使用OKTA SAML SSO配置ISE 2.3访客门户

目录

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。

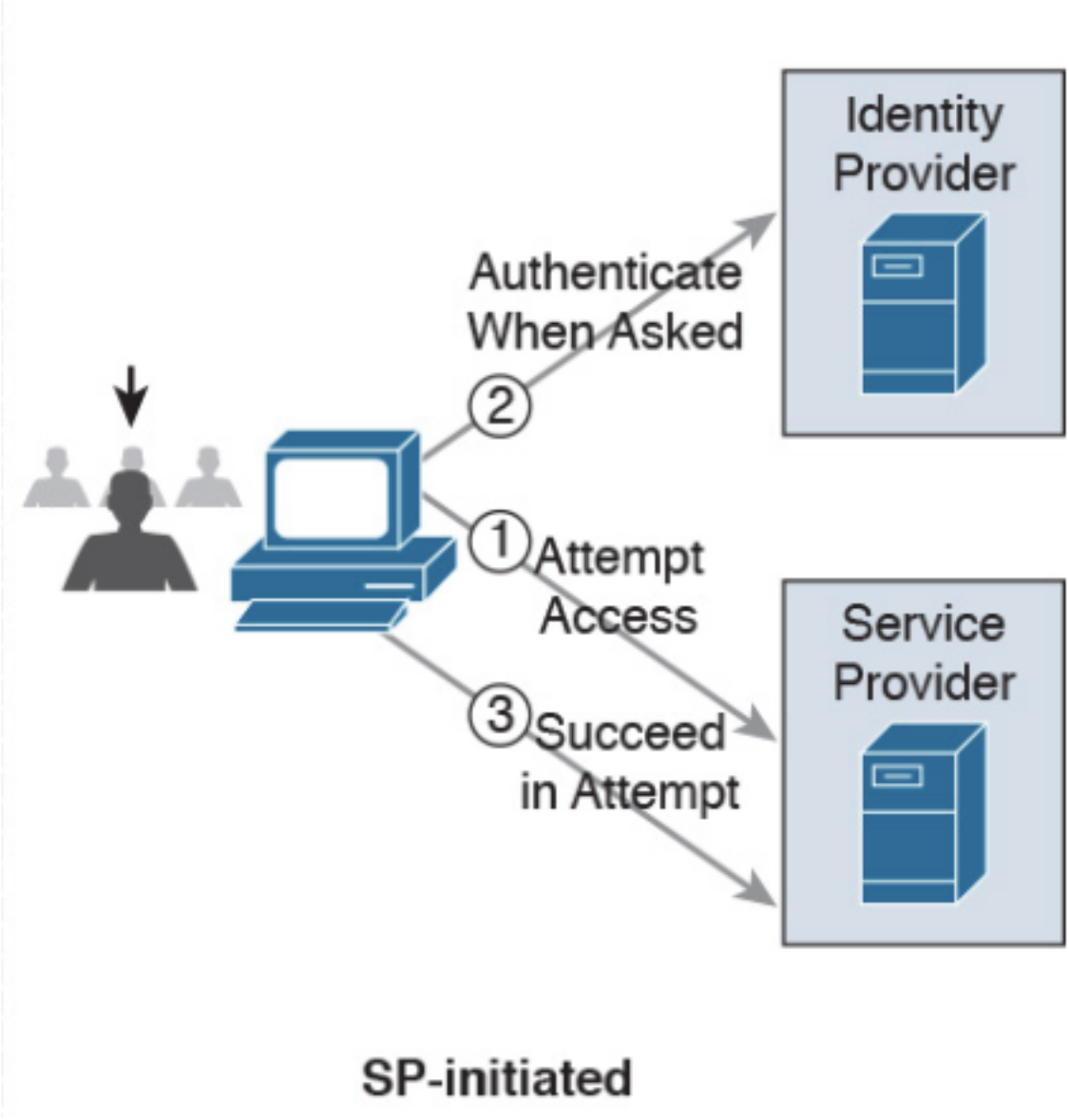
联合的概念：

- 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。

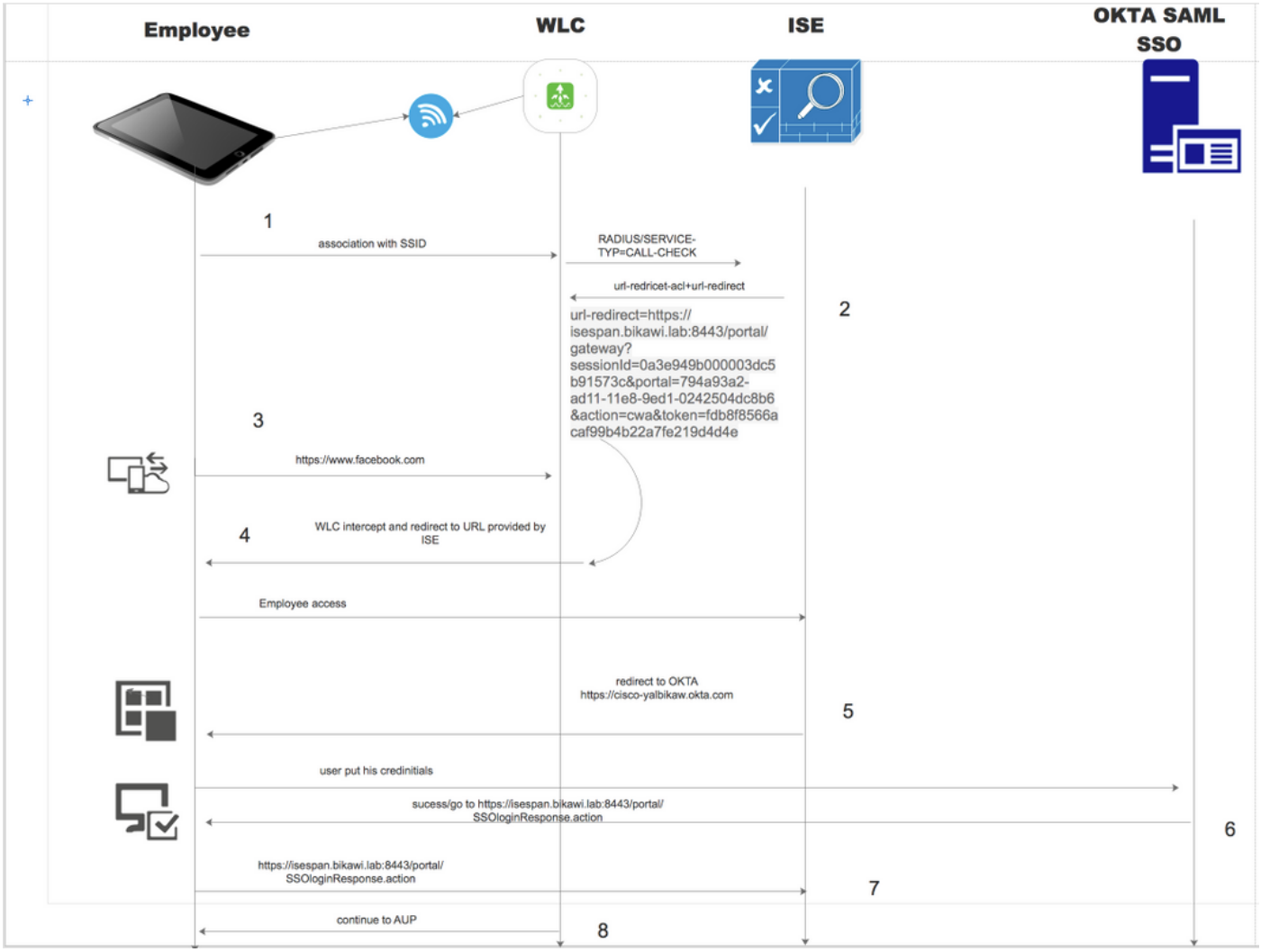
多种协议实施SSO，如OAuth2和OpenID。ISE使用SAML。

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。


Identity Provider
Authenticate When Asked
2
1 Attempt Access
3 Succeed in Attempt
Service Provider
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。
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

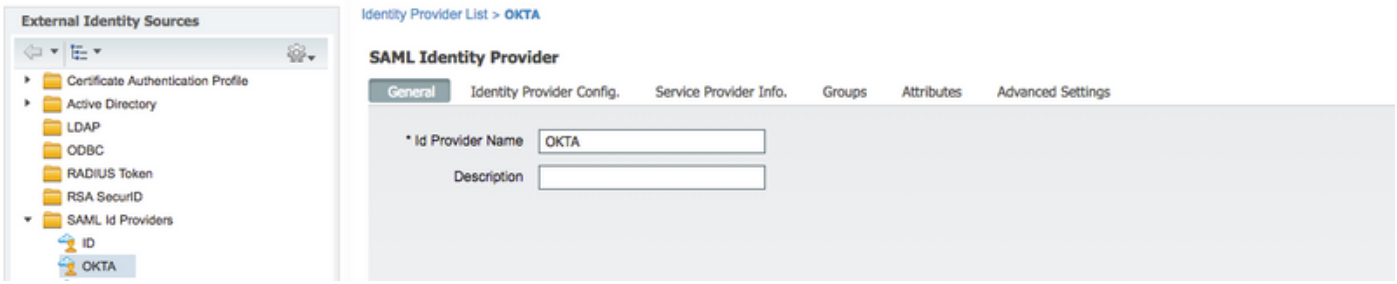
https://developer.okta.com/standards/SAML/

