

Configurar o portal de convidados do ISE 2.3 com OKTA SAML SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[SSO Federado](#)

[Fluxo de rede](#)

[Configurar](#)

[Etapa 1. Configure o provedor de identidade e o portal de convidado do SAML no ISE.](#)

[1. Preparar Fonte de Identidade Externa.](#)

[2. Criar portal para SSO.](#)

[3. Configure o login alternativo.](#)

[Etapa 2. Configure o aplicativo OKTA e as configurações do provedor de identidade SAML.](#)

[1. Criar Aplicativo OKTA.](#)

[2. Exportar informações de SP do provedor de identidade SAML.](#)

[3. Configurações do OKTA SAML.](#)

[4. Exportar metadados do aplicativo.](#)

[5. Atribuir usuários ao aplicativo.](#)

[6. Importar Metadados de Idp para ISE.](#)

[Etapa 3. Configuração do CWA.](#)

[Verificar](#)

[Verificação do usuário final](#)

[Verificação do ISE](#)

[Troubleshoot](#)

[Solução de problemas OKTA](#)

[Solução de problemas do ISE](#)

[Problemas e soluções comuns](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como integrar o Identity Services Engine (ISE) ao OKTA, para fornecer autenticação SAML SSO (Security Assertion Markup Language Single Sign-On) para o portal do convidado.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviços para convidados do Cisco Identity Services Engine.
- SAML SSO.
- (opcional) configuração de Wireless LAN Controller (WLC).

Componentes Utilizados

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

- Identity Services Engine 2.3.0.298
- aplicativo SSO OKTA SAML
- Controlador sem fio Cisco 5500 versão 8.3.141.0
- Lenovo Windows 7

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

SSO Federado

Um usuário na organização pode se autenticar uma vez e, em seguida, ter acesso a vários recursos. Essa identidade usada em organizações é chamada de identidade federada.

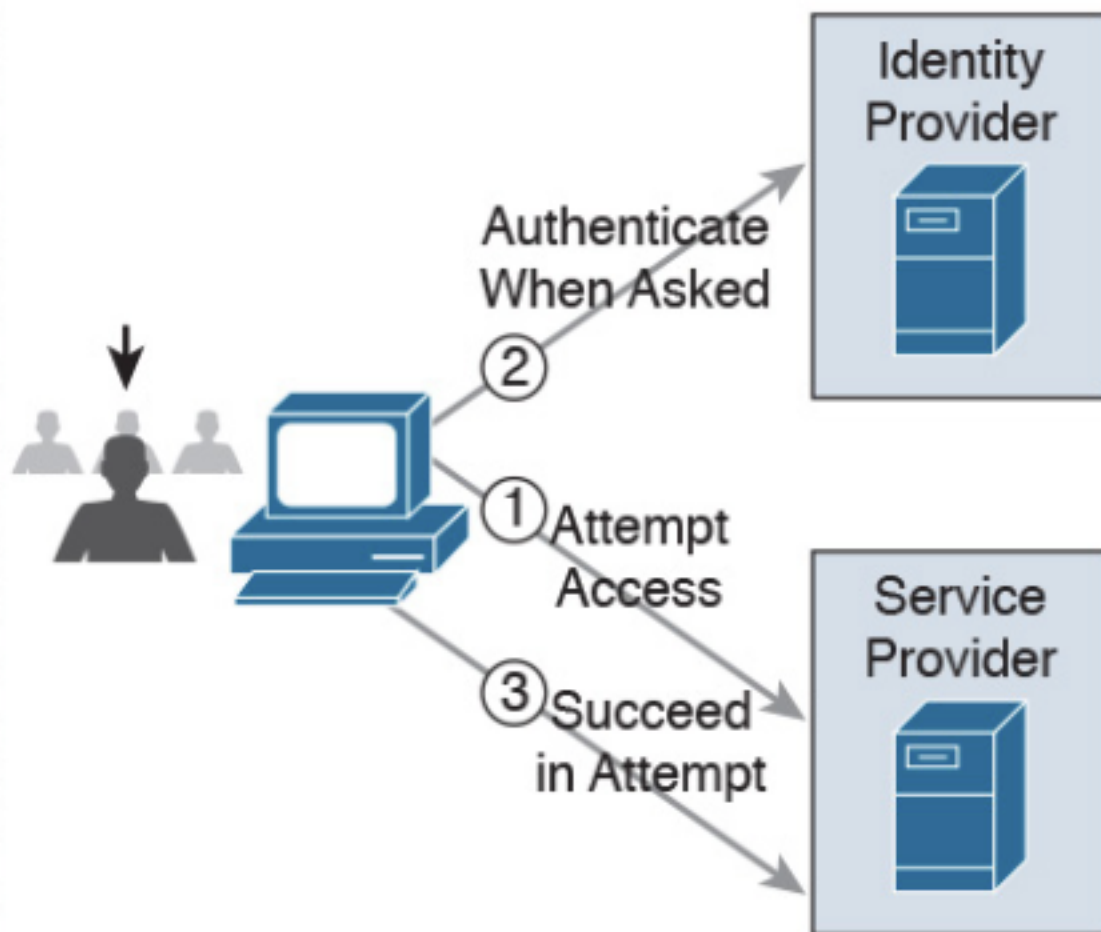
O conceito de federação:

- Princípio: Usuário final (o que solicita um serviço), navegador da Web, neste caso, é o endpoint.
- Provedor de serviços (SP): às vezes chamado de entidade confiadora (RP), que é o sistema que fornece um serviço, neste caso, ISE.
- Provedor de identidade (IdP): que gerencia a autenticação, o resultado da autorização e os atributos que são enviados de volta à controladora de armazenamento, nesse caso, o OKTA.
- Declaração: as informações do usuário enviadas pelo IdP ao SP.

Vários protocolos implementam SSO, como OAuth2 e OpenID. O ISE usa SAML.

