

# Configure ISE 2.3 Guest Portal with OKTA SAML SSO

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Federated SSO](#)

[Network Flow](#)

[Configure](#)

[Step 1. Configure SAML Identity Provider and Guest portal on ISE.](#)

[1. Prepare External Identity Source.](#)

[2. Create Portal for SSO.](#)

[3. Configure Alternative Login.](#)

[Step 2. Configure OKTA Application and SAML Identity Provider Settings.](#)

[1. Create OKTA Application.](#)

[2. Export SP Information from SAML Identity Provider.](#)

[3. OKTA SAML Settings.](#)

[4. Export Metadata from the Application.](#)

[5. Assign Users to the Application.](#)

[6. Import Metadata from Idp to ISE.](#)

[Step 3.CWA Configuration.](#)

[Verify](#)

[End-user Verification](#)

[ISE Verification](#)

[Troubleshoot](#)

[OKTA Troubleshoot](#)

[ISE Troubleshoot](#)

[Common Issues and Solutions](#)

[Related Information](#)

## Introduction

This document describes how to integrate Identity Services Engine (ISE) with OKTA, to provide Security Assertion Markup Language Single Sign-On (SAML SSO) authentication for the guest portal.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine guest services.
- SAML SSO.
- (optional) Wireless LAN Controller (WLC) configuration.

## Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine 2.3.0.298
- OKTA SAML SSO application
- Cisco 5500 wireless controller version 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. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

### Federated SSO

A user within organization can authenticate once and then have access to multiple resources. This identity used across organisations is called federated identity.

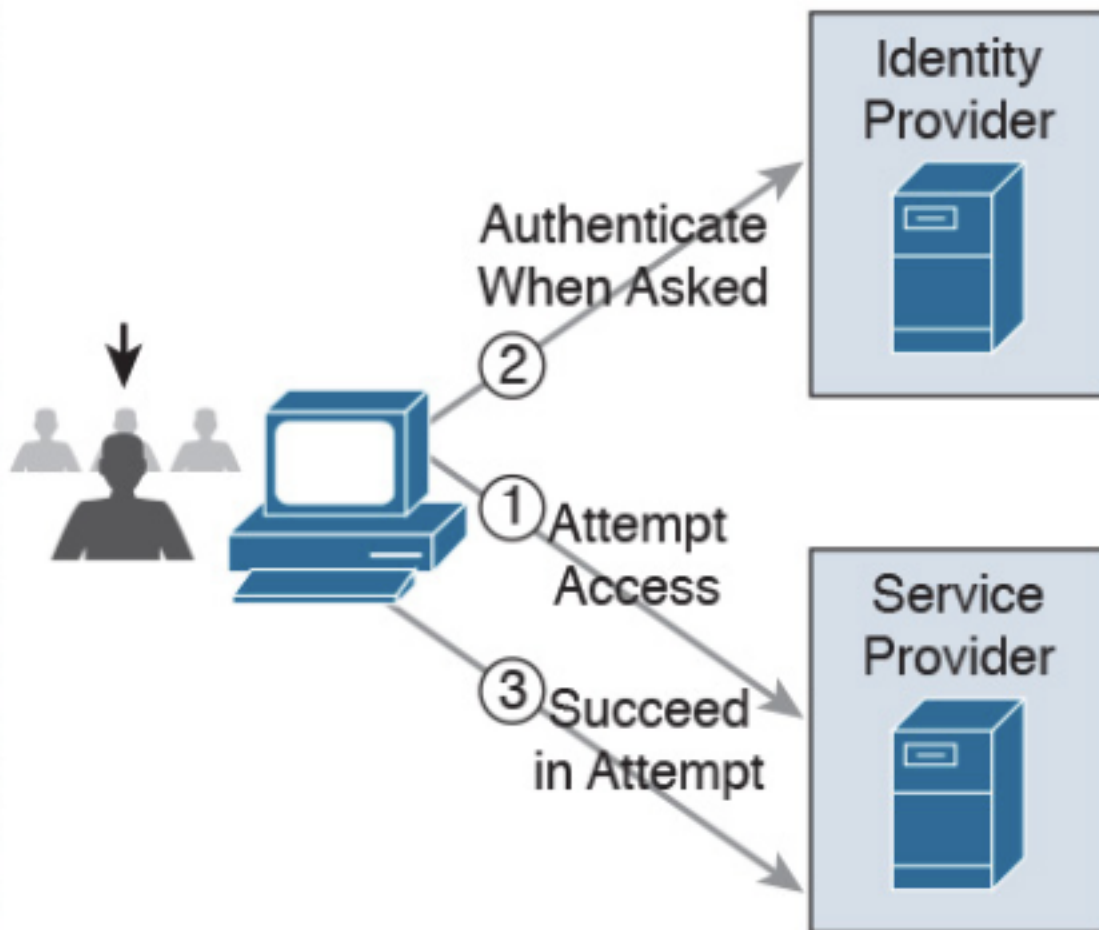
The concept of federation:

- Principle: End-user (the one, who requests a service), web browser, in this case, is the endpoint.
- Service provider (SP): sometimes called relying party (RP), which is the system that provides a service, in this case, ISE.
- Identity provider (IdP): which manages the authentication, authorization result and attributes that are sent back to SP, in this case, OKTA.
- Assertion: the user information sent by IdP to SP.

Several protocols implement SSO such as OAuth2 and OpenID. ISE uses SAML.

