

Okta 識別プロバイダとのコンタクトセンター SSO

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[識別サービスプロバイダーとして設定 Okta](#)

[識別サービスを設定して下さい](#)

[単一サインオンのための設定を促進して下さい](#)

[参考資料](#)

概要

この資料は識別サービス (ID) および Okta クラウドによって基づく単一サインのための識別プロバイダ (IdP) の設定を説明したものです (SSO) 。

製品 導入

UCCX 共存

PCCE CUIC (Cisco Unified Intelligence Center) と LD (ライブ データ) の共存

UCCE 2k 導入用の CUIC と LD の共存。

UCCE 4k および 12k 導入用のスタンドアロン。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise (UCCE) 、
または Packaged Contact Center Enterprise (PCCE)
- セキュリティ アサーション マークアップ言語 (SAML) 2.0
- Okta

使用するコンポーネント

- UCCE 11.6
- Okta 注: この資料はスクリーン ショットおよび例で設定が Cisco 識別サービス (UCCX/UCCE/PCCE) および IdP に関して類似したであるどんなに、UCCE を参照します。

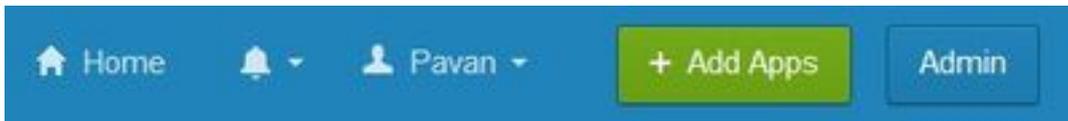
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ

さい。

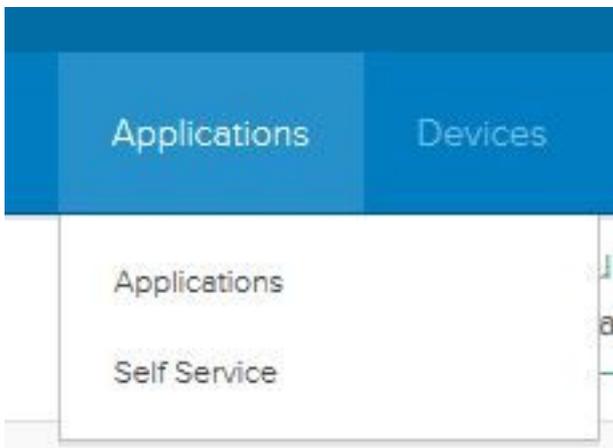
識別サービス プロバイダーで Okta を設定して下さい

ステップ 1. 識別サービス (ID) Web ページへのログインおよび設定への移動はメタデータ ファイルを『Download』 をクリック することクリックしておよびメタデータ ファイルをダウンロードします。

ステップ 2. Okta サーバへのログインは Admin タブを選択し。



ステップ 3 Okta ダッシュボードから、> **アプリケーション** 『Applications』 を選択 して下さい。

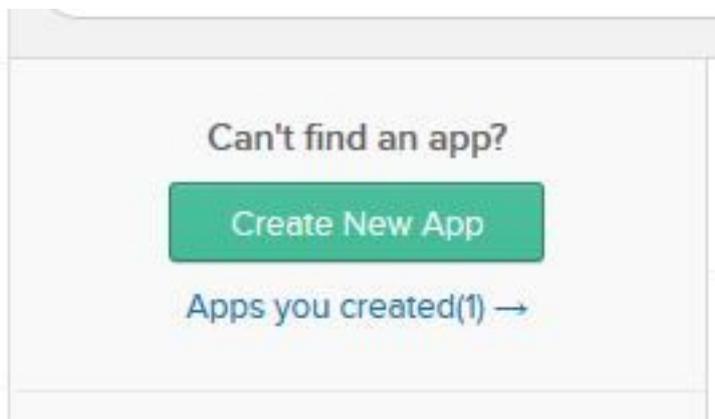


ステップ 4. ウィザードを使用して新しいカスタム アプリケーションを作成するために**新しいアプリケーション**を『Create』 をクリック して下さい。

Applications



ステップ 5 作成で新しいアプリケーション統合ウィンドウ、なぜならプラットフォームは方式のサインとしてドロップダウン リストおよび選定された **SAML 2.0 の Web** を選択し、『Create』 を選択 します。



ステップ 6.アプリケーション名前を入力し、『Next』 をクリックして下さい。

1 General Settings

App name

App logo (optional) 

App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

ステップ 7 SAML 統合で、SAML ページを入力します詳細を作成して下さい。

- URL の単一 サイン-メタデータ ファイルから、AssertionConsumerService のインデックス 0 として規定される URL を入力して下さい。

```
<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cuicpub-ids.pavdave.xyz:8553/ids/saml/response" index="0" isDefault="true"/>
```

