Configurar o SSO no CCX e nas soluções do Contact Center Local com o Okta IDP

Contents

Introdução

Este documento descreve a configuração do SSO (Single Sign On, Logon único) com OKTA para várias soluções Cisco On Prem Contact Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) ou Packaged Contact Center Enterprise (PCCE)
- Linguagem de marcação de asserção de segurança
- OKTA

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Unified Contact Center Express (UCCX) 15.0
- OKTA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração no lado IDS/Cisco

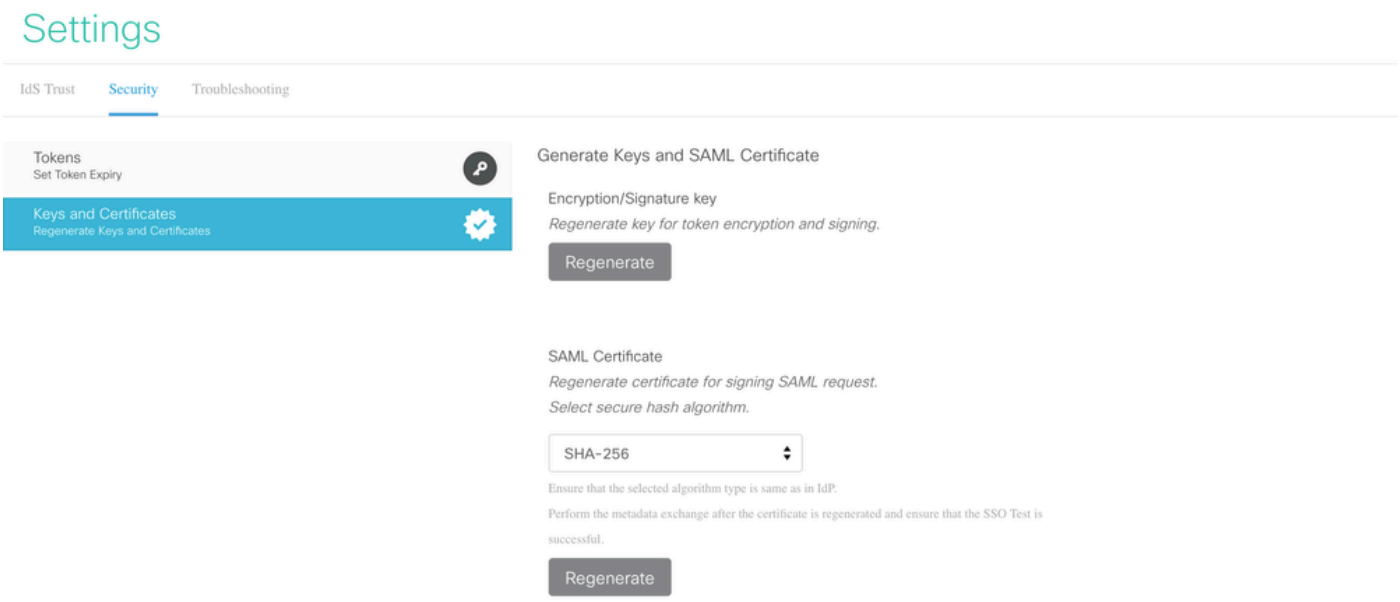
1. Execute o comando utils ids set_property IS_IdP_OKTA true na CLI e reinicie o serviço do Identity Service (IDS).

2. Se houver HA (High Availability, alta disponibilidade), execute este comando em ambos os nós e reinicie o serviço IDS.

