Konfigurieren von SSO auf CCX- und Prem Contact Center-Lösungen mit Okta IDP

Inhalt

Einleitung

In diesem Dokument wird die Single Sign On (SSO)-Konfiguration mit OKTA für verschiedene Cisco On Prem Contact Center-Lösungen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Unified Contact Center Express (UCCX) 15.0
- OKTA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration auf IDS/Cisco Seite

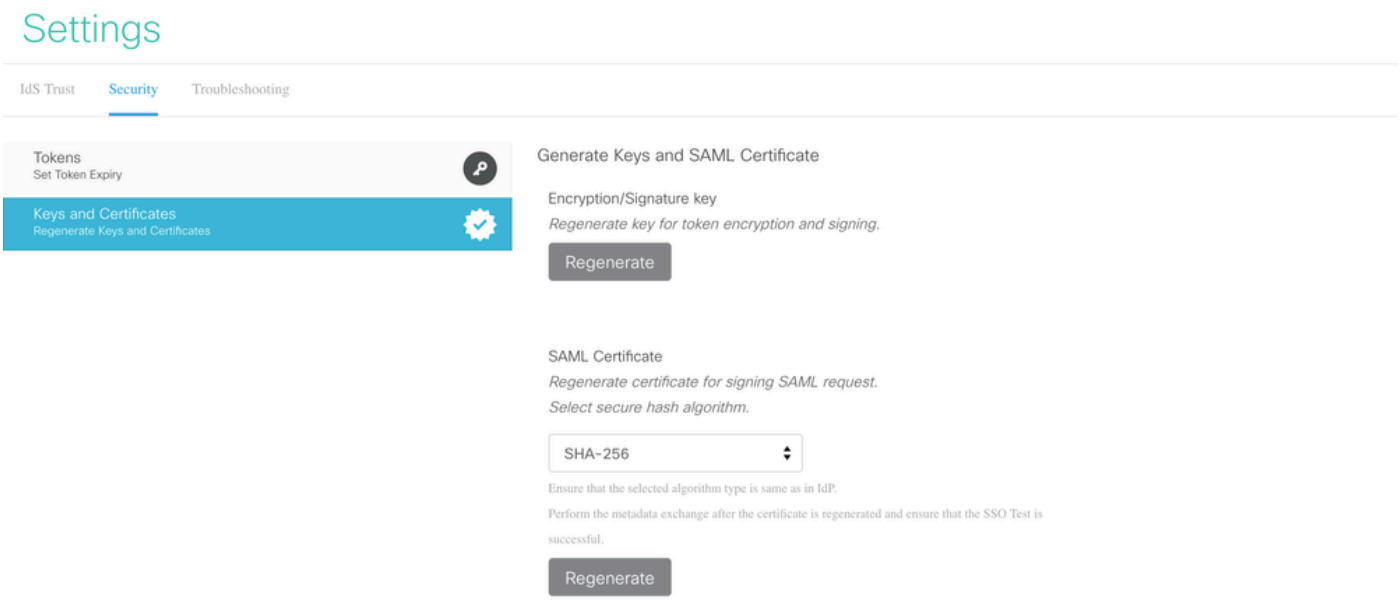
1. Führen Sie den Befehl utils ids set_property IS_IdP_OKTA true für CLI aus, und starten Sie den Identity Service (IDS)-Dienst neu.

2. Wenn High Availability (HA), dann führen Sie diesen Befehl auf beiden Knoten und starten Sie IDS-Dienst neu.

3. Melden Sie sich bei der UCCX Cisco IDS-Admin-Schnittstelle https://<UCCX-Serveradresse>:8553/idsadmin auf dem PUB-Knoten an.

