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. OKTA 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声明标记语言单点登录(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）无线局域网控制器(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
- Cisco 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

组织内的用户只需进行一次身份验证，即可访问多个资源。跨组织使用的这种身份称为联合身份。

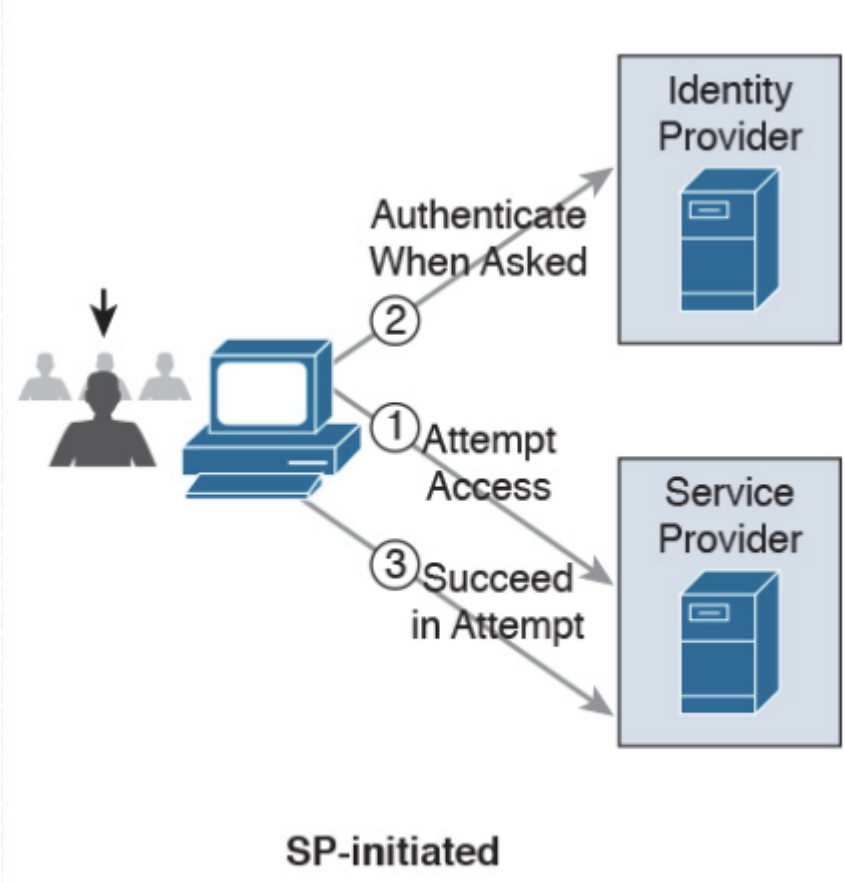
联合的概念：

- 原则：最终用户（请求服务的用户）、Web浏览器（在本例中，是终端）。
- 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):用于管理发送回SP（在本例中为OKTA）的身份验证、授权结果和属性。
- 断言：IdP发送到SP的用户信息。

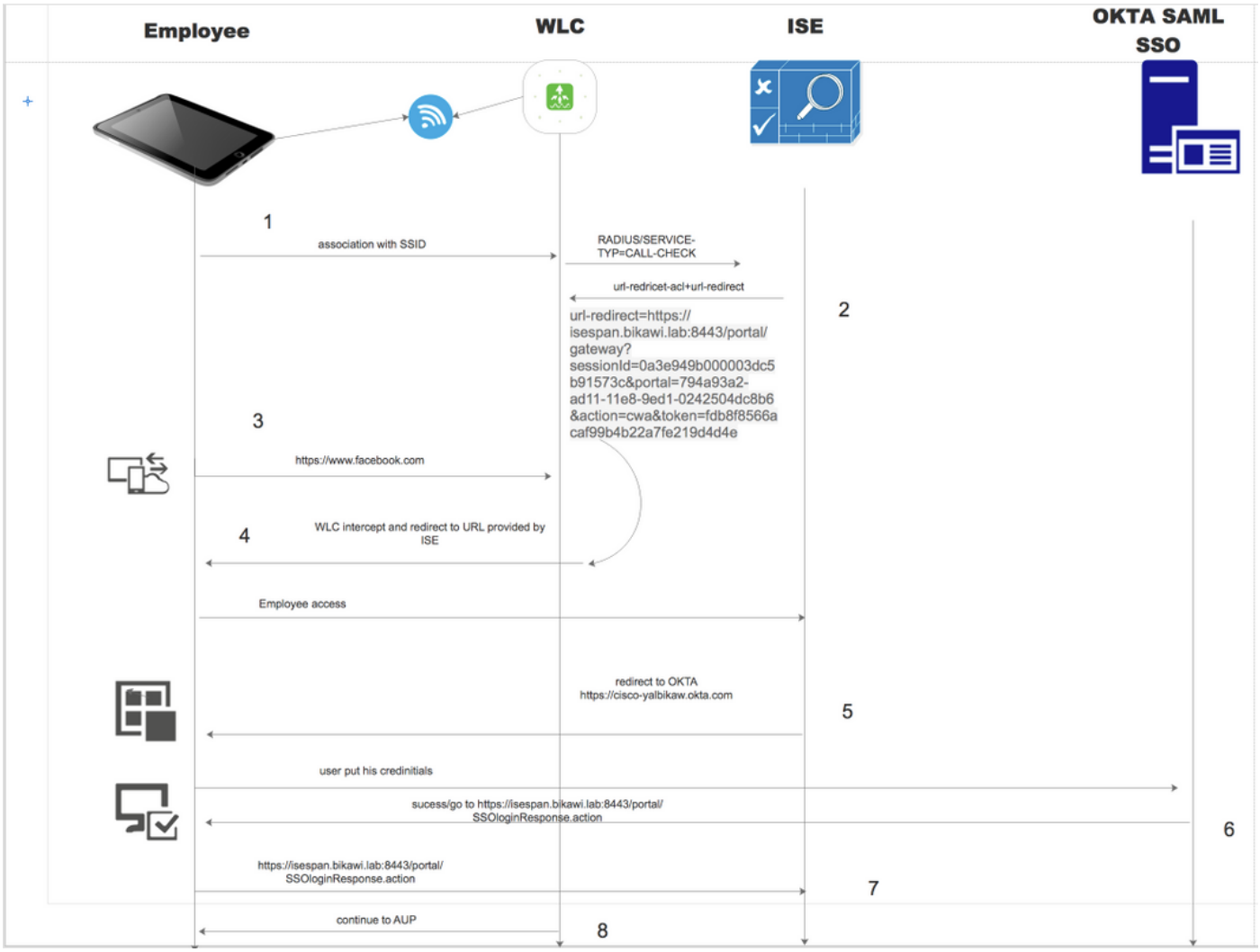
一些协议实施SSO，例如OAuth2和OpenID。ISE使用SAML。

SAML是一个基于XML的框架，它以安全的方式描述业务实体之间对SAML断言的使用和交换。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，它将重定向回ISE。验证请求后，用户继续访问访客或自行登录，具体取决于门户配置。


Identity
Provider
Authenticate
When Asked
2
1 Attempt
Access
Service
Provider
3 Succeed
in Attempt
SP-initiated

网络流



1. 用户连接到SSID，身份验证为mac过滤(mab)。

2. ISE使用包含Redirect-URL和Redirect-ACL属性的访问接受进行响应
3. 用户尝试访问www.facebook.com。
4. WLC拦截请求并将用户重定向到ISE访客门户，用户点击员工访问权限以便使用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，如果用户正确通过身份验证，它会进入AUP，然后进行设备注册。

有关SAML的详细信息，请查看以下链接

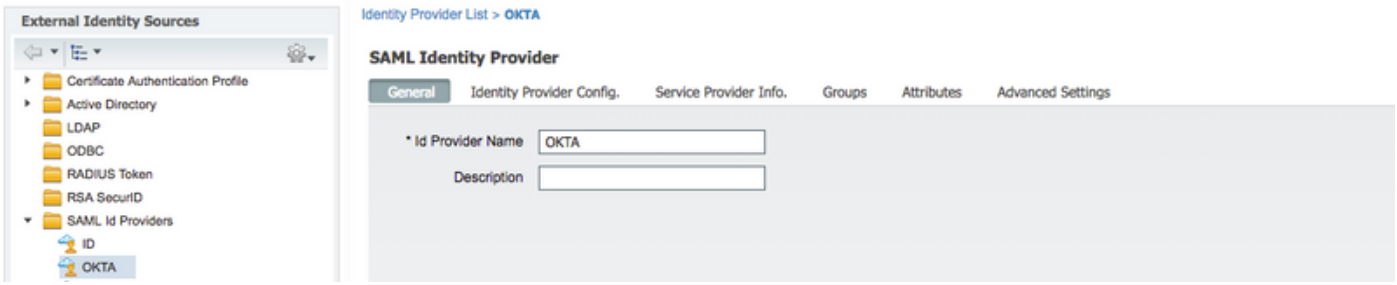
https://developer.okta.com/standards/SAML/