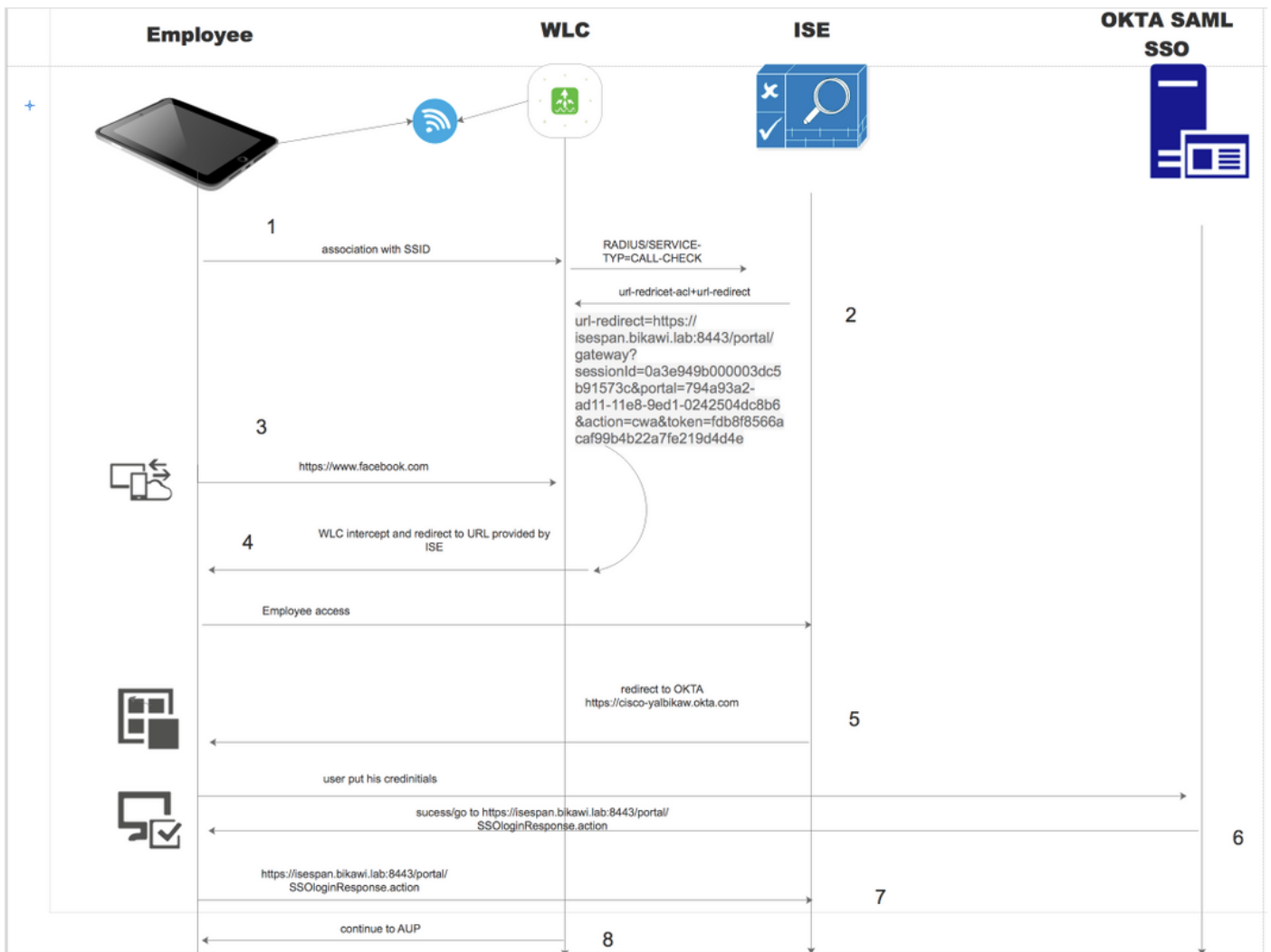
SAML is an XML-based framework that describes the use and exchange of SAML assertions in a secure way between business entities. The standard describes the syntax and rules to request, create, use, and exchange these assertions.

ISE uses SP initiated mode. The user is redirected to the Guest portal, then ISE redirects it to IdP to authenticate. After that, it redirects back to ISE. The request is validated, the user proceeds with guest access or on-boarding, depending on the portal configuration.



**SP-initiated**

**Network Flow**



1. The user connects to the SSID, and the authentication is mac filtering (mab).
2. ISE responds back with access-accept that contains Redirect-URL and Redirect-ACL attributes
3. User tries to access [www.facebook.com](https://www.facebook.com).
4. WLC intercepts the request and redirects the user to the ISE guest portal, the user clicks on employee access in order to register the device with SSO credentials.
5. ISE redirects the user to OKTA application for authentication.
6. After successful authentication, OKTA sends the SAML assertion response to the browser.
7. Browser relays the assertion back to ISE.
8. ISE verifies the assertion response and if the user is properly authenticated, it proceeds to AUP and then with device registration.

Check the below link for more information about SAML

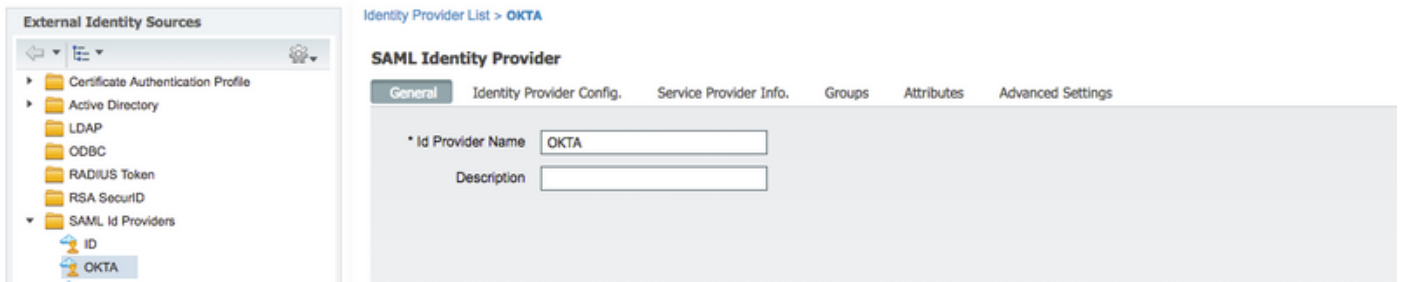
<https://developer.okta.com/standards/SAML/>

## Configure

### Step 1. Configure SAML Identity Provider and Guest portal on ISE.

#### 1. Prepare External Identity Source.

Step 1. Navigate to **Administration > External Identity Sources > SAML id Providers**.

