Configuración de SSO en soluciones de Contact Center de CCX y Prem con Okta IDP

Contenido

Introducción

Este documento describe la configuración de Inicio de sesión único (SSO) con OKTA para varias soluciones de Contact Center in situ de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) o Packaged Contact Center Enterprise (PCCE)
- lenguaje de marcado de aserción de seguridad
- OKTA

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Unified Contact Center Express (UCCX) 15.0
- OKTA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración en el lado IDS/Cisco

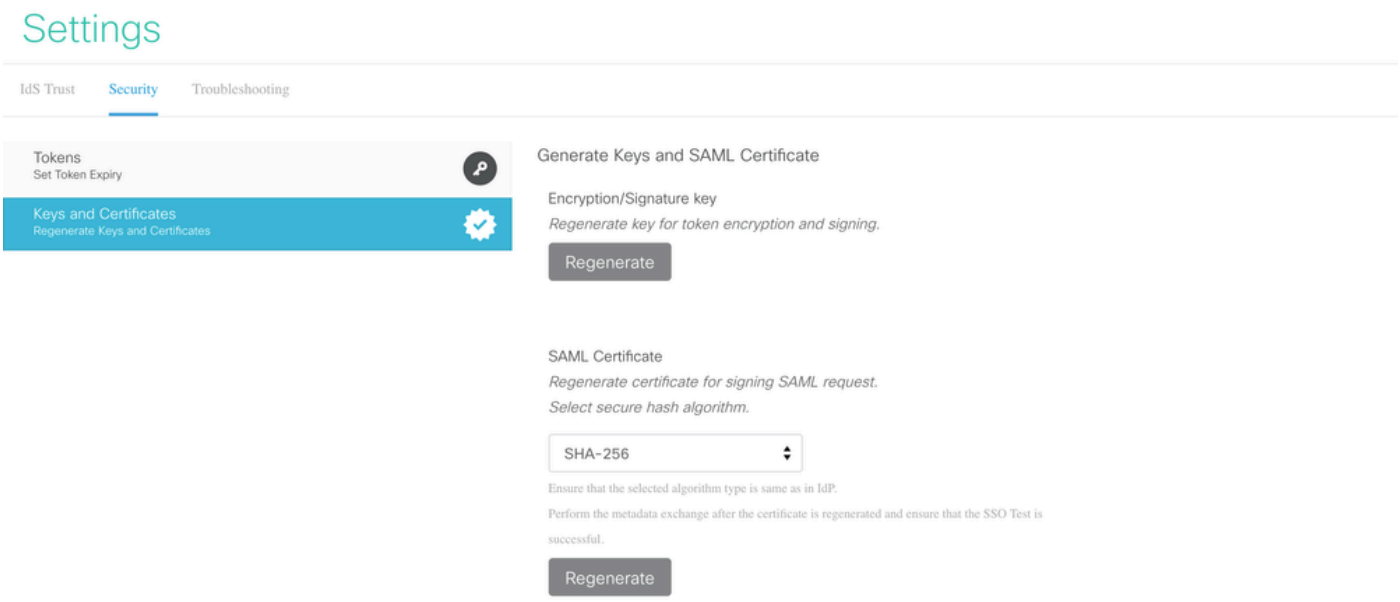
1. Ejecute el comando utils ids set_property IS_IdP_OKTA true en CLI y reinicie el servicio Identity Service (IDS).

2. Si es alta disponibilidad (HA), ejecute este comando en ambos nodos y reinicie el servicio IDS.

3. Inicie sesión en la interfaz de administración de UCCX Cisco IDS https://<dirección del servidor UCCX>:8553/idsadmin en el nodo PUB.

