

Configure SSO on CCX and Prem Contact Center Solutions with Okta IDP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration on IDS/Cisco Side](#)

[Configuration on OKTA IDP Side](#)

[Verify](#)

Introduction

This document describes the Single Sign On (SSO) configuration with OKTA for various Cisco On Prem Contact Center Solutions.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

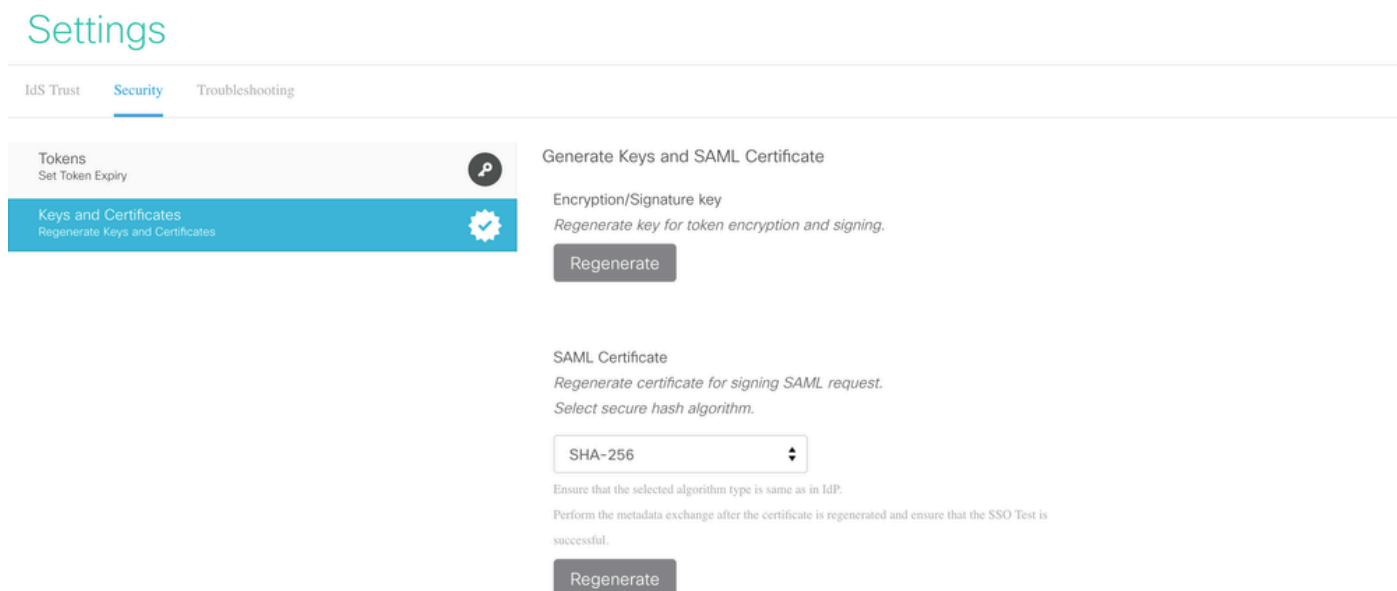
The information in this document is based on these software and hardware versions:

- Unified contact center express (UCCX) 15.0
- OKTA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration on IDS/Cisco Side

1. Run the command `utils ids set_property IS_IdP_OKTA true` on CLI and restart the Identity Service (IDS) service.
2. If High Availability (HA) then run this command on both nodes and restart IDS service.
3. Login to UCCX Cisco IDS admin interface `https://<UCCX server address>:8553/idsadmin` on PUB node.
4. Navigate to **Settings > Security > Keys and Certificates**.
5. Regenerate Security Assertion Markup Language (SAML) Certificate.



The screenshot displays the 'Settings' page of the Cisco IDS admin interface. The 'Security' tab is selected, and the 'Keys and Certificates' sub-tab is active. The page is divided into two main sections: 'Generate Keys and SAML Certificate' and 'SAML Certificate'.

Generate Keys and SAML Certificate

Encryption/Signature key
Regenerate key for token encryption and signing.

SAML Certificate
Regenerate certificate for signing SAML request.
Select secure hash algorithm.

SHA-256

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. From IDS Trust tab, download **SAML SP metadata 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.

