Configurazione di SSO su CCX e delle soluzioni per contact center principali con Okta IDP

Sommario

Introduzione

Questo documento descrive la configurazione di Single Sign On (SSO) con OKTA per diverse soluzioni Cisco On Prem Contact Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Unified contact center express (UCCX) 15.0
- OKTA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione su IDS/Cisco Side

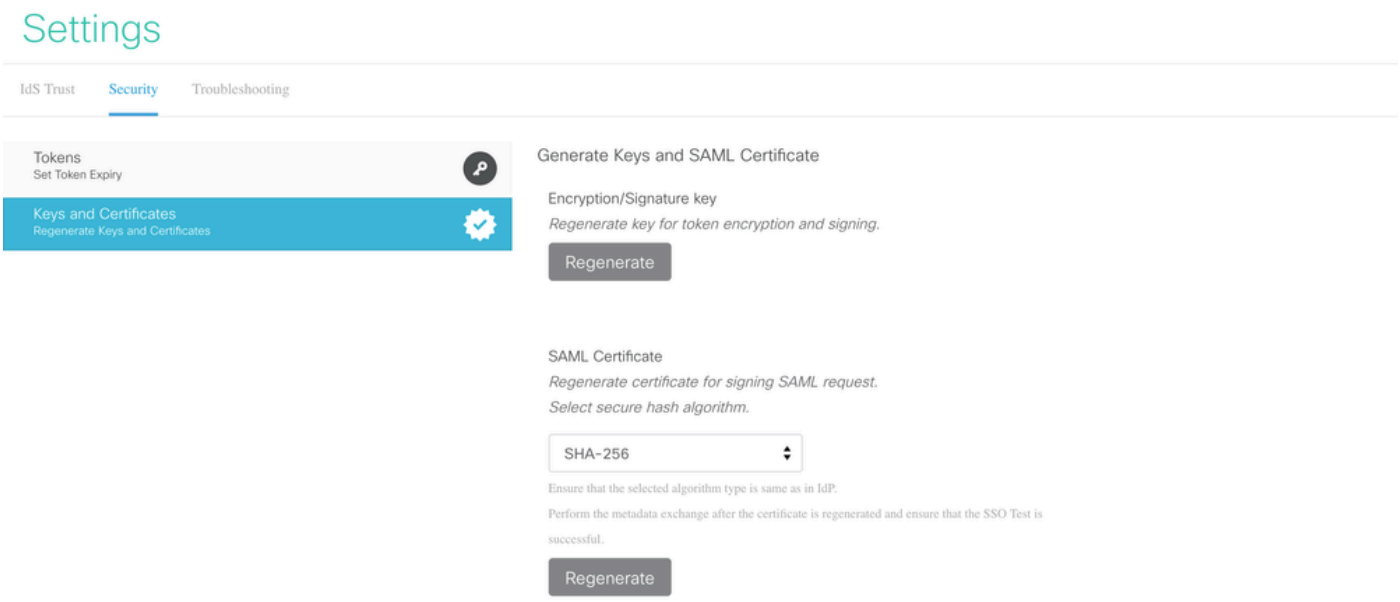
1. Eseguire il comando utilizza ids set_property IS_IdP_OKTA true sulla CLI e riavviare il servizio Identity Service (IDS).

2. Se High Availability (HA), eseguire questo comando su entrambi i nodi e riavviare il servizio IDS.

3. Accedere all'interfaccia di amministrazione di UCCX Cisco IDS https://<UCCX server address>:8553/idsadmin sul nodo PUB.