4. Vaya a Configuración > Seguridad > Claves y certificados.

5. Regenere el certificado de Lenguaje de marcado de aserción de seguridad (SAML).



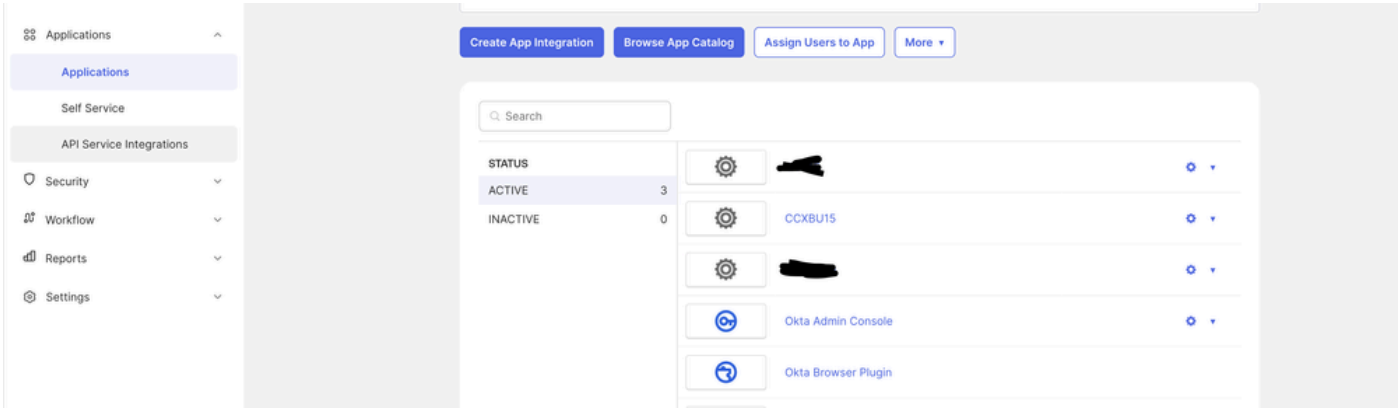
6. Desde la pestaña IDS Trust, descargue XML de metadatos SP de SAML.

7. Abra el XML de metadatos del proveedor de servicios (SP) y anote el valor del atributo 'Location' para los IDS de editor y suscriptor dentro de la etiqueta 'AssertionConsumerService'. AssertionConsumerServiceURL en los metadatos SAML ahora incluye metaAlias como parte de la URL de respuesta SAML en lugar del parámetro de consulta para PUB.

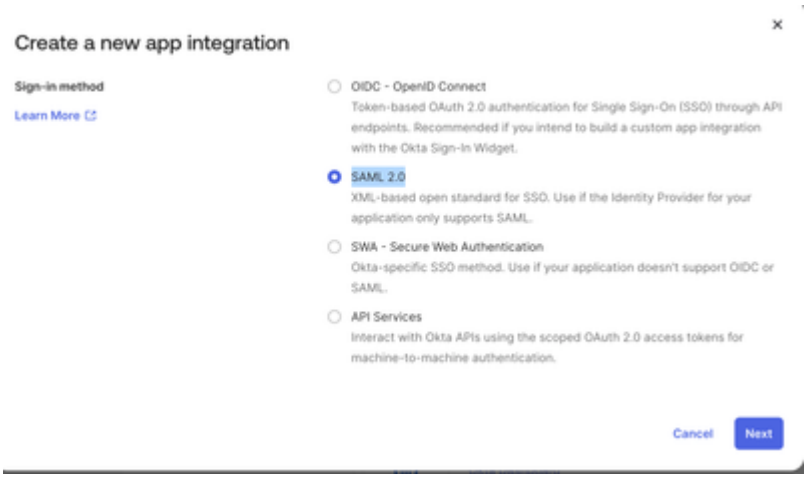
8. Para el suscriptor, se muestra con el parámetro de consulta y se puede ignorar.

