

# 使用OKTA SAML SSO配置ISE 2.3访客门户

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[联合SSO](#)

[网络流](#)

[配置](#)

[步骤1.在ISE上配置SAML身份提供程序和访客门户。](#)

[1.准备外部身份源。](#)

[2.创建SSO门户。](#)

[3.配置备用登录。](#)

[步骤2.配置OKTA应用和SAML身份提供程序设置。](#)

[1.创建OKTA应用程序。](#)

[2.从SAML身份提供程序导出SP信息。](#)

[3.确定SAML设置。](#)

[4.从应用程序导出元数据。](#)

[5.将用户分配给应用程序。](#)

[6.将元数据从Idp导入ISE。](#)

[步骤3.CWA配置。](#)

[验证](#)

[最终用户验证](#)

[ISE验证](#)

[故障排除](#)

[OKTA故障排除](#)

[ISE故障排除](#)

[常见问题和解决方案](#)

[相关信息](#)

## 简介

本文档介绍如何将身份服务引擎(ISE)与OKTA集成，为访客门户提供安全断言标记语言单点登录(SAML SSO)身份验证。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎访客服务。
- SAML SSO。
- ( 可选 ) 无线LAN控制器(WLC)配置。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎2.3.0.298
- OKTA SAML SSO应用
- 思科5500无线控制器版本8.3.141.0
- 联想Windows 7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 ( 默认 ) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

### 联合SSO

组织内的用户可以进行一次身份验证，然后访问多个资源。组织间使用的此标识称为联合标识。

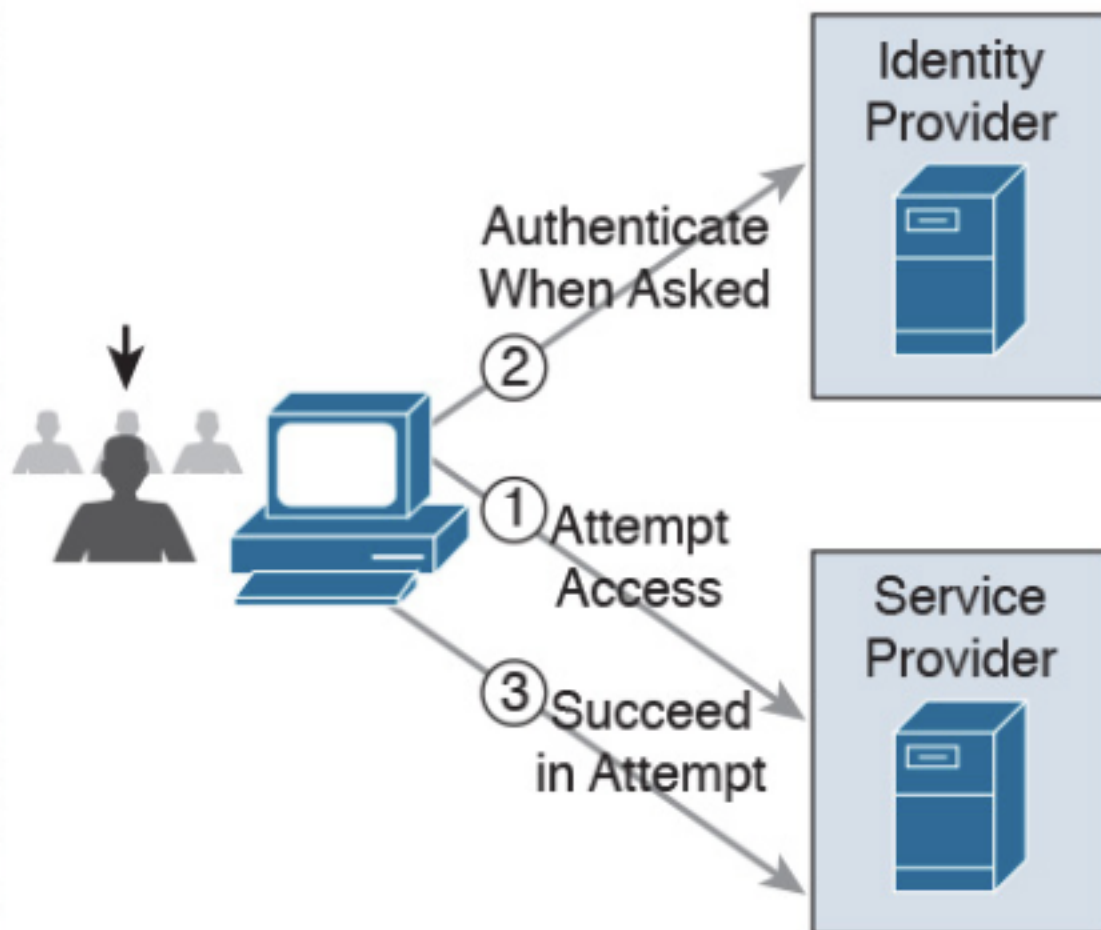
联合的概念：

- 原则：最终用户 ( 请求服务的用户 )、Web浏览器 ( 在本例中为终端 )。
- 服务提供商(SP):有时称为信赖方(RP)，即提供服务的系统，在本例中为ISE。
- 身份提供程序(IdP):管理发回SP ( 本例中为OKTA ) 的身份验证、授权结果和属性。
- 断言：IdP发送给SP的用户信息。

