Configurer SSO sur les solutions CCX et Prem Contact Center avec Okta IDP

Table des matières

Introduction

Ce document décrit la configuration de l'authentification unique (SSO) avec OKTA pour diverses solutions de centre de contacts Cisco On Prem.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) ou Packaged Contact Center Enterprise (PCCE)
- langage de balisage des assertions de sécurité
- OKTA

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration côté IDS/Cisco

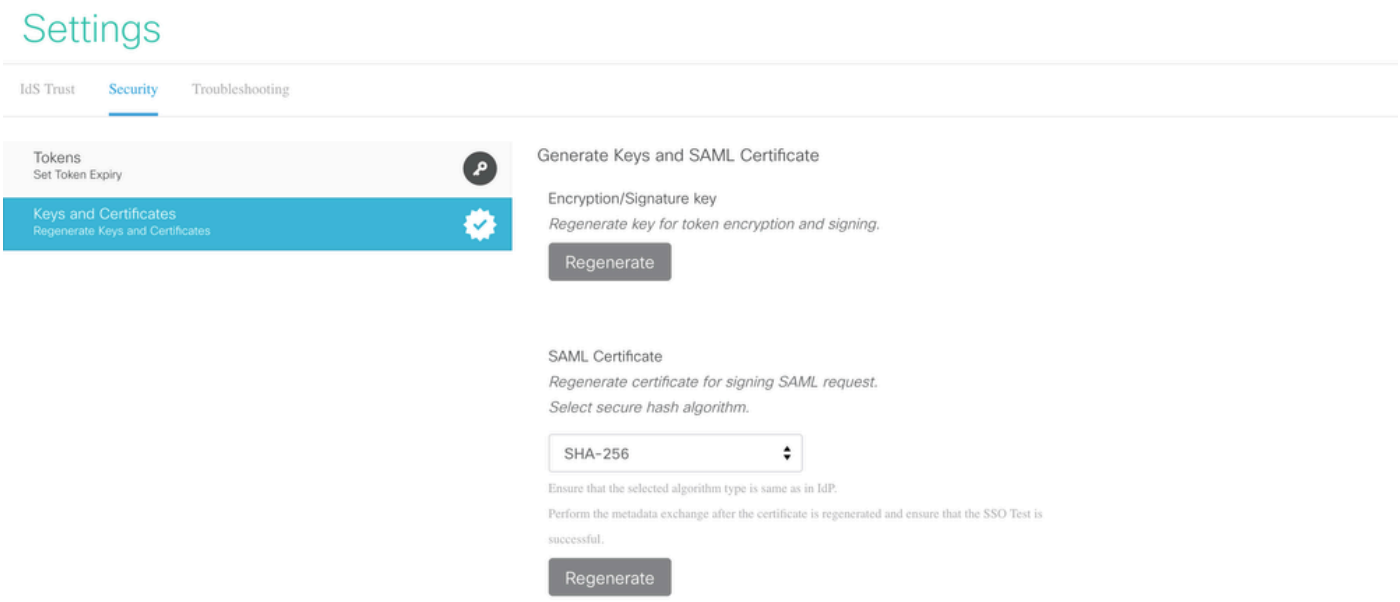
1. Exécutez la commande utils ids set_property IS_IdP_OKTA true sur CLI et redémarrez le service Identity Service (IDS).

2. Si la haute disponibilité (HA), exécutez cette commande sur les deux noeuds et redémarrez le service IDS.

3. Connectez-vous à l'interface d'administration Cisco IDS UCCX https://<adresse du serveur UCCX>:8553/idsadmin sur le noeud PUB.

