Centro de contato SSO com o fornecedor da identidade de Okta

Índice

Introdução

Este original descreve a configuração do serviço da identidade (IdS) e do fornecedor da identidade (IdP) para sinal baseado nuvem de Okta o único sobre (SSO).

Produto	Desenvolvimento
UCCX	Co-residente
PCCE	Co-residente com CUIC (centro unificado Cisco da inteligência) e LD (dados vivos)
UCCE	Co-residente com CUIC e LD para as disposições 2k. Autônomo para as disposições 4k e 12k.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE), ou empresa empacotada do centro de contato (PCCE)
- Linguagem de marcação da afirmação da Segurança (SAML) 2.0
- Okta

Componentes Utilizados

- UCCE 11.6
- Okta **Note**: Este original provê UCCE nos screenshots e nos exemplos, porém a configuração é similar no que diz respeito ao serviço da identidade de Cisco (UCCX/UCCE/PCCE) e ao IdP.

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 sua rede estiver ativa, certifique-se de que entende o impacto

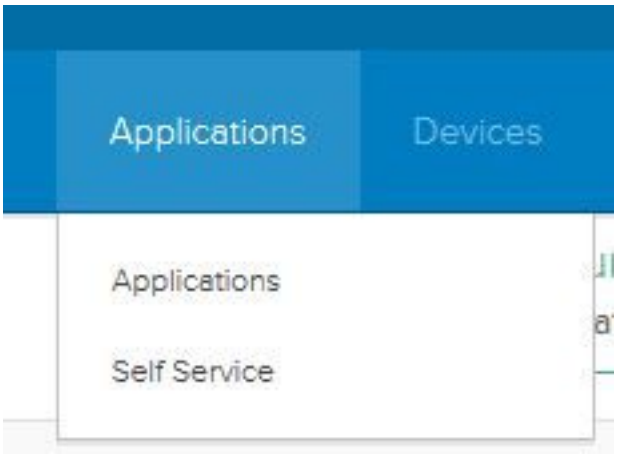
potencial de qualquer comando.

Configurar Okta como o provedor de serviços da identidade

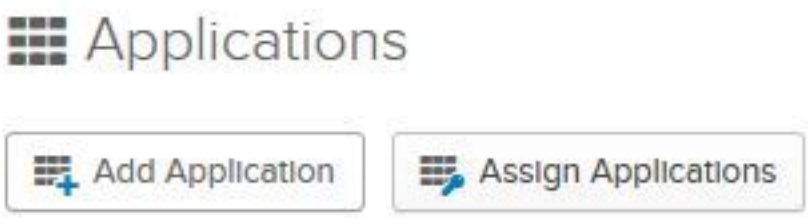
Etapa 1. Entre ao Web page do serviço da identidade (IdS) e navegue aos **ajustes** e transfira os metadata arquivam clicando o **arquivo dos Metadata da transferência.**

Etapa 2. Entre ao server de Okta e selecione a aba **Admin**.

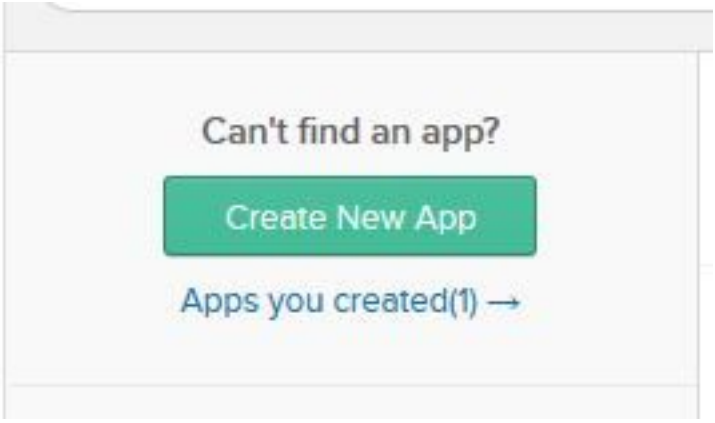
Etapa 3. Do painel de Okta, selecione **aplicativos > aplicativos.**



