Contact Center SSO mit Okta Identity Provider

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration von Identity Service (IDS) und Identity Provider (IdP) für Okta Cloud-basierte Single Sign On (SSO).

Produkt	Bereitstellung
UCCX	Co-Resident
PCCE	Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)
UCCE	Resident gemeinsam mit CUIC und LD für 2.000 Bereitstellungen. Standalone für 4.000- und 12.000-Bereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit den folgenden Themen vertraut zu machen:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) oder Packaged Contact Center Enterprise (PCCE)
- Security Assertion Markup Language (SAML) 2.0
- Okta

Verwendete Komponenten

- UCCE 11,6
- Okta **Hinweis**: In diesem Dokument wird auf UCCE in den Screenshots und Beispielen verwiesen. Die Konfiguration ähnelt jedoch in Bezug auf den Cisco Identity Service (UCCX/UCCE/PCCE) und die IdP.

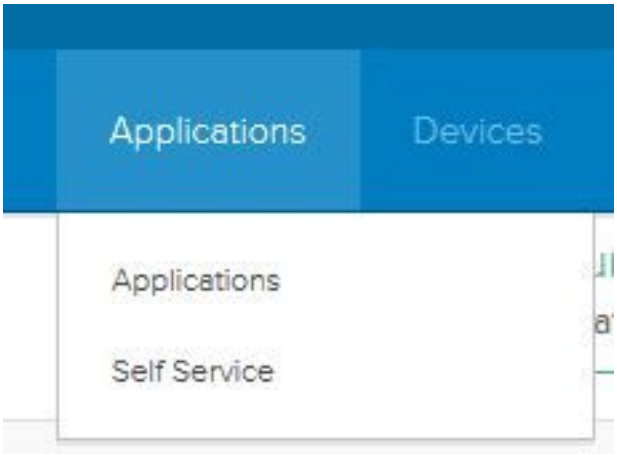
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren von Okta als Identity Service Provider

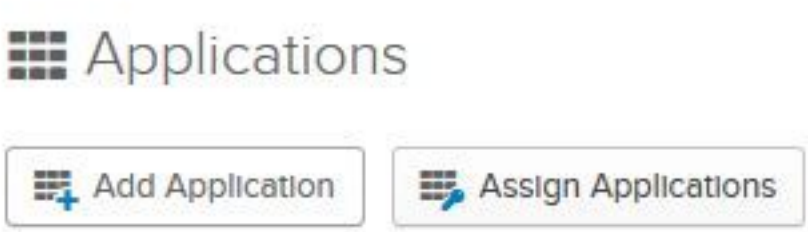
Schritt 1: Melden Sie sich auf der Webseite des Identitätsdienstes (IDs) an, navigieren Sie zu **Einstellungen** und laden Sie die Metadatendatei herunter, indem Sie auf **Metadatendatei herunterladen klicken.**

Schritt 2: Melden Sie sich beim Okta-Server an, und wählen Sie die Registerkarte **Admin aus**.

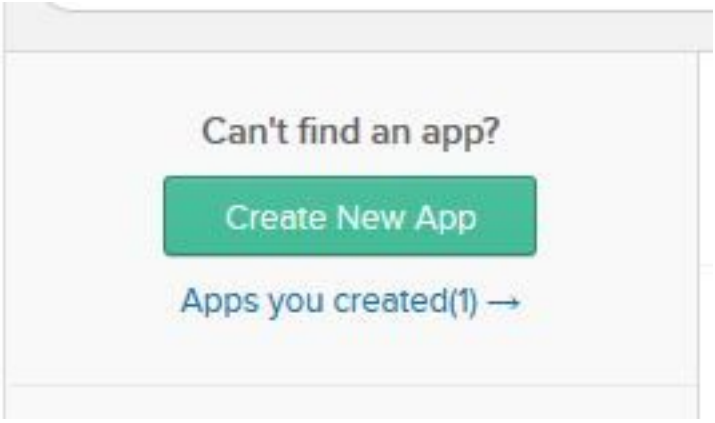
Schritt 3: Wählen Sie im Okta-Dashboard **Anwendungen > Anwendungen aus.**