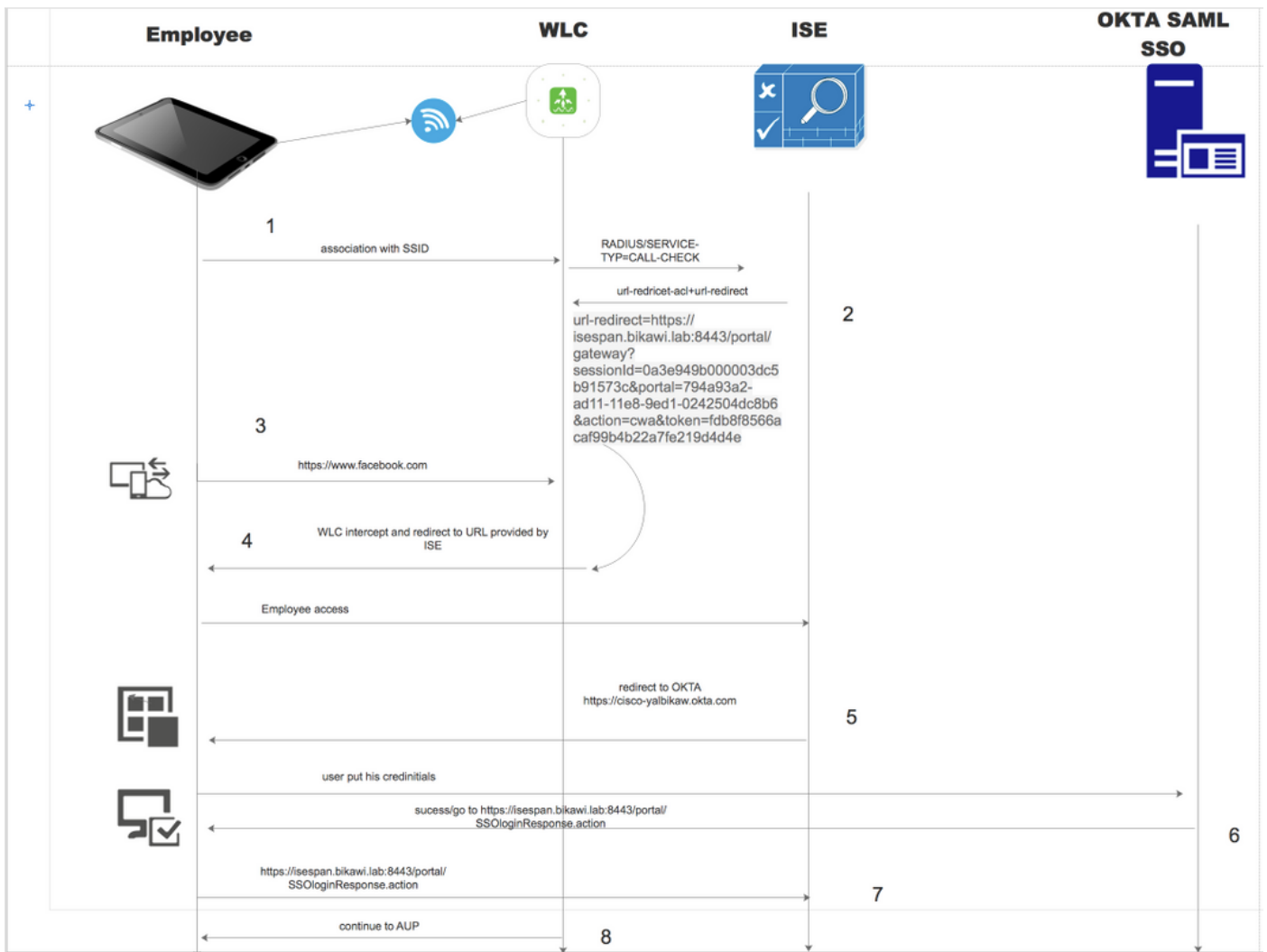
SAML é uma estrutura baseada em XML que descreve o uso e a troca de asserções SAML de forma segura entre entidades de negócios. O padrão descreve a sintaxe e as regras para solicitar, criar, usar e trocar essas asserções.

O ISE usa o modo iniciado pelo SP. O usuário é redirecionado para o portal Convidado e, em seguida, o ISE o redireciona para o IdP para autenticação. Depois disso, ele redireciona de volta para o ISE. A solicitação é validada, o usuário prossegue com o acesso do convidado ou com a integração, dependendo da configuração do portal.



SP-initiated

Fluxo de rede



1. O usuário se conecta ao SSID e a autenticação é a filtragem mac (mab).
2. O ISE responde com aceitação de acesso que contém atributos Redirect-URL e Redirect-ACL
3. O usuário tenta acessar www.facebook.com.
4. A WLC intercepta a solicitação e redireciona o usuário para o portal de convidados do ISE, o usuário clica no acesso do funcionário para registrar o dispositivo com credenciais de SSO.
5. O ISE redireciona o usuário para o aplicativo OKTA para autenticação.
6. Após a autenticação bem-sucedida, o OKTA envia a resposta de asserção SAML ao navegador.
7. O navegador retransmite a asserção de volta ao ISE.
8. O ISE verifica a resposta da asserção e, se o usuário estiver corretamente autenticado, ele continua para AUP e, em seguida, com registro de dispositivo.

Verifique o link abaixo para obter mais informações sobre o SAML

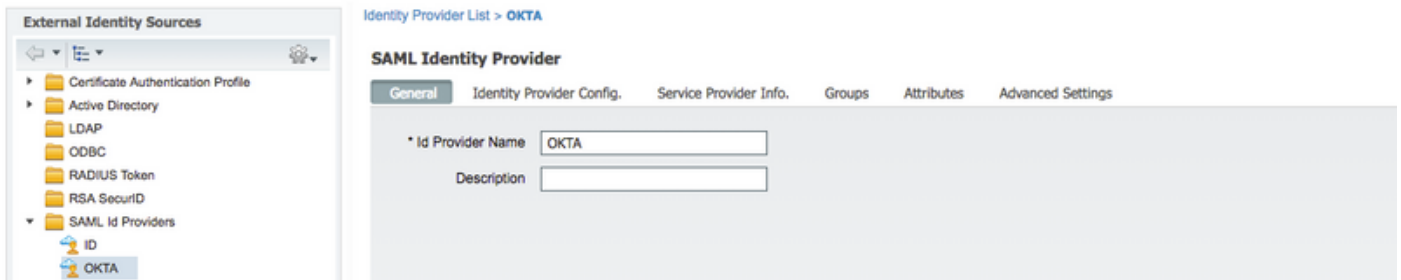
<https://developer.okta.com/standards/SAML/>

Configurar

Etapa 1. Configure o provedor de identidade e o portal de convidado do SAML no ISE.

1. Preparar Fonte de Identidade Externa.

Etapa 1. Navegue até **Administration > External Identity Sources > SAML id Providers**.

