

Configuración de ISE 2.3 Guest Portal con OKTA SAML SSO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[SSO federado](#)

[Flujo de red](#)

[Configurar](#)

[Paso 1. Configure SAML Identity Provider y el portal de invitados en ISE.](#)

[1. Preparar origen de identidad externo.](#)

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

[3. Configuración de inicio de sesión alternativo.](#)

[Paso 2. Configure la aplicación OKTA y los parámetros del proveedor de identidad SAML.](#)

[1. Crear aplicación OKTA.](#)

[2. Exportar información SP del proveedor de identidad SAML.](#)

[3. Configuración de OKTA SAML.](#)

[4. Exportar metadatos de la aplicación.](#)

[5. Asignar usuarios a la aplicación.](#)

[6. Importar metadatos de Idp a ISE.](#)

[Paso 3. Configuración de CWA.](#)

[Verificación](#)

[Verificación del usuario final](#)

[Verificación de ISE](#)

[Troubleshoot](#)

[Solución de problemas de OKTA](#)

[Solución de problemas de ISE](#)

[Problemas comunes y soluciones](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo integrar Identity Services Engine (ISE) con OKTA, para proporcionar autenticación de Lenguaje de marcado de aserción de seguridad de inicio de sesión único (SAML SSO) para el portal de invitados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios de invitados de Cisco Identity Services Engine.
- SAML SSO.
- (opcional) Configuración del controlador de LAN inalámbrica (WLC).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine 2.3.0.298
- aplicación OKTA SAML SSO
- Controlador inalámbrico Cisco 5500 versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

SSO federado

Un usuario dentro de la organización puede autenticarse una vez y después tener acceso a varios recursos. Esta identidad utilizada en las organizaciones se denomina identidad federada.

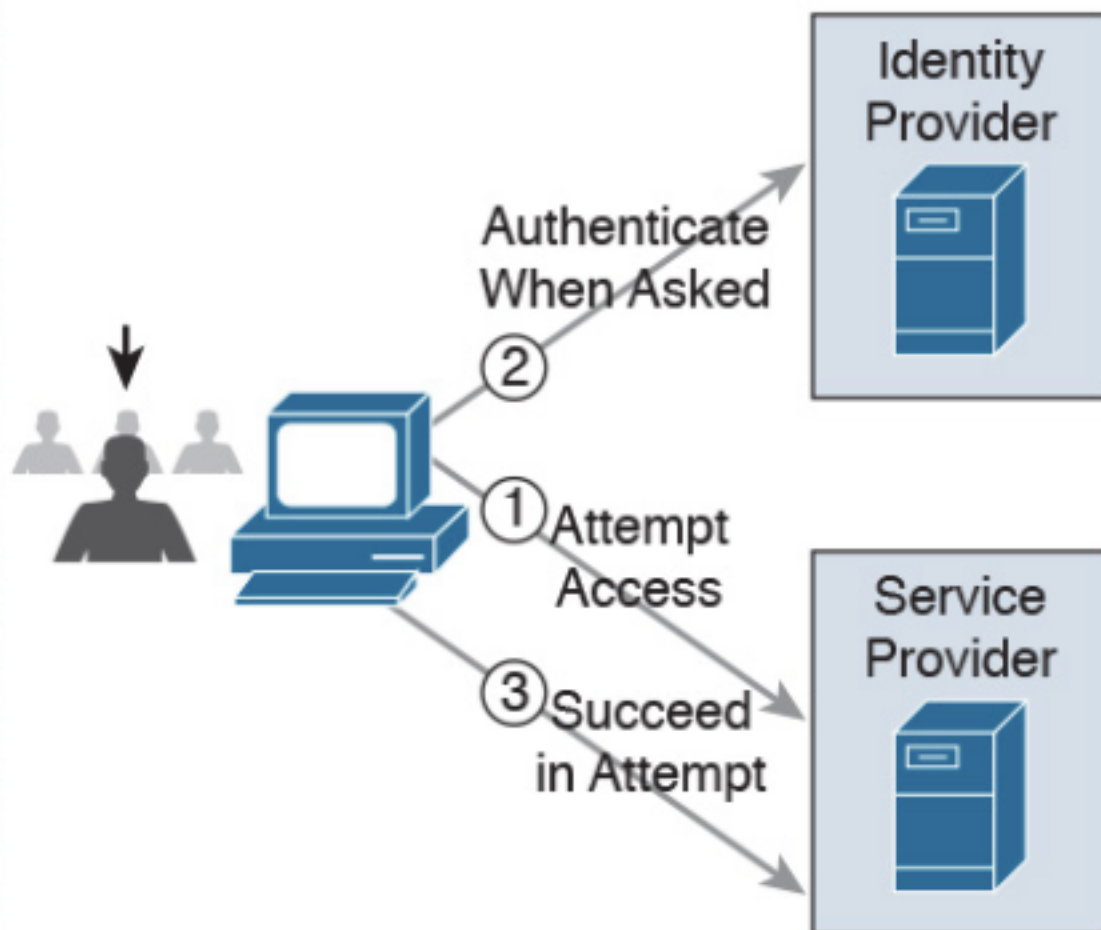
El concepto de federación:

- Principio: El usuario final (el que solicita un servicio), el navegador web, en este caso, es el terminal.
- Proveedor de servicios (SP): a veces se denomina parte de confianza (RP), que es el sistema que proporciona un servicio, en este caso, ISE.
- Proveedor de identidad (IdP): que administra la autenticación, el resultado de la autorización y los atributos que se envían de vuelta al SP, en este caso, OKTA.
- Afirmación: la información de usuario enviada por IdP al SP.

Varios protocolos implementan SSO como OAuth2 y OpenID. ISE utiliza SAML.