4. Navigieren Sie zu Einstellungen > Sicherheit > Schlüssel und Zertifikate.

5. Generieren Sie das SAML-Zertifikat (Security Assertion Markup Language) neu.



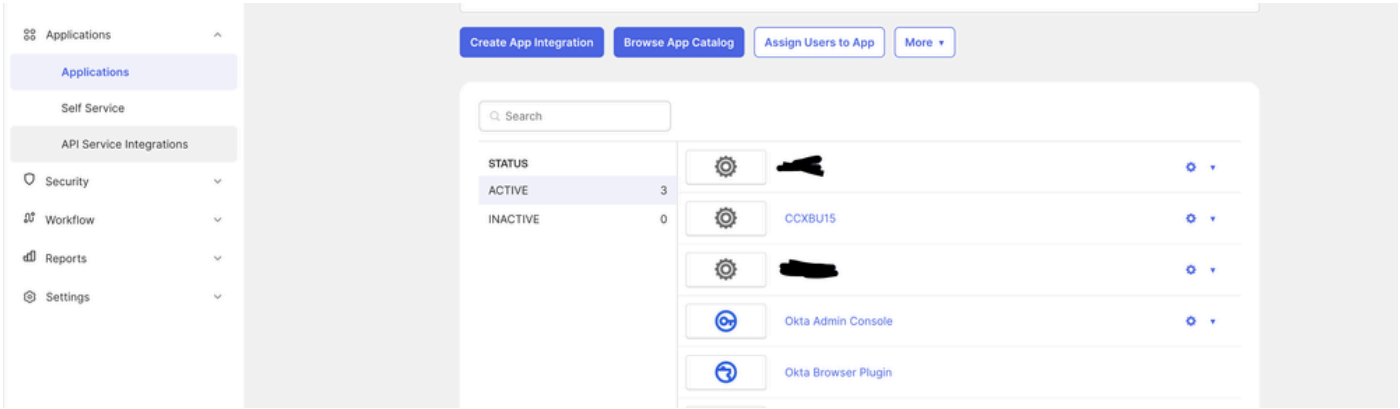
6. Laden Sie auf der Registerkarte IDS Trust SAML SP-Metadaten-XML herunter.

7. Öffnen Sie Service Provider (SP)-Metadaten-XML, und notieren Sie sich den Wert des Attributs 'Location' für Publisher- und Subscriber-IDS innerhalb des AssertionConsumerService-Tags. Die AssertionConsumerServiceURL in SAML-Metadaten enthält jetzt metaAlias als Teil der SAML-Antwort-URL anstelle des Abfrageparameters für PUB.

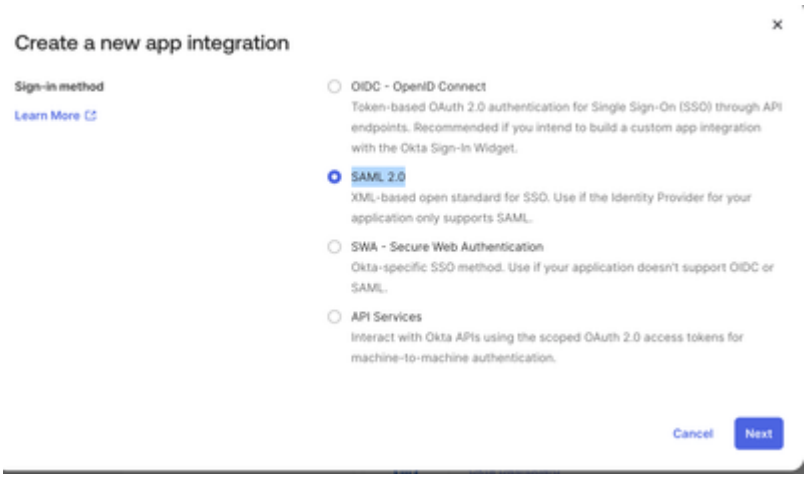
8. Für Abonnent wird dies mit Abfrageparametern angezeigt und kann ignoriert werden.