- 受信者 URL および宛先 URL のためにこれを使用して下さい-受信者および宛先 URL の一致を有効にするためにこのオプションをチェックして下さい
- このアプリケーションが他の SSO URL を要求するようにして下さい-配備で複数の ID ノードがあったら ID パブリッシャのほかの他の SSO URL からの要求を許可したいと思うためにチェックすればこのオプションを。
 - Requestable SSO URL —このフィールドは上のチェックボックスをチェックするときだけ現われます。他のノードのための SSO URL を入力することができます。

AssertionConsumerService すべての (ACS) アドレスを捜すことによって HTTP-POST バインディングを使用するメタデータ ファイルの ACS URL を検索できます。このフィールドのためのそれらの詳細を追加して下さい。 multiple URL を追加するために追加を別のボタン クリックして下さい。

- 聴衆 URI (SP エンティティ ID) は-メタデータ ファイルからの...、 entityID アドレスを入力します。

```
<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cuicpub-ids.pavdave.xyz">
```

- デフォルト RelayState -このフィールドは空白を残して下さい。
- 挙げて下さい ID 形式-ドロップダウン リストからトランジェントを選択して下さい。
- アプリケーション ユーザー名-統一された CCE Administration で設定されるユーザー名と > 管理する > エージェント一致するユーザー名形式を選択して下さい。



注: このスクリーン ショット

トは UCCE/PCCE に特定です。

ステップ 8.必須 属性文を追加して下さい。

- uid -アプリケーションに送信 されるクレームの認証済みユーザを識別します
- user_principal - Cisco 識別サービスに送信 されるアサーションのユーザの認証レームを識別します

を探します。

GENERAL

Single sign on URL [?]

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Requestable SSO URLs

URL	Index	
<input type="text" value="https://cuicpub-ids.pavdave.xyz:8553/ids/saml/respon"/>	<input type="text" value="0"/>	<input type="button" value="X"/>
<input type="text" value="https://cuicsub-ids.pavdave.xyz:8553/ids/saml/respon:"/>	<input type="text" value="1"/>	<input type="button" value="X"/>

Audience URI (SP Entity ID) [?]

Default RelayState [?]

If no value is set, a blank RelayState is sent

Name ID format [?]

Application username [?]

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="user_principal"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>	<input type="button" value="X"/>
<input type="text" value="uid"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.login"/>	<input type="button" value="X"/>

ステップ 9. 『Next』 を選択して下さい。

ステップ 10. 「**ですソフトウェアベンダー**選択して下さい。 **アプリケーションを Okta と**」統合、 『Finish』 をクリックすることを望みます。

ステップ 11: **サイン ON タブ**ダウンロード**識別プロバイダ** **メタデータ**。

ステップ 12: ダウンロードされたメタデータ ファイルを開き、次に NameIDFormat の 2 つの行を変更し、ファイルを保存して下さい。

```
<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cuicpub-ids.pavdave.xyz">
```

識別サービスを設定して下さい

ステップ 1.識別サービス サーバへの移動。

ステップ 2. 『Settings』 をクリックして下さい。

ステップ 3. 『Next』 をクリックして下さい。

ステップ 4. Okta からダウンロードされるメタデータ ファイルをアップロードし、『Next』 をクリックして下さい。

ステップ 5. **SSO 設定**を 『Test』 をクリックして下さい。New ウィンドウはログインを Okta に認証するためにプロンプト表示します。正常なログインは **SSO 設定**のチェックマークが画面のより低い右隅で完全にテストされることを示します。



注: Okta に既に認証されていればログインに再度プロンプト表示されませんが、ID が資格情報を確認する間、ために簡潔なポップアップを参照して下さい。

この時点で識別サービスおよび識別プロバイダの設定は完了した、ノード稼働中を見るはずですよ。

A screenshot of the Cisco Identity Service Management (ISM) interface. The top left shows the Cisco logo and "Identity Service Management". The main heading is "Nodes". Below it, a table lists two nodes. The first node, "cuicpub-ids.pavdave.xyz", is marked as the primary node with a star. Both nodes are in "In Service" status and have a SAML Certificate Expiry of "01-18-2020 13:13 (841 days left)". A sidebar on the left contains icons for Nodes, Settings, and Clients.

Node	Status	SAML Certificate Expiry
cuicpub-ids.pavdave.xyz ★	In Service	01-18-2020 13:13 (841 days left)
cuicsub-ids.pavdave.xyz	In Service	01-18-2020 13:13 (841 days left)

単一サインオンのためのそれ以上の設定

識別の後で保守すれば識別プロバイダは設定されます、次のステップは UCCE または UCCX のための単一サインオンを設定することです。

- [UCCE/PCCE](#)
- [UCCX](#)

参考資料

- [UCCE/PCCE 単一サインオン](#)
- [UCCX 単一サインオン](#)

- [Cisco Unified Communications Manager \(CUCM \) - Okta 識別プロバイダーの構成](#)