Okta IDPによるCCXおよび構内コンタクトセンターソリューションでのSSOの設定

内容

はじめに

このドキュメントでは、さまざまなCisco On Prem Contact Center(OCC)ソリューションのOKTAを使用したシングルサインオン(SSO)の設定について説明します。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise(UCCE)、またはPackaged Contact Center Enterprise(PCCE)
- Security Assertion Markup Language(SAML)
- オクタ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Unified Contact Center Express(UCCX)15.0
- オクタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

IDS/Cisco側の設定

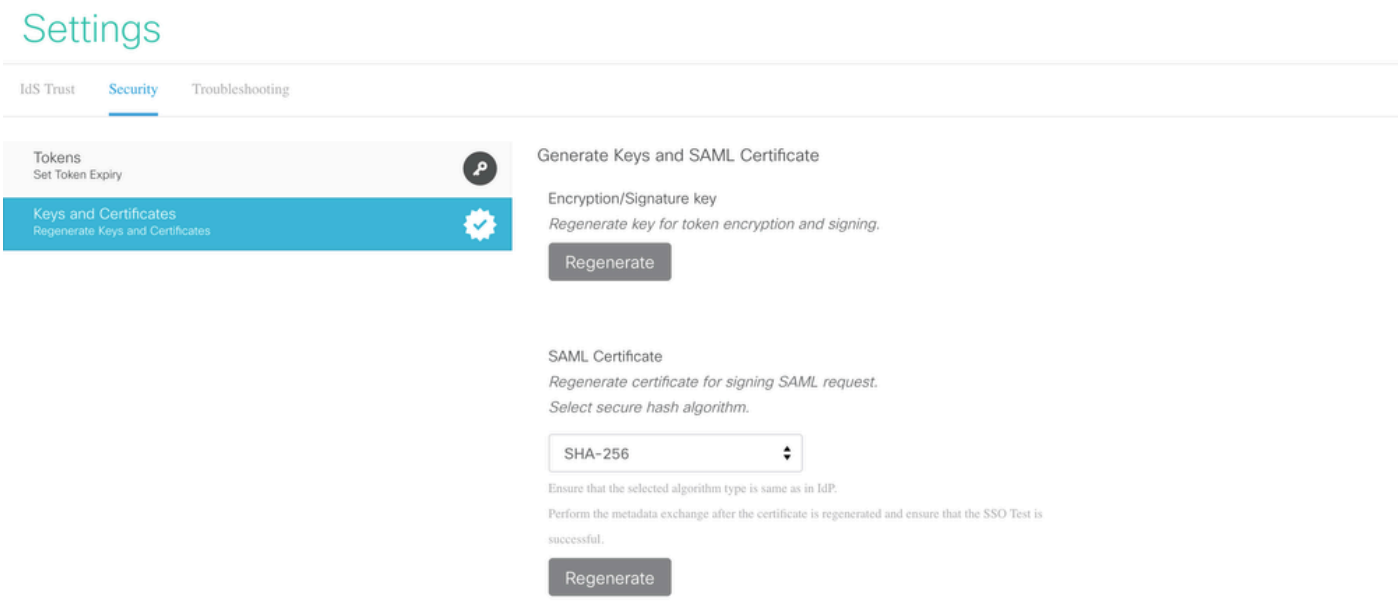
1. コマンドutils ids set_property IS_IdP_OKTA trueをCLIで実行し、アイデンティティサービス(IDS)サービスを再起動します。