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。

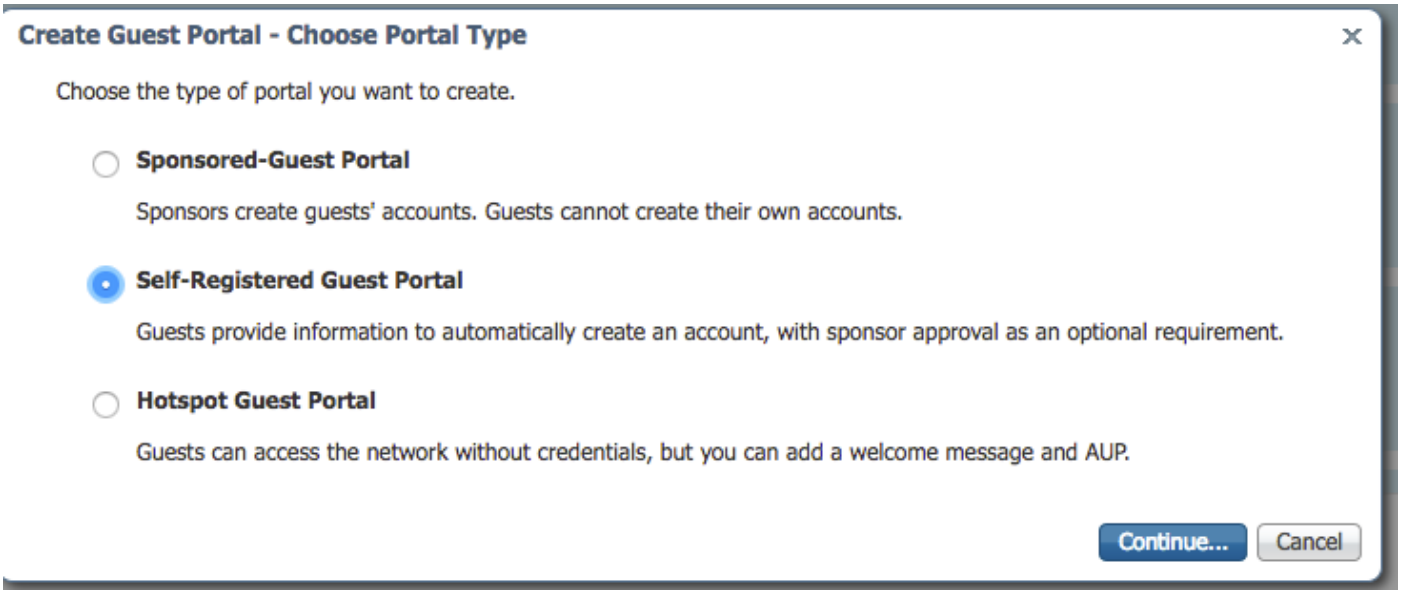


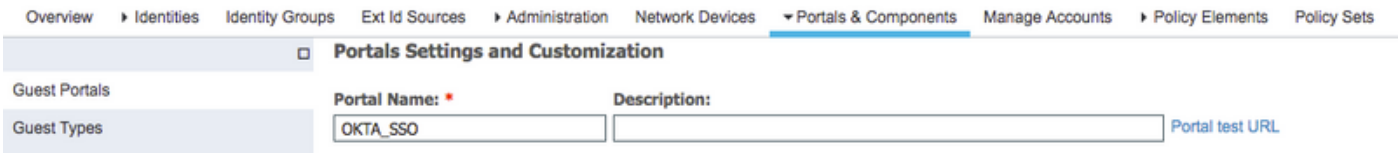
步骤2.为ID提供程序分配名称并提交配置。

2.创建SSO门户。

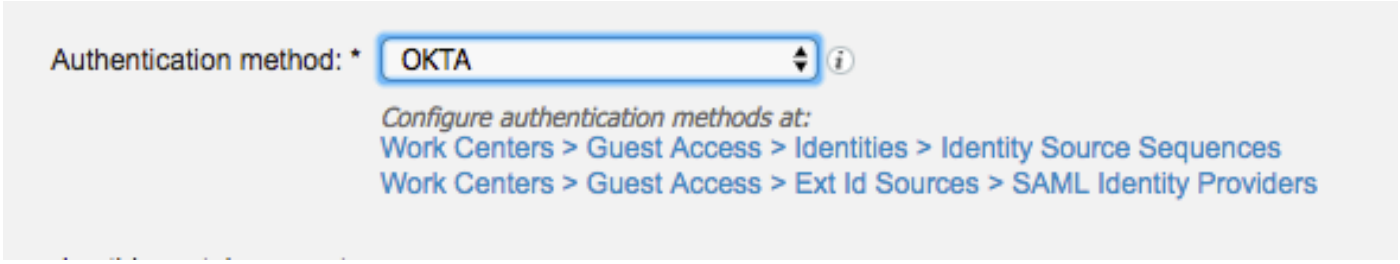
步骤1.创建分配给OKTA的门户作为身份源。BYOD、设备注册、访客等的任何其他配置与普通门户的配置完全相同。在本文档中，该门户映射到访客门户，作为员工的替代登录。