Configuración en el lado OKTA IDP

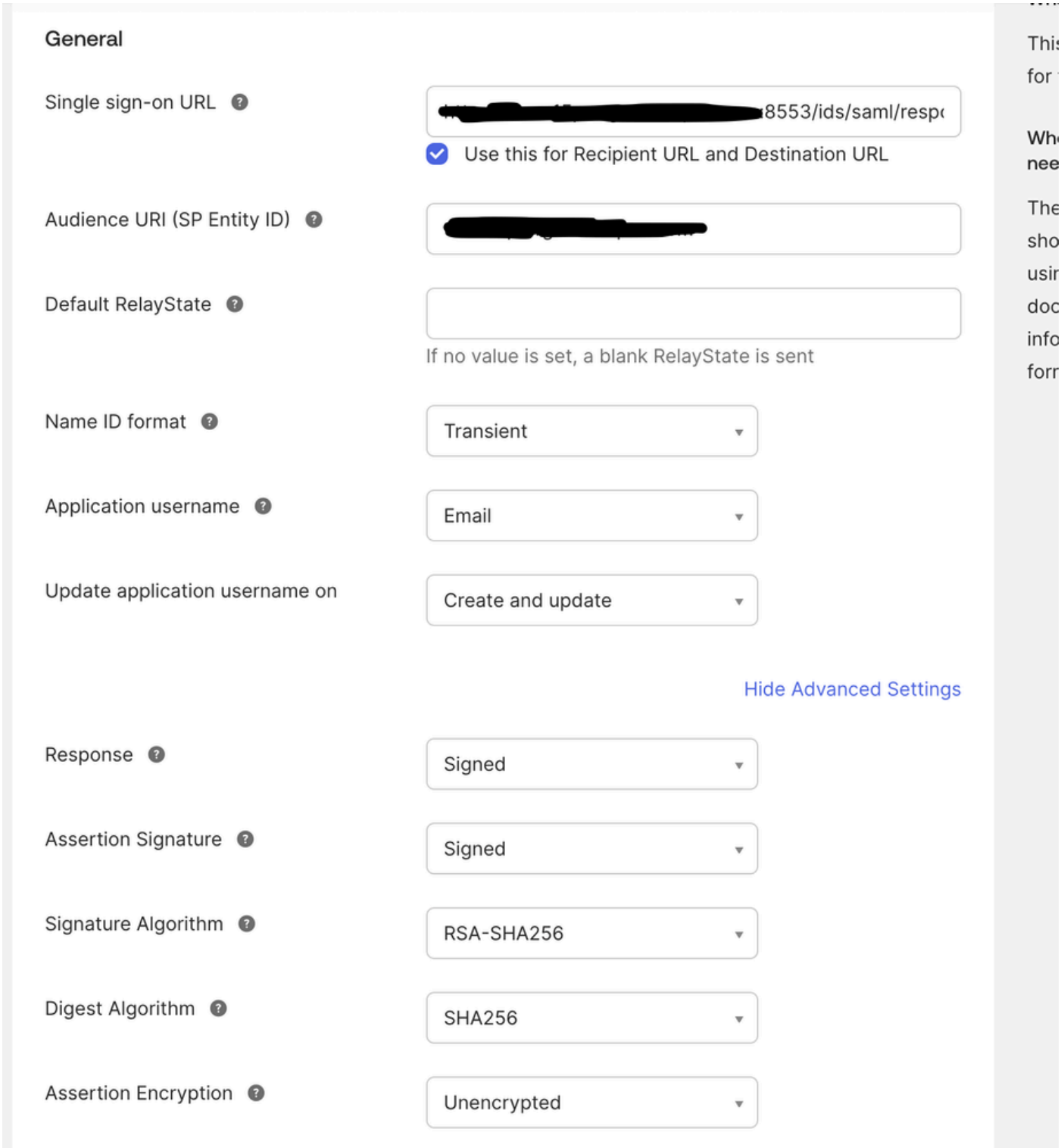
1. En Aplicaciones, haga clic en Crear integración de aplicaciones.



