

Auth0 社

- 概要 (1ページ)
- ・はじめに (1ページ)

概要

ここでは、Security Cloud Sign On と統合する Auth0 SAML アプリケーションを作成する方法に ついて説明します。

はじめに

始める前に

- ・管理者権限でAuth0管理コンソールにサインインできる必要があります。
- ステップ1:エンタープライズの作成とステップ2:電子メールドメインの申請と検証が 完了している必要があります。

ステップ1 Auth0 ダッシュボードにサインインし、次の手順を実行します。

- a) [アプリケーション (Applications)]メニューから[アプリケーション (Applications)]を選択します。
- b) [アプリケーションの作成 (Create Application)]をクリックします。
- c) [名前 (Name)]フィールドに「Secure Cloud Sign On」または他の名前を入力します。
- d) アプリケーションタイプとして[通常のWebアプリケーション (Regular Web Applications)]を選択し、 [作成 (Create)]をクリックします。
- e) [アドオン (Addons)] タブをクリックします。
- f) [SAML2 Web App (SAML2 Web App)] トグルをクリックしてアドオンを有効にします。

SAML2 Web App の構成ダイアログが開きます。

Addon: SAML	2 Web App	×
	Settings Usage	
SAML Protocol	Configuration Parameters	
 SAML Version: 2. 	0	
Issuer: urn:dev-	.us.auth0.com	
Identity Provider	Certificate: Download Auth0 certificate	e
Identity Provider	SHA1 fingerprint:	
82:87:E5:ED:3D:	67:D3:46:97:8E:72:27:E7:FD:09:FF:BD):FA:A2:94
Identity Provider	Login URL: https://dev-	
q2xwaipwfp2liro8	.us.auth0.com/samlp/A62Y6'	JYYWL
 Identity Provider 	Metadata: Download	
行元(Issuer)] フィー, ドの値をコピーします。	レドと [IDプロバイダーログインURL	(Identity Provider Login URI
th0証明書のダウンロー	・ド(Download Auth0 certificate)] をク	リックして ID プロバイダ・

- **ステップ2** エンタープライズ設定ウィザードの [IDプロバイダーの統合(Integrate Identity Provider)] 画面を開き、次の手順を実行します。
 - a) [IDプロバイダー名 (Identity Provider Name)]フィールドに IdP の名前 (例: Auth0 SSO) を入力しま す。
 - b) [シングルサインオンサービスURL (Single Sign On Service URL)]フィールドに、SAMLアドオンダイ アログからコピーした [IDプロバイダーログインURL (Identity Provider Login URL)]の値を入力しま す。
 - c) [エンティティID (Entity ID)]フィールドに、SAML アドオンダイアログからコピーした[発行元 (Issuer)]フィールドの値を入力します。
 - d) [ファイルの追加(Add File)]をクリックし、AuthOからダウンロードした SAML 署名証明書を選択します。
 - e) 必要に応じて、Duo ベースの無料の MFA サービスからユーザーをオプトアウトします。

ダウンロードします。

f)

g)

Integrate Identity Provider		
1 Set Up 2 D	ownload 3 C	onfigure (4) Activate
Set Up		
Identity Provider (IdP) Name	Auth0 SSO	
Single Sign-On Service URL 🕧	https://dev-q2xwaipwfp2liro8.u	us.auth0.cor
Entity ID (Audience URI) 🚯	urn:dev-q2xwaipwfp2liro8.us.a	uth0.com
SAML Signing Certificate 🌒	Auth0 SSO.pem File must be in PEM format	Add
By default, SecureX Sign-On enrolls all users into recommend MFA, with a session timeout no greate Security products.	Duo MultiFactor Authentication (MFA) at no r than 2 hours, to help protect your sensiti	o cost. We strongly ive data within Cisco
Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On?	• Yes 💿 No	
[次へ(Next)] をクリックして [ダウ	ウンロード(Download)] 計	設定ページに進みます。
後で使用するために [シングルサイ: ティID(Entity ID)] の値をコピーし	ンオンサービスURL(Singl 、SAML署名証明書(cisc	le Sign-On Service URL)] と [エンテー co-securex.pem)をダウンロードします
Set Up 2 Downloa	ad ③ Configure	4 Activate