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.导航到管理>外部身份源> SAML ID提供程序。

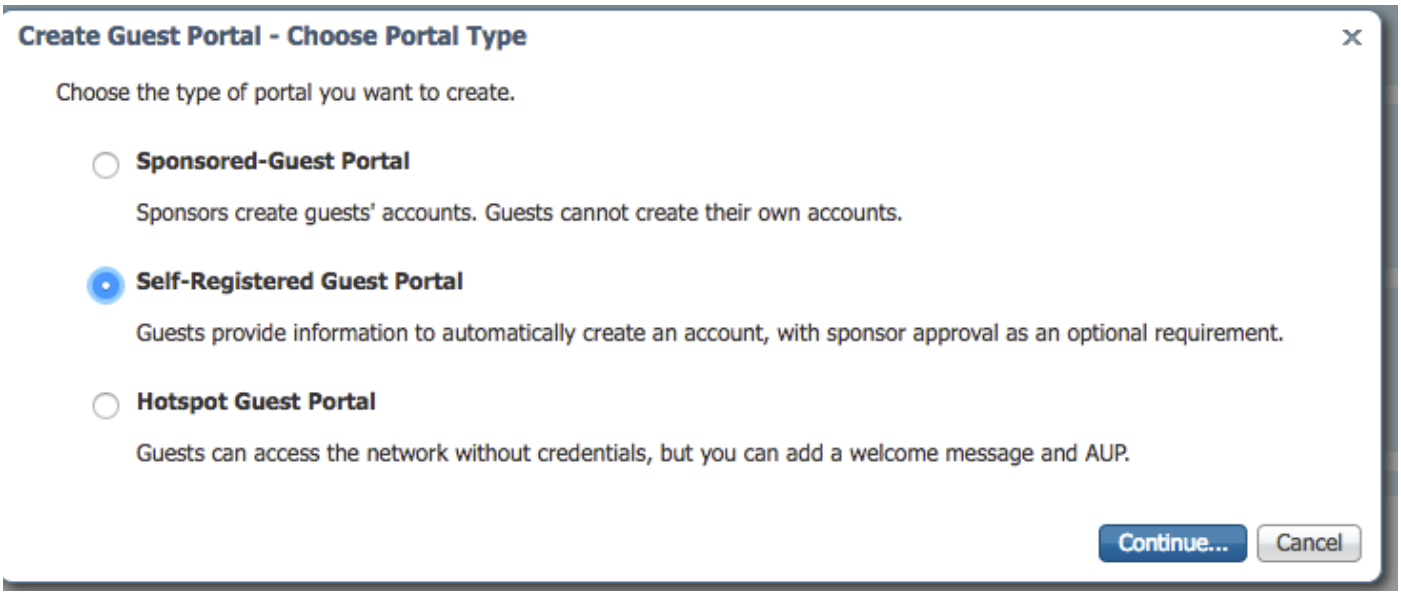


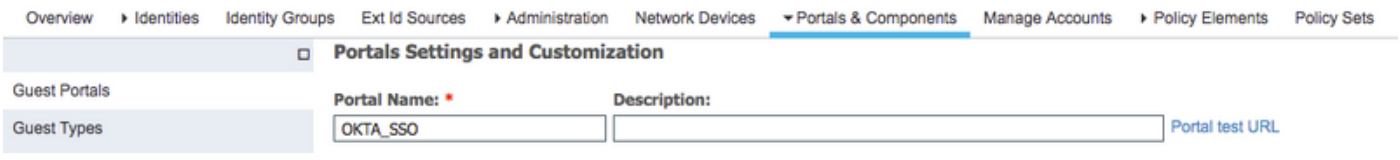
步骤2.为ID提供程序分配名称并提交配置。

2.创建SSO门户。

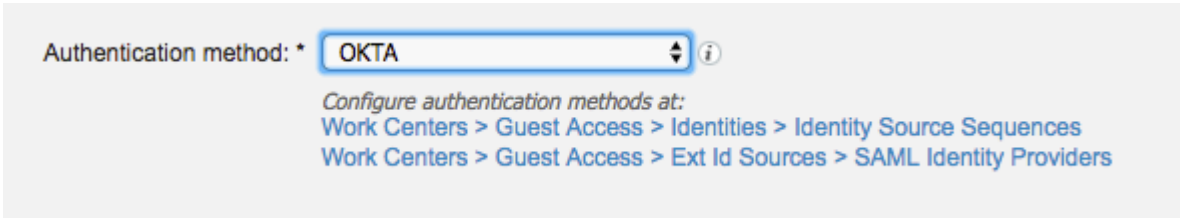
步骤1.创建作为身份源分配给OKTA的门户。BYOD、设备注册、访客等的任何其他配置与普通门户完全相同。在本文档中，门户会映射到访客门户，作为员工的备用登录。

