

# Okta IDPによるCCXおよび構内コンタクトセンターソリューションでのSSOの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[IDS/Cisco側の設定](#)

[OKTA IDP側の設定](#)

[確認](#)

---

## はじめに

このドキュメントでは、さまざまなCisco On Prem Contact Center(OCC)ソリューションのOKTAを使用したシングルサインオン(SSO)の設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise(UCCE)、またはPackaged Contact Center Enterprise(PCCE)
- Security Assertion Markup Language(SAML)
- オクタ

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Unified Contact Center Express(UCCX)15.0
- オクタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## IDS/Cisco側の設定

1. コマンド `utils ids set_property IS_IdP_OKTA true` を CLI で実行し、アイデンティティサービス (IDS) サービスを再起動します。
2. 高可用性(HA)の場合は、両方のノードでこのコマンドを実行し、IDSサービスを再起動します。
3. PUBノードでUCCX Cisco IDS管理インターフェイス `https://<UCCX server address>:8553/idsadmin` にログインします。
4. Settings > Security > Keys and Certificatesの順に移動します。
5. Security Assertion Markup Language(SAML)証明書を再生成します。

### Settings

The screenshot shows the 'Settings' page for IDS, specifically the 'Security' section and 'Keys and Certificates' tab. The page has a navigation bar with 'IdS Trust', 'Security', and 'Troubleshooting'. The 'Keys and Certificates' tab is active, showing a 'Regenerate Keys and Certificates' button. Below this, there are two main sections: 'Generate Keys and SAML Certificate' and 'SAML Certificate'. The 'Generate Keys and SAML Certificate' section has a 'Regenerate' button. The 'SAML Certificate' section has a dropdown menu set to 'SHA-256' and a 'Regenerate' button. A note below the dropdown states: '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. IDS Trustタブから、SAML SPメタデータXMLをダウンロードします。

## 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.

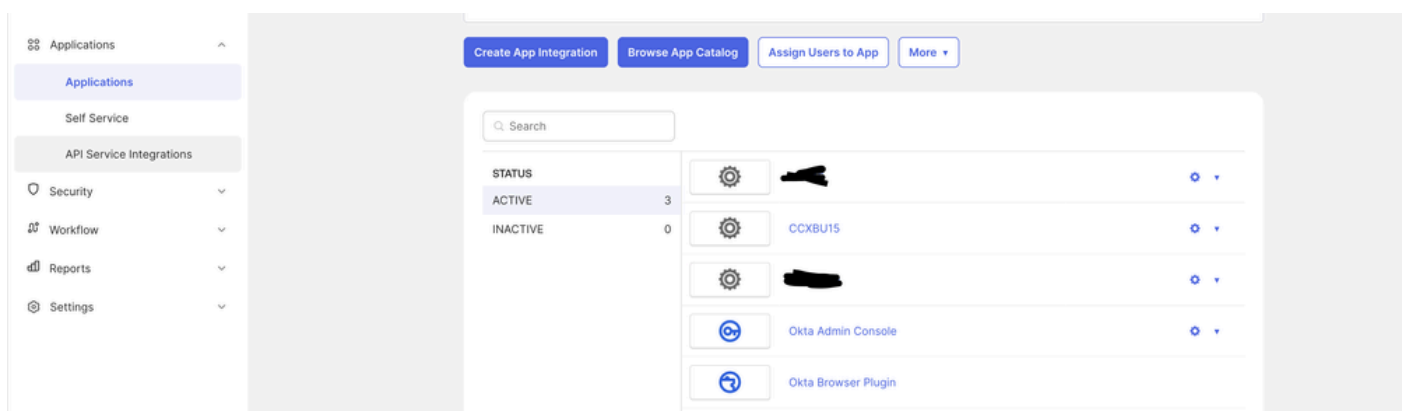
7. サービスプロバイダー(SP)のメタデータXMLを開き、「AssertionConsumerService」タグ内のパブリッシャおよびサブスクライバIDの「Location」属性値をメモします。SAMLメタデータ内のAssertionConsumerServiceURLに、PUBのクエリパラメータの代わりにSAML応答URLの一部としてmetaAliasが含まれるようになりました。

8. サブスクライバの場合は、クエリパラメータとともに表示され、無視できます。

```
</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>
```

## OKTA IDP側の設定

1. 「アプリケーション」で、「アプリケーション統合の作成」をクリックします。



2. SAML2.0オプションを選択します。

## 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. SAML設定のSSO URLで、このドキュメントの「IDS/Cisco側での設定」の手順7でコピーしたパブリッシャのSSO URLを指定します。Audience Uniform Resource Identifier (URI) (SP Entity ID)で、アイデンティティサービス管理の設定のIDS trustタブにあるSPエンティティを貼り付けます。

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. 'Other Requestable SSO URLs'で、SUB

<https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp>のURLを、インデックス値1を使用して任意の形式で入力します。

Other Requestable SSO URLs

URL

Index

+ Add Another

5. NextおよびFinishをクリックして、アプリケーションの設定を完了します。

6. URLを使用して「サインオン」タブからメタデータをコピーし、xmlとして保存します。

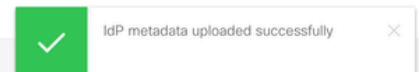
7. CCX側のアイデンティティサービス管理Webページで、手順6.のメタデータをアップロードします。

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.

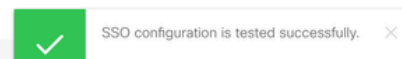


8. TEST SSOセットアップを実行します。このセットアップは成功する必要があります。



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. 管理者ユーザでCCXの管理Webページにログインし、システム>シングルサインオンに移動します。

10. 「登録」ボタンをクリックして構成部品を登録します。

**On-Boarding SSO Components**

i SSO components are registered successfully

[Register](#)


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

11. Cisco Unified CCX管理者にレポート機能を割り当て ( Administrator Capabilityビューで割り当て )、CLIコマンド `utils cuic user make-admin CCX\<Admin User Id>` を実行して、Cisco Unified Intelligence Centerに管理者権限を提供します。SSOテスト操作に管理者権限を持つ設定済みのユーザを使用します。

12. SSOテスト操作を実行します。

13. SSOテストが成功すると、enable操作が許可されます。

SSO Status

 Current status: SSO Mode

Enable operation is allowed only after the SSO Test is successful

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

## 確認

CCX、Cisco Unified Intelligence Center(CUIC)、およびFinesseで、エージェントおよび管理者とのログイン操作を確認します。これらは成功するはずです。

Finesseでエージェントにログインすると、OKTAページにリダイレクトされます。

Connecting to 

Sign in with your account to access CCXBU15

**okta**

Sign In

Username

Password

Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)

クレデンシャルを入力すると、Finesseログインページで内線番号の入力だけを求められます。

Cisco Finesse

[Redacted]

1023

Submit

この入力後、ログインが成功し、すべてのライブレポートが正常にロードされる必要があります。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。