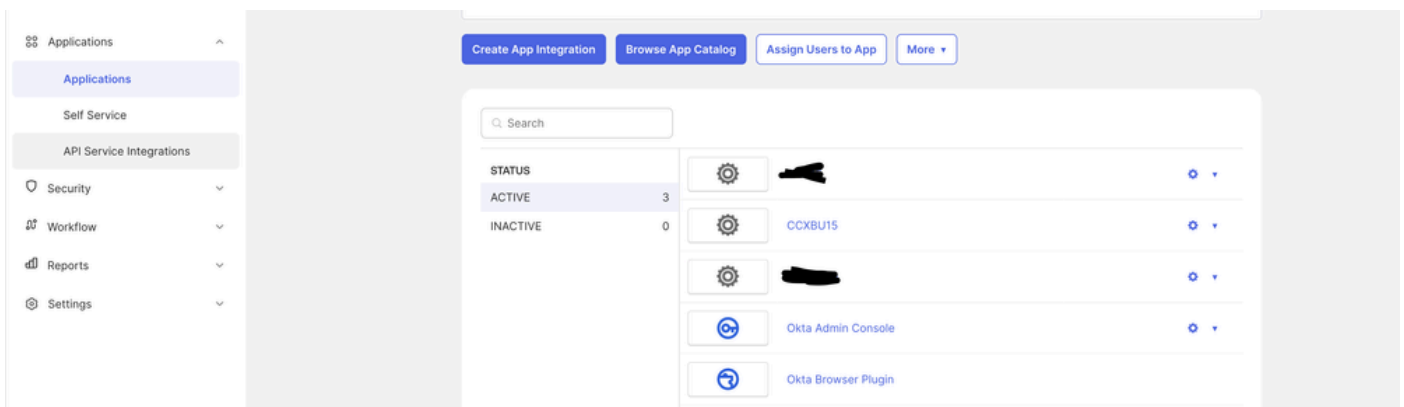
7. Open Service Provider (SP) metadata XML and make a note of the 'Location' attribute value for Publisher and Subscriber IDS within 'AssertionConsumerService' tag. The AssertionConsumerServiceURL in SAML metadata now includes metaAlias as part of the SAML response URL instead of the query parameter for PUB.

8. For Subscriber, it shows with query parameter and can be ignored.

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

Configuration on OKTA IDP Side

1. Under **Applications**, click **Create App Integration**.



2. Choose the **SAML2.0** option.

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. On the SAML setting SSO URL, provide the SSO URL of the PUB that was copied in Step 7. under 'Configuration on IDS/Cisco Side' in this document. In the Audience Uniform resource identifier (URI) (SP Entity ID) paste the SP entity under IDS trust tab on settings in the Identity service management.

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. Under the 'Other Requestable SSO URLs', enter the URL of SUB <https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp> in the given format with index value as 1.

Other Requestable SSO URLs

URL

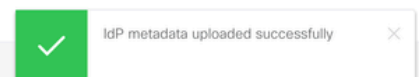
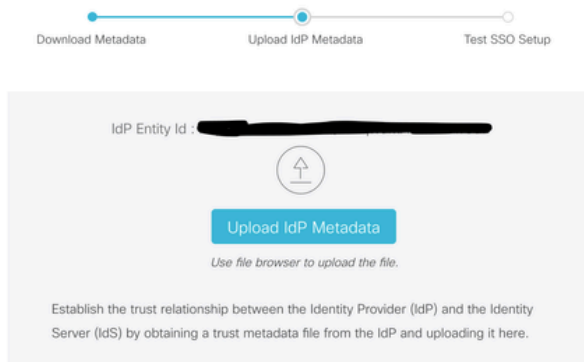
Index

[+ Add Another](#)

5. Click **Next** and **Finish** to complete the application configuration.

6. Copy the Metadata from Sign On tab using the URL and save it as **xml**.

7. Upload the Metadata from Step 6. on Identity service management webpage on CCX side.



8. Run a TEST SSO setup and it must be successful.



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. Login into the admin webpage on CCX with admin user and navigate to **System > Single Sign On**.

10. Click the **Register** button to on board the components.

On-Boarding SSO Components

i SSO components are registered successfully

Register

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

11. Assigned reporting capability to Cisco Unified CCX Administrator (assigned in Administrator Capability view) and execute CLI command **utils cuic user make-admin CCX\<Admin User Id>** to provide administrator rights in Cisco Unified Intelligence Center. Use the configured user with administrator rights for the SSO Test operation.

12. Run the SSO Test operation.

13. After the SSO Test is successful, the enable operation is allowed.

SSO Status

i Current status: SSO Mode

Enable Disable


Enable operation is allowed only after the SSO Test is successful


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

Verify

Check for login operations with agent and administrators on CCX, Cisco Unified Intelligence Center (CUIC), and Finesse. They must be successful.

When logging in agent on finesse it redirects to OKTA page.