第2步：导航到工作中心>访客接入>门户和组件，然后创建门户。



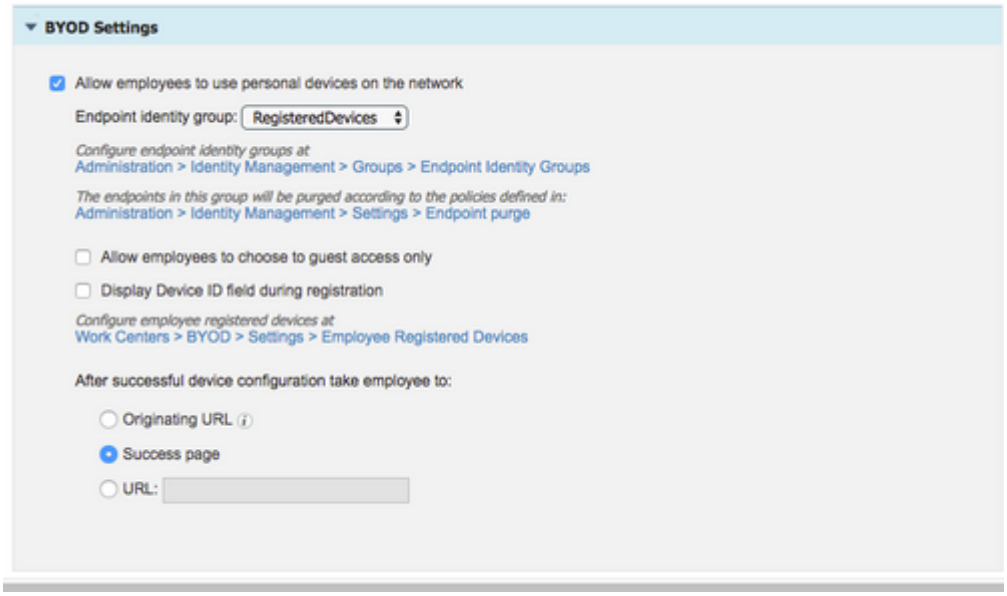


步骤3.选择身份验证方法，以指向之前配置的身份提供程序。

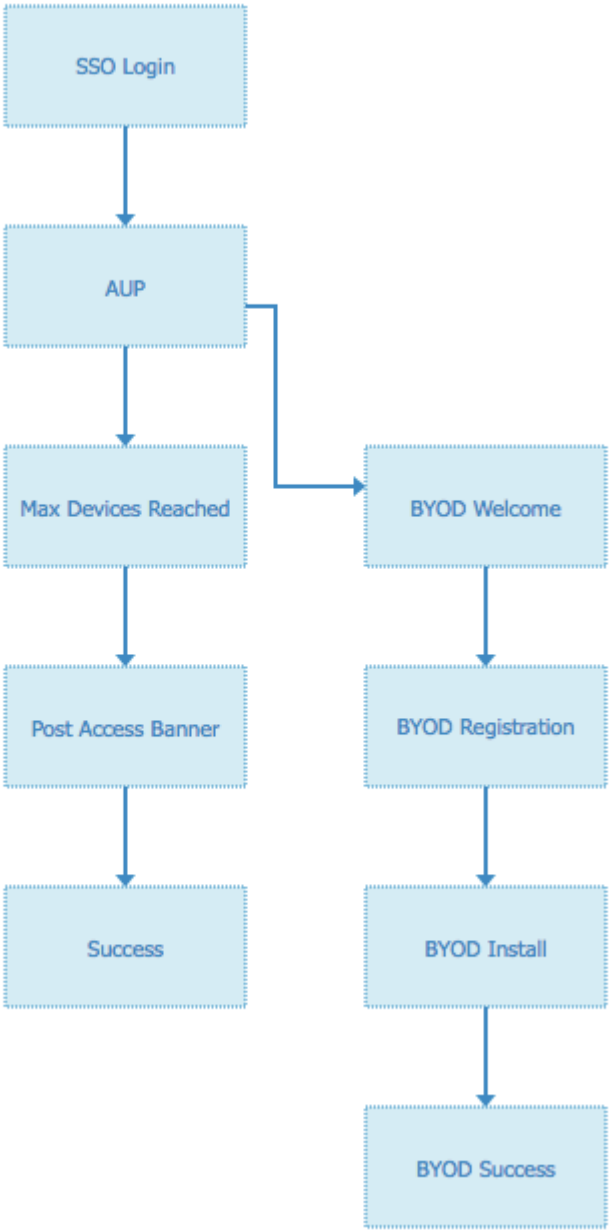


步骤4.选择OKTA身份源作为身份验证方法。

（可选）选择自带设备设置。



步骤5.保存门户配置，使用BYOD时，流程如下所示：

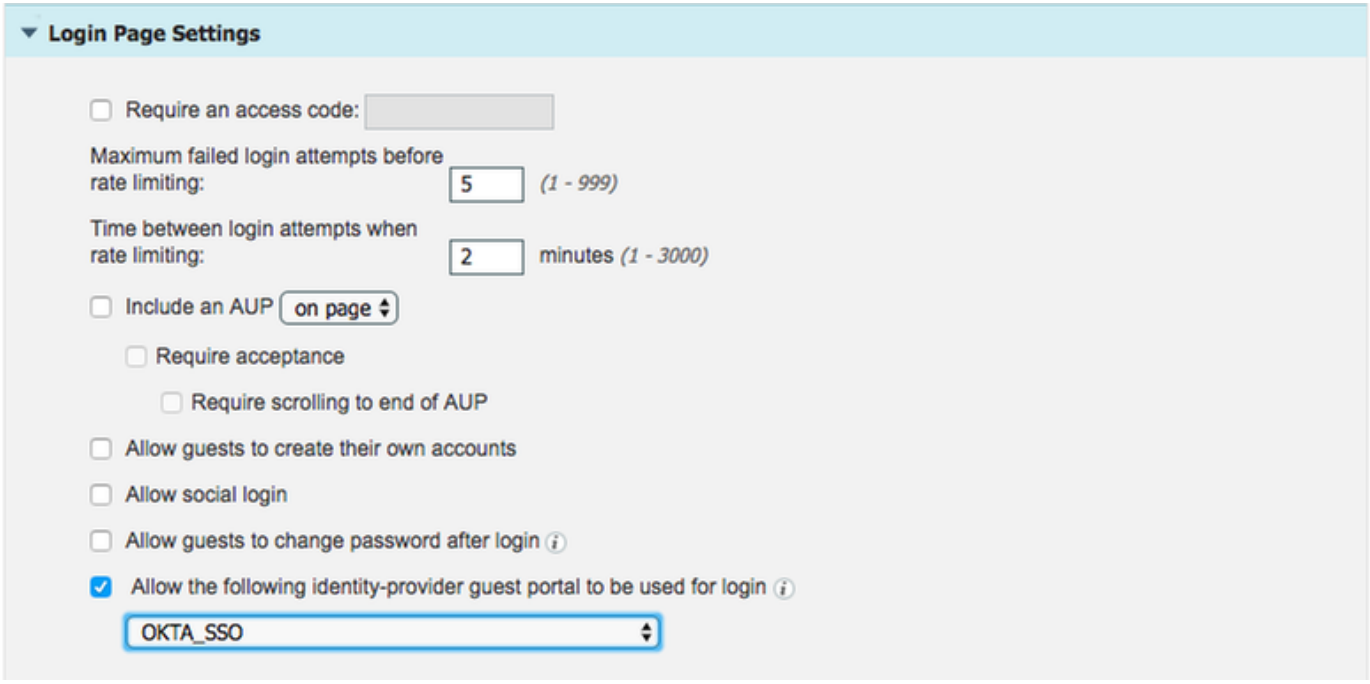


3.配置备用登录。

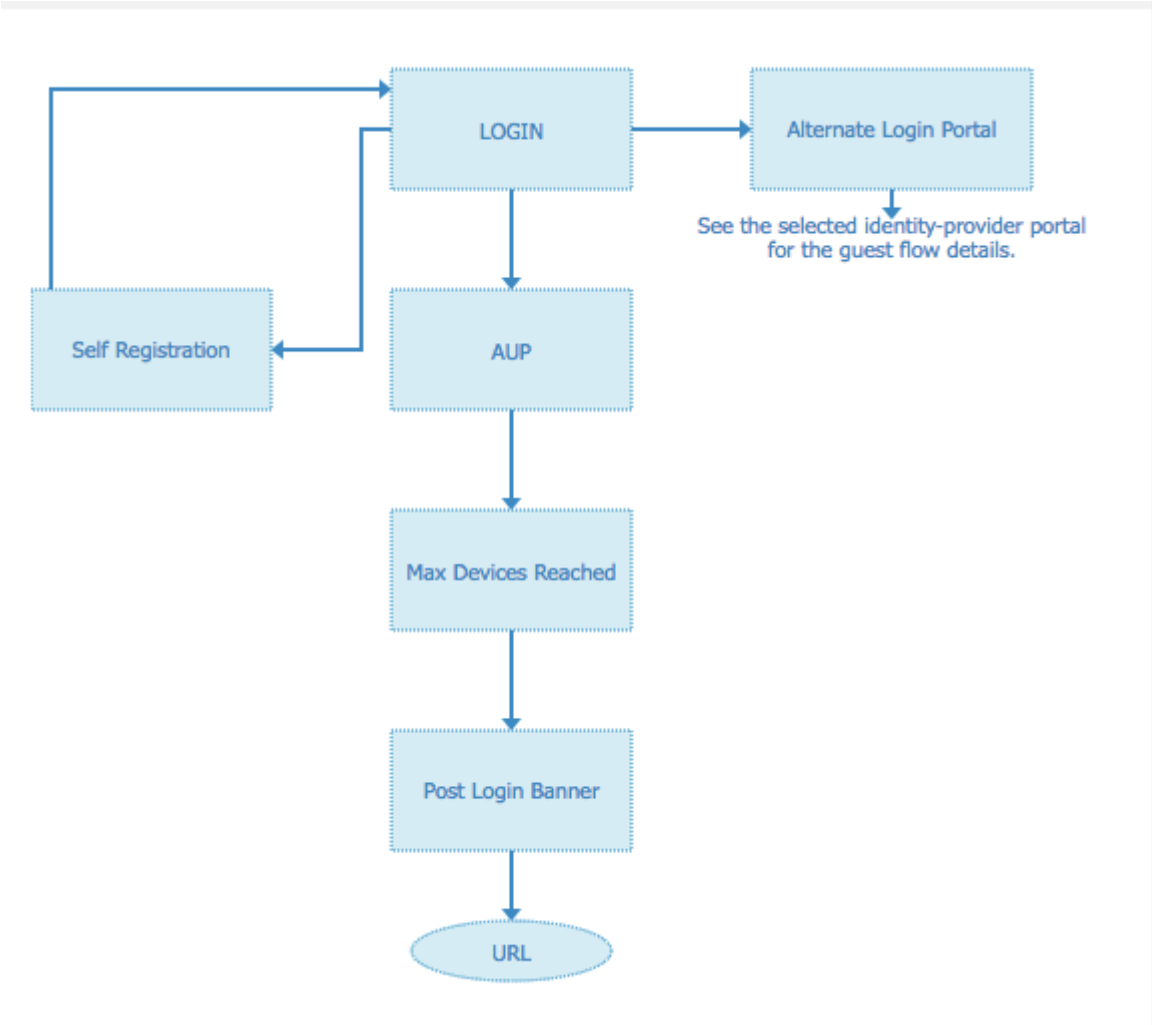
注意：如果不使用Alternative登录，可以跳过此部分。

导航到自助注册访客门户或任何其他为访客访问定制的门户。

在登录页面设置上，添加备用登录门户：OKTA_SSO。



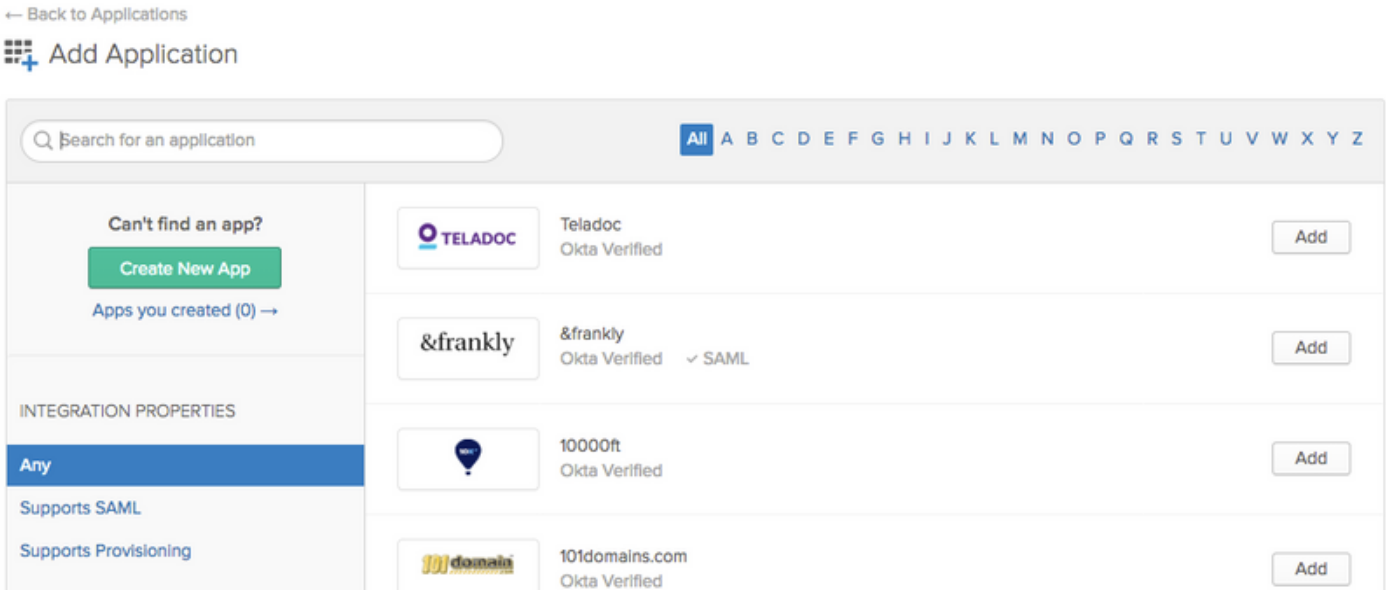
这是现在的门户流。



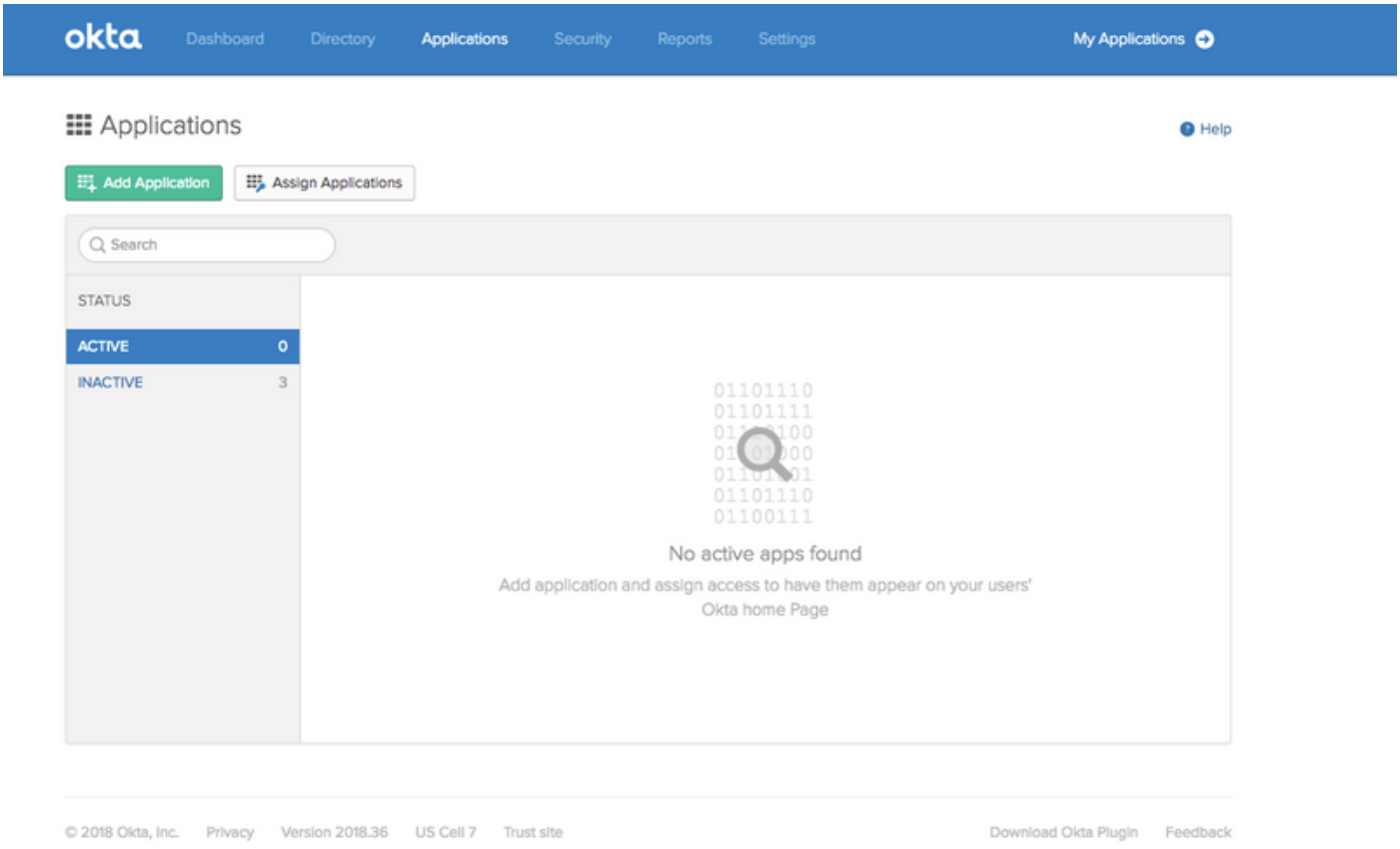
