください。
- LDAP属性ドロップダウンから、E-Mail-Addresses.を選択してください。
- 送信クレームタイプのドロップダウンから、**Eメールアドレス**を選択してください。

7. 選択 **完了。**

ウェブアプリに戻る

この時点で、AD FSサーバー管理者のコンテスト内で必要なすべてを設定しました。次のフィールドを設定するために、 Bitwardenウェブアプリに戻ってください:

フィールド	説明
権限	あなたのAD FSサーバーのホスト名を入力し、/adfs を追加してください。例えば、 https://adfs.mybusiness.com/adfsのようになります。
クライアントID	取得したクライアントIDを入力してください。
クライアントシークレット	取得したクライアントシークレットを入力してください。
メタデータアドレス	指定された 権限 の値に/.well-known/openid-configuration を追加して入力してください。例えば、https://adfs.mybusiness.com/adfs/. well-known/openid-configurationのようになります。
OIDCリダイレクトの振る舞い	リダイレクト GET を選択します。
ユーザー情報エンドポイントから請求を取得する	このオプションを有効にすると、URLが長すぎるエラー(HTTP 414) 、 切り捨てられたURL、および/またはSSO中の失敗が発生した場合に対応します。
カスタムスコープ	リクエストに追加するカスタムスコープを定義します(カンマ区切り)。
顧客ユーザーID請求タイプ	ユーザー識別のためのカスタムクレームタイプキーを定義します(カンマ区切り)。 定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。
メールアドレス請求タイプ	ユーザーのメールアドレスのためのカスタムクレームタイプキーを定義します (カンマ区切り)。定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。
カスタム名前請求タイプ	ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します (カンマ区切り)。定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。
顧客ユーザーID請求タイプ メールアドレス請求タイプ カスタム名前請求タイプ	ユーザー識別のためのカスタムクレームタイプキーを定義します(カンマ区切り)。 定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。 ユーザーのメールアドレスのためのカスタムクレームタイプキーを定義します (カンマ区切り)。定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。 ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します (カンマ区切り)。定義された場合、カスタムクレームタイプキーを定義します (カンマ区切り)。定義された場合、カスタムクレームのタイプは、 標準のタイプに戻る前に検索されます。

フィールド	説明
要求された認証コンテキストクラス参照値	認証コンテキストクラス参照識別子(<mark>acr_values</mark>)(スペース区切り) を定義してください。リスト <mark>acr_values</mark> を優先順位で並べてください。
応答で期待される "acr" 請求値	Bitwardenがレスポンスで期待し、検証するための <mark>acr</mark> クレーム値を定義してください。
これらのフィールド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
– Maste	er password (required)
	©
⊗ Input is	a required.
Get ma	ister password hint
	Log in with master password
_	

設定された組織ID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、AD FS SSOログイン画面にリダイレクトされます。AD FSの資格情報で認証した後、 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!

(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。