Connecting to 
Sign in with your account to access CCXBU15



Sign In

Username

Password

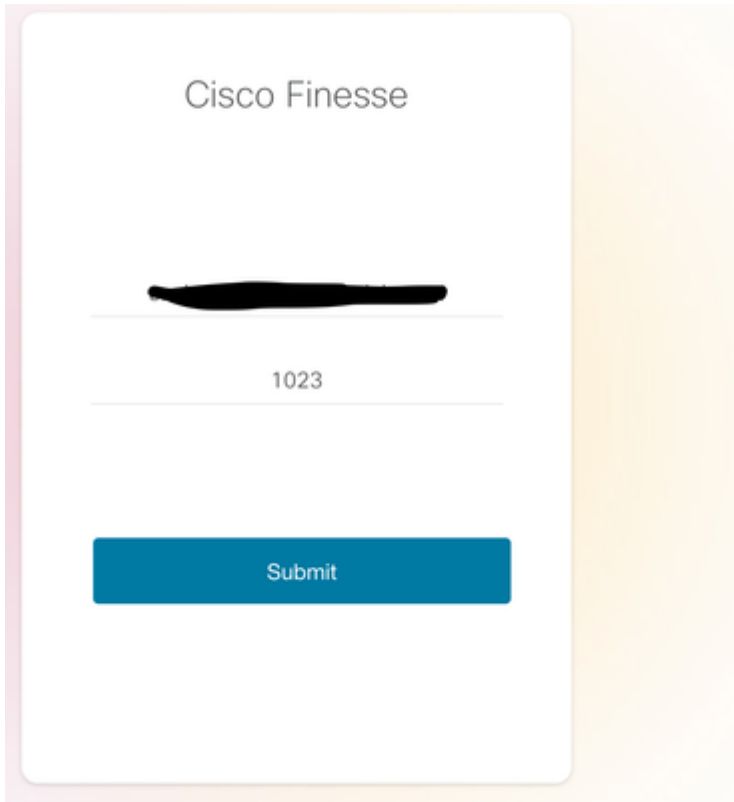
Keep me signed in

Sign in

[Forgot password?](#)

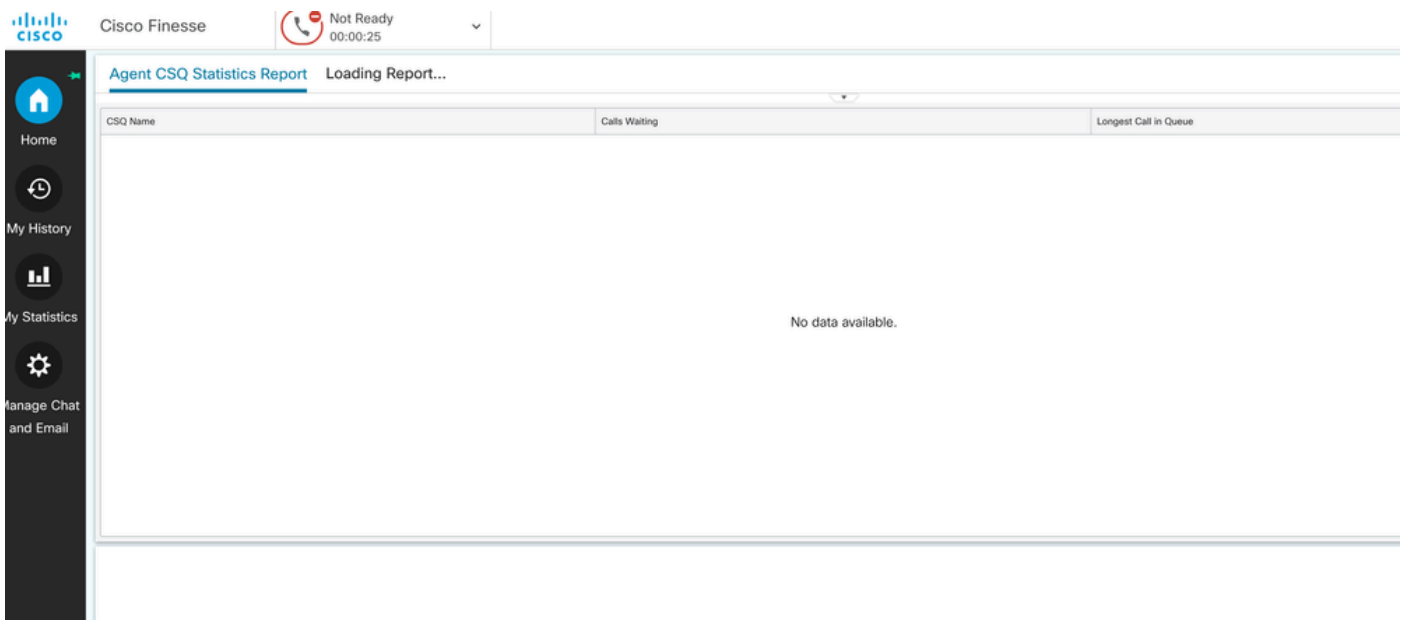
[Help](#)

After putting in the credentials, it asks for only the extension now on the finesse login page.



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 name. Underneath is another text input field containing the extension number "1023". At the bottom of the form is a blue "Submit" button.

After this is entered, the login must be successful and all live reports must be loading fine.



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 with a slash and the text "Not Ready 00:00:25". Below this is a navigation bar with "Agent CSQ Statistics Report" and "Loading Report...". The main content area is a table with columns "CSQ Name", "Calls Waiting", and "Longest Call in Queue". The table is empty, and the text "No data available." is displayed in the center.