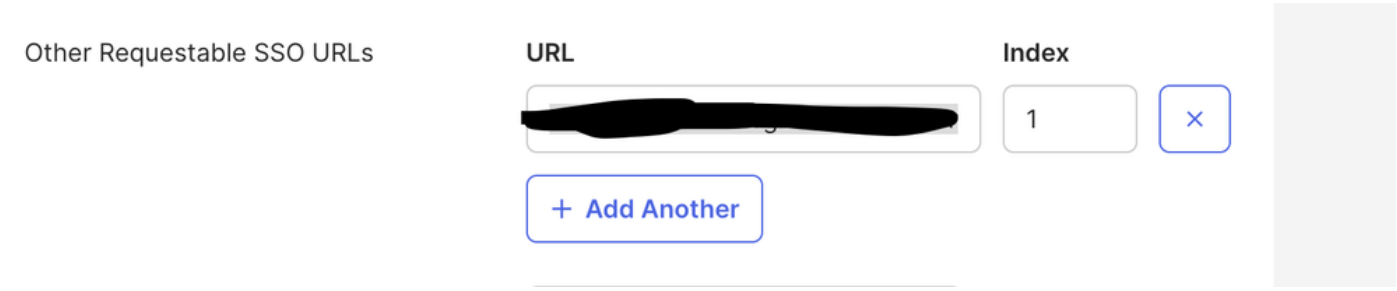
2. Seleccione la opción SAML2.0.



3. En la URL SSO de configuración SAML, proporcione la URL SSO del PUB que se copió en el paso 7. en "Configuración en el lado IDS/Cisco" en este documento. En el identificador uniforme de recursos (URI) (ID de entidad SP) de Audience, pegue la entidad SP en la ficha de confianza IDS en la configuración de la administración de Identity Service.



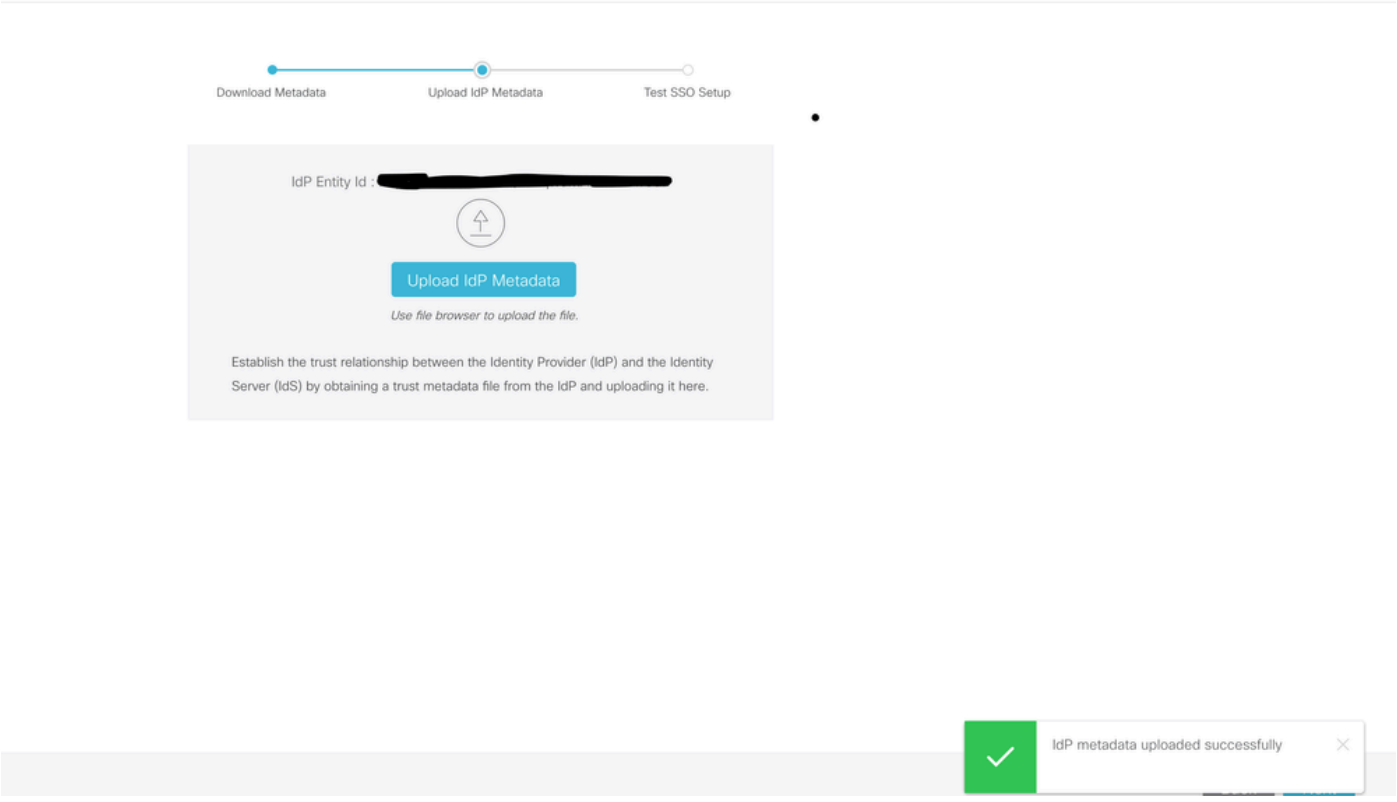
4. En "Otras URL de SSO solicitables", introduzca la URL de SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp en el formato especificado con el valor de índice como 1.