多种协议实施SSO，如OAuth2和OpenID。ISE使用SAML。

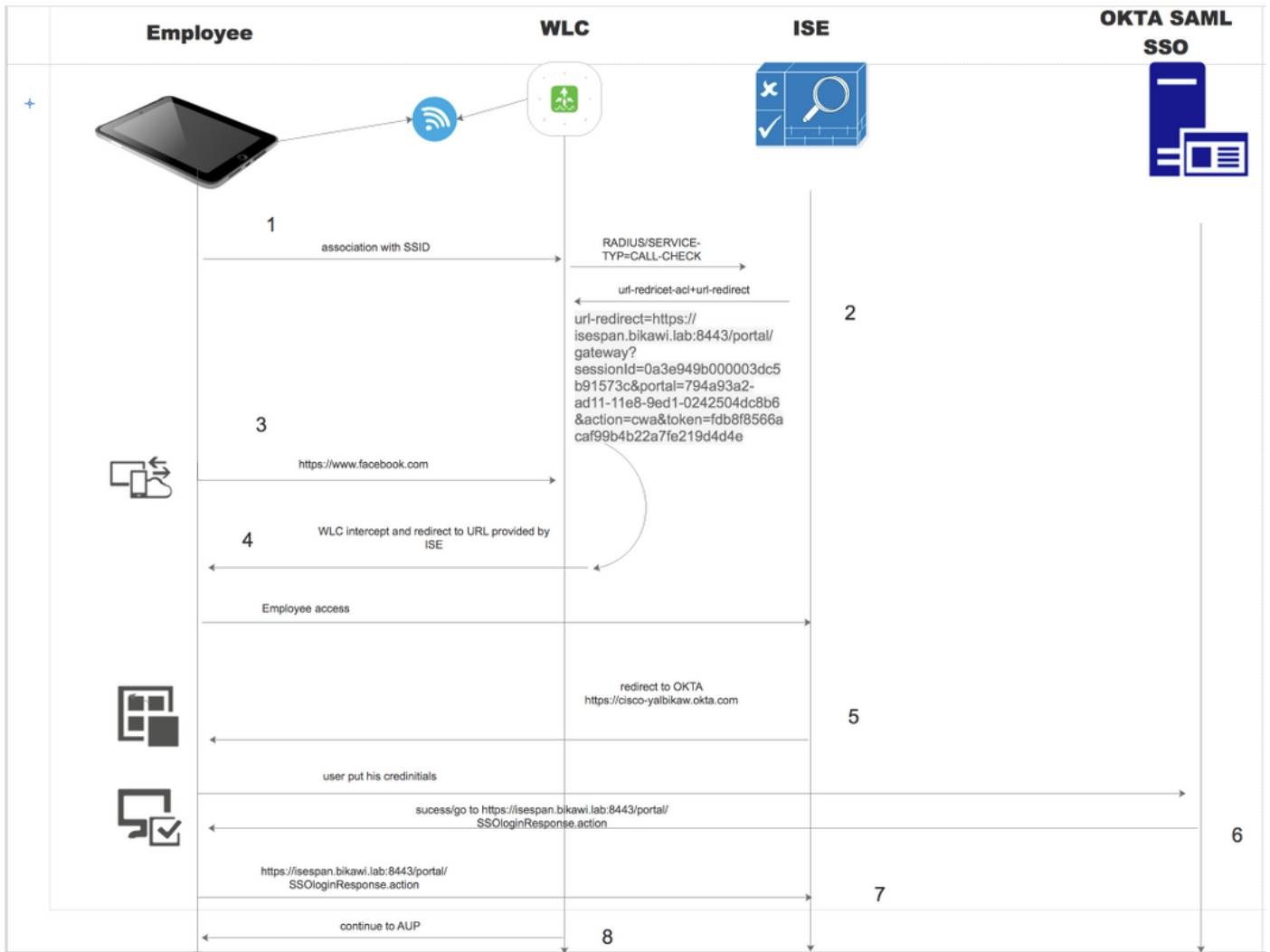
SAML是一个基于XML的框架，它描述以安全方式在业务实体之间使用和交换SAML断言。该标准描述了请求、创建、使用和交换这些断言的语法和规则。

ISE使用SP启动模式。用户被重定向到访客门户，然后ISE将其重定向到IdP进行身份验证。之后，它会重定向回ISE。请求经过验证，用户继续访客访问或自注册，具体取决于门户配置。



**SP-initiated**

网络流



1. 用户连接到SSID，身份验证为mac过滤(mab)。
2. ISE以包含重定向URL和重定向ACL属性的access-accept回应
3. 用户尝试访问[www.facebook.com](https://www.facebook.com)。
4. WLC拦截请求并将用户重定向到ISE访客门户，用户点击员工访问以使用SSO凭证注册设备。
5. ISE将用户重定向到OKTA应用进行身份验证。
6. 身份验证成功后，OKTA将SAML断言响应发送到浏览器。
7. 浏览器将断言中继回ISE。
8. ISE验证断言响应，如果用户已正确进行身份验证，则继续AUP，然后进行设备注册。

有关SAML的详细信息，请查看以下链接

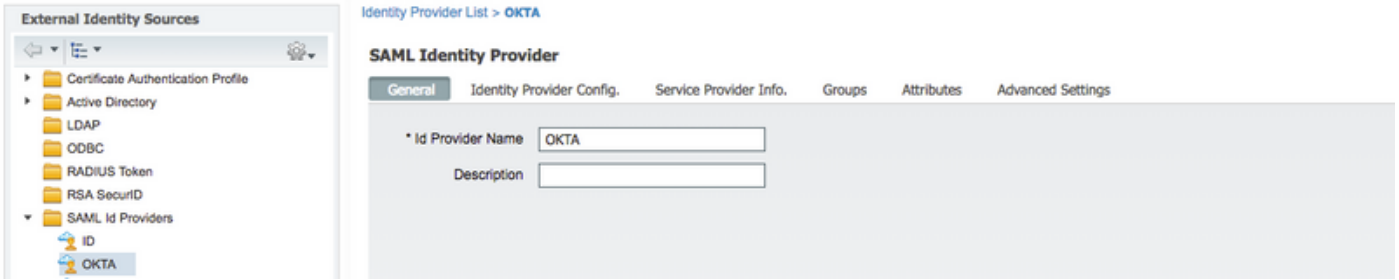
<https://developer.okta.com/standards/SAML/>