4. Accédez à Paramètres > Sécurité > Clés et certificats.

5. Régénérer le certificat SAML (Security Assertion Markup Language).



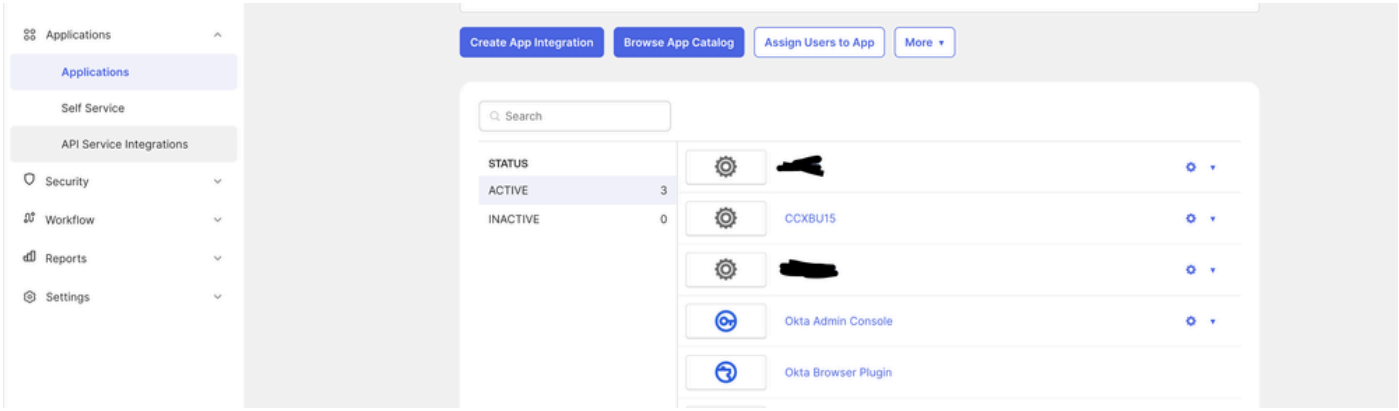
6. Dans l'onglet IDS Trust, téléchargez le fichier XML de métadonnées SAML SP.

7. Ouvrez le fichier XML de métadonnées du fournisseur de services (SP) et notez la valeur de l'attribut « Location » pour les ID de l'éditeur et de l'abonné dans la balise « AssertionConsumerService ». L'AssertionConsumerServiceURL dans les métadonnées SAML inclut maintenant metaAlias comme partie de l'URL de réponse SAML au lieu du paramètre de requête pour PUB.

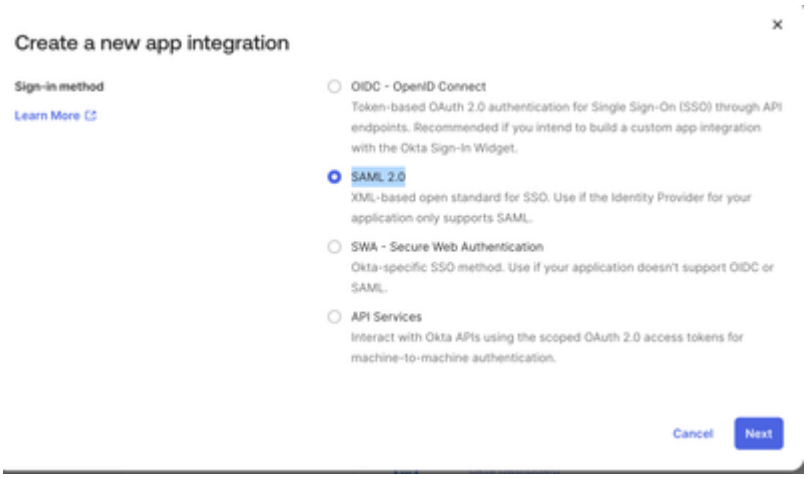
8. Pour l'Abonné, il s'affiche avec le paramètre de requête et peut être ignoré.