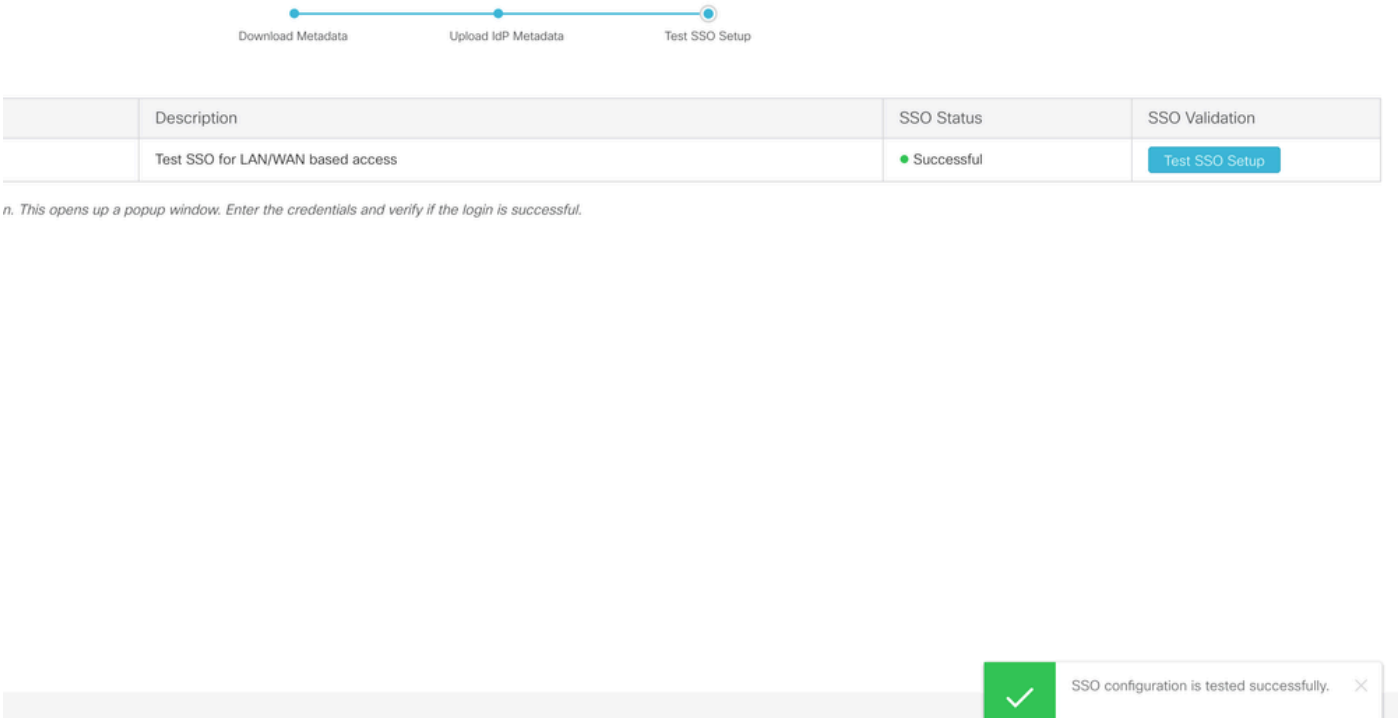
5. Haga clic en Next y Finish para completar la configuración de la aplicación.