Konfiguration auf OKTA IDP-Seite

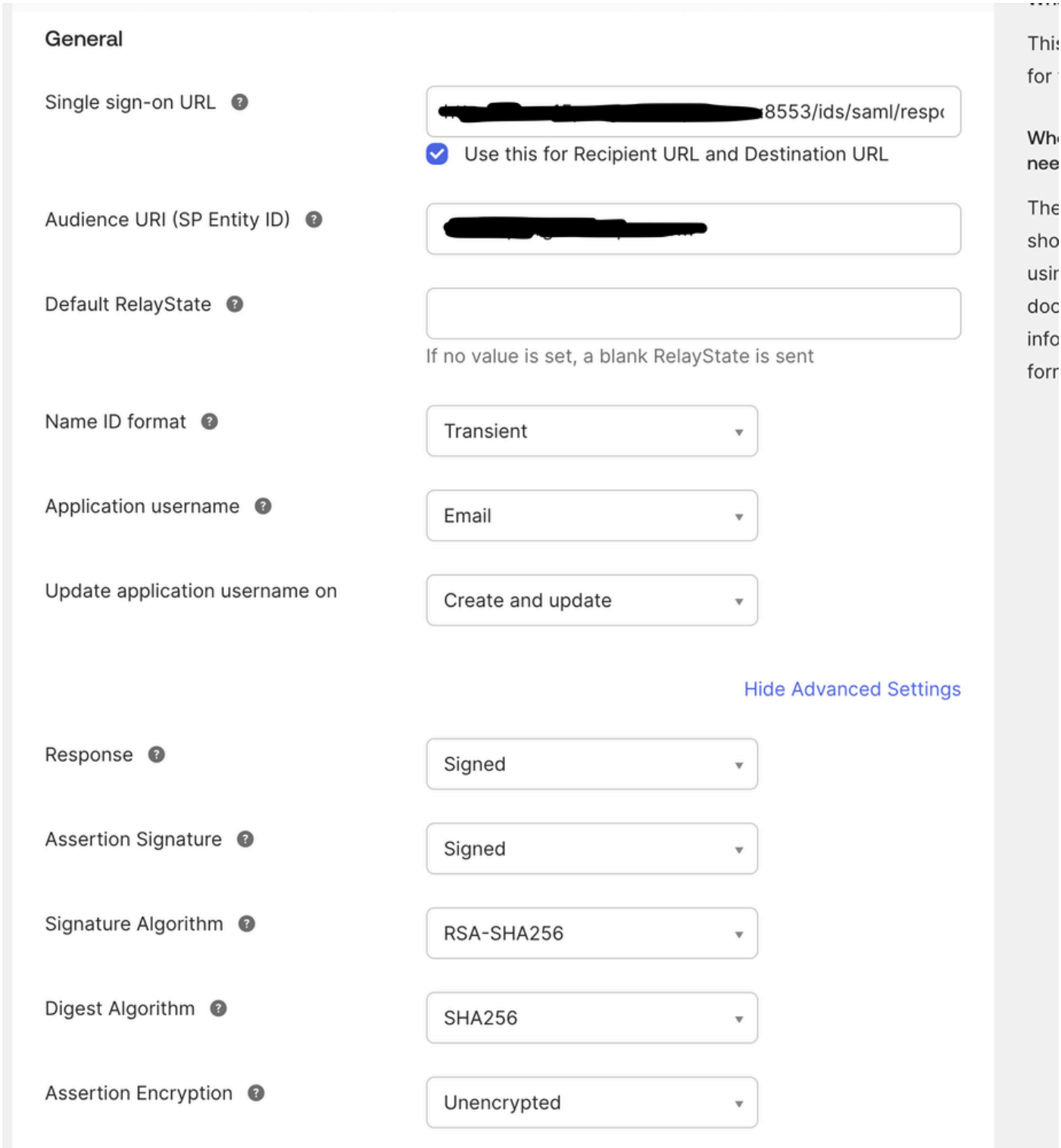
1. Klicken Sie unter Anwendungen auf Anwendungsintegration erstellen.



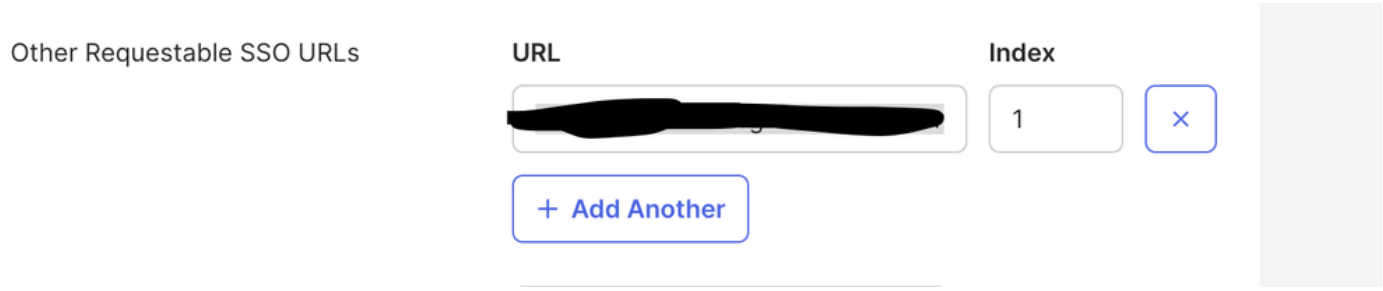
2. Wählen Sie die Option SAML2.0.