Configuration côté OKTA IDP

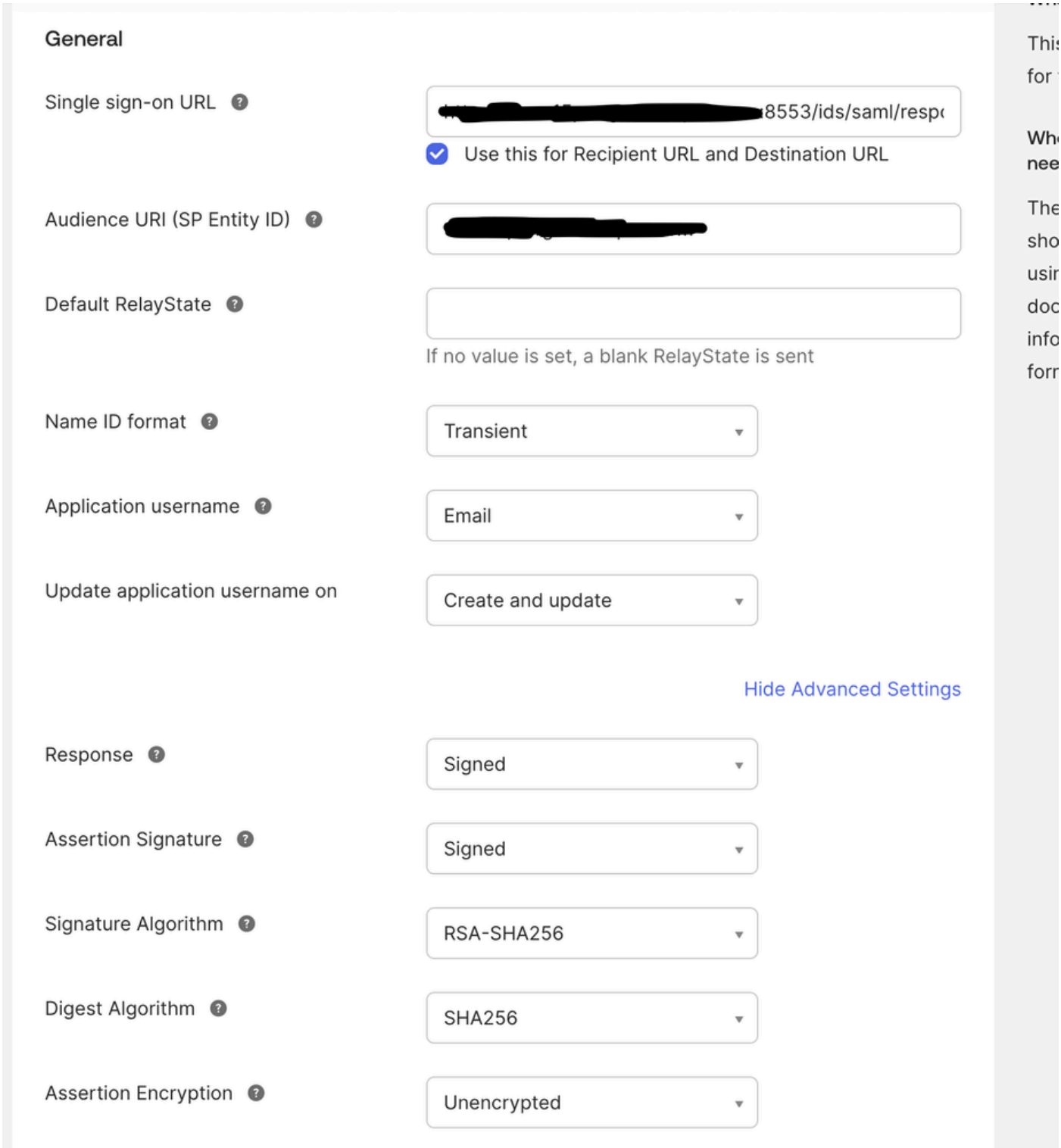
1. Sous Applications, cliquez sur Create App Integration.



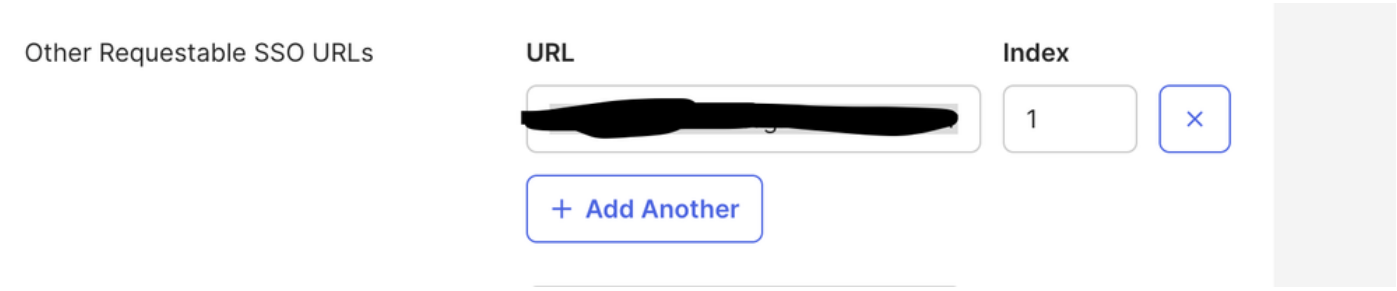
2. Sélectionnez l'option SAML2.0.