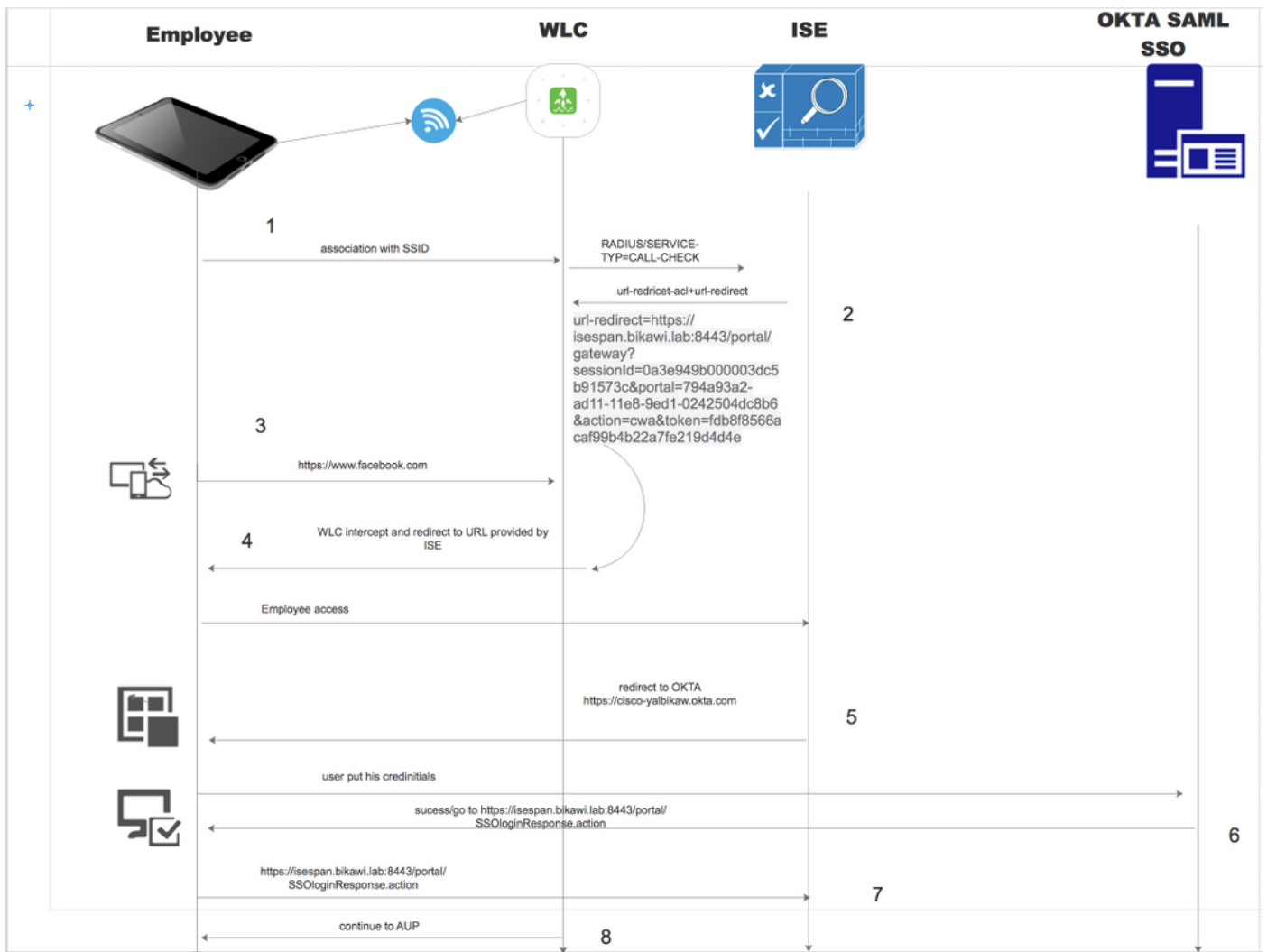
SAML es un marco basado en XML que describe el uso y el intercambio de aserciones SAML de forma segura entre entidades empresariales. El estándar describe la sintaxis y las reglas para solicitar, crear, utilizar e intercambiar estas afirmaciones.

ISE utiliza el modo iniciado por SP. El usuario se redirige al portal de invitados y, a continuación, ISE lo redirige a IdP para autenticarse. Después de eso, vuelve a redirigir a ISE. La solicitud se valida, el usuario continúa con el acceso de invitado o la incorporación, dependiendo de la configuración del portal.



SP-initiated

Flujo de red



1. El usuario se conecta al SSID y la autenticación es el filtrado mac (mab).
2. ISE responde con access-accept que contiene atributos Redirect-URL y Redirect-ACL
3. El usuario intenta acceder a www.facebook.com.
4. El WLC intercepta la solicitud y redirige al usuario al portal de invitados ISE, el usuario hace clic en el acceso del empleado para registrar el dispositivo con credenciales SSO.
5. ISE redirige al usuario a la aplicación OKTA para la autenticación.
6. Después de una autenticación exitosa, OKTA envía la respuesta de afirmación SAML al navegador.
7. El navegador retransmite la afirmación a ISE.
8. ISE verifica la respuesta de afirmación y, si el usuario está autenticado correctamente, pasa a AUP y luego con el registro del dispositivo.

Consulte el siguiente enlace para obtener más información sobre SAML

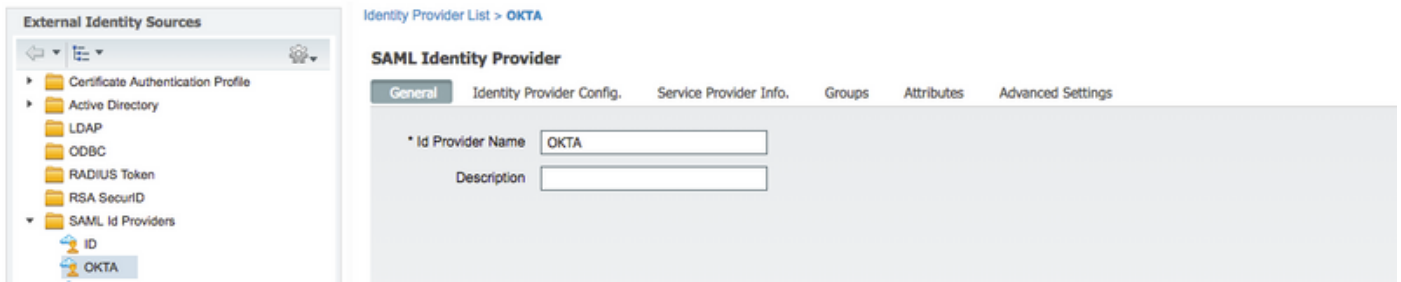
<https://developer.okta.com/standards/SAML/>

Configurar

Paso 1. Configure SAML Identity Provider y el portal de invitados en ISE.

1. Preparar origen de identidad externo.

Paso 1. Vaya a **Administration > External Identity Sources > SAML id Providers**.

