

SSO configureren voor CCX- en Prem-contactcenteroplossingen met Okta IDP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie aan de IDS/Cisco-zijde](#)

[Configuratie aan OKTA IDP-zijde](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft de Single Sign On (SSO)-configuratie met OKTA voor verschillende Cisco On Prem Contact Center-oplossingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) of Packaged Contact Center Enterprise (PCCE)
- Security Assertion Markup Language
- OKTA

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Unified Contact Center Express (UCCX) 15.0
- OKTA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie aan de IDS/Cisco-zijde

1. Voer de opdracht `ids set_property IS_IdP_OKTA true` uit op CLI en start de ID-service (Identity Service) opnieuw.
2. Als High Availability (HA) is ingesteld, voert u deze opdracht uit op beide knooppunten en start u de IDS-service opnieuw.
3. Meld u aan bij UCCX Cisco IDS-beheerinterface <https://<UCCX-serveradres>:8553/idsadmin> op PUB-node.
4. Navigeer naar Instellingen > Beveiliging > Sleutels en certificaten.
5. Certificaat van de Regenerate Security Assertion Markup Language (SAML).

Settings

The screenshot shows the 'Settings' page for Cisco IDS, specifically the 'Security' section. The page has a navigation bar with 'IdS Trust', 'Security', and 'Troubleshooting'. The 'Security' section is active. On the left, there are two menu items: 'Tokens' (Set Token Expiry) and 'Keys and Certificates' (Regenerate Keys and Certificates). The 'Keys and Certificates' item is selected. The main content area is titled 'Generate Keys and SAML Certificate'. It contains two sections: 'Encryption/Signature key' and 'SAML Certificate'. The 'Encryption/Signature key' section has a 'Regenerate' button. The 'SAML Certificate' section has a dropdown menu set to 'SHA-256' and a 'Regenerate' button. Below the dropdown, 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. Download SAML SP-metagegevens XML op het tabblad IDS-vertrouwen.

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.

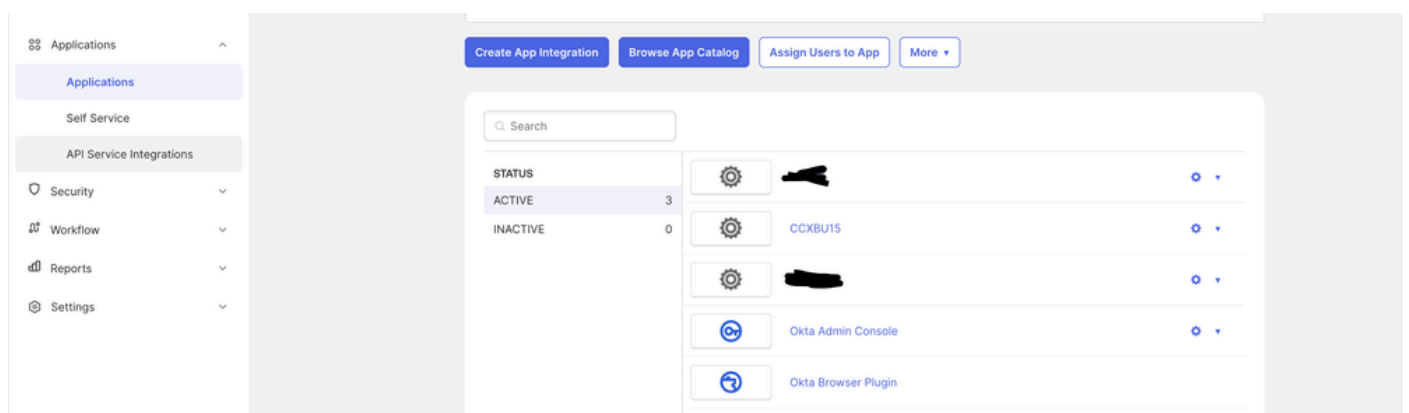
7. Open Service Provider (SP) metadata XML en noteer de 'Location' attribuutwaarde voor Publisher en Subscriber IDS binnen 'AssertionConsumerService' tag. De AssertionConsumerServiceURL in SAML-metagegevens bevat nu metaAlias als onderdeel van de SAML-reactie-URL in plaats van de queryparameter voor PUB.

8. Voor Abonnee, het toont met query parameter en kan worden genegeerd.

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

Configuratie aan OKTA IDP-zijde

1. Klik onder Toepassingen op App-integratie maken.



2. Kies de optie 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. Geef in de SSO-URL van de SAML-instelling de SSO-URL van de PUB op die in stap 7 is gekopieerd. Geef in dit document onder 'Configuratie op IDS/Cisco-zijde' op. Plak in de Audience Uniform Resource Identifier (URI) (SP Entity ID) de SP-entiteit onder het tabblad IDS-vertrouwen op instellingen in het servicebeheer Identiteit.

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. Voer onder de 'Overige aangevraagde SSO-URL's' de URL van SUB <https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp> in de opgegeven indeling in met indexwaarde als 1.

Other Requestable SSO URLs

URL

Index

+ Add Another


5. Klik op Volgende en Voltooien om de toepassingsconfiguratie te voltooien.

6. Kopieer de metagegevens van het tabblad Aanmelden met behulp van de URL en sla deze op als xml.

7. Upload de metagegevens vanaf stap 6 op de webpagina voor identiteitsbeheer aan de CCX-zijde.

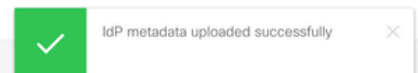
Download Metadata Upload IdP Metadata Test SSO Setup

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.

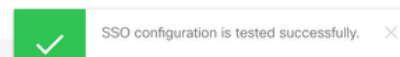


8. Voer een TEST-SSO-installatie uit en deze moet succesvol zijn.



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. Meld u aan bij de beheerderspagina op CCX met de beheerdersgebruiker en navigeer naar **Systeem > Eenmalige aanmelding**.

10. Klik op de knop **Registreren** om aan boord van de onderdelen te gaan.

On-Boarding SSO Components

i SSO components are registered successfully

[Register](#)

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

11. Aan Cisco Unified CCX Administrator toegewezen rapportagemogelijkheid (toegewezen in de weergave Administrator Capability) en CLI-opdrachtregels uitvoeren met cuic user make-admin CCX\

12. Voer de SSO-testbewerking uit.

13. Nadat de SSO-test succesvol is, is de activeringsbewerking toegestaan.

SSO Status

 Current status: SSO Mode

Enable operation is allowed only after the SSO Test is successful

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

Verifiëren

Controleer of er aanmeldingsbewerkingen zijn met agent en beheerders op CCX, Cisco Unified Intelligence Center (CUIC) en Finesse. Ze moeten succesvol zijn.

Wanneer u zich aanmeldt bij de agent op finesse, wordt deze omgeleid naar de OKTA-pagina.

Connecting to 

Sign in with your account to access CCXBU15

okta

Sign In

Username

Password

Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)

Na het invoeren van de referenties, vraagt het alleen om de extensie nu op de finesse-inlogpagina.

Cisco Finesse

[Redacted]

1023

Submit

Nadat dit is ingevoerd, moet de login succesvol zijn en moeten alle live rapporten goed worden geladen.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.