

Configurar o SSO no CCX e nas soluções do Contact Center Local com o Okta IDP

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração no lado IDS/Cisco](#)

[Configuração no lado OKTA IDP](#)

[Verificar](#)

Introdução

Este documento descreve a configuração do SSO (Single Sign On, Logon único) com OKTA para várias soluções Cisco On Prem Contact Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) ou Packaged Contact Center Enterprise (PCCE)
- Linguagem de marcação de asserção de segurança
- OKTA

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Unified Contact Center Express (UCCX) 15.0
- OKTA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração no lado IDS/Cisco

1. Execute o comando `utils ids set_property IS_IdP_OKTA true` na CLI e reinicie o serviço do Identity Service (IDS).
2. Se houver HA (High Availability, alta disponibilidade), execute este comando em ambos os nós e reinicie o serviço IDS.
3. Faça login na interface de administrador do Cisco IDS do UCCX `https://<UCCX server address>:8553/idsadmin` no nó PUB.
4. Navegue até Configurações > Segurança > Chaves e Certificados.
5. Regenerar o Certificado SAML (Security Assertion Markup Language).

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'. On the left, there are two menu items: 'Tokens' (Set Token Expiry) and 'Keys and Certificates' (Regenerate Keys and Certificates). The 'Keys and Certificates' section is active and contains two main options: 'Generate Keys and SAML Certificate' and 'SAML Certificate'. The 'Generate Keys and SAML Certificate' section includes a description: 'Encryption/Signature key. Regenerate key for token encryption and signing.' and a 'Regenerate' button. The 'SAML Certificate' section includes a description: 'Regenerate certificate for signing SAML request. Select secure hash algorithm.' and a dropdown menu currently set to 'SHA-256'. 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.' and another 'Regenerate' button.

6. Na guia IDS Trust, baixe o XML dos metadados SP SAML.

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.

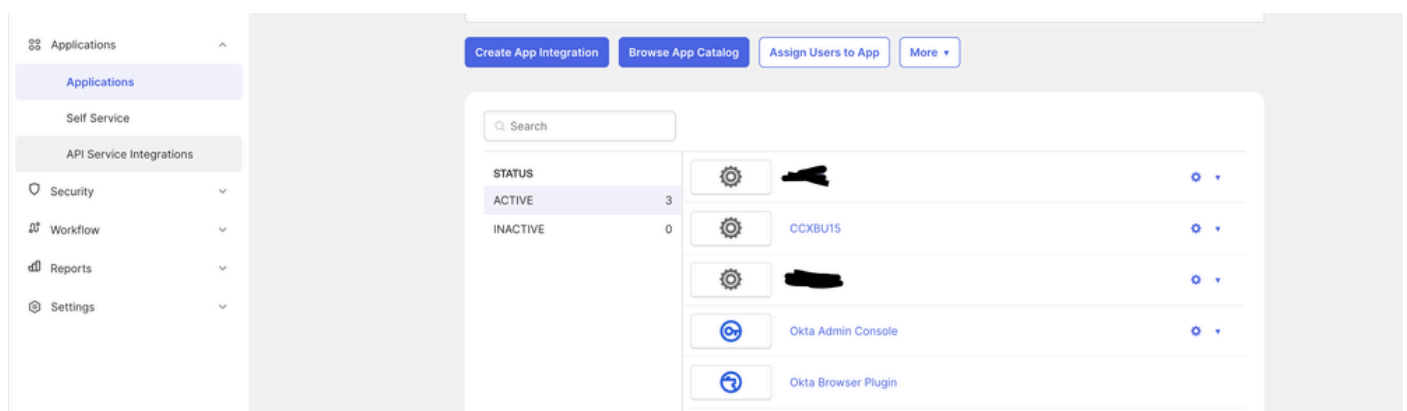
7. Abra o XML de metadados do SP (Provedor de Serviços) e anote o valor do atributo 'Location' para as IDS do Publicador e do Assinante na marca 'AssertionConsumerService'. A AssertionConsumerServiceURL nos metadados SAML agora inclui metaAlias como parte da URL de resposta SAML em vez do parâmetro de consulta para PUB.

8. Para o Assinante, ele é mostrado com o parâmetro query e pode ser ignorado.

```
</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>
```

Configuração no lado OKTA IDP

1. Em Aplicativos, clique em Criar Integração de Aplicativos.



2. Escolha a opção 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. Na URL SSO da configuração SAML, forneça a URL SSO do PUB que foi copiada na Etapa 7. em "Configuração no IDS/Cisco Side" neste documento. No URI (identificador de recurso) Uniforme da Audiência (ID da entidade da controladora de armazenamento) cole a entidade da controladora de armazenamento na guia Confiança de IDS nas configurações do Gerenciamento do serviço de identidade.

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. Em 'Other Requestable SSO URLs', insira o URL de SUB <https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp> no formato especificado com o valor de índice 1.

Other Requestable SSO URLs

URL

Index

+ Add Another


5. Clique em Próximo e Concluir para concluir a configuração do aplicativo.

6. Copie os Metadados da guia Sign On usando o URL e salve-o como xml.

7. Carregue os metadados da Etapa 6. na página da Web de gerenciamento do serviço de identidade no CCX.

Download Metadata Upload IdP Metadata Test SSO Setup

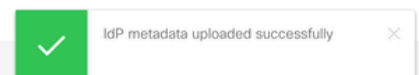
IdP Entity Id : [REDACTED]



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.

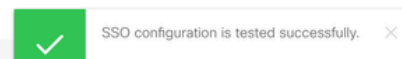


8. Execute uma configuração TEST SSO e ela deverá ser bem-sucedida.



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. Faça login na página da Web do administrador no CCX com o usuário admin e navegue para Sistema > Logon único.

10. Clique no botão Registrar para integrar os componentes.

On-Boarding SSO Components

SSO components are registered successfully

[Register](#)

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

11. O recurso de relatórios foi atribuído ao Cisco Unified CCX Administrator (atribuído na exibição do recurso do administrador) e execute o comando CLI `utils cuic user make-admin CCX\<Admin User Id>` para fornecer direitos de administrador no Cisco Unified Intelligence Center. Use o usuário configurado com direitos de administrador para a operação de Teste de SSO.

12. Execute a operação de Teste de SSO.

13. Depois que o Teste de SSO for bem-sucedido, a operação de ativação será permitida.

The screenshot shows the 'SSO Status' page. At the top, it says 'Current status: SSO Mode' with an information icon. Below this are 'Enable' and 'Disable' buttons. A blue banner reads 'Enable operation is allowed only after the SSO Test is successful'. A table follows with two columns of redacted component names and three rows of test results for CCX, CUIC, and Finesse Desktop, all showing green checkmarks.

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

Verificar

Verifique as operações de login com agentes e administradores no CCX, no Cisco Unified Intelligence Center (CUIC) e no Finesse. Elas têm de ser bem sucedidas.

Ao fazer logon do agente no Finesse, ele é redirecionado para a página 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](#)

Depois de colocar as credenciais, ele solicita apenas a extensão agora na página de login do finesse.

Cisco Finesse

[Redacted]

1023

Submit

Depois que isso for inserido, o logon deverá ser bem-sucedido e todos os relatórios ao vivo deverão estar carregados corretamente.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.