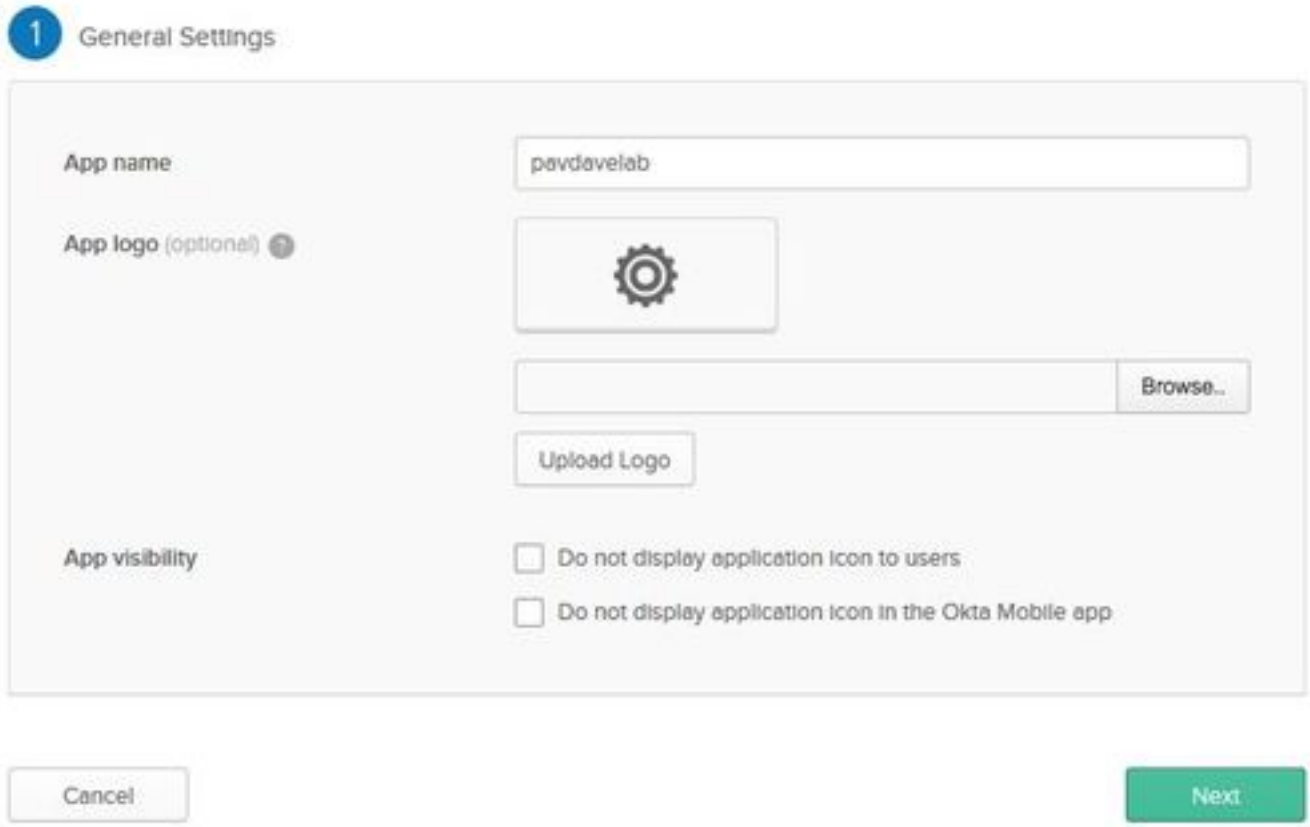
Etapa 4. O clique **cria um App novo** para criar um aplicativo feito sob encomenda novo usando o assistente.



Etapa 5. Na criação uma janela de integração do aplicativo novo, porque a **Web** seleta da plataforma na lista de drop-down e **SAML** seleto **2.0** como o sinal no método e seleto criam.



Etapa 6. Dê entrada com o nome do App e clique-o **em seguida**.



Etapa 7. Na integração de SAML, crie a página de SAML incorporam os detalhes.

- **Escolha o sinal na URL** - Dos metadata arquive, incorpore a URL especificados dentro como o deslocamento predeterminado 0 de AssertionConsumerService.

```
<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cuicpub-ids.pavdave.xyz:8553/ids/saml/response" index="0" isDefault="true"/>
```

- **Use isto para o receptor URL e o destino URL** - verifique esta opção para permitir a harmonização do receptor e do destino URL
- **Permita que este app peça o outro SSO URL** - verifique esta opção se você tem Nós múltiplos dos IdS em seu desenvolvimento e para querer permitir pedidos do outro SSO URL além do editor dos IdS.
  - **Requestable SSO URL** — Este campo aparece somente se você verifica a caixa de verificação acima. Você pode incorporar SSO URL para seus outros Nós. Você pode

encontrar que o ACS URL nos metadata arquiva procurando por todos os endereços de AssertionConsumerService (ACS) que usam o emperramento HTTP-POST. Adicionar aqueles detalhes para este campo. Clique adicionar um outro botão para adicionar URL múltiplas.