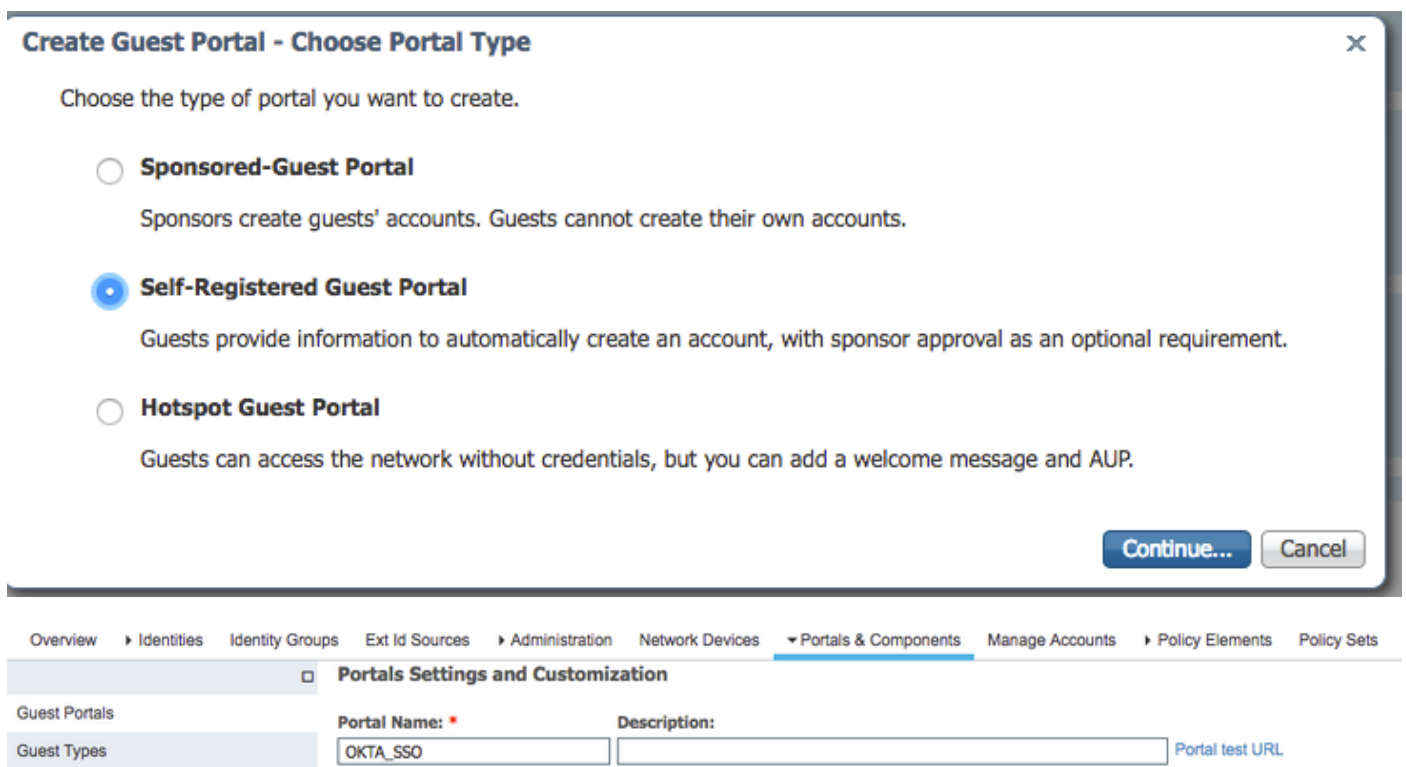


Etapa 2. Atribua um nome ao provedor de ID e envie a configuração.

2. Criar portal para SSO.

Etapa 1. Crie o portal atribuído ao OKTA como fonte de identidade. Qualquer outra configuração para BYOD, registro de dispositivos, Convidado etc. é exatamente a mesma do portal normal. Neste documento, o portal é mapeado para o portal do convidado como um login alternativo para o funcionário.

Etapa 2. Navegue até **Centros de trabalho > Acesso de convidado > Portais e componentes** e crie o portal.



Etapa 3. Escolha o método de autenticação para apontar para o provedor de identidade configurado anteriormente.

Authentication method: * **OKTA** ⓘ

Configure authentication methods at:
[Work Centers > Guest Access > Identities > Identity Source Sequences](#)
[Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers](#)

Etapa 4. Escolha a origem da identidade OKTA como um método de autenticação.

(opcional) escolha as configurações de BYOD.

▼ **BYOD Settings**

Allow employees to use personal devices on the network

Endpoint identity group: **RegisteredDevices** ⓘ

Configure endpoint identity groups at
[Administration > Identity Management > Groups > Endpoint Identity Groups](#)

The endpoints in this group will be purged according to the policies defined in:
[Administration > Identity Management > Settings > Endpoint purge](#)

Allow employees to choose to guest access only

Display Device ID field during registration

Configure employee registered devices at
[Work Centers > BYOD > Settings > Employee Registered Devices](#)

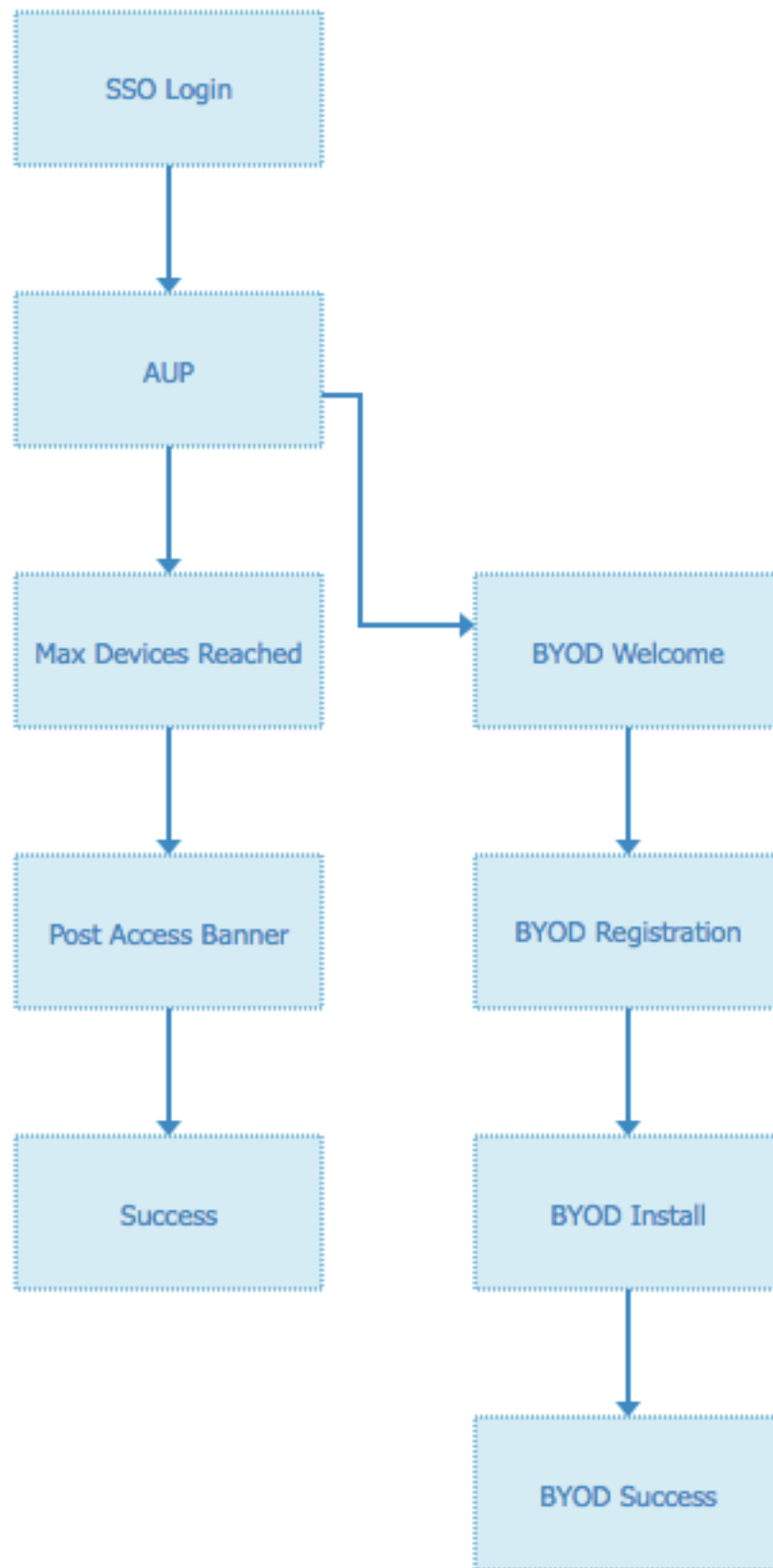
After successful device configuration take employee to:

Originating URL ⓘ

Success page

URL:

Etapa 5. Salve a configuração do portal, com a consumerização de TI, o fluxo é semelhante a este:



3. Configure o login alternativo.

Note: Você pode pular esta parte se não estiver usando o login alternativo.