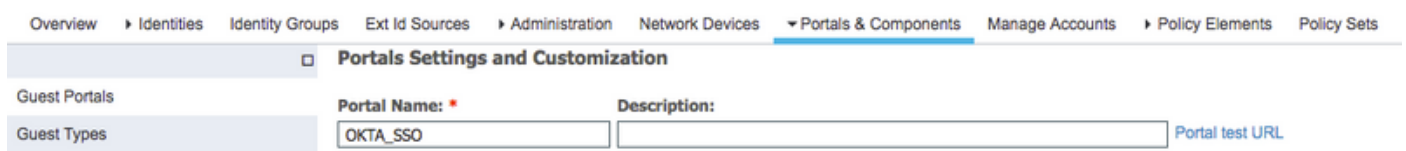
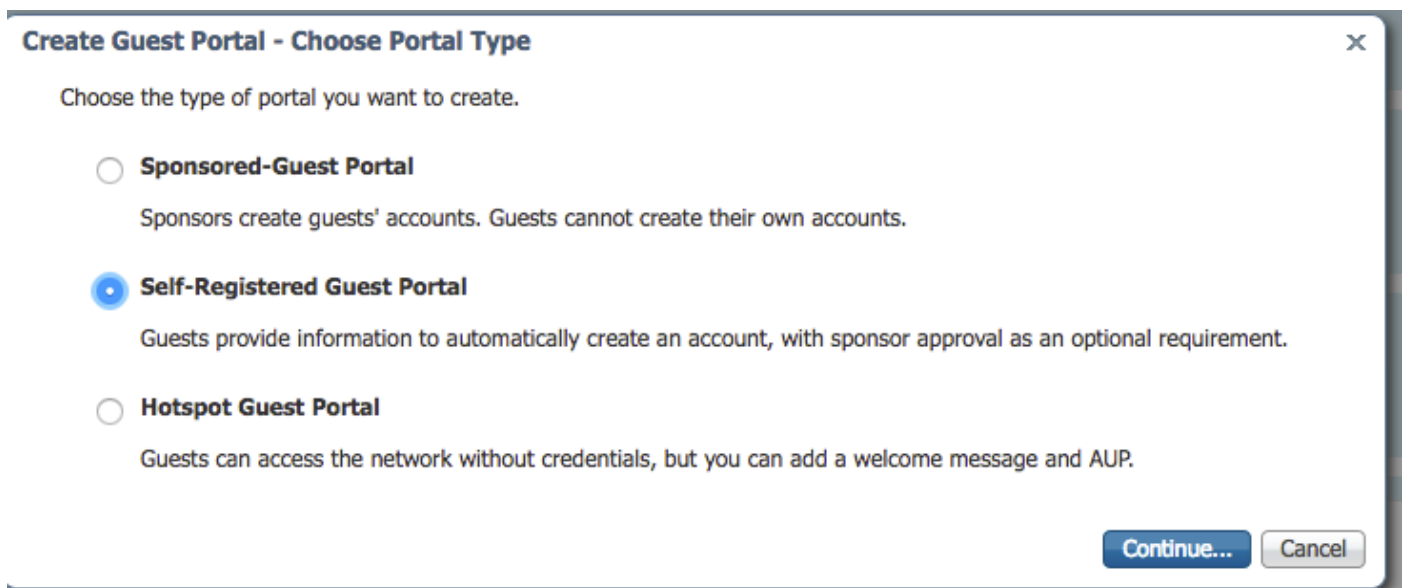


Paso 2. Asigne un nombre al proveedor de ID y envíe la configuración.

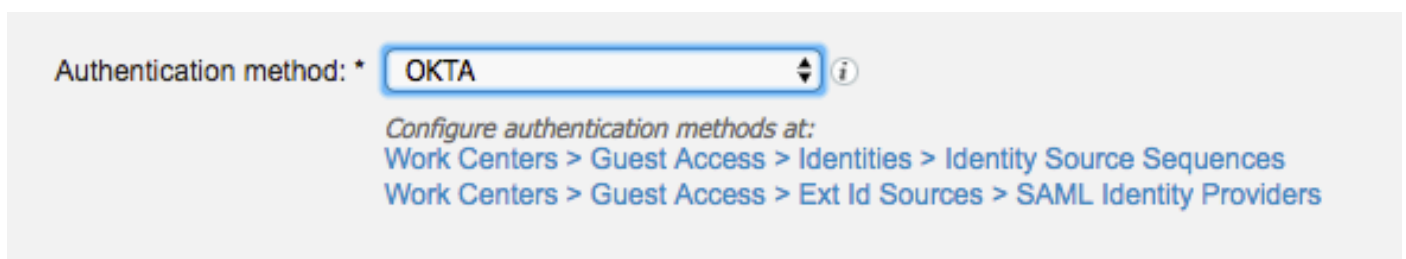
2. Crear portal para SSO.

Paso 1. Cree el portal que se asigna a OKTA como origen de identidad. Cualquier otra configuración para BYOD, registro de dispositivos, Invitado, etc., es exactamente la misma que para el portal normal. En este documento, el portal se asigna al portal de invitados como inicio de sesión alternativo para Empleado.

Paso 2. Navegue hasta **Centros de trabajo > Acceso de invitado > Portales y componentes** y cree el portal.

