OKTA SAML SSOによるISE 2.3ゲストポータルの設定

内容

概要

このドキュメントでは、Identity Services Engine(ISE)をOKTAと統合して、ゲストポータルにSecurity Assertion Markup Language(SAML)シングルサインオン(SSO)認証を提供する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine ゲスト サービス
- SAML SSO
- （オプション）ワイヤレスLANコントローラ(WLC)の設定。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)2.3.0.298
- OKTA SAML SSOアプリケーション
- Cisco 5500ワイヤレスコントローラバージョン8.3.141.0
- Lenovo Windows 7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

フェデレーテッドSSO

組織内のユーザは1回だけ認証を行い、複数のリソースにアクセスできます。組織全体で使用されるこのIDは、連合IDと呼ばれます。

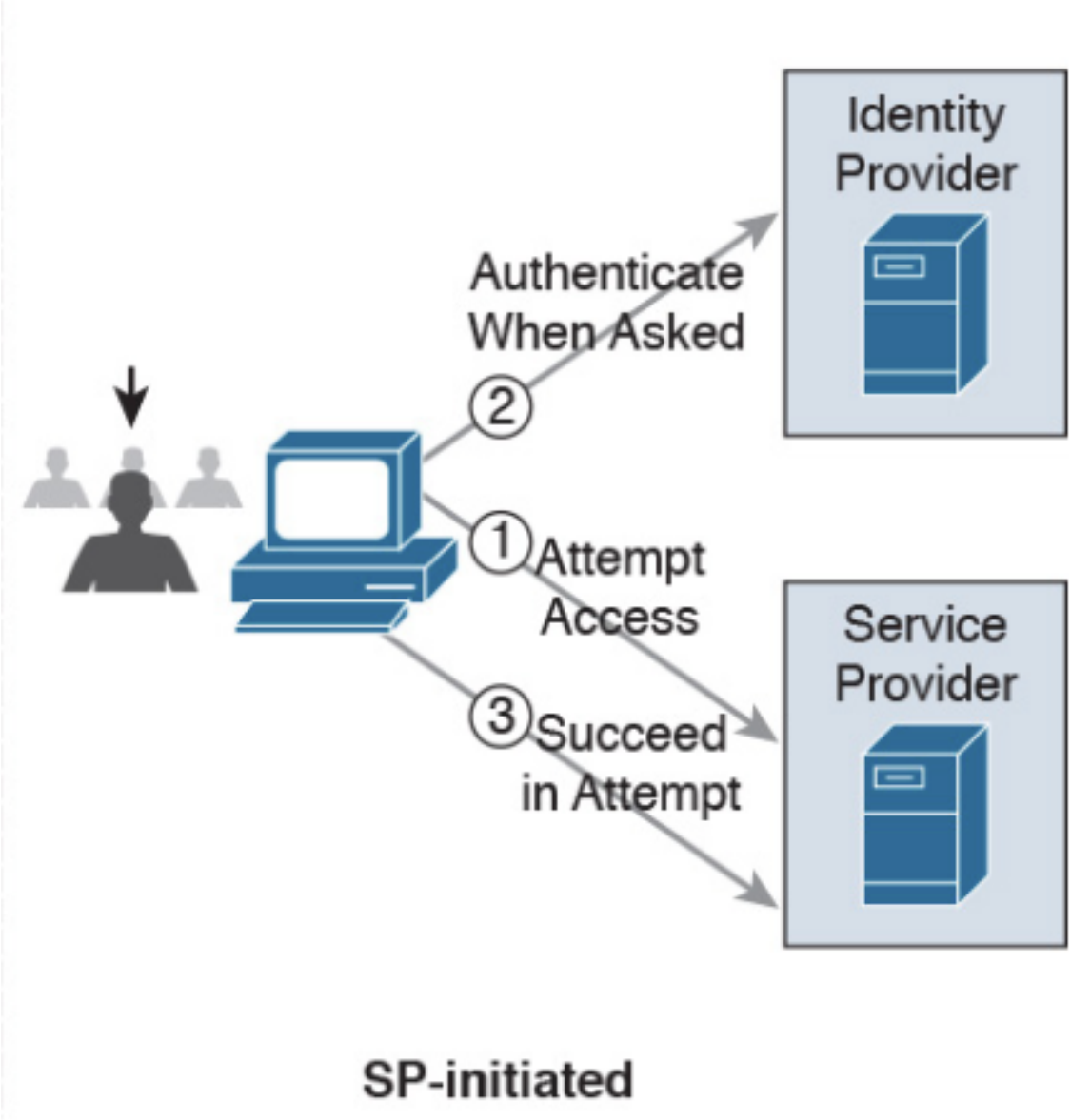
フェデレーションの概念：

- 原則：エンドユーザ（サービスを要求するユーザ）であるWebブラウザ（この場合はエンドポイント）です。
- サービスプロバイダー(SP):証明書利用者(RP)とも呼ばれ、これはサービスを提供するシステムであり、この場合はISEです。
- アイデンティティプロバイダー(IdP):SPに送り返される認証、許可結果、属性（この場合はOKTA）を管理します。
- アサーション：IdPからSPに送信されるユーザ情報。