Navegue até o Portal de convidado de registro automático ou qualquer outro portal personalizado

para acesso de convidado.

Nas configurações da página de login, adicione o portal de login alternativo: OKTA_SSO.

▼ Login Page Settings

Require an access code:

Maximum failed login attempts before rate limiting: (1 - 999)

Time between login attempts when rate limiting: minutes (1 - 3000)

Include an AUP ↕

Require acceptance

Require scrolling to end of AUP

Allow guests to create their own accounts

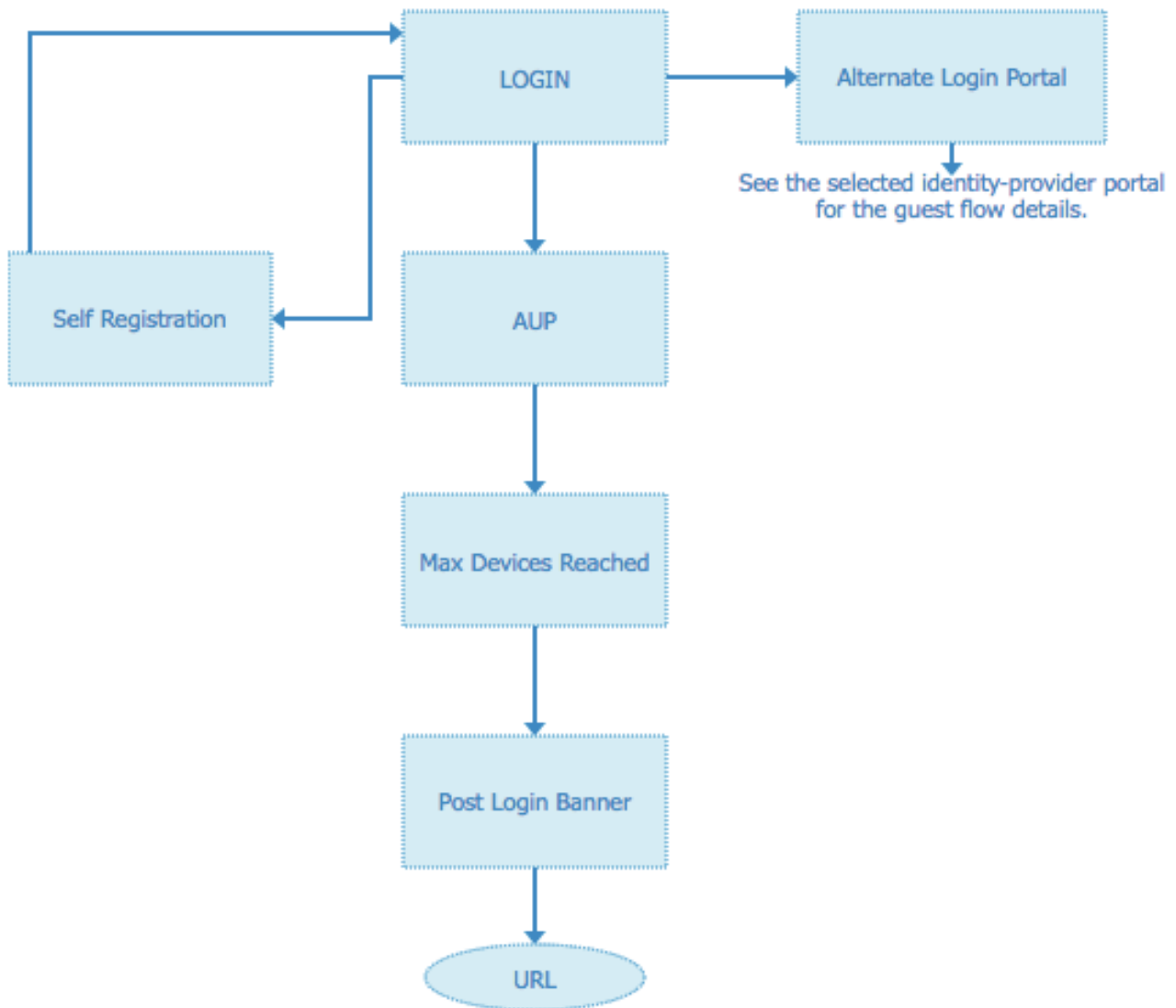
Allow social login

Allow guests to change password after login ⓘ

Allow the following identity-provider guest portal to be used for login ⓘ

↕

Esse é o fluxo do portal agora.



Etapa 2. Configure o aplicativo OKTA e as configurações do provedor de identidade SAML.

1. Criar Aplicativo OKTA.

Etapa 1. Faça login no site OKTA com uma conta de administrador.

← Back to Applications

Add Application

Search for an application

All A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Can't find an app?
Create New App
Apps you created (0) →

INTEGRATION PROPERTIES

Any
Supports SAML
Supports Provisioning

	Teladoc Okta Verified	Add
	&frankly Okta Verified ✓ SAML	Add
	10000ft Okta Verified	Add
	101domains.com Okta Verified	Add

Etapa 2. Clique em Add Application (Adicionar aplicativo).

okta Dashboard Directory Applications Security Reports Settings My Applications

Applications Help

Add Application Assign Applications

Q Search

STATUS

ACTIVE	0
INACTIVE	3

No active apps found
Add application and assign access to have them appear on your users' Okta home Page

© 2018 Okta, Inc. Privacy Version 2018.36 US Cell 7 Trust site Download Okta Plugin Feedback

Etapa 3. Criar novo aplicativo, escolha-o como SAML2.0

Create a New Application Integration



Platform

Web

Sign on method



Secure Web Authentication (SWA)

Uses credentials to sign in. This integration works with most apps.



SAML 2.0

Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.



OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

Configurações gerais

Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

1 General Settings

App name

ISE-OKTA

App logo (optional) ?



Browse..