2. 高可用性(HA)の場合は、両方のノードでこのコマンドを実行し、IDSサービスを再起動します。

3. PUBノードでUCCX Cisco IDS管理インターフェイスhttps://<UCCX server address>:8553/idsadminにログインします。

4. Settings > Security > Keys and Certificatesの順に移動します。

5. Security Assertion Markup Language(SAML)証明書を再生成します。



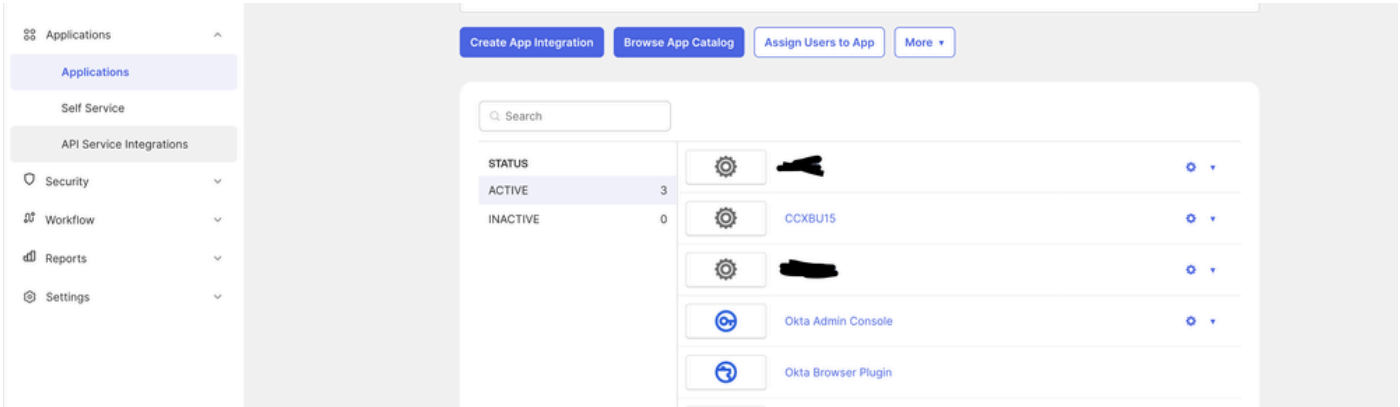
6. IDS Trustタブから、SAML SPメタデータXMLをダウンロードします。

7. サービスプロバイダー(SP)のメタデータXMLを開き、「AssertionConsumerService」タグ内のパブリッシャおよびサブスクライバIDの「Location」属性値をメモします。SAMLメタデータ内のAssertionConsumerServiceURLに、PUBのクエリパラメータの代わりにSAML応答URLの一部としてmetaAliasが含まれるようになりました。

