

Configurer SSO sur les solutions CCX et Prem Contact Center avec Okta IDP

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration côté IDS/Cisco](#)

[Configuration côté OKTA IDP](#)

[Vérifier](#)

Introduction

Ce document décrit la configuration de l'authentification unique (SSO) avec OKTA pour diverses solutions de centre de contacts Cisco On Prem.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) ou Packaged Contact Center Enterprise (PCCE)
- langage de balisage des assertions de sécurité
- OKTA

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Unified contact center express (UCCX) 15.0
- OKTA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration côté IDS/Cisco

1. Exécutez la commande `utils ids set_property IS_IdP_OKTA true` sur CLI et redémarrez le service Identity Service (IDS).
2. Si la haute disponibilité (HA), exécutez cette commande sur les deux noeuds et redémarrez le service IDS.
3. Connectez-vous à l'interface d'administration Cisco IDS UCCX `https://<adresse du serveur UCCX>:8553/idsadmin` sur le noeud PUB.
4. Accédez à Paramètres > Sécurité > Clés et certificats.
5. Régénérer le certificat SAML (Security Assertion Markup Language).

The screenshot shows the 'Settings' page for Cisco IDS UCCX, specifically the 'Security' section. The left sidebar has 'Tokens' and 'Keys and Certificates' (highlighted in blue). 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. Dans l'onglet IDS Trust, téléchargez le fichier XML de métadonnées SAML SP.

Settings

IdS Trust Security Troubleshooting



SP Entity ID	Description	Metadata file
[REDACTED]	SAML SP to configure IdS access via LAN/WAN	Download

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

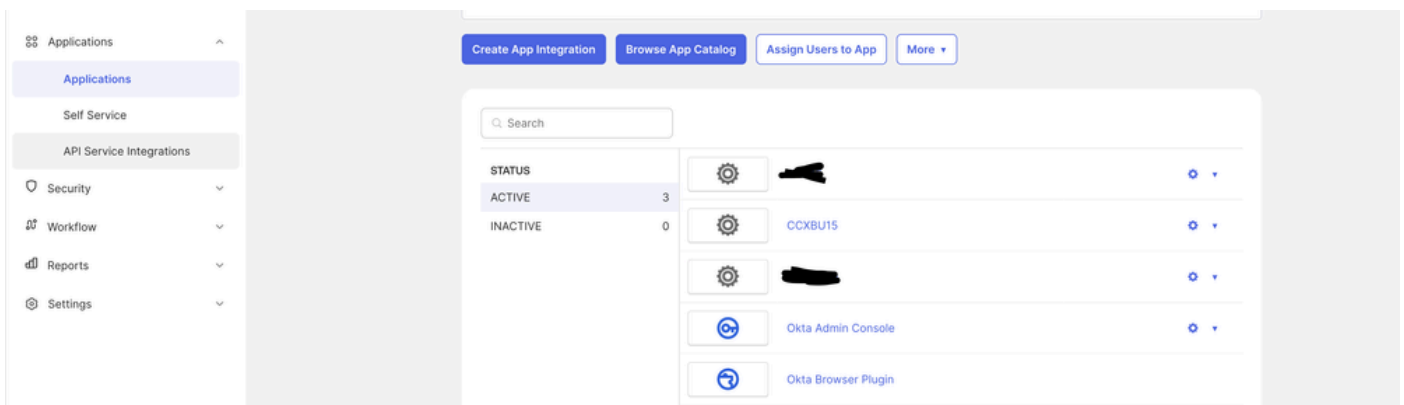
7. Ouvrez le fichier XML de métadonnées du fournisseur de services (SP) et notez la valeur de l'attribut « Location » pour les ID de l'éditeur et de l'abonné dans la balise « AssertionConsumerService ». L'AssertionConsumerServiceURL dans les métadonnées SAML inclut maintenant metaAlias comme partie de l'URL de réponse SAML au lieu du paramètre de requête pour PUB.

8. Pour l'Abonné, il s'affiche avec le paramètre de requête et peut être ignoré.

```
</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>
```

Configuration côté OKTA IDP

1. Sous Applications, cliquez sur Create App Integration.



2. Sélectionnez l'option SAML2.0.

Create a new app integration x

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. Sur le paramètre SAML SSO URL, fournissez l'URL SSO du PUB qui a été copié à l'étape 7. sous 'Configuration côté IDS/Cisco' dans ce document. Dans l'URI (Uniform resource identifier) d'auditoire (SP Entity ID), collez l'entité SP sous l'onglet de confiance IDS sur les paramètres de la gestion du service d'identité.

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 ?

[Empty field]

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. Sous 'Other Requestable SSO URLs', entrez l'URL de SUB <https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp> dans le format donné avec la valeur d'index 1.

Other Requestable SSO URLs

URL

Index

+ Add Another

5. Cliquez sur Next et sur Finish pour terminer la configuration de l'application.

6. Copiez les métadonnées de l'onglet Connexion à l'aide de l'URL et enregistrez-les au format xml.

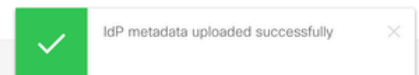
7. Téléchargez les métadonnées à partir de l'étape 6. sur la page Web de gestion des services d'identité côté CCX.

Download Metadata Upload IdP Metadata Test SSO Setup

IdP Entity Id : [REDACTED]

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.



8. Exécutez une configuration TEST SSO et elle doit aboutir.



Description	SSO Status	SSO Validation
Test SSO for LAN/WAN based access	● Successful	Test SSO Setup

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



9. Connectez-vous à la page Web admin sur CCX avec l'utilisateur admin et naviguez jusqu'à System > Single Sign On.

10. Cliquez sur le bouton Register pour intégrer les composants.

On-Boarding SSO Components

i SSO components are registered successfully

[Register](#)

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

11. Attribution d'une fonction de création de rapports à Cisco Unified CCX Administrator (attribuée dans la vue Administrator Capability) et exécution de la commande CLI utilise cuic user make-admin CCX\

12. Exécutez l'opération de test SSO.

13. Une fois le test SSO réussi, l'opération d'activation est autorisée.

SSO Status

 Current status: SSO Mode

Enable operation is allowed only after the SSO Test is successful

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

Vérifier

Vérifiez les opérations de connexion avec les agents et les administrateurs sur CCX, Cisco Unified Intelligence Center (CUIC) et Finesse. Ils doivent réussir.

Lors de la connexion de l'agent sur finesse, il redirige vers la page 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](#)

Après avoir saisi les informations d'identification, il ne demande que l'extension maintenant sur la page de connexion finesse.

Cisco Finesse

[Redacted]

1023

Submit

Une fois cette valeur saisie, la connexion doit aboutir et tous les rapports en direct doivent être correctement chargés.

Cisco Finesse Not Ready 00:00:25

Agent CSQ Statistics Report Loading Report...

CSQ Name	Calls Waiting	Longest Call in Queue
No data available.		

- Home
- My History
- My Statistics
- Manage Chat and Email

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.