步骤2.配置OKTA应用和SAML身份提供程序设置。

1.创建OKTA应用程序。

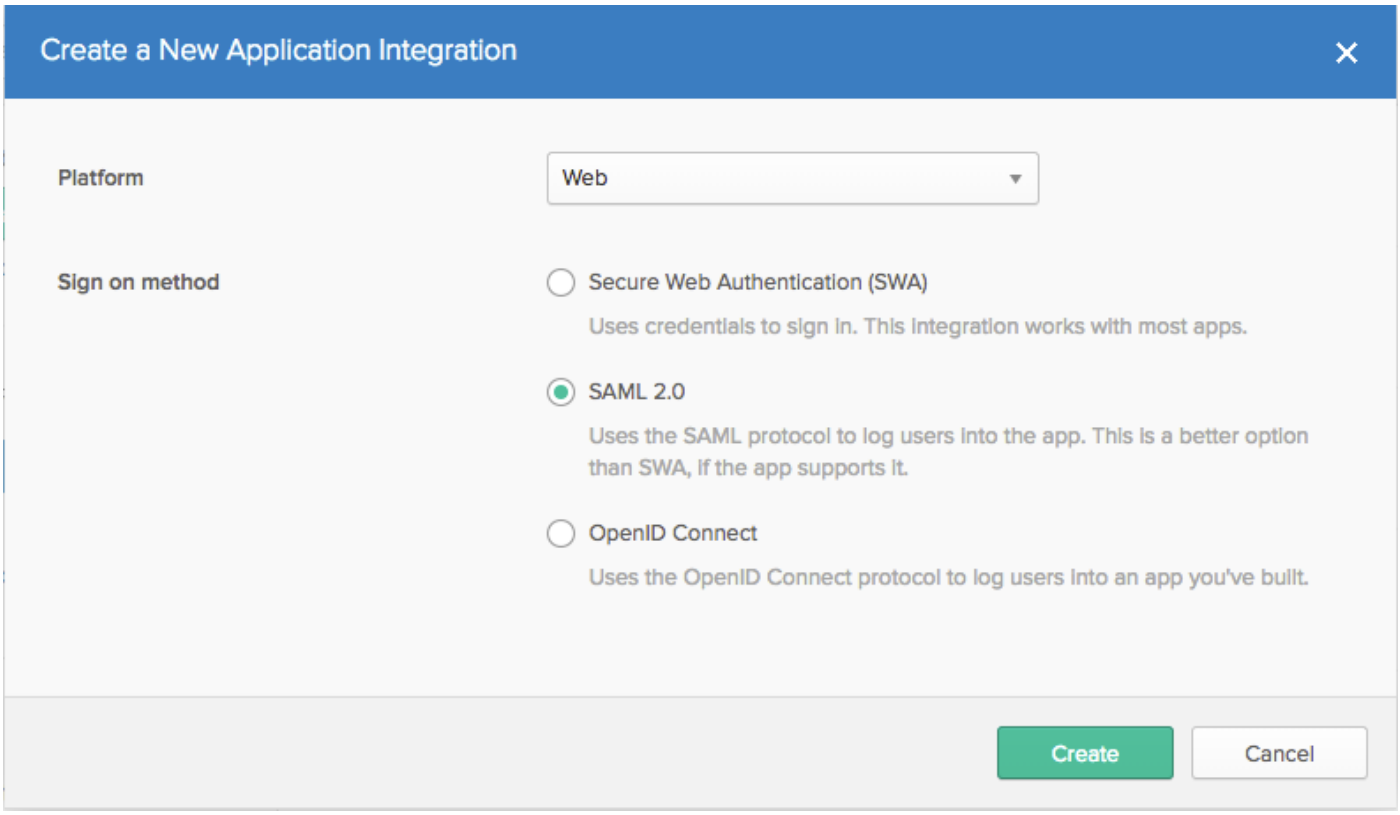
步骤1.使用管理员帐户登录OKTA网站。



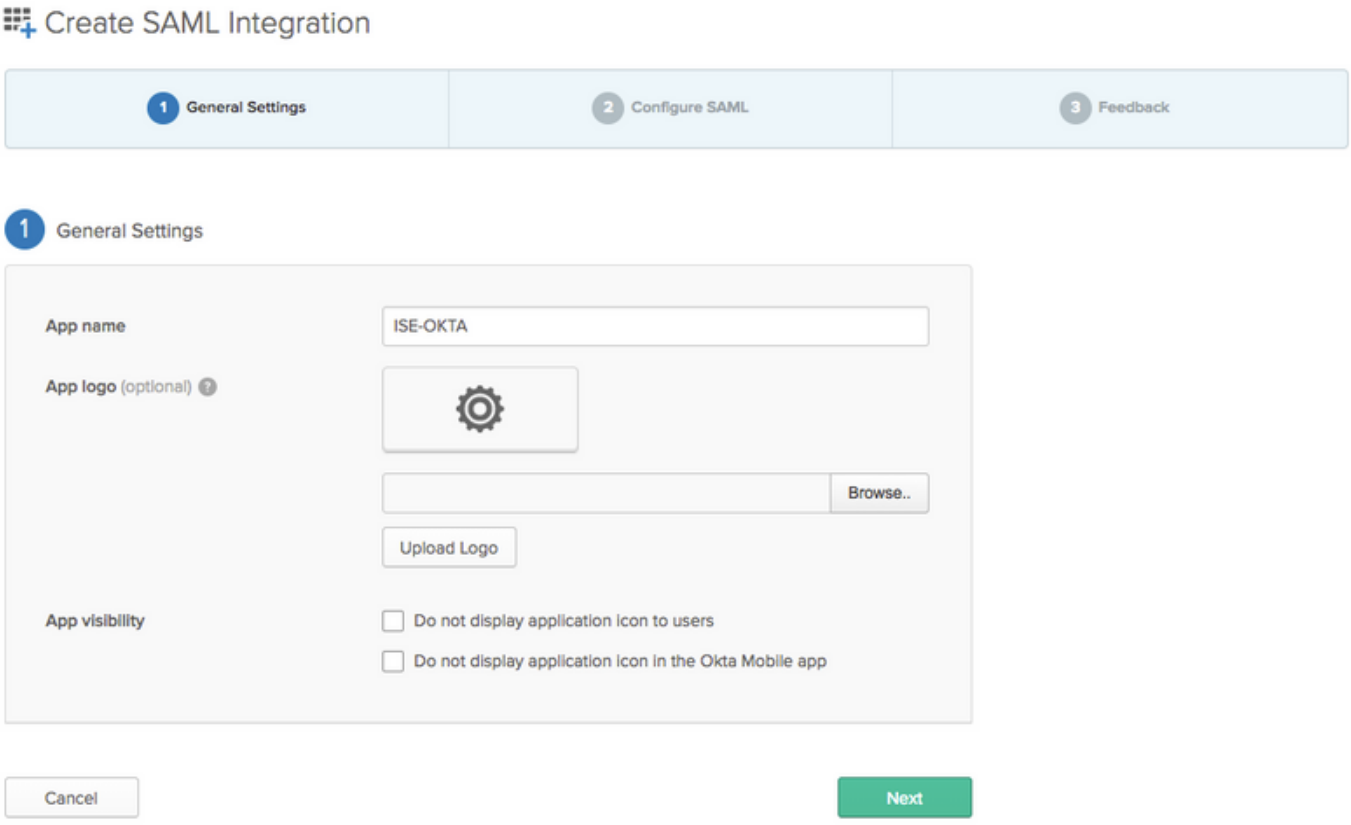
步骤2.点击Add Application。

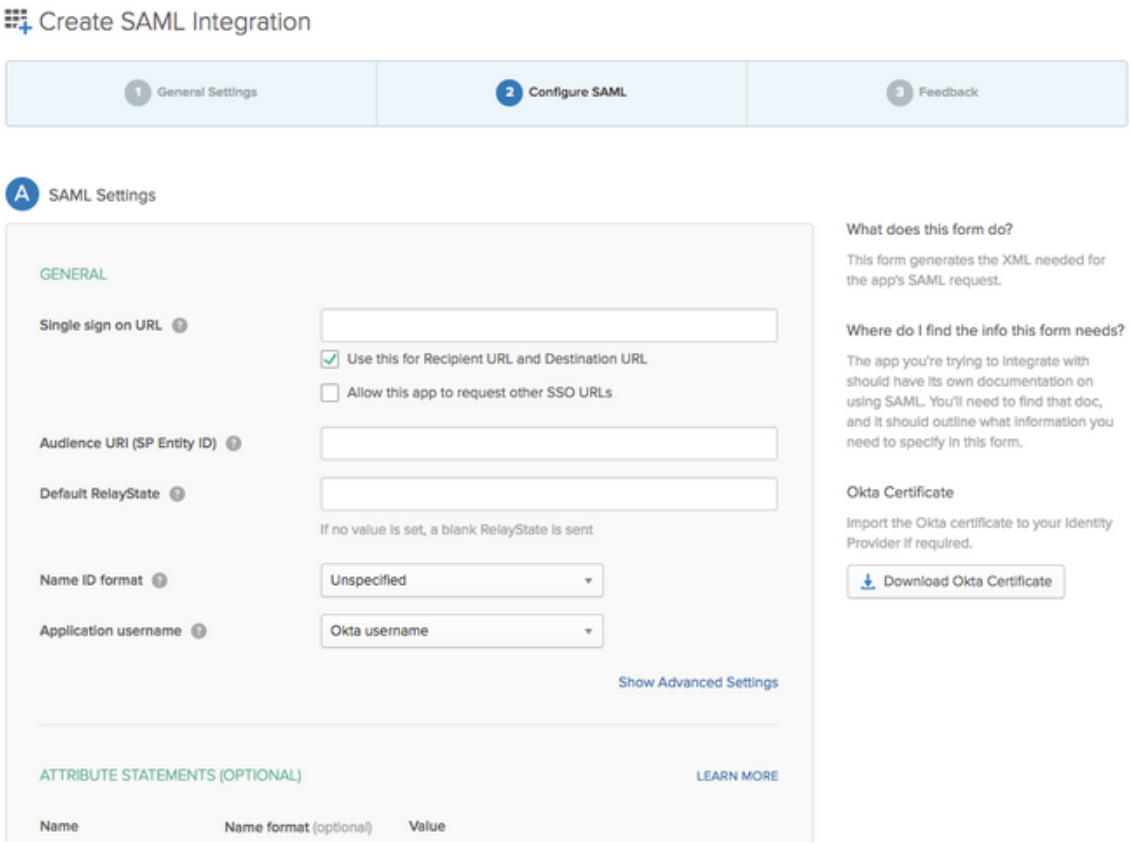


步骤3.创建新应用，选择为SAML2.0

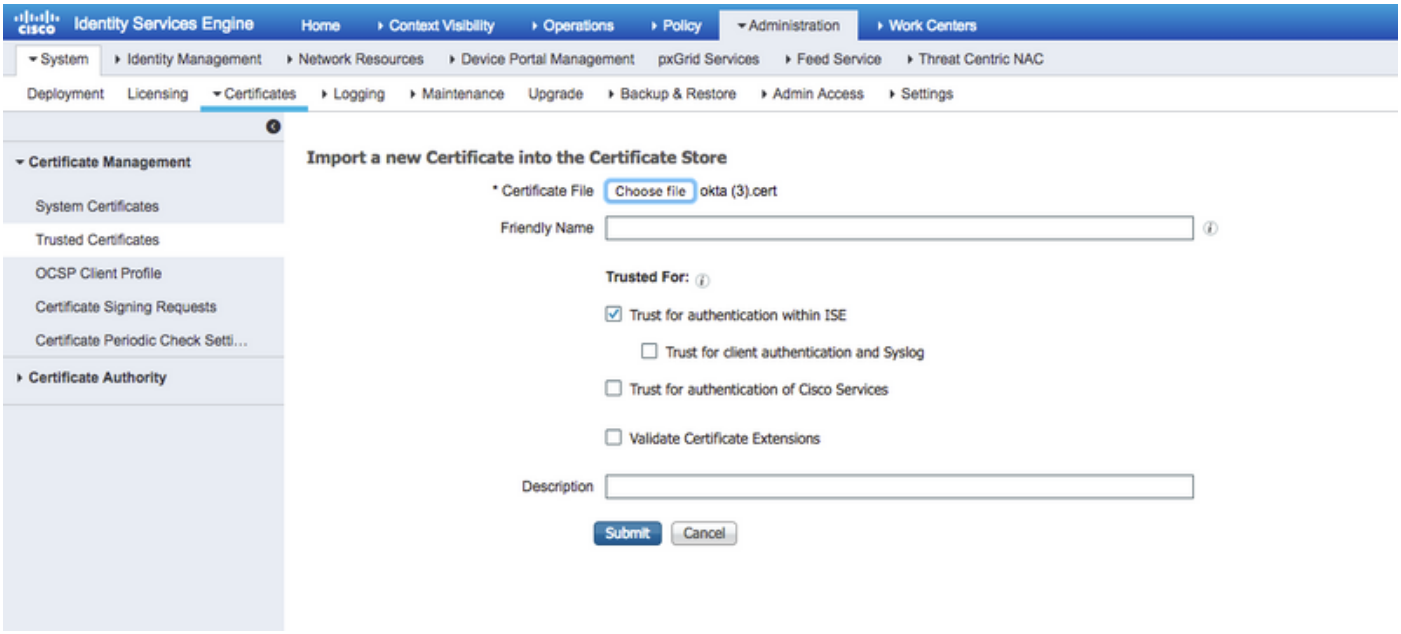

Create a New Application Integration
Platform
Web
Sign on method
Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
OpenID Connect
Uses 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