## 配置

**步骤1.在ISE上配置SAML身份提供程序和访客门户。**

1.准备外部身份源。

步骤1.导航至Administration > External Identity Sources > SAML id Providers。

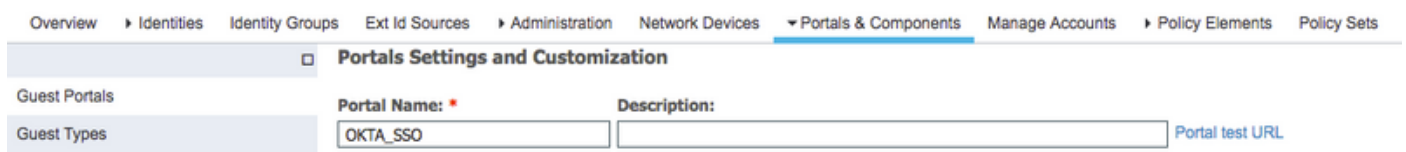
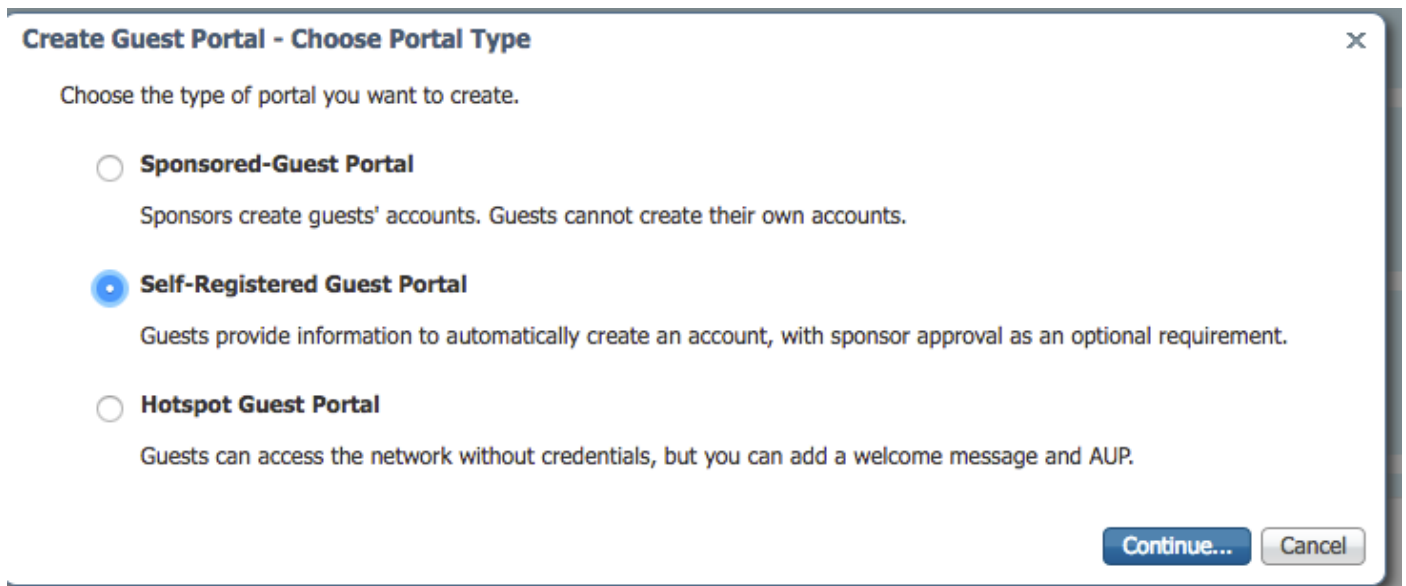


步骤2.为ID提供程序分配名称并提交配置。

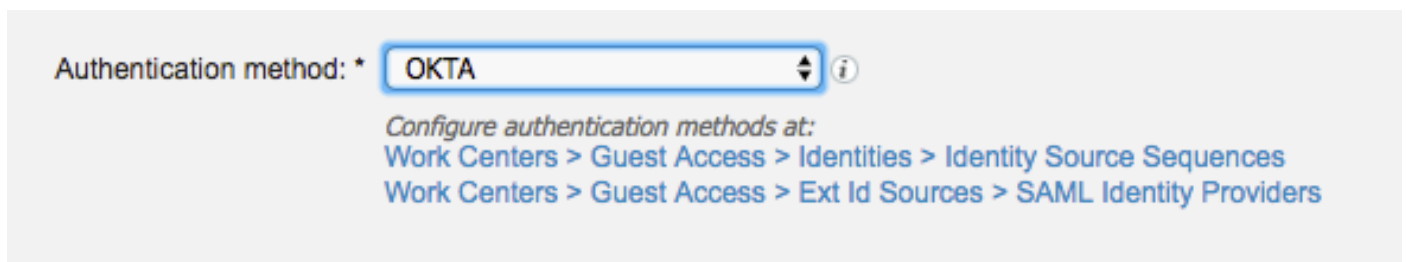
## 2.创建SSO门户。

步骤1.创建分配给OKTA的门户作为身份源。BYOD、设备注册、访客等的任何其他配置与普通门户的配置完全相同。在本文档中，该门户映射到访客门户，作为员工的替代登录。

步骤2.导航至“工作中心”>“访客访问”>“门户和组件”并创建门户。



步骤3.选择身份验证方法以指向之前配置的身份提供程序。



步骤4.选择OKTA身份源作为身份验证方法。

( 可选 ) 选择BYOD设置。

## ▼ 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](#)

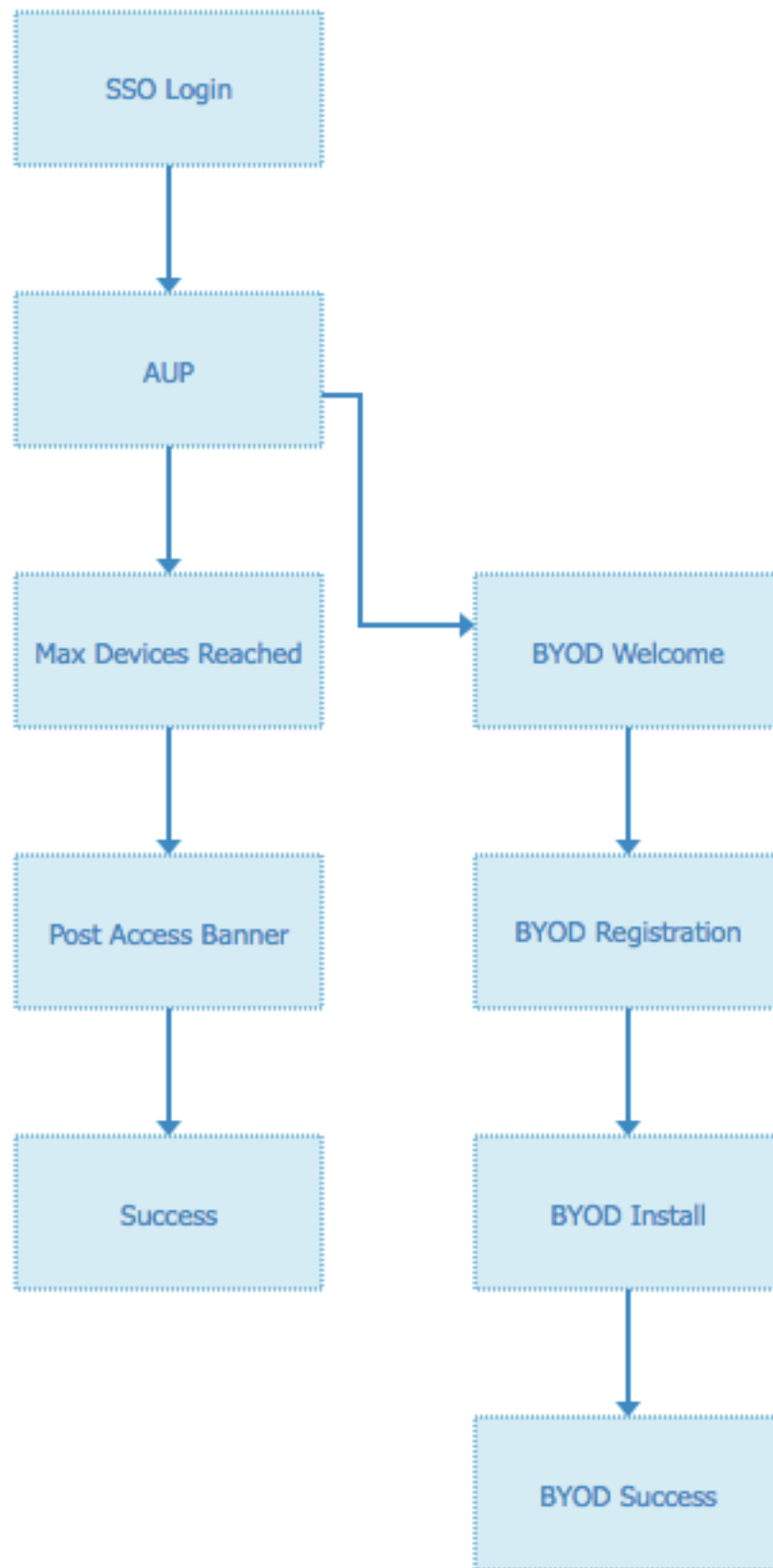
After successful device configuration take employee to:

- Originating URL [\(i\)](#)

- Success page

- URL:

步骤5.保存门户配置，使用BYOD时，流程如下所示：



### 3.配置备用登录。

注意：如果不使用备用登录名，可跳过此部分。

导航至自助注册访客门户或为访客访问自定义的任何其他门户。

在登录页面设置中，添加备用登录门户：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

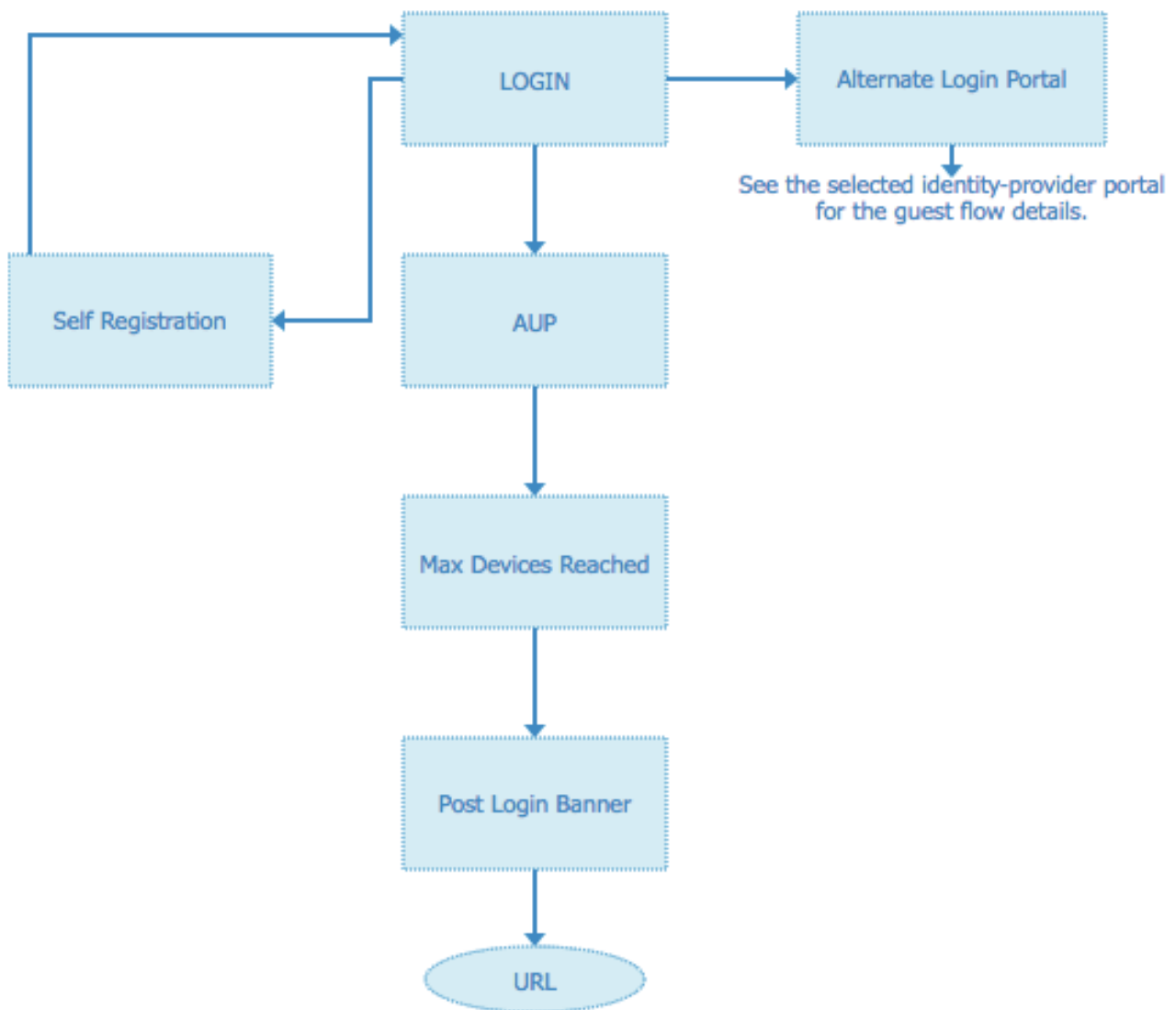
Allow guests to change password after login ⓘ

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

▼

这是入口流。





## 步骤2.配置OKTA应用和SAML身份提供程序设置。

### 1.创建OKTA应用程序。

步骤1.使用管理员帐户登录OKTA网站。

← 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

步骤2. 点击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

步骤3. 创建新应用，将其选为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

## 常规设置

### 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

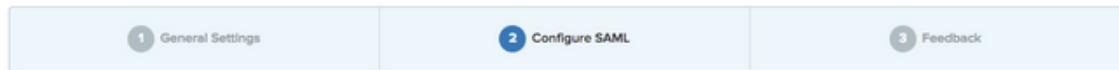


Do not display application icon in the Okta Mobile app

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?

