

SSO per contact center con provider di identità Okta

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configura Okta come provider di servizi di identità](#)

[Configurare il servizio di identità](#)

[Ulteriore configurazione per Single Sign-On](#)

[Ulteriori letture](#)

Introduzione

In questo documento viene descritta la configurazione di Identity Service (IdS) e Identity Provider (IdP) per Single Sign-On (SSO) basato su cloud Okta.

Prodotto Implementazione

UCCX Coresidente

PCCE Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data)

UCCE Coresidenti con CUIC e LD per installazioni 2k.

Standalone per installazioni a 4k e 12k.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

- UCCE 11.6
- Okta **Nota:** Questo documento fa riferimento all'UCCE nelle schermate e negli esempi, ma la configurazione è simile per quanto riguarda Cisco Identity Service (UCCX/UCCE/PCCE) e l'IdP.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

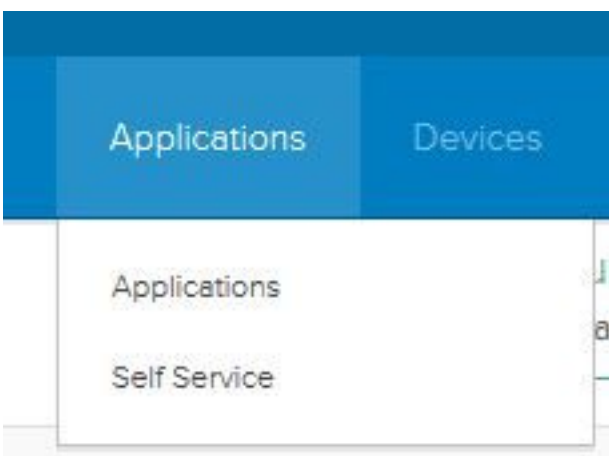
Configura Okta come provider di servizi di identità

Passaggio 1. Accedere alla pagina Web Identity Service (IdS) e selezionare **Settings** e scaricare il file di metadati facendo clic su **Download Metadata File**.

Passaggio 2. Accedere al server Okta e selezionare la scheda **Admin**.



Passaggio 3. Dal pannello di controllo Okta, selezionare **Applicazioni** > **Applicazioni**.

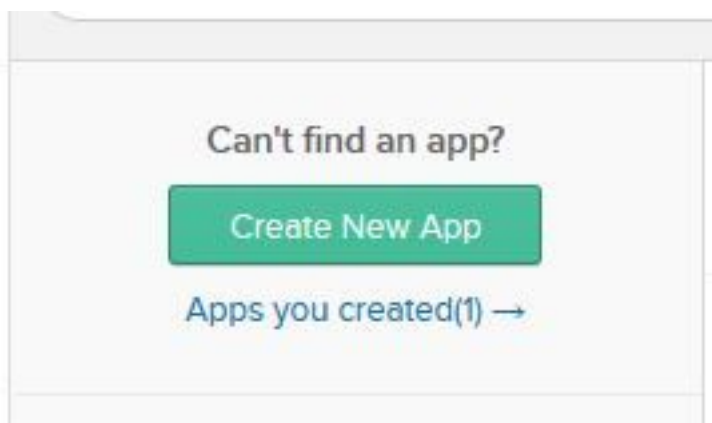


Passaggio 4. Fare clic su **Crea nuova app** per creare una nuova applicazione personalizzata utilizzando la procedura guidata.

Applications




Passaggio 5. Nella finestra Crea nuova integrazione applicazione, per Piattaforma selezionare **Web** nell'elenco a discesa e selezionare **SAML 2.0** come metodo di accesso, quindi selezionare **Crea**.



Passaggio 6. Immettere il nome dell'app e fare clic su **Avanti**.

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

Passaggio 7. Nella pagina Integrazione SAML, Crea SAML, immettere i dettagli.