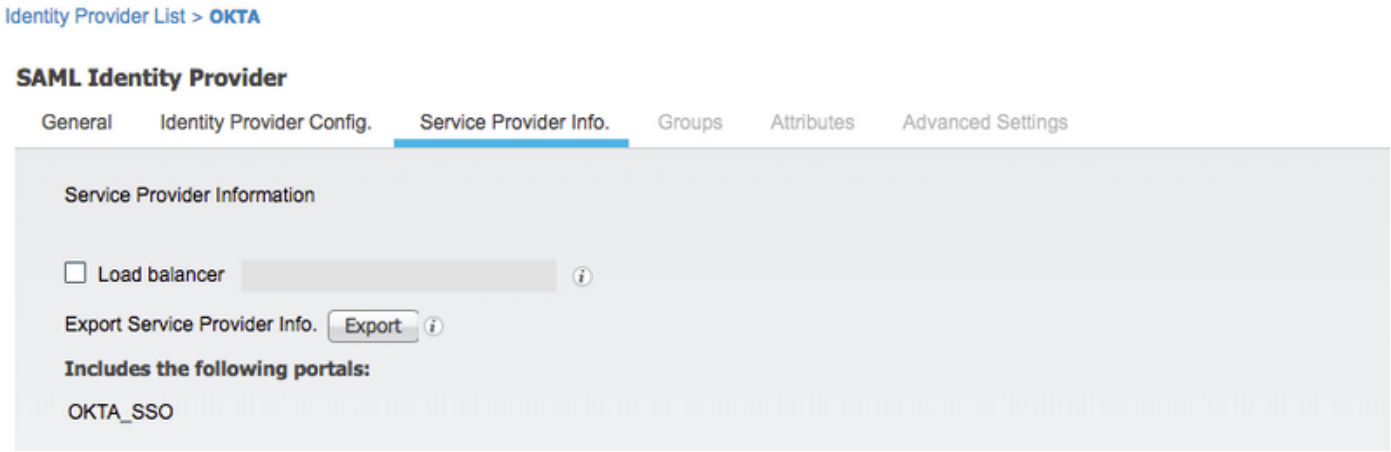


步骤4.下载证书并将其安装在ISE受信任证书中。



2.从SAML身份提供程序导出SP信息。

导航到之前配置的身份提供程序。单击Service Provider Info并将其导出，如图所示。



导出的zip文件夹包含XML文件和readme.txt



对于某些Identity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XML。

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

- SP实体Id

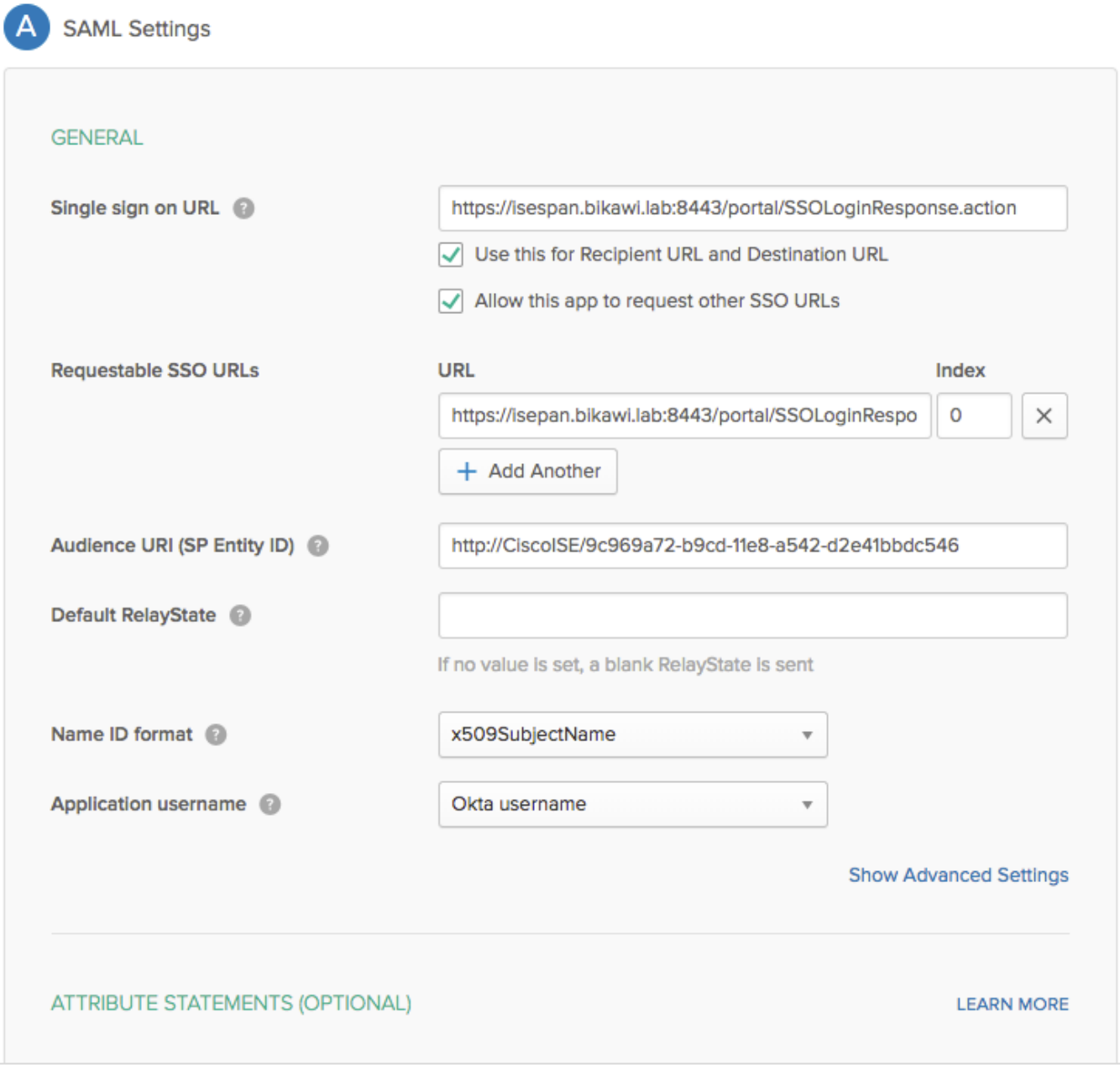
```
entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"
```

以IP地址和FQDN格式提供的SSO URL。

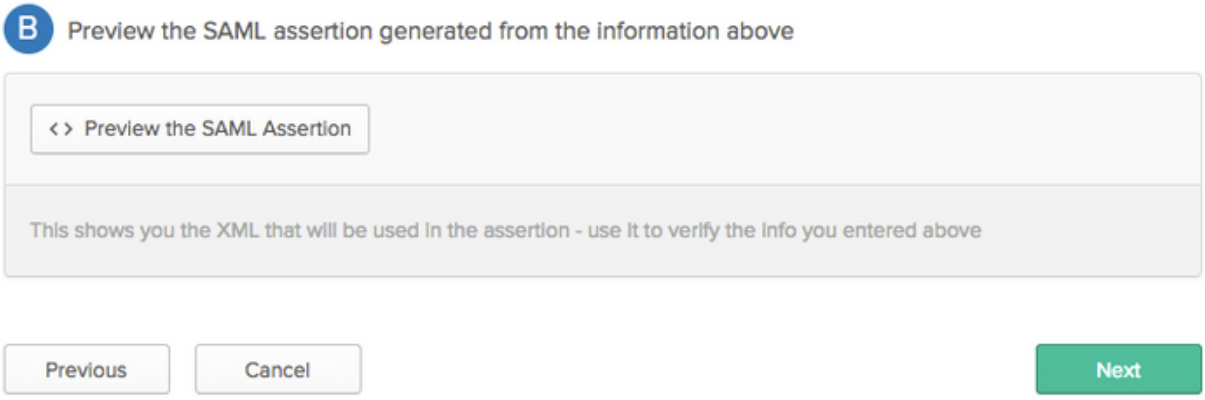
⚠ 警告：格式选择取决于授权配置文件上的重定向设置，如果使用静态ip，则应使用SSO URL的ip地址。