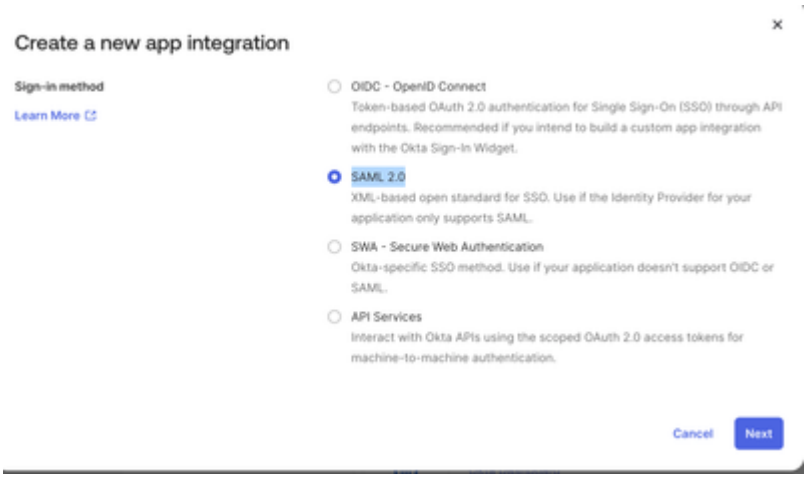
8. サブスクライバの場合は、クエリパラメータとともに表示され、無視できます。

OKTA IDP側の設定

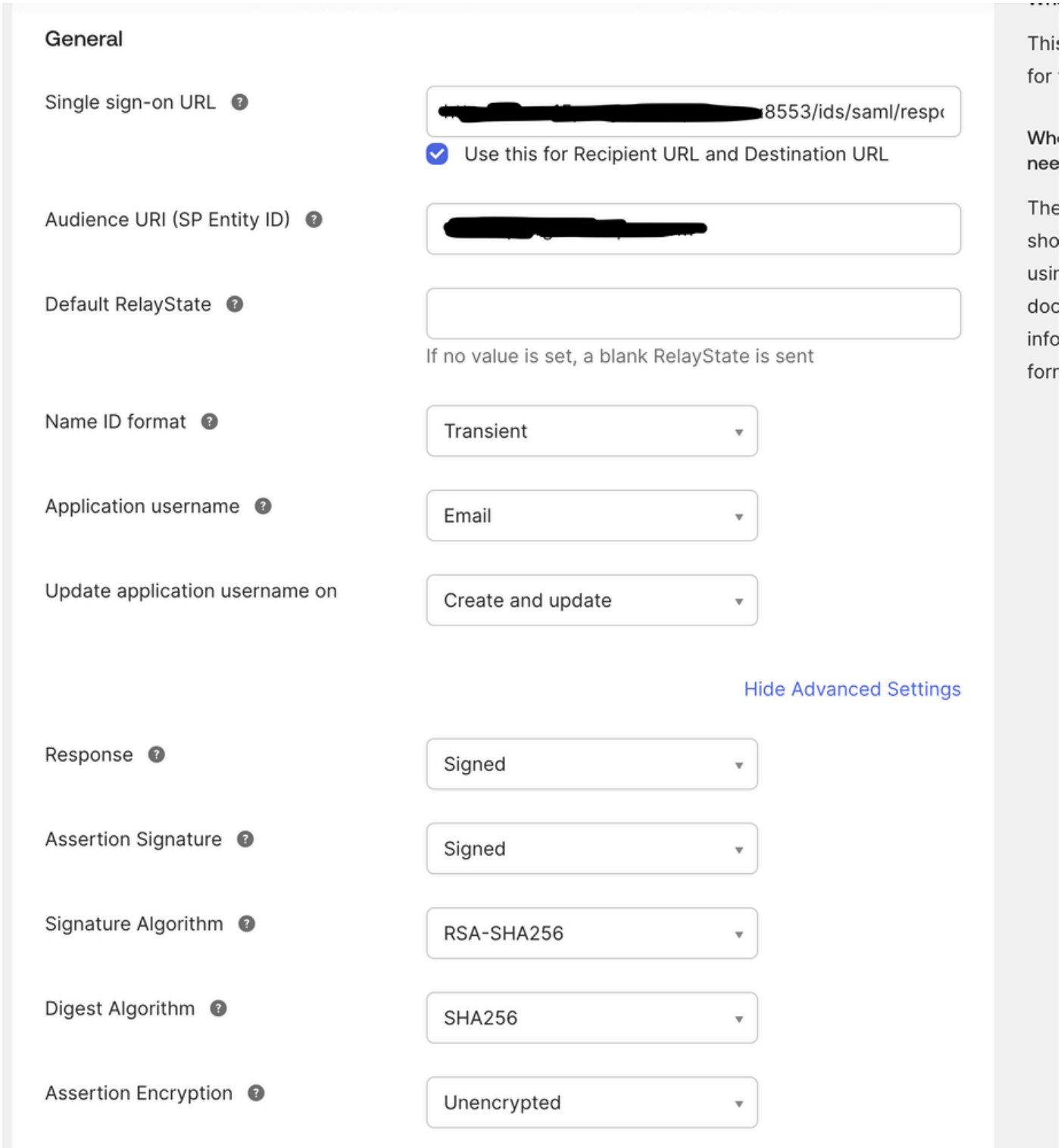
1. 「アプリケーション」で、「アプリケーション統合の作成」をクリックします。



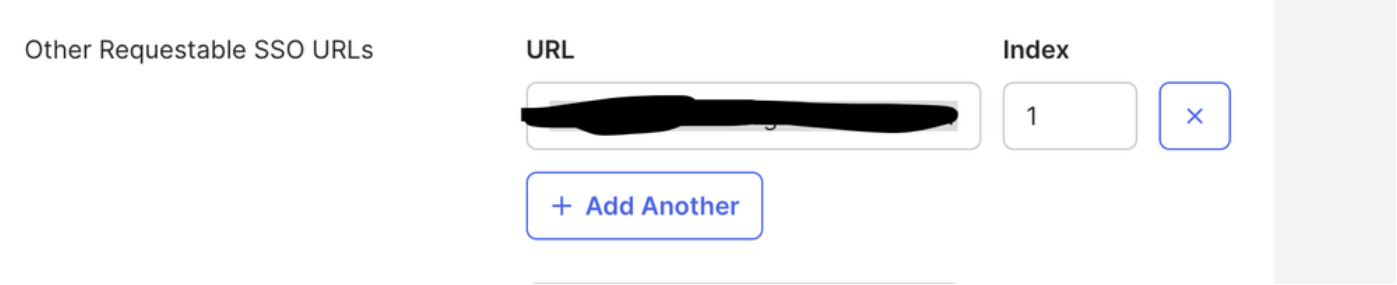
2. SAML2.0オプションを選択します。



3. SAML設定のSSO URLで、このドキュメントの「IDS/Cisco側での設定」の手順7でコピーしたパブリッシャのSSO URLを指定します。Audience Uniform Resource Identifier (URI) (SP Entity ID)で、アイデンティティサービス管理の設定のIDS trustタブにあるSPエンティティを貼り付けます。