4. Passare a Impostazioni > Protezione > Chiavi e certificati.

5. Rigenerare il certificato SAML (Security Assertion Markup Language).



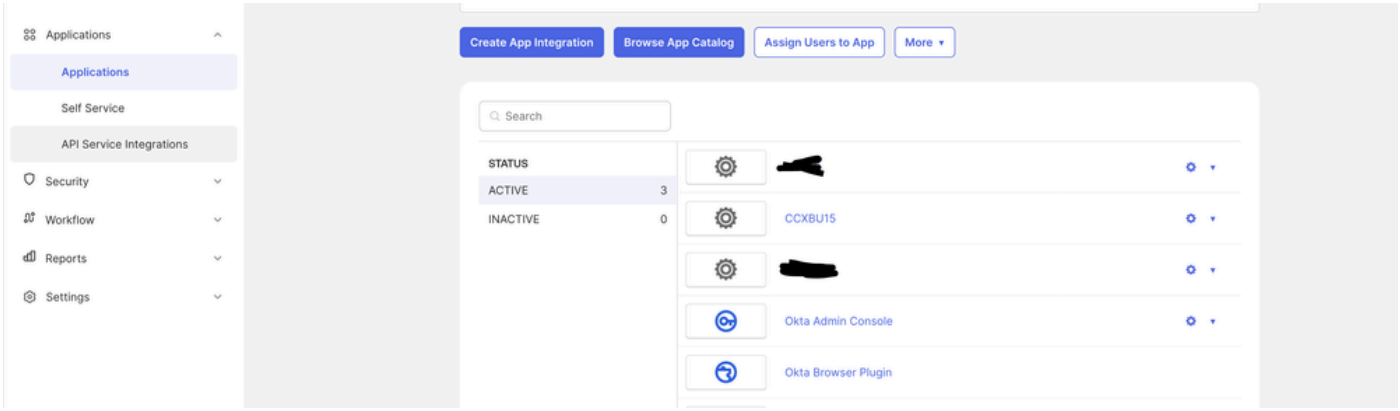
6. Dalla scheda IDS Trust, scaricare SAML SP metadata XML.

7. Aprire il file XML dei metadati del provider di servizi (SP) e prendere nota del valore dell'attributo 'Location' per gli ID del server di pubblicazione e del sottoscrittore all'interno del tag 'AssertionConsumerService'. L'oggetto AssertionConsumerServiceURL nei metadati SAML include ora metaAlias come parte dell'URL di risposta SAML anziché il parametro di query per PUB.

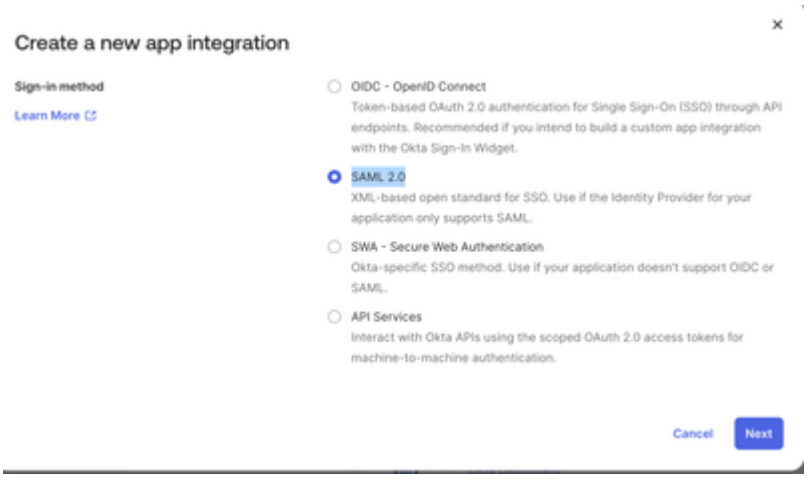
8. Per il Sottoscrittore, viene visualizzato con il parametro query e può essere ignorato.