3. Sur le paramètre SAML SSO URL, fournissez l'URL SSO du PUB qui a été copié à l'étape 7. sous 'Configuration côté IDS/Cisco' dans ce document. Dans l'URI (Uniform resource identifier) d'auditoire (SP Entity ID), collez l'entité SP sous l'onglet de confiance IDS sur les paramètres de la gestion du service d'identité.



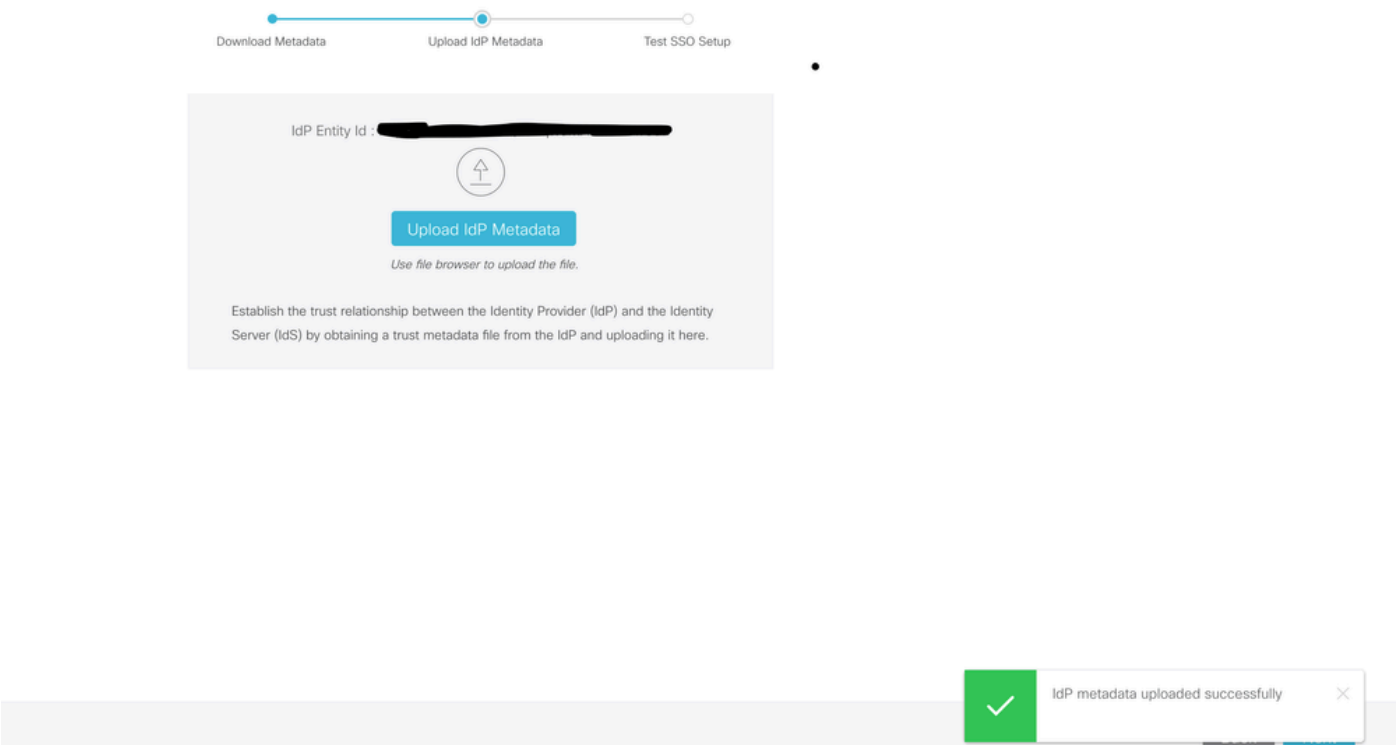
4. Sous 'Other Requestable SSO URLs', entrez l'URL de SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp dans le format donné avec la valeur d'index 1.