3. Faça login na interface de administrador do Cisco IDS do UCCX https://<UCCX server address>:8553/idsadmin no nó PUB.

4. Navegue até Configurações > Segurança > Chaves e Certificados.

5. Regenerar o Certificado SAML (Security Assertion Markup Language).



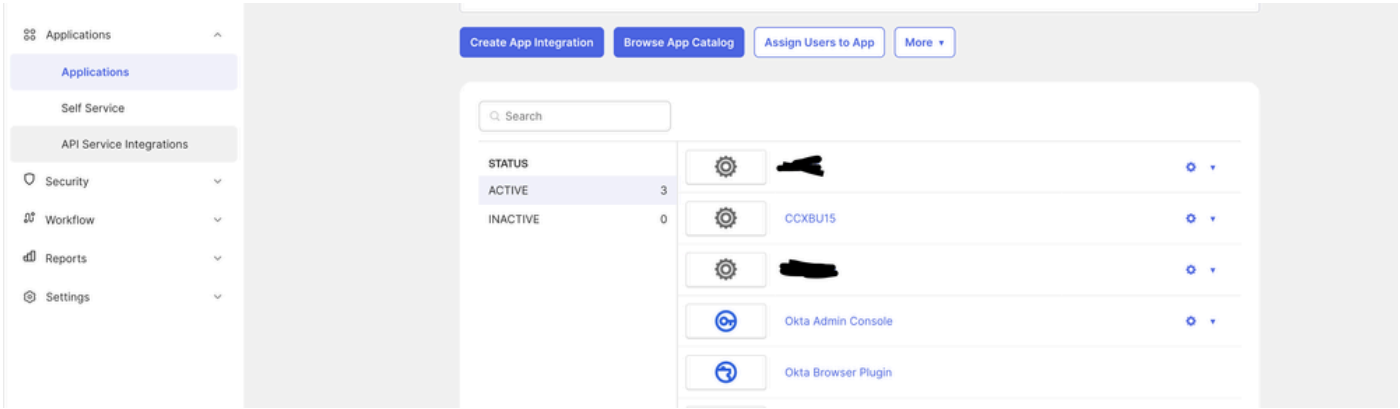
6. Na guia IDS Trust, baixe o XML dos metadados SP SAML.

7. Abra o XML de metadados do SP (Provedor de Serviços) e anote o valor do atributo 'Location' para as IDS do Publicador e do Assinante na marca 'AssertionConsumerService'. A AssertionConsumerServiceURL nos metadados SAML agora inclui metaAlias como parte da URL de resposta SAML em vez do parâmetro de consulta para PUB.

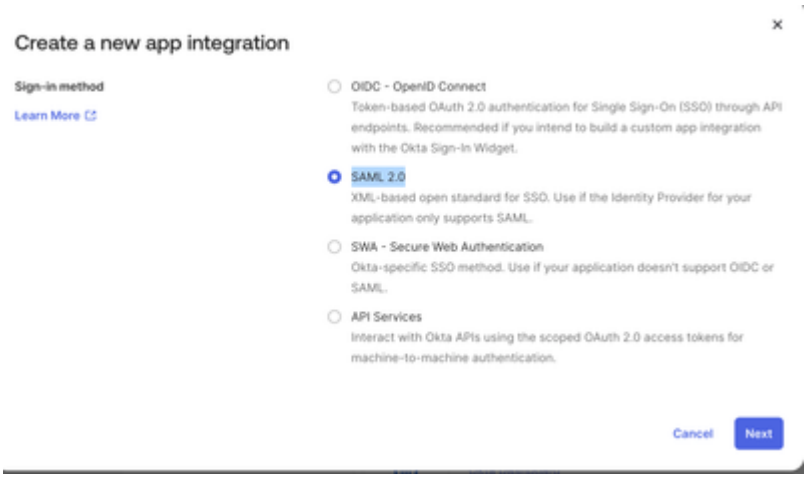
8. Para o Assinante, ele é mostrado com o parâmetro query e pode ser ignorado.