3. Geben Sie auf der SSO-URL der SAML-Einstellung die SSO-URL der PUB an, die in Schritt 7 unter "Konfiguration auf IDS/Cisco-Seite" in dieses Dokument kopiert wurde. Fügen Sie die SP-Einheit im URI (Audience Uniform Resource Identifier) (SP Entity ID) unter der Registerkarte IDS trust (IDS-Vertrauenswürdigkeit) in die Einstellungen im Identity Service Management ein.



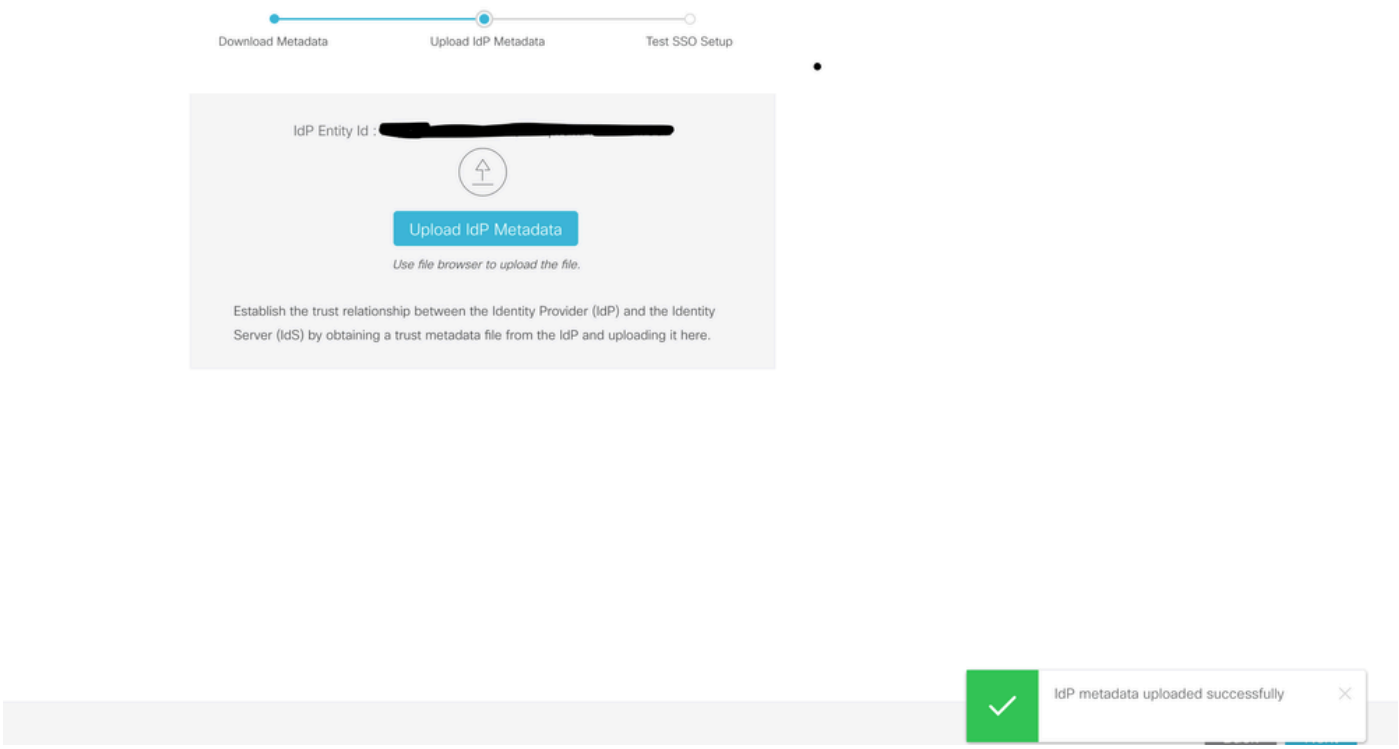
4. Geben Sie unter "Other Requestable SSO URLs" (Andere anforderbare SSO-URLs) die URL von SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp im angegebenen Format mit dem Indexwert 1 ein.