6. Copie los metadatos de la ficha Iniciar sesión mediante la URL y guárdelos como xml.

7. Cargue los metadatos del paso 6 en la página web de gestión de servicios de identidad en el lado de CCX.

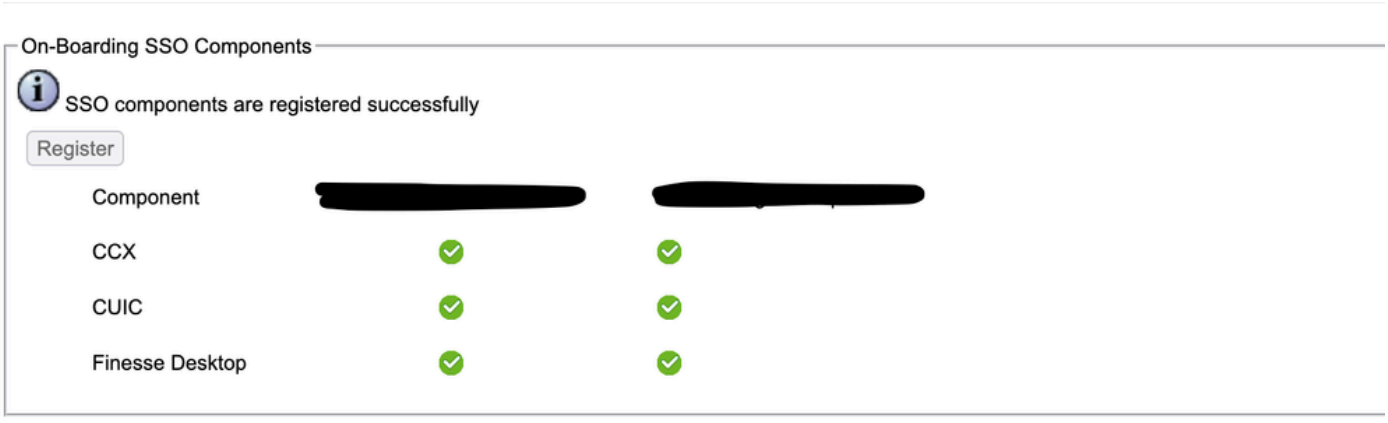


8. Ejecute una configuración TEST SSO y debe ser exitosa.



9. Inicie sesión en la página web de administración en CCX con el usuario administrador y navegue hasta Sistema > Inicio de sesión único.

10. Haga clic en el botón Register para incorporar los componentes.



11. Capacidad de generación de informes asignada al administrador de Cisco Unified CCX (asignada en la vista de capacidad del administrador) y ejecución del comando CLI utils cuic user make-admin CCX\<Admin User Id> para proporcionar derechos de administrador en Cisco Unified Intelligence Center. Utilice el usuario configurado con derechos de administrador para la operación de prueba de SSO.