Configurazione su OKTA IDP Side

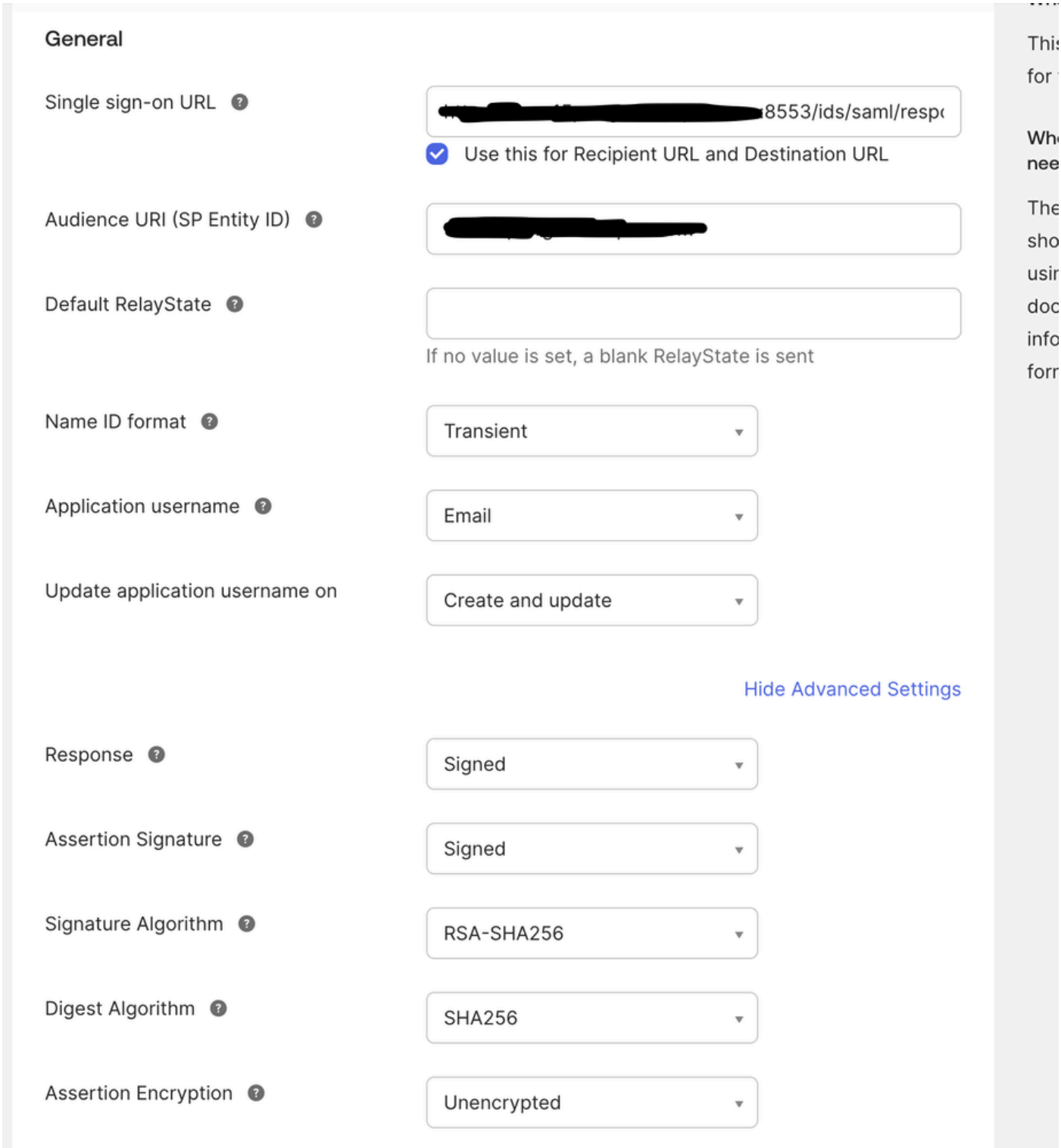
1. In Applicazioni, fare clic su Crea integrazione applicazione.



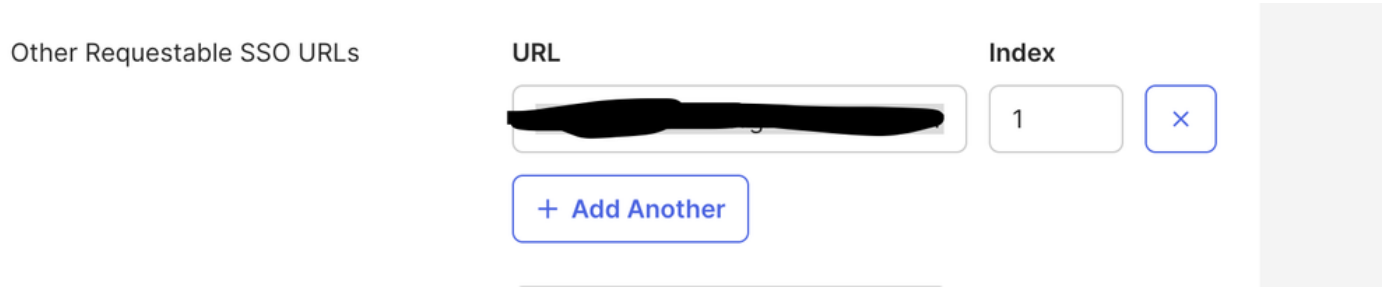
2. Scegliere l'opzione SAML2.0.