Configuração no lado OKTA IDP

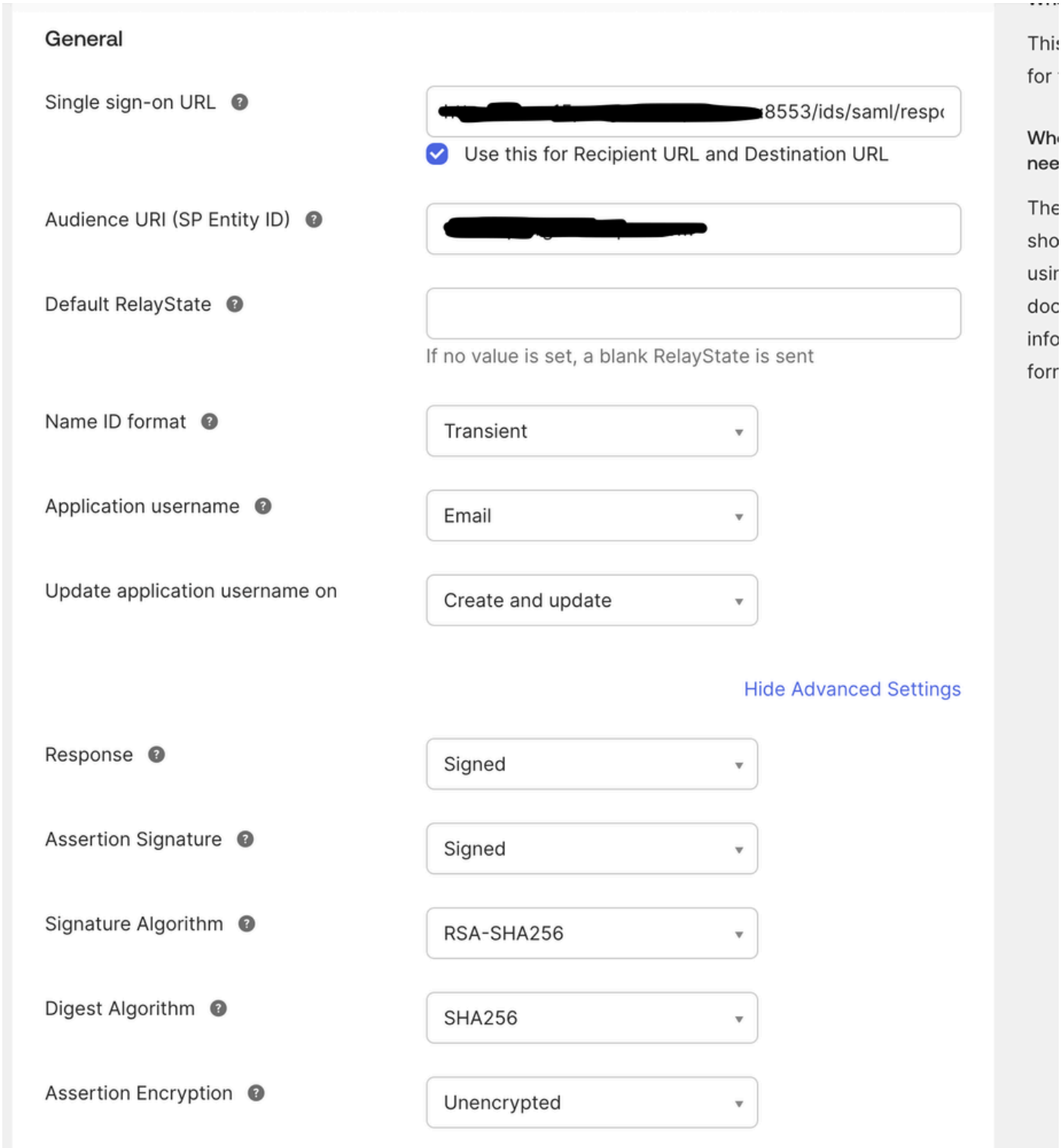
1. Em Aplicativos, clique em Criar Integração de Aplicativos.



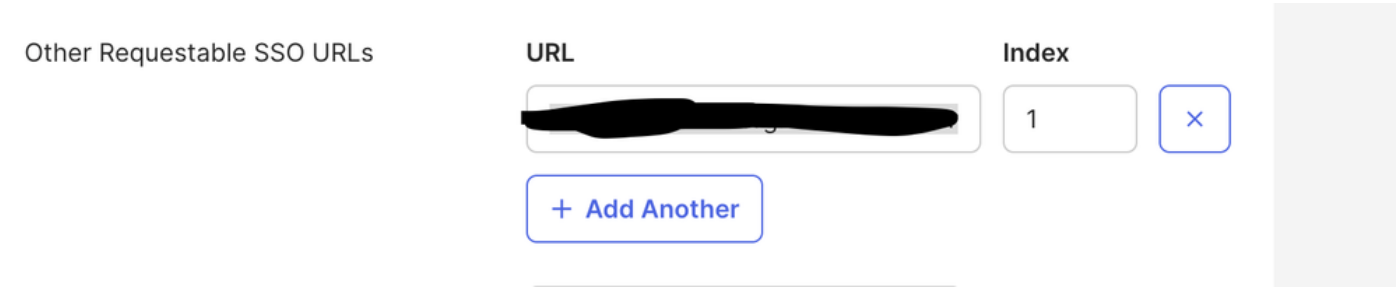
2. Escolha a opção SAML2.0.