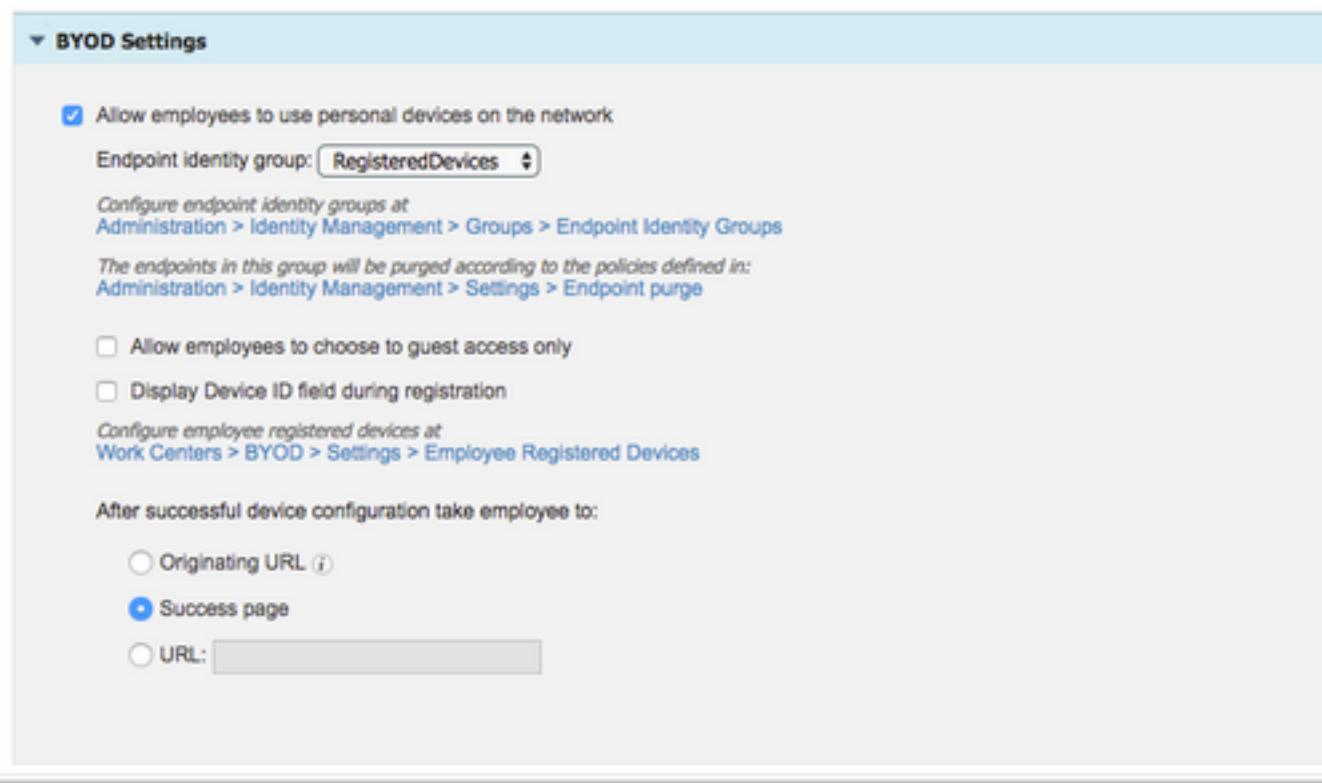


Paso 3. Elija el método de autenticación para señalar al proveedor de identidad configurado previamente.



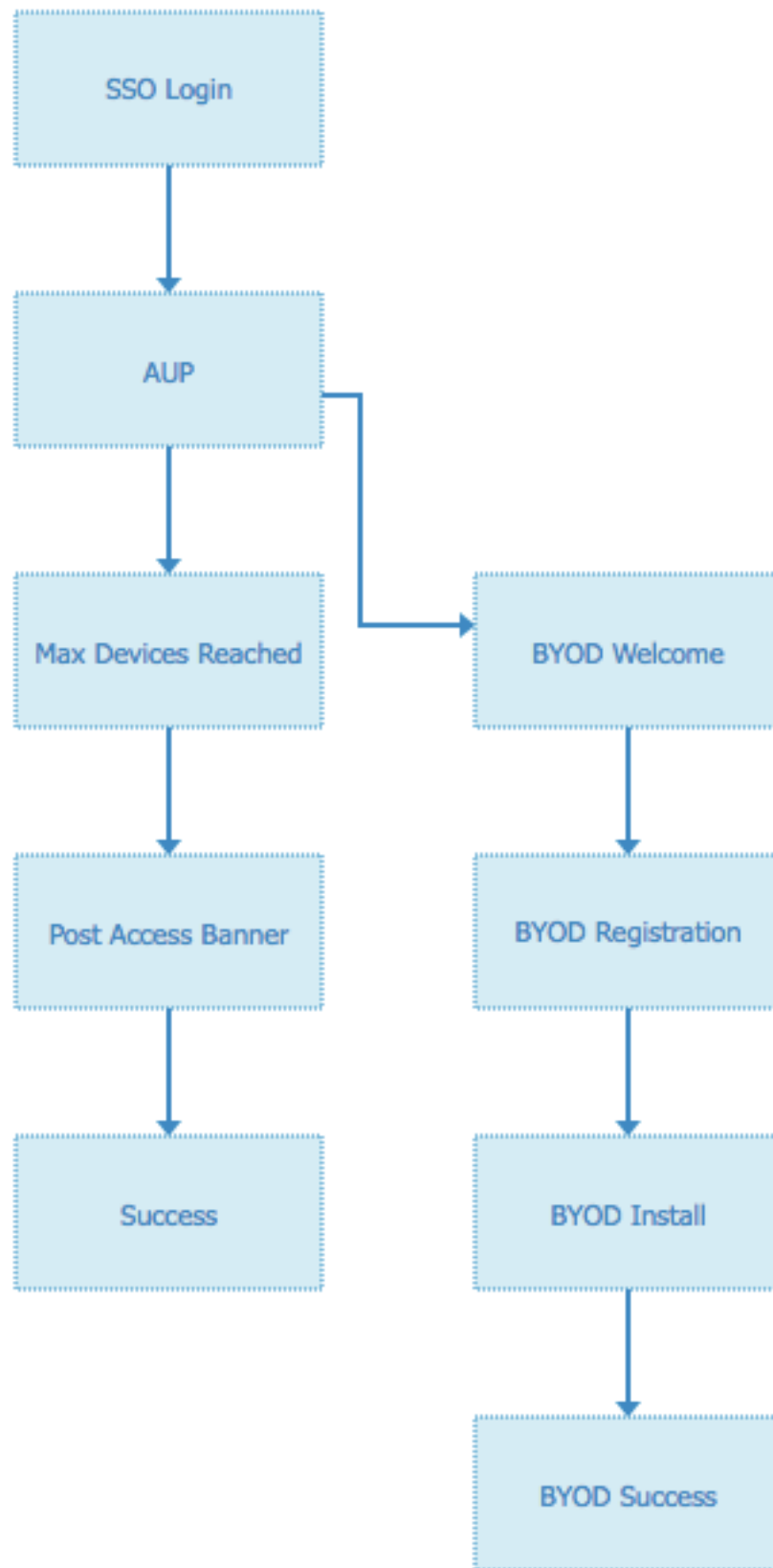
Paso 4. Elija la fuente de identidad OKTA como método de autenticación.

(opcional) seleccione la configuración de BYOD.



The screenshot shows the 'BYOD Settings' configuration page. At the top, there is a section header 'BYOD Settings' with a dropdown arrow. Below this, the first option is 'Allow employees to use personal devices on the network', which is checked with a blue square. Underneath this option, there is a label 'Endpoint identity group:' followed by a dropdown menu showing 'RegisteredDevices'. Below the dropdown, there are two lines of instructional text: 'Configure endpoint identity groups at Administration > Identity Management > Groups > Endpoint Identity Groups' and 'The endpoints in this group will be purged according to the policies defined in: Administration > Identity Management > Settings > Endpoint purge'. The second option is 'Allow employees to choose to guest access only', which is unchecked. The third option is 'Display Device ID field during registration', also unchecked. Below these options, there is another line of instructional text: 'Configure employee registered devices at Work Centers > BYOD > Settings > Employee Registered Devices'. The final section is 'After successful device configuration take employee to:', which contains three radio button options: 'Originating URL' (with an information icon), 'Success page' (which is selected with a blue dot), and 'URL:' followed by an empty text input field.