步骤2.导航至“工**作中心”>“访客访问”>“门户和组**件”并创建门户。



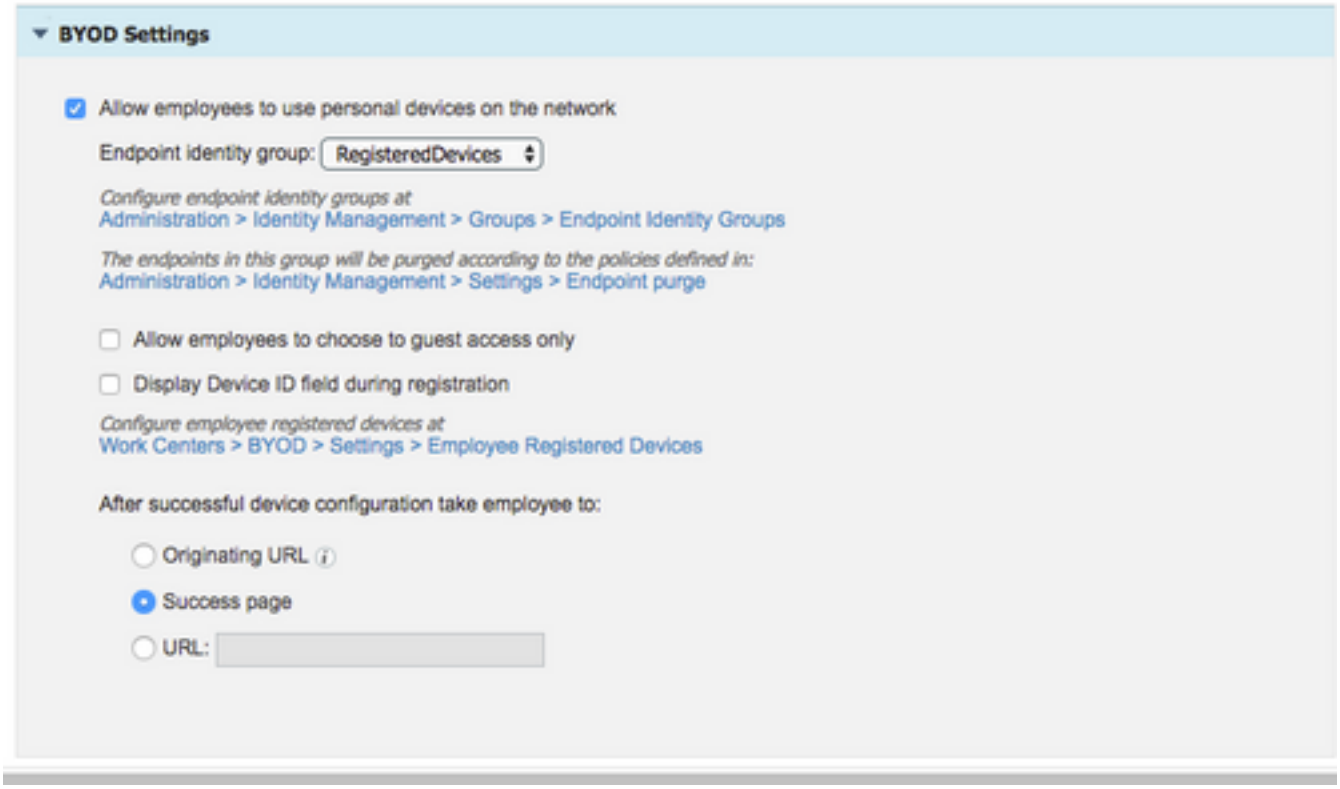


步骤3.选择身份验证方法以指向之前配置的身份提供程序。

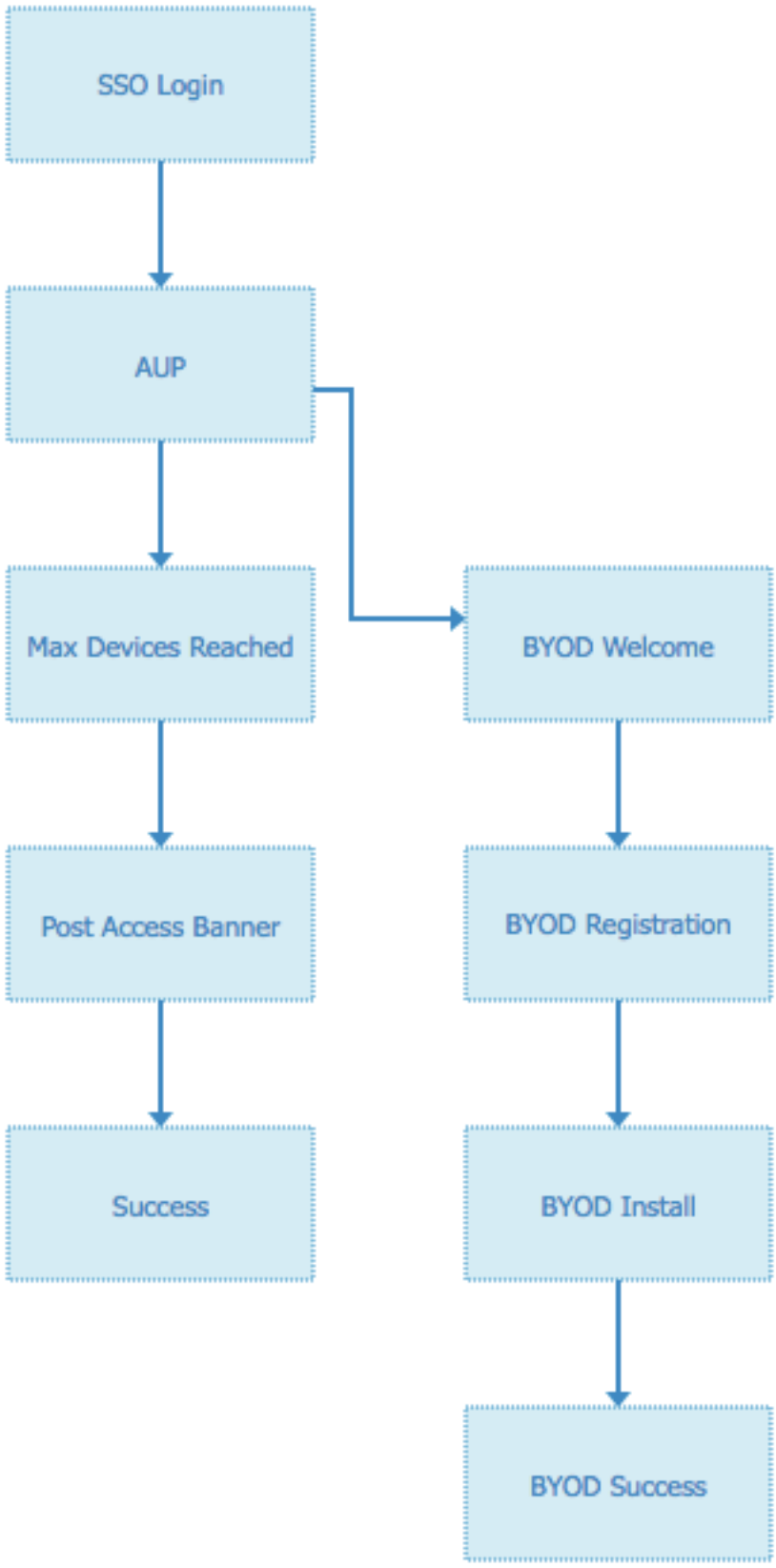


步骤4.选择OKTA身份源作为身份验证方法。

（可选）选择BYOD设置。



步骤5.保存门户配置，使用BYOD时，流程如下所示：

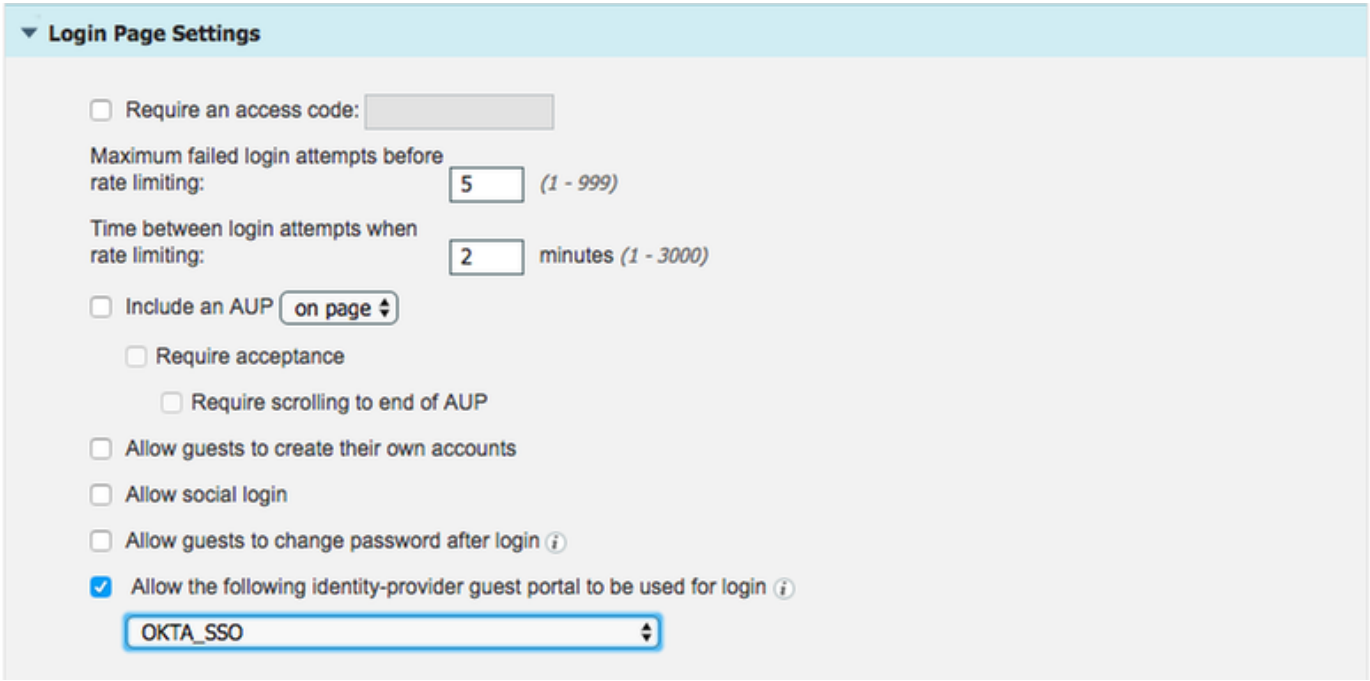


3.配置备用登录。

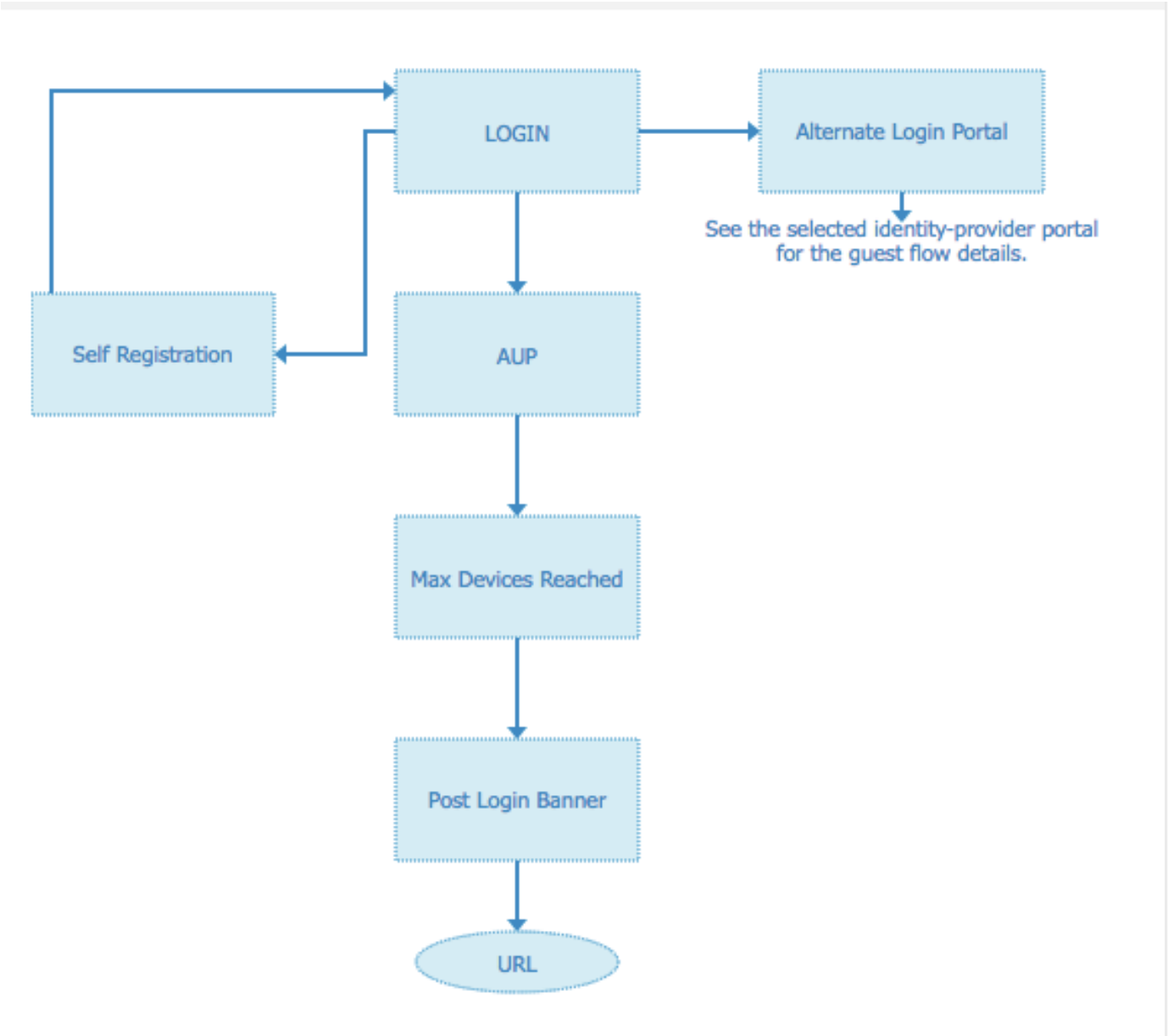
注意：如果不使用备用登录名，可跳过此部分。

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。



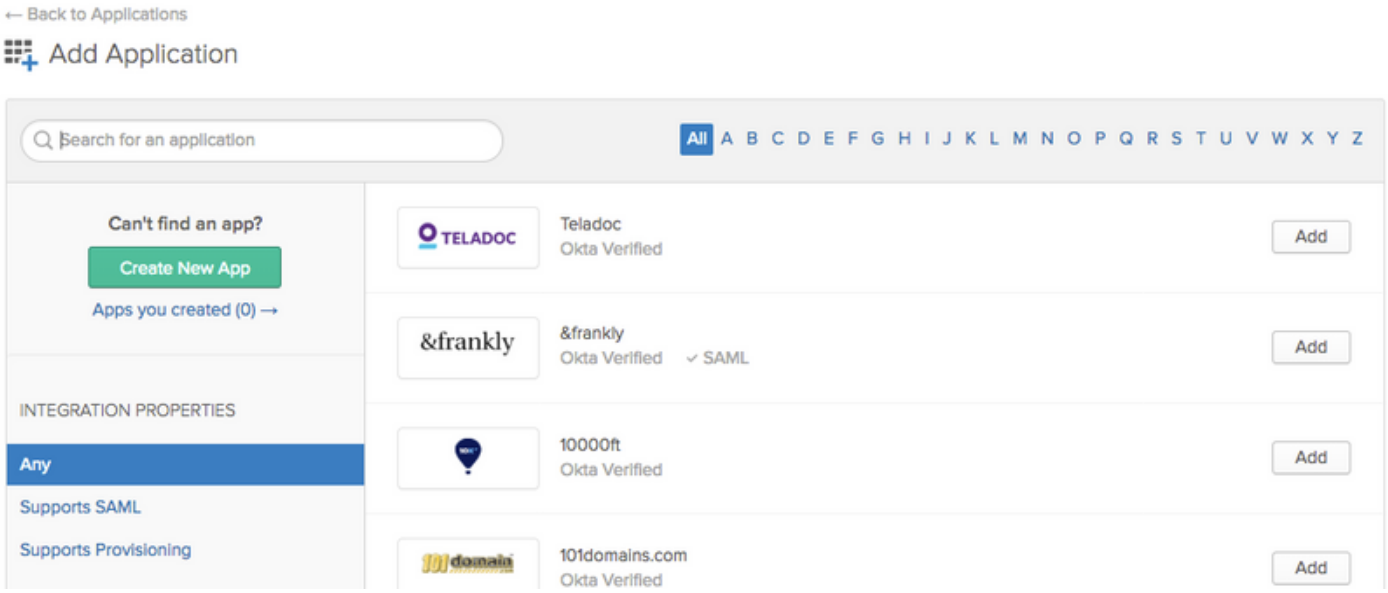
这是入口流。



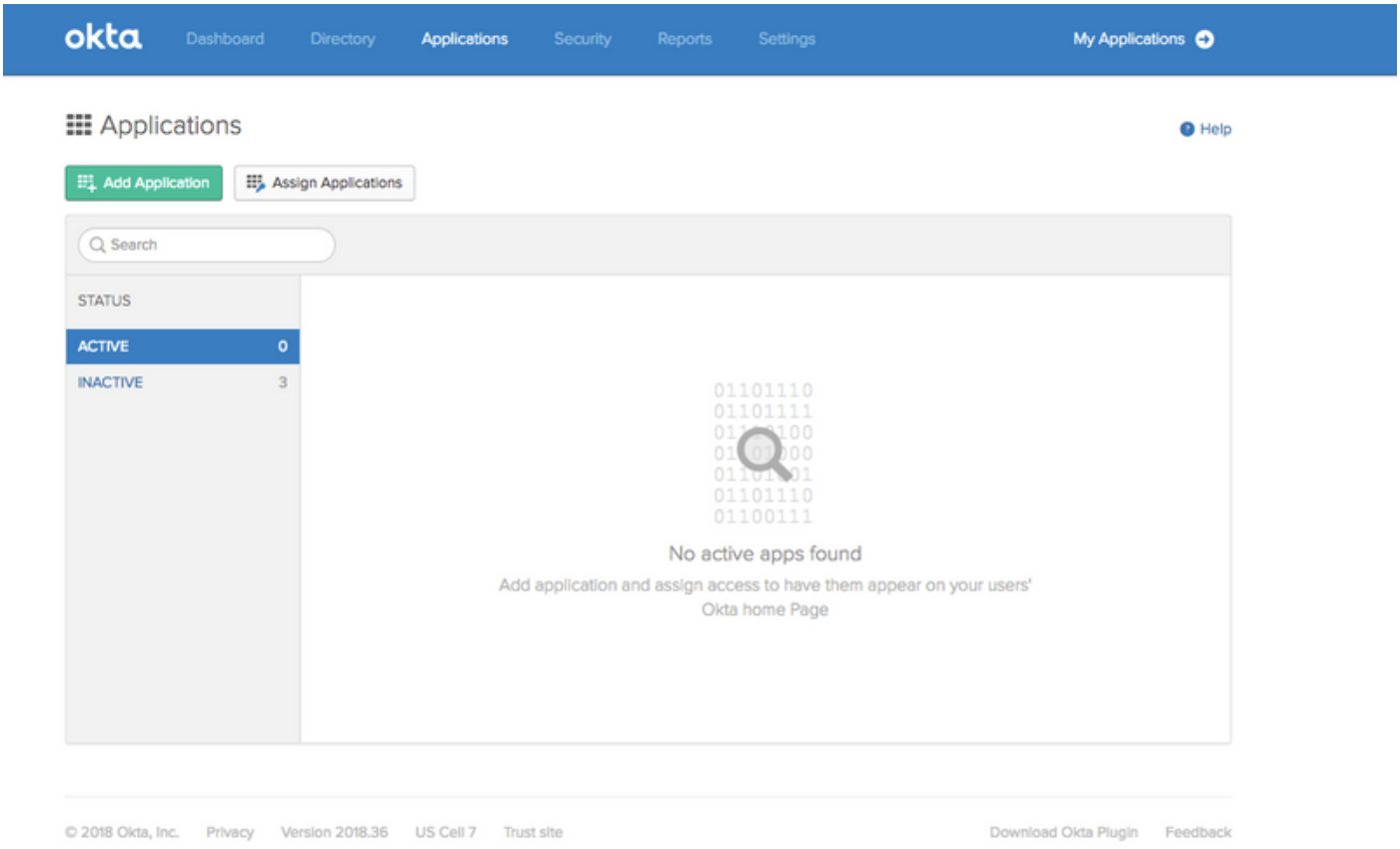