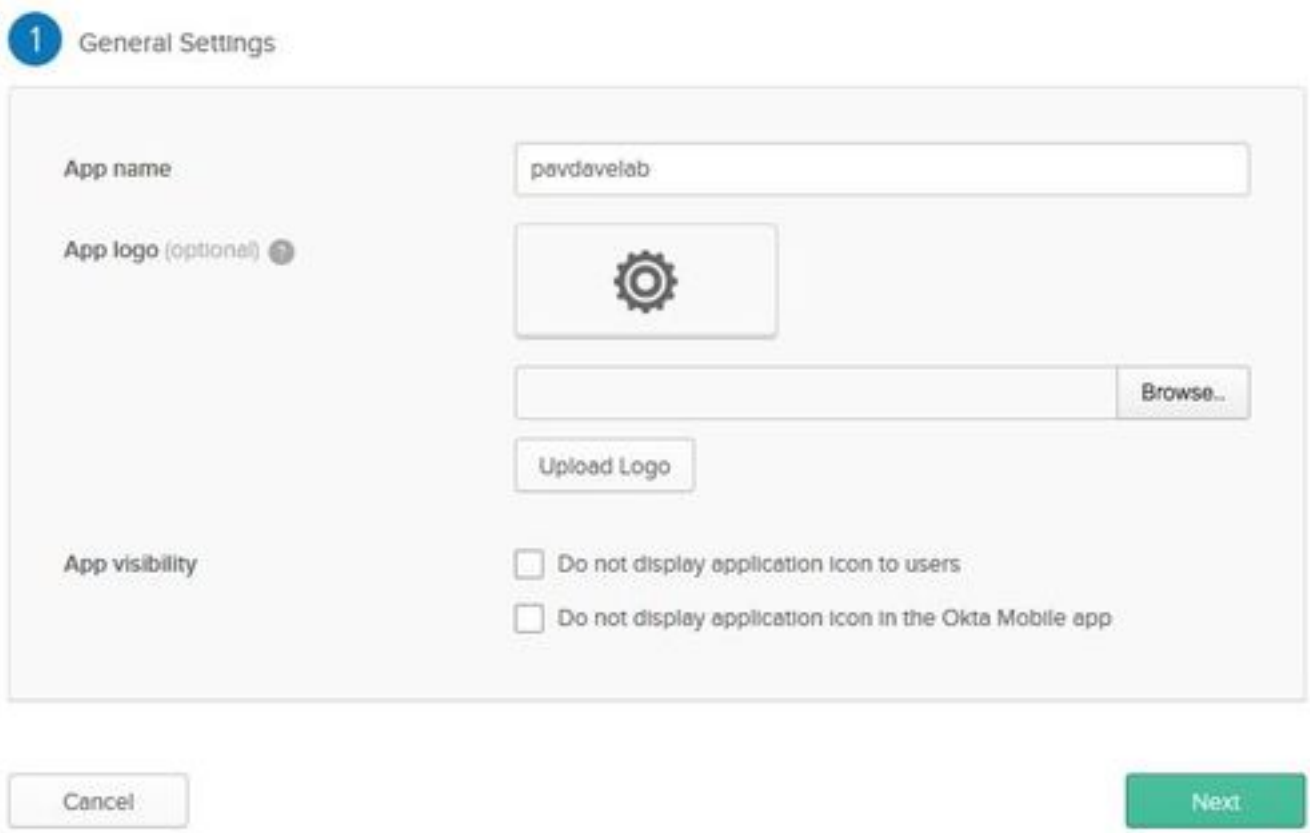
Schritt 4: Klicken Sie auf **Neue App erstellen**, um mithilfe des Assistenten eine neue benutzerdefinierte Anwendung zu erstellen.



Schritt 5: Wählen Sie im Fenster Create a New Application Integration (Neue Anwendungsintegration erstellen) für Platform **Web** in der Dropdown-Liste aus, und wählen Sie **SAML 2.0** als Anmeldungsmethode aus, und wählen Sie Create (Erstellen) aus.



Schritt 6: Geben Sie den Namen der App ein, und klicken Sie auf **Weiter**.



Schritt 7: Geben Sie auf der Seite SAML Integration (SAML-Integration erstellen) die Details ein.

- **URL für einmalige Anmeldung**: Geben Sie in der Metadatendatei den URL ein, der als Index 0 von AssertionConsumerService angegeben ist.

```
<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"/>
```

- **Für Empfänger-URL und Ziel-URL verwenden** - Aktivieren Sie diese Option, um die Zuordnung der Empfänger- und Ziel-URLs zu aktivieren.
- **Lassen Sie zu, dass diese App andere SSO-URLs anfordert**: Aktivieren Sie diese Option, wenn in der Bereitstellung mehrere IDs vorhanden sind und Anforderungen von anderen SSO-URLs neben dem IdS-Publisher zugelassen werden sollen.
    - **Anforderbare SSO-URLs** - Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen oben aktivieren. Sie können SSO-URLs für Ihre anderen Knoten

eingeben. Sie können die ACS-URLs in der Metadatendatei finden, indem Sie nach allen AssertionConsumerService (ACS)-Adressen suchen, die die HTTP-POST-Bindung verwenden. Fügen Sie diese Details für dieses Feld hinzu. Klicken Sie auf die Schaltfläche Add Another (Weiteres hinzufügen), um mehrere URLs hinzuzufügen.

- **Audience URI (SP Entity ID)** - Geben Sie in der Metadatendatei die **entityID-**Adresse ein.