3. Na URL SSO da configuração SAML, forneça a URL SSO do PUB que foi copiada na Etapa 7. em "Configuração no IDS/Cisco Side" neste documento. No URI (identificador de recurso) Uniforme da Audiência (ID da entidade da controladora de armazenamento) cole a entidade da controladora de armazenamento na guia Confiança de IDS nas configurações do Gerenciamento do serviço de identidade.



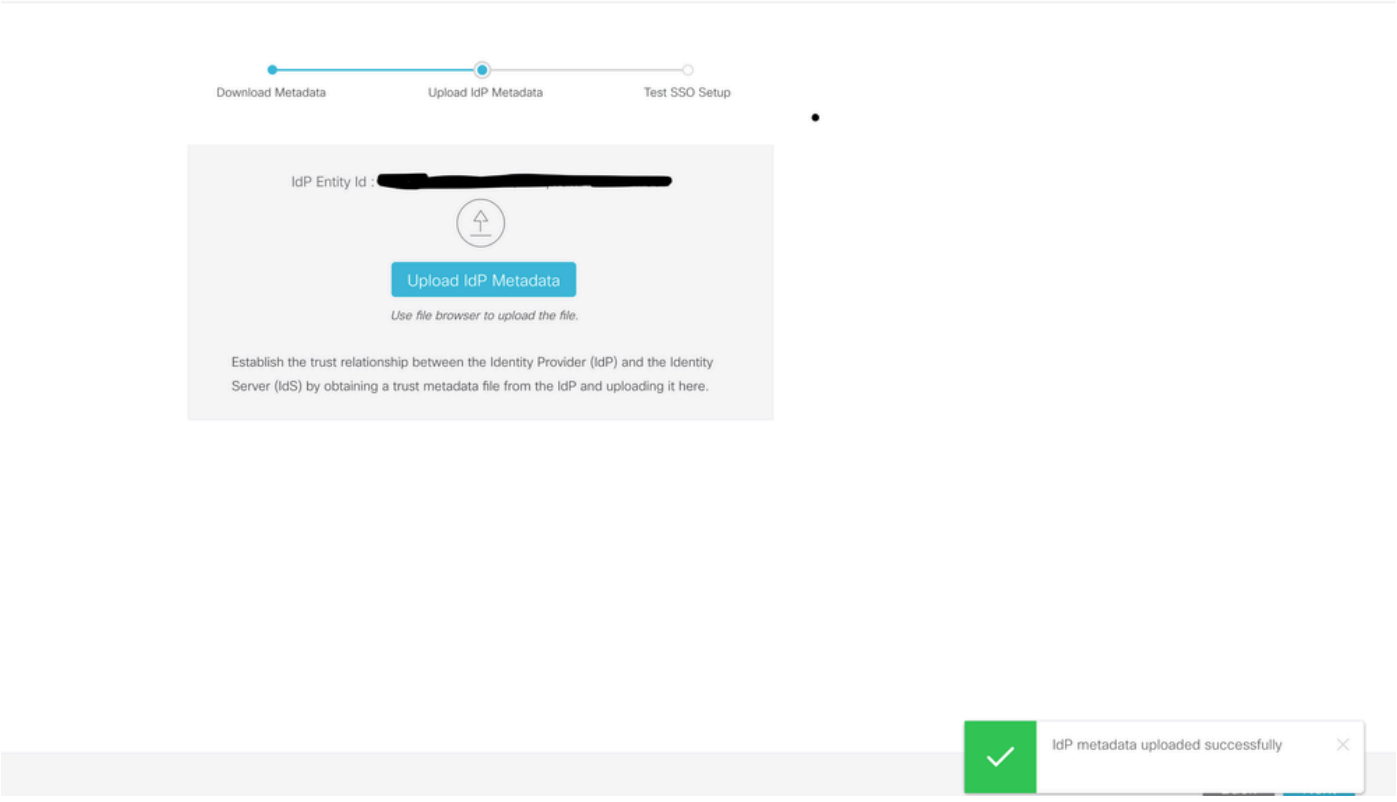
4. Em 'Other Requestable SSO URLs', insira o URL de SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp no formato especificado com o valor de índice 1.