3. Sull'URL SSO dell'impostazione SAML, fornire l'URL SSO del PUB copiato nel passaggio 7. in 'Configurazione su IDS/Cisco Side' in questo documento. Nell'URI (Uniform Resource Identifier) del gruppo di destinatari (ID entità SP) incollare l'entità SP nella scheda di attendibilità IDS delle impostazioni di gestione del servizio di identità.



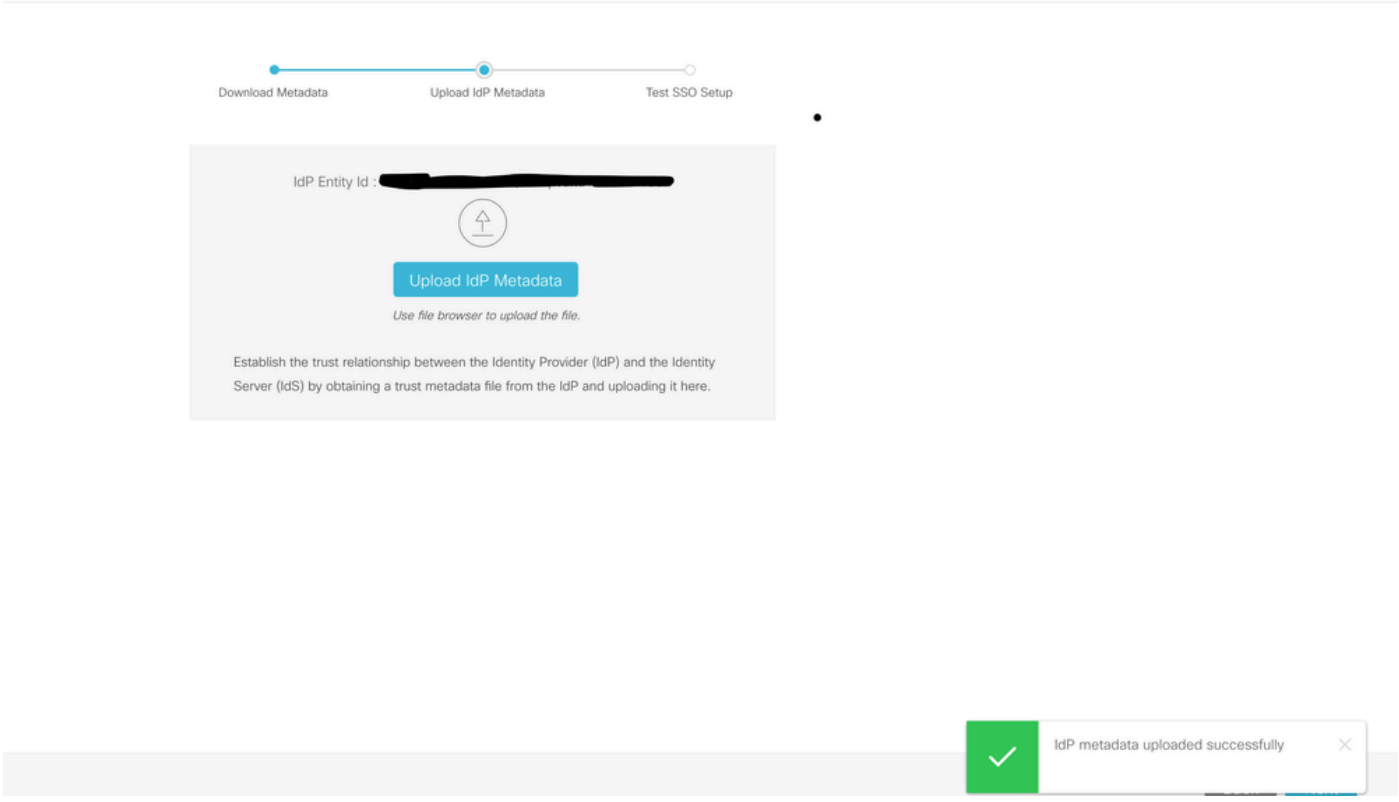
4. In 'Altri URL SSO richiesti', immettere l'URL di SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp nel formato specificato con il valore di indice 1.