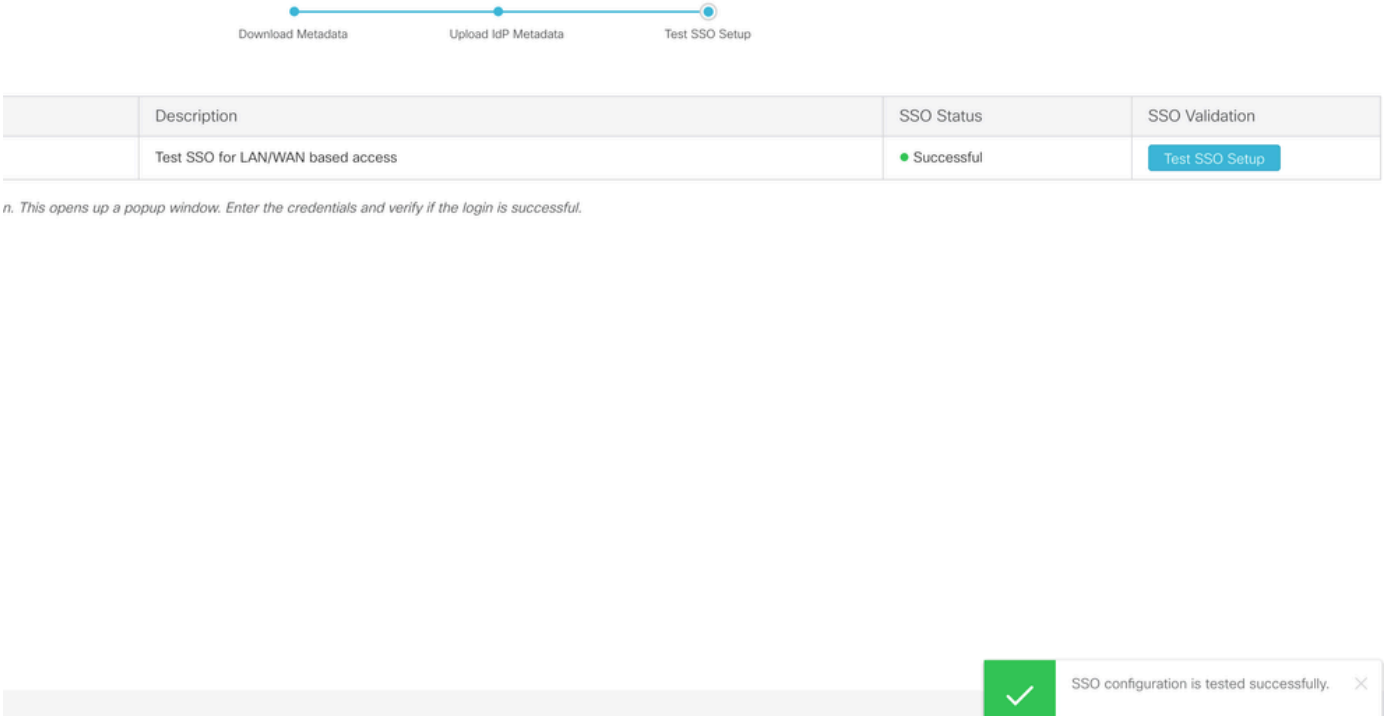
5. Cliquez sur Next et sur Finish pour terminer la configuration de l'application.