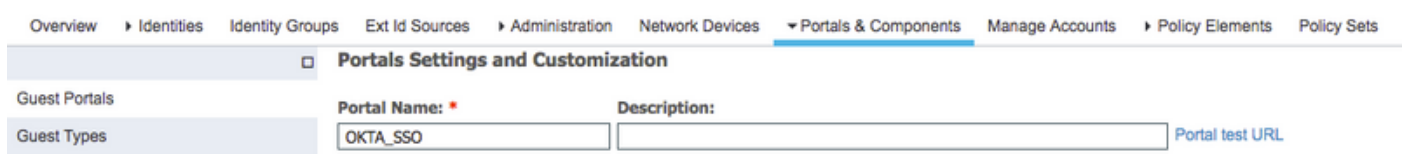
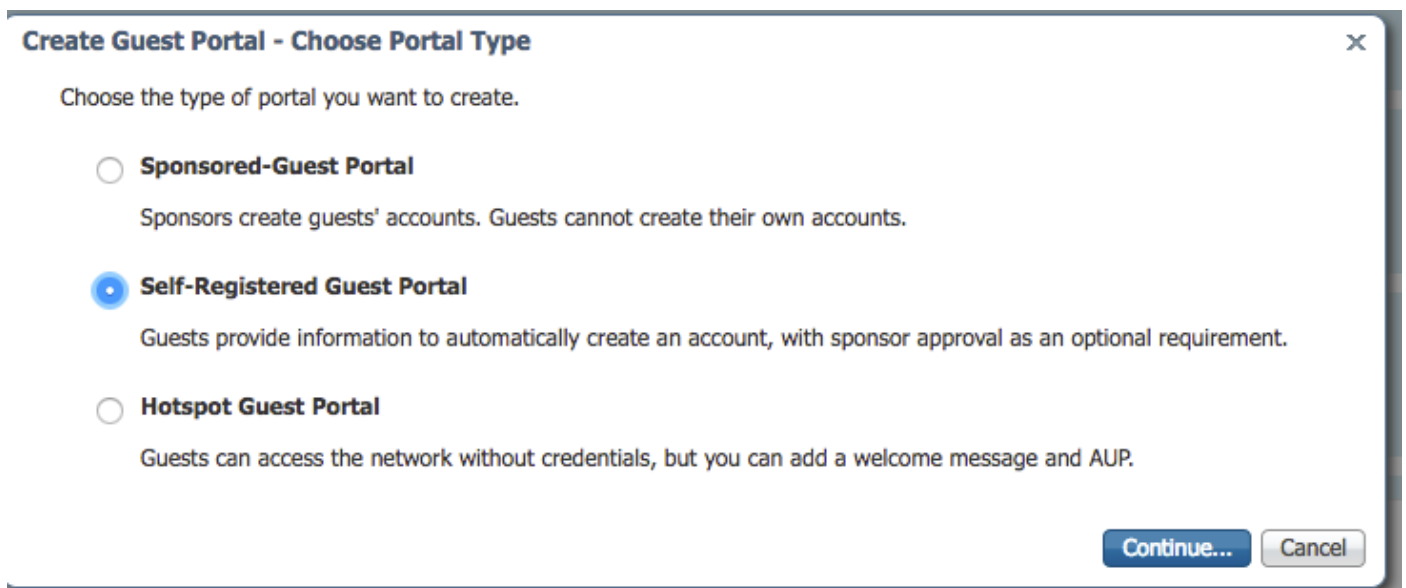


Step 2. Assign a name to the id provider and submit the configuration.

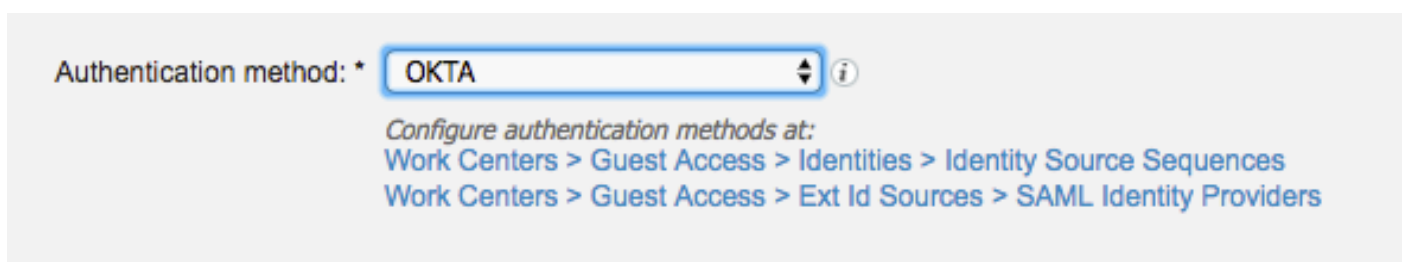
## 2. Create Portal for SSO.

Step 1. Create the portal which is assigned to OKTA as identity source. Any other configuration for BYOD, device registration, Guest ..etc, is exactly the same as for normal portal. In this document, the portal is mapped to the guest portal as an alternative login for Employee.

Step 2. Navigate to **Work Centers > Guest Access > Portals & Components** and create the portal.



Step 3. Choose the authentication method to point to the identity provider configured previously.



Step 4. Choose OKTA identity source as an authentication method.

(optional) choose the BYOD settings.

▼ BYOD Settings

Allow employees to use personal devices on the network

Endpoint identity group:

*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](#)

