

# Configurazione di SSO su CCX e delle soluzioni per contact center principali con Okta IDP

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione su IDS/Cisco Side](#)

[Configurazione su OKTA IDP Side](#)

[Verifica](#)

---

## Introduzione

Questo documento descrive la configurazione di Single Sign On (SSO) con OKTA per diverse soluzioni Cisco On Prem Contact Center.

## 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)
- Security Assertion Markup Language
- OKTA

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Unified contact center express (UCCX) 15.0
- OKTA

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.

## Configurazione su IDS/Cisco Side

1. Eseguire il comando `ids set_property IS_IdP_OKTA true` sulla CLI e riavviare il servizio Identity Service (IDS).
2. Se High Availability (HA), eseguire questo comando su entrambi i nodi e riavviare il servizio IDS.
3. Accedere all'interfaccia di amministrazione di UCCX Cisco IDS `https://<UCCX server address>:8553/idsadmin` sul nodo PUB.
4. Passare a Impostazioni > Protezione > Chiavi e certificati.
5. Rigenerare il certificato SAML (Security Assertion Markup Language).

The screenshot shows the 'Settings' page of the Cisco IDS Administration console. The 'Security' tab is selected. On the left sidebar, 'Keys and Certificates' is highlighted. The main content area is titled 'Generate Keys and SAML Certificate'. It contains two sections: 'Encryption/Signature key' with a 'Regenerate' button, and 'SAML Certificate' with a dropdown menu set to 'SHA-256' and another 'Regenerate' button. Below the SAML Certificate section, there is a note: 'Ensure that the selected algorithm type is same as in IdP. Perform the metadata exchange after the certificate is regenerated and ensure that the SSO Test is successful.'

6. Dalla scheda IDS Trust, scaricare SAML SP metadata XML.

## Settings

IdS Trust Security Troubleshooting



SP Entity ID	Description	Metadata file
[REDACTED]	SAML SP to configure IdS access via LAN/WAN	<a href="#">Download</a>

Note : This operation can be performed only on the primary node.

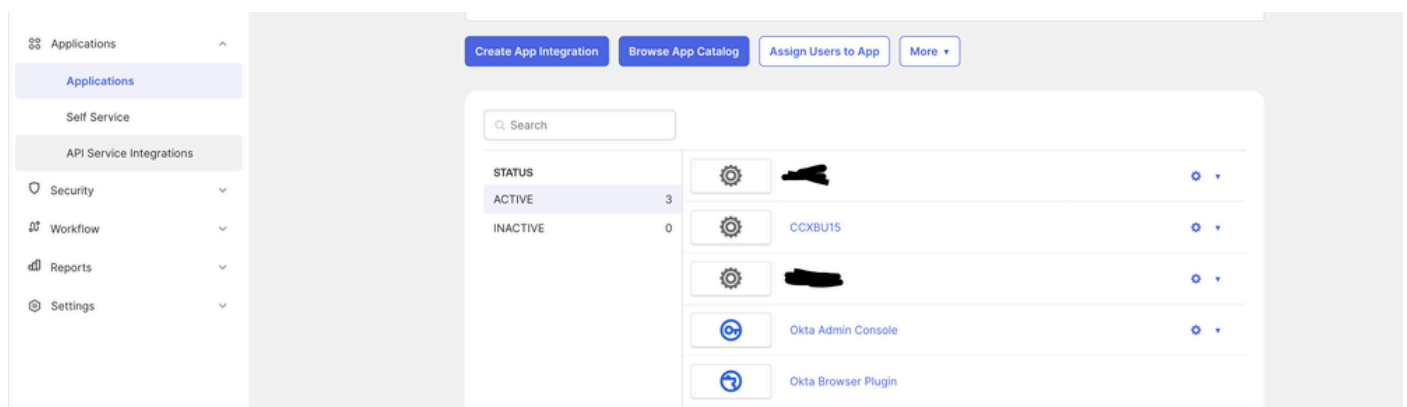
7. Aprire il file XML dei metadati del provider di servizi (SP) e prendere nota del valore dell'attributo 'Location' per gli ID del server di pubblicazione e del sottoscrittore all'interno del tag 'AssertionConsumerService'. L'oggetto AssertionConsumerServiceURL nei metadati SAML include ora metaAlias come parte dell'URL di risposta SAML anziché il parametro di query per PUB.

