Configure ISE 2.3 Guest Portal with OKTA SAML SSO

Contents

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.

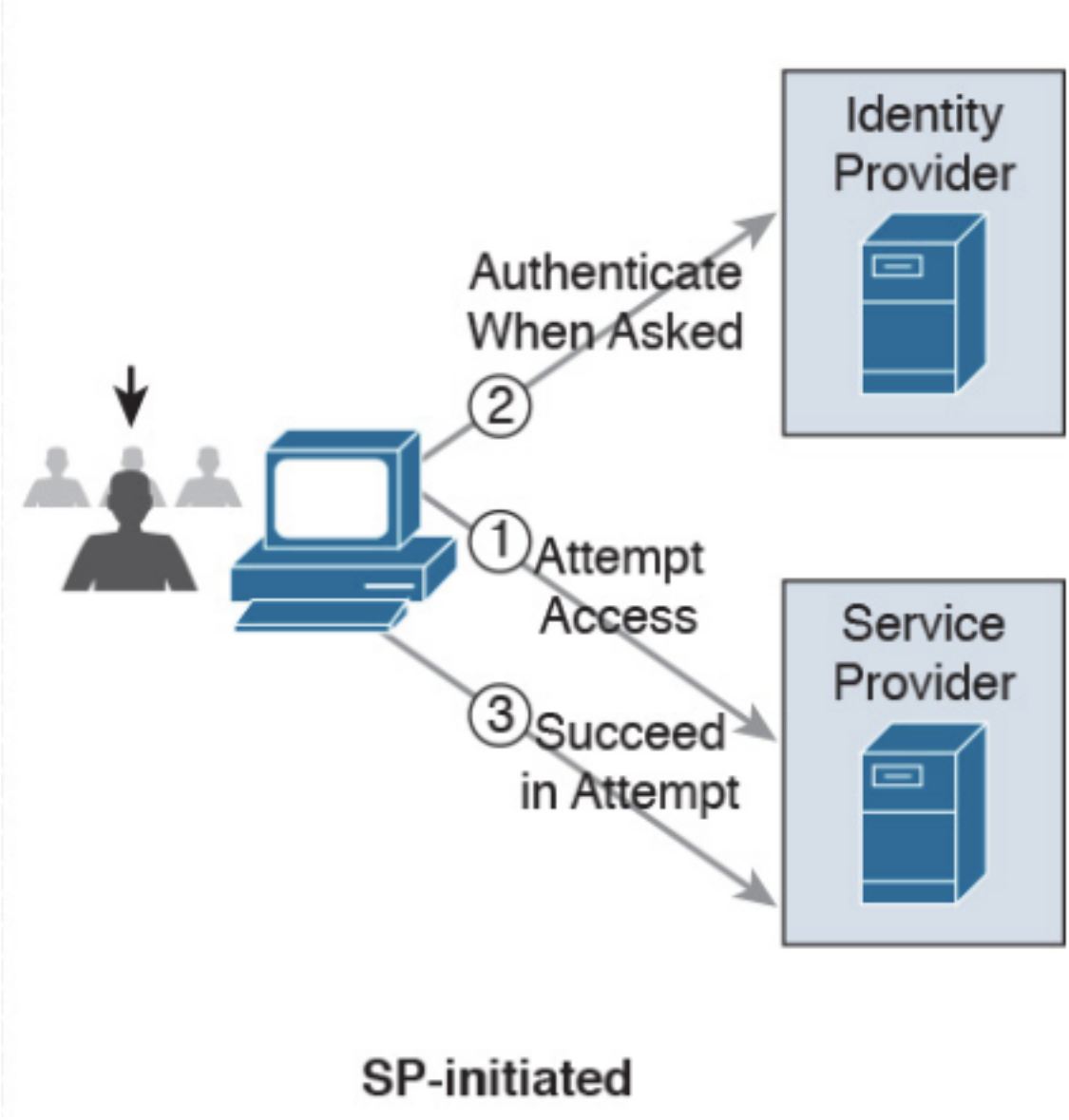
The concept of federation:

- 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.

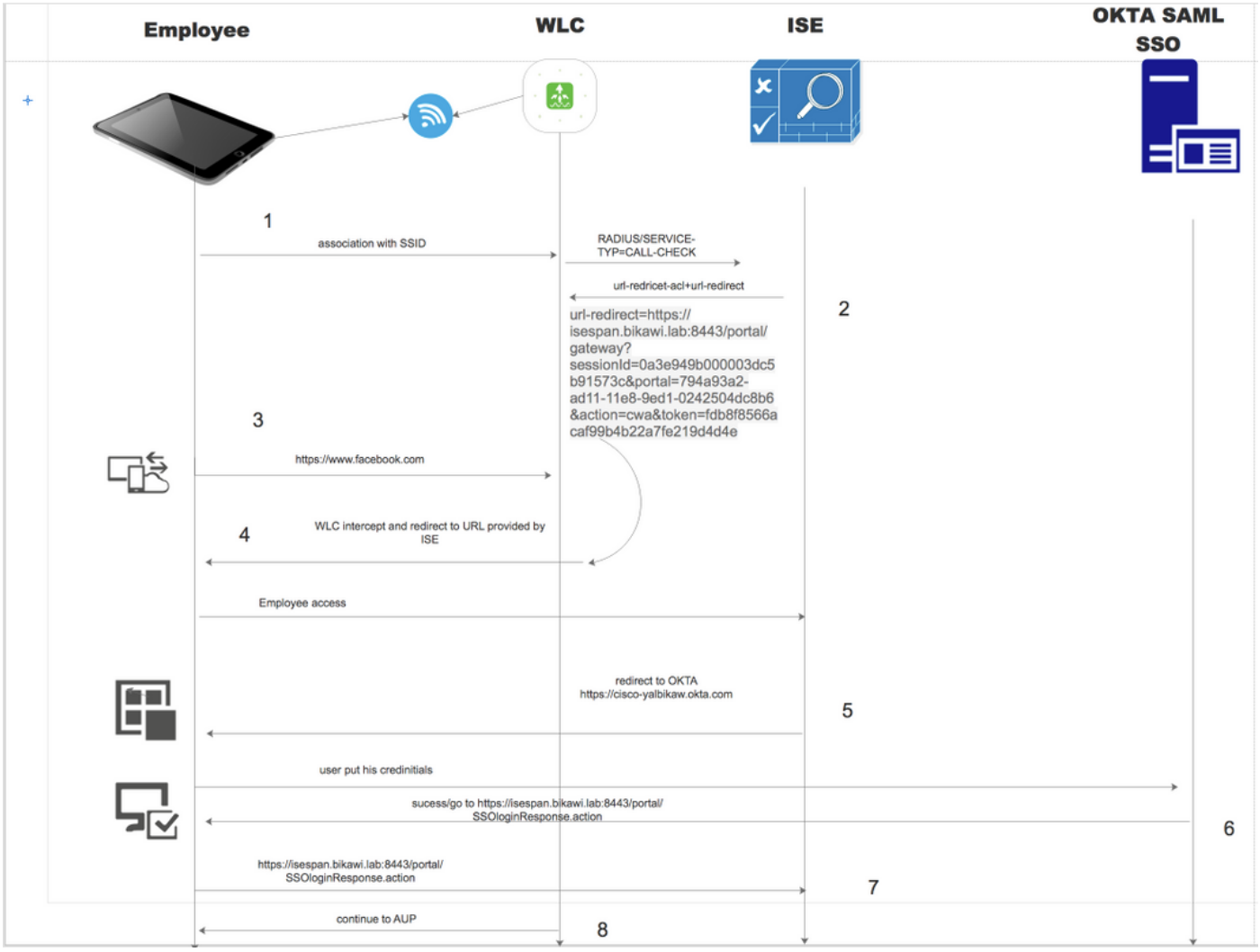
Several protocols implement SSO such as OAuth2 and OpenID. ISE uses SAML.

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.



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.
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

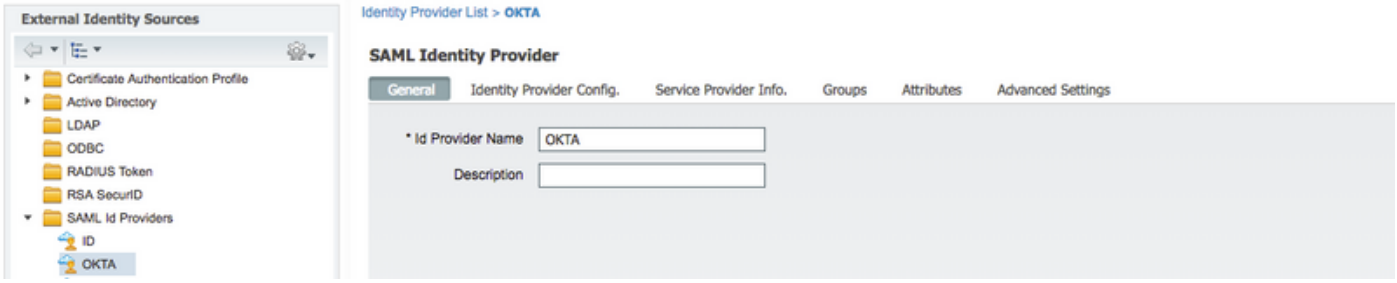
https://developer.okta.com/standards/SAML/

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**.

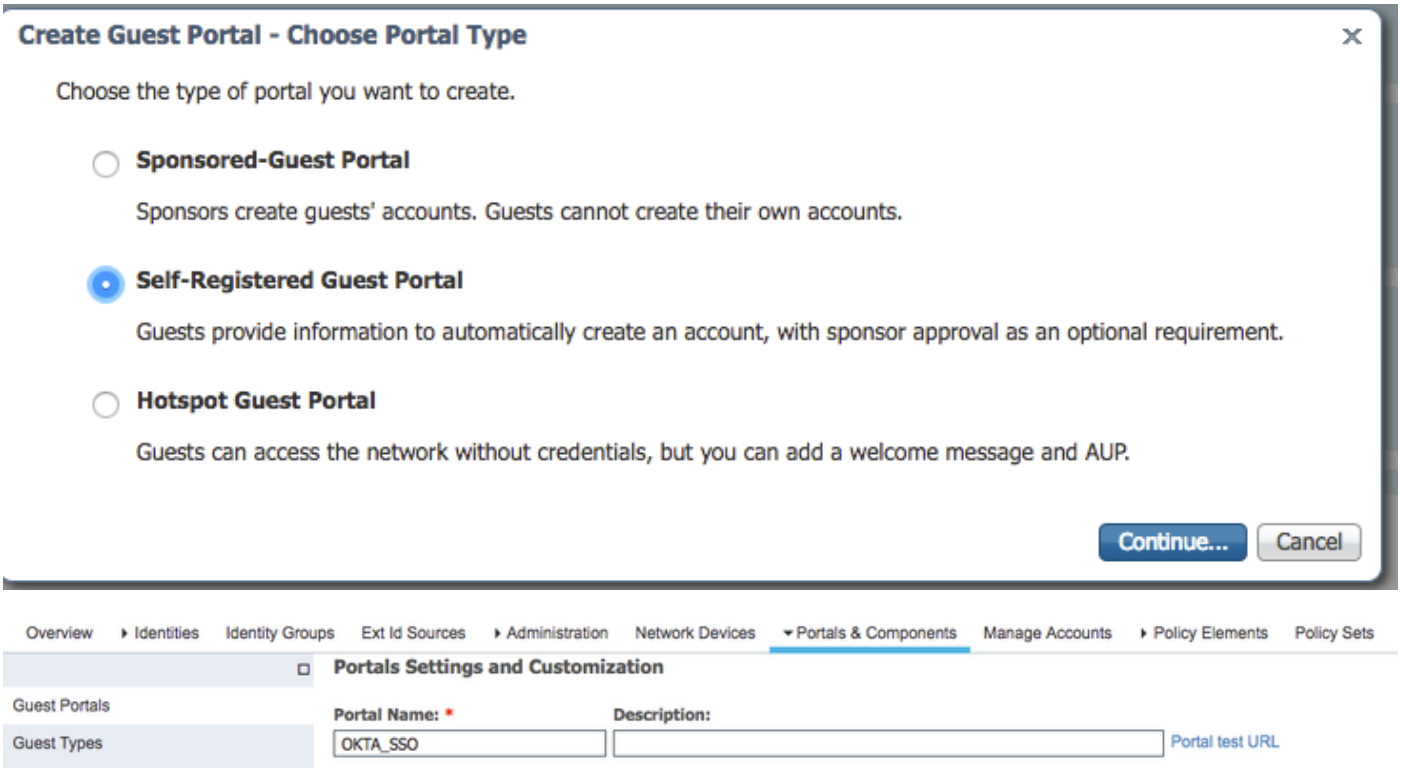


Step 2. Assign a name to the id provider and submit the configuration.