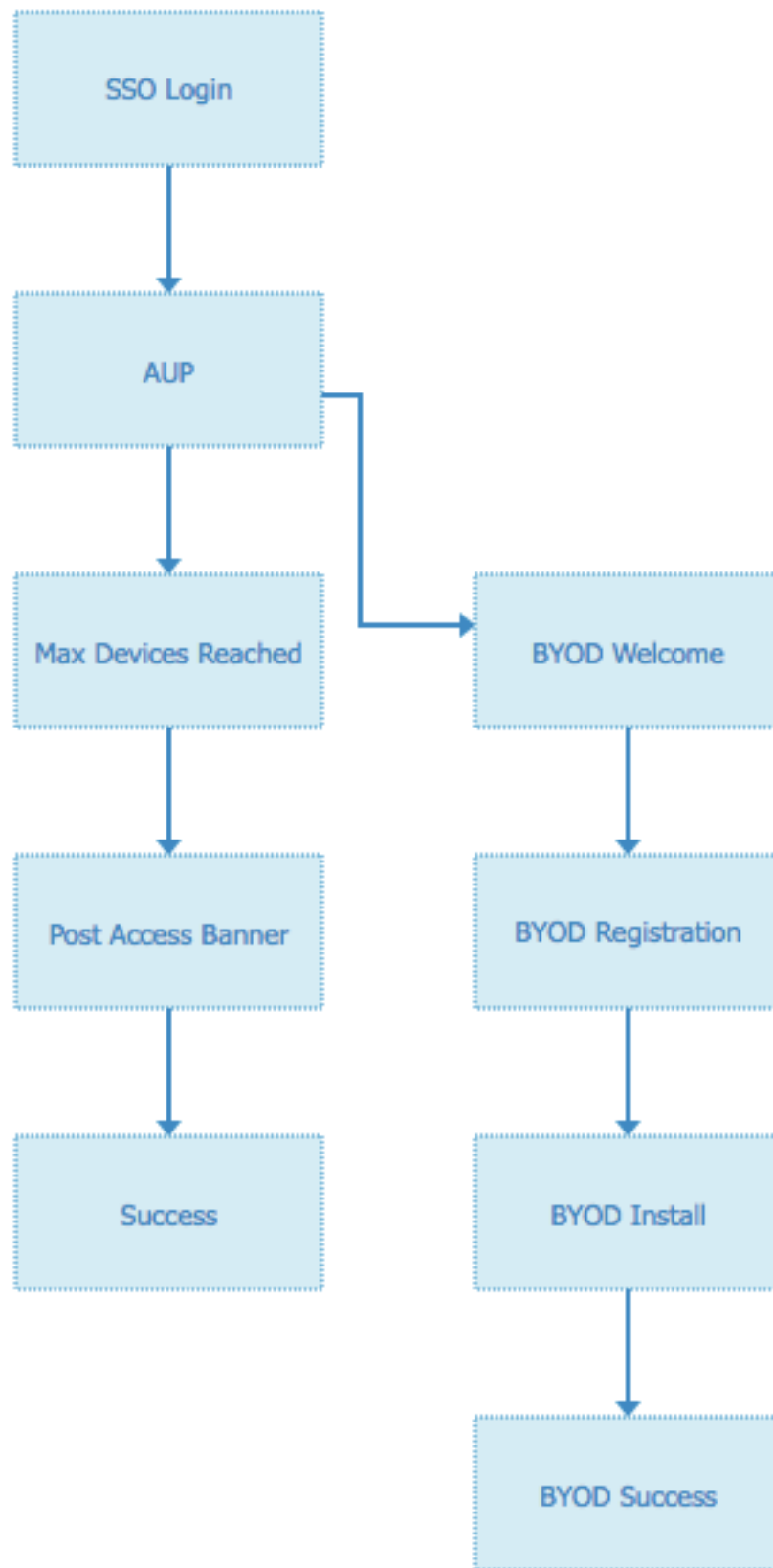
After successful device configuration take employee to:

Originating URL (i)

Success page

URL:

Step 5. Save the portal configuration, with BYOD the flow looks like this:



### 3. Configure Alternative Login.

**Note:** You can skip this part if you are not using the Alternative login.

Navigate to self-registration Guest Portal or any other portal customized for guest access.

On login page settings add the alternative login portal: 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

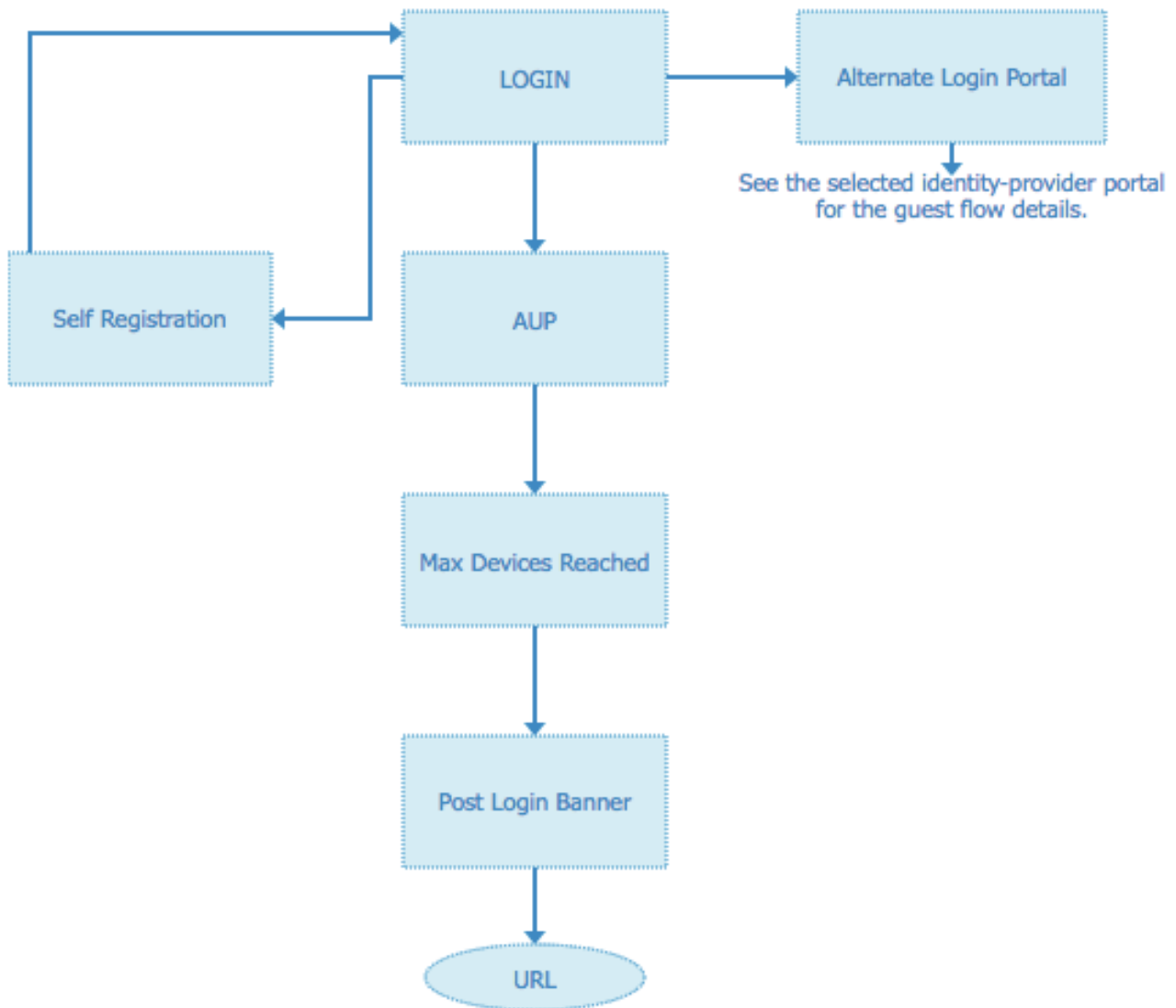
Allow social login

Allow guests to change password after login ⓘ

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

This is the portal flow now.





## Step 2. Configure OKTA Application and SAML Identity Provider Settings.

### 1. Create OKTA Application.

Step 1. Login to OKTA website with an admin account.