8. Per il Sottoscrittore, viene visualizzato con il parametro query e può essere ignorato.

```
</KeyDescriptor>
<NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[REDACTED]:8553/ids/saml/response/metaAlias/sp?index=0" isDefault="true" />
<md:AssertionConsumerService xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[REDACTED]:8553/ids/saml/response?metaAlias=/sp?index=1" isDefault="false" />
</SPSSODescriptor>
```

## Configurazione su OKTA IDP Side

1. In Applicazioni, fare clic su Crea integrazione applicazione.



2. Scegliere l'opzione SAML2.0.

## Create a new app integration

✕

Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

3. Sull'URL SSO dell'impostazione SAML, fornire l'URL SSO del PUB copiato nel passaggio 7. in 'Configurazione su IDS/Cisco Side' in questo documento. Nell'URI (Uniform Resource Identifier) del gruppo di destinatari (ID entità SP) incollare l'entità SP nella scheda di attendibilità IDS delle impostazioni di gestione del servizio di identità.

This  
for  
Wh  
nee  
The  
sho  
usin  
doc  
info  
forr

## General

Single sign-on URL ?

[REDACTED]8553/ids/saml/respr

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

[REDACTED]

Default RelayState ?

[REDACTED]

If no value is set, a blank RelayState is sent

Name ID format ?

Transient ▼

Application username ?

Email ▼

Update application username on

Create and update ▼

[Hide Advanced Settings](#)

Response ?

Signed ▼

Assertion Signature ?

Signed ▼

Signature Algorithm ?

RSA-SHA256 ▼

Digest Algorithm ?

SHA256 ▼

Assertion Encryption ?

Unencrypted ▼

4. In 'Altri URL SSO richiesti', immettere l'URL di SUB

<https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp> nel formato specificato con il valore di indice 1.

Other Requestable SSO URLs

URL

Index

+ Add Another


5. Fare clic su Avanti e Fine per completare la configurazione dell'applicazione.

6. Copiare i metadati dalla scheda Accedi utilizzando l'URL e salvarli in formato xml.

7. Caricare i metadati dal passaggio 6. nella pagina Web Identity Service Management sul lato CCX.

Download Metadata    Upload IdP Metadata    Test SSO Setup


IdP Entity Id : REDACTED



**Upload IdP Metadata**

*Use file browser to upload the file.*

Establish the trust relationship between the Identity Provider (IdP) and the Identity Server (IdS) by obtaining a trust metadata file from the IdP and uploading it here.

 IdP metadata uploaded successfully

8. Eseguire un'impostazione TEST SSO che deve essere completata correttamente.



Description	SSO Status	SSO Validation
Test SSO for LAN/WAN based access	● Successful	<a href="#">Test SSO Setup</a>

n. This opens up a popup window. Enter the credentials and verify if the login is successful.



9. Accedere alla pagina web dell'amministratore su CCX con l'utente dell'amministratore e selezionare Sistema > Single Sign-On.

10. Fare clic sul pulsante Registra per incorporare i componenti.

**On-Boarding SSO Components**

i SSO components are registered successfully

[Register](#)

Component	[Redacted]	[Redacted]
CCX	✓	✓
CUIC	✓	✓
Finesse Desktop	✓	✓

11. La funzionalità di creazione di rapporti assegnata a Cisco Unified CCX Administrator (assegnata nella visualizzazione della capacità dell'amministratore) ed esecuzione del comando CLI utilizza l'utente cuic make-admin CCX\

12. Eseguire l'operazione di test SSO.

13. Dopo il completamento del test SSO, l'operazione di abilitazione è consentita.

SSO Status

 Current status: SSO Mode

Enable operation is allowed only after the SSO Test is successful

Component	[Redacted]	[Redacted]
CCX	✓	✓
CUIC	✓	✓
Finesse Desktop	✓	✓

## Verifica

Verificare le operazioni di login con agenti e amministratori su CCX, Cisco Unified Intelligence Center (CUIC) e Finesse. Devono avere successo.

Quando accede all'agente su finesse, reindirizza alla pagina OKTA.