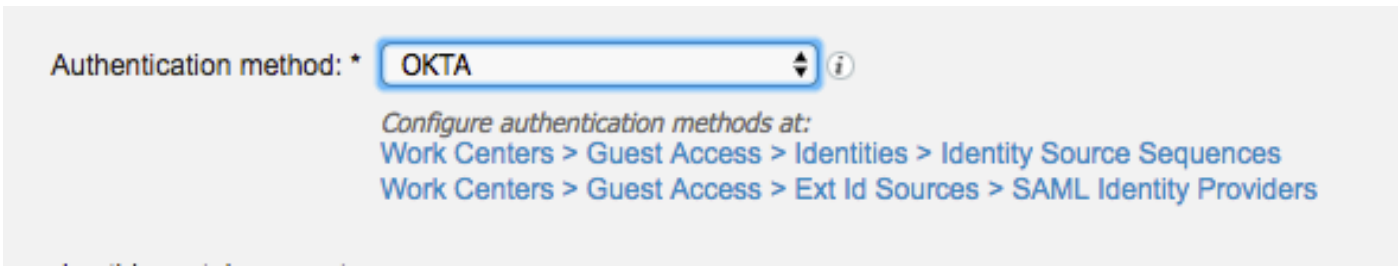
2. Create Portal for SSO.

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.

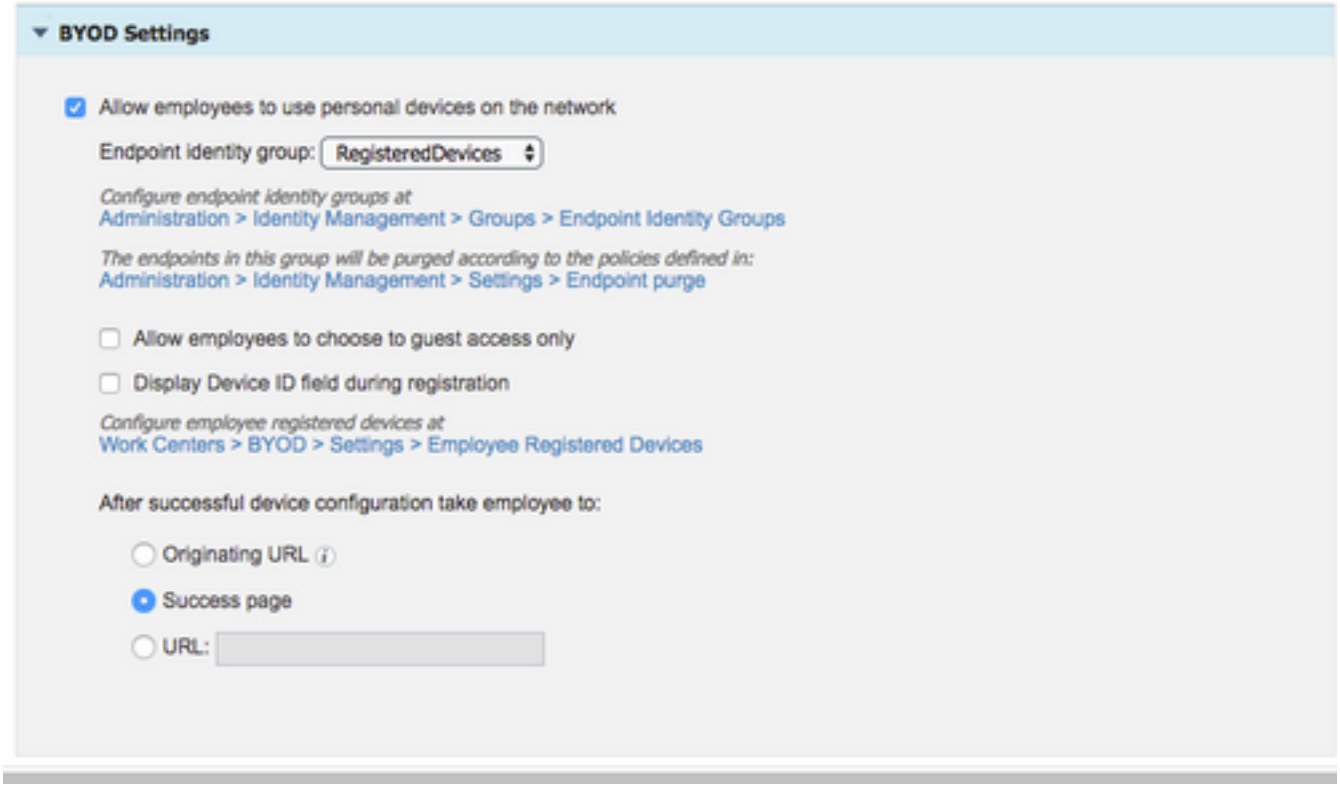


Step 3. Choose the authentication method to point to the identity provider configured previously.

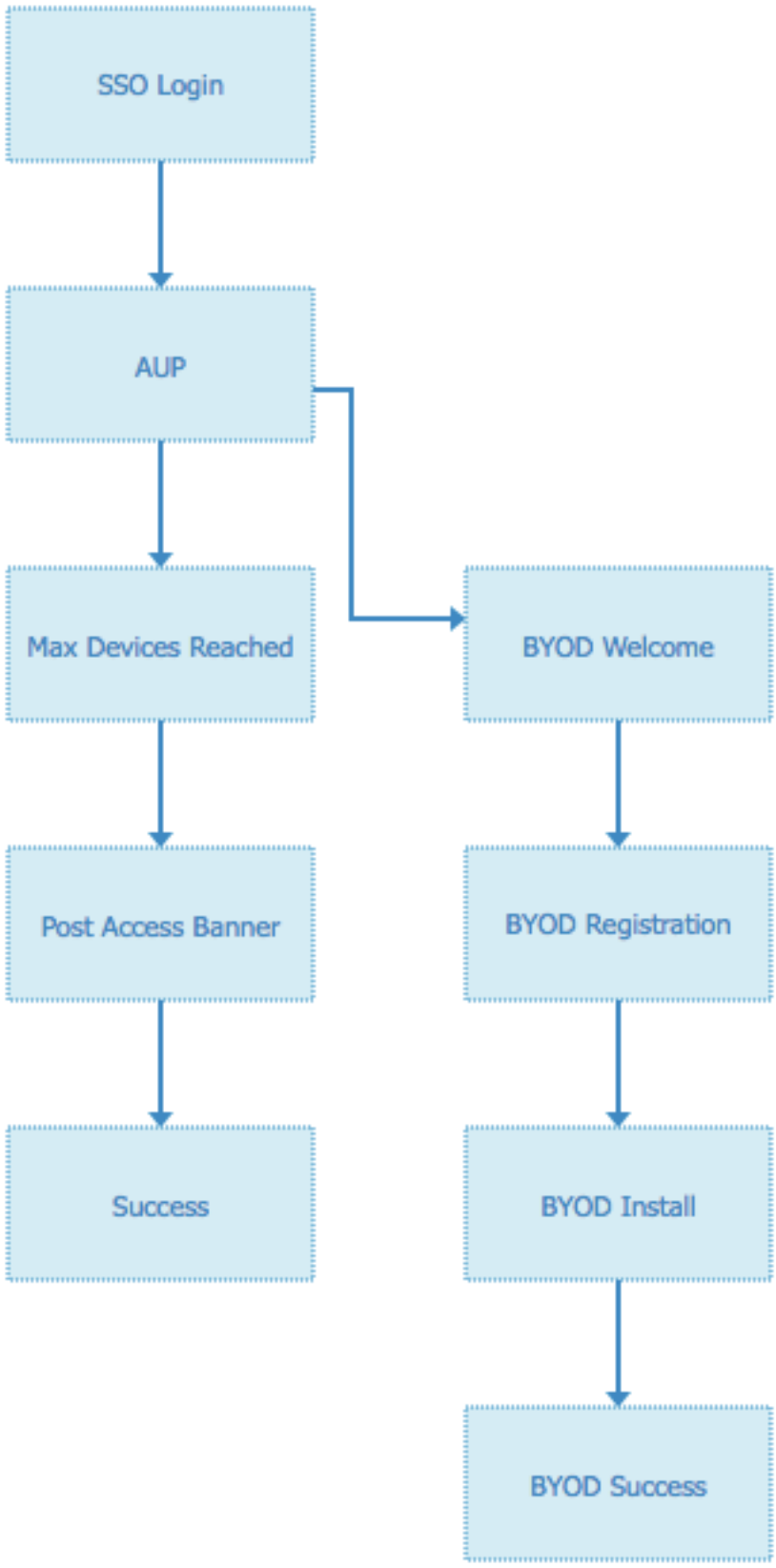


Step 4. Choose OKTA identity source as an authentication method.

(optional) choose the BYOD settings.