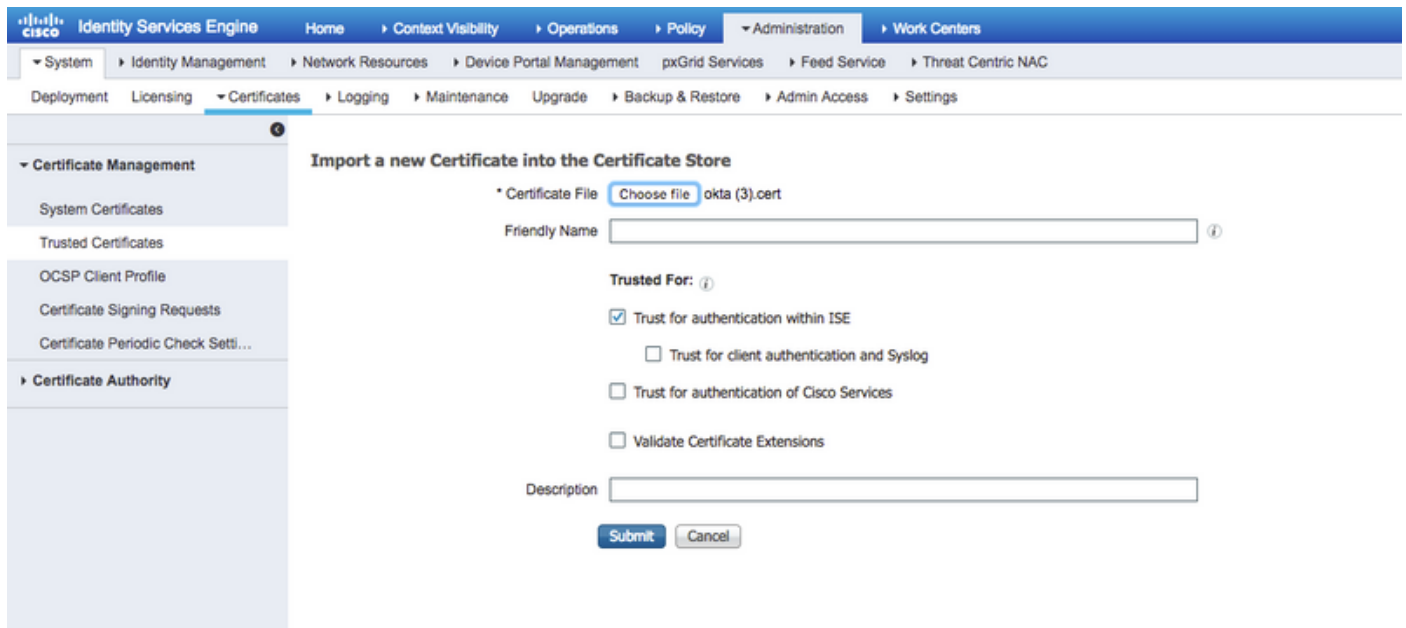
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

#### Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

步骤4. 下载证书并将其安装在ISE受信任证书中。



2. 从SAML身份提供程序导出SP信息。

导航至之前配置的身份提供程序。单击“Service Provider Info(服务提供商信息)”并将其导出，如图所示。

### SAML Identity Provider

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

#### Service Provider Information

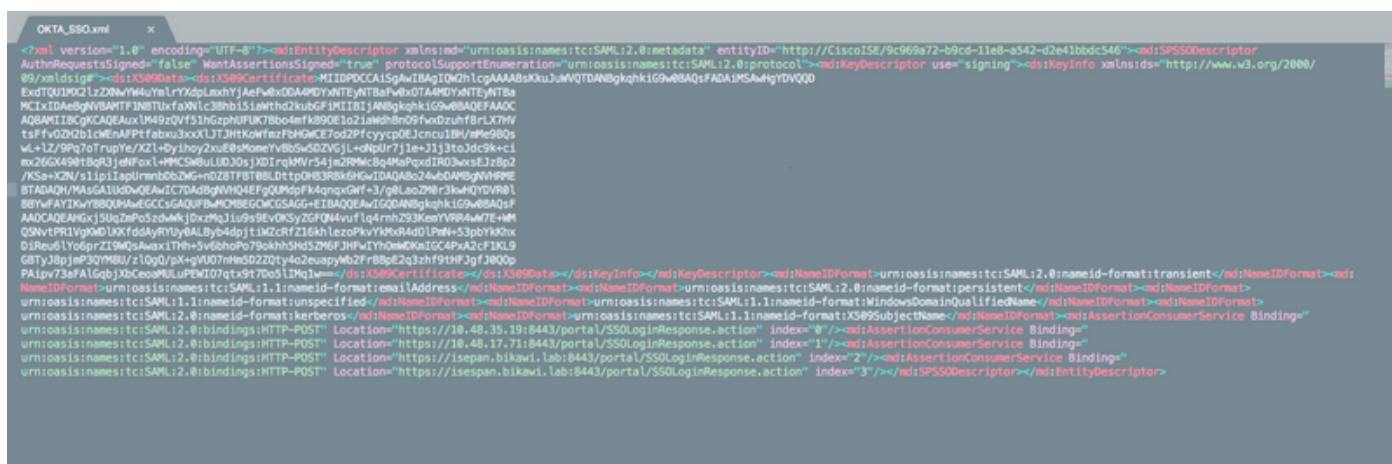
Load balancer ?

Export Service Provider Info. Export ?

Includes the following portals:

OKTA\_SSO

导出的zip文件夹包含XML文件和readme.txt



对于某些身份提供程序，您可以直接导入XML，但在这种情况下，需要手动导入。

- 单点登录URL ( saml断言 )