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

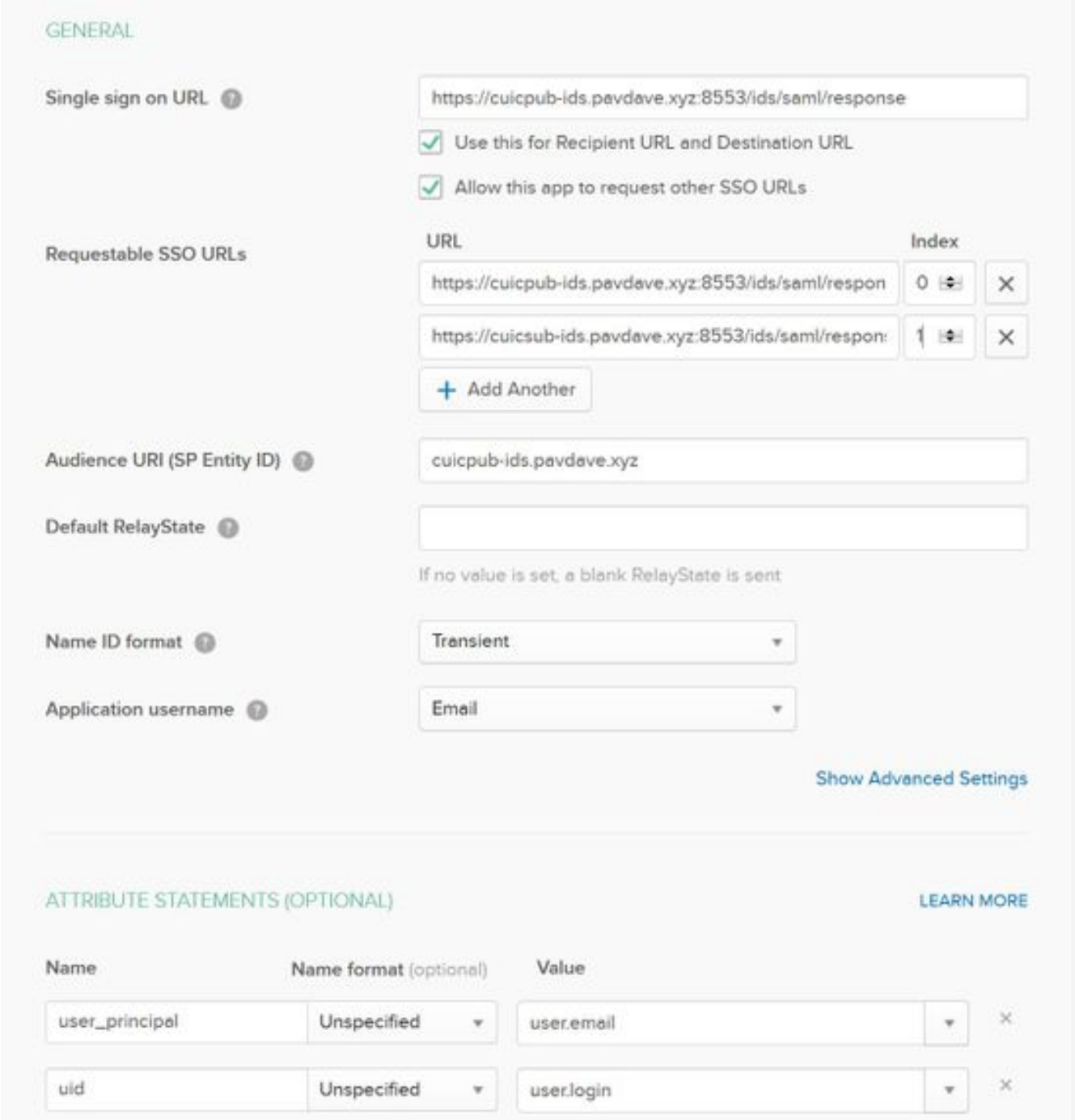
- **Standard-RelayState**: Lassen Sie dieses Feld leer.
- **Name-ID-Format:** Wählen Sie in der Dropdown-Liste die Option **Übergangsfunktion** aus.
- **Anwendungsbenutzername** - Wählen Sie das Format des Benutzernamens aus, der dem in **Unified CCE Administration > Manage > Agents** konfigurierten **Benutzernamen** entspricht.

Hinweis: Dieser Screenshot bezieht sich auf UCCE/PCCE.

Schritt 8: Fügen Sie die erforderlichen Attributanweisungen hinzu.

- **uid**: Identifiziert den authentifizierten Benutzer in dem an die Anwendungen gesendeten Antrag.
- **user_main**: Gibt den Authentifizierungsbereich des Benutzers in der an den Cisco Identity Service gesendeten Assertion an.

.