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

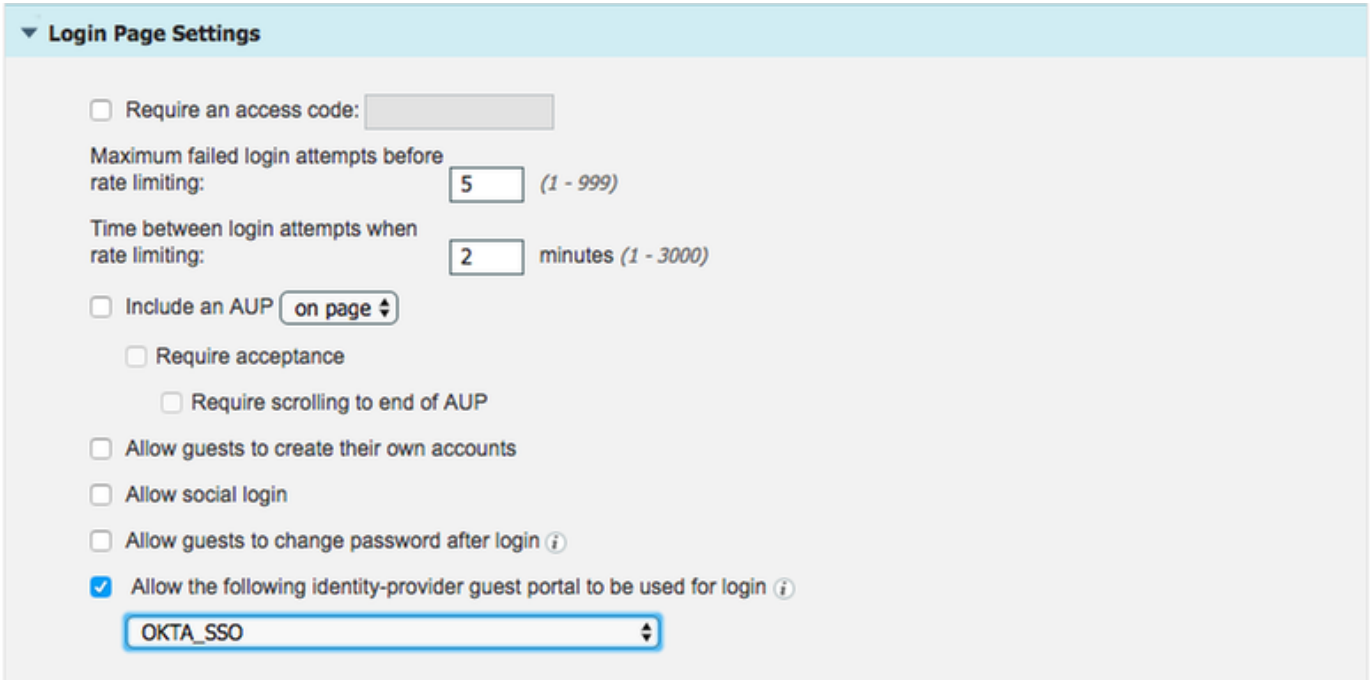


3. Configure Alternative Login.

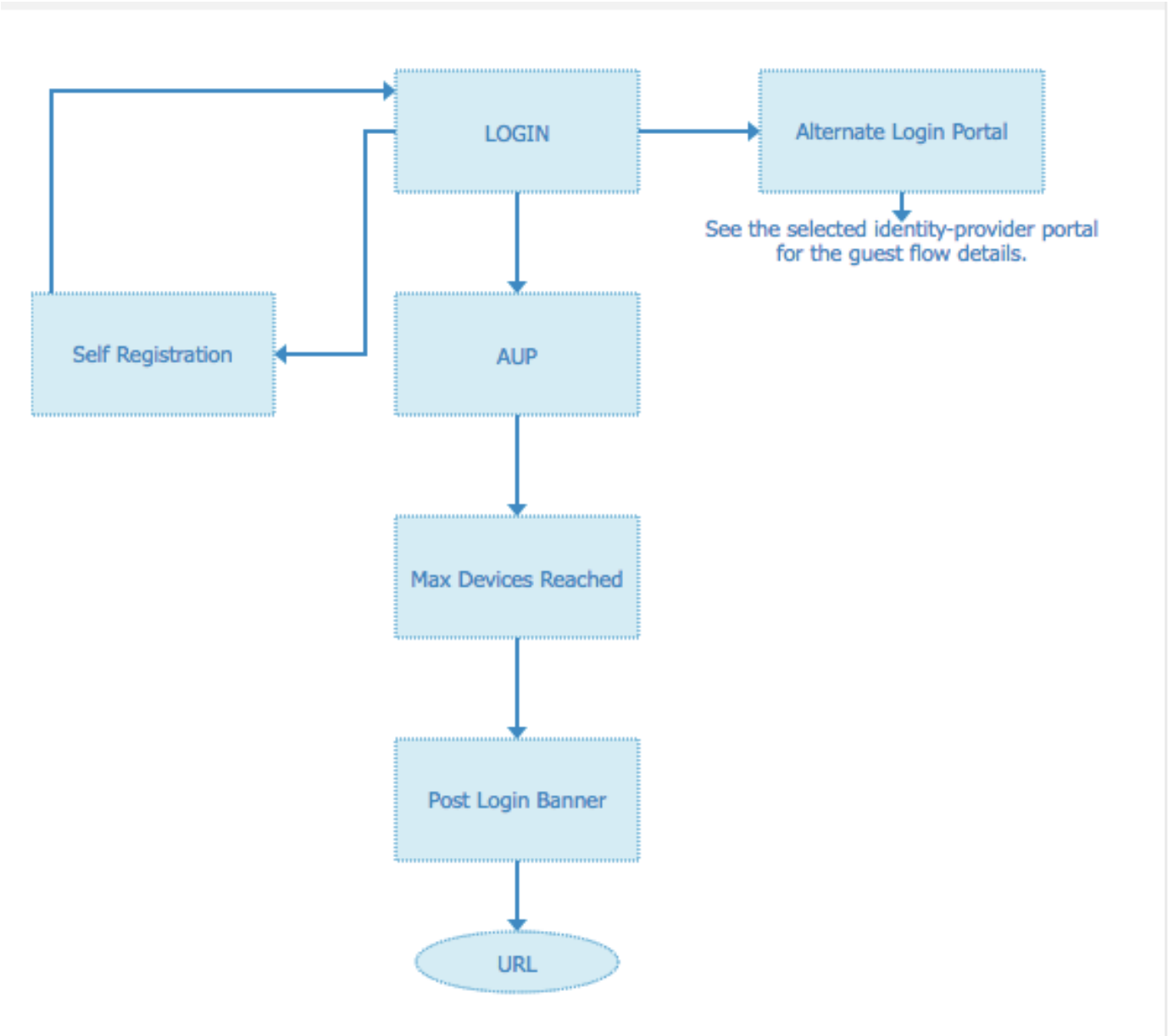
Note: You can skip this part if you are not using the Alternative login.

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.



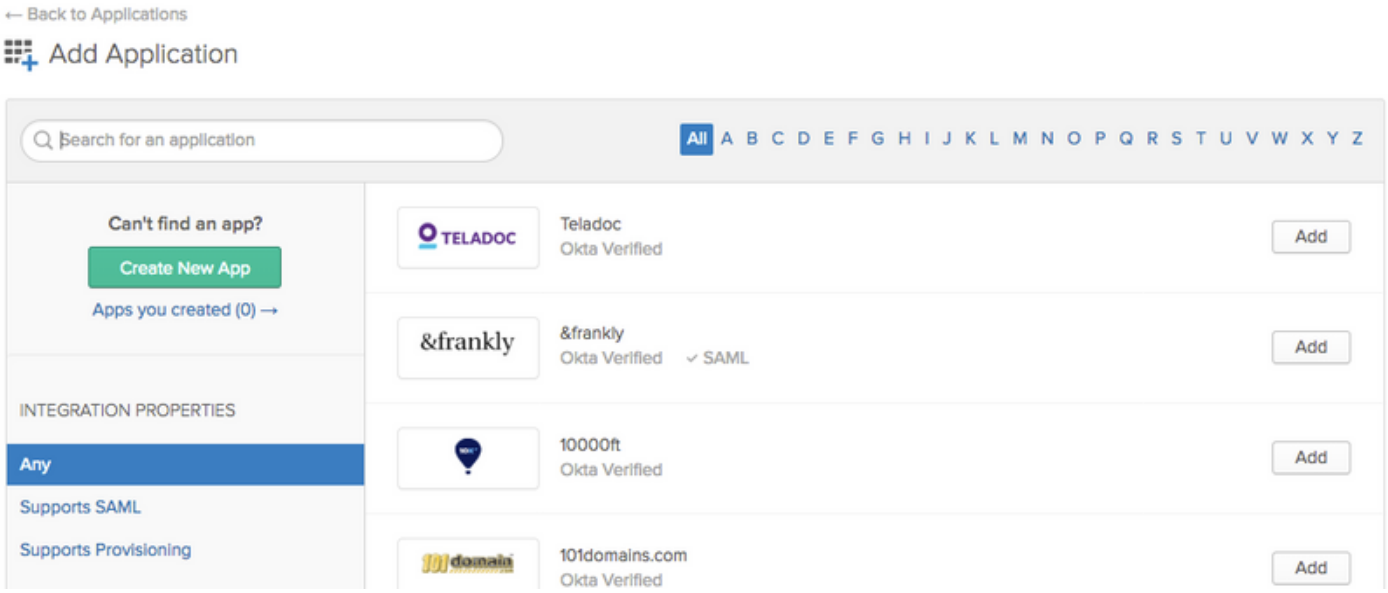
This is the portal flow now.



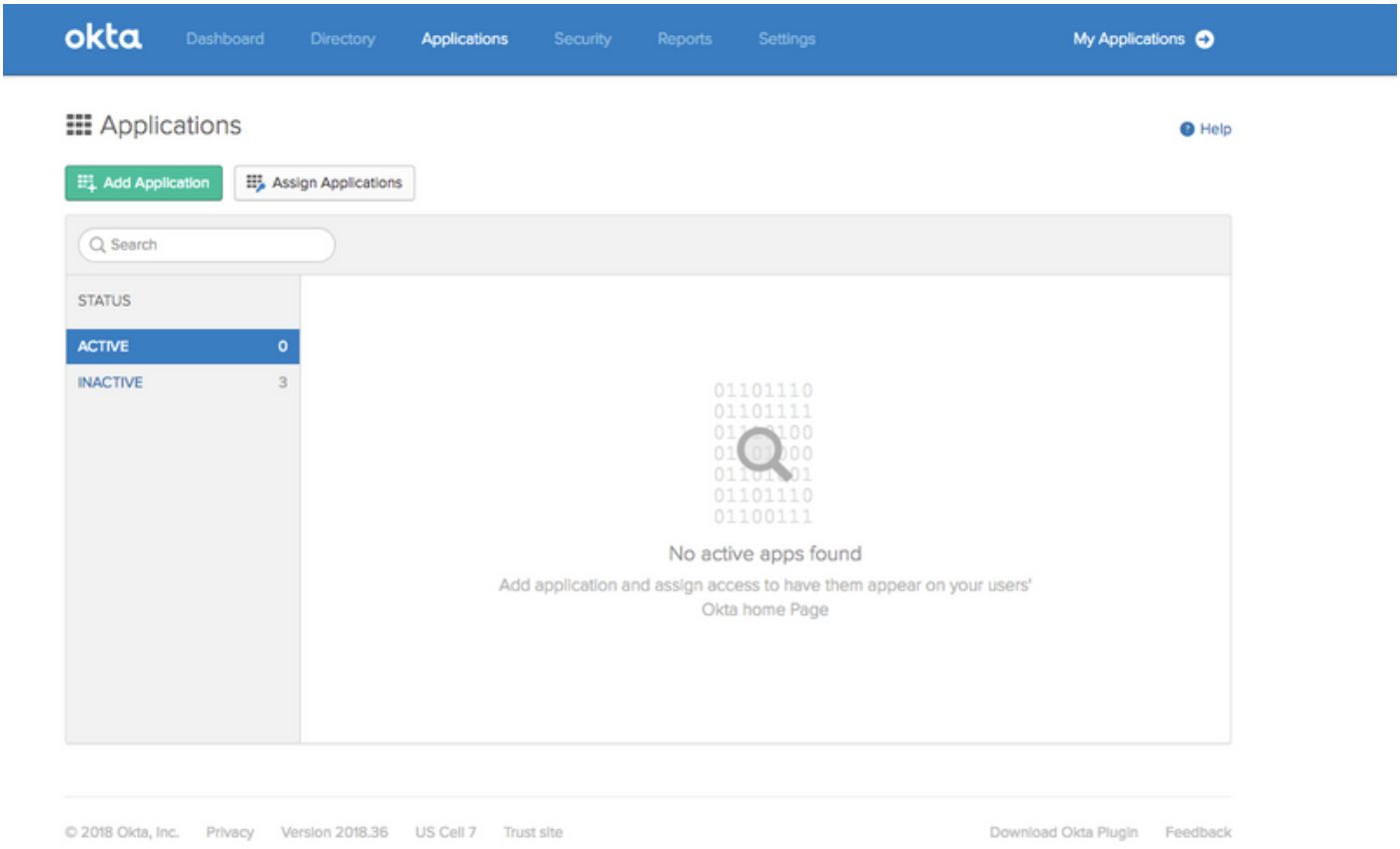
Step 2. Configure OKTA Application and SAML Identity Provider Settings.