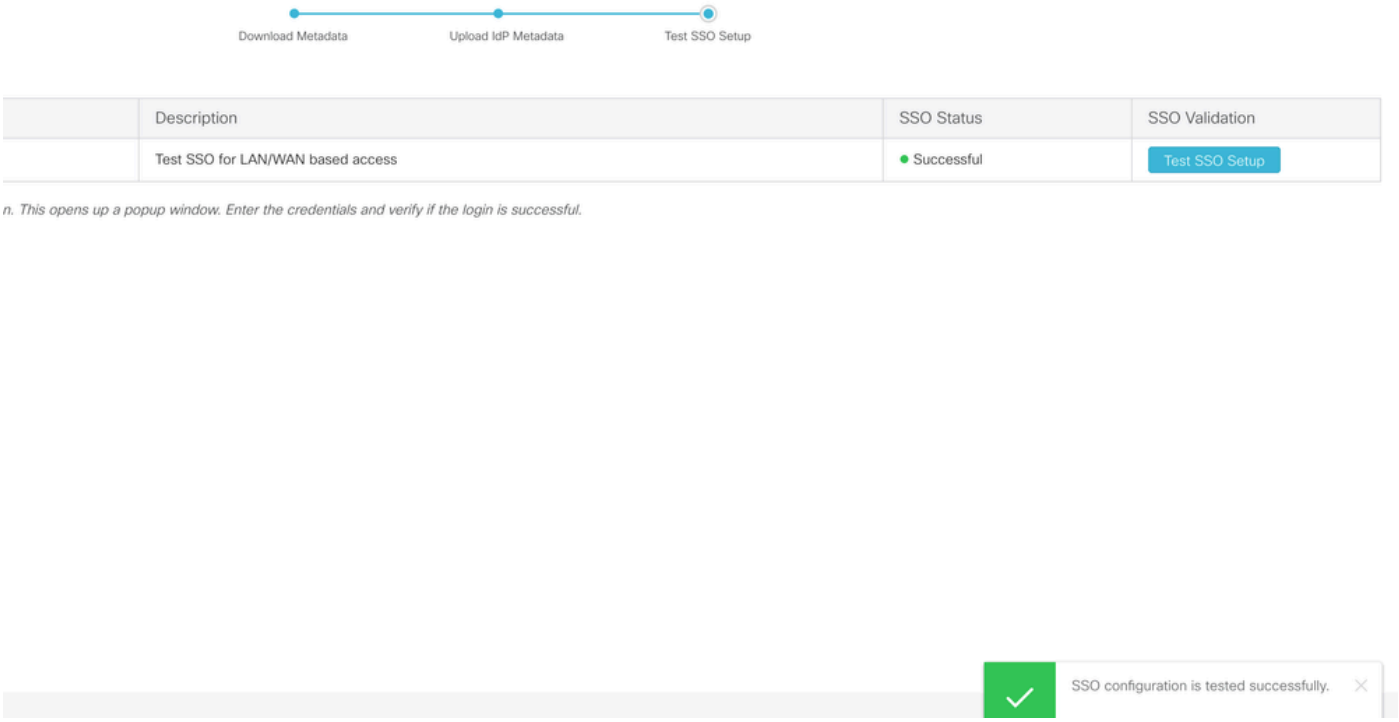
5. Klicken Sie auf Weiter und Beenden, um die Anwendungskonfiguration abzuschließen.