-		
Download		
Depending on your provider, use the followin	g information to set up your Identity Pro	ovider (IdP).
Single Sign-On Service URL (ACS URL)	https://sso-preview.test.se	P _B
Entity ID (Audience URI)	https://www.okta.com/saml	E.
SAML Signing Certificate	cisco-securex.pem	Download
SecureX Sign-On SAML Metadata	cisco-securex-saml- metadata.xml	Download

h) [次へ (Next)] をクリックして [構成 (Configure)] 画面に進みます。

ステップ3 Auth0 コンソールのアドオン設定ダイアログに戻ります。

- a) [設定 (Settings)] タブをクリックします。
- b) [アプリケーションコールバックURL(Application Callback URL)]フィールドに、エンタープライズ設 定ウィザードからコピーした[シングルサインオンサービスURL(Single Sign-On Service URL)]の値を 入力します。

- c) 必要に応じて、[デバッグ(Debug)]をクリックしてサンプル SAML 応答の構造と内容を確認します (応答をデバッグするには、Auth0 ユーザーを SAML アプリケーションに割り当てる必要がありま す)。
- d) [設定 (Settings)] フィールドに次の JSON オブジェクトを入力します。<ENTITY_ID_URI>を、前にコ ピーした [エンティティID (オーディエンスURI) (Entity ID (Audience URI))]の値に置き換え、
 <SIGNING_CERT>を、ダウンロードした SecureX Sign On 署名証明書 (PEM ファイル)を1行の文字列に 変換した内容に置き換えます。

```
{
  "audience": "https://www.okta.com/saml2/...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
    },
    "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
    "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
    ],
    "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```

	Settings Usage
Applicat	tion Callback URL
https:	//sso-preview.test.security.cisco.com/sso/saml2/0oa 0h8
SAML TO	oken will be POSTed to this URL.
Sattinaa	
settings	
2	\$ {
2 3	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "aigningCost": "</pre>
2 3 4	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { </pre>
2 3 4 5	<pre>s { audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email" } } </pre>
2 3 4 5 6 7	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given name": "firstName".</pre>
2 3 4 5 6 7 8	<pre>{ audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName"</pre>
2 3 4 5 6 7 8 9	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName" }, </pre>
2 3 4 5 6 7 8 9 10	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName" }, "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nam </pre>
2 3 4 5 6 7 8 9 10 11	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName" }, "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nam "nameIdentifierProbes": [</pre>
2 3 4 5 6 7 8 9 10 11 12	<pre>{ audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName" }, "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nam "nameIdentifierProbes": ["http://schemas.xmlsoap.org/ws/2005/05/identity/claims " } </pre>
2 3 4 5 6 7 8 9 10 11 12 13	<pre>{ { "audience": "https://www.okta.com/saml2/service-provider "signingCert": "BEGIN CERTIFICATE\nMIIfjc\n "mappings": { "email": "email", "given_name": "firstName", "family_name": "lastName" }, "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nam "nameIdentifierProbes": ["http://schemas.xmlsoap.org/ws/2005/05/identity/claims], . } } </pre>

e) ダイアログの下部にある[有効化(Enable)]をクリックしてSAMLアプリケーションを有効にします。

ステップ4 エンタープライズ設定ウィザードの[構成 (Configure)] 画面に戻ります。

- a) 表示された URL をコピーし、プライベート(シークレット)ブラウザウィンドウで開きます。 ブラウザが Autho SSO ページにリダイレクトされます。
- b) 申請したドメインと一致する電子メールアドレスで Auth0 にサインインします。 SecureX アプリケーションポータルに戻れば、テストは成功です。
- c) 設定ウィザードで[次へ (Next)]をクリックして[アクティブ化 (Activate)] 画面に進みます。
- d) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化(Activate my IdP)]をクリックします。
- e) ダイアログで選択内容を確認します。

I

etting			
	IdP Activation	×	
	Once the IdP integration is activated:		
vide	 Users sign in using their enterprise IdP password Users no longer manage their MFA settings (if you opted out of Duo MFA during setup). 		
	Cancel		Activ

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。