步骤2.配置OKTA应用和SAML身份提供程序设置。

1.创建OKTA应用程序。

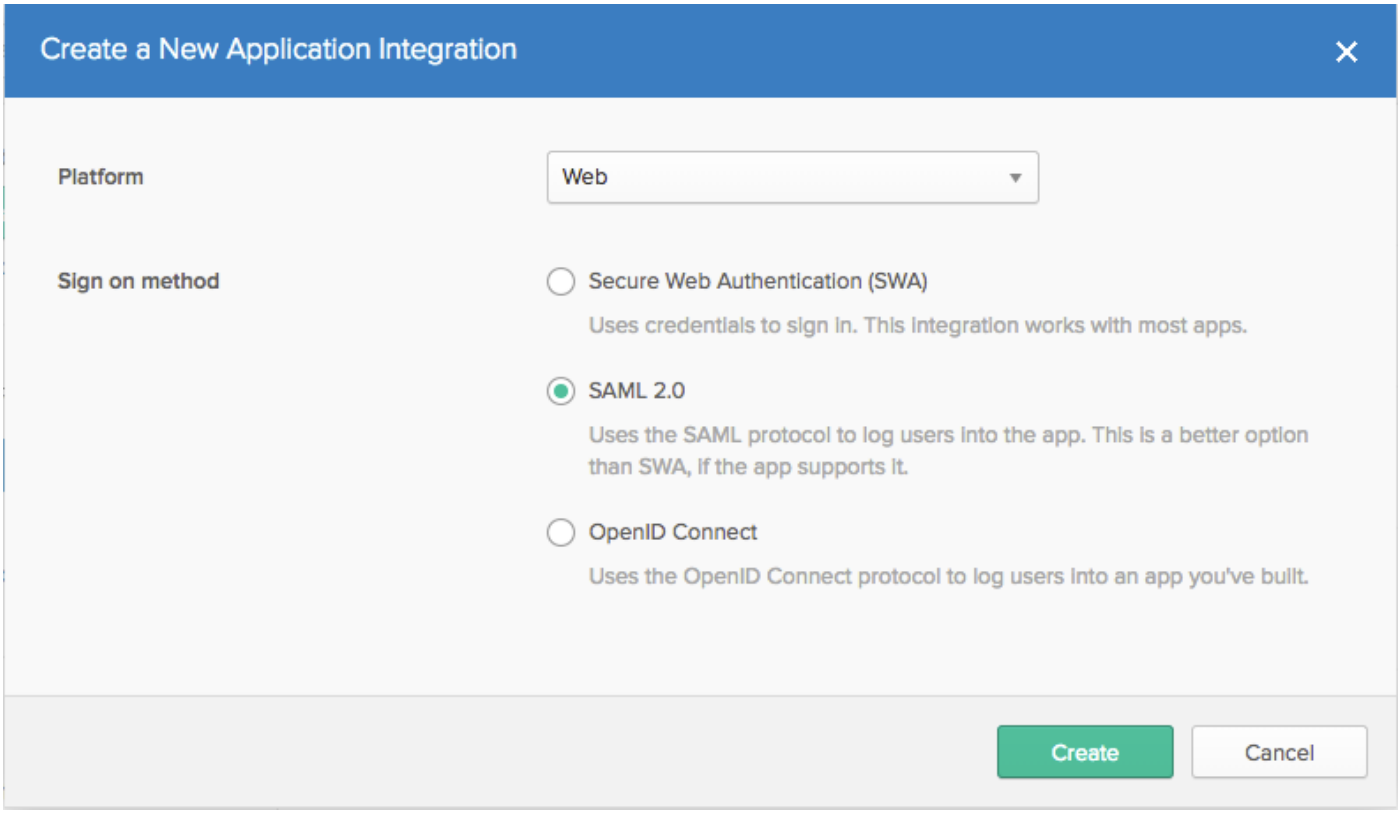
步骤1.使用管理员帐户登录OKTA网站。



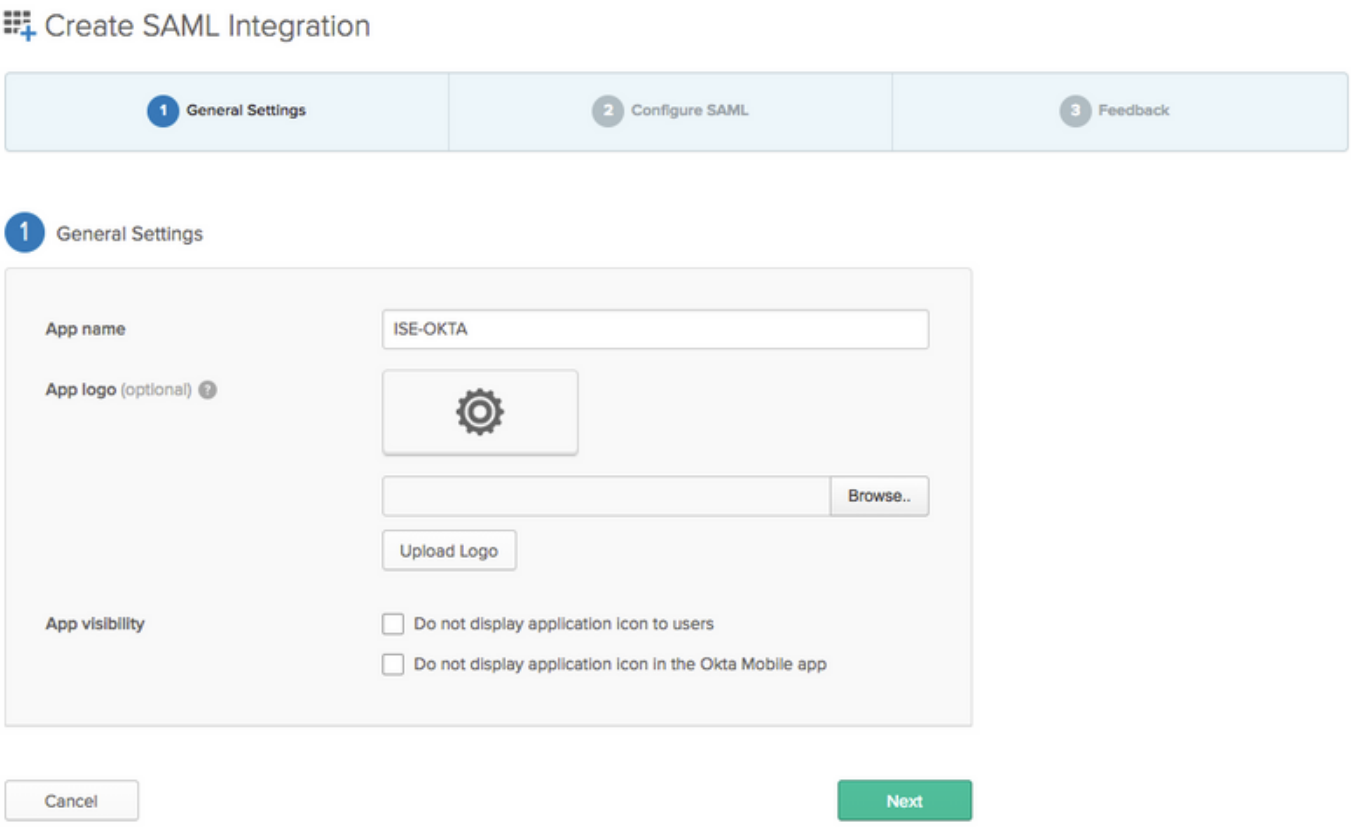
步骤2.点击Add Application。

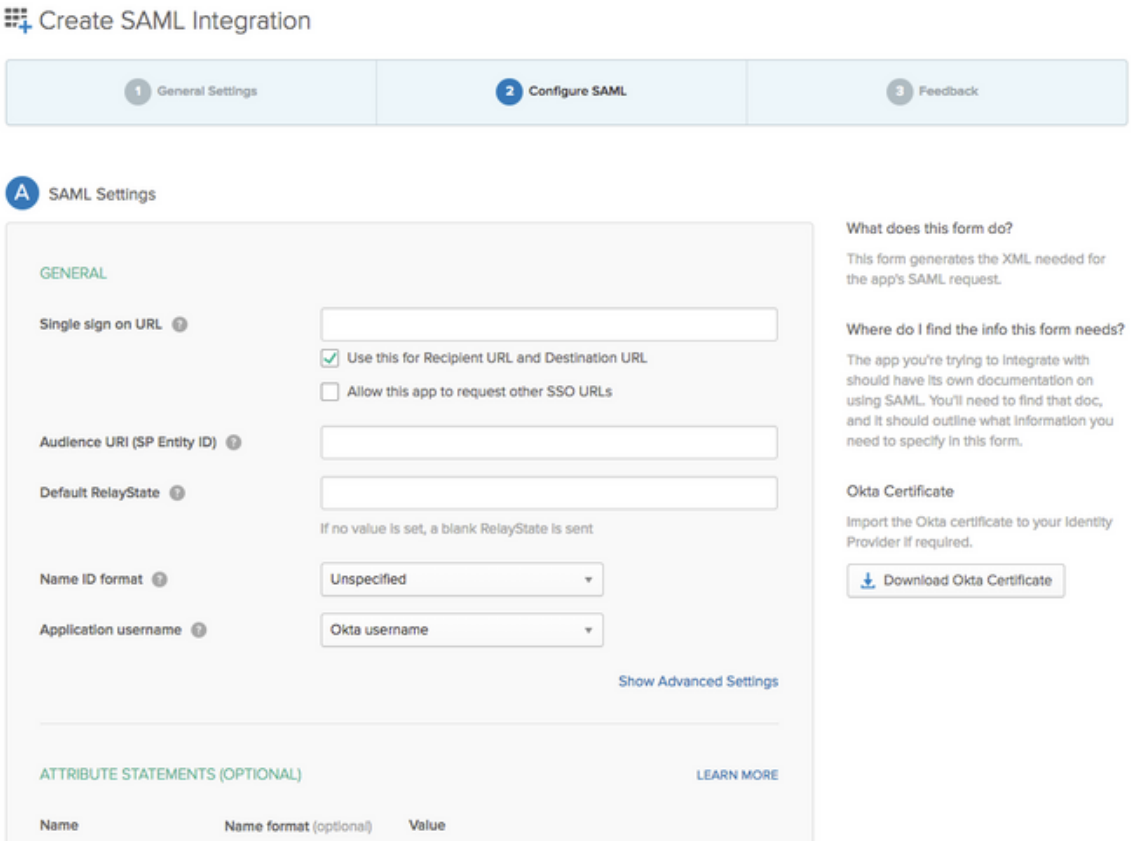


步骤3.创建新应用，将其选为SAML2.0

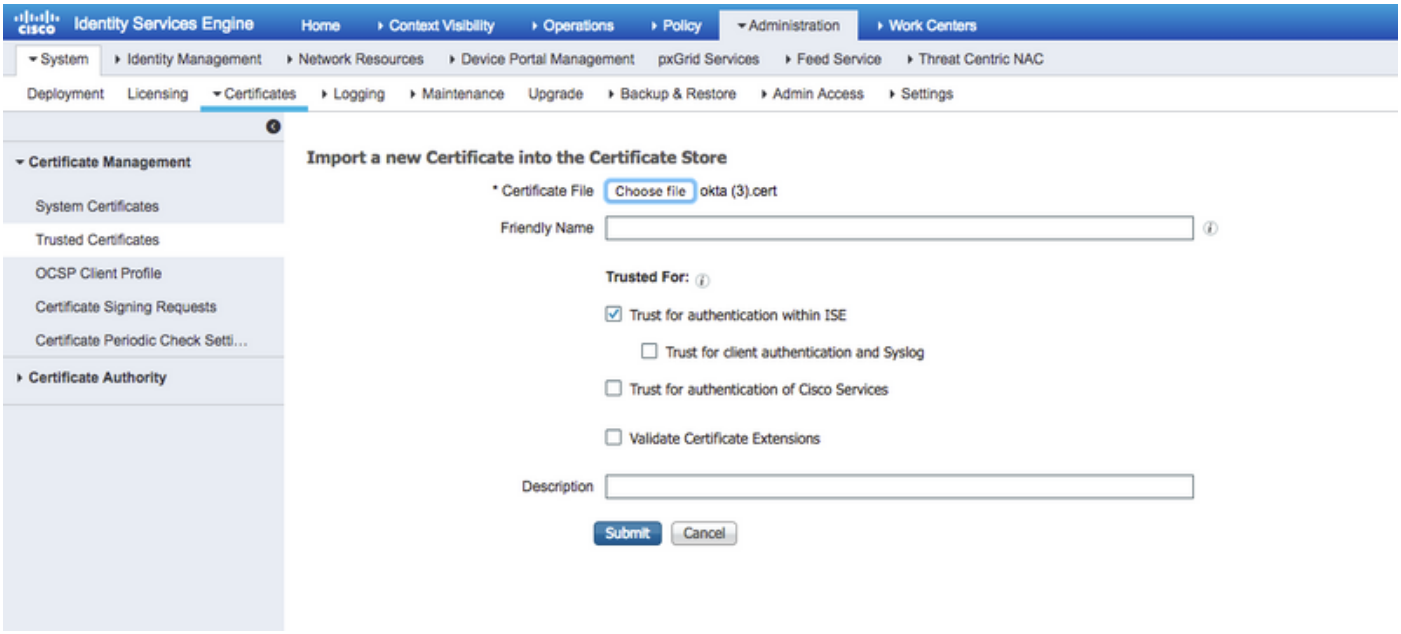

Create a New Application Integration
Platform
Web
Sign on method
Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
OpenID Connect
Uses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