Paso 5. Guarde la configuración del portal, con BYOD el flujo se ve de la siguiente manera:



3. Configuración de inicio de sesión alternativo.

Nota: Puede omitir esta parte si no utiliza el inicio de sesión alternativo.

Navegue hasta el portal de invitados de registro automático o cualquier otro portal personalizado

para el acceso de invitados.

En la configuración de la página de inicio de sesión, agregue el portal de inicio de sesión 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

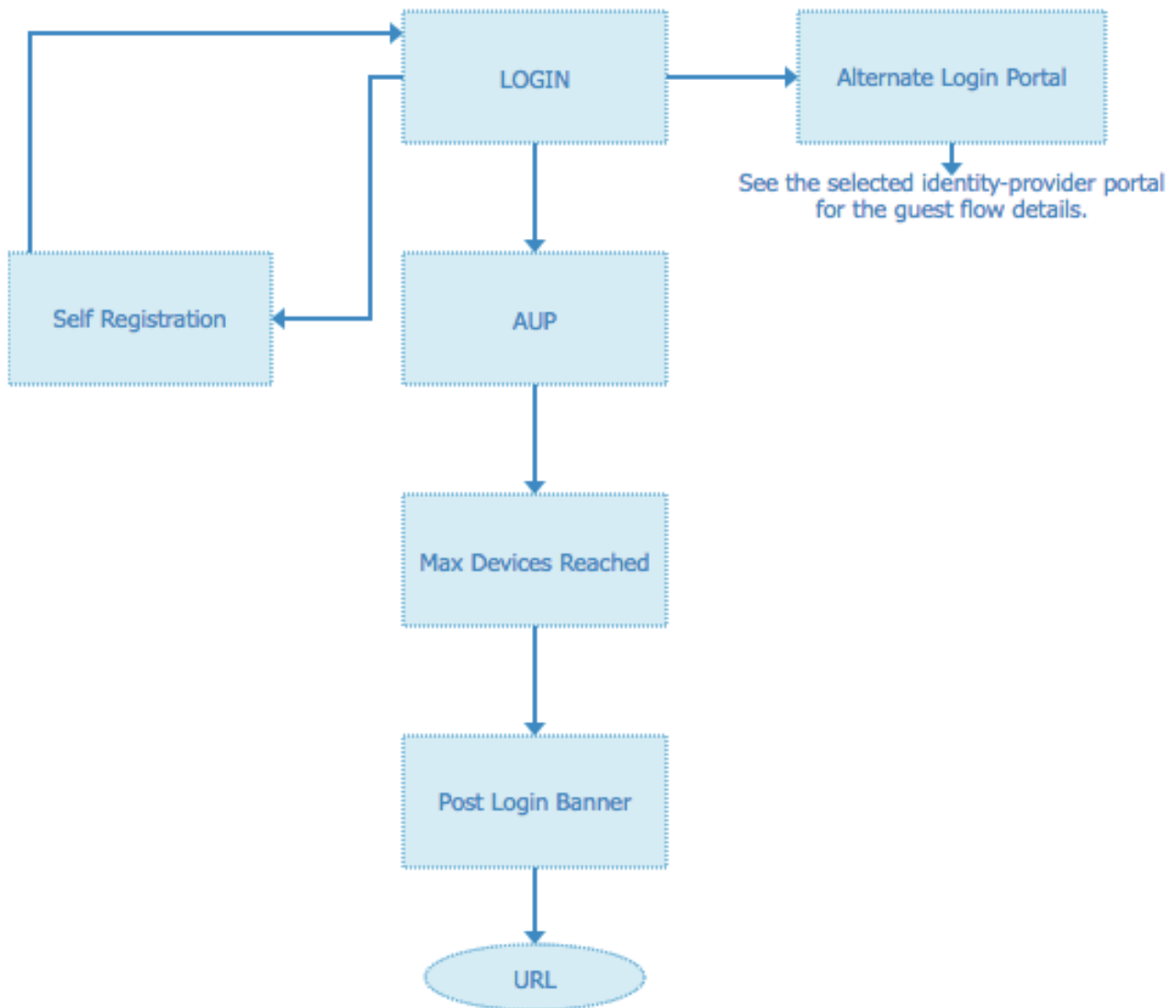
Allow social login

Allow guests to change password after login ⓘ

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

▼

Este es el flujo del portal ahora.



Paso 2. Configure la aplicación OKTA y los parámetros del proveedor de identidad SAML.

1. Crear aplicación OKTA.

Paso 1. Inicie sesión en el sitio web de OKTA con una cuenta de administrador.

← Back to Applications





Add 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

Paso 2. Haga clic en Add Application (Agregar aplicación).

okta [Dashboard](#) [Directory](#) [Applications](#) [Security](#) [Reports](#) [Settings](#) [My Applications](#) [Help](#)

Applications

[Add Application](#) [Assign Applications](#)

STATUS	
ACTIVE	0
INACTIVE	3

01101110
01101111
01101100
01101000
01101101
01101110
01100111

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](#)

Paso 3. Crear nueva aplicación, elija que sea 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

Configuración general

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

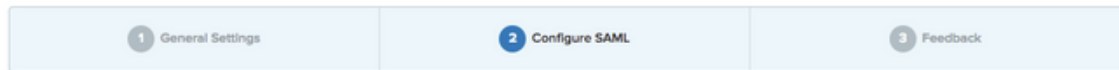


Do not display application icon in the Okta Mobile app

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](#)

Paso 4. Descargue el certificado e instálelo en Certificados de confianza ISE.

Import a new Certificate into the Certificate Store

* Certificate File okta (3).cert

Friendly Name

Trusted For:

Trust for authentication within ISE
 Trust for client authentication and Syslog
 Trust for authentication of Cisco Services
 Validate Certificate Extensions

Description

2. Exportar información SP del proveedor de identidad SAML.

Navegue hasta el proveedor de identidad configurado previamente. Haga clic en **Información del proveedor de servicios** y exporte la información, como se muestra en la imagen.

Paso 1. Agregue esas URL en la configuración 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
<input type="text" value="https://isespan.bikawilab:8443/portal/SSOLoginRespo"/>	<input type="text" value="0"/> <input type="button" value="X"/>

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](#)

Paso 2. Puede agregar más de una URL del archivo XML, en función del número de PSN que alojan este servicio. El formato de ID de nombre y el nombre de usuario de la aplicación dependen del diseño.

B Preview the SAML assertion generated from the information above

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

```
<?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</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

Paso 3. Haga clic en next (Siguiente) y elija la segunda opción.

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 metadatos de la aplicación.