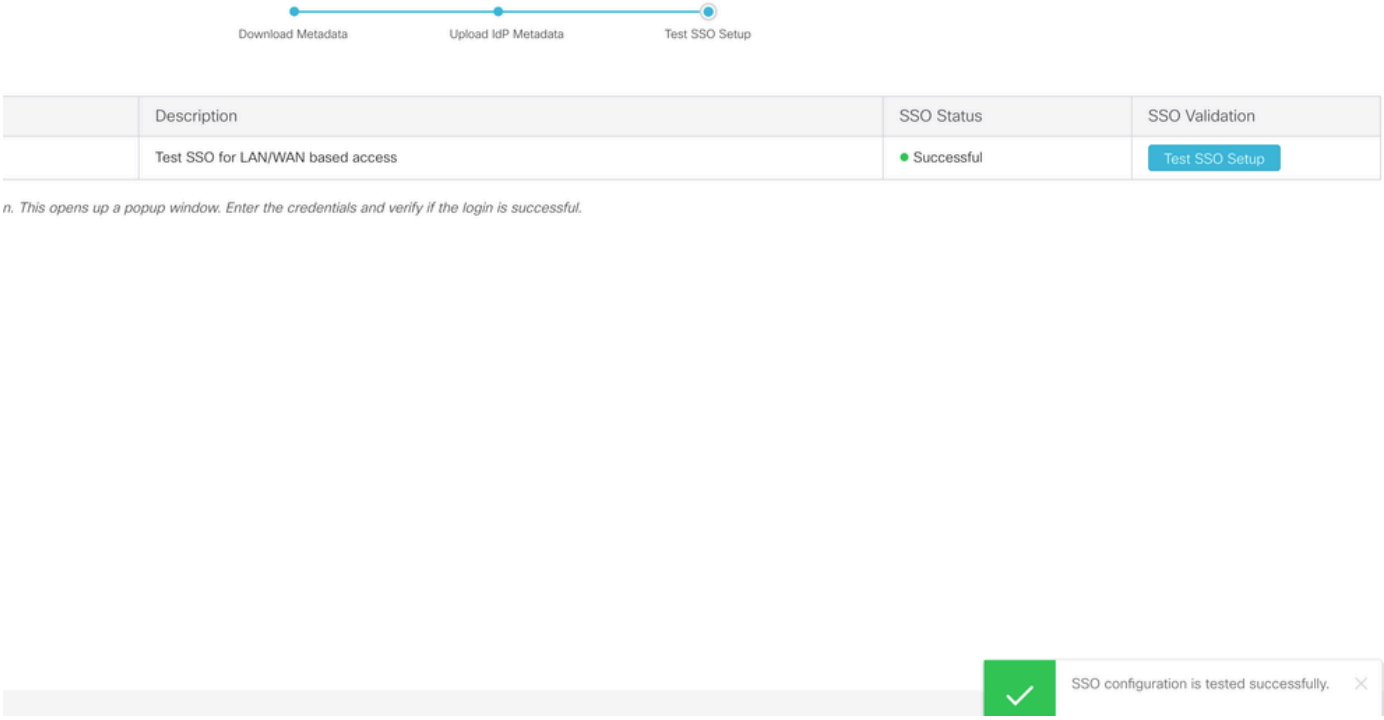
5. Fare clic su Avanti e Fine per completare la configurazione dell'applicazione.