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实体ID

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

SSO URL以IP地址和FQDN格式提供。

**警告：**格式的选择取决于授权配置文件上的重定向设置，如果使用静态IP，则应将IP地址用于SSO URL。

### 3.确定SAML设置。

步骤1.在SAML设置上添加这些URL。

## 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](#)

步骤2.根据托管此服务的PSN的数量，可以从XML文件添加多个URL。名称ID格式和应用用户名取决于您的设计。

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

步骤3.单击“下一步”并选择第二个选项。

**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.从应用程序导出元数据。

**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.

**元数据 :**

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exk1rq81oEmedZSf4356">
<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>
MIIDrDCCApSgAwIBAgIGAWWP1TasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXl1hbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFglpbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNDMwNDMwNDMwNDMwNDMwNDMwNDMwNDMw
BgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEXMBUGA1UEAwwOY2l1Z28teWFsYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0wCwYD
VQQKDA1TYW4gRnJhbmNpc2NvMQ0wCwYDVQQEJ2l1Z28teWFsYmlrYXcxHDAaBgkqhkiG9w0BCQEW
DmNpc2NvLXl1hbGJpa2F3MRwwGgYJKoZIhvcNAQELBQADggEBAJUK5zGPZwxECv5dN6YERuV5C5e
HUXq3KGul2yI fiH7x8EartZ4/wGP/HYUCNCNw3HTh+6T3oLSAevm6U3ClNELRvG2kG39b/9+Er
PG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI TJ2Tq2uuYpSveIMxQmy7r5qFz
iWOTvDF2Xp0Ag1e91H6nbdtsz3e5MMSKYGr9HaigGgqG4yXHkAs77ifQonRz7au0Uo9sInH6r
WG+eOesysecPuWQtEqNqt+MyZn1CurJ0e+JTvKYH1dSWapM1dzqoXOzyF7yiId9KPP6I4Ndc+B
Xe1dA8imneYy5MH7/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>
```

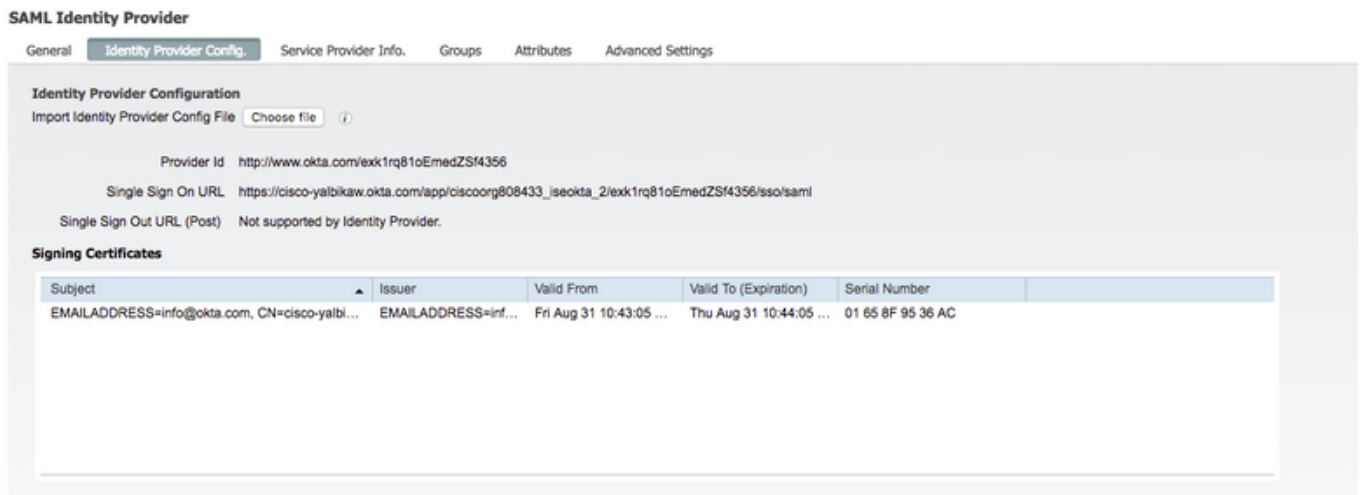
以XML格式保存文件。

## 5.将用户分配给应用程序。

将用户分配到此应用程序时，有一种AD集成方法，其解释如下：[OKTA活动目录](#)

## 6.将元数据从Idp导入ISE。

步骤1.在SAML身份提供程序下，选择身份提供程序配置和导入元数据。



**SAML Identity Provider**

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

**Identity Provider Configuration**

Import Identity Provider Config File  (?)

Provider Id `http://www.okta.com/exk1rq81oEmedZSf4356`

Single Sign On URL `https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml`

Single Sign Out URL (Post) Not supported by Identity Provider.

**Signing Certificates**

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

步骤2.保存配置。

## 步骤3.CWA配置。

本文档介绍ISE和WLC的配置。

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

在重定向ACL中添加URL。

<https://cisco-yalbikaw.okta.com> /添加您的应用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.

## 验证

测试门户并验证您是否能够访问OKTA应用

Portal Name: \*

Description:

OKTA\_SSO

[Portal test URL](#)



#### Portal Behavior and Flow Settings

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



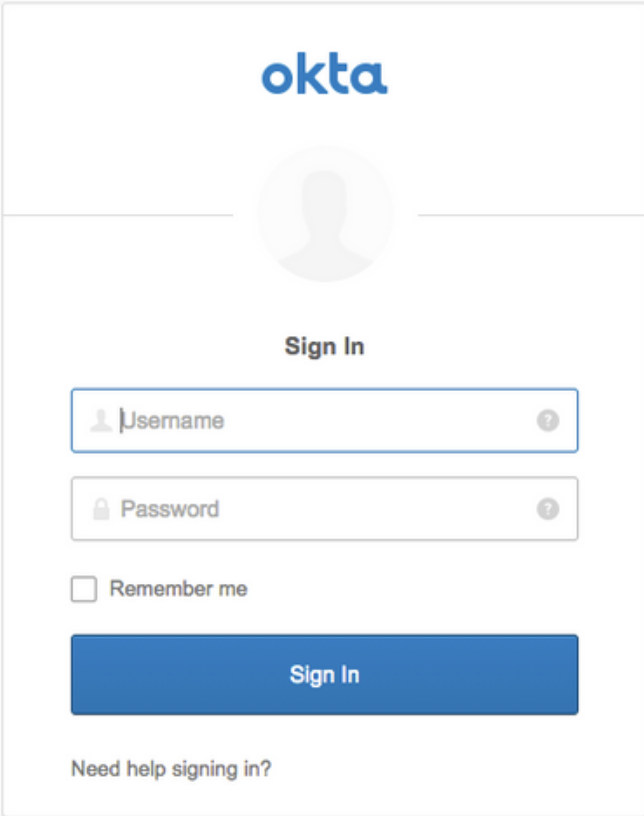
#### Portal Page Customization

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

步骤1. 点击门户测试，您应被重定向到SSO应用。

## Connecting to

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



The image shows a web-based sign-in form for Okta. 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 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?".

步骤2.检查与的信息连接

步骤3.如果输入可能看到错误的saml请求的凭据，这并不一定意味着此时配置错误。

## 最终用户验证



The image shows a screenshot of a web browser displaying the Cisco Guest Portal. The browser's address bar shows a URL starting with "https://campus.bkarelab@44.5/portal/PortalSetup.action?portal=794a93a2-ad15-11e8-9ed1-0242504acdb6&sessionId=0a3e949e000002c15eb0036e0...". Below the browser window, there is a blue header with the Cisco logo and the text "Guest Portal". The main content area features a "Sign On" section with the subtext "Sign on for guest access". This section includes two input fields for "Username" and "Password", a blue "Sign On" button, and a link that says "Or register for guest access". Below this, there is a section titled "You can also login with" which includes a "Microsoft account" link with a small icon of a person.

before 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



**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 usernames 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验证

检查生命日志以验证身份验证状态。