1. Create OKTA Application.

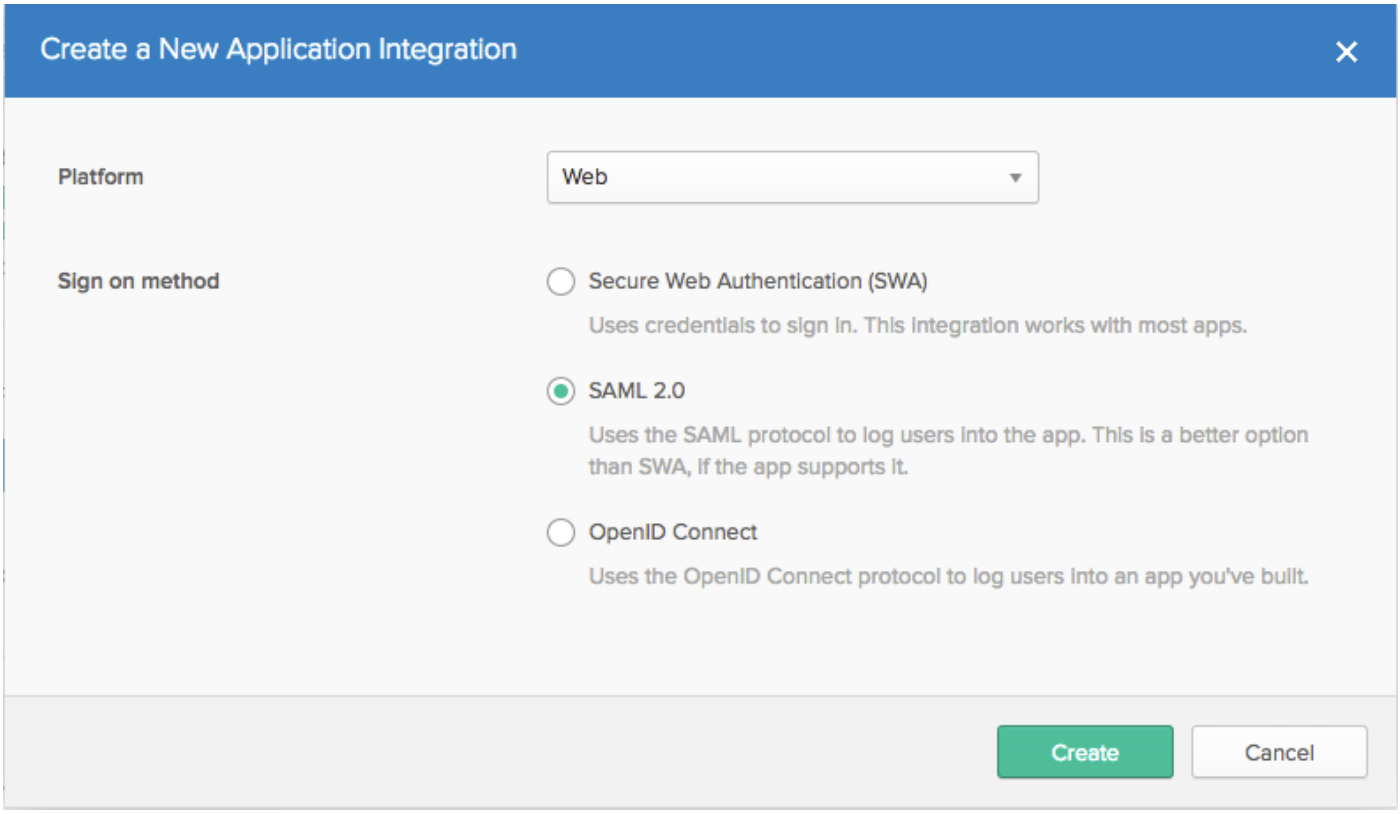
Step 1. Login to OKTA website with an admin account.



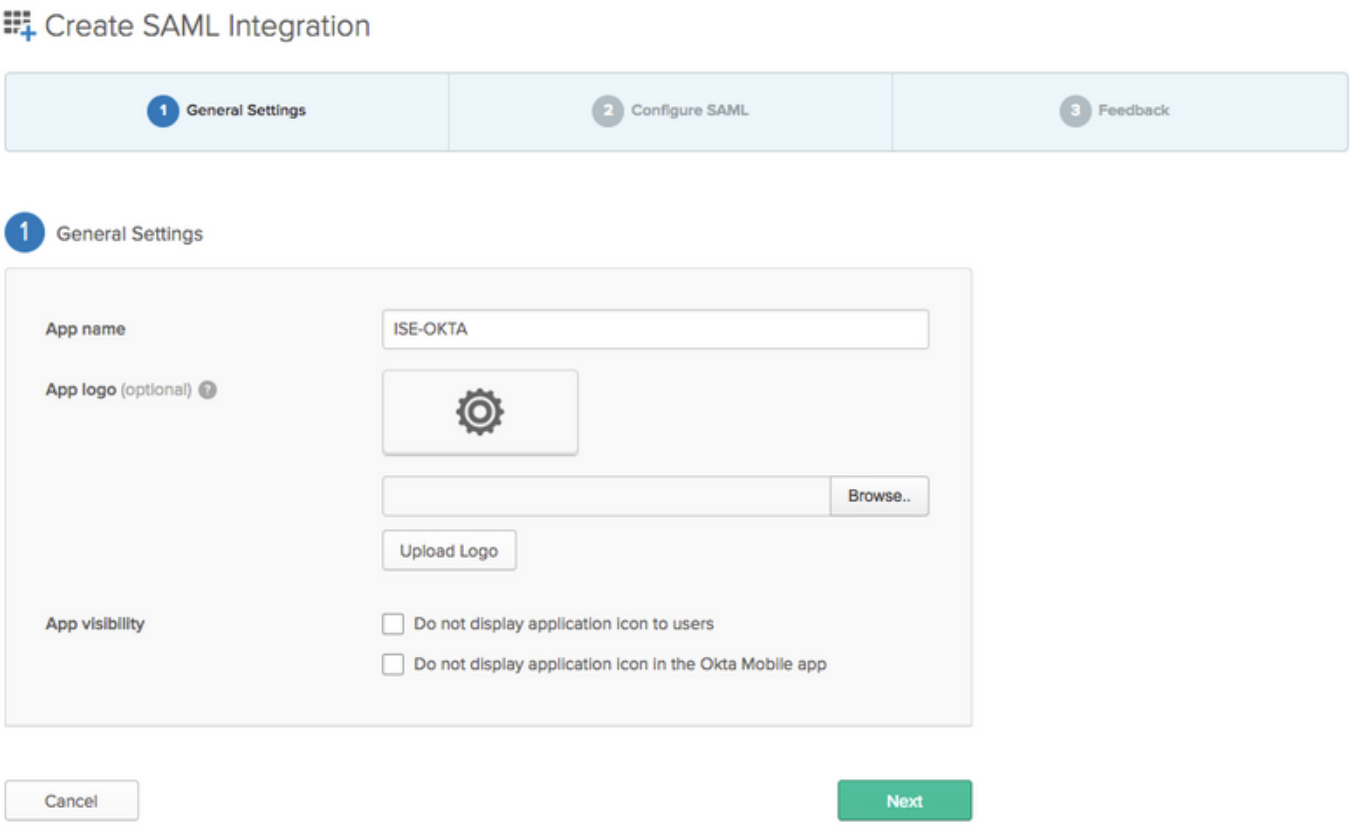
Step 2. Click on Add Application.