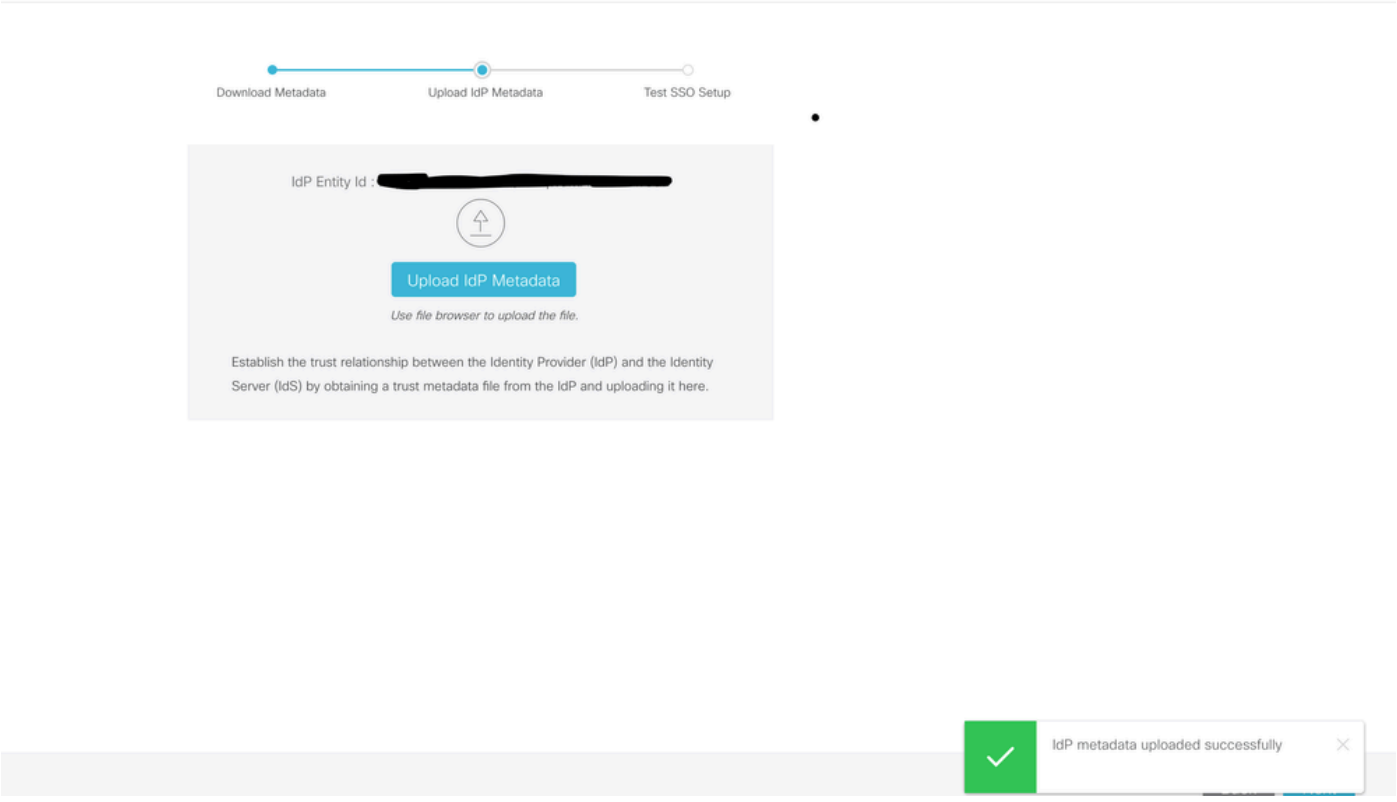
4. 'Other Requestable SSO URLs'で、SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/spのURLを、インデックス値1を使用して任意の形式で入力します。