Sep 30, 2018 12:39:09.514 AM	✓	🔒	okta-test@cisco.c...	3C:A9:F4:34:9F:70				
Sep 30, 2018 12:33:32.640 AM	✓	🔒	3C:A9:F4:34:9F:70	3C:A9:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest	yazan-cpp

## 故障排除

### OKTA故障排除

步骤1.检查“报告”选项卡中的日志。

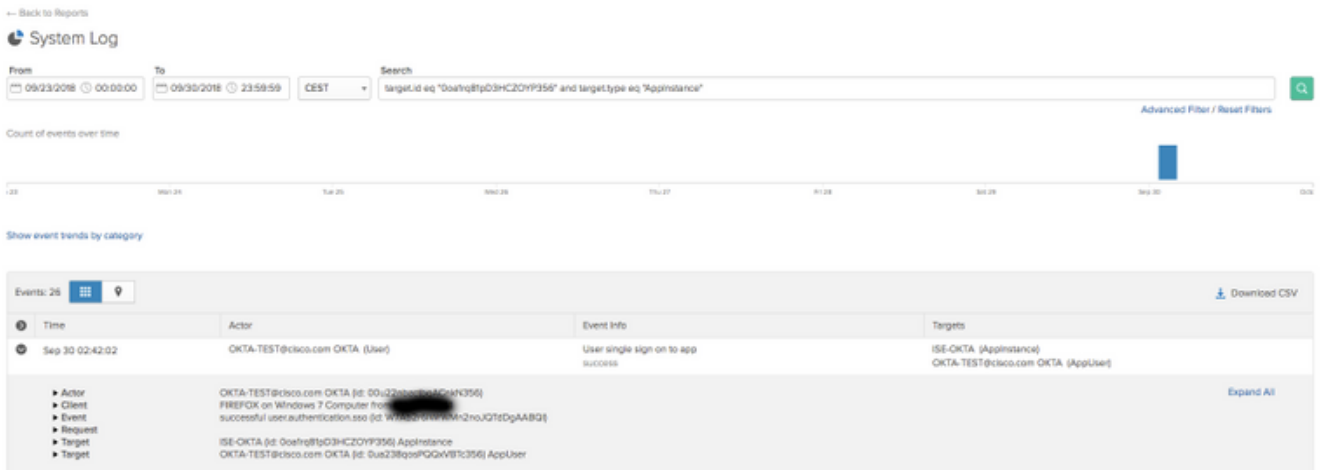
The screenshot shows the Okta Reports dashboard. At the top, there is a navigation bar with the Okta logo and links for Dashboard, Directory, Applications, Security, Reports, and Settings. On the right, there is a 'My Applications' dropdown menu. The main content area is titled 'Reports' and includes a 'Help' icon. The dashboard is organized into several sections:

- Okta Usage (LAST 30 DAYS):** Shows 0 users who have never signed in and 3 users who have signed in. A link for 'Okta Password Health' is provided.
- Application Usage (LAST 30 DAYS):** Shows 8 apps with unused assignments and 2 unused app assignments. Links for 'App Password Health' and 'SAML Capable Apps' are included.
- Auth Troubleshooting:** Contains links for 'Okta Logins (Total, Failed)', 'SSO Attempts', and 'Auths Via AD Agent (Total, Failed)'.
- Application Access Audit:** Includes a link for 'Current Assignments'.
- Multifactor Authentication:** Includes links for 'MFA Usage' and 'Yubikey Report'.

On the right side, there is a 'System Log' section with a list of activity types: Agent Activity, Application Access, Application Membership Change, Authentication Activity, Policy Activity, Provisioning Activity, System Import Activity, User Account Activity, and User Lifecycle Activity.

步骤2.也从应用程序查看相关日志。

The screenshot shows the configuration page for an application named 'ISE-OKTA'. At the top left, there is a '← Back to Applications' link. The application is represented by a gear icon and is currently set to 'Active'. A 'View Logs' button is visible next to the application name. Below the application name, there are tabs for 'General', 'Sign On', 'Import', and 'Assignments', with 'Assignments' being the active tab.



## ISE故障排除

有两个日志文件要检查

- ise-psc.log
- guest.log

导航至**管理>系统>日志记录>调试日志配置**。启用DEBUG级别。

SAML ise-psc.log  
访客接入 guest.log  
门户 guest.log

下表显示要调试的组件及其相应的日志文件。

## 常见问题和解决方案

场景1. SAML请求错误。



# 400

## BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

Go to Homepage

此错误是一般错误，请检查日志以验证流并查明问题。在ISE访客.log上：

## ISE# show logging application guest.log |最后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:

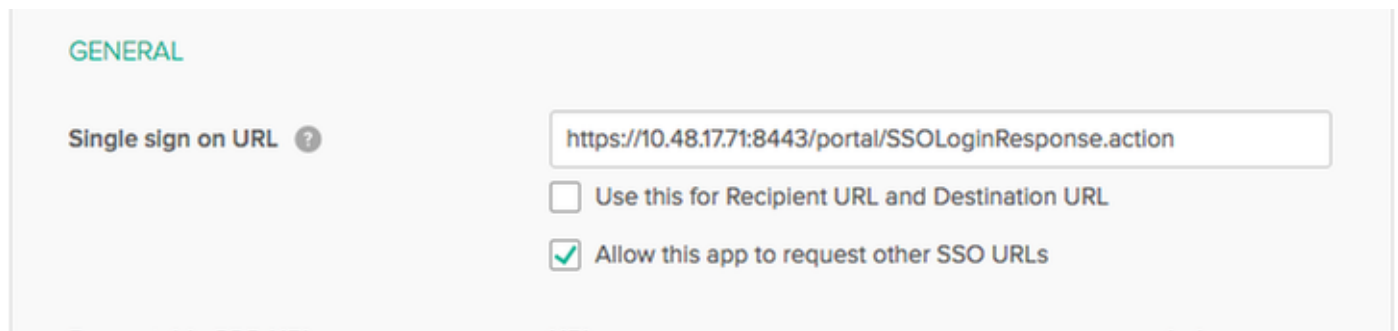
    Portal Name: OKTA_SSO
    Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546
    Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
    Identity Provider: com.cisco.cpm.acs.im.identitystore.saml.IdentityProvider@56c50ab6
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
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%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoEuyPu95j9%2FzJ0Ob4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrzGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVspuHEPdhPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwLrfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnCh3jF072v2xmatdQLUyIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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
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%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoEuyPu95j9%2FzJ0Ob4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJ
o1WVnFVI29qDGjrzGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DEcRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVspuHEPdhPk79CJe4T6KQRElvECbfkdb6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwLrfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1z
X6nmngdq3YIO37q9fBlQnCh3jF072v2xmatdQLUyIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWl
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_DELIMITERisespan.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:
/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
```