```
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>
```

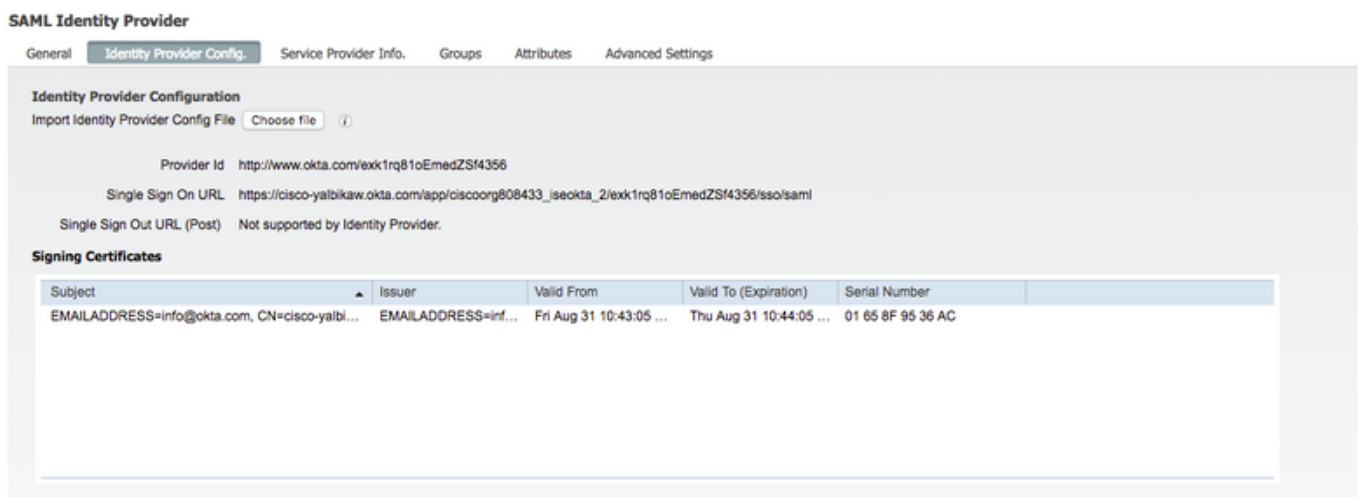
Guarde el archivo en formato XML.

5. Asignar usuarios a la aplicación.

Asigne usuarios a esta aplicación, hay una forma de integración de AD, explicada en: [direccionamiento activo de okta](#)

6. Importar metadatos de Idp a ISE.

Paso 1. En **Proveedor de identidad SAML**, seleccione **Configuración del proveedor de identidad**. e **Importar metadatos**.



Paso 2. Guarde la configuración.

Paso 3. Configuración de CWA.

Este documento describe la configuración para ISE y WLC.

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

Agregue URL en Redirect-ACL.

<https://cisco-yalbikaw.okta.com> / agregue su URL de aplicación

<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.

Verificación

Pruebe el portal y verifique si puede alcanzar la aplicación OKTA

Portal Name: *

Description:

OKTA_SSO

[Portal test URL](#)



Portal Behavior and Flow Settings

Use these settings to specify the guest experience for this portal.



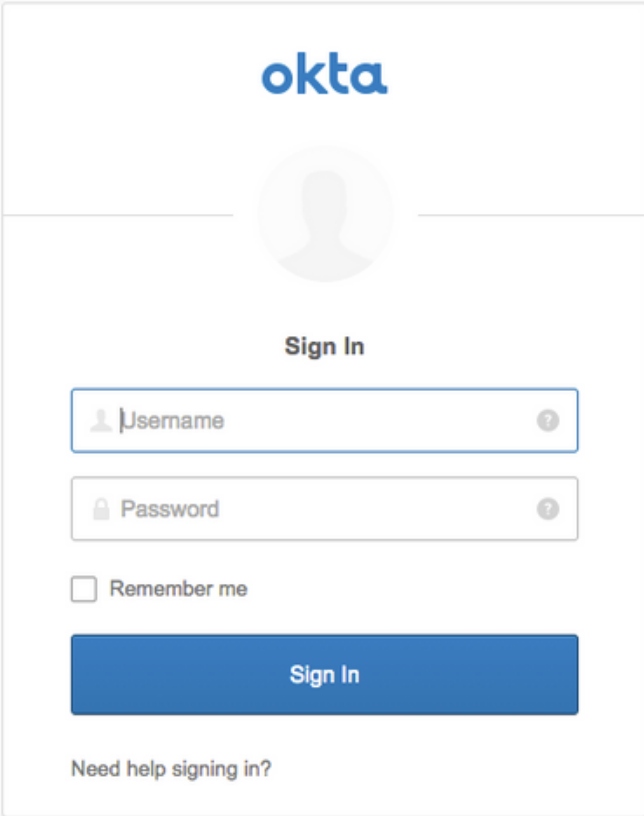
Portal Page Customization

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

Paso 1. Haga clic en la prueba del portal y, a continuación, debe redirigirse a la aplicación 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 profile picture, the text "Sign In" is centered. There are two input fields: the first is labeled "Username" and the second is labeled "Password". 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?".

Paso 2. Compruebe la **conexión** de información **a <nombre de la aplicación>**

Paso 3. Si introduce las credenciales, puede que vea una solicitud de ejemplo incorrecta, esto no significa necesariamente que la configuración sea incorrecta en este momento.

Verificación del usuario 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

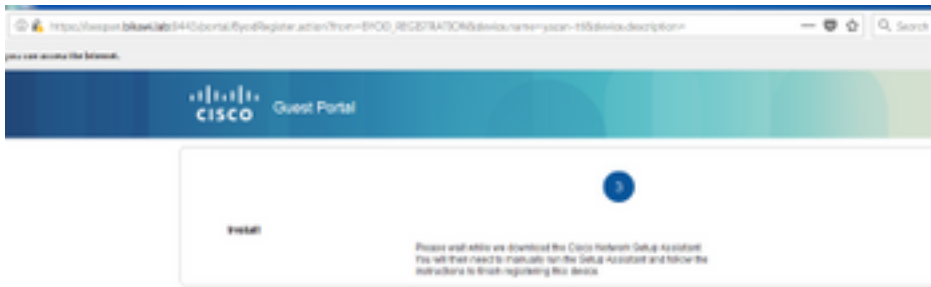
Acceptable Use Policy

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



Verificación de ISE

Verifique los registros de vida para verificar el estado de autenticación.

Sep 30, 2018 12:39:09.514 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	okta-test@cisco.c...	3C:A8:F4:34:9F:70					
Sep 30, 2018 12:33:32.640 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3C:A8:F4:34:9F:70	3C:A8:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest		yazan-cpp

Troubleshoot

Solución de problemas de OKTA

Paso 1. Verifique los registros en la pestaña **Informes**.

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

Paso 2. También desde la aplicación ver los 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 "00af98f9b03HC20YF356" and target.type eq "AppInstance" [Advanced Filter / Reset Filters](#)

Count of events over time



Show event trends by category

Events: 25 [Download CSV](#)

Time	Actor	Event Info	Targets
Sep 30 02:42:02	OKTA-TEST@cisco.com OKTA (User)	User single sign on to app SUCCESS	ISE-OKTA (AppInstance) OKTA-TEST@cisco.com OKTA (AppUser)
<ul style="list-style-type: none"> Actor: OKTA-TEST@cisco.com OKTA (id: 00a23899f90000000000000000000000) Client: FIREFOX on Windows 7 Computer from [REDACTED] Event: successful user.authentication.sso (id: WYkz000000000000000000000000000000) Request: ISE-OKTA (id: 00af98f9b03HC20YF356) AppInstance Target: OKTA-TEST@cisco.com OKTA (id: 00a23899f90000000000000000000000) AppUser 			

Solución de problemas de ISE

Hay dos archivos de registro que comprobar

- ise-psc.log
- guest.log

Vaya a **Administration > System > Logging > Debug Log Configuration**. Habilite el nivel en DEBUG.

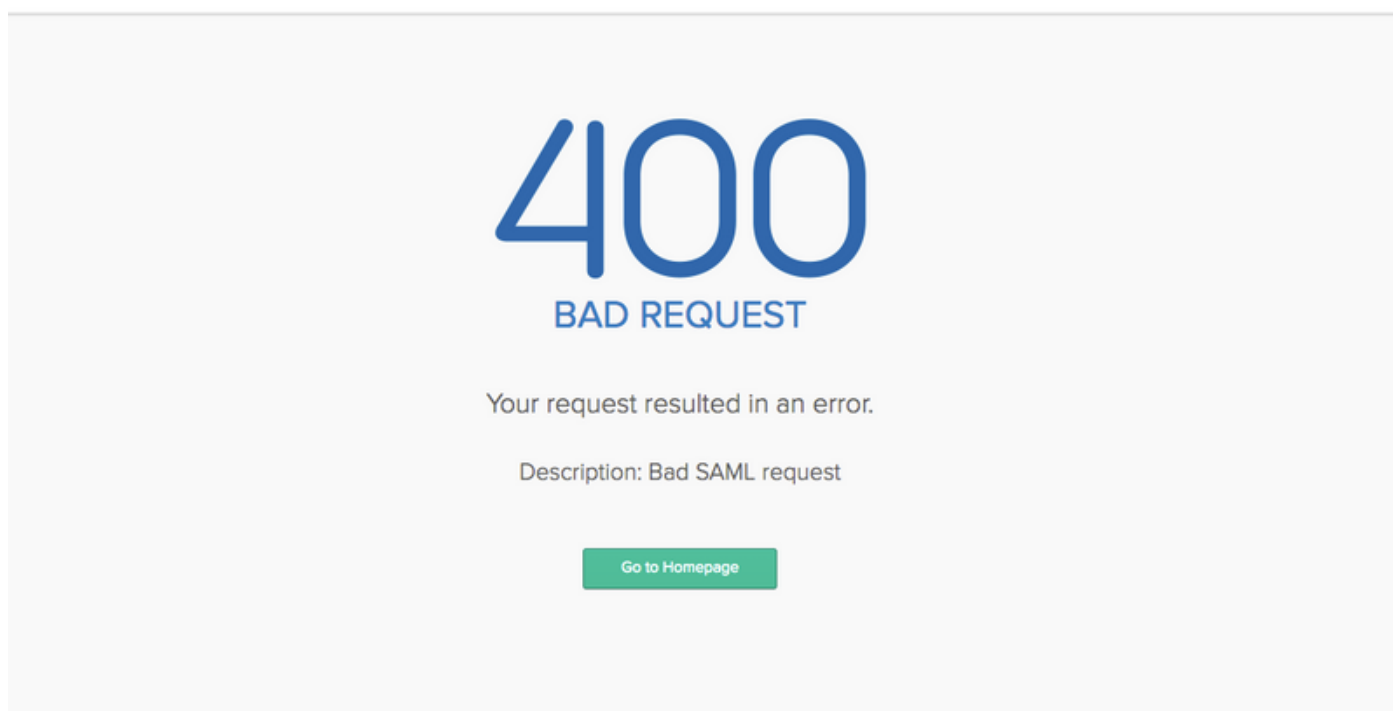
SAML	ise-psc.log
Acceso a invitados	guest.log
Portal	guest.log

La tabla muestra el componente que se va a depurar y su archivo de registro correspondiente.

Problemas comunes y soluciones

Escenario 1. Solicitud de SAML incorrecta.

okta



Este error es genérico, verifique los registros para verificar el flujo y señalar el problema. En 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:
```