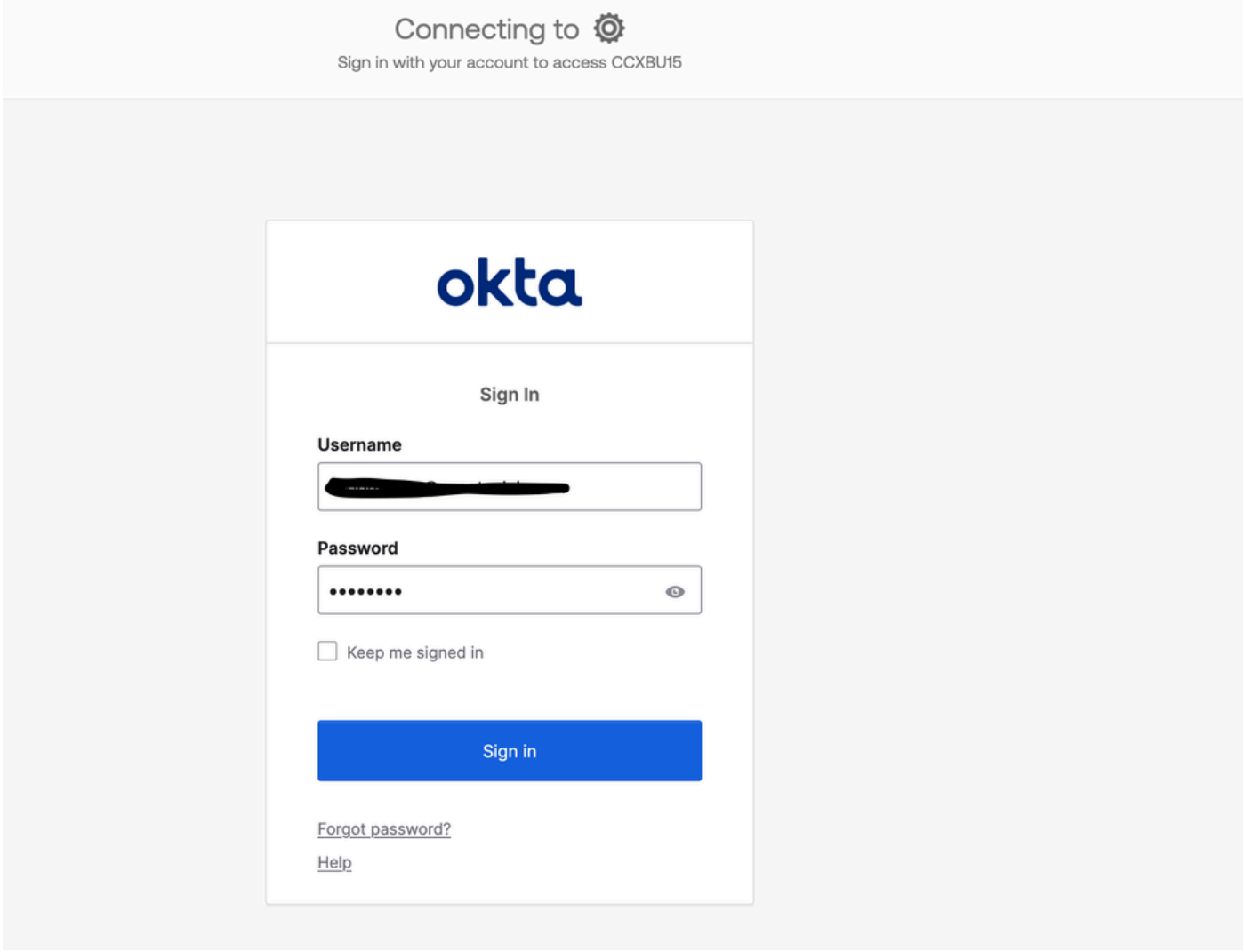
12. Ejecute la operación de prueba de SSO.