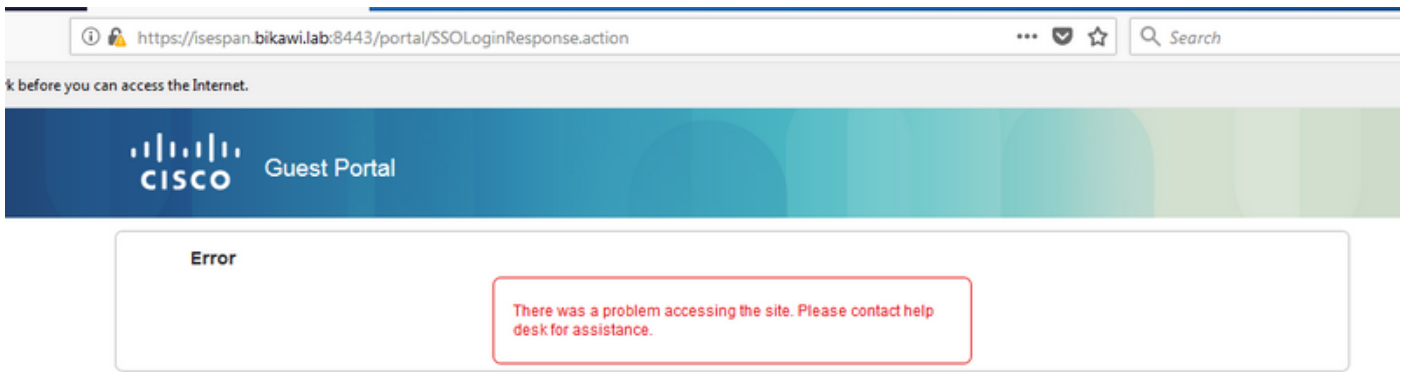
ISE已成功将用户重定向到IDP。但是，不响应ISE，并且出现错误的SAML请求。确定OKTA不接受我们的SAML请求是请求。

```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1h0iulyQcIeJo1WVnFVI29qDGjrjGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0SltA0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfk6XdcnITsIPtot64oM%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_DELIMITERisespan.bikawi.lab
现在再次检查应用程序，可能已进行更改。
```



SSO URL使用IP地址，但是，访客正在发送FQDN，如我们在最后一行上方的请求中看到的，包含 SEMI\_DELIMITER<FQDN>以解决此问题，请在OKTA设置中将IP地址更改为FQDN。

场景2.“访问站点时出现问题。请联系帮助台寻求帮助”。



## Guest.log

```

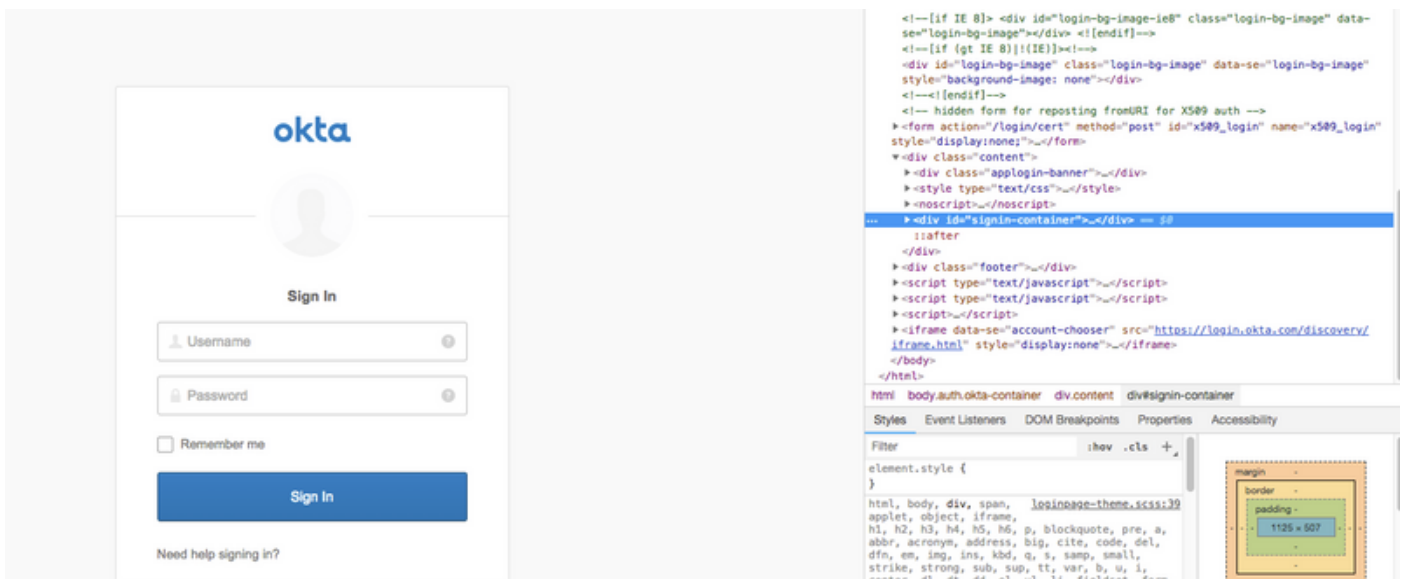
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1] []
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::: SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
contain ma
tching service provider identifier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

```

从日志中，ISE报告断言不正确。检查OKTA受众URI，确保它与SP匹配以解析它。

场景3.已重定向到“空白”页面，或登录选项未显示。

它取决于环境和门户配置。在此类问题中，您需要检查OKTA应用及其身份验证所需的URL。点击门户测试，然后检查元素以检查哪些网站必须可访问。



在此场景中，仅有两个URL:application和login.okta.com — 应允许在WLC上使用。

## 相关信息

- <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>