6. Kopieren Sie die Metadaten aus der Registerkarte Anmelden mit der URL und speichern Sie sie als XML.

7. Laden Sie die Metadaten aus Schritt 6 auf die Webseite für das Identity Service Management auf CCX-Seite hoch.

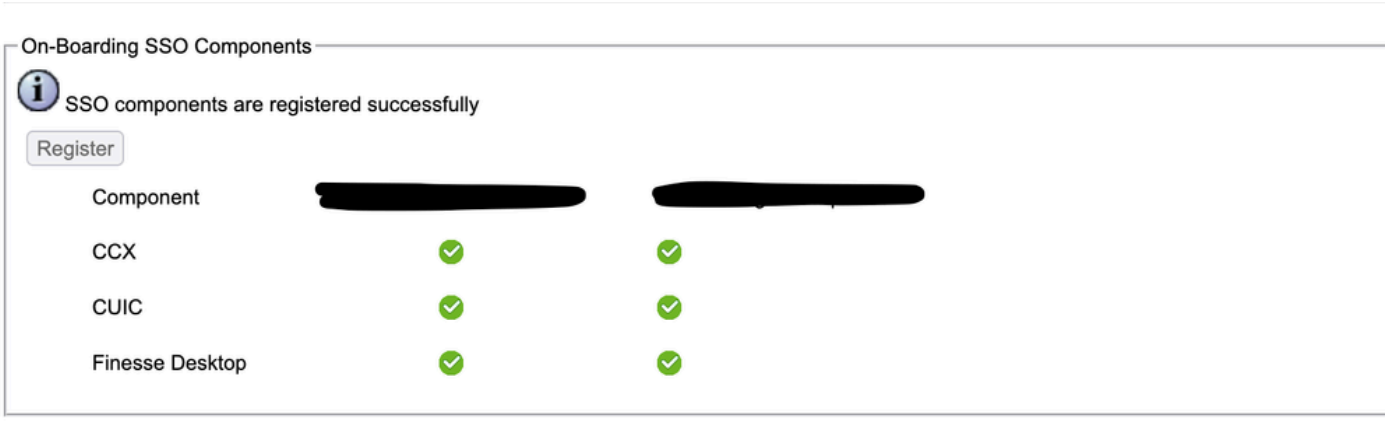


8. Führen Sie ein TEST SSO-Setup aus, und es muss erfolgreich sein.



9. Melden Sie sich mit dem Admin-Benutzer bei der Admin-Webseite auf CCX an, und navigieren Sie zu System > Single Sign On.

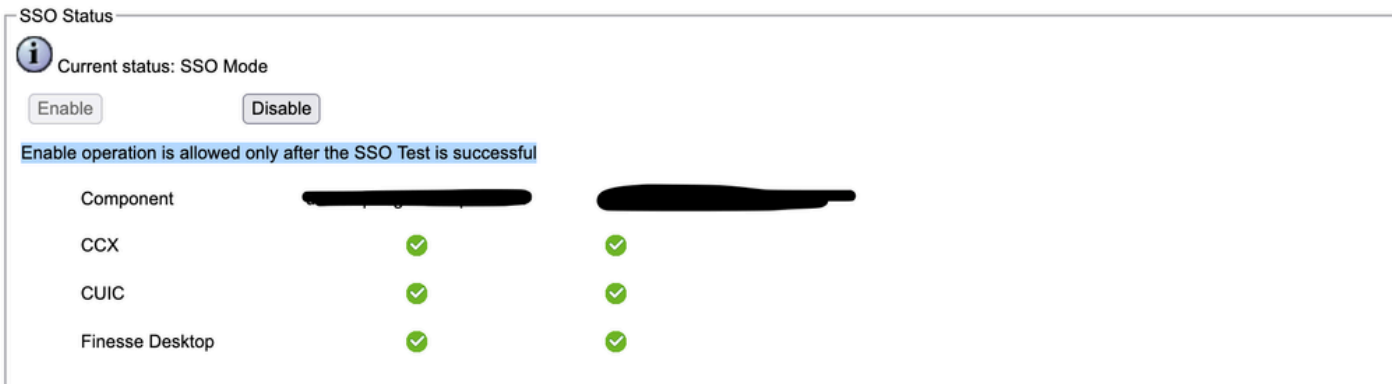
10. Klicken Sie auf die Schaltfläche Registrieren, um die Komponenten einzubinden.



11. Cisco Unified CCX Administrator (in der Ansicht "Administrator Capability" (Administratorfunktion) zugewiesen) wurde eine Berichtsfunktion zugewiesen, und die CLI-Befehle werden mit cuic user make-admin CCX\<Admin User Id> ausgeführt, um Administratorrechte in Cisco Unified Intelligence Center bereitzustellen. Verwenden Sie den konfigurierten Benutzer mit Administratorrechten für den SSO-Testvorgang.