3. OKTA SAML设置。

步骤1.在SAML设置中添加这些URL。

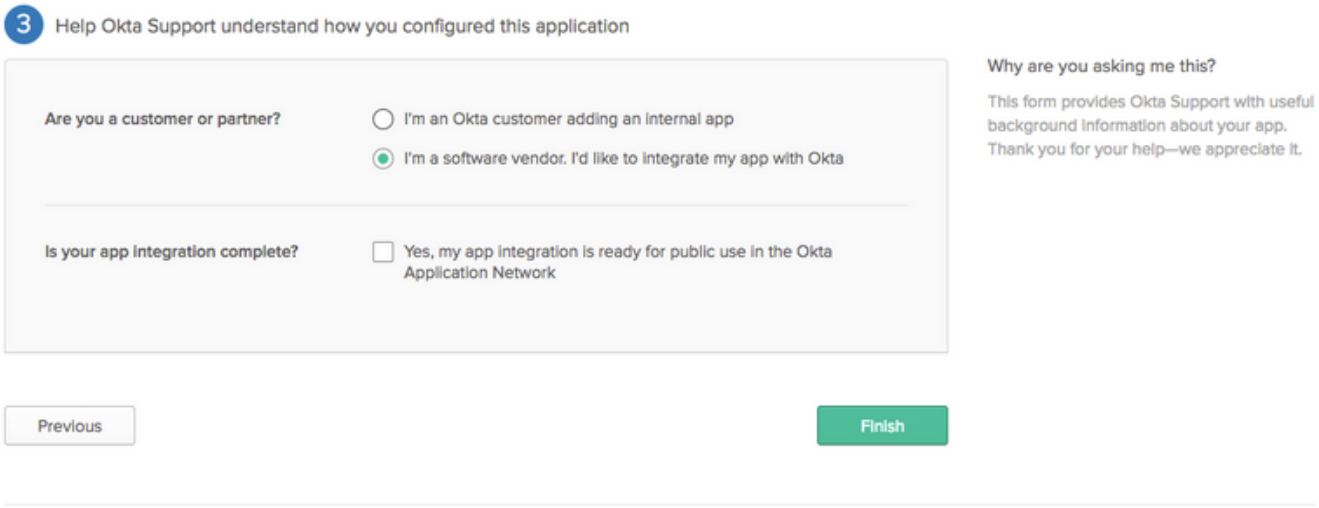


步骤2.您可以根据托管此服务的PSN的数量，从XML文件中添加多个URL。名称ID格式和应用用户名取决于您的设计。

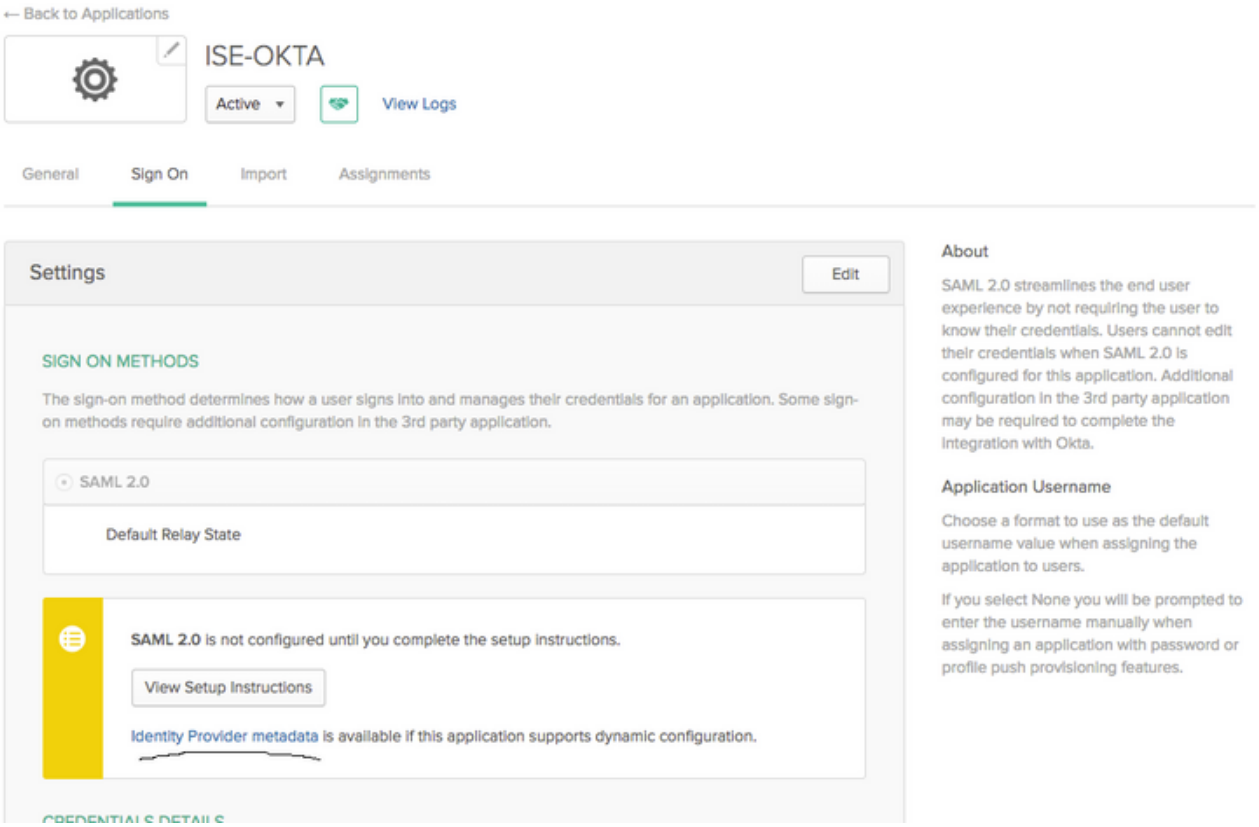



```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124" IssueInstant=
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://www.okta.com/Issuer<
    <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName">userName</saml
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2018-09-21T15:52:03.823Z" Recipient="https://i
        </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:PasswordProtectedTranspo
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
</saml2:Assertion>
```

步骤3.单击“下一步”并选择第二个选项。



4.从应用程序导出元数据。



元数据：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk1
<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAM
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIDrDCCApSgAwIBAgIGAWWPlTasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMB
</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://cisc
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

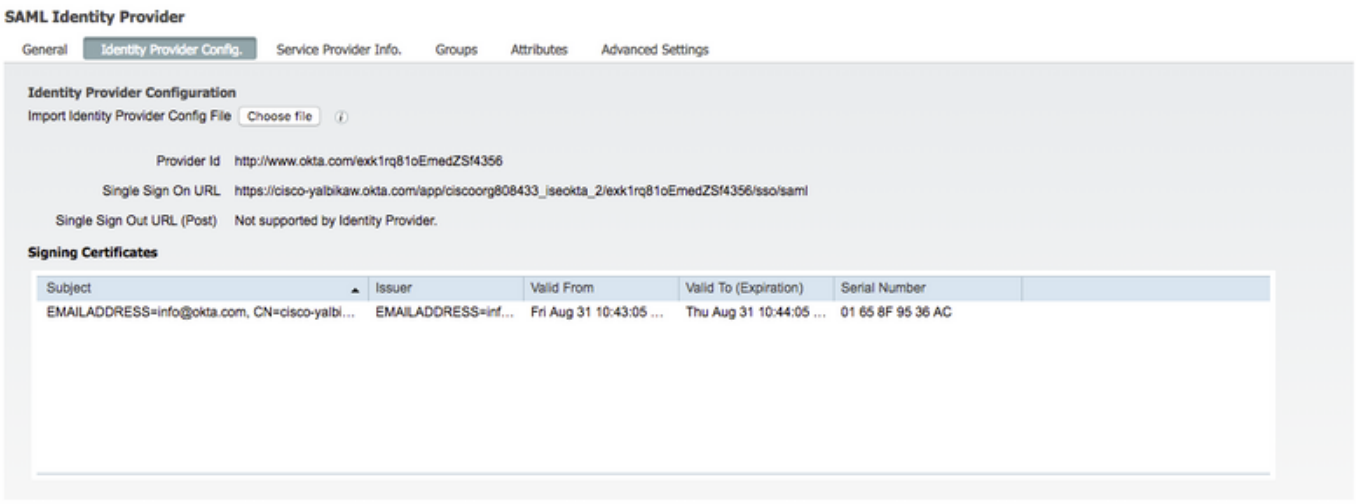
以XML格式保存文件。

5.将用户分配给应用程序。

将用户分配给此应用程序，有一个进行AD集成的方法，如中所述：OKTA活动目录

6.将元数据从Idp导入ISE。

步骤1.在SAML Identity Provider下，选择Identity Provider Config.和Import Metadata。



步骤2.保存配置。

步骤3.CWA配置。

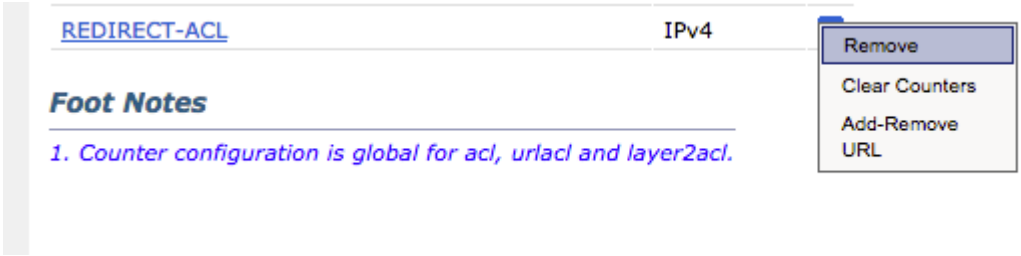
本文档介绍ISE和WLC的配置。

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。

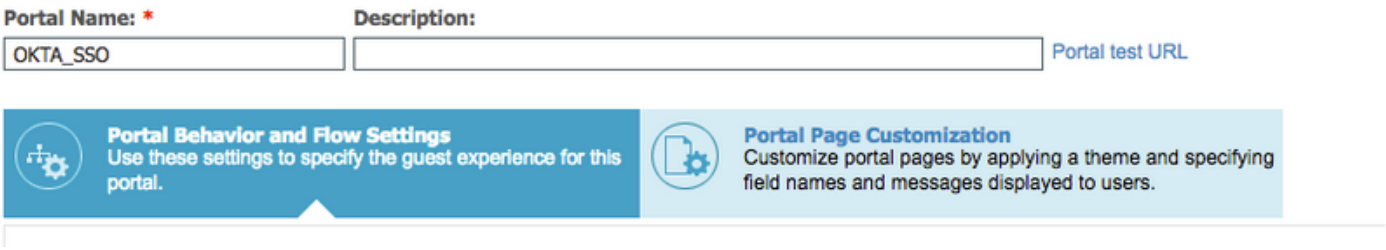
https://cisco-yalbikaw.okta.com /添加您的应用URL

