

在具有Okta IDP的CCX和高級聯絡中心解決方案上配置SSO

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[IDS/思科端上的組態](#)

[OKTA IDP端上的配置](#)

[驗證](#)

簡介

本檔案介紹各種思科高級版客服中心解決方案的單點登入(SSO)配置和OKTA。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise(UCCE)或 Packaged Contact Center Enterprise(PCCE)
- 安全斷言標籤語言
- OKTA

採用元件

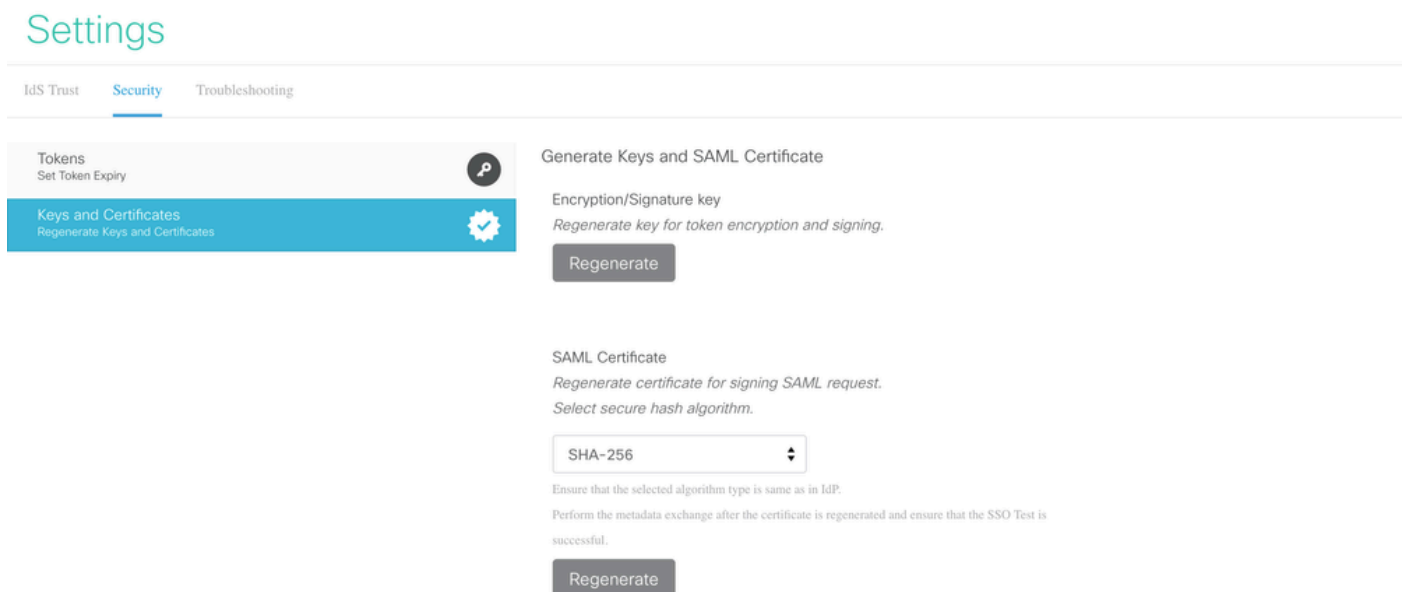
本文中的資訊係根據以下軟體和硬體版本：

- 整合客服中心express版(UCCX)15.0
- OKTA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

IDS/思科端上的組態

- 1.在CLI上運行utils ids set_property IS_IdP_OKTA true命令，然後重新啟動身份服務(IDS)服務。
- 2.如果高可用性(HA)，則在兩個節點上運行此命令並重新啟動IDS服務。
- 3.登入PUB節點上的UCCX Cisco IDS管理介面<https://<UCCX伺服器地址>:8553/idsadmin>。
- 4.定位至「設定」>「安全性」>「金鑰和證書」。
- 5.重新生成安全斷言標籤語言(SAML)證書。



The screenshot shows the 'Settings' page for 'IDS Trust' under the 'Security' tab. The left sidebar has 'Keys and Certificates' selected. 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. 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.從IDS Trust頁籤，下載SAML SP後設資料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.