12. Führen Sie den SSO-Testvorgang aus.

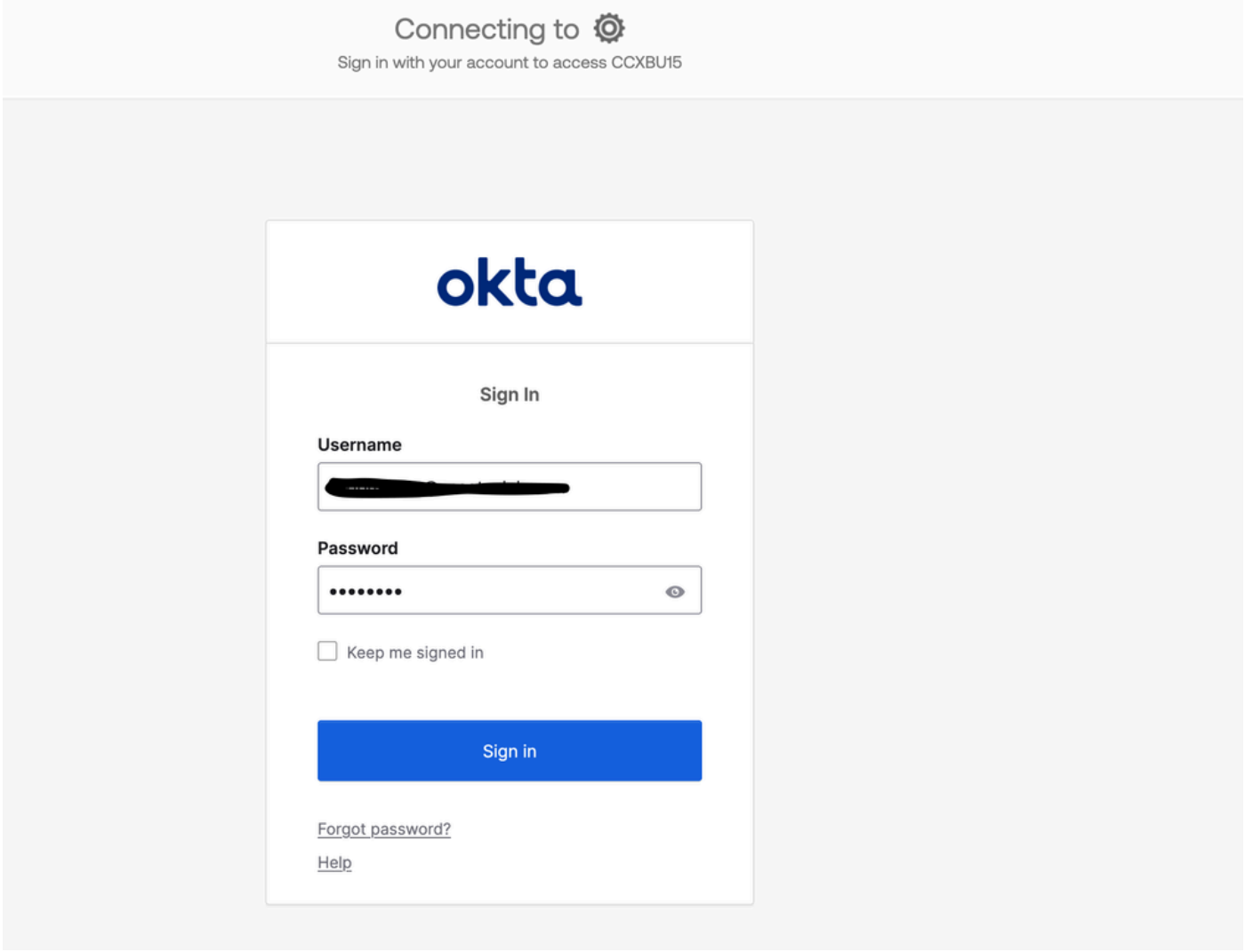
13. Nach erfolgreichem SSO-Test ist der Aktivierungsvorgang zulässig.