6. Copiare i metadati dalla scheda Accedi utilizzando l'URL e salvarli in formato xml.

7. Caricare i metadati dal passaggio 6. nella pagina Web Identity Service Management sul lato CCX.

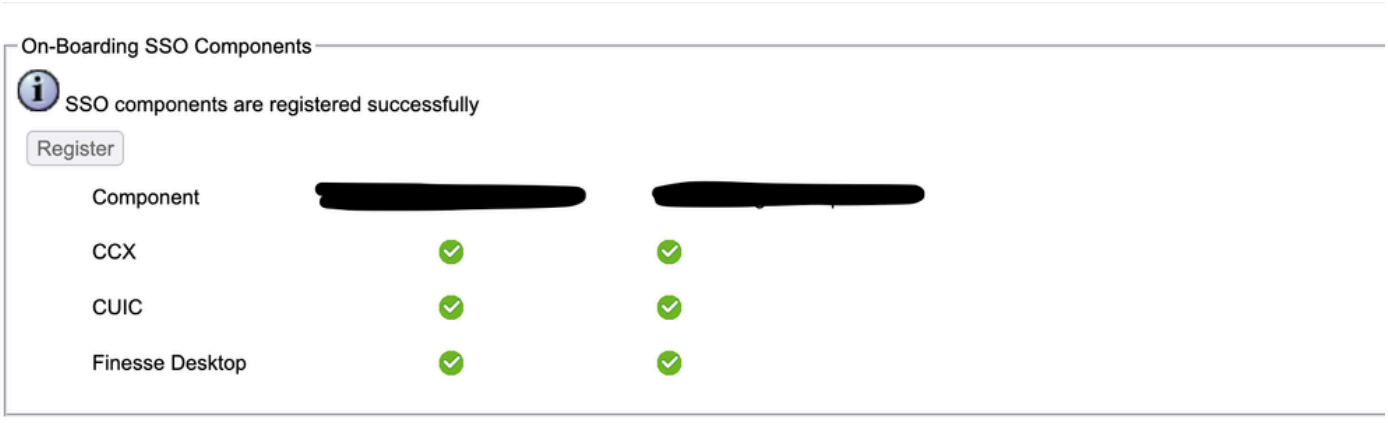


8. Eseguire un'impostazione TEST SSO che deve essere completata correttamente.



9. Accedere alla pagina web dell'amministratore su CCX con l'utente dell'amministratore e selezionare Sistema > Single Sign-On.

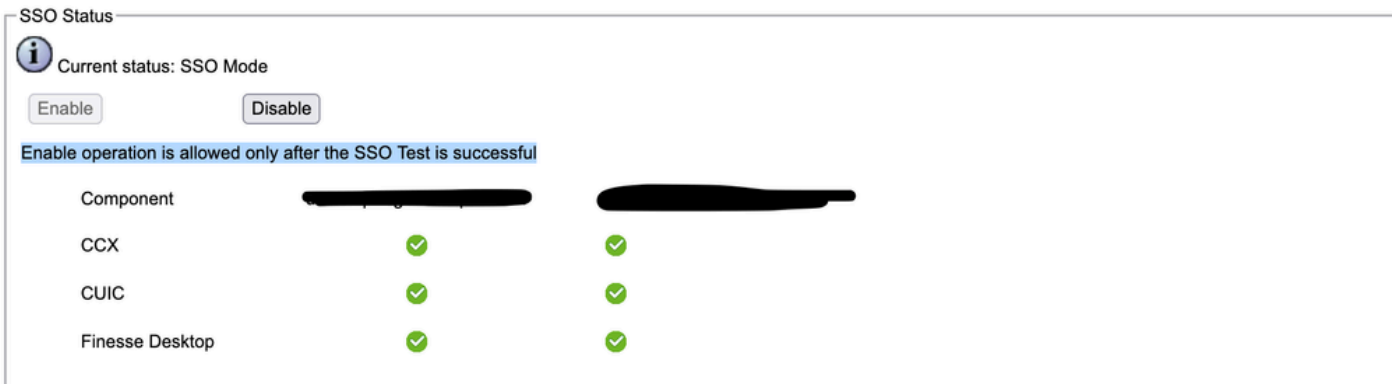
10. Fare clic sul pulsante Registra per incorporare i componenti.



11. La funzionalità di creazione di rapporti assegnata a Cisco Unified CCX Administrator (assegnata nella visualizzazione della capacità dell'amministratore) ed esecuzione del comando CLI utilizza l'utente cuic make-admin CCX\<ID utente amministratore> per fornire i diritti di amministratore in Cisco Unified Intelligence Center. Utilizzare l'utente configurato con diritti di amministratore per l'operazione di test SSO.