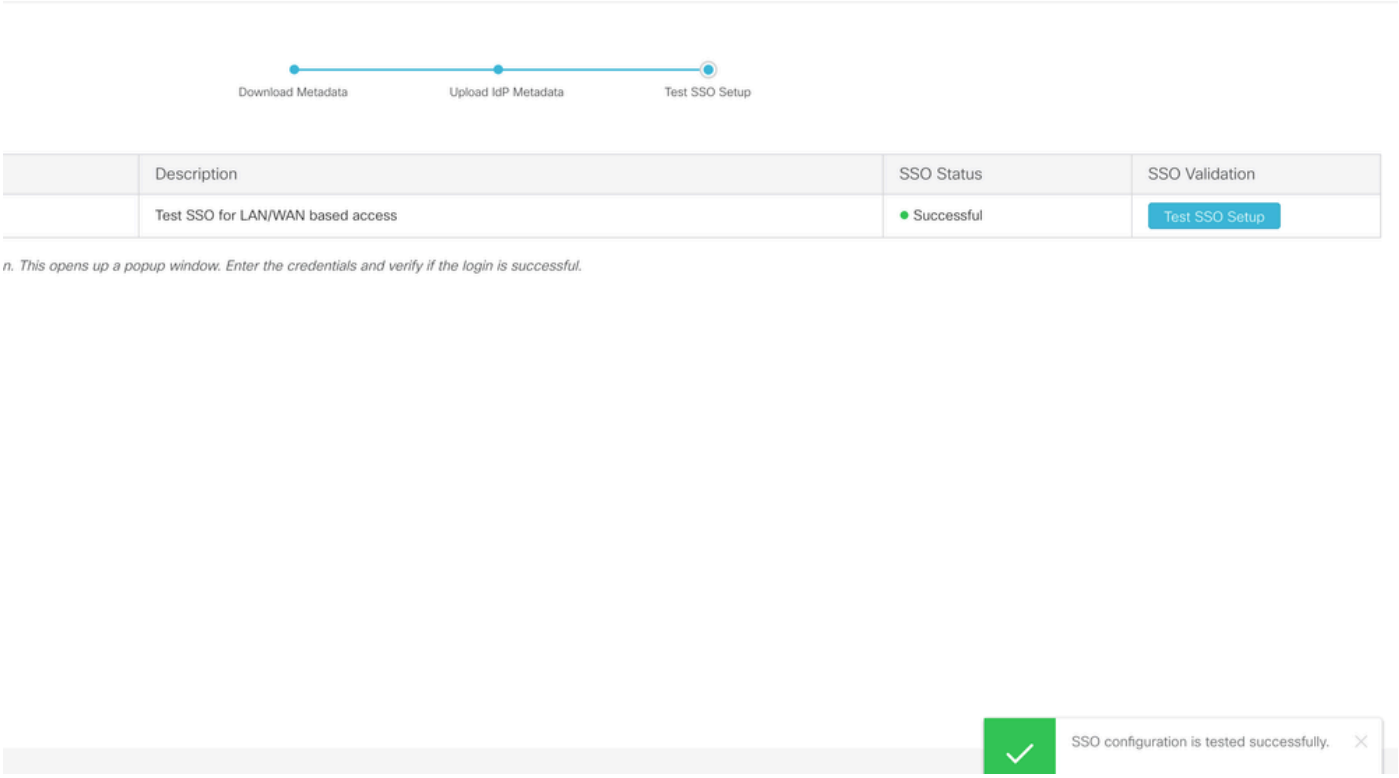
5. Clique em Próximo e Concluir para concluir a configuração do aplicativo.