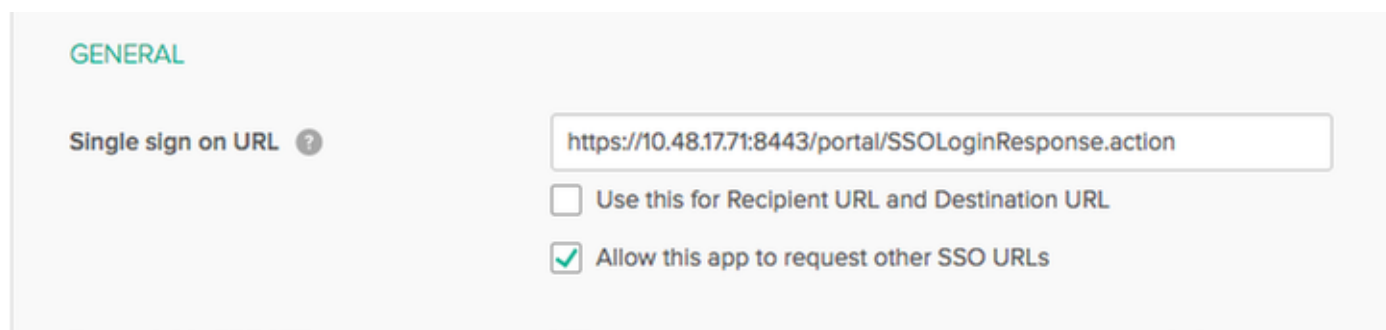
```
Portal Name: OKTA_SSO  
Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546  
Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
```


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/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoEuyPu95j9%2FzJOOb4672DqCNUDJJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHhloiuQcIeJo1WVnFVI29qDGjrzGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnC
h3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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_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/exk1rq81oEmedZSf4356/sso/saml
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoEuyPu95j9%2FzJO
Ob4672DqCNUDJJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHhloiuQcIeJ
o1WVnFVI29qDGjrzGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1z
X6nmngdq3YIO37q9fBlQnC3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWl
Z7wL%2B6zyT7uxfgUzOu7n8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e4
1bbdc546_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

ISE ha redirigido correctamente el usuario a IDP. Sin embargo, no aparece ninguna respuesta a ISE y aparece la solicitud SAML incorrecta. Identifique que OKTA no acepte nuestra solicitud SAML a continuación.