← Back to Applications

## Add Application





Q 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

Step 2. Click on Add Application.

okta Dashboard Directory Applications Security Reports Settings My Applications ↻

### Applications Help

Add Application Assign Applications

Q Search

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

Step 3. Create New App, choose it to be 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

## General settings

### 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

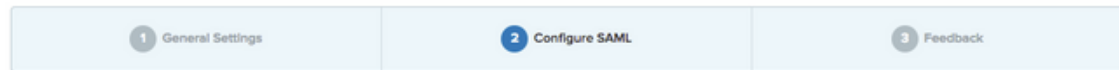


Do not display application icon in the Okta Mobile app

Cancel

Next

## Create SAML Integration



### A SAML Settings

**GENERAL**

Single sign on URL <sup>?</sup>

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

Audience URI (SP Entity ID) <sup>?</sup>

Default RelayState <sup>?</sup>

If no value is set, a blank RelayState is sent

Name ID format <sup>?</sup>

Application username <sup>?</sup>

[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?

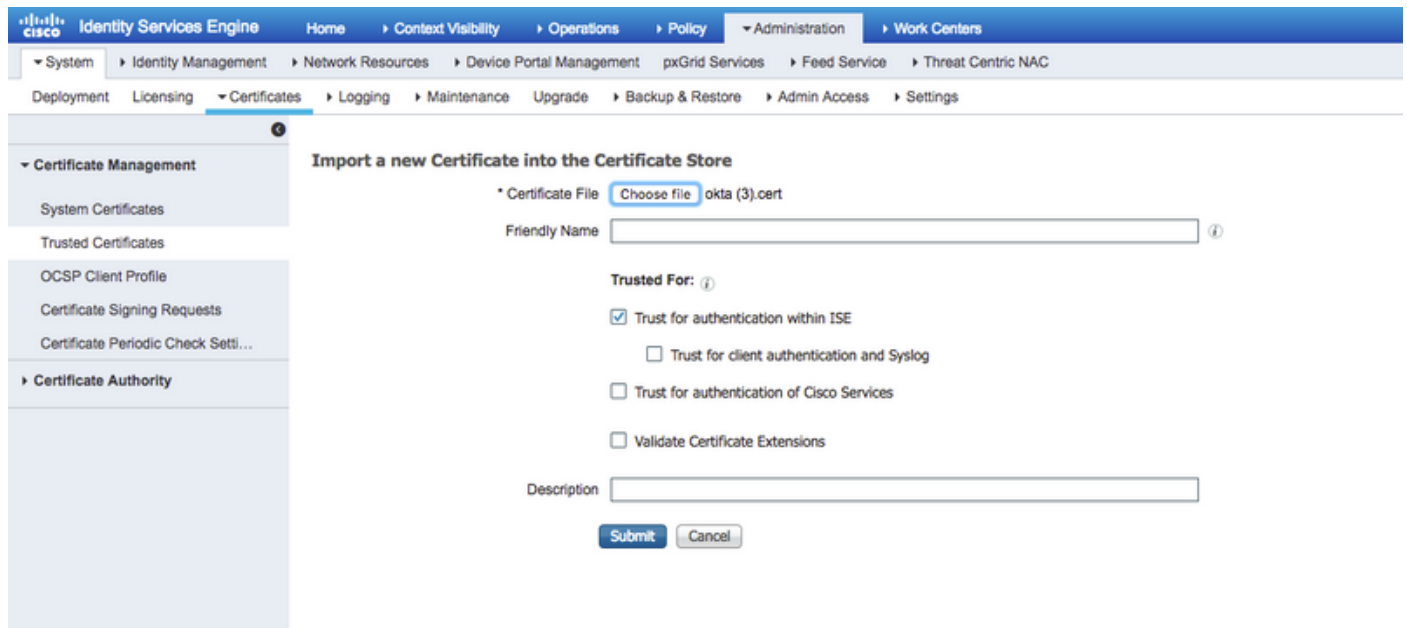
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

#### Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

## Step 4. Download the certificate and install it in ISE Trusted Certificates.



## 2. Export SP Information from SAML Identity Provider.

Navigate to the previously configured Identity Provider. Click on **Service Provider Info** and export it, as shown in the image.

### SAML Identity Provider

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

**Service Provider Information**

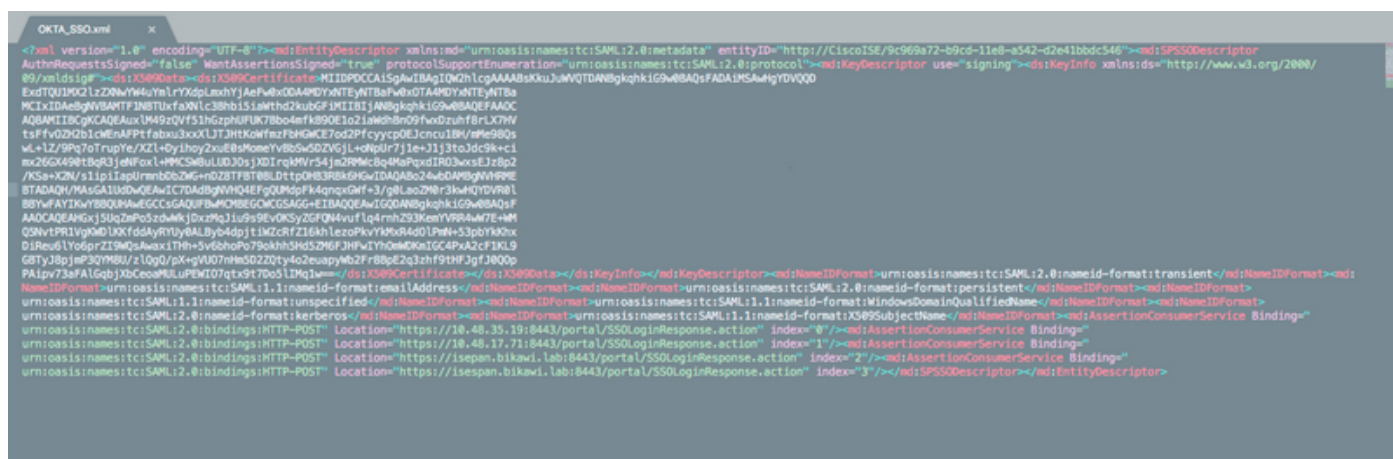
Load balancer

Export Service Provider Info.