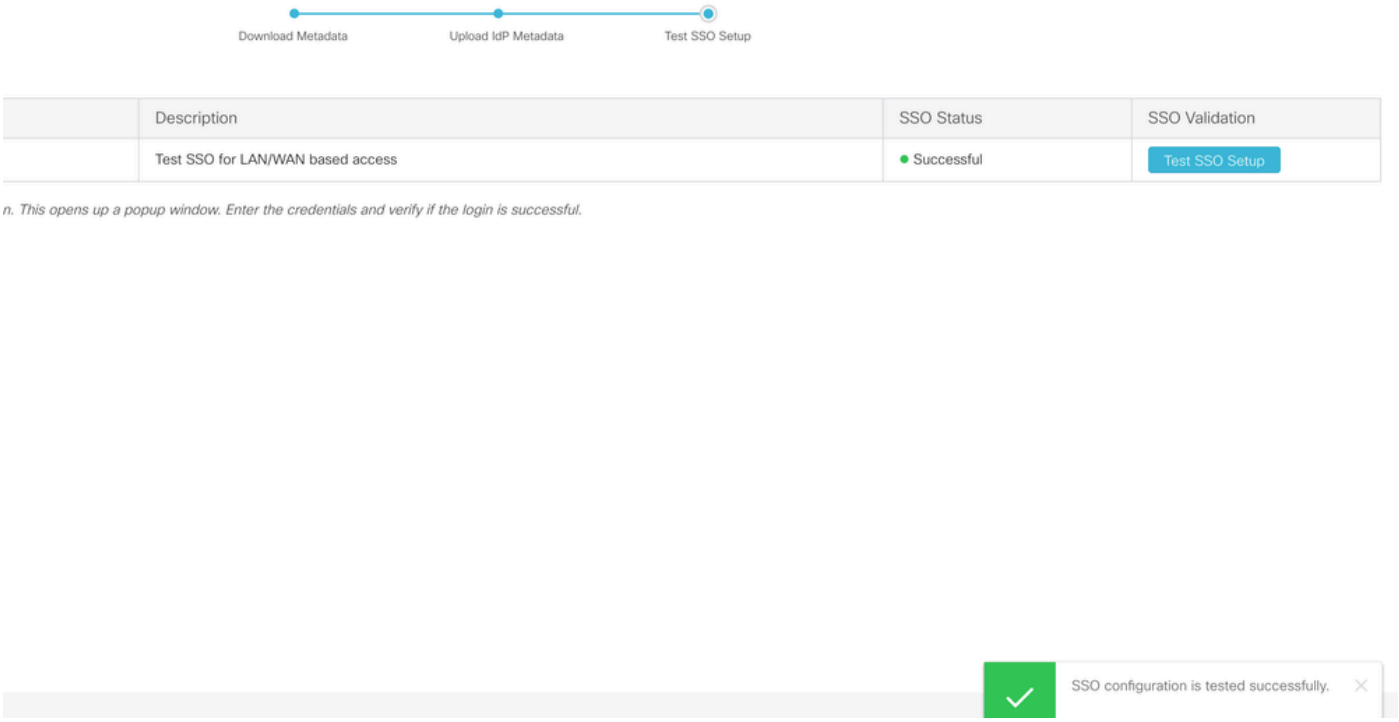
5. NextおよびFinishをクリックして、アプリケーションの設定を完了します。