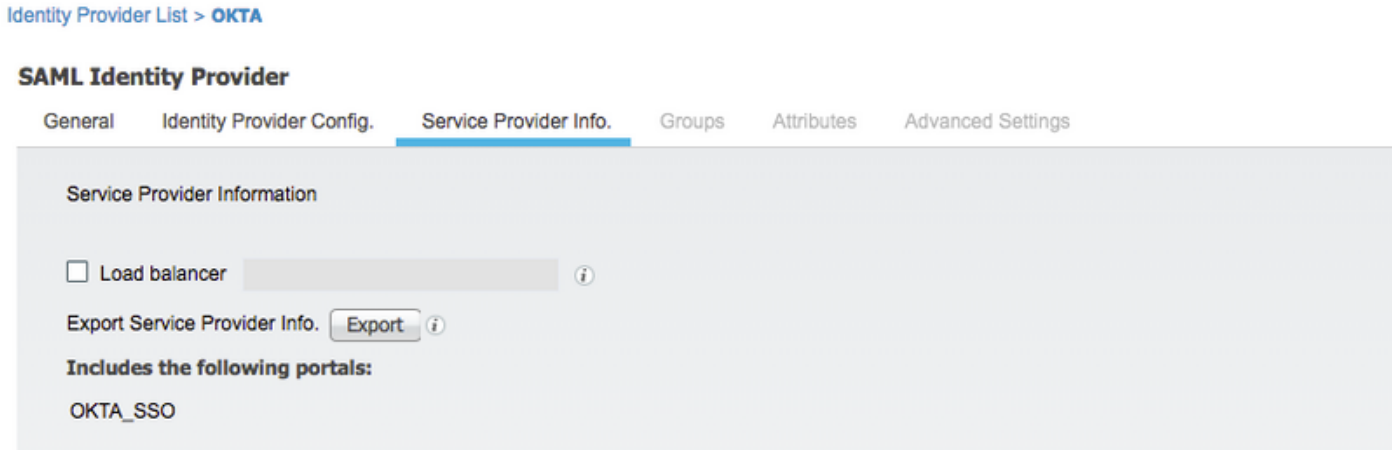


步骤4.下载证书并将其安装在ISE受信任证书中。



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。



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

- SP实体ID

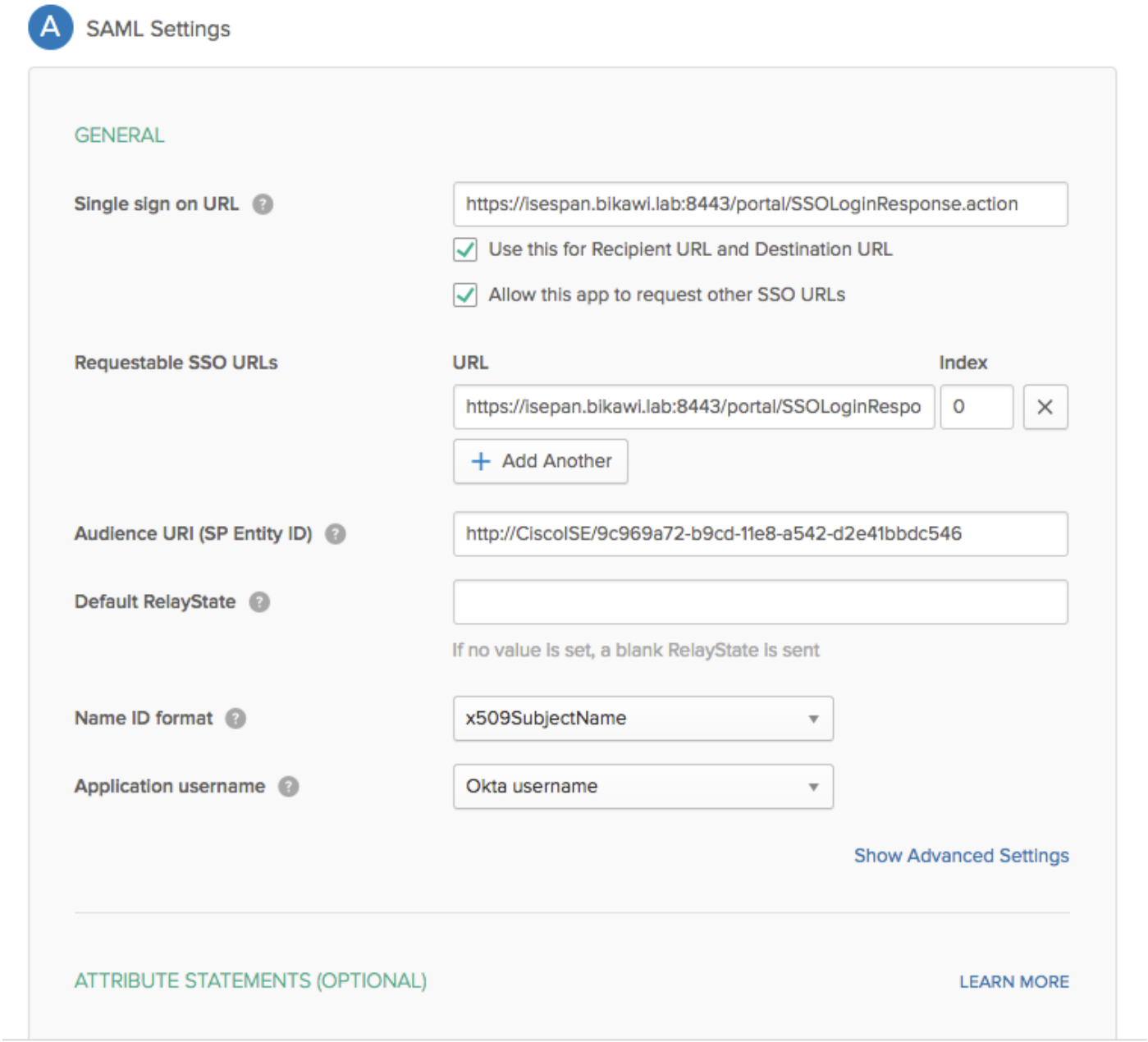
```
entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"
```

SSO URL以IP地址和FQDN格式提供。

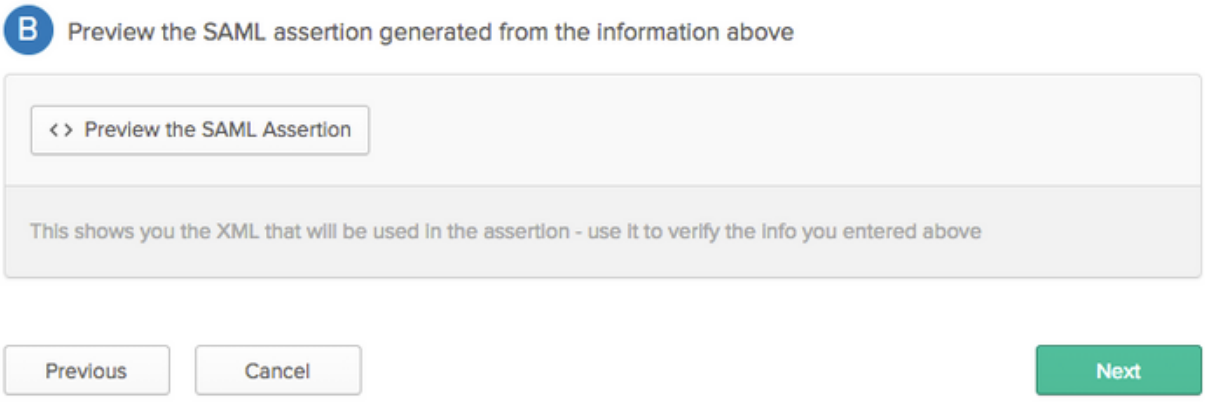
> **警告**：格式的选择取决于授权配置文件上的重定向设置，如果使用静态IP，则应将IP地址用于SSO URL。

3.确定SAML设置。

步骤1.在SAML设置上添加这些URL。



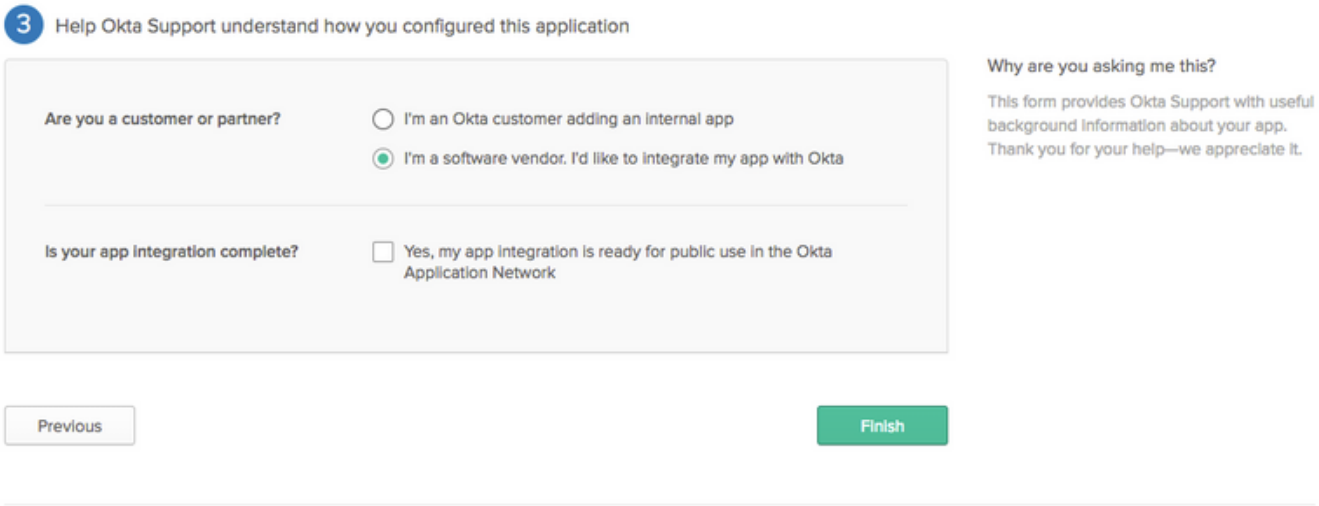
步骤2.根据托管此服务的PSN的数量，可以从XML文件添加多个URL。名称ID格式和应用用户名取决于您的设计。