https://login.okta.com

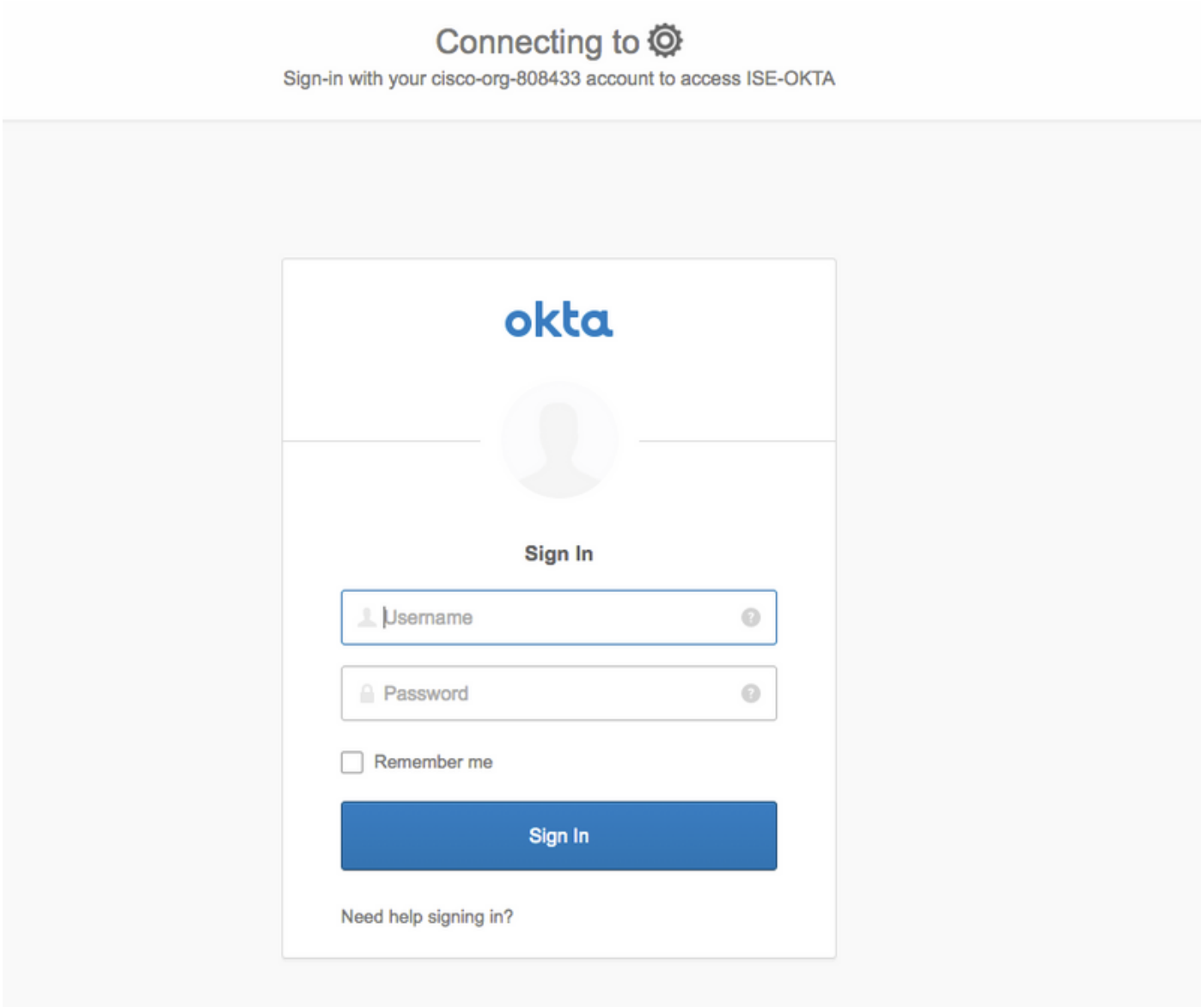


验证

测试门户并验证您是否能够访问OKTA应用



步骤1.点击门户测试，然后您应该被重定向到SSO应用。

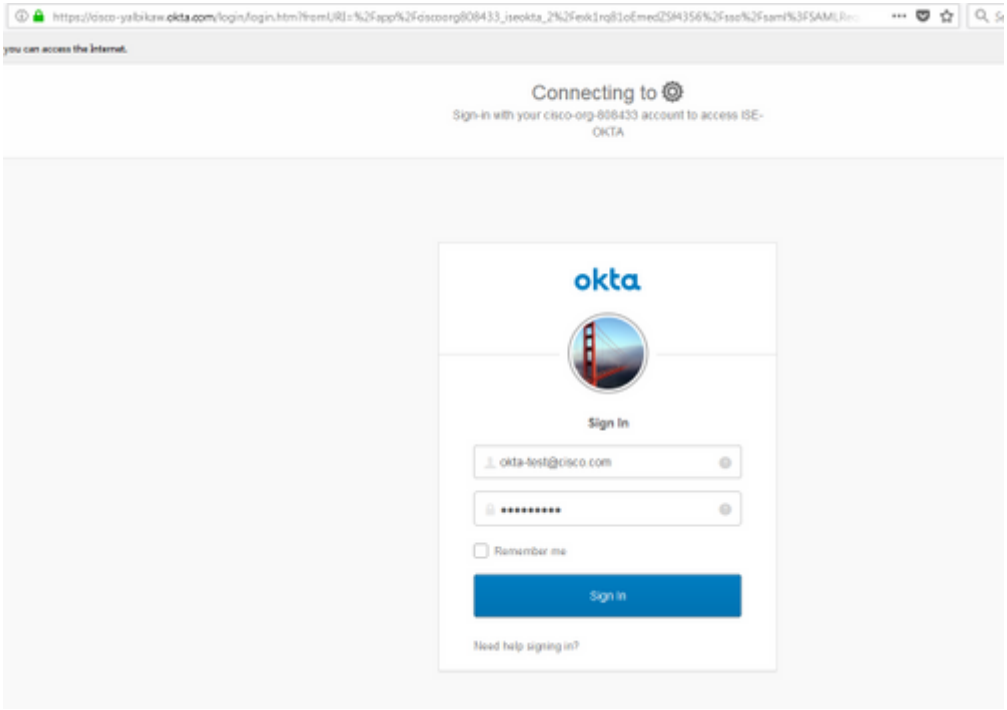


步骤2.检查与<application name>的信息连接

步骤3.如果您输入可能看到错误的saml请求的凭证，这并不意味着此时配置错误。

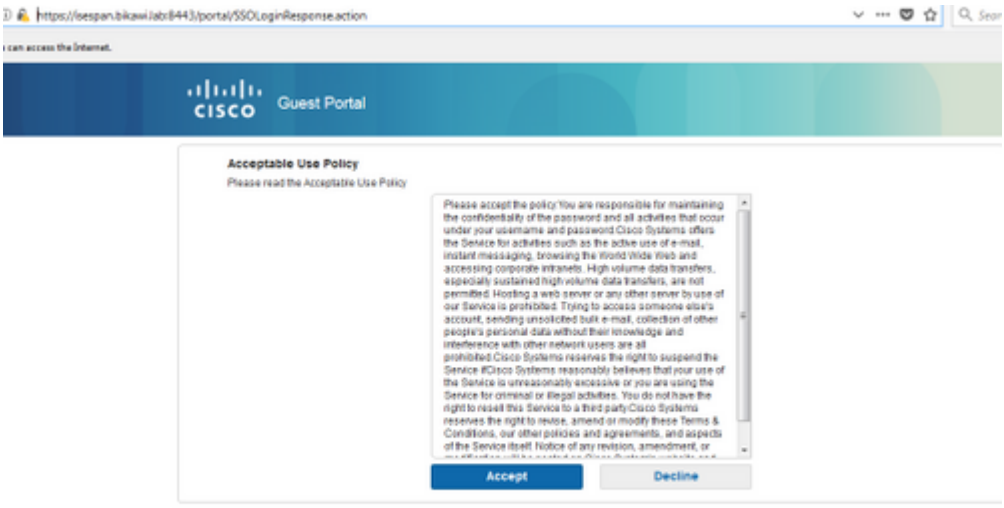
最终用户验证

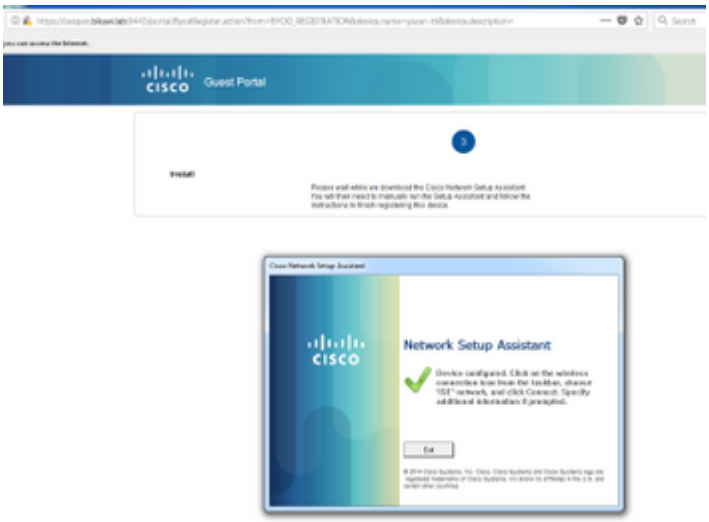






Signing in to ISE-OKTA





ISE验证

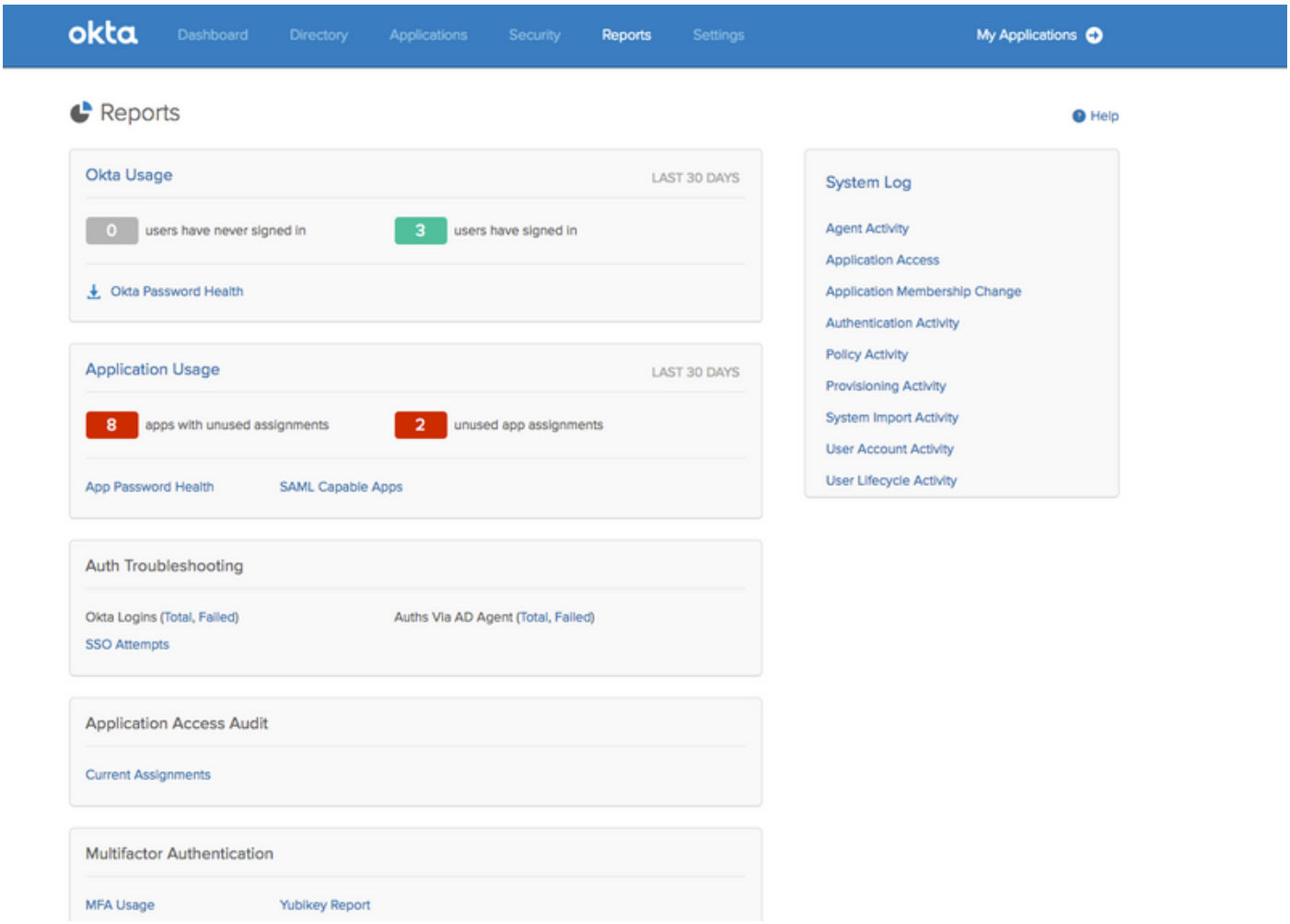
检查生命日志以验证身份验证状态。



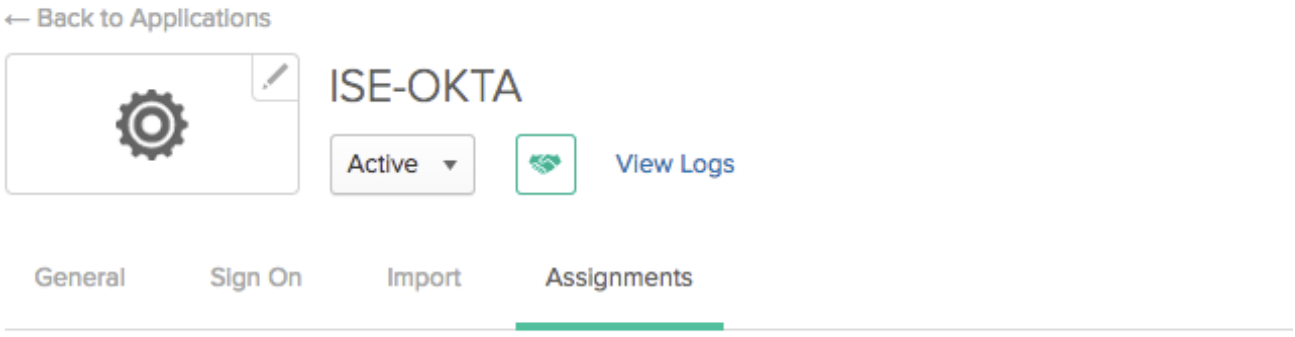
故障排除

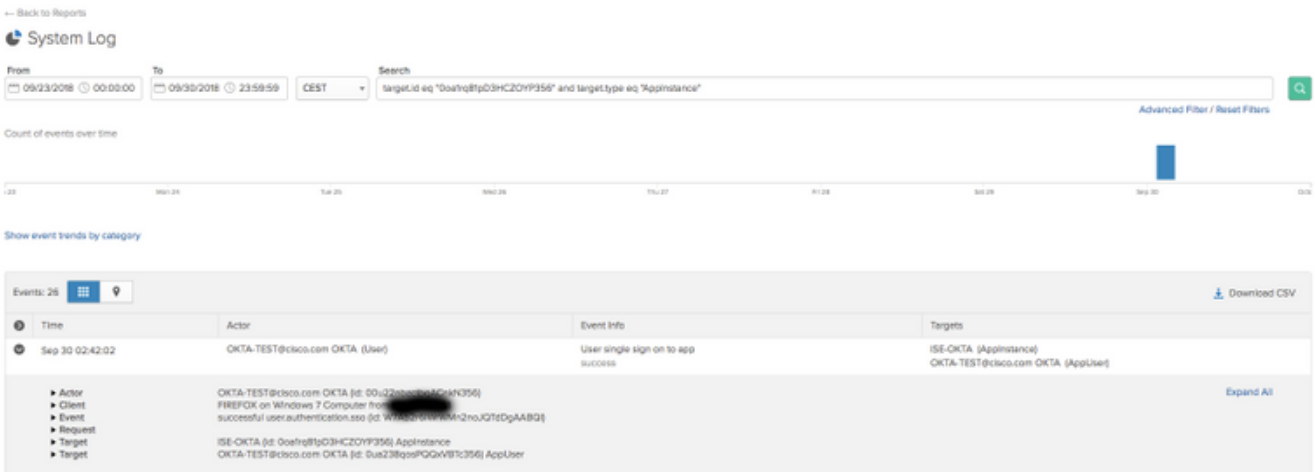
OKTA故障排除

步骤1.检查Reports选项卡中的日志。



步骤2.也从应用程序查看相关日志。





ISE故障排除

有两个要检查的日志文件

- ise-psc.log
- guest.log

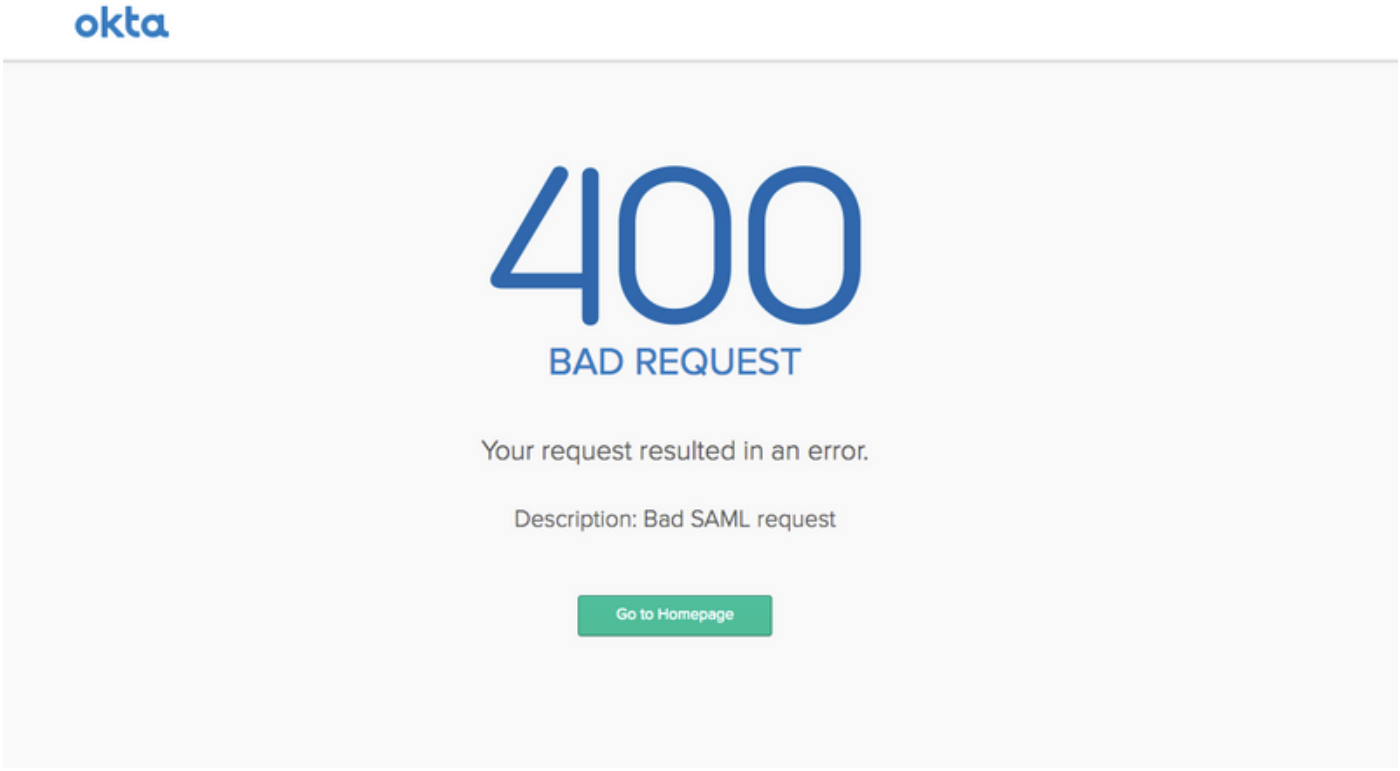
导航到Administration > System > Logging > Debug Log Configuration。启用级别DEBUG。

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

该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.错误的SAML请求。



此错误是一般性的，请检查日志以验证流并查明问题。在ISE guest.log上：

ISE# show logging application guest.log |最后50个

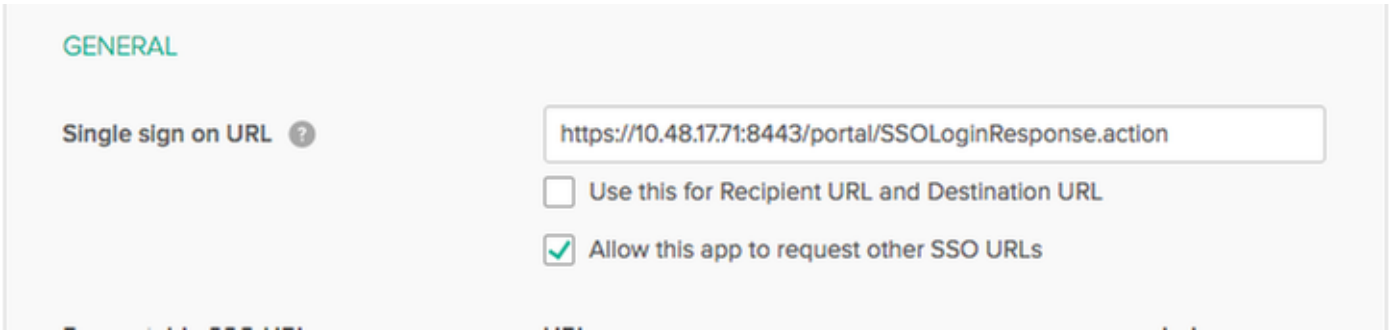
```
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont

        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.cont
onId=0a3e949b000002c55bb023b3;
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEfl
HO4QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3ugJMm%2B