**Includes the following portals:**

OKTA\_SSO

The exported zip folder contains XML file and **readme.txt**



For some Identity providers you can import the XML directly, but in this case, it needs to import manually.

- Single Sign On URL (saml assertion)

```
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"
```

- SP Entity ID

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

The SSO URL available in ip address and FQDN format.

**Caution:** The selection of format depends on the redirect settings on Authorization profile, if you use static ip then you should use the ip address for SSO URL.

### 3. OKTA SAML Settings.

Step 1. Add those URLs on SAML settings.

## 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://lspan.bikawi.lab: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](#)

Step 2. You can add more than one URL from the XML file, based on the number of PSN's hosting this service. Name ID format and Application username depend on your design.

## 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</s
aml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

Step 3. Click next and choose the second option.

**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

Previous
Finish

**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.

#### 4. Export Metadata from the Application.





```
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>
```

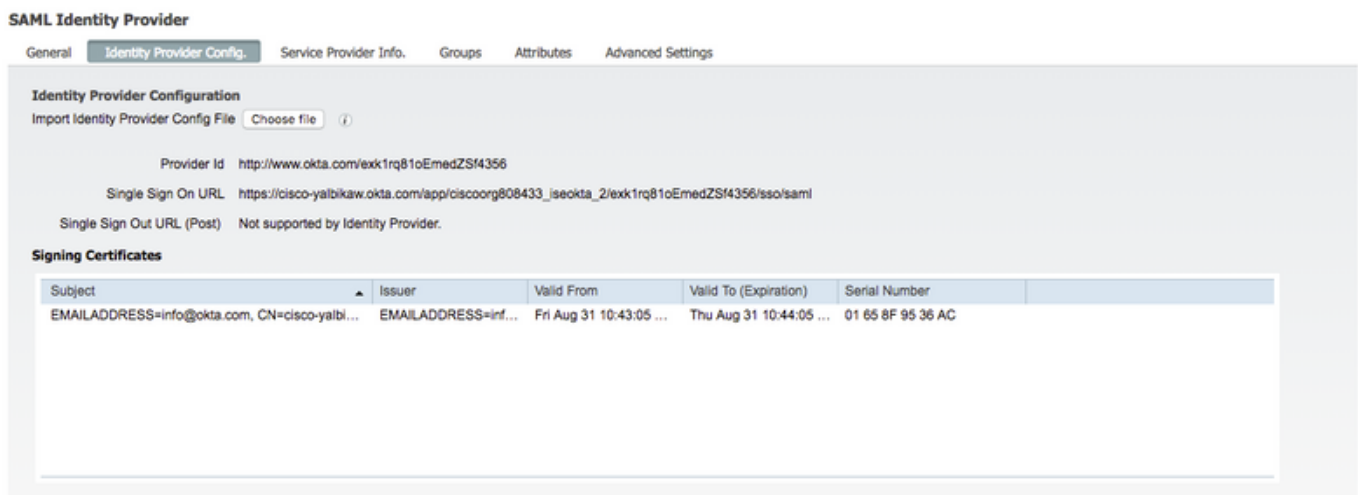
Save the file in XML format.

## 5. Assign Users to the Application.

Assign users to this application, there is a way for AD integration, its explained in: [okta-active driectory](#)

## 6. Import Metadata from Idp to ISE.

Step 1. Under **SAML Identity Provider**, select **Identity Provider Config.** and Import Metadata.



Step 2. Save the configuration.

## Step 3.CWA Configuration.

This document describes the configuration for ISE and WLC.

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

Add URLs in Redirect-ACL.

<https://cisco-yalbikaw.okta.com/> / add your Application URL

<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.

## Verify

Test the portal and verify if you are able to reach the OKTA application

Portal Name: \*

Description:

OKTA\_SSO

[Portal test URL](#)



#### Portal Behavior and Flow Settings

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



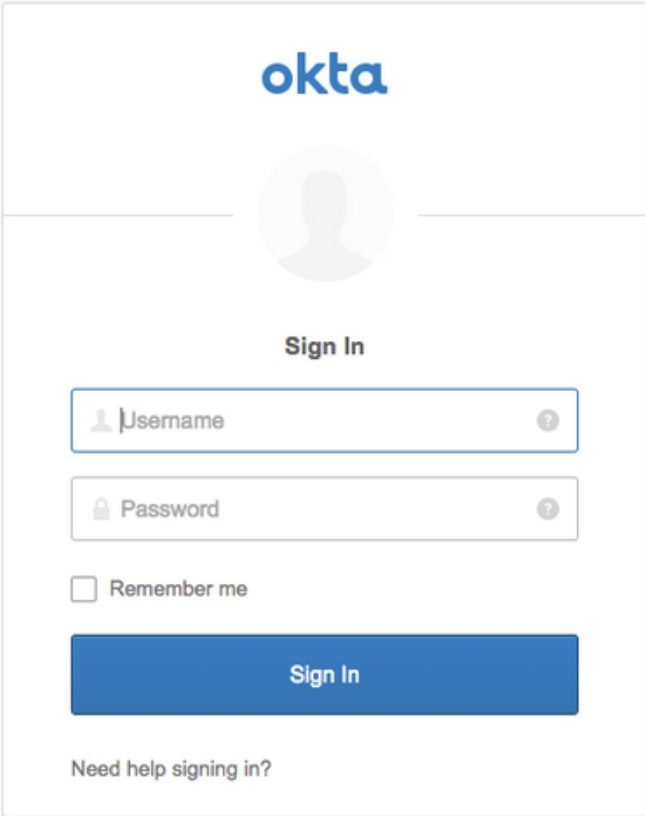
#### Portal Page Customization

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

Step 1. Click on the portal test, then you should be redirected to SSO application.

## 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". Both fields have a small question mark icon to their right. Below the password field 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?".

Step 2. Check the information ***connection to <application name>***

Step 3. If you enter the credentials you might see bad saml request, this does not necessarily mean that the configuration is wrong at this point.