- **A audiência URI (entidade ID SP)** - dos metadata arquiva, incorpora o endereço do **entityID**.
  `<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="`**`cuicpub-ids.pavdave.xyz`**`">`

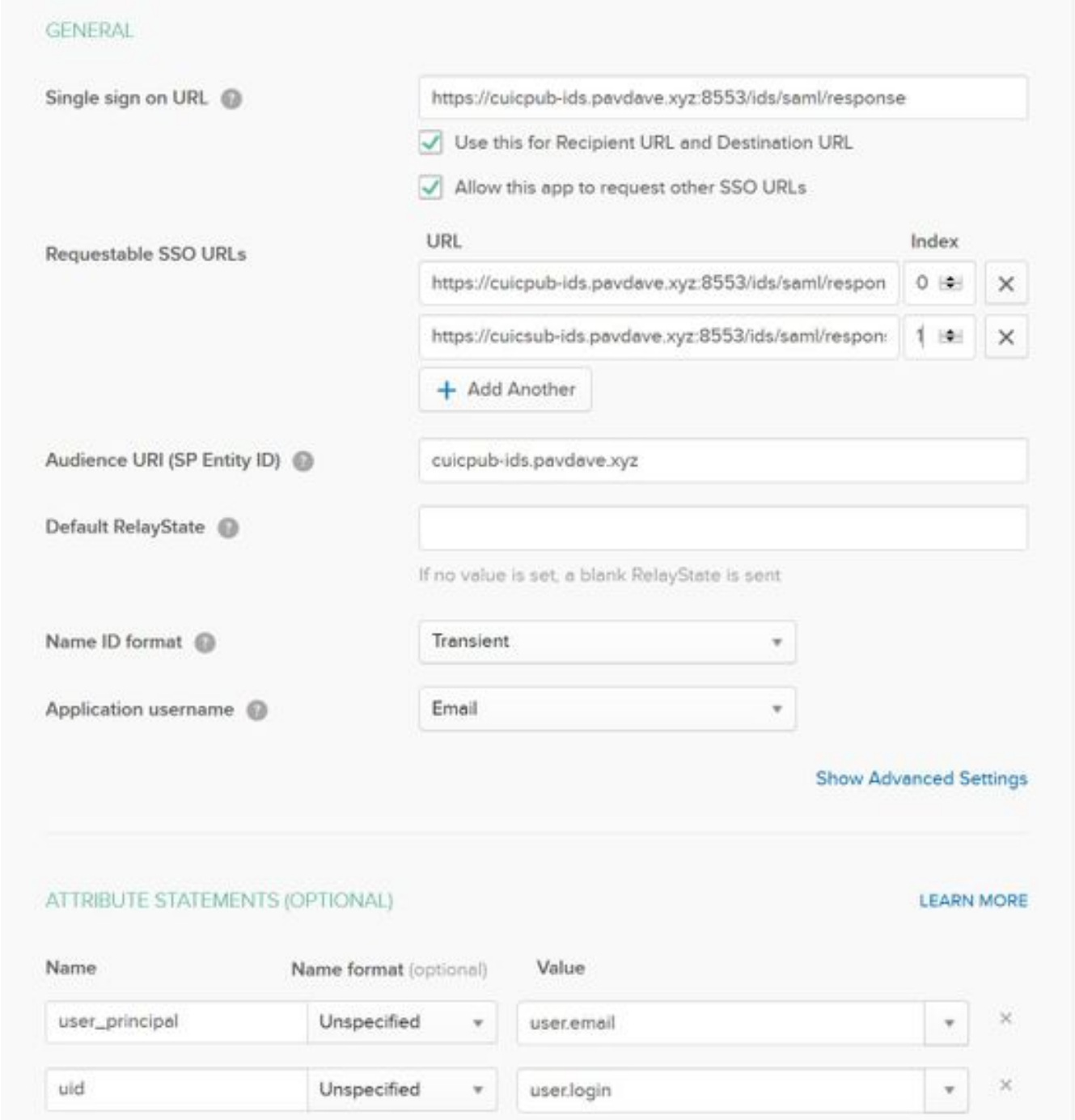
- **Padrão RelayState** - Deixe esta placa do campo.
- **Nomeie o formato ID -** Escolha o **transeunte da** lista de drop-down.
- **Username do aplicativo** - Escolha o formato username que combina o **username** configurado na **administração unificada CCE > controla > agentes.**

Note: Este tiro de tela é específico a UCCE/PCCE.

Etapa 8. Adicionar as indicações do atributo requerido.

- **uid** - Identifica o usuário autenticado na reivindicação enviada aos aplicativos
- **user_principal** - Identifica o reino da autenticação do usuário na afirmação enviada ao serviço da identidade de Cisco

.