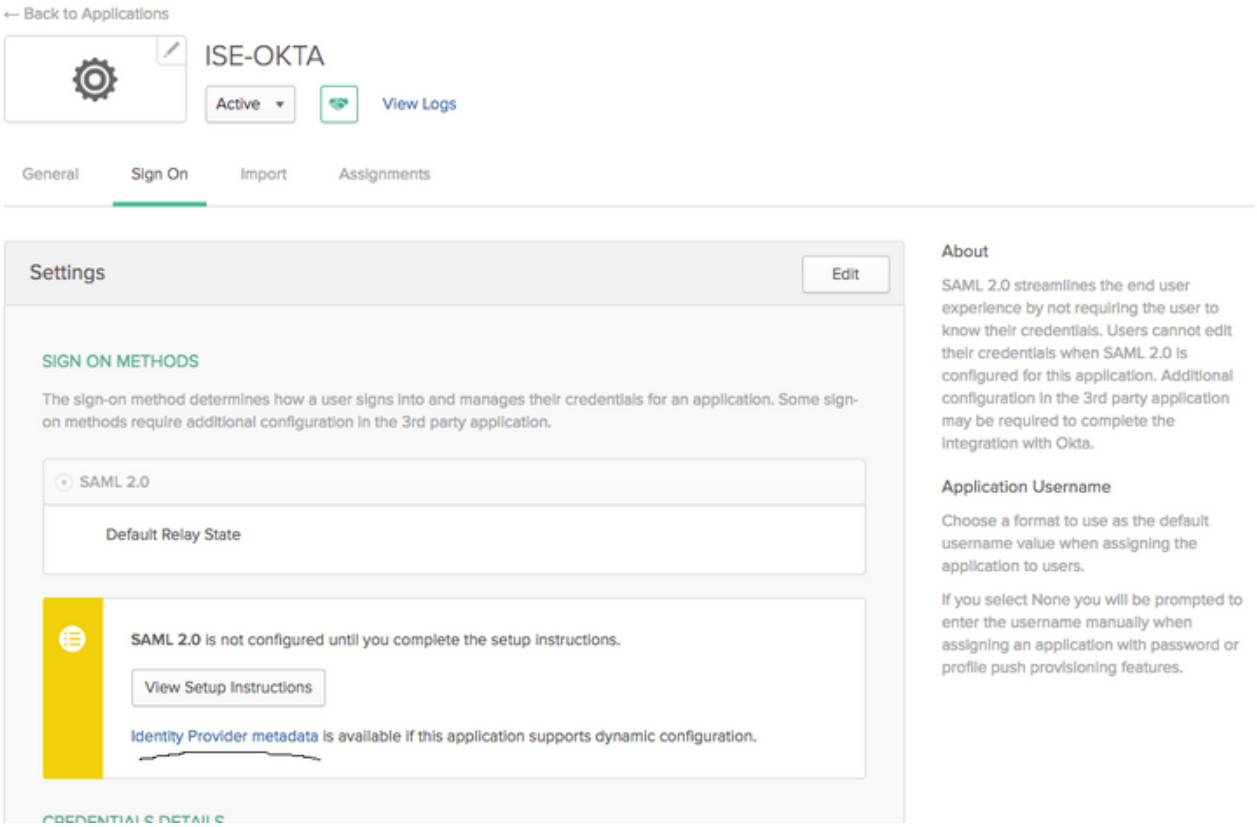

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124"
```

```
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>
```

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/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>
MIIDrDCCApSgAwIBAgIGAWWPlTasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXlhbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFg1pbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNVoXDTI4MDgzMTEwNDQwNVowgZYxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEXMBUGA1UEAwwOY2lzY28teWFsYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQClP7DvzVng7wSQWVOzgShwn+Yq2U4f3kbVgXWGuM0a7Bk6lAUBoq485EQJ1+heB/6x
IMt8u1Z8HUsOspBECLYcI75gH4rpc2FM4kzZiDbNLb95AW6dlUztC66x42uhRYgduD5+w3/yvdwx
l99upWb6SdRtnwK8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgjYQO/7GRK2RzOj
bSZgeAp5YyytjA3NCn9x6FMY5Rppc3HjtG4cjQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dN6YERuV5C5eHUXq3KGul2yIfiH7x8EartZ4/wGP/HYuCNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdtSz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesyysecPuWQtEqNqt+MyZnlCurJ0e+JTvKYH1dSWapM1dzqoX
OzyF7yiId9KPP6I4Ndc+BXe1dA8imneYy5MHH7/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>
```

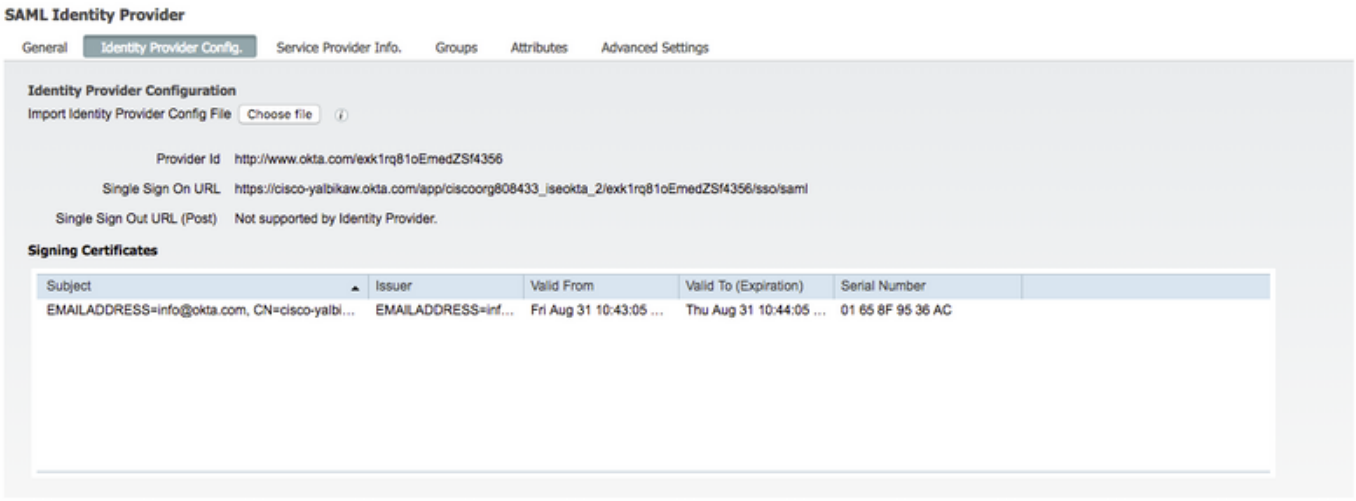
以XML格式保存文件。

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。



步骤2.保存配置。

步骤3.CWA配置。

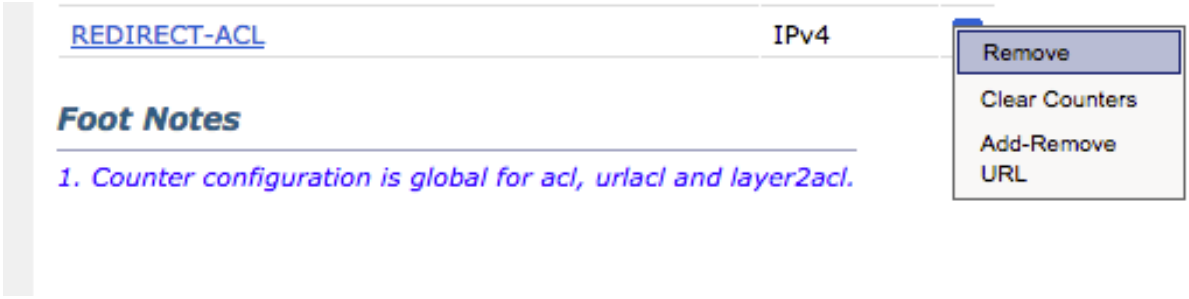
本文档介绍ISE和WLC的配置。

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。

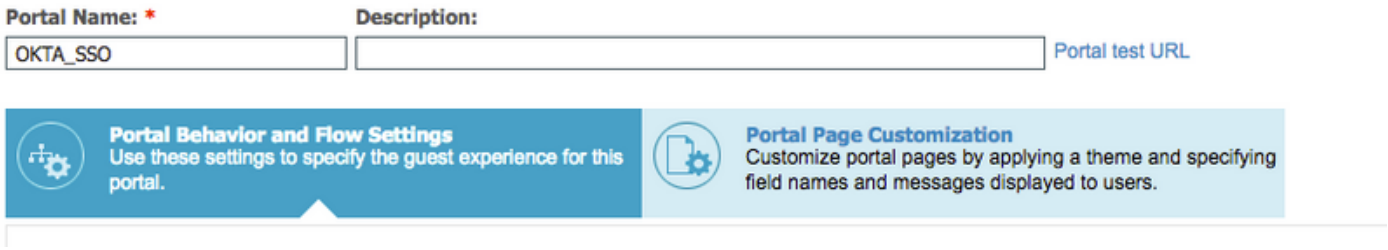
https://cisco-yalbikaw.okta.com /添加您的应用URL