Upload Logo

App visibility



Do not display application icon to users

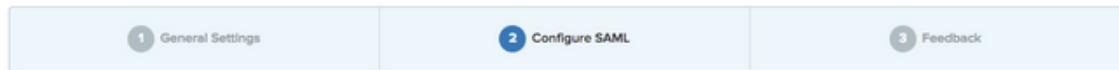


Do not display application icon in the Okta Mobile app

Cancel

Next

Create SAML Integration



A SAML Settings

GENERAL

Single sign on URL

Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
------	------------------------	-------

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

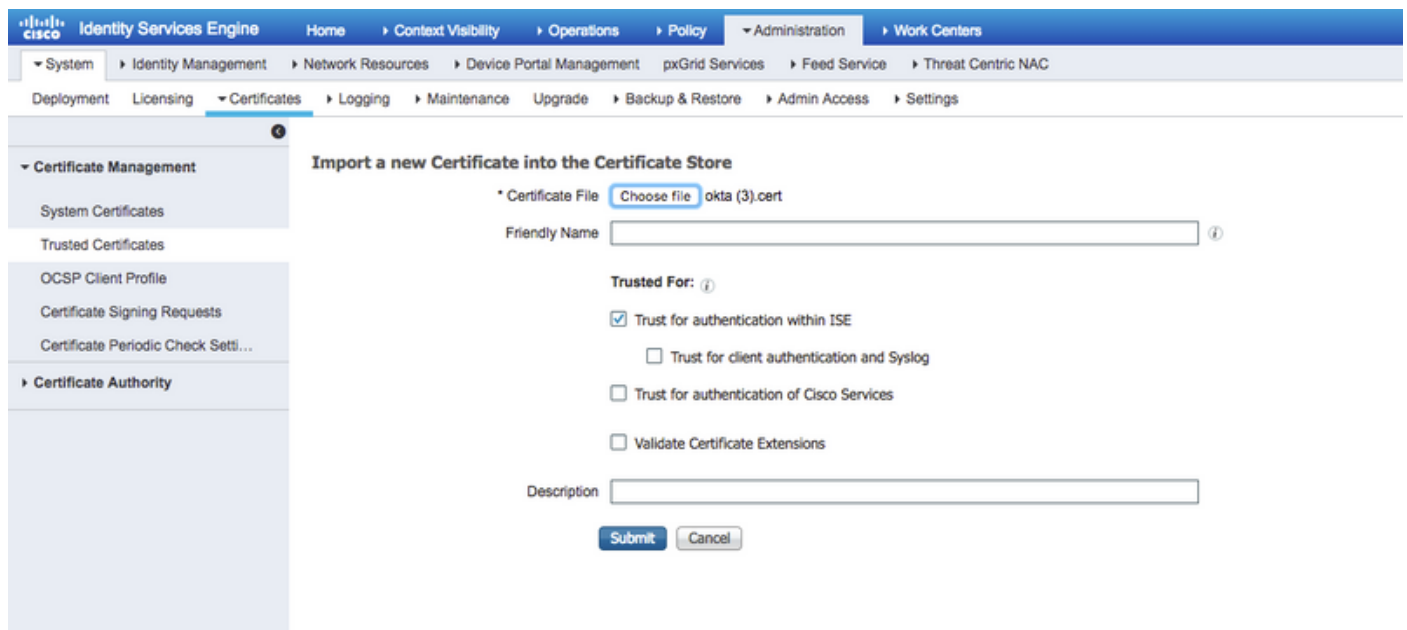
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

Etapa 4. Baixe o certificado e instale-o em certificados confiáveis do ISE.



2. Exportar informações de SP do provedor de identidade SAML.

Navegue até o provedor de identidade configurado anteriormente. Clique em **Informações do provedor de serviços** e exporte-as, como mostrado na imagem.

SAML Identity Provider

- General
- Identity Provider Config.
- Service Provider Info.**
- Groups
- Attributes
- Advanced Settings

Service Provider Information

Load balancer

Export Service Provider Info.

Includes the following portals:

OKTA__SSO

A pasta zip exportada contém o arquivo XML e **readme.txt**

```
<?xml version="1.0" encoding="UTF-8" ?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546" ?><md:SPSSODescriptor
AuthnRequestsSupported="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" ?><md:KeyDescriptor use="signing" ?><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/
ExportQ1UQXZLz29NkYw4YmlrY0pLaxhYjAePvbyQDA4MDYNTTEyNTBaPwBwOTA4NDYxNTEyNTBa
MCDxIDAeBgnVBAITfNBtUxfaW1c3hb1S1amhd2kubGFJHTIIBjANBkgkhk1G9wBQAOC
AQ8AMITBcGKCAQEAuxUM49zQVf51hGzphUFUK7Bbo4mf890E1o21amdb8o9FwoDzuHf8rLX7WV
tsFfv0Zb1cWEnAFPTfabxu3ooXLTJHTKofmzF8GwCE7od2PfCyycoEJcncu1Bh/mfe980s
vL+1Z/Pq7oTrupYe/XZLHdyIhoy2xuE8sMomevB85w5DZVJL+nNpUr7j1e+31j3toJdc9k+c1
mxz6GX49R1BqR3jehFoxL+PMCSMbULUJ0sJdInqNv754jnzR9McBqWapQxdIR03wxsEj2BpZ
7X5s+2M/51p1IapUrmtdo2K+h0Z2FT8T8BLDtp0B3R8K9KwIDMqA8o24wDmVgkHMYE
BTADQh/PASGA11dVdQEAwLCTDAdB9VWQEFp0L8pFk4enoxGf+3/p8LaoZ9h3h4WdV98L
BBYvAYIXWY8BQKAwEGCCsGAQJFBNwCHBEGOMCGSAGG+EIBA0QEAwLGG0ANBqkqh1G9wBQAQsP
AAOCQAQEAHxj5Ug2pPozdVkkjDxzMoj1u9s9EvOKSyzGFQ4vuF1q4rh293KkayVRR4w7E+HM
QSNvEPRI1VgQMDLKKfddAyRUYy8ALBye4dppjt1KZcRfZ1Bkhlez0PkVYk9xR4d01PnH+53pbYk9hx
D1Reu6LYo6prZI9MqsAwax1THh+5v6h0Po79okhh3HdsZM6FJHFwTYh0mKwIGC4PxA2CF1KL9
GBTyJ8pJmP3YMBU/z1oG/pX+gVU07nHed02Z0ty4o2eupYwBzFr88pE2q3zHf9THfJgFJ00Op
PALpV38FA1GqbJbXcooAPULPEKID7q1xstD05Llq4e==</ds:KeyInfo></md:KeyDescriptor><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:
NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:windowsDomainQualifiedName</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.48.35.19:8443/portal/SSOLoginResponse.action" index="0"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.48.17.71:8443/portal/SSOLoginResponse.action" index="1"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action" index="2"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action" index="3"/></md:SPSSODescriptor></md:EntityDescriptor>
```

Para alguns provedores de identidade, você pode importar o XML diretamente, mas nesse caso, ele precisa importar manualmente.

- URL de início de sessão único (asserção de exemplo)

```
Location="https://10.48.35.19:8443/portal/SSOLoginResponse.action"
Location="https://10.48.17.71:8443/portal/SSOLoginResponse.action"

Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action"
Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action"
```

- ID da entidade do SP

entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"

O URL SSO disponível no endereço IP e formato FQDN.

Caution: A seleção de formato depende das configurações de redirecionamento no perfil de autorização. Se você usar o ip estático, use o endereço ip para o URL do SSO.