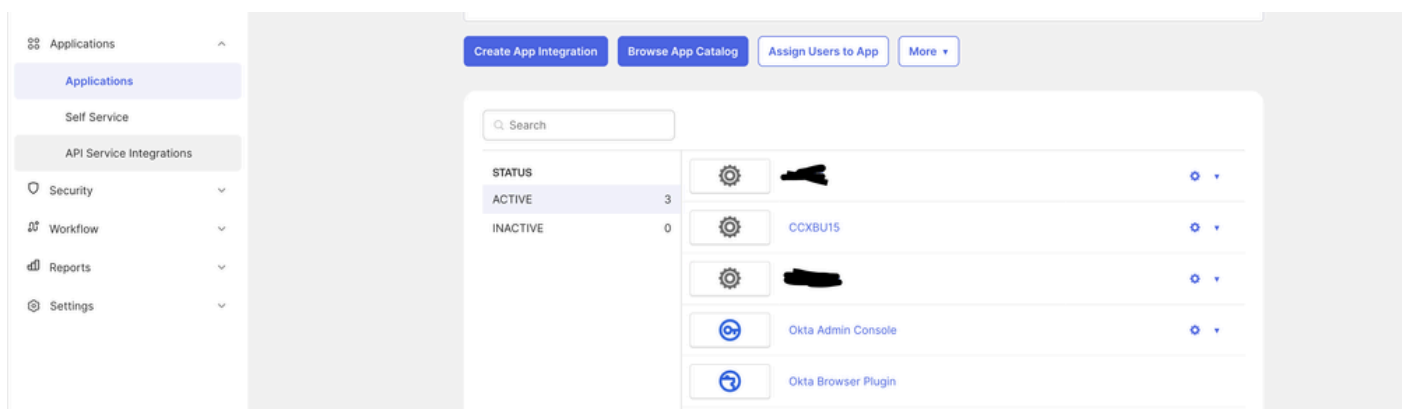
7. 打開服務提供商(SP)後設資料XML，並記下「AssertionConsumerService」標籤中發佈者和訂戶ID的「Location」屬性值。SAML後設資料中的AssertionConsumerServiceURL現在將metaAlias作為SAML響應URL的一部分，而不是PUB的查詢引數。

8. 對於訂戶，它會顯示查詢引數，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，按一下Create App Integration。



2. 選擇SAML2.0選項。

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.在SAML設定SSO URL上，提供在步驟7中複製的PUB的SSO URL。在本文檔的「IDS/Cisco Side上的配置」下。在Audience Uniform resource Identifier(URI)(SP Entity ID)中，將SP實體貼上到Identity Service管理設定的IDS trust頁籤下。

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「其他可請求SSO URL」下，以給定格式輸入SUB
<https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp>的URL，索引值為1。

Other Requestable SSO URLs

URL

Index

+ Add Another


5.按一下下一步和完成以完成應用程式配置。

6.使用URL從「登入」頁籤複製後設資料並將其另存為xml。

7.上傳步驟6中的後設資料。在CCX端的身分服務管理網頁上。

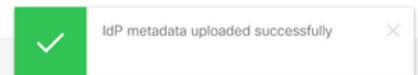
Download Metadata Upload IdP Metadata Test SSO Setup

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.

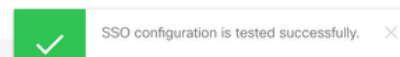


8.運行TEST SSO安裝程式，並且必須成功。



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. 使用管理員使用者登入到CCX上的管理網頁，然後導航到System > Single Sign On。

10. 按一下Register按鈕將元件裝入。

On-Boarding SSO Components

SSO components are registered successfully

[Register](#)


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

11. 向Cisco Unified CCX管理員分配報告功能（在「管理員功能」檢視中分配），然後執行CLI命令 `utils cuic user make-admin CCX<Admin User Id>` 以提供Cisco Unified Intelligence Center中的管理員許可權。使用具有管理員許可權的已配置使用者執行SSO測試操作。