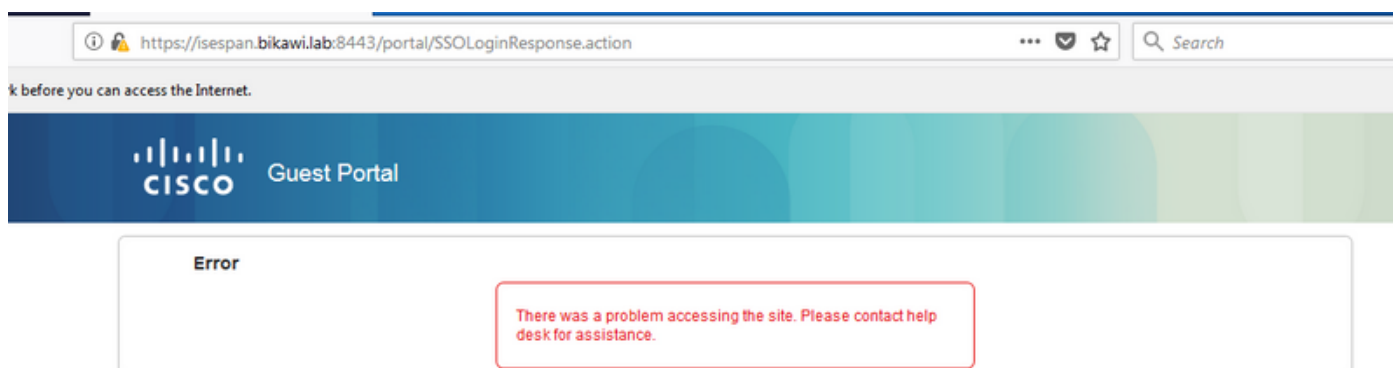
```
https://cisco-  
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrjGZKmv0  
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u  
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BvYWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fB1QnC  
h3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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
```

Ahora vuelva a comprobar la aplicación tal vez haya cambios realizados.



La dirección URL de SSO está utilizando la dirección IP; sin embargo, el invitado está enviando FQDN, como se puede ver en la solicitud anterior en la que la última línea contiene SEMI_DELIMITER<FQDN> para solucionar este problema, cambie la dirección IP a FQDN en la configuración de OKTA.

Situación hipotética 2. "Se ha producido un problema al acceder al sitio. Póngase en contacto con el servicio de asistencia técnica para obtener asistencia".



Guest.log

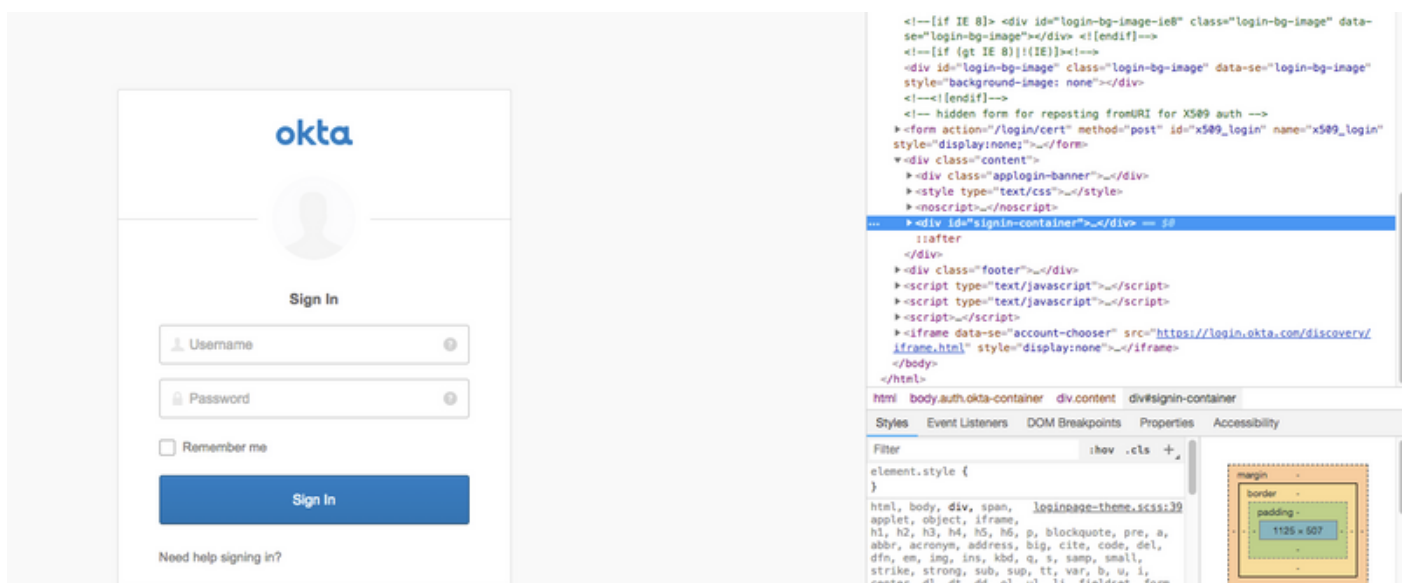
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][  
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or
```

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

Desde los registros, ISE informa que la afirmación no es correcta. Verifique el URI de audiencia OKTA para asegurarse de que coincide con el SP para resolverlo.

Situación hipotética 3. Redirigido a la página en blanco o la opción de inicio de sesión no se muestra.

Depende del entorno y de la configuración del portal. En este tipo de problema debe verificar la aplicación OKTA y la URL que necesita para autenticarse. Haga clic en la prueba del portal y, a continuación, inspeccione el elemento para comprobar qué sitios web deben estar accesibles.



En este escenario, solo dos URL: application and login.okta.com - se deben permitir en el WLC.

Información Relacionada

- <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>