3. Configurações do OKTA SAML.

Etapa 1. Adicione esses URLs às configurações de SAML.

A SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Requestable SSO URLs

URL

Index

[+ Add Another](#)

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Etapa 2. Você pode adicionar mais de um URL do arquivo XML, com base no número de PSNs que hospedam esse serviço. O formato de ID de nome e o nome de usuário do aplicativo dependem do seu design.

B Preview the SAML assertion generated from the information above

[<> Preview the SAML Assertion](#)

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

[Previous](#)

[Cancel](#)

[Next](#)

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
```

```
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124"
IssueInstant="2018-09-21T15:47:03.790Z" Version="2.0">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">http://www.okta.com/Issuer</saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:x509SubjectName">userName</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2018-09-21T15:52:03.823Z"
Recipient="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2018-09-21T15:42:03.823Z" NotOnOrAfter="2018-09-
21T15:52:03.823Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>http://CiscoISE/9c969a72-b9cd-11e8-a542-
d2e41bbdc546</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2018-09-21T15:47:03.790Z">
    <saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</s
aml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

Etapa 3. Clique em Next (Avançar) e escolha a segunda opção.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

Is your app integration complete?

Yes, my app integration is ready for public use in the Okta Application Network

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Previous

Finish

4. Exportar metadados do aplicativo.

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Metadados:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exklrq8loEmedZSf4356">
<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIDrDCCApSgAwIBAgIGAWWPlTasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXlhbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFglpbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNDMwNDMwNDMwNDMwNDMwNDMwNDMwNDMw
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEjEXMBUGA1UEAwwOY2lzMTEwNDMwNDMw
YXcXcHDAaBgkqhkiG9w0BCQEWDWluZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
ggEKAoIBAQC1P7DvZvng7wSQWVOzGShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8ulZ8HUsOspBECLYcI75gH4rpc2FM4kzZiDbNLb95AW6dlUztC66x42uhRYgduD5+w3/yvdwx
l99upWb6SdrtnwK8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgJYQO/7GRK2RzOj
bSZgeAp5Yyytja3NCn9x6FMY5Rppc3HjtG4cJQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dN6YERuV5C5eHUXq3KGul2yIfih7x8EartZ4/wGP/HYucNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbFqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdTsz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesysecPuWQtEqNqt+MyZnlCurJ0e+JTvKYH1dSWapM1dzqoX
OzyF7yiId9KPP6I4Ndc+BXe1dA8imneYy5MH7/nE/g=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</md:NameIDFormat>
<md:NameIDFormat>
```



```
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml" />
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml" />
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Salve o arquivo no formato XML.

5. Atribuir usuários ao aplicativo.

Atribuir usuários a este aplicativo, há uma forma de integração do AD, explicada em: [diretório octa-ativo](#)

6. Importar Metadados de Idp para ISE.

Etapa 1. Em **SAML Identity Provider**, selecione **Identity Provider Config.** e Importar Metadados.

Subject	Issuer	Valid From	Valid To (Expiration)	Serial Number
EMAILADDRESS=info@okta.com, CN=cisco-yalbi...	EMAILADDRESS=inf...	Fri Aug 31 10:43:05 ...	Thu Aug 31 10:44:05 ...	01 65 8F 95 36 AC

Etapa 2. Salve a configuração.

Etapa 3. Configuração do CWA.

Este documento descreve a configuração para ISE e WLC.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

Adicione URLs na ACL de redirecionamento.

<https://cisco-yalbikaw.okta.com> / adicione o URL do seu aplicativo

<https://login.okta.com>

[REDIRECT-ACL](#)

IPv4

- Remove
- Clear Counters
- Add-Remove URL


Foot Notes


1. Counter configuration is global for acl, urlacl and layer2acl.

Verificar

Teste o portal e verifique se você consegue acessar o aplicativo OKTA

Portal Name: * Description: [Portal test URL](#)

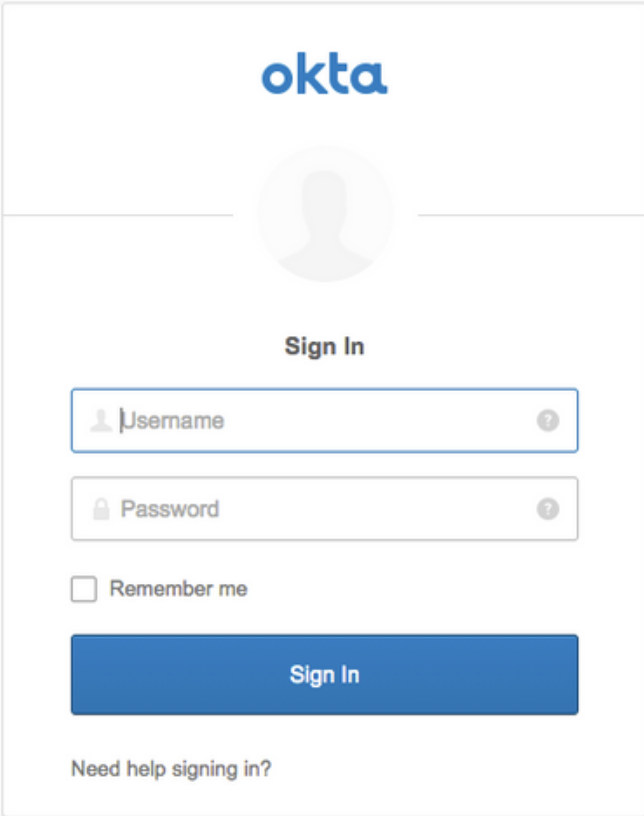
 **Portal Behavior and Flow Settings**
Use these settings to specify the guest experience for this portal.

 **Portal Page Customization**
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Etapa 1. Clique no teste do portal e, em seguida, você deve ser redirecionado para o aplicativo SSO.

Connecting to

Sign-in with your cisco-org-808433 account to access ISE-OKTA



The image shows a screenshot of the Okta sign-in interface. At the top, the Okta logo is displayed in blue. Below the logo is a circular placeholder for a user profile picture. Underneath the picture is the text "Sign In". The form contains two input fields: "Username" and "Password", each with a small question mark icon to its right. Below these fields is a checkbox labeled "Remember me". A large blue button with the text "Sign In" is positioned below the checkbox. At the bottom of the form, there is a link that says "Need help signing in?".

Etapa 2. Verifique a **conexão** de informações **com o <nome do aplicativo>**

Etapa 3. Se você digitar as credenciais que podem estar com uma solicitação de amostra incorreta, isso não significa necessariamente que a configuração esteja errada neste ponto.

Verificação do usuário final

You can access the Internet.



Sign On
Sign on for guest access.

Username:

Password:

Sign On

[Or register for guest access](#)

You can also login with



You can access the Internet.