6. Copie os Metadados da guia Sign On usando o URL e salve-o como xml.

7. Carregue os metadados da Etapa 6. na página da Web de gerenciamento do serviço de identidade no CCX.

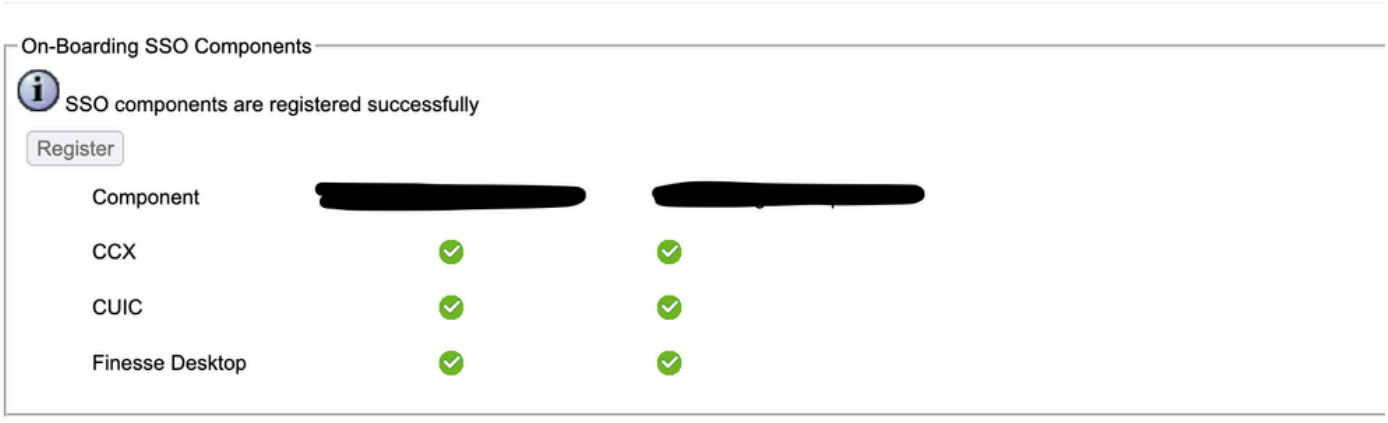


8. Execute uma configuração TEST SSO e ela deverá ser bem-sucedida.



9. Faça login na página da Web do administrador no CCX com o usuário admin e navegue para Sistema > Logon único.

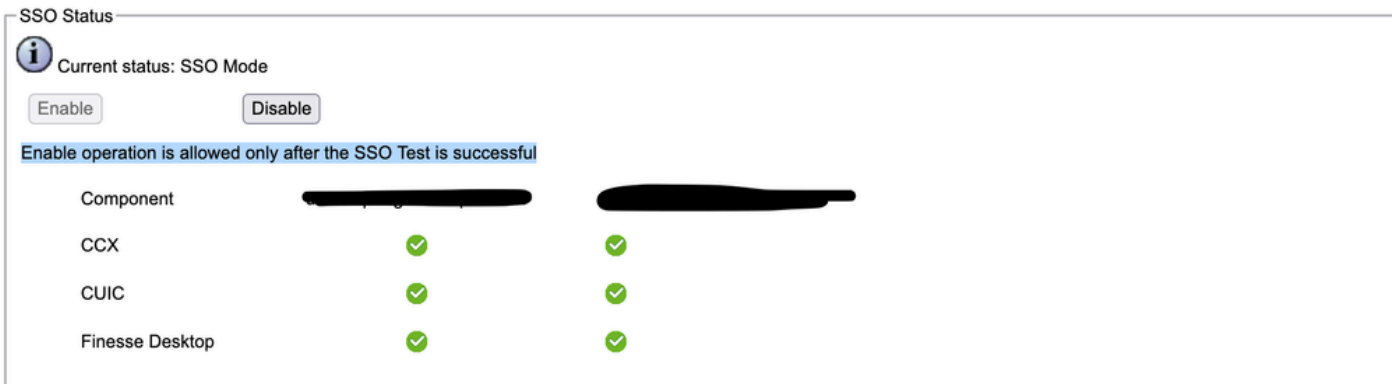
10. Clique no botão Registrar para integrar os componentes.



11. O recurso de relatórios foi atribuído ao Cisco Unified CCX Administrator (atribuído na exibição do recurso do administrador) e execute o comando CLI utils cuic user make-admin CCX\<Admin User Id> para fornecer direitos de administrador no Cisco Unified Intelligence Center. Use o usuário configurado com direitos de administrador para a operação de Teste de SSO.