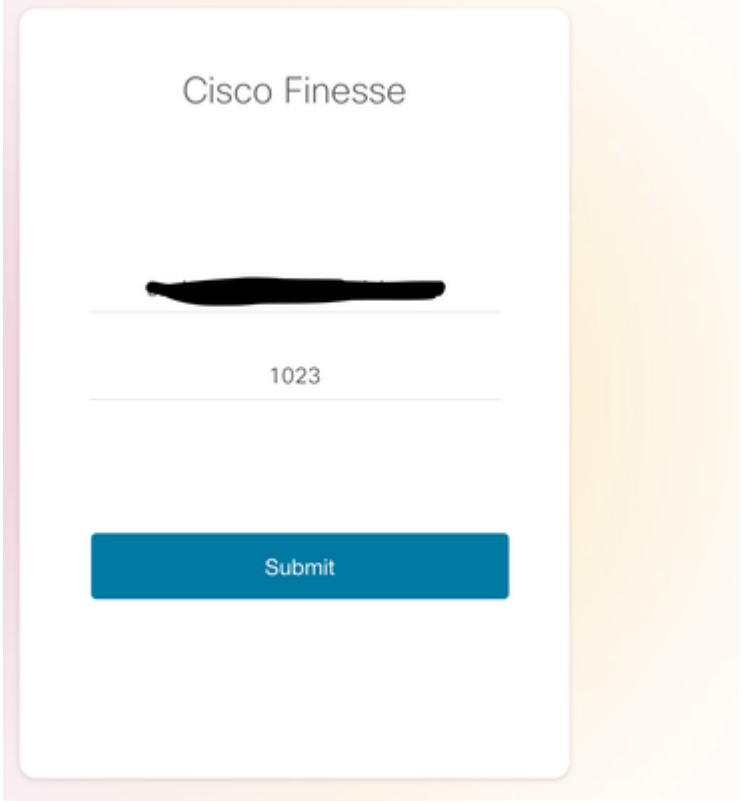
Überprüfung

Suchen Sie nach Anmeldevorgängen mit Agenten und Administratoren für CCX, Cisco Unified Intelligence Center (CUIC) und Finesse. Sie müssen erfolgreich sein.

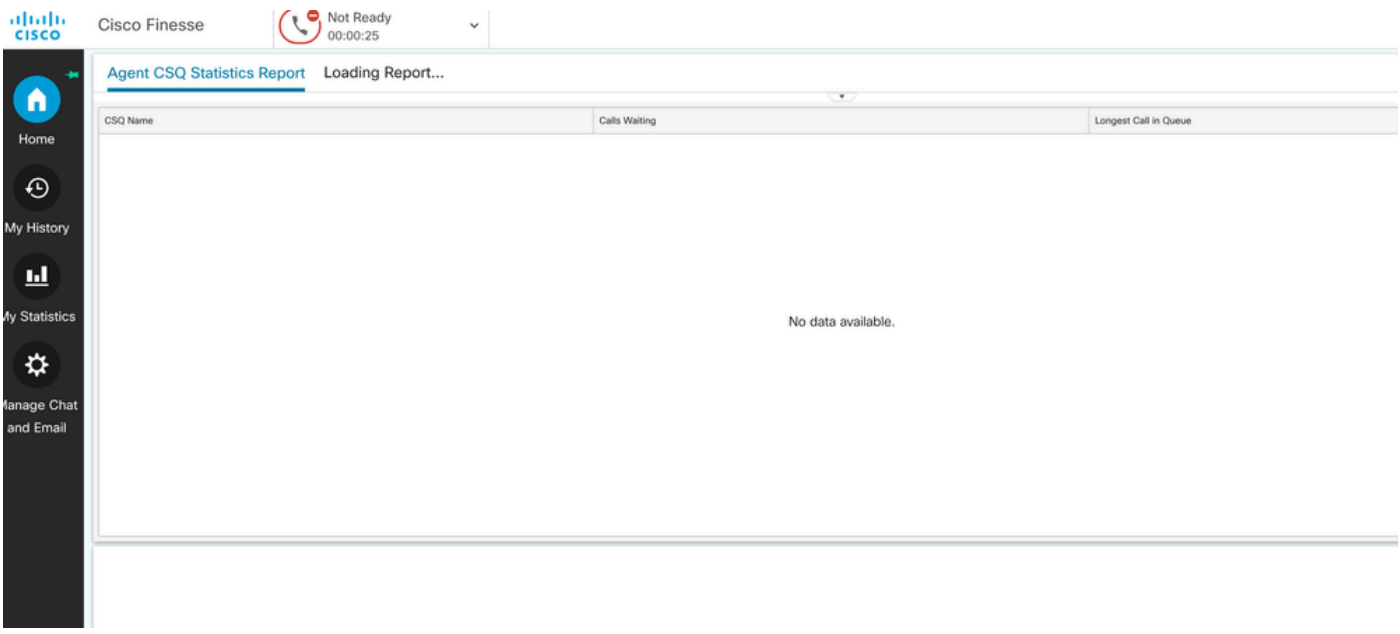
Bei der Anmeldung Agent auf Finesse wird auf die OKTA-Seite umgeleitet.



Nach der Eingabe der Anmeldeinformationen, fragt es nur für die Erweiterung jetzt auf der Finesse-Anmeldeseite.



Nach der Eingabe muss die Anmeldung erfolgreich sein, und alle Live-Berichte müssen ordnungsgemäß geladen werden.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.