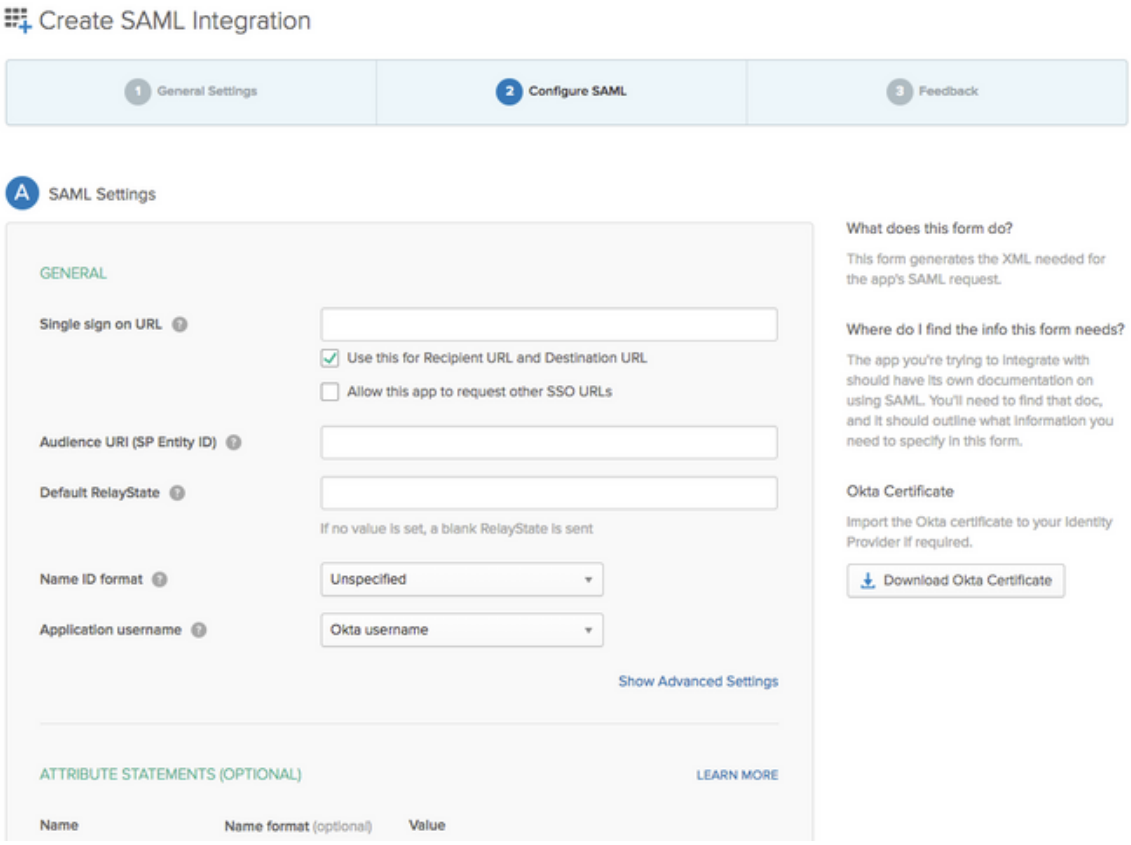


Step 3. Create New App, choose it to be SAML2.0

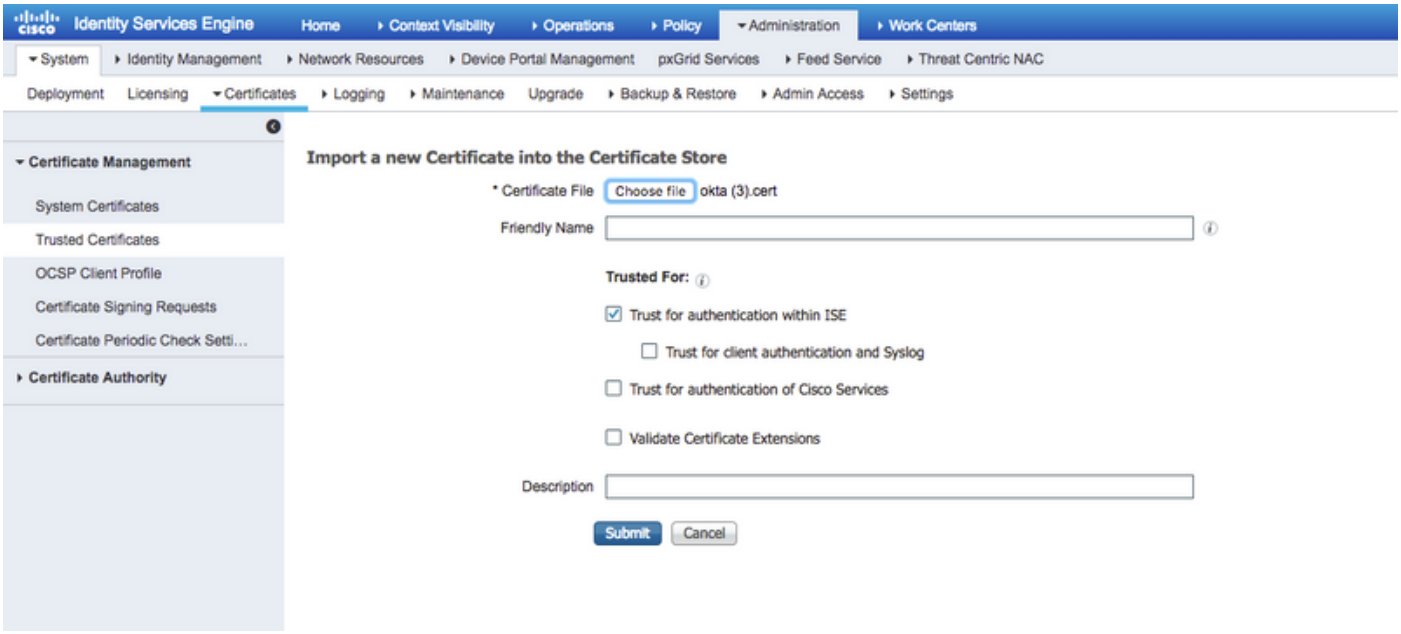


General settings



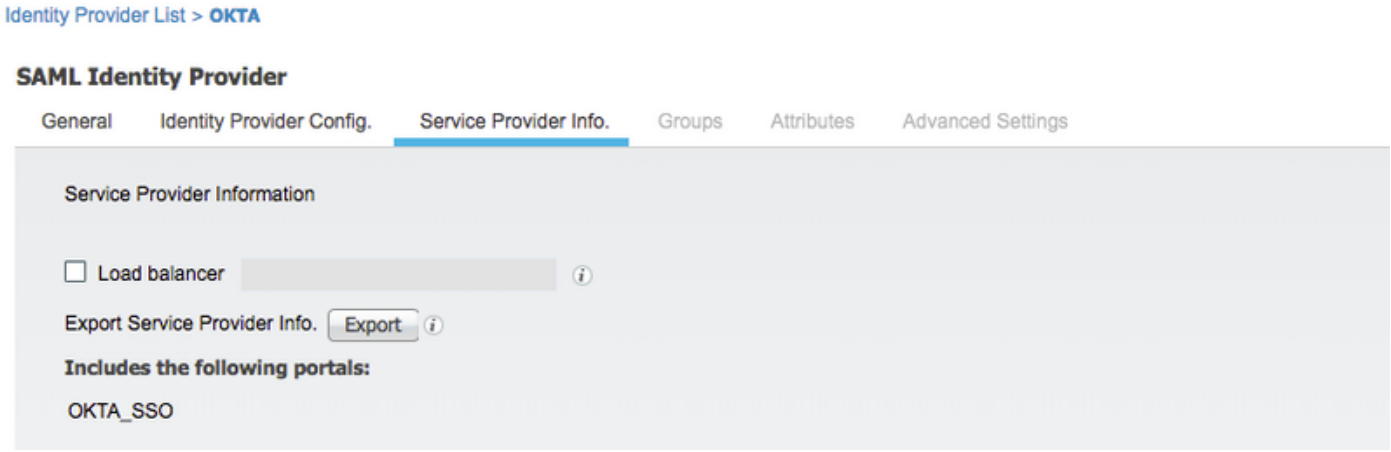


Step 4. Download the certificate and install it in ISE Trusted Certificates.



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.



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

- SP Entity ID

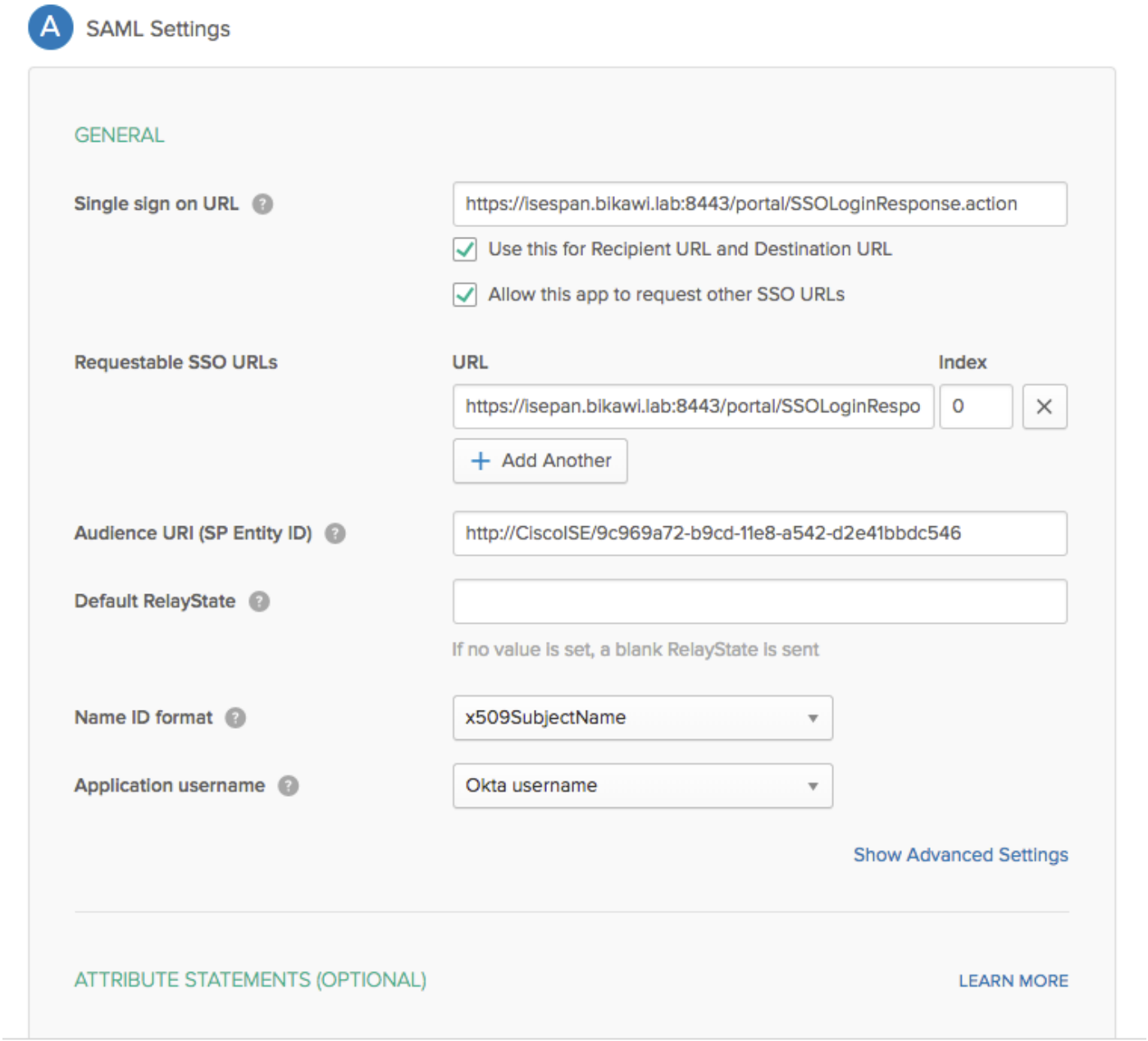
```
entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"
```

The SSO URL available in ip address and FQDN format.

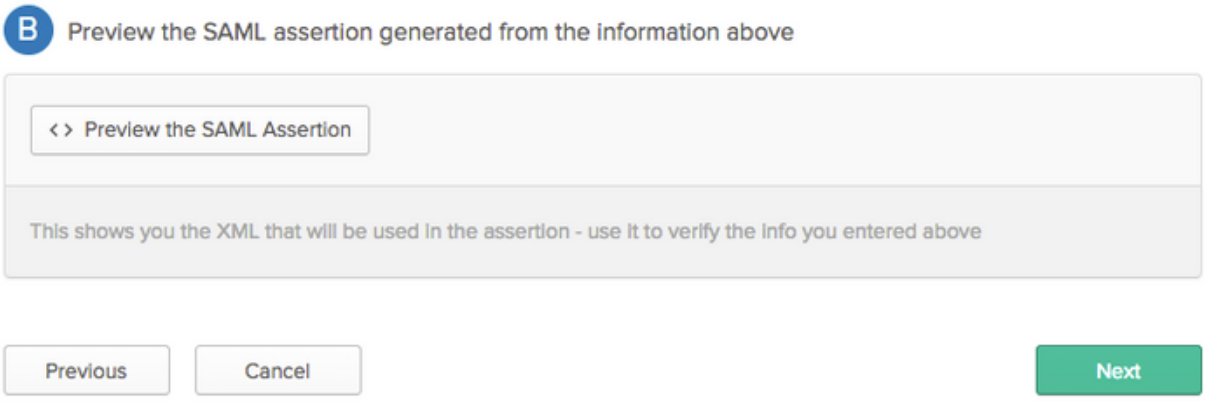
> **Caution**: The selection of format depends on the redirect settings on Authorization profile, if you use static ip then you should use the ip address for SSO URL.

3. OKTA SAML Settings.

Step 1. Add those URLs on SAML settings.



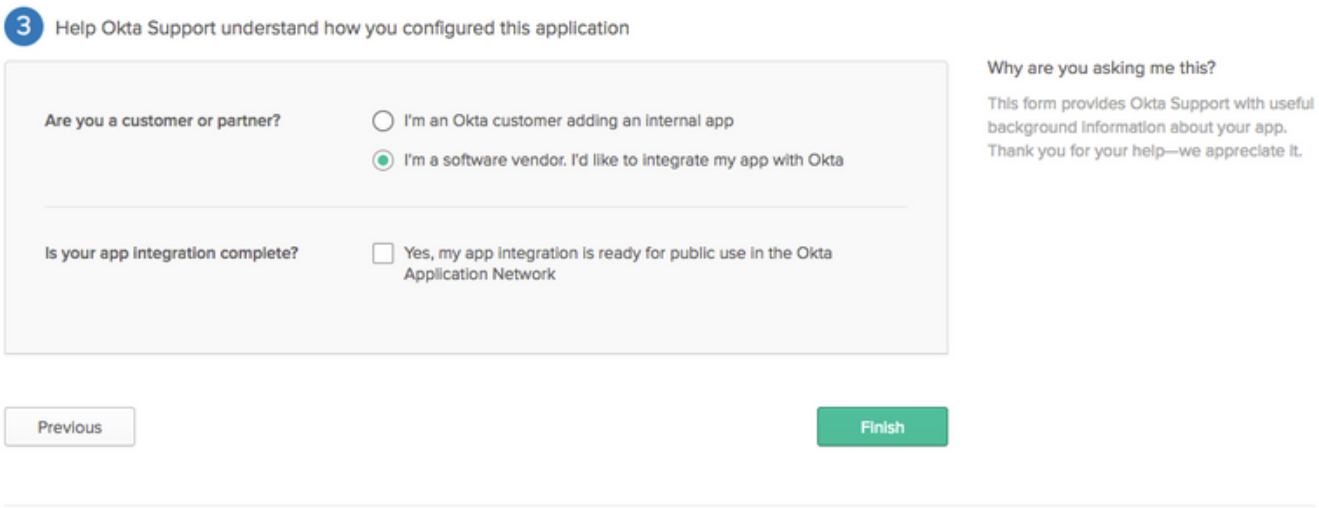
Step 2. You can add more than one URL from the XML file, based on the number of PSN's hosting this service. Name ID format and Application username depend on your design.