6. URLを使用して「サインオン」タブからメタデータをコピーし、xmlとして保存します。

7. CCX側のアイデンティティサービス管理Webページで、手順6.のメタデータをアップロードします。

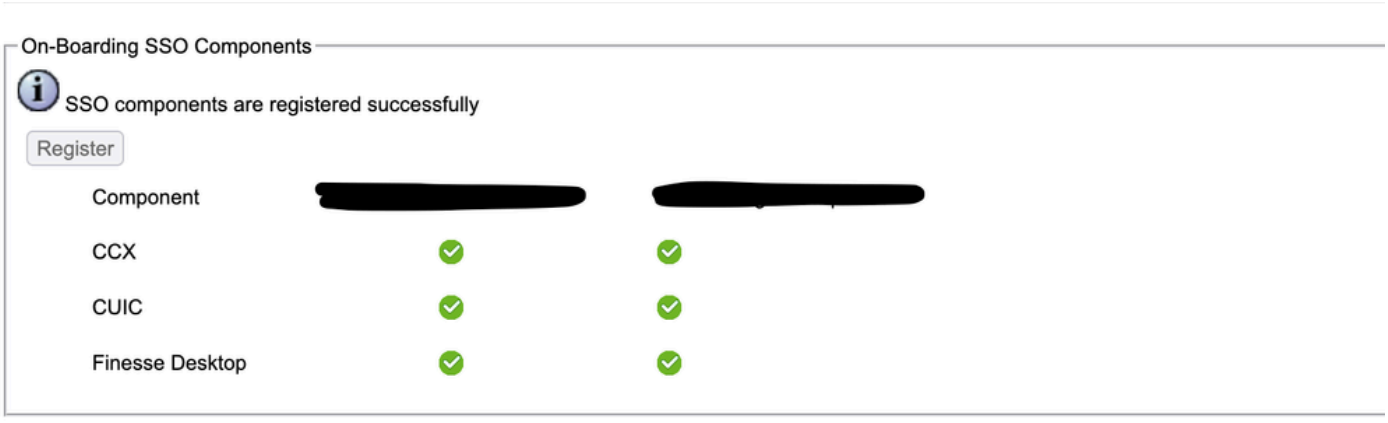


8. TEST SSOセットアップを実行します。このセットアップは成功する必要があります。



9. 管理者ユーザでCCXの管理Webページにログインし、システム>シングルサインオンに移動します。

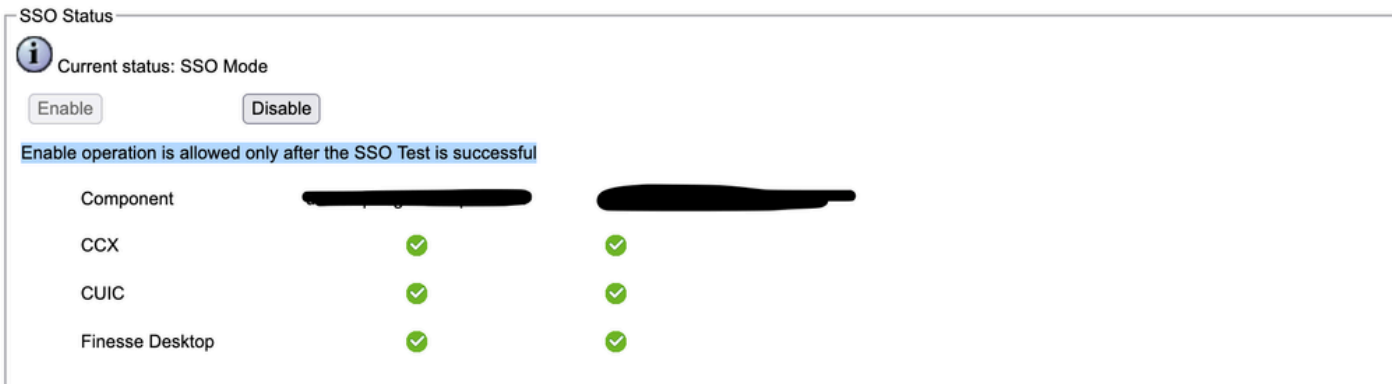
10. 「登録」ボタンをクリックして構成部品を登録します。



11. Cisco Unified CCX管理者にレポート機能を割り当て（Administrator Capabilityビューで割り当て）、CLIコマンドutils cuic user make-admin CCX\<Admin User Id>を実行して、Cisco Unified Intelligence Centerに管理者権限を提供します。SSOテスト操作に管理者権限を持つ設定済みのユーザを使用します。