Schritt 9: Wählen Sie **Weiter aus.**

Schritt 10: Wählen Sie "**Ich bin Softwareanbieter. Ich möchte meine App mit Okta integrieren**" und auf Fertig stellen klicken.

Schritt 11: Laden Sie auf der Registerkarte **Anmelden** die **Metadaten** des **Identitätsanbieters herunter.**

Schritt 12: Öffnen Sie die heruntergeladene Metadatendatei, ändern Sie die beiden Zeilen NameIDFormat in die folgende Zeile, und speichern Sie die Datei.

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

Konfigurieren des Identitätsdienstes

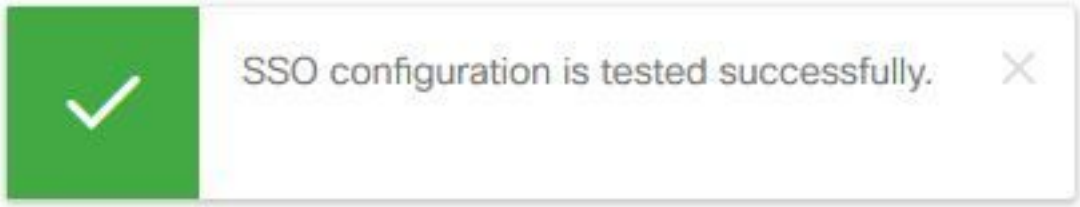
Schritt 1: Navigieren Sie zu Ihrem Identity Service-Server.

Schritt 2: Klicken Sie auf **Einstellungen.**

Schritt 3: Klicken Sie auf **Weiter.**

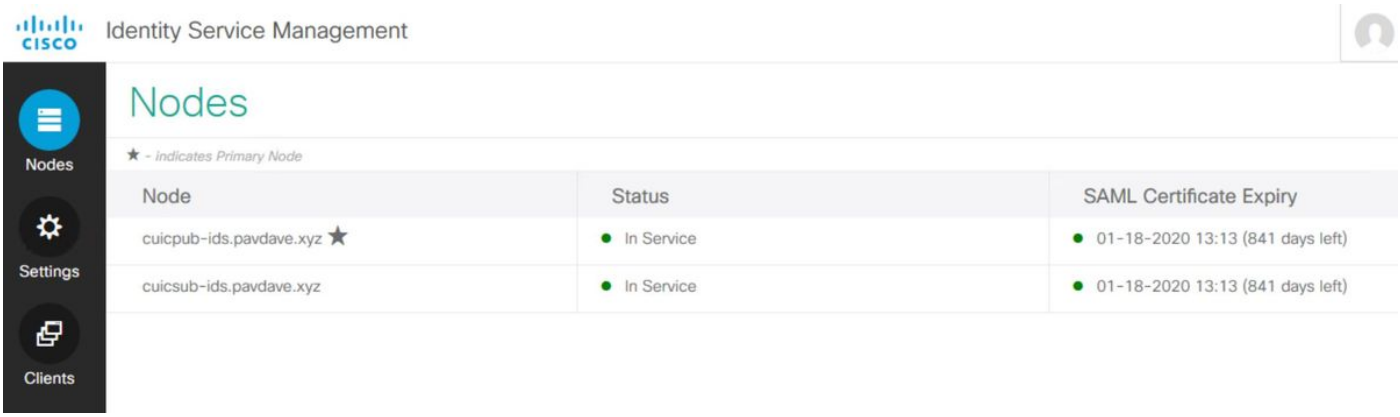
Schritt 4: Laden Sie Metadatendatei aus Okta herunter und klicken Sie auf **Weiter**.

Schritt 5: Klicken Sie auf **Test SSO Setup**. Ein neues Fenster fordert Sie auf, sich anzumelden, um sich bei Okta zu authentifizieren. Bei einer erfolgreichen Anmeldung wird unten rechts im Bildschirm ein Häkchen mit **der erfolgreichen Testphase** der **SSO-Konfiguration angezeigt**.



> **Hinweis**: Wenn Sie bereits auf Okta authentifiziert sind, werden Sie nicht aufgefordert, sich erneut anzumelden, sondern ein kurzes Popup-Fenster mit einer Überprüfung der Anmeldeinformationen durch die IDs angezeigt.

An diesem Punkt ist die Konfiguration des Identitätsdienstes und der Identitätsanbieter abgeschlossen und sollte die Knoten im Dienst sehen.



Weitere Konfiguration für einmalige Anmeldung

Nach der Konfiguration des Identitätsdiensts und Identitätsanbieters besteht der nächste Schritt in der Einrichtung einer einmaligen Anmeldung für UCCE oder UCCX.

- UCCE/PCCE
- UCCX

Weitere Informationen

- Einmalige Anmeldung für UCCE/PCCE
- UCCX Single Sign-On

- Cisco Unified Communications Manager (CUCM) - Konfiguration des Okta Identity Providers