Connecting to

Sign-in with your cisco-org-808433 account to access ISE-OKTA

okta



Sign In

okta-test@cisco.com

Remember me

Sign In

[Need help signing in?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



Guest Portal

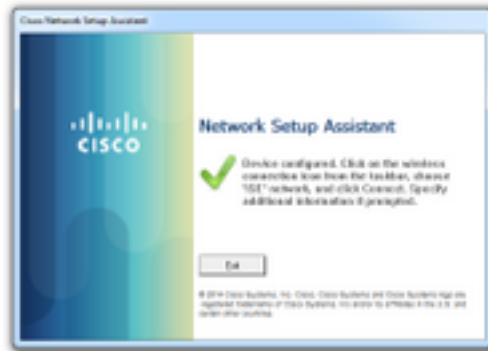
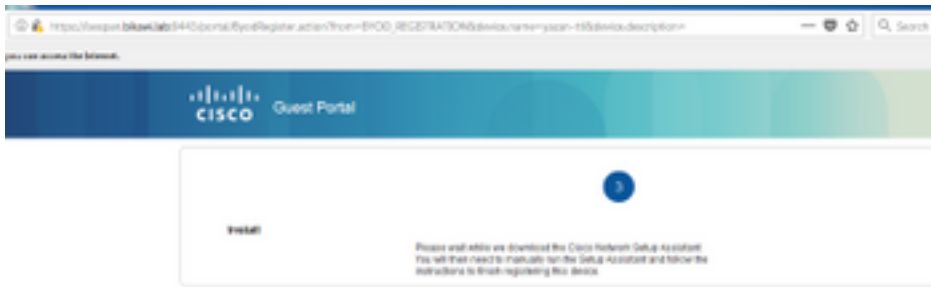
Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy. You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Verificação do ISE

Verifique os registros de vida útil para verificar o status da autenticação.

Sep 30, 2018 12:39:09.514 AM	✓	🔒	okta-test@cisco.c...	3C:A8:F4:34:9F:70					
Sep 30, 2018 12:33:32.640 AM	✓	🔒		3C:A8:F4:34:9F:70	3C:A8:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest	yazan-cpp

Troubleshoot

Solução de problemas OKTA

Etapa 1. Verifique os registros na guia **Relatórios**.

Reports

Help

Okta Usage LAST 30 DAYS

0 users have never signed in 3 users have signed in

[Okta Password Health](#)

Application Usage LAST 30 DAYS

8 apps with unused assignments 2 unused app assignments

[App Password Health](#) [SAML Capable Apps](#)

Auth Troubleshooting

Okta Logins (Total, Failed) Auths Via AD Agent (Total, Failed)

[SSO Attempts](#)

Application Access Audit

[Current Assignments](#)

Multifactor Authentication

[MFA Usage](#) [Yubikey Report](#)

System Log

- Agent Activity
- Application Access
- Application Membership Change
- Authentication Activity
- Policy Activity
- Provisioning Activity
- System Import Activity
- User Account Activity
- User Lifecycle Activity

Etapa 2. Também no aplicativo, veja os registros relacionados.

← Back to Applications



ISE-OKTA

Active ▾



[View Logs](#)

General Sign On Import **Assignments**

← Back to Reports

System Log

From: 09/23/2018 00:00:00 To: 09/30/2018 23:59:59 CEST Search: target.id eq "0ea7e81b031c201f9356" and target.type eq "AppInstance" [Advanced Filter / Reset Filters](#)



Show event trends by category

Events: 25 [Download CSV](#)

Time	Actor	Event Info	Targets
Sep 30 02:42:02	OKTA-TEST@ciscc.com OKTA (User)	User single sign on to app SUCCESS	ISE-OKTA (AppInstance) OKTA-TEST@ciscc.com OKTA (AppUser)
<ul style="list-style-type: none">Actor: OKTA-TEST@ciscc.com OKTA (id: 00122101010101010101010101010101)Client: FIREFOX on Windows 7 Computer from [REDACTED]Event: successful user.authentication.sso (id: W1a2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6)Request: ISE-OKTA (id: 0ea7e81b031c201f9356) AppInstanceTarget: OKTA-TEST@ciscc.com OKTA (id: 0ea218q9sPQqWbTc356) AppUser Expand All			

Solução de problemas do ISE

Há dois arquivos de log a serem verificados

- ise-psc.log
- guest.log

Navegue até **Administration > System > Logging > Debug Log Configuration**. Ative o nível para DEBUG.

SAML	ise-psc.log
Guestaccess	guest.log
Portal	guest.log

A tabela mostra o componente a ser depurado e seu arquivo de log correspondente.

Problemas e soluções comuns

Cenário 1. Solicitação SAML incorreta.

okta



400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

Esse erro é genérico, verifique os registros para verificar o fluxo e aponte o problema. No ISE guest.log:

ISE#show logging application guest.log | últimos 50

```
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][  
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:  
SSOLoginTransitionResult:
```

```
Portal Name: OKTA_SSO  
Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546  
Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
```

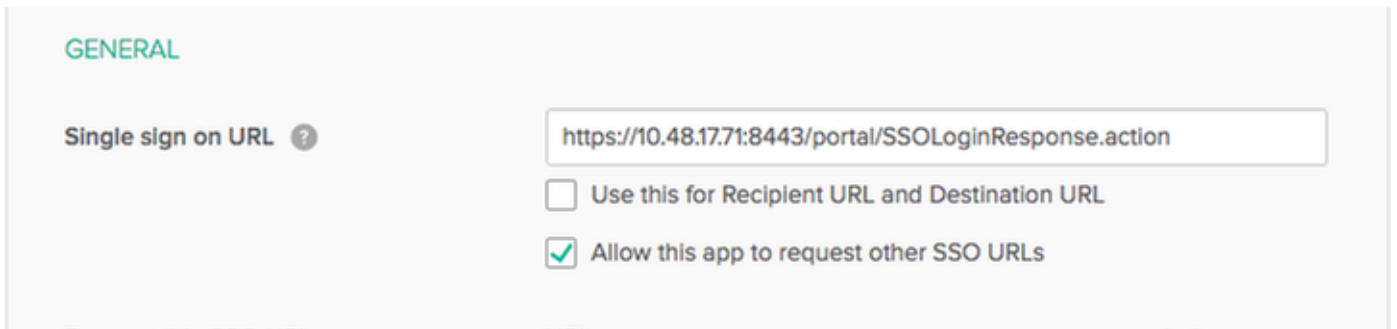


```
Identity Provider: com.cisco.cpm.acs.im.identitystore.saml.IdentityProvider@56c50ab6
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- portalSessionInfo:
portalId=9c969a72-b9cd-11e8-a542-d2e41bbdc546;portalSessionId=6770f0a4-bc86-4565-940a-
b0f83cbe9372;radiusSessi
onId=0a3e949b000002c55bb023b3;
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- no Load balancer is
configured; no redirect should be made
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- No redirect manipulation is
required - start the SAML flow with 'GET'...
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- Redirect to IDP:
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bzil1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnCh3jF072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_DELIMITERisepan.bikawi.lab
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.utils.Combiner -::- combined map: {redirect_required=TRUE,
sso_login_action_url=https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exklrq81oEmedZSf4356/sso/saml
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bzil1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnCh3jF072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_DELIMITERisepan.bikawi.lab
}
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalStepController -::- targetUrl:
pages/ssoLoginRequest.jsp
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalStepController -::- portalId: 9c969a72-b9cd-11e8-a542-d2e41bbdc546
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalStepController -::- webappPath: /portal
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalStepController -::- portalPath:
/portal/portals/9c969a72-b9cd-11e8-a542-d2e41bbdc546
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalPreResultListener -::- No page transition config.
Bypassing transition.
2018-09-30 01:32:35,627 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- result: success
```

O ISE redirecionou o usuário para o IDP com êxito. No entanto, nenhuma resposta de volta ao ISE e a solicitação SAML incorreta é exibida. Identifique se OKTA não aceita nossa solicitação SAML abaixo.