12. Eseguire l'operazione di test SSO.

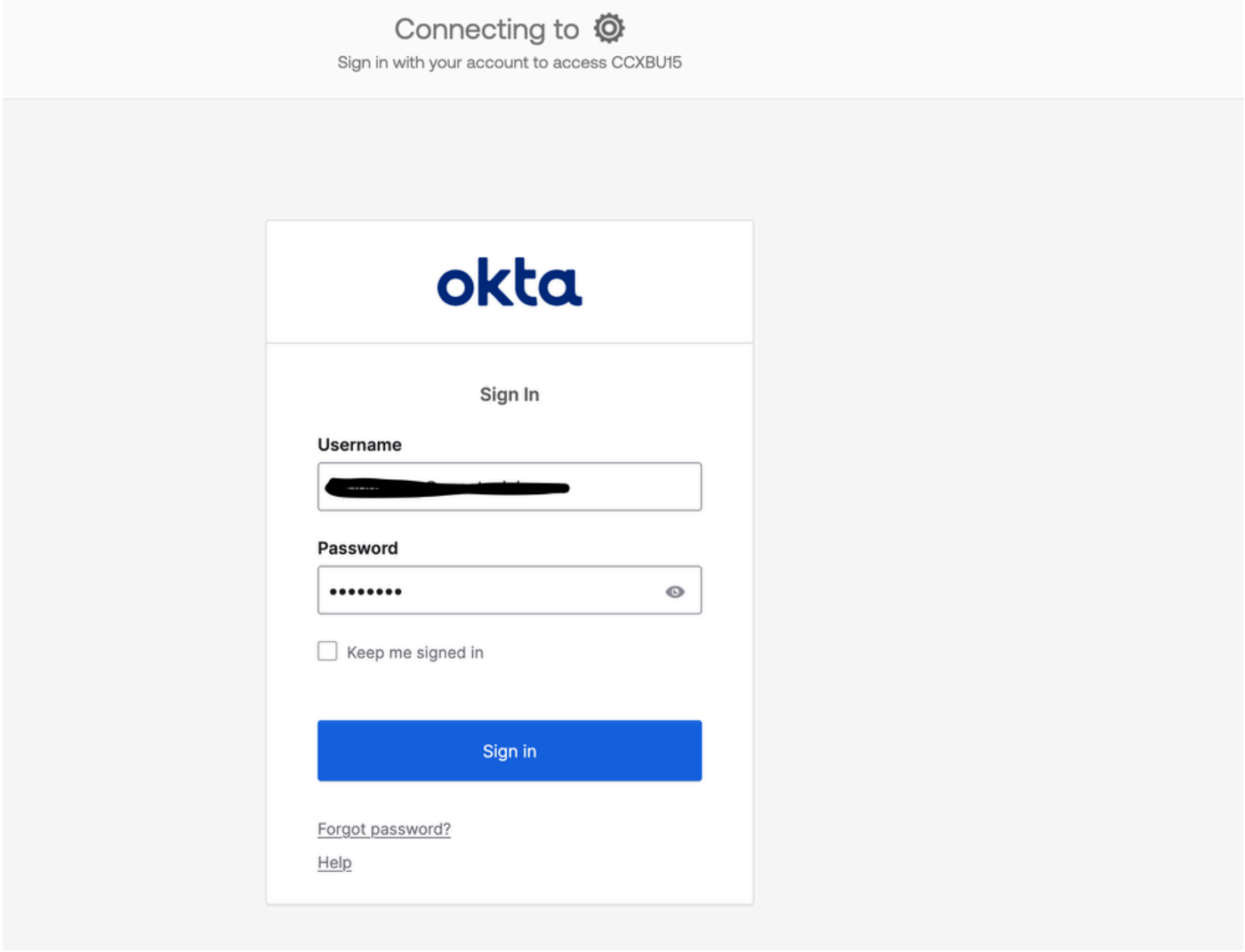
13. Dopo il completamento del test SSO, l'operazione di abilitazione è consentita.