12. SSOテスト操作を実行します。

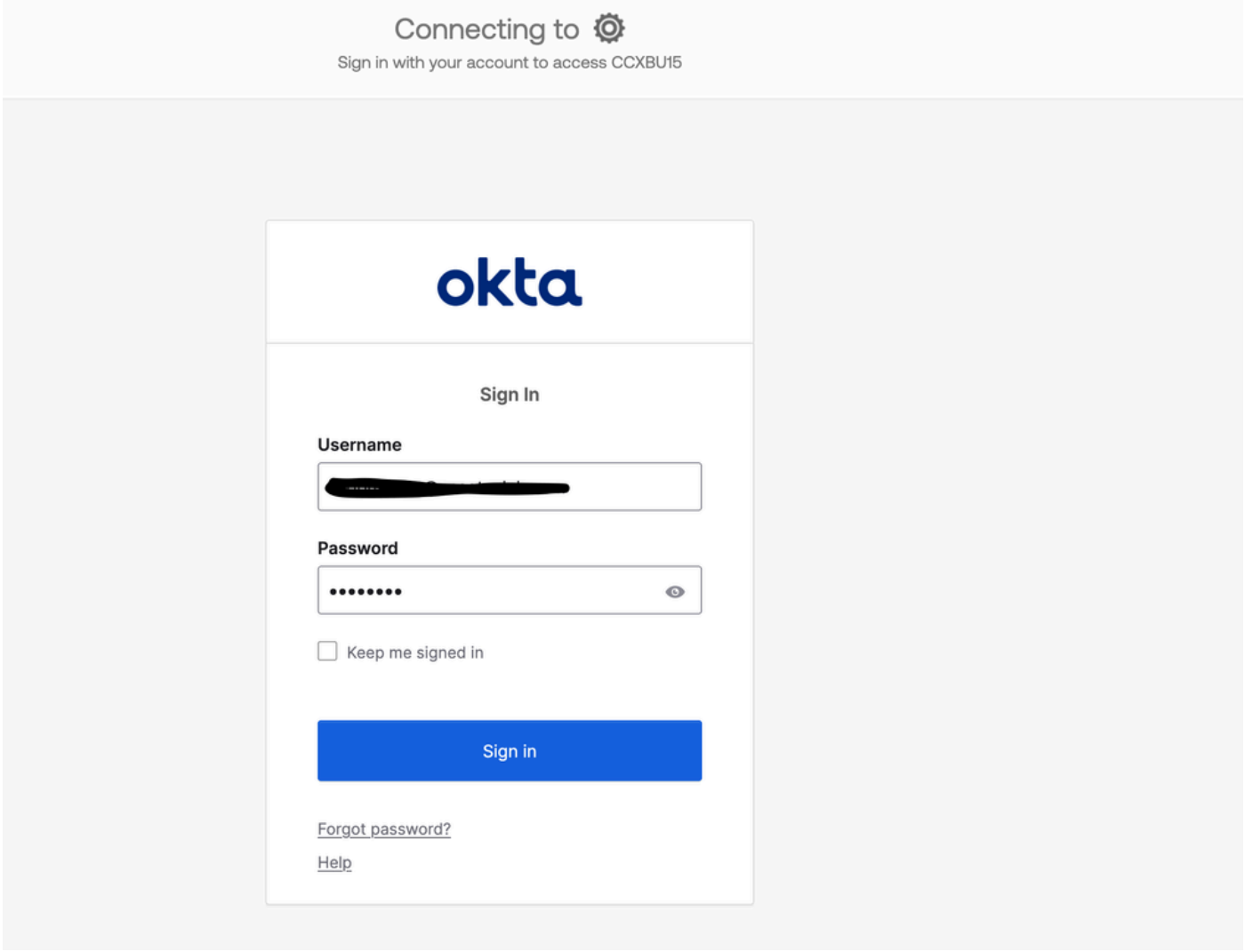
13. SSOテストが成功すると、enable操作が許可されます。



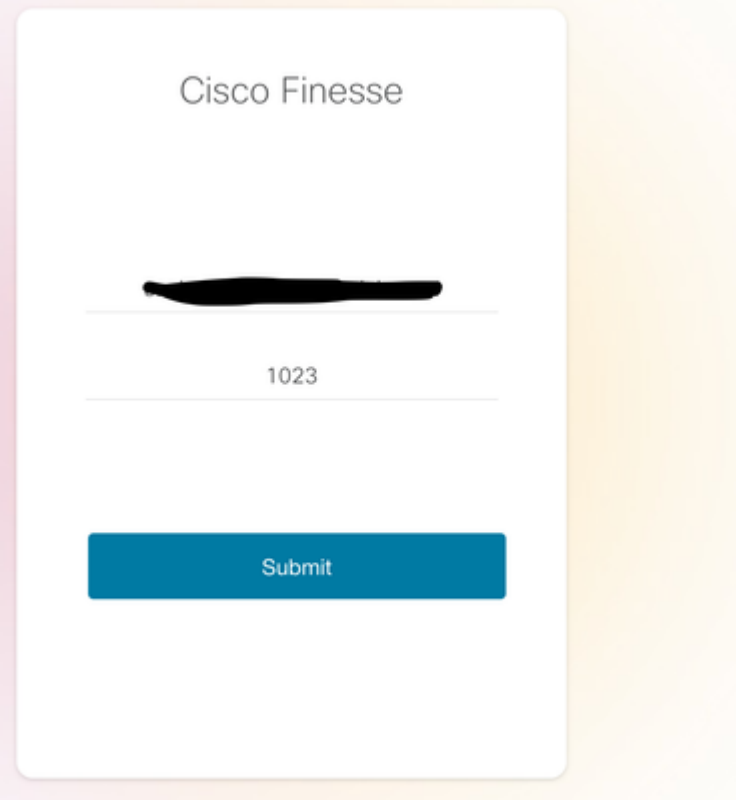
確認

CCX、Cisco Unified Intelligence Center(CUIC)、およびFinesseで、エージェントおよび管理者とのログイン操作を確認します。これらは成功するはずです。