## End-user Verification

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

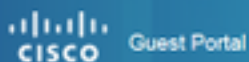
[Need help signing in?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



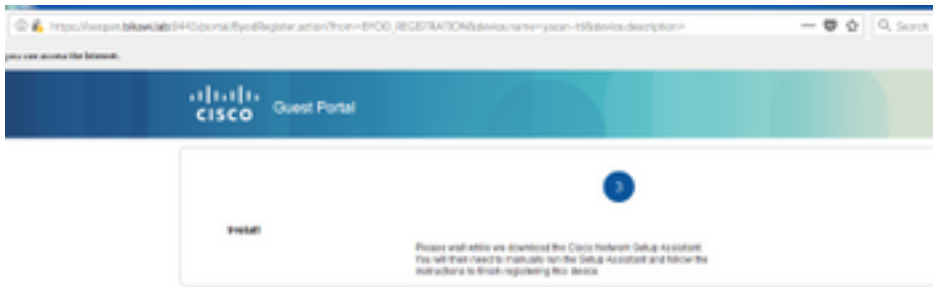
**Acceptable Use Policy**

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



## ISE Verification

Check life logs to verify the authentication status.

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

### OKTA Troubleshoot

Step 1. Check the logs in **Reports** tab.

### 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

Step 2. Also from the application view the related logs.

← 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 "00a7f81b031c201f9356" 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@ciscc.com OKTA (User)	User single sign on to app SUCCESS	ISE-OKTA (AppInstance) OKTA-TEST@ciscc.com OKTA (AppUser)

Expand All

- Actor: OKTA-TEST@ciscc.com OKTA (id: 00u221b031c201f9356)
- Client: FIREFOX on Windows 7 Computer from [REDACTED]
- Event: successful user.authentication.sso (id: W1a2c0r0m1Mh2noJGtDgAABQ)
- Request: [REDACTED]
- Target: ISE-OKTA (id: 00a7f81b031c201f9356) AppInstance
- Target: OKTA-TEST@ciscc.com OKTA (id: 00a238qssPQGW8Tc356) AppUser

## ISE Troubleshoot

There are two log files to check

- ise-psc.log
- guest.log

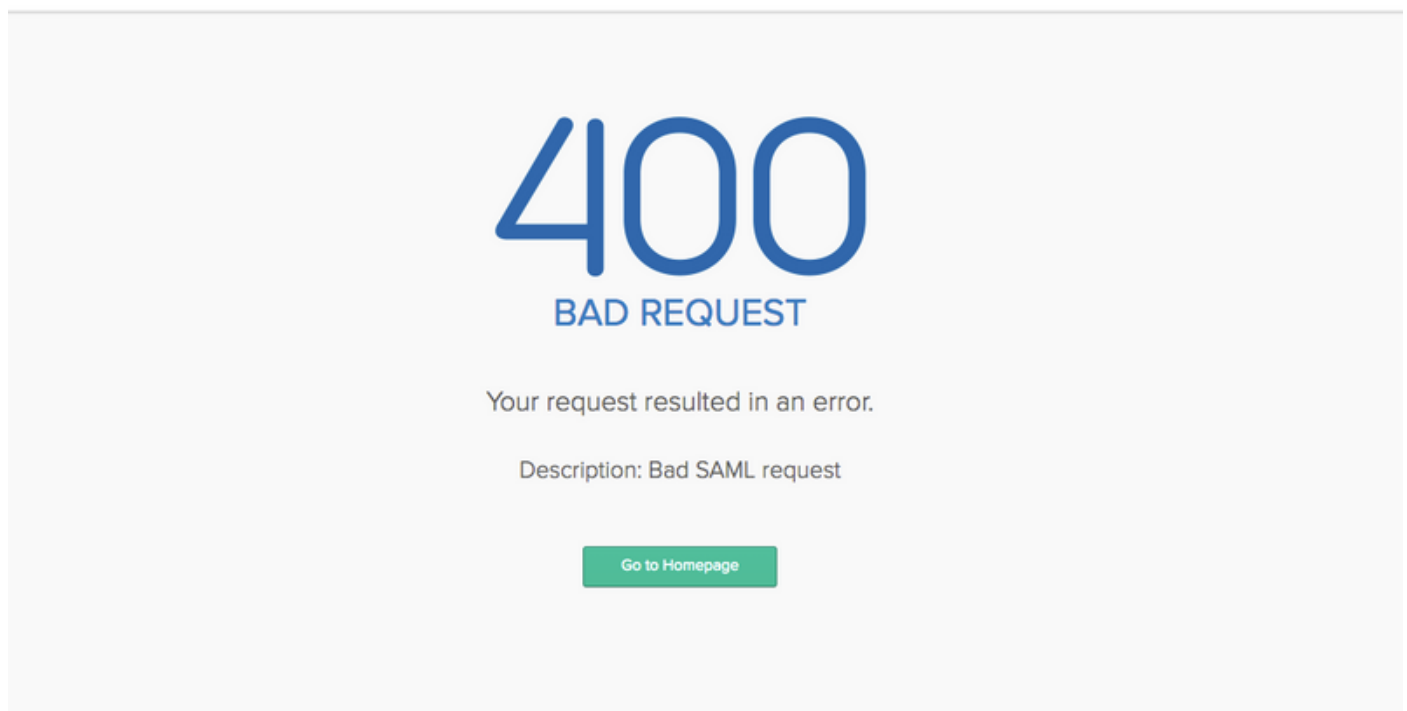
Navigate to **Administration > System > Logging > Debug Log Configuration**. Enable the level to DEBUG.

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

The table shows the component to debug and their corresponding log file.

## Common Issues and Solutions

Scenario 1. Bad SAML request.



This error is generic, check the logs in order to verify the flow and pinpoint the issue. On ISE guest.log:

ISE# show logging application guest.log | last 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
```

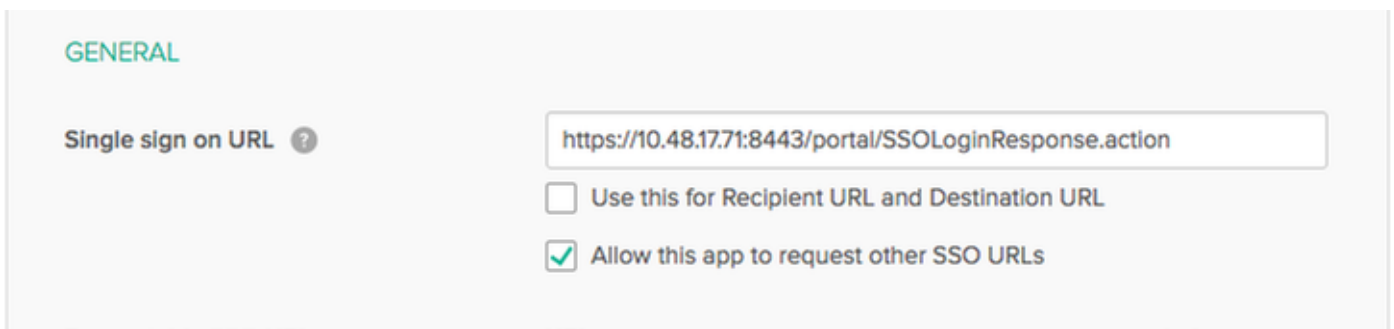


Identity Provider: com.cisco.cpm.acs.im.identitystore.saml.IdentityProvider@56c50ab6  
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][  
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- portalSessionInfo:  
portalId=9c969a72-b9cd-11e8-a542-d2e41bbdc546;portalSessionId=6770f0a4-bc86-4565-940a-  
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%2FzJOOb4672DqCNUJD%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  
Ob4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHhloiuQcIeJ  
o1WVnFVI29qDGjrzGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv  
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L  
nn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh  
DecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIP  
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlrFz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1z  
X6nmngdq3YIO37q9fBlQnCh3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWl  
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 has successfully redirected the user to IDP. However, no response back to ISE and the bad SAML request appears. Identify that OKTA does not accept our SAML request below is the request.

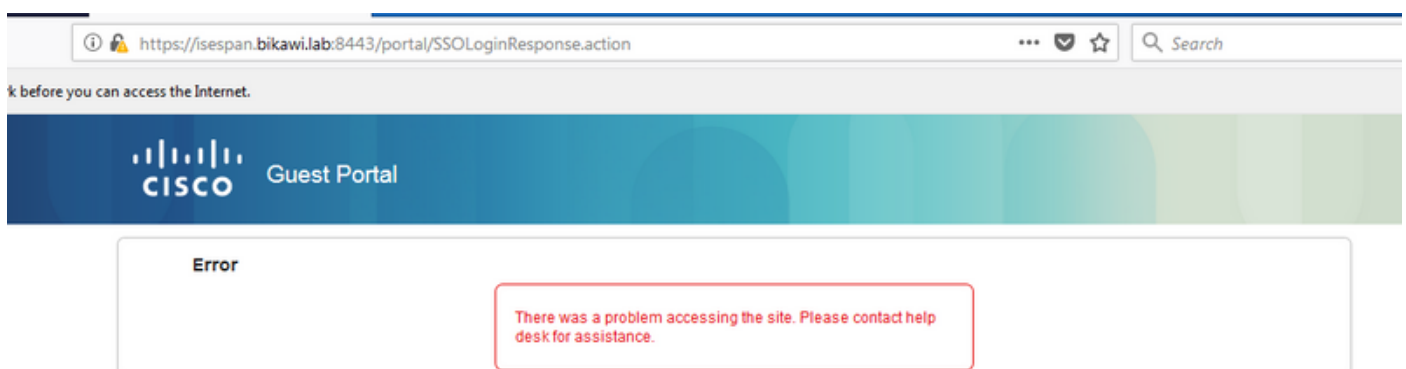
```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1hOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnC
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_DELIMITERisesperan.bikawi.lab
```

Now check again the application perhaps there are changes made.



The SSO URL is using IP address, however, guest is sending FQDN as we can see in the request above the last line contains SEMI\_DELIMITER<FQDN> to fix this issue change the IP address to FQDN on OKTA settings.

Scenario 2. "There was a problem accessing the site. Please contact helpdesk for assistance".



## Guest.log

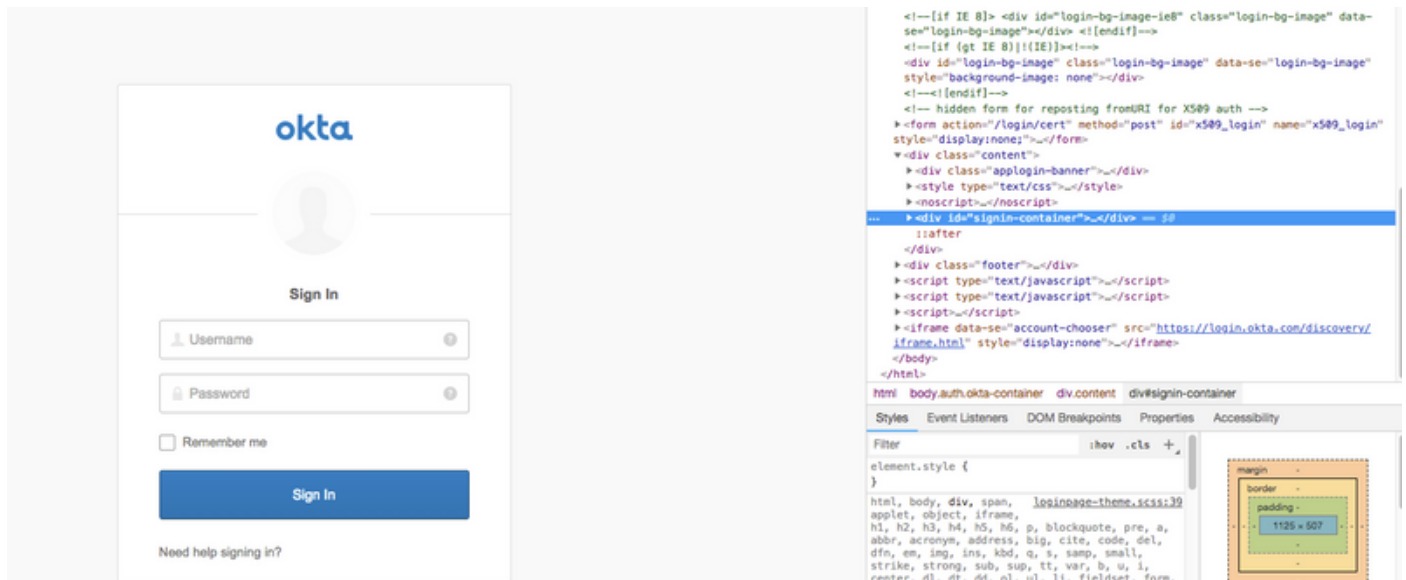
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
contain ma
```

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

From the logs, ISE reports that the Assertion is not correct. Check OKTA Audience URI ensure that it matches the SP to resolve it.

Scenario 3. Redirected to the Blank page, or the login option does not show.

It depends on the environment and the portal configuration. In this kind of issue you need to check the OKTA application and what URL's it require to authenticate. Click on the portal test then inspect element to check what websites must be reachable.



In this scenario only two URLs: application and login.okta.com - those should be permitted on the WLC.

## Related Information

- <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>