12. Execute a operação de Teste de SSO.

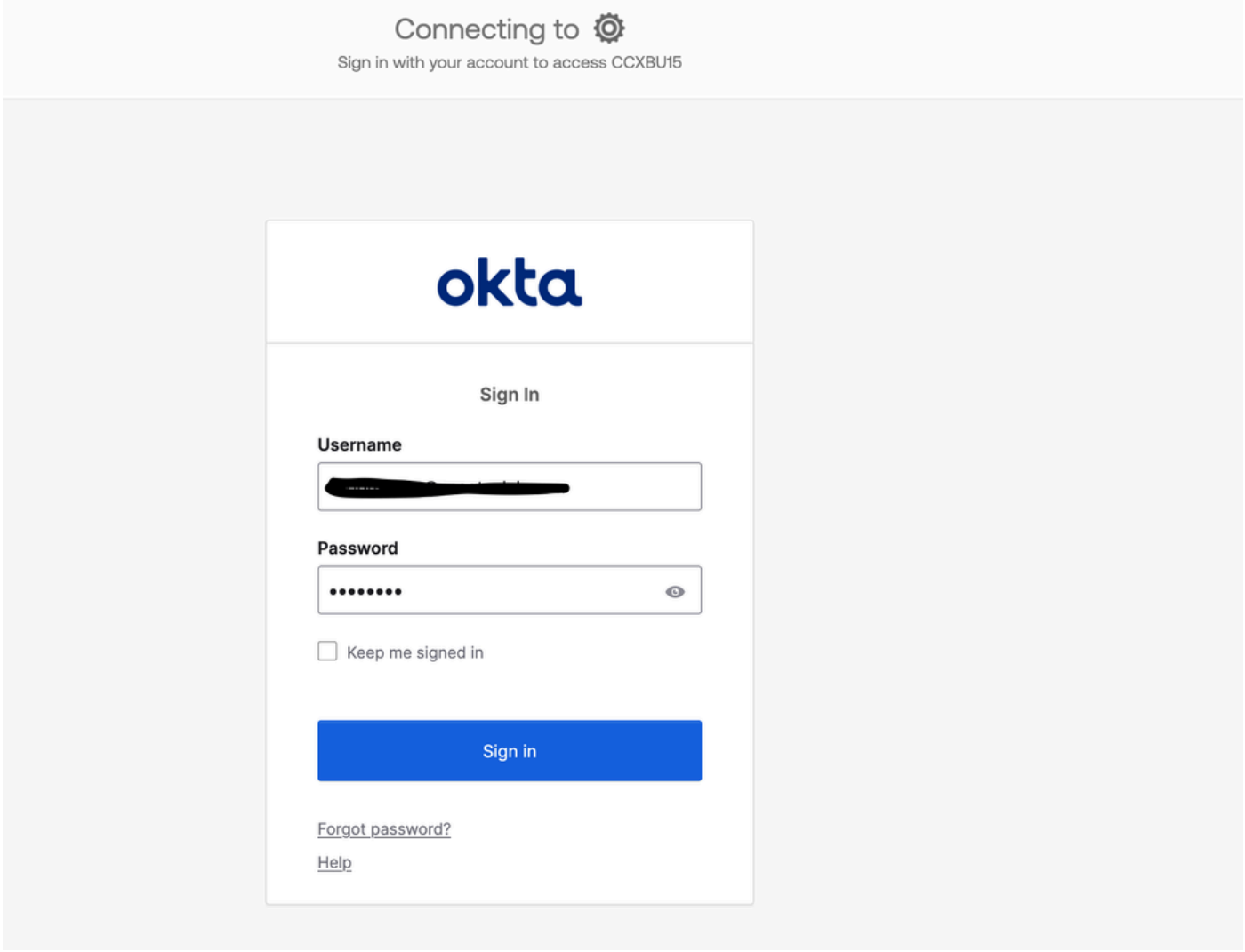
13. Depois que o Teste de SSO for bem-sucedido, a operação de ativação será permitida.