12. 運行SSO測試操作。

13. 在SSO測試成功後，允許啟用操作。

SSO Status

 Current status: SSO Mode


Enable operation is allowed only after the SSO Test is successful


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

驗證

通過CCX、Cisco Unified Intelligence Center(CUIC)和Finesse上的代理和管理員檢查登入操作。他們必須成功。

在finesse上登入代理時，它會重定向到OKTA頁。

Connecting to 
 Sign in with your account to access CCXBU15



Sign In

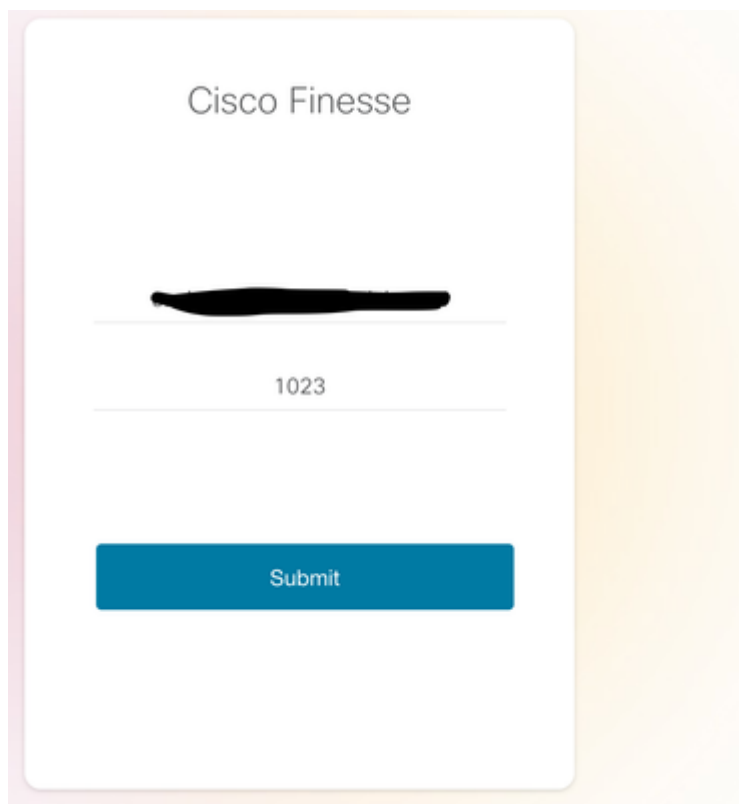
Username

Password

Keep me signed in

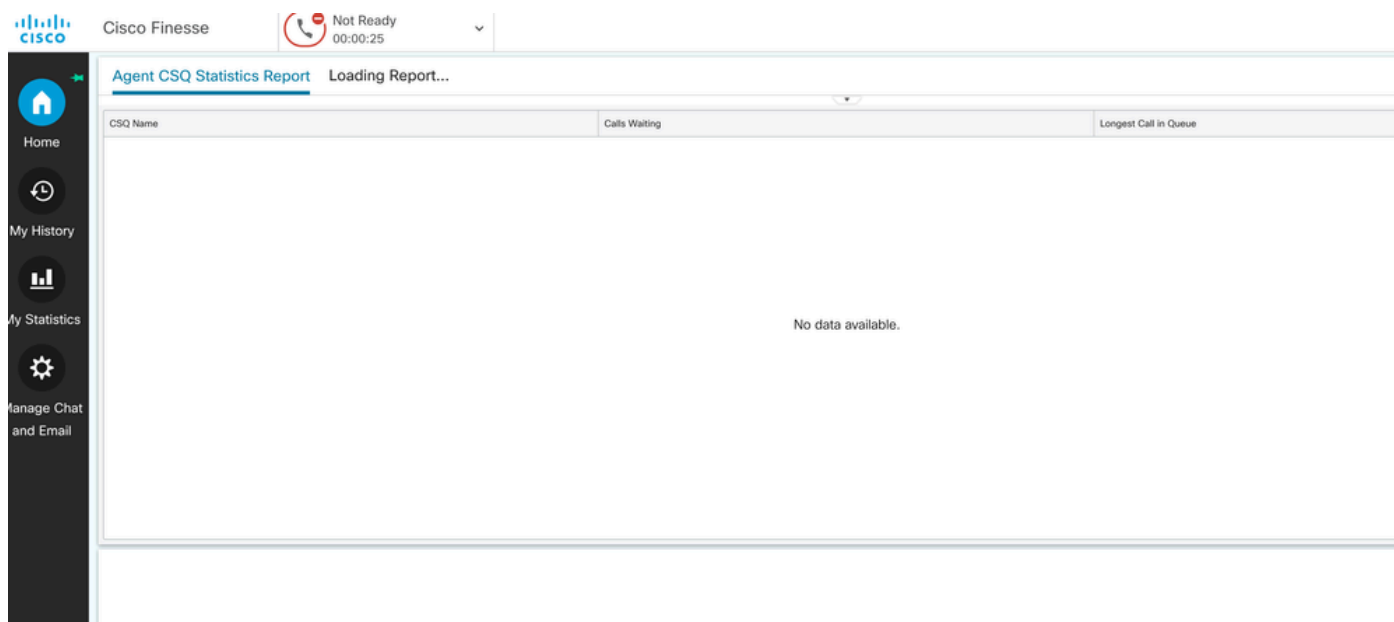
[Forgot password?](#)
[Help](#)

輸入憑證後，在finesse登入頁面上只要求分機。



The image shows the Cisco Finesse login interface. 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 "Submit" button.

輸入此命令後，登入必須成功，並且所有即時報告必須正常載入。



The image shows the Cisco Finesse dashboard. The top bar includes the Cisco logo, the text "Cisco Finesse", and a status indicator "Not Ready 00:00:25". Below the top bar is a navigation menu with icons for Home, My History, My Statistics, and Manage Chat and Email. The main content area is titled "Agent CSQ Statistics Report" and shows "Loading Report...". Below this is a table with columns for "CSQ Name", "Calls Waiting", and "Longest Call in Queue". The table is currently empty, displaying "No data available."

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。