6. Copiez les métadonnées de l'onglet Connexion à l'aide de l'URL et enregistrez-les au format xml.

7. Téléchargez les métadonnées à partir de l'étape 6. sur la page Web de gestion des services d'identité côté CCX.

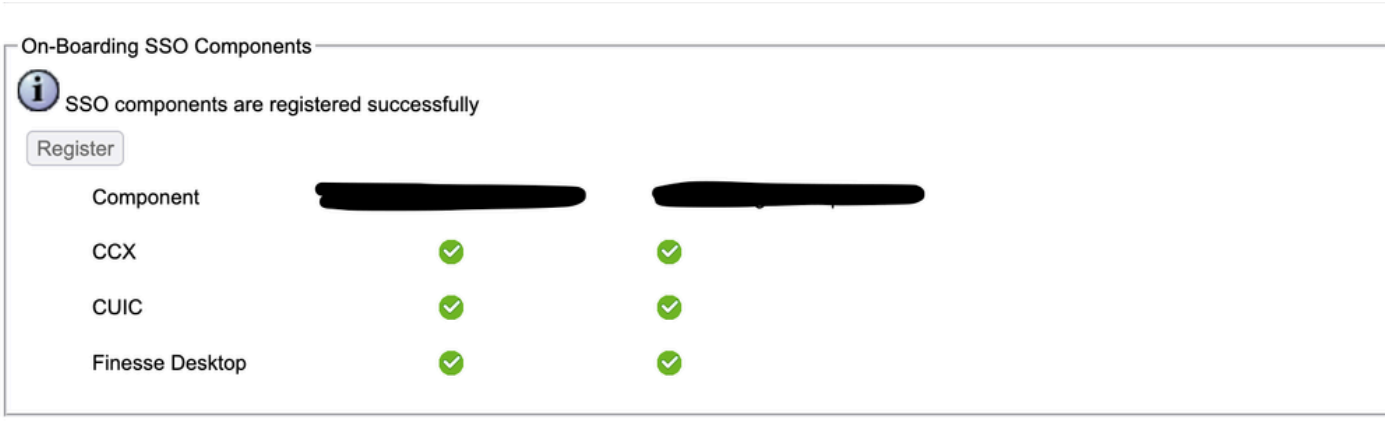


8. Exécutez une configuration TEST SSO et elle doit aboutir.



9. Connectez-vous à la page Web admin sur CCX avec l'utilisateur admin et naviguez jusqu'à System > Single Sign On.

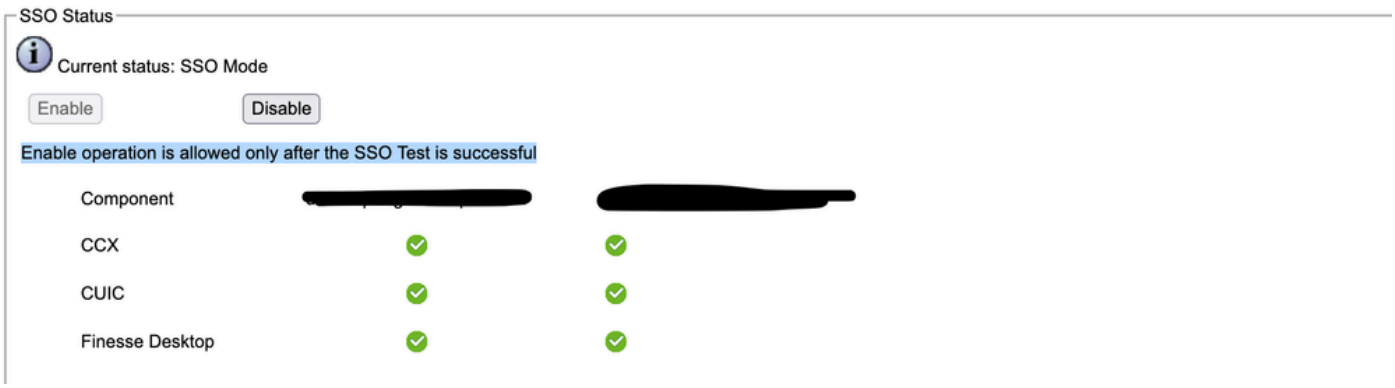
10. Cliquez sur le bouton Register pour intégrer les composants.



11. Attribution d'une fonction de création de rapports à Cisco Unified CCX Administrator (attribuée dans la vue Administrator Capability) et exécution de la commande CLI utilise cuic user make-admin CCX\<Admin User Id> pour fournir des droits d'administrateur dans Cisco Unified Intelligence Center. Utilisez l'utilisateur configuré avec des droits d'administrateur pour l'opération de test SSO.