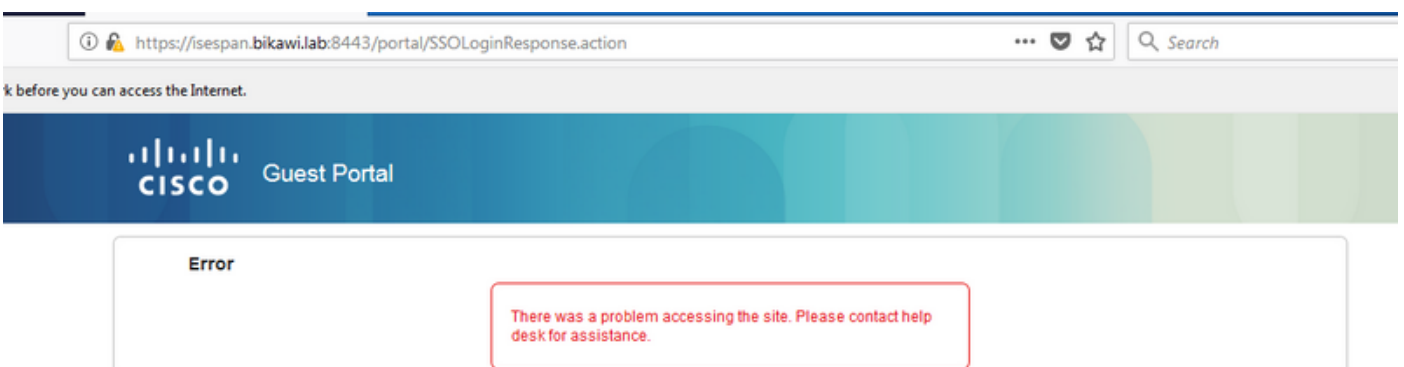
```
https://cisco-  
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0  
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTWSspuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BVyWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fB1QnC  
h3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n  
8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERport  
alId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-  
940a-  
b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_DELIMITERisespan.bikawi.lab
```

Agora, verifique novamente o aplicativo, talvez haja alterações feitas.



A URL do SSO está usando o endereço IP, no entanto, o convidado está enviando FQDN como podemos ver na solicitação acima da última linha contém SEMI_DELIMITER<FQDN> para corrigir esse problema e alterar o endereço IP para FQDN nas configurações OKTA.

Cenário 2. "Ocorreu um problema ao acessar o site. Entre em contato com o helpdesk para obter assistência".



Guest.log

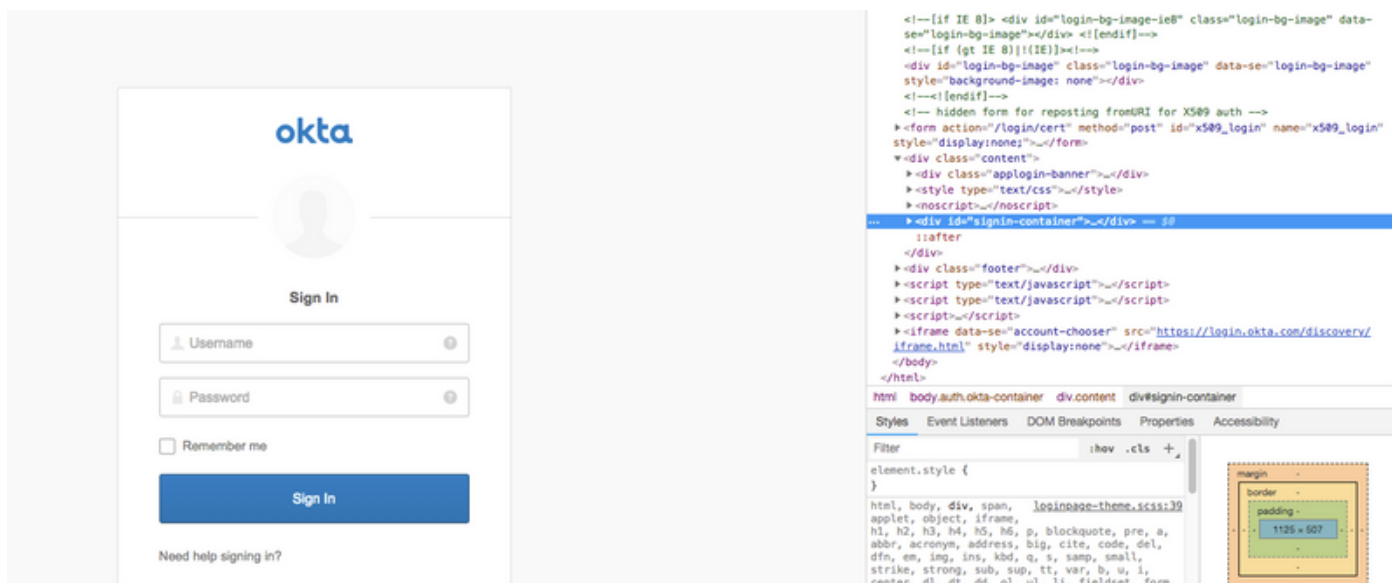
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][  
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::: SSO Authentication failed or  
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
```

```
contain ma
tching service provider identifier in the audience restriction conditions
2018-09-30 02:25:00,609 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][]
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- Login error with idp
```

Nos registros, o ISE informa que a Asserção não está correta. Verifique o URI do público OKTA para garantir que ele corresponda ao SP para resolvê-lo.

Cenário 3. Redirecionado para a página em branco ou a opção de login não é exibida.

Depende do ambiente e da configuração do portal. Nesse tipo de problema, você precisa verificar o aplicativo OKTA e qual URL ele precisa para autenticar. Clique no teste do portal e inspecione o elemento para verificar quais sites devem estar acessíveis.



Neste cenário, somente dois URLs: application e login.okta.com - esses devem ser permitidos na WLC.

Informações Relacionadas

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200551-Configure-ISE-2-1-Guest-Portal-with-Pin.html>
- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-23/213352-configure-ise-2-3-sponsor-portal-with-ms.html>
- <https://www.safaribooksonline.com/library/view/ccna-cyber-ops/9780134609003/ch05.html>
- <https://www.safaribooksonline.com/library/view/spring-security-essentials/9781785282621/ch02.html>
- <https://developer.okta.com>