- **URL Single Sign-On:** dal file di metadati, immettere l'URL specificato in come indice 0 di AssertionConsumerService.

```
<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"/>
```

- **Usa per URL destinatario e URL destinazione** - Selezionare questa opzione per abilitare la corrispondenza degli URL di destinazione e destinatario
- **Consenti all'app di richiedere altri URL SSO:** selezionare questa opzione se nella distribuzione sono presenti più nodi IdS e si desidera consentire le richieste da altri URL SSO oltre a IdS Publisher.
 - **URL SSO richiesti:** questo campo viene visualizzato solo se si seleziona la casella di controllo precedente. È possibile immettere URL SSO per gli altri nodi. Per trovare gli

URL ACS nel file di metadati, cercare tutti gli indirizzi AssertionConsumerService (ACS) che utilizzano l'associazione HTTP-POST. Aggiungere i dettagli per questo campo. Fare clic sul pulsante Add Another per aggiungere più URL.

- **URI gruppo di destinatari (ID entità SP)** - Dal file di metadati, immettere l'indirizzo **entityID**.

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

- **RelayState predefinito:** lasciare vuoto questo campo.
- **Formato ID nome:** scegliere **Transitorio** dall'elenco a discesa.
- **Nome utente applicazione:** scegliere il formato del nome utente corrispondente al **nome utente** configurato in **Amministrazione CCE unificata > Gestisci > Agenti**.



Nota: Questa schermata è

specificata di UCCE/PCCE.

Passaggio 8. Aggiungere le istruzioni attributo richieste.

- **uid** - Identifica l'utente autenticato nell'attestazione inviata alle applicazioni
- **user_principal**: identifica il realm di autenticazione dell'utente nell'asserzione inviata a Cisco Identity Service

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"/>

Passaggio 9. Selezionare **Avanti**.

Passaggio 10. Selezionare **"Sono un fornitore di software. Vorrei integrare la mia app con Okta"** e fare clic su **Fine**.

Passaggio 11. Nella scheda **Sign On** scaricare i **metadati** del **provider di identità**.

Passaggio 12. Aprire il file di metadati scaricato e modificare le due righe di **NameIDFormat** come indicato di seguito e salvare il file.

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

Configurare il servizio di identità

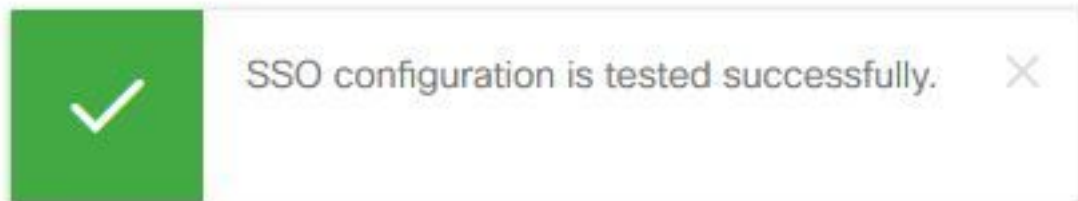
Passaggio 1. Passare al server del servizio di identità.

Passaggio 2. Fare clic su **Impostazioni**.

Passaggio 3. Fare clic su **Avanti**.



Passaggio 4. Caricare il file di metadati scaricato da Okta e fare clic su **Next** (Avanti).

Passaggio 5. Fare clic su **Test SSO Setup**. Una nuova finestra richiederà un accesso per l'autenticazione a Okta. Se l'accesso viene eseguito correttamente, verrà visualizzato un segno di spunta con la **configurazione SSO testata correttamente** nell'angolo inferiore destro della schermata.



Nota: Se si è già autenticati per Okta, non verrà richiesto di eseguire nuovamente l'accesso, ma verrà visualizzato un breve popup durante la verifica delle credenziali da parte dell'IdS.

A questo punto la configurazione dei provider di identità e dei servizi di identità è completa e i nodi dovrebbero essere visualizzati in servizio.

 Identity Service Management 

Nodes ★ - Indicates Primary Node

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)

Navigation sidebar: Nodes, Settings, Clients

Ulteriore configurazione per Single Sign-On

Dopo aver configurato Identity Service e Identity Provider, il passaggio successivo consiste nell'impostare Single Sign-On per UCCE o UCCX.

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

Ulteriori letture

- [UCCE/PCCE Single Sign-On](#)
- [UCCX Single Sign-On](#)

- [Cisco Unified Communications Manager \(CUCM\) - Configurazione provider di identità Okta](#)