12. Exécutez l'opération de test SSO.

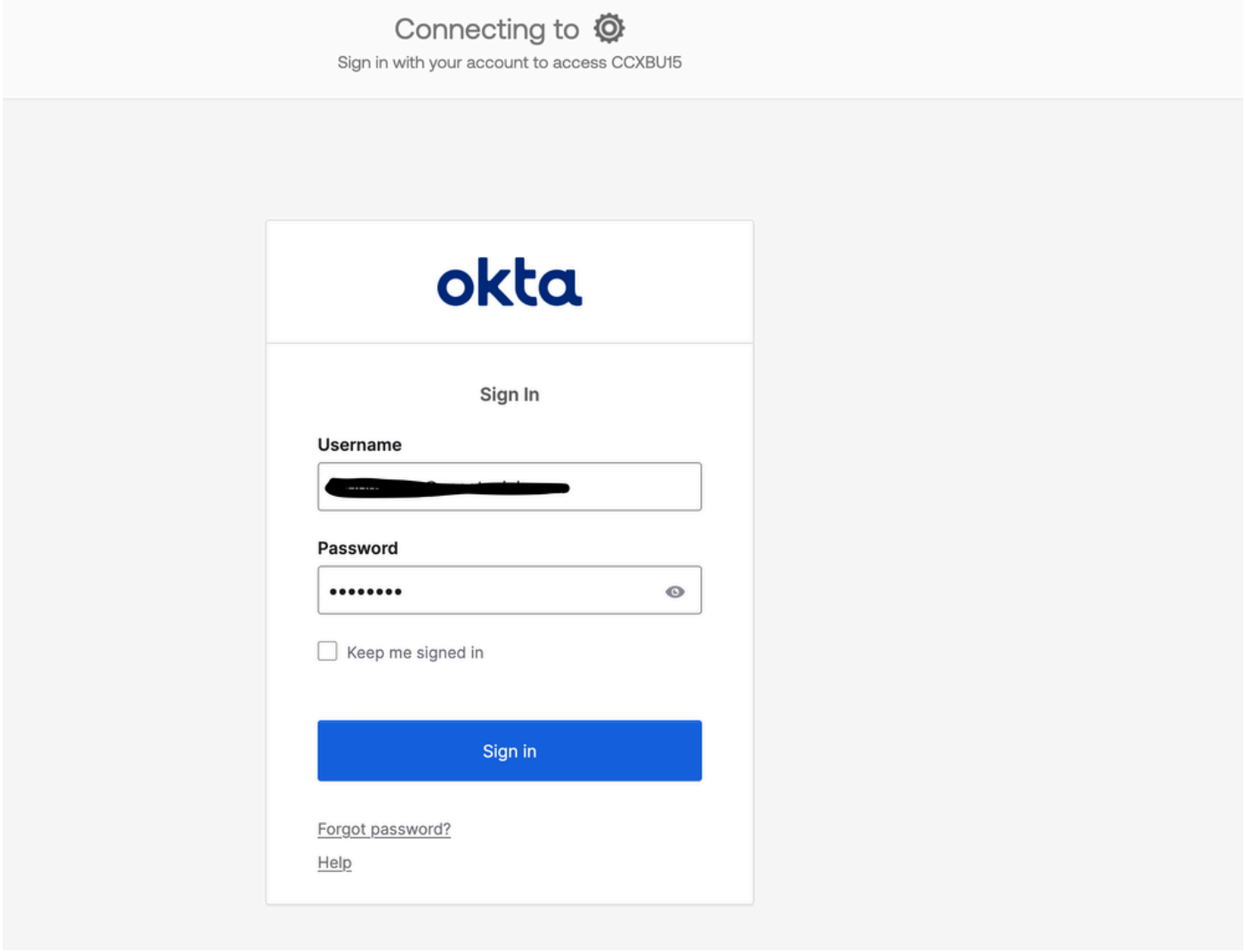
13. Une fois le test SSO réussi, l’opération d’activation est autorisée.