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnCh3jFo72
alId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.util
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJOOb4672D
1CPwo1hGtcFepS3HZF3pzSHO4QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq
1bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
2018-09-30 01:32:35,627 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.cont
```

ISE已成功将用户重定向到IDP。但是，没有响应ISE并显示错误的SAML请求。确定OKTA不接受下面我们的SAML请求是请求。

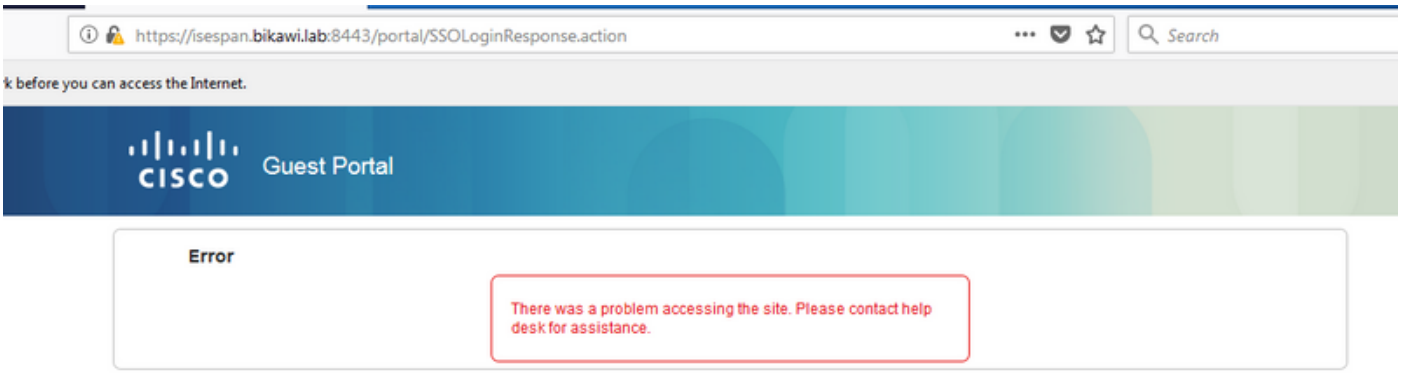
```
https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEf
HO4QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3ugJMm%2B
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnCh3jFo72
alId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83
```

现在再次检查应用程序，可能进行了更改。



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

场景2. “访问站点时出现问题。如需帮助，请与技术支持联系”。



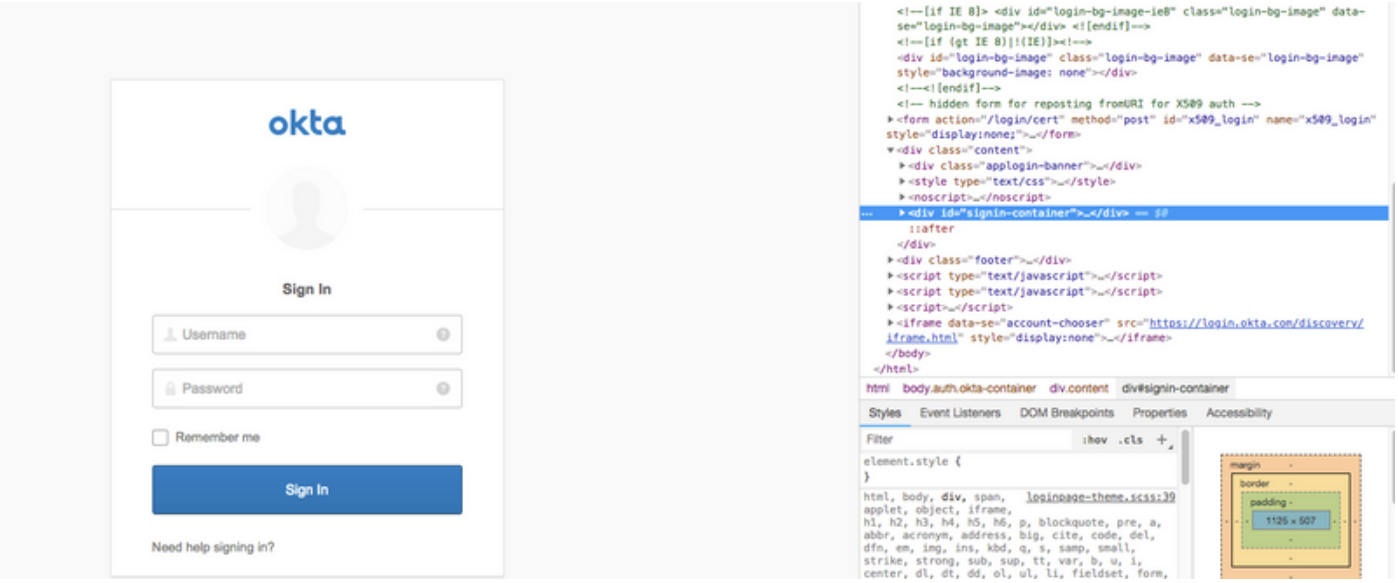
Guest.log

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

从日志中，ISE报告断言不正确。检查OKTA受众URI，确保它与SP匹配以解决此问题。

场景3.已重定向至“空白”页面，或者未显示登录选项。

这取决于环境和门户配置。在此类问题中，您需要检查OKTA应用以及进行身份验证所需的URL。点击门户测试，然后检查元素，检查哪些网站必须可访问。



在此场景中，只有两个URL:application和login.okta.com — 应允许在WLC上使用这些应用。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。