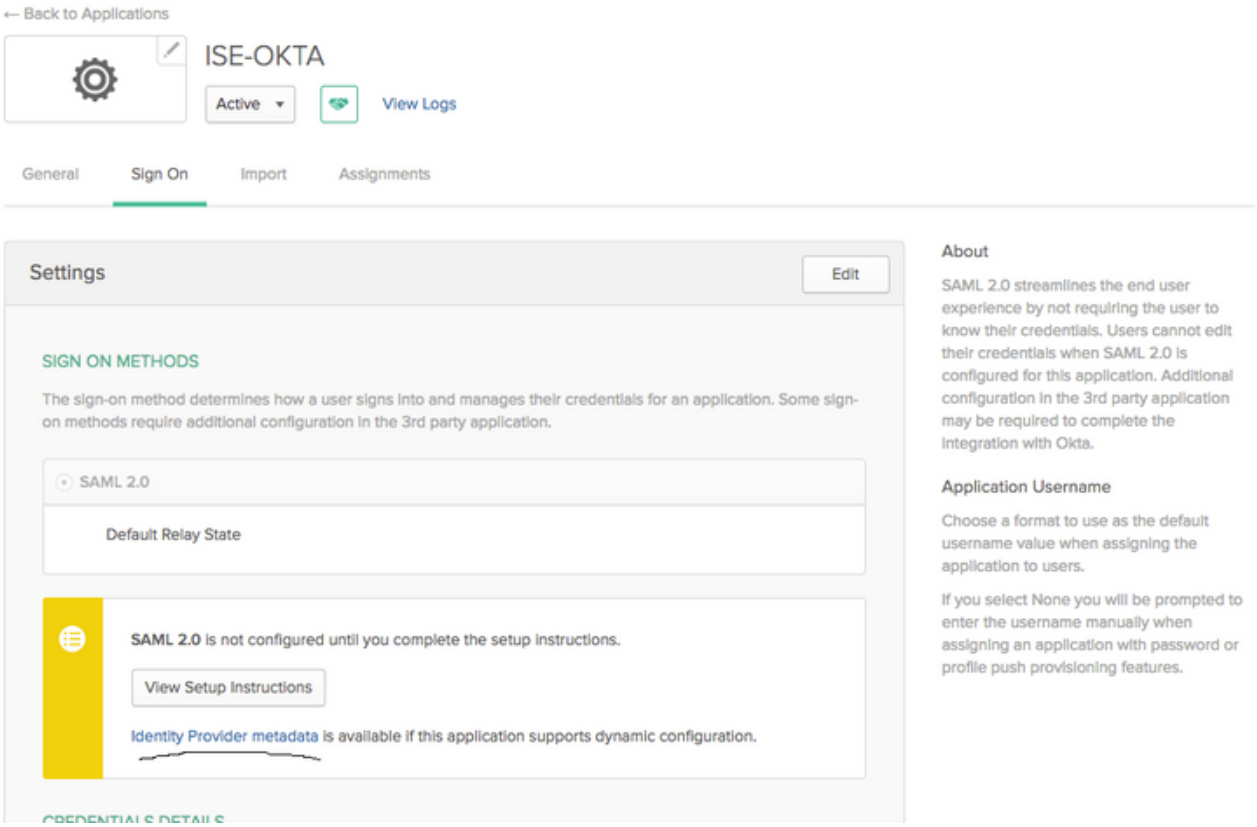

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124"
```

```
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.



4. Export Metadata from the Application.



Metadata:


```
<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>
```

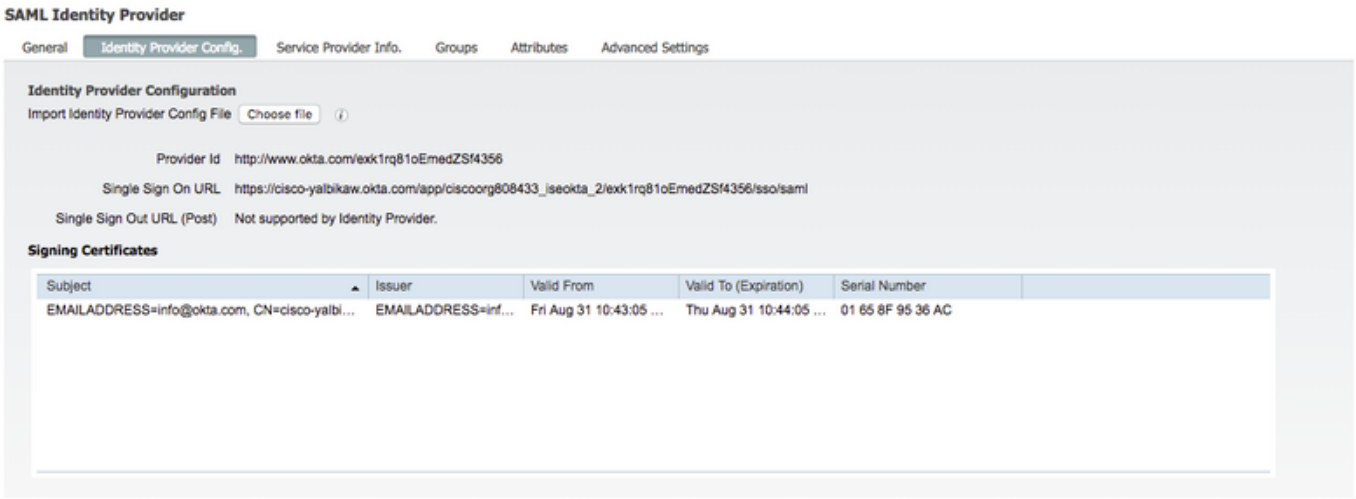
Save the file in XML format.

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.

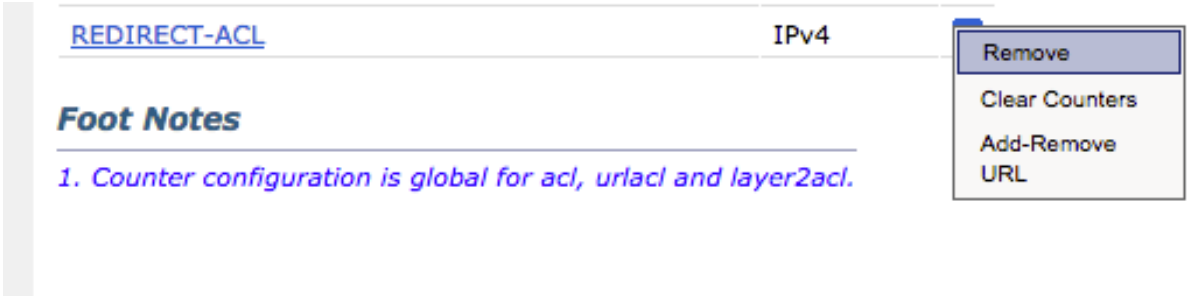
This document describes the configuration for ISE and WLC.

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

Add URLs in Redirect-ACL.

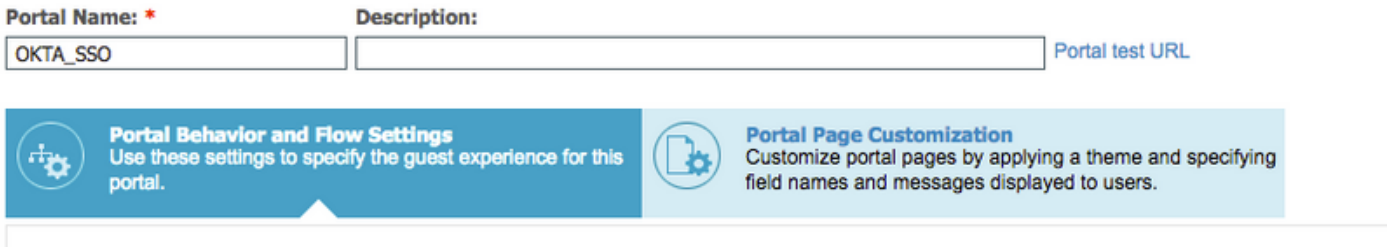
https://cisco-yalbikaw.okta.com / add your Application URL