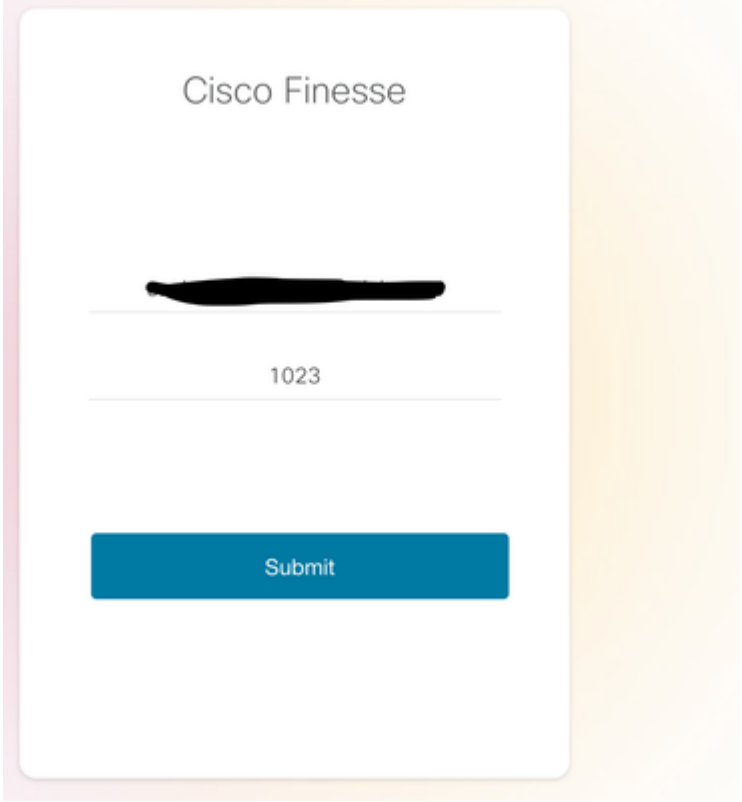
Verifica

Verificare le operazioni di login con agenti e amministratori su CCX, Cisco Unified Intelligence Center (CUIC) e Finesse. Devono avere successo.

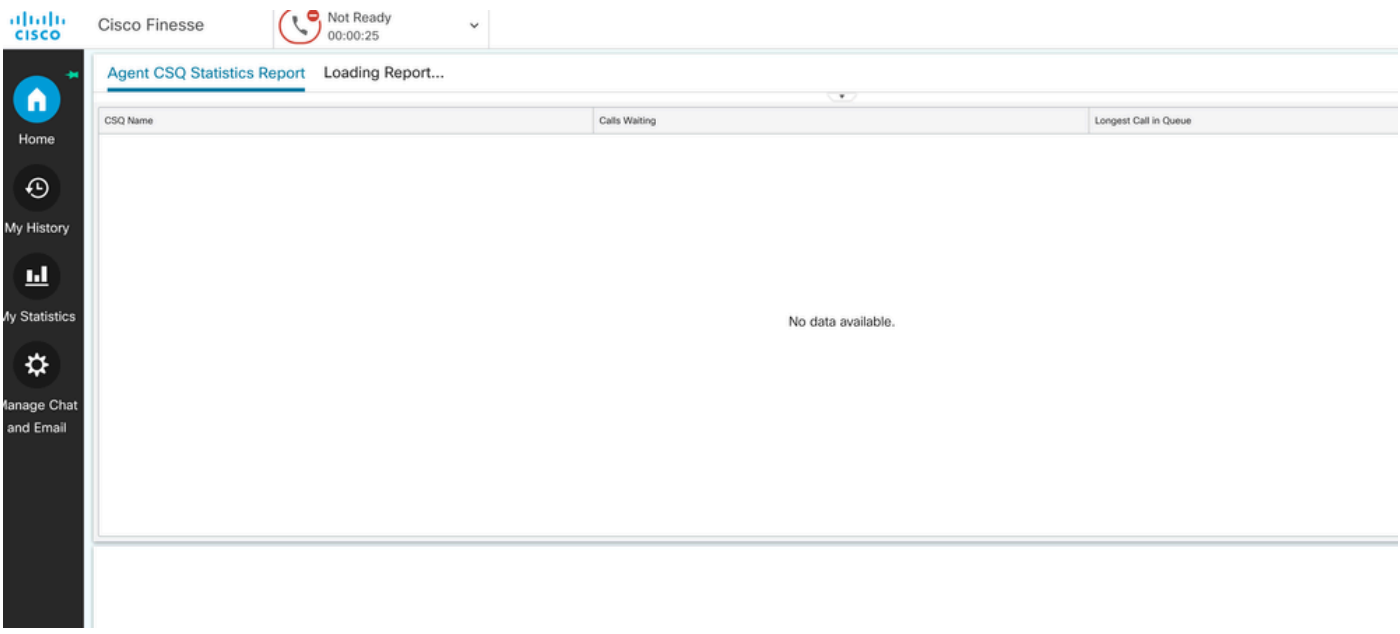
Quando accede all'agente su finesse, reindirizza alla pagina OKTA.



Dopo aver inserito le credenziali, richiede solo l'estensione ora nella pagina di accesso finesse.



Dopo l'immissione di questa opzione, l'accesso deve essere riuscito e tutti i report in tempo reale devono essere caricati correttamente.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).