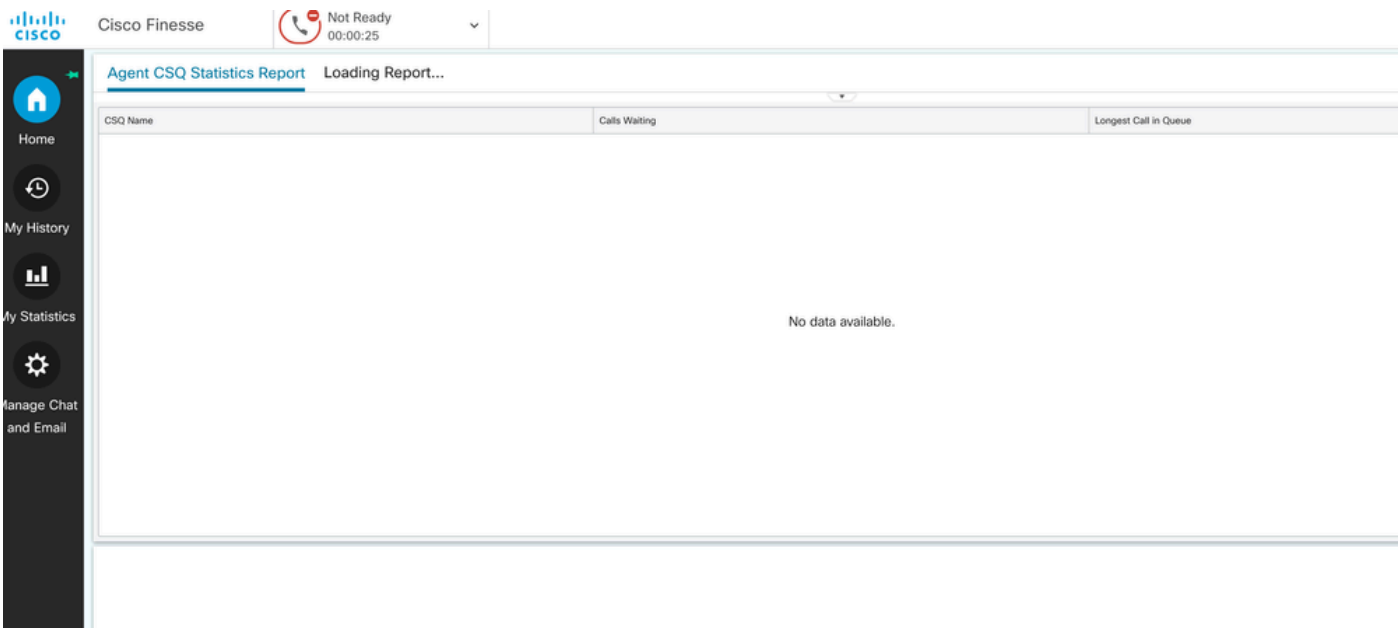
Finesseでエージェントにログインすると、OKTAページにリダイレクトされます。



クレデンシャルを入力すると、Finesseログインページで内線番号の入力だけを求められます。



この入力後、ログインが成功し、すべてのライブレポートが正常にロードされる必要があります。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。