https://login.okta.com

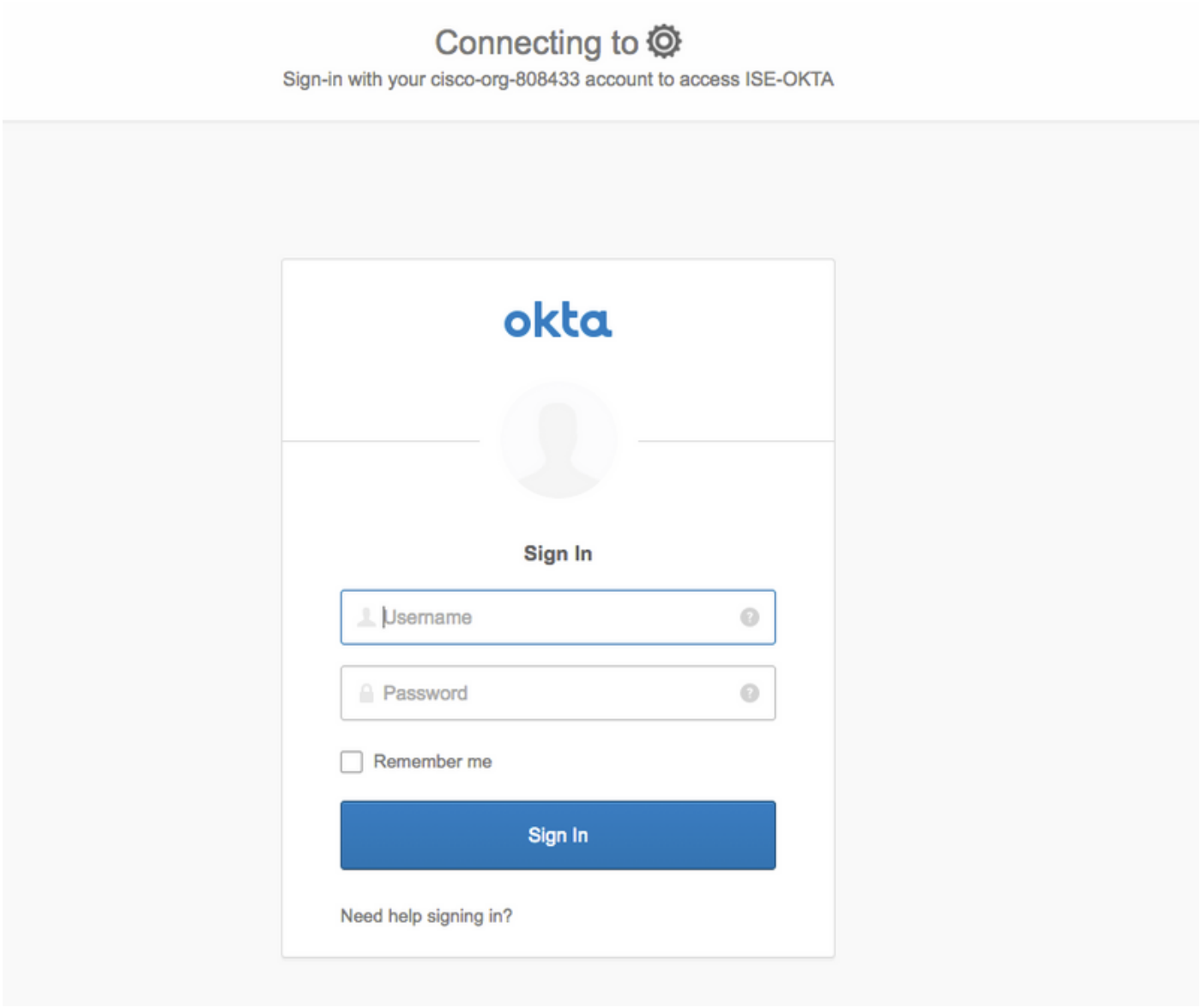


Verify

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



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

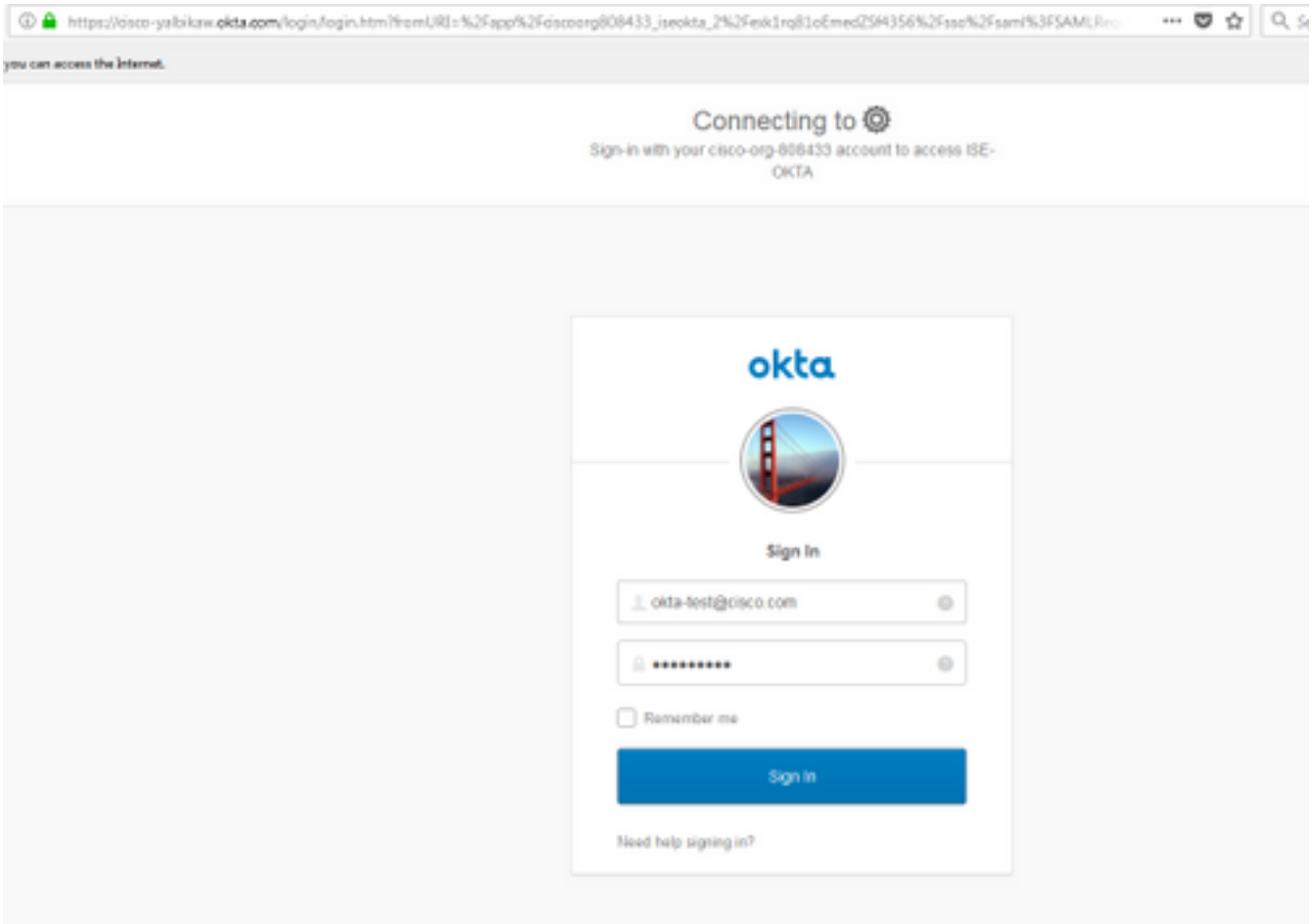


Step 2. Check the information ***connection to <application name>***

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.

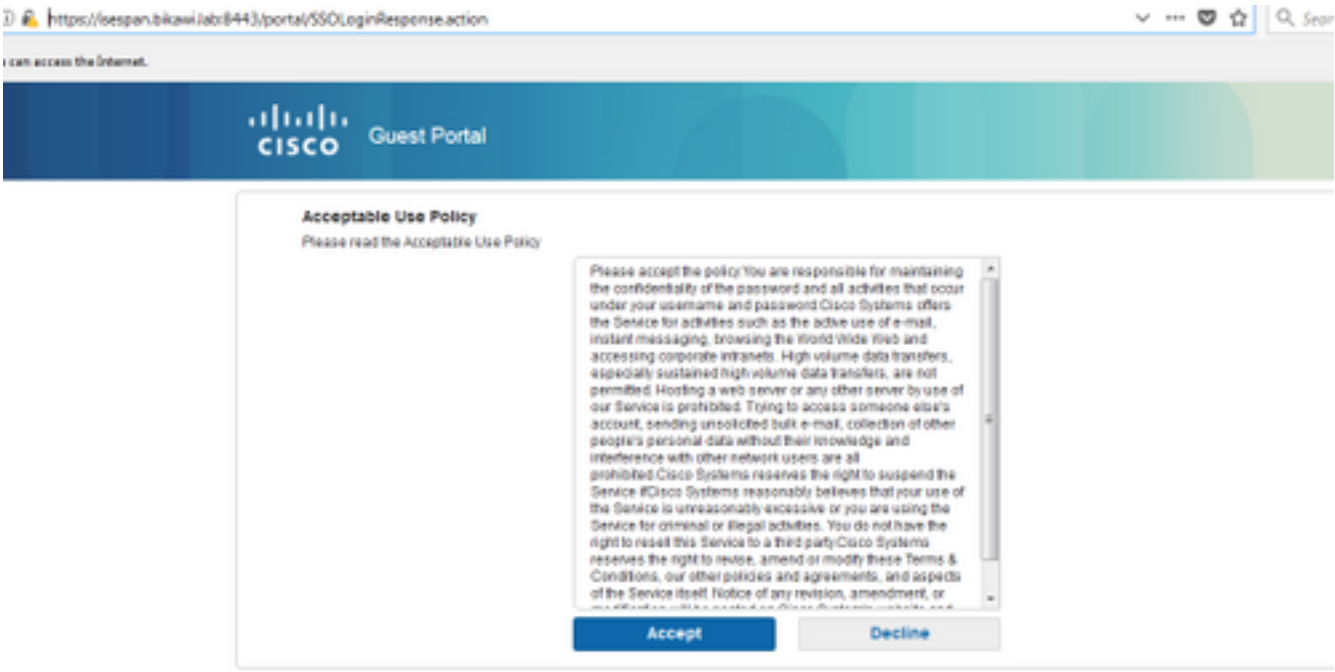
End-user Verification

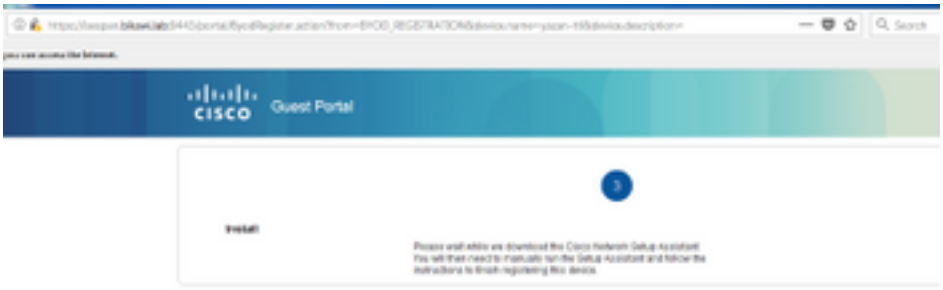

Search
you can access the Internet.
cisco
Guest Portal
Sign On
Sign on for guest access.
Username:
Password:
Sign On
Or register for guest access
You can also login with


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?


https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
before you can access the Internet.


Signing in to ISE-OKTA


https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
can access the Internet.
Guest Portal
Acceptable Use Policy
Please read the Acceptable Use Policy
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or
Accept
Decline



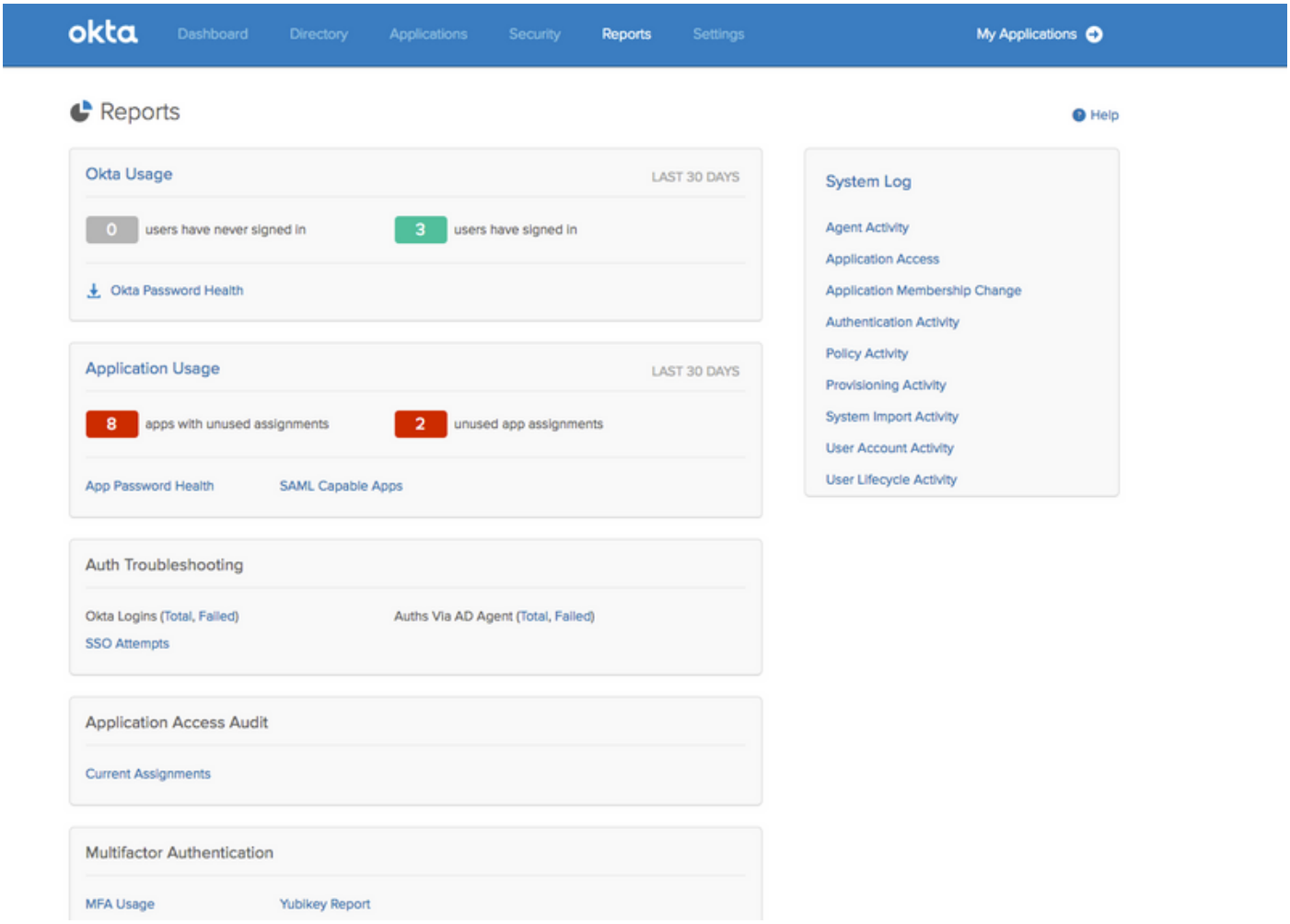
ISE Verification

Check life logs to verify the authentication status.