https://login.okta.com

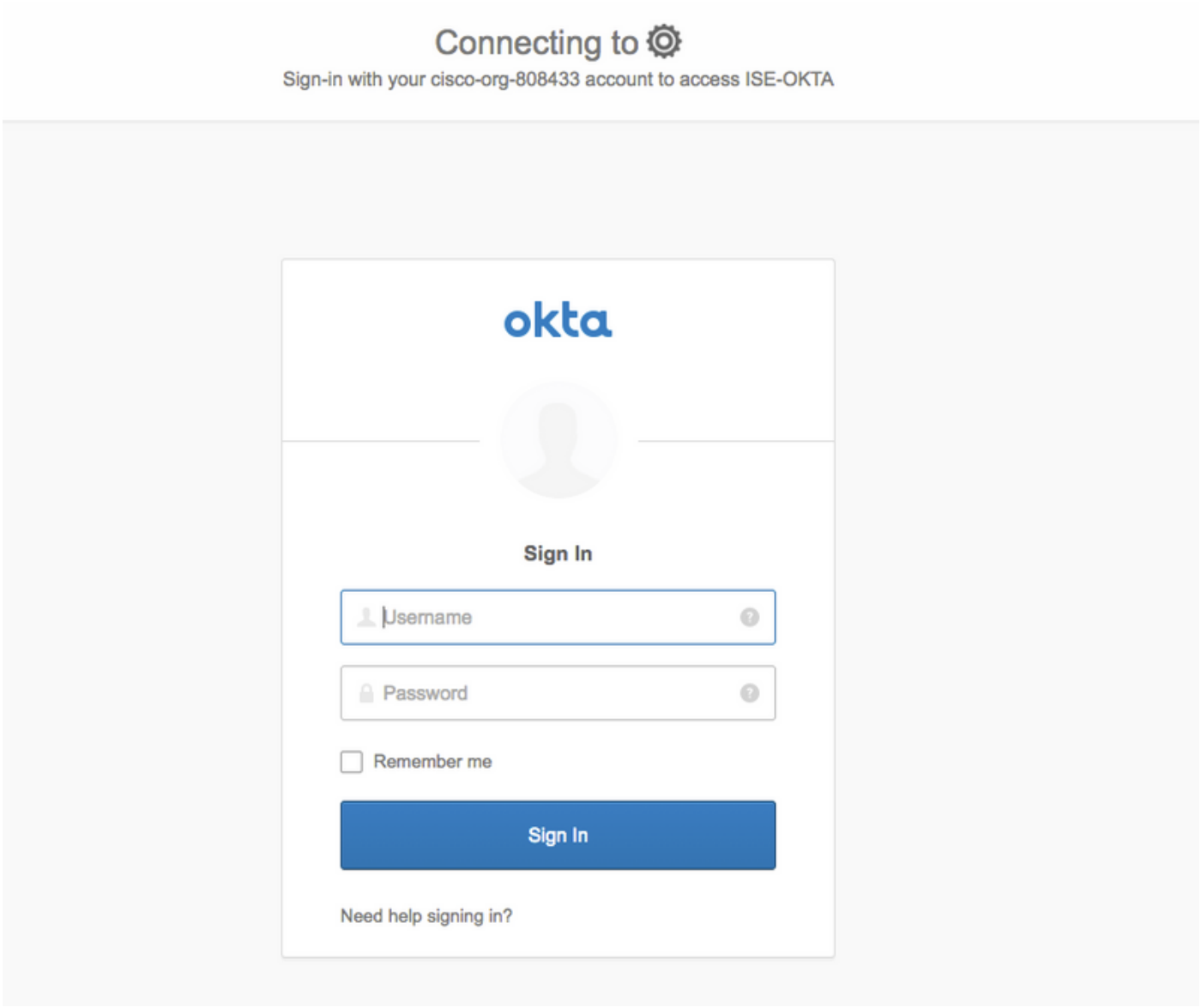


验证

测试门户并验证您是否能够访问OKTA应用



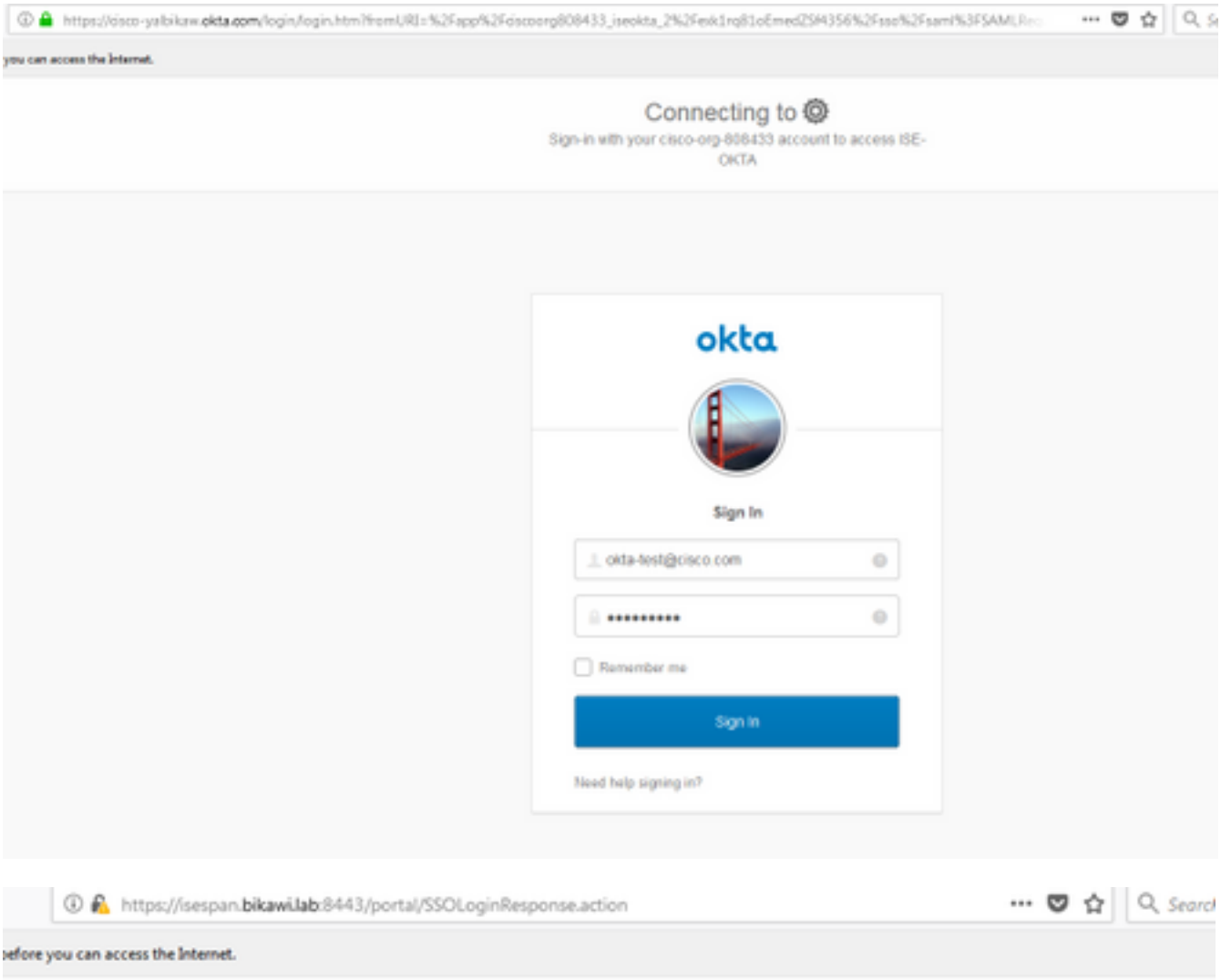
步骤1.点击门户测试，您应被重定向到SSO应用。



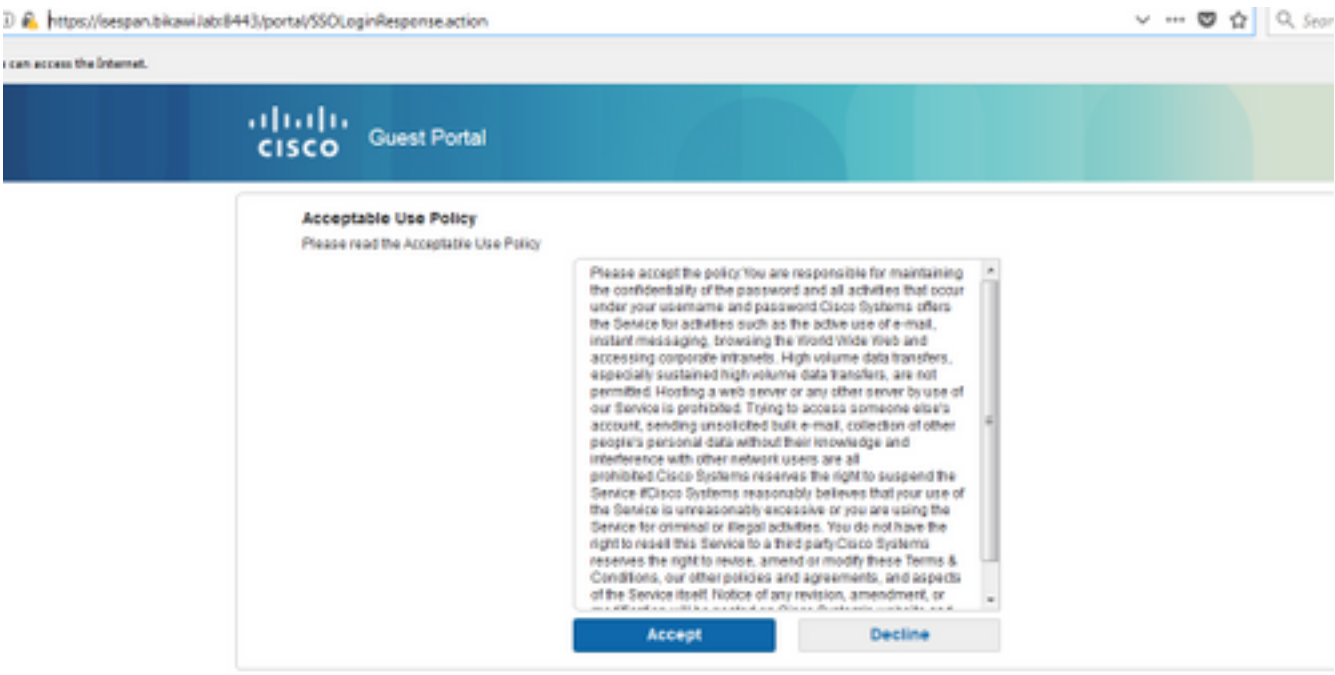
步骤2.检查与***的信息连接***

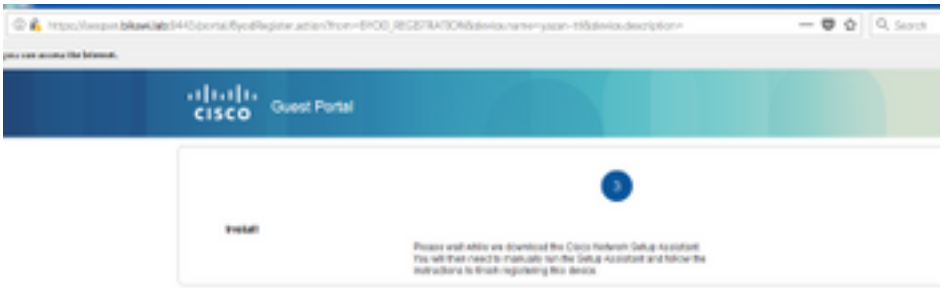
步骤3.如果输入可能看到错误的saml请求的凭据，这并不一定意味着此时配置错误。