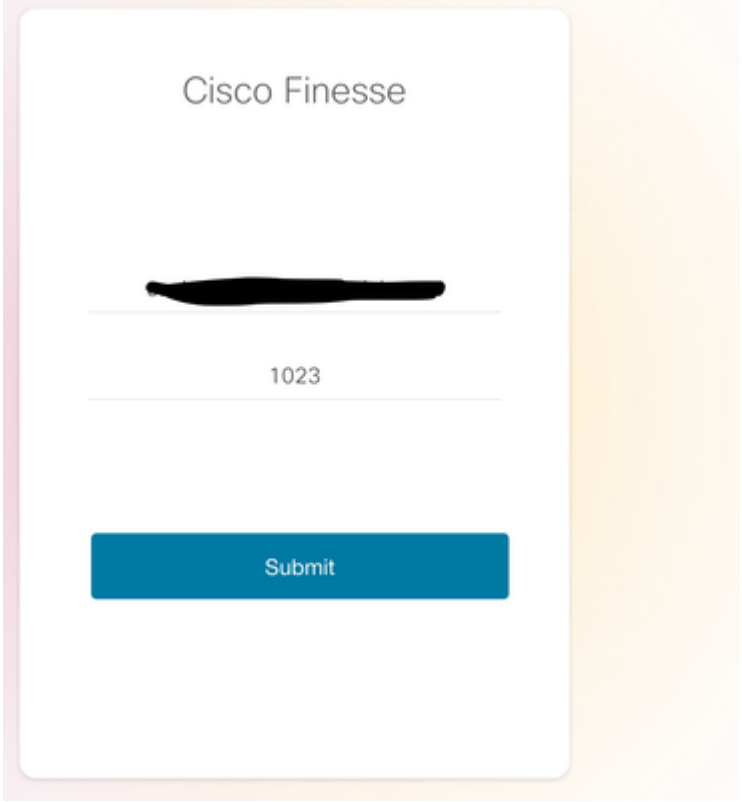
Vérifier

Vérifiez les opérations de connexion avec les agents et les administrateurs sur CCX, Cisco Unified Intelligence Center (CUIC) et Finesse. Ils doivent réussir.

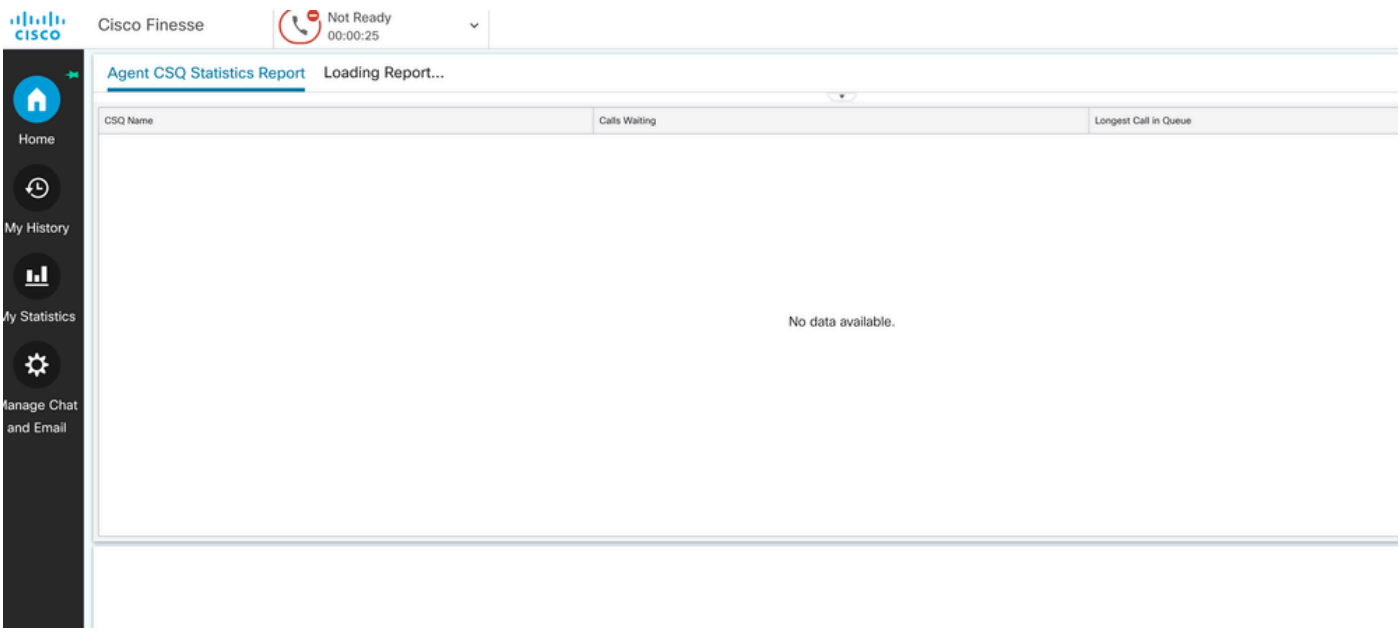
Lors de la connexion de l'agent sur finesse, il redirige vers la page OKTA.



Après avoir saisi les informations d'identification, il ne demande que l'extension maintenant sur la page de connexion finesse.



Une fois cette valeur saisie, la connexion doit aboutir et tous les rapports en direct doivent être correctement chargés.



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.