Etapa 9. Selecione **em seguida.**

Etapa 10. Seleto “**eu sou um fornecedor de software. Eu gostaria de integrar meu app com Okta**” e de clicar o revestimento.

Etapa 11. **No sinal na** transferência da aba os **metadata do fornecedor da identidade.**

Etapa 12. Abra os metadata transferidos arquivam e mudam as duas linhas de NameIDFormat ao seguinte e salvar o arquivo.

```
<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cuicpub-ids.pavdave.xyz">
```

Configurar o serviço da identidade

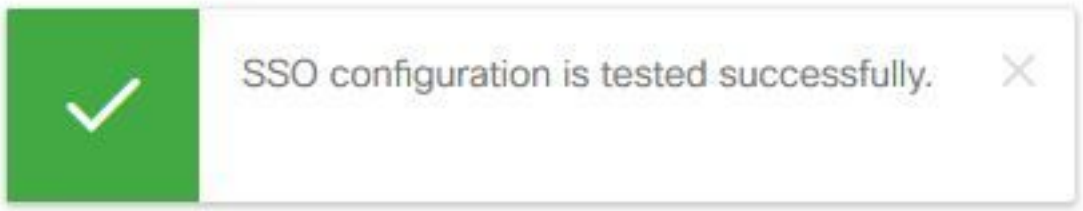
Etapa 1. Navegue a seu server do serviço da identidade.

Etapa 2. **Ajustes do** clique**.**

Etapa 3. Clique **em seguida.**

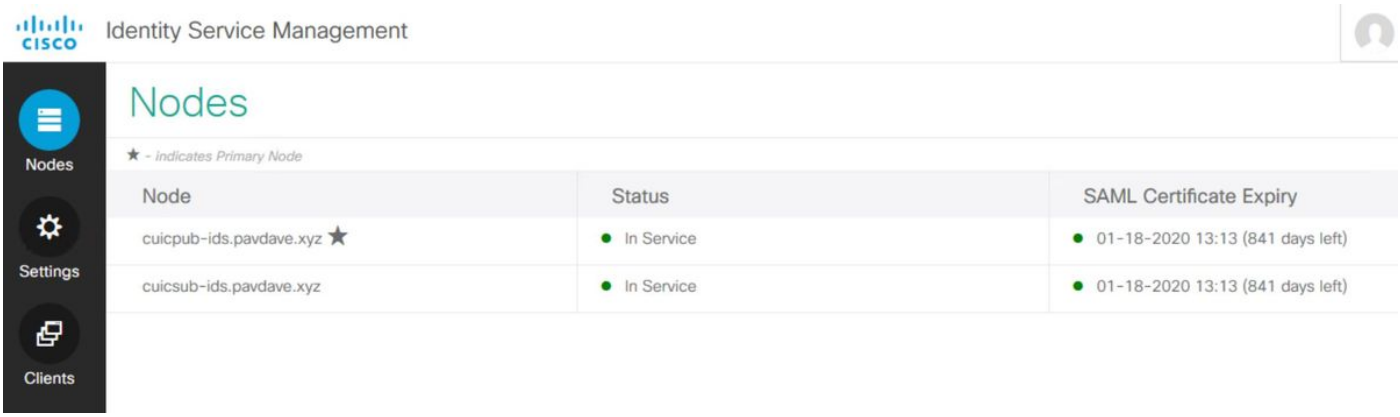
Etapa 4. Os metadata da transferência de arquivo pela rede arquivam transferido de Okta e clicam **em seguida**.

Etapa 5. **Instalação do teste SSO do** clique. Uma nova janela alertará um início de uma sessão autenticar a Okta. Um login bem-sucedido mostrará que um sinal com **configuração SSO está testado com sucesso no** canto inferior direito da tela.



> **Note**: Se você é autenticado já a Okta você não estará alertado entrar outra vez mas verá um breve PNF-acima quando os IdS verificarem credenciais.

Neste momento a configuração do serviço da identidade e dos fornecedores da identidade está completa e deve considerar os Nós no serviço.



Configuração mais adicional para único Sinal-em

Após a identidade preste serviços de manutenção e o fornecedor da identidade é configurado, a próxima etapa é estabelecer único Sinal-para em UCCE ou em UCCX.

- UCCE/PCCE
- UCCX

Leitura futura

- UCCE/PCCE escolhem Sinal-em
- UCCX escolhem Sinal-em

- Gerente das comunicações unificadas de Cisco (CUCM) - Configuração do fornecedor da identidade de Okta