最终用户验证



Signing in to ISE-OKTA





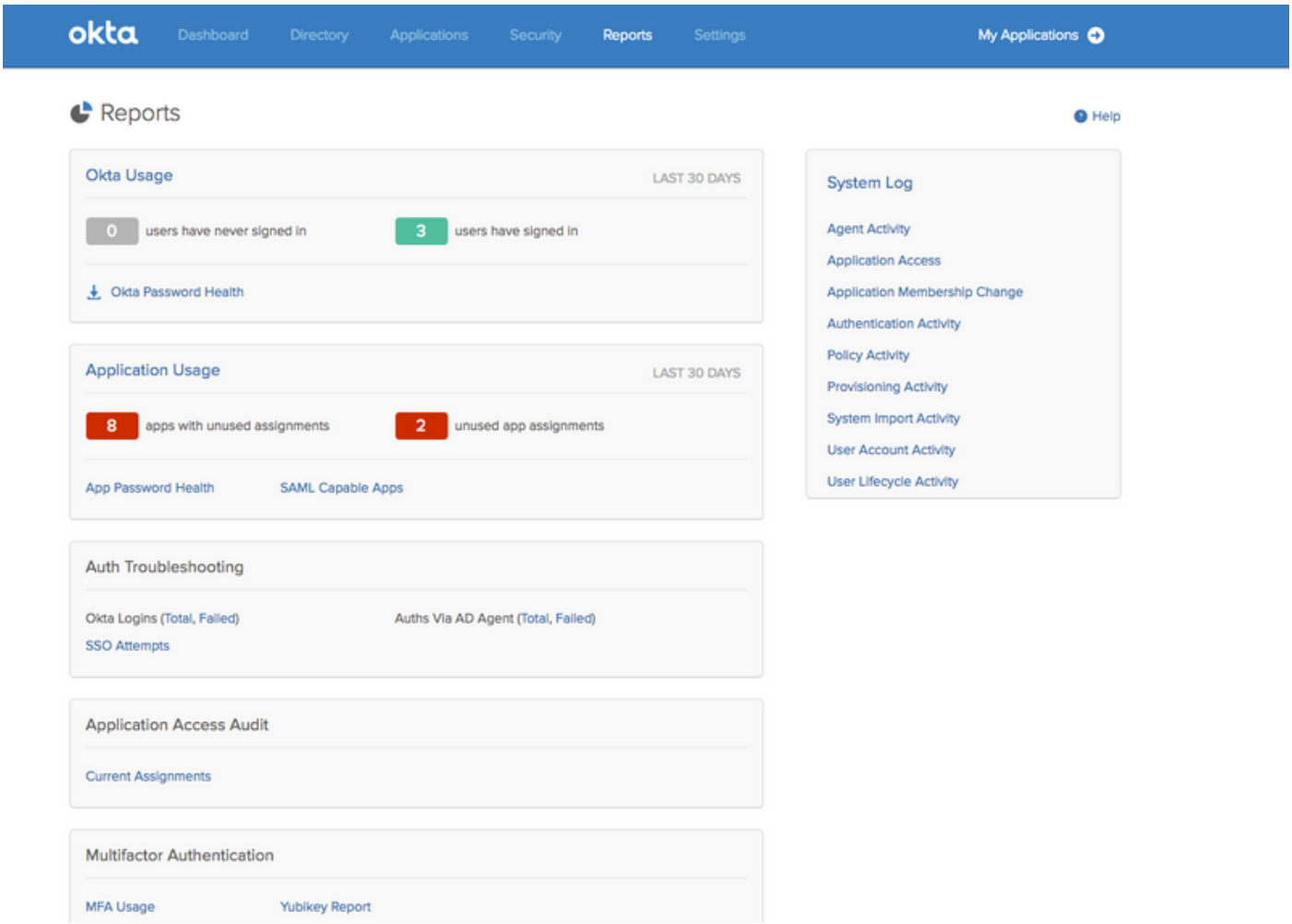
ISE验证

检查生命日志以验证身份验证状态。

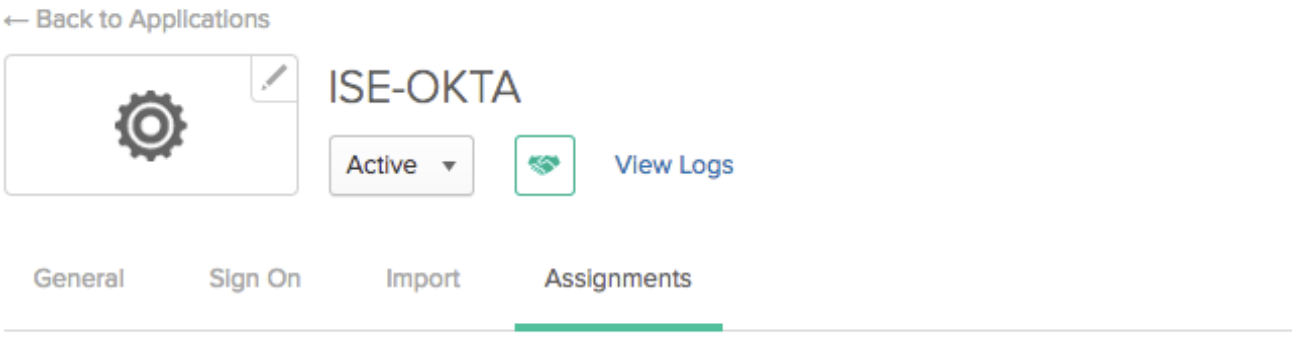
故障排除

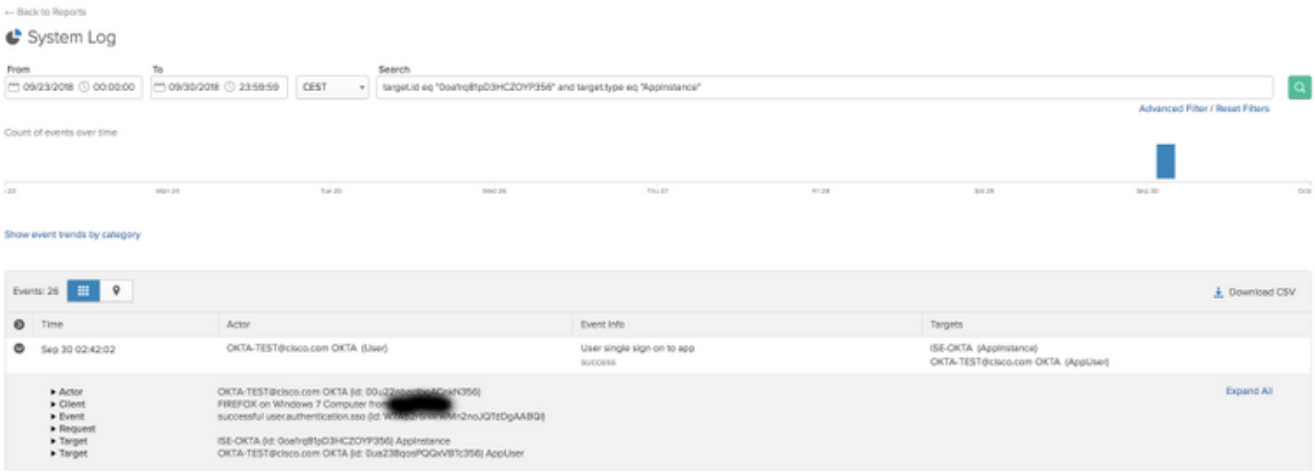
OKTA故障排除

步骤1.检查“报告”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

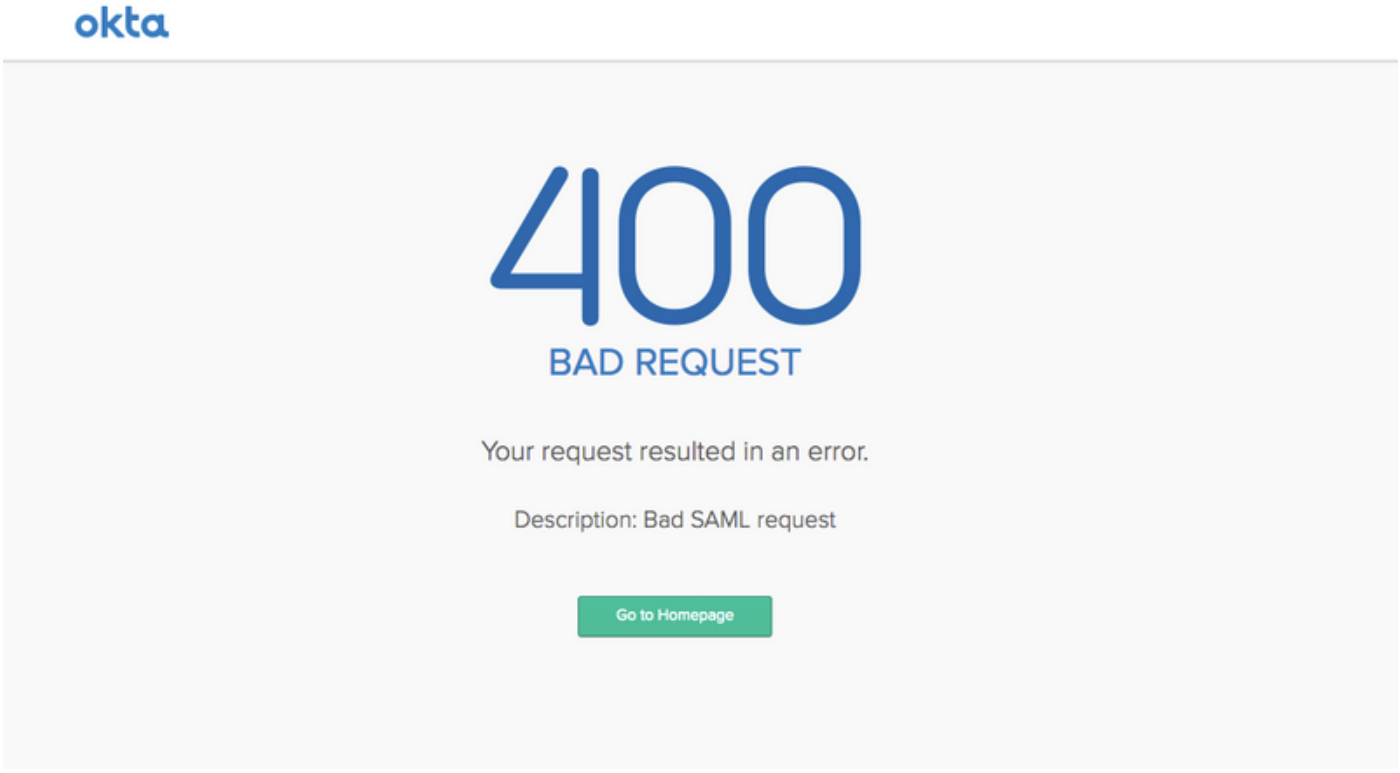
导航至**管理>系统>日志记录>调试日志配置**。启用DEBUG级别。

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。



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

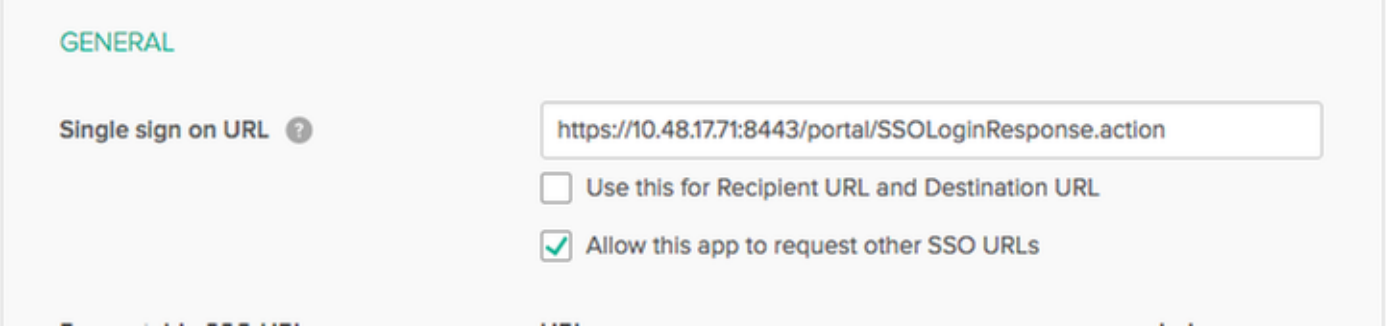
```
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:
SSOLoginTransitionResult:

        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%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0SltaB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3u
gJMm%2BObfDAc4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfkbd6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnC
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
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%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJ
OOb4672DqCNUDJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhlhOiulyQcIeJ
o1WVnFVI29qDGjrjGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0SltaB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJl3ugJMm%2BObfDAc4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DEcRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfkbd6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1z
X6nmmgdq3YIO37q9fBlQnCh3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVmX5YxglvW7vXLUPPSlctE8DdzUpNpWl
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:
/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。

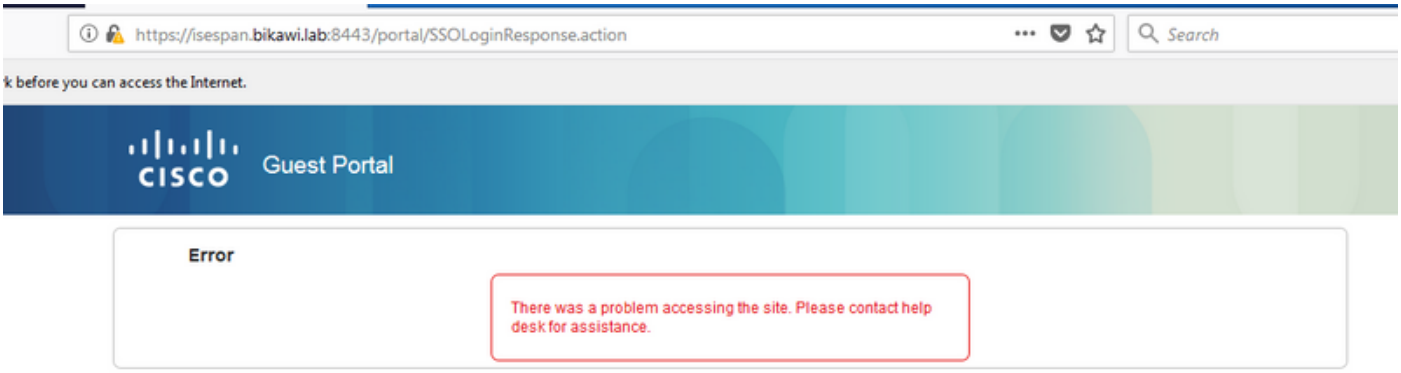
```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9owF
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0SltaB0Vxv1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3ugJMm%2BObfDAc4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfkbd6XdcnITsIPtot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnCh3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-
b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_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”。



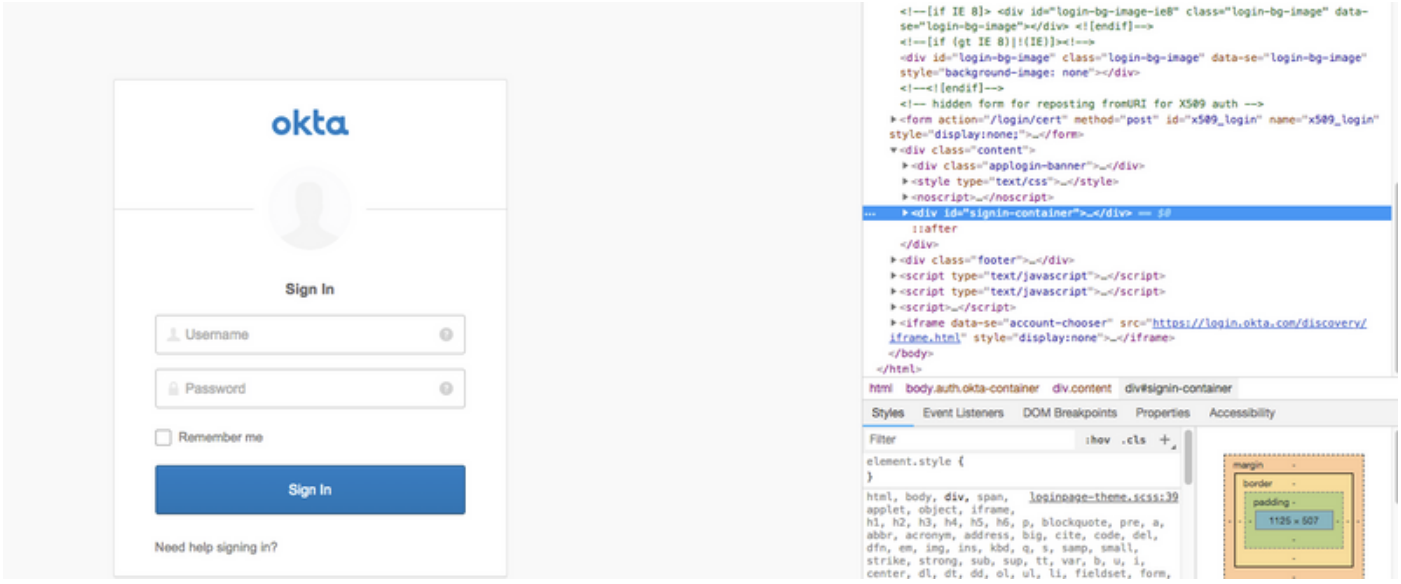
Guest.log

```
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