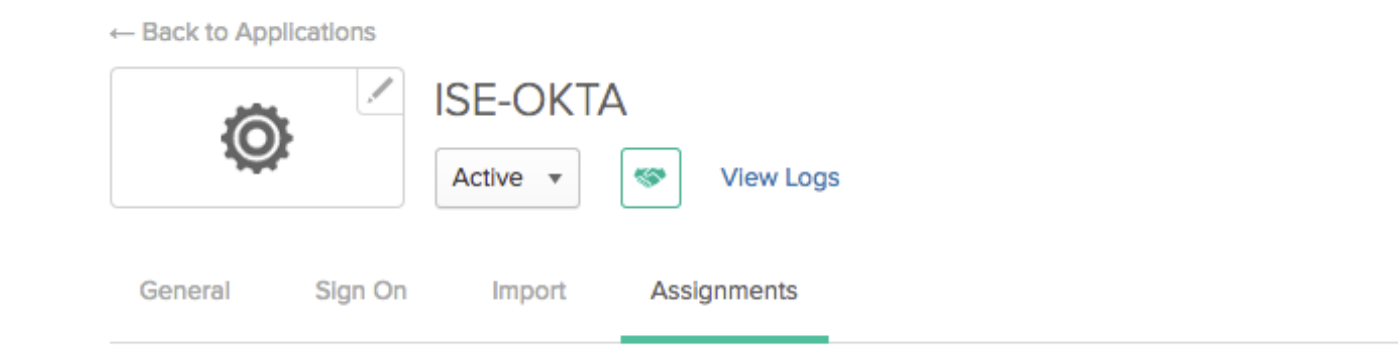
Troubleshoot

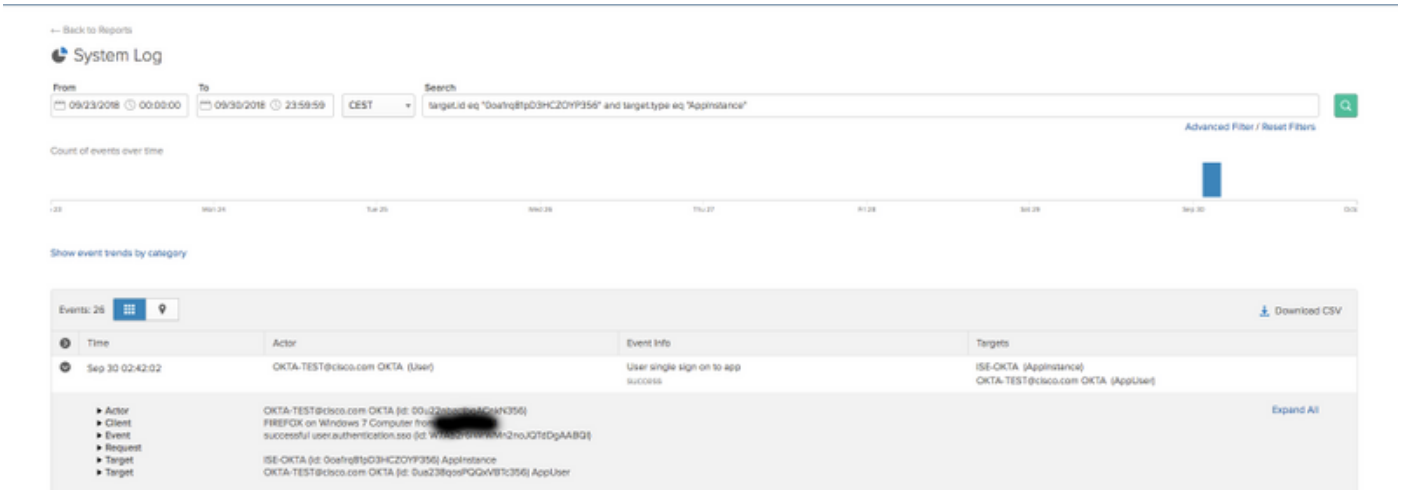
OKTA Troubleshoot

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



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





ISE Troubleshoot

There are two log files to check

- ise-psc.log
- guest.log

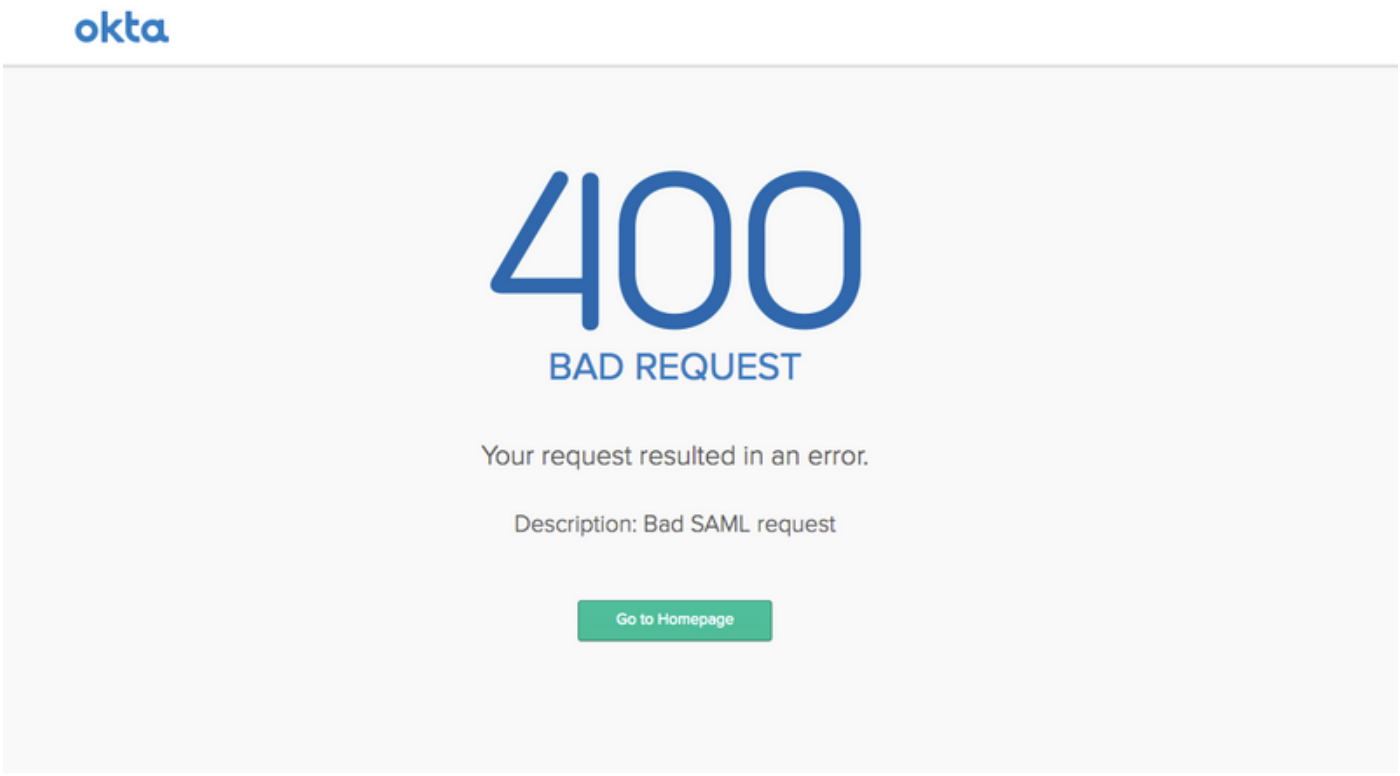
Navigate to **Administration > System > Logging > Debug Log Configuration**. Enable the level to DEBUG.

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

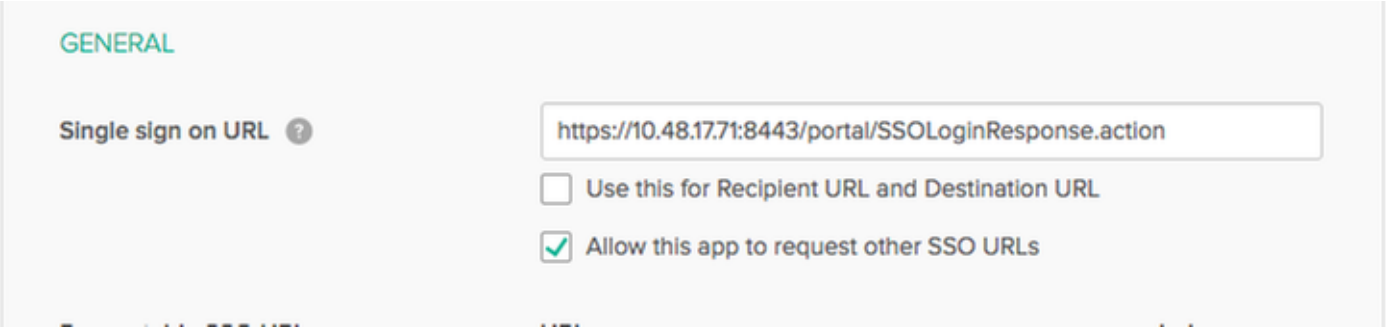
```
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:
SSOLoginTransitionResult:

        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%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 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.

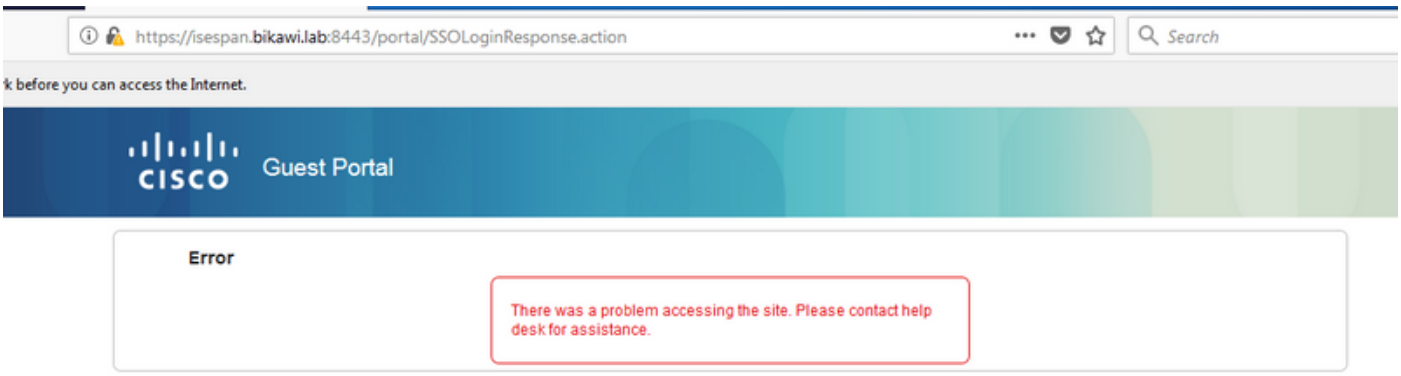
```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0
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
```

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

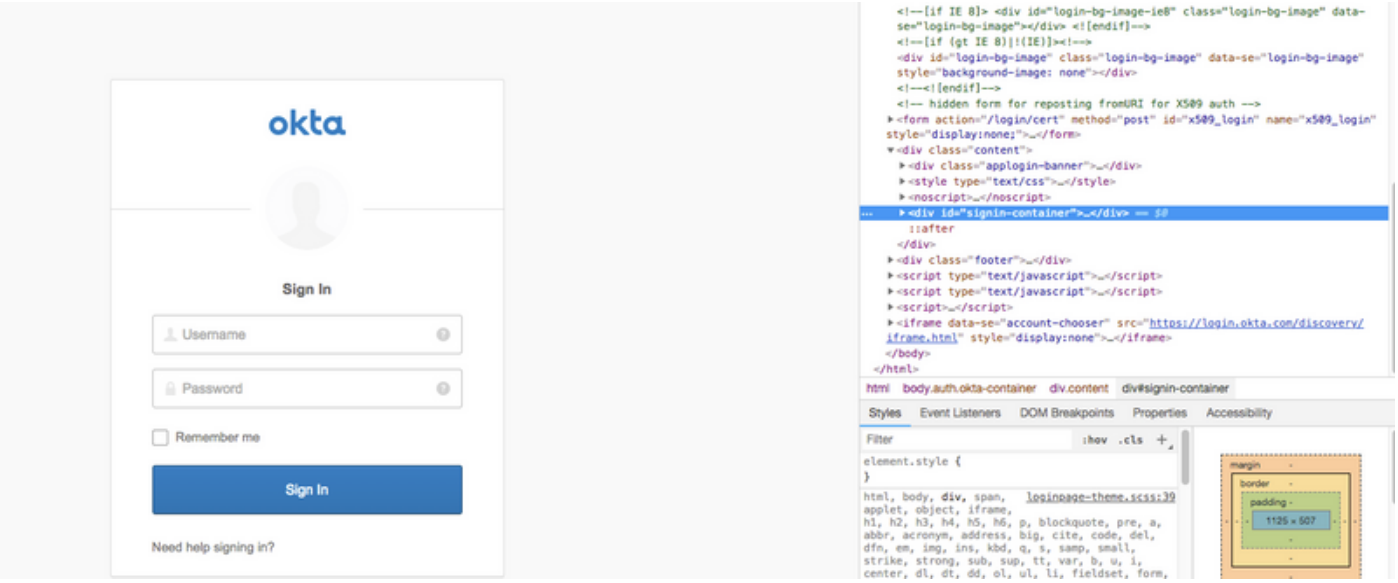
```
2018-09-30 02:25:00,595 ERROR  [https-jsse-nio-10.48.17.71-8443-exec-1][]
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
contain ma
```

```
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