Connecting to 

Sign in with your account to access CCXBU15

**okta**

Sign In

Username

Password

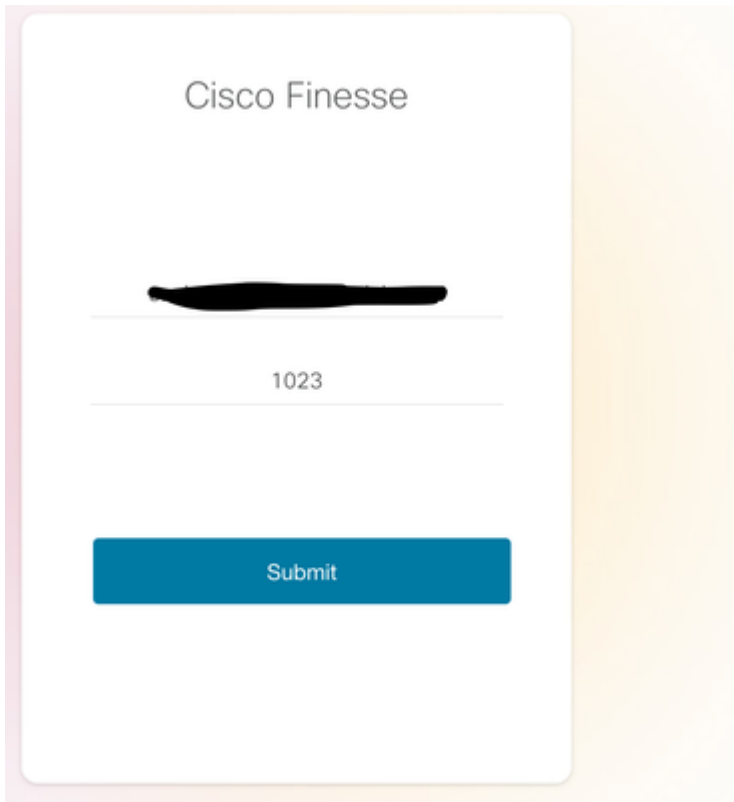
Keep me signed in

Sign in

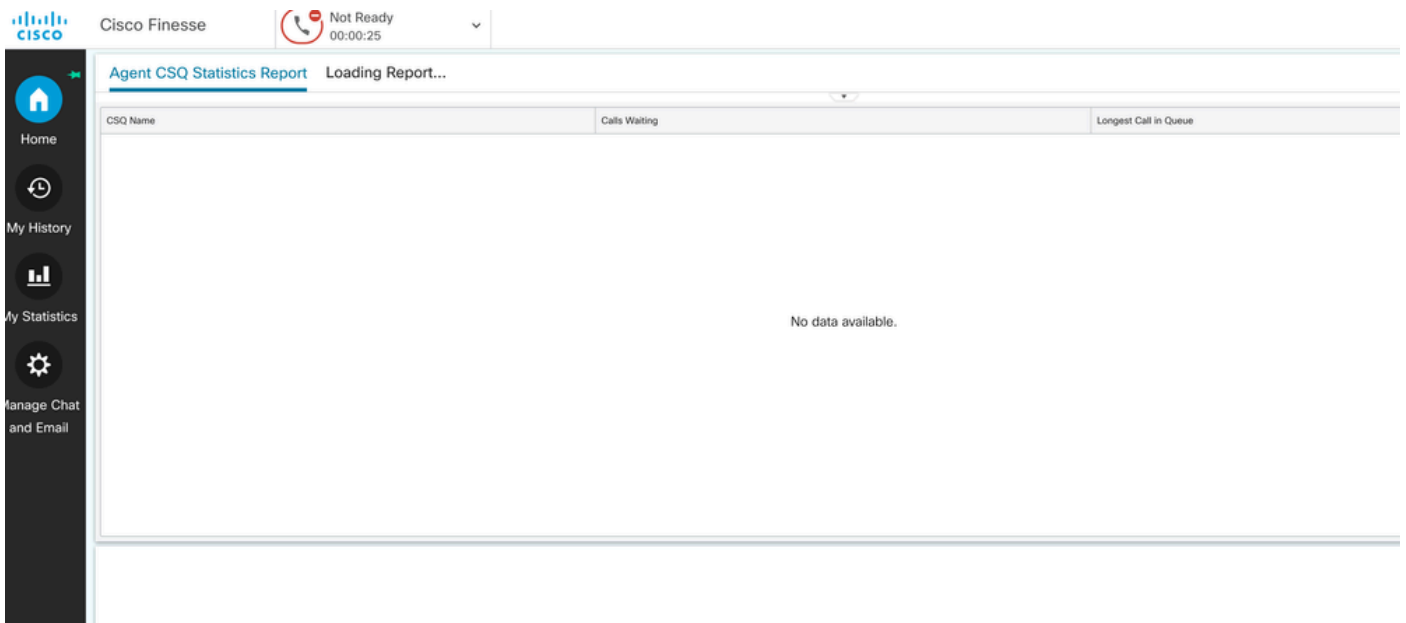
[Forgot password?](#)

[Help](#)

Dopo aver inserito le credenziali, richiede solo l'estensione ora nella pagina di accesso finesse.



Dopo l'immissione di questa opzione, l'accesso deve essere riuscito e tutti i report in tempo reale devono essere caricati correttamente.



## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).