13. Una vez que la prueba de SSO se ha realizado correctamente, se permite la operación de activación.

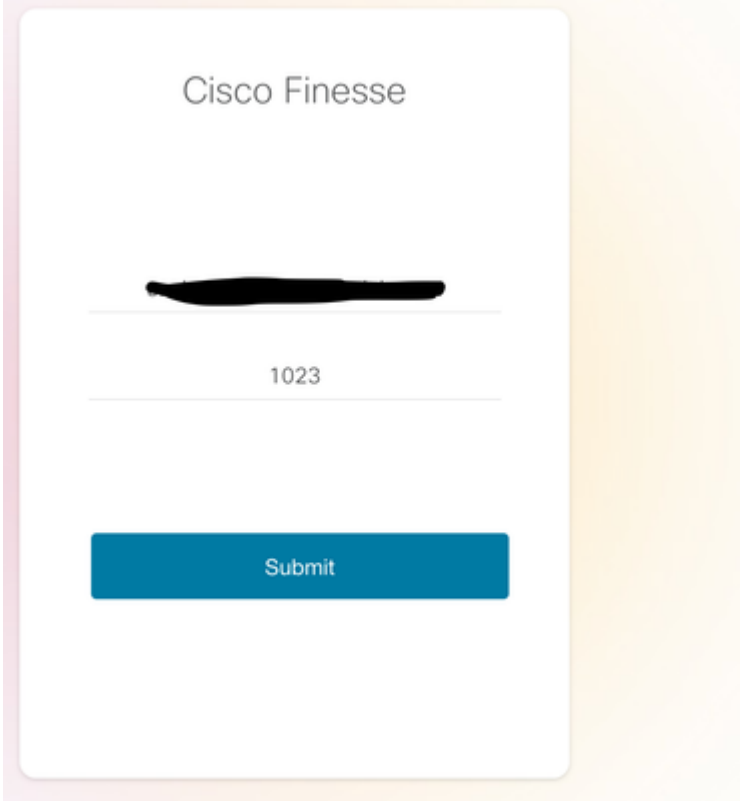
Verificación

Compruebe las operaciones de inicio de sesión con agentes y administradores en CCX, Cisco Unified Intelligence Center (CUIC) y Finesse. Deben tener éxito.

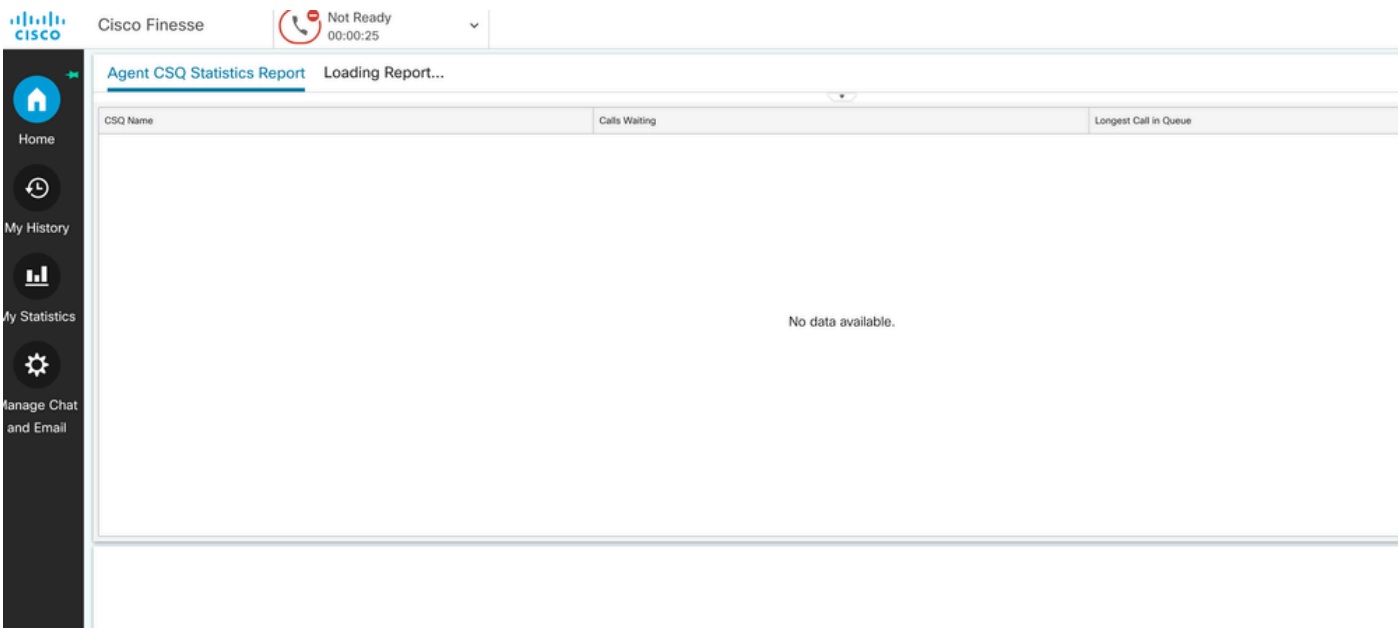
Al iniciar sesión en el agente en finesse se redirige a la página OKTA.



Después de poner en las credenciales, se pide solo la extensión ahora en la página de inicio de sesión finesse.



Una vez introducido esto, el inicio de sesión debe realizarse correctamente y todos los informes en directo deben cargarse correctamente.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).