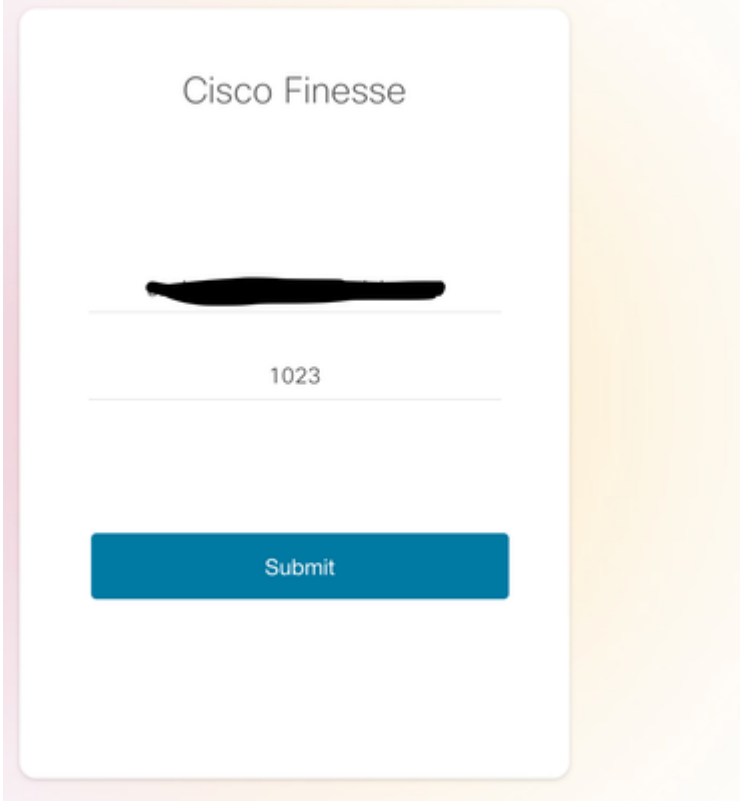
Verificar

Verifique as operações de login com agentes e administradores no CCX, no Cisco Unified Intelligence Center (CUIC) e no Finesse. Elas têm de ser bem sucedidas.

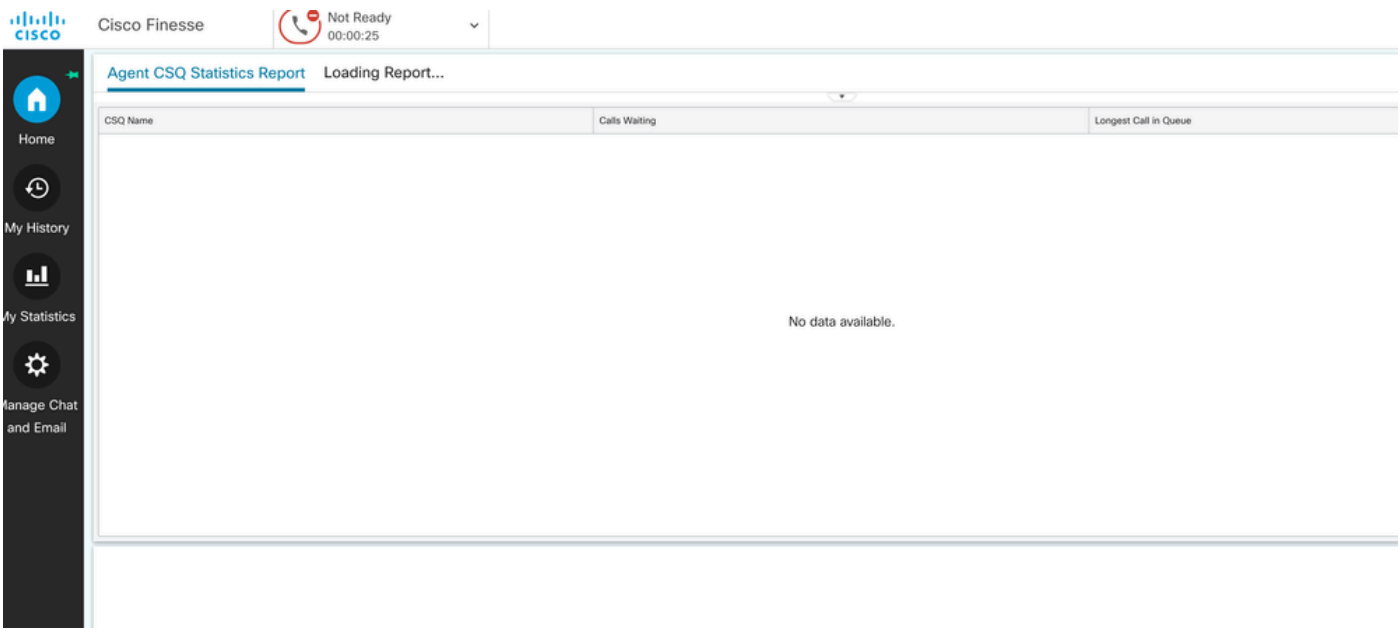
Ao fazer logon do agente no Finesse, ele é redirecionado para a página OKTA.



Depois de colocar as credenciais, ele solicita apenas a extensão agora na página de login do finesse.



Depois que isso for inserido, o logon deverá ser bem-sucedido e todos os relatórios ao vivo deverão estar carregados corretamente.



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.