

使用Okta IDP在CCX和高级联系中心解决方案上配置SSO

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[IDS/思科端配置](#)

[OKTA IDP端上的配置](#)

[验证](#)

简介

本文档介绍适用于各种思科在线高级联系中心解决方案的OKTA单点登录(SSO)配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise(UCCE)或 Packaged Contact Center Enterprise(PCCE)
- 安全断言标记语言
- OKTA

使用的组件

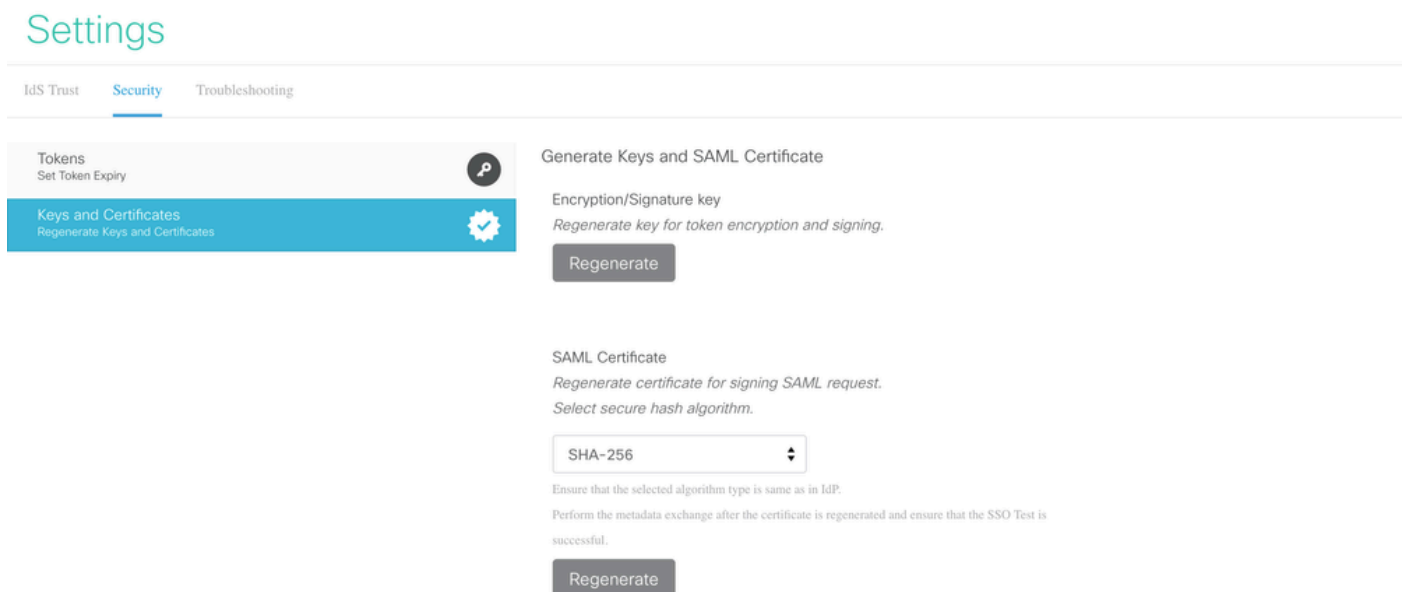
本文档中的信息基于以下软件和硬件版本：

- 统一联络中心快捷版(UCCX)15.0
- OKTA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

IDS/思科端配置

- 1.在CLI上运行utils ids set_property IS_IdP_OKTA true命令，然后重新启动身份服务(IDS)服务。
- 2.如果高可用性(HA)，则在两个节点上运行此命令并重新启动IDS服务。
- 3.登录PUB节点上的UCCX Cisco IDS管理接口https://<UCCX服务器地址>:8553/idsadmin。
- 4.导航到设置>安全>密钥和证书。
- 5.重新生成安全断言标记语言(SAML)证书。



The screenshot shows the 'Settings' page for Cisco IDS, specifically the 'Security' section. The left sidebar has 'Keys and Certificates' selected. The main content area is titled 'Generate Keys and SAML Certificate' and 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.从“IDS信任”选项卡下，下载SAML SP元数据XML。

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.

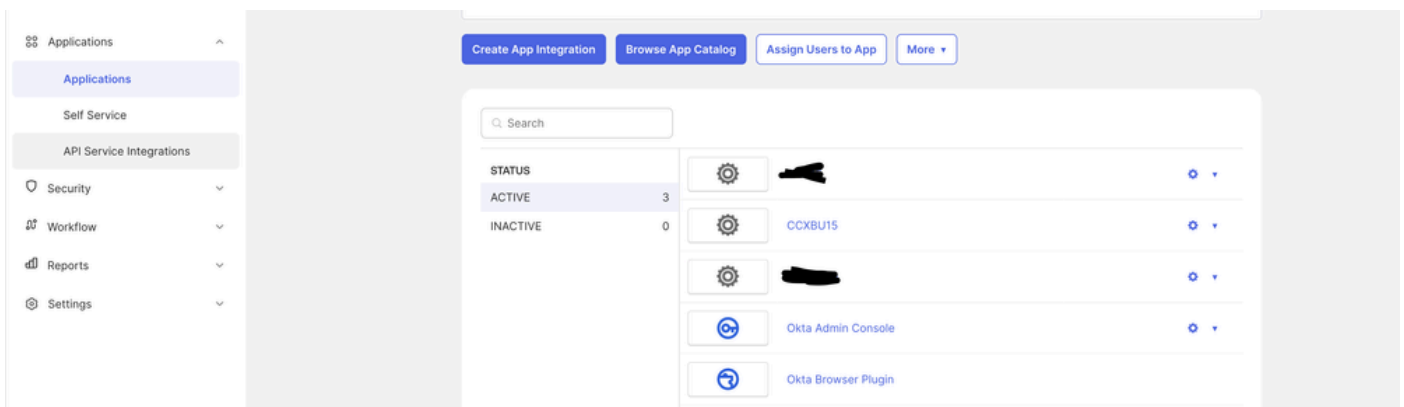
7. 打开服务提供商(SP)元数据XML，并记下“AssertionConsumerService”标记中发布服务器和订用服务器ID的“Location”属性值。SAML元数据中的AssertionConsumerServiceURL现在将metaAlias作为SAML响应URL的一部分，而不是PUB的查询参数。

8. 对于订户，它显示查询参数，可以忽略。

```
</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="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="8553/ids/saml/response?metaAlias=/sp" index="1" isDefault="false" />
</SPSSODescriptor>
```

OKTA IDP端上的配置

1. 在Applications下，单击Create App Integration。



2. 选择SAML2.0选项。

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.在SAML设置SSO URL上，在本文档的“在IDS/Cisco端配置”下提供步骤7中复制的PUB的SSO URL。在Audience Uniform resource identifier(URI)(SP Entity ID)中，将SP实体粘贴到身份服务管理中的设置的IDS trust选项卡下。

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.在“其他可请求SSO URL”下方，以给定格式输入子

<https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp>的URL，索引值为1。

Other Requestable SSO URLs

URL

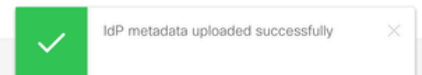
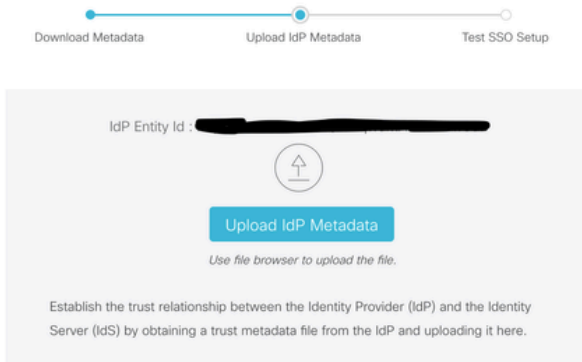
Index

+ Add Another

5.单击下一步和完成以完成应用程序配置。

6.使用URL从“登录”选项卡复制元数据并将其保存为xml。

7.将步骤6中的元数据上传到CCX端的身份服务管理网页上。

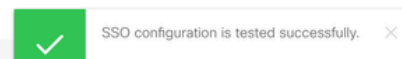


8.运行测试SSO设置，该设置必须成功。



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.使用管理员用户登录CCX上的管理员网页，然后导航到System > Single Sign On。

10.单击Register按钮将组件安装到主板上。

On-Boarding SSO Components

i SSO components are registered successfully

Register


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

11.向Cisco Unified CCX管理员分配报告权能（在“管理员权能”视图中分配），然后执行CLI命令 `utils cuic user make-admin CCX\<Admin User Id>` 以在Cisco Unified Intelligence Center中提供管理员权限。使用已配置具有SSO测试操作管理员权限的用户。

12.运行SSO测试操作。

13.在SSO测试成功后，允许启用操作。

SSO Status

 Current status: SSO Mode


Enable operation is allowed only after the SSO Test is successful


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

验证

在CCX、Cisco Unified Intelligence Center(CUIC)和Finesse上与代理和管理员一起检查登录操作。他们必须成功。

在Finesse上登录代理时，会重定向到OKTA页面。


Connecting to 
 Sign in with your account to access CCXBU15



Sign In

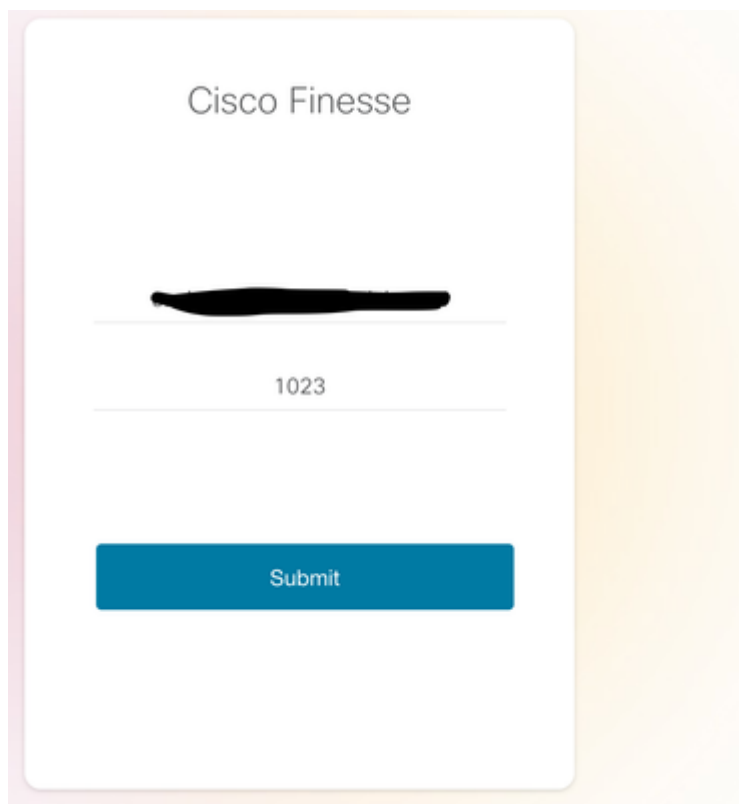
Username

Password

 
 Keep me signed in

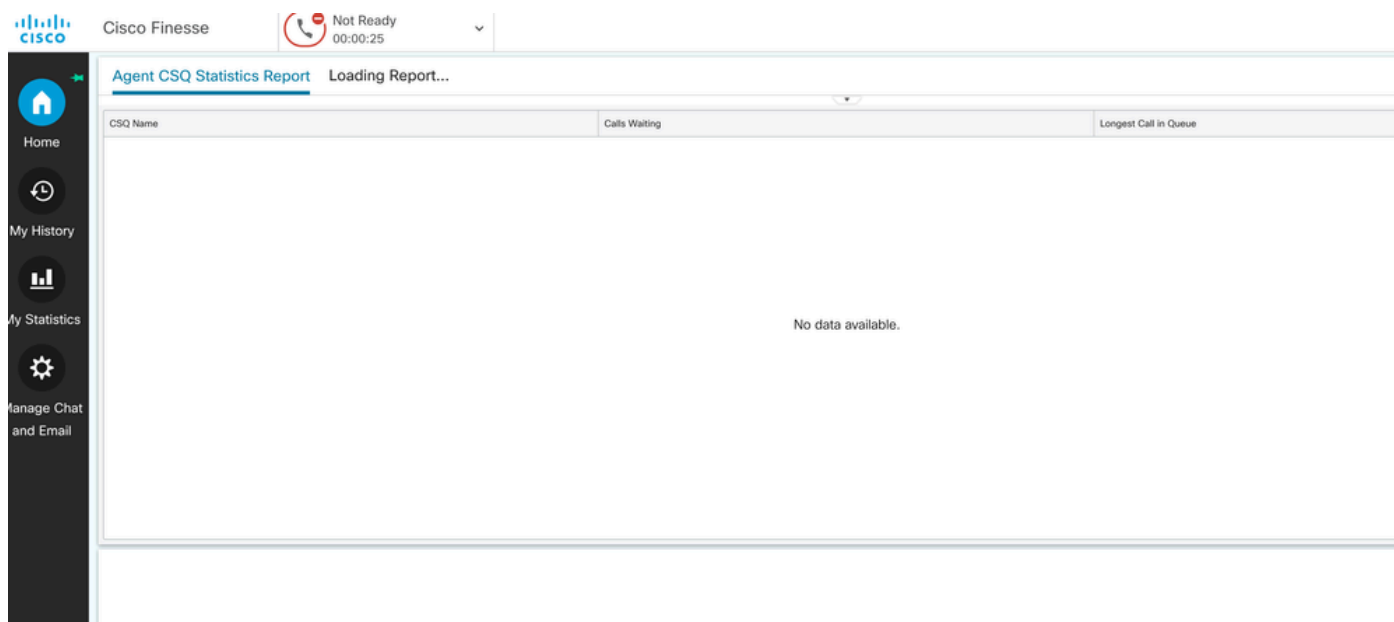
[Forgot password?](#)
[Help](#)

输入凭证后，它现在只在finesse登录页面上请求分机。



The image shows a login form for Cisco Finesse. At the top, it says "Cisco Finesse". Below that is a text input field containing a redacted phone number. Underneath is another text input field containing the extension number "1023". At the bottom of the form is a blue button labeled "Submit".

输入此命令后，登录必须成功，并且所有实时报告必须正常加载。



The image shows the Cisco Finesse dashboard. At the top left is the Cisco logo. To its right is the text "Cisco Finesse". Further right is a status indicator showing a red phone icon, the text "Not Ready", and a timer "00:00:25". Below this is a navigation bar with the following items: "Agent CSQ Statistics Report" (highlighted), "Loading Report...", and a dropdown arrow. Below the navigation bar is a table with the following columns: "CSQ Name", "Calls Waiting", and "Longest Call in Queue". The table is currently empty, and the text "No data available." is displayed in the center of the table area. On the left side of the dashboard is a vertical sidebar with the following icons and labels: "Home", "My History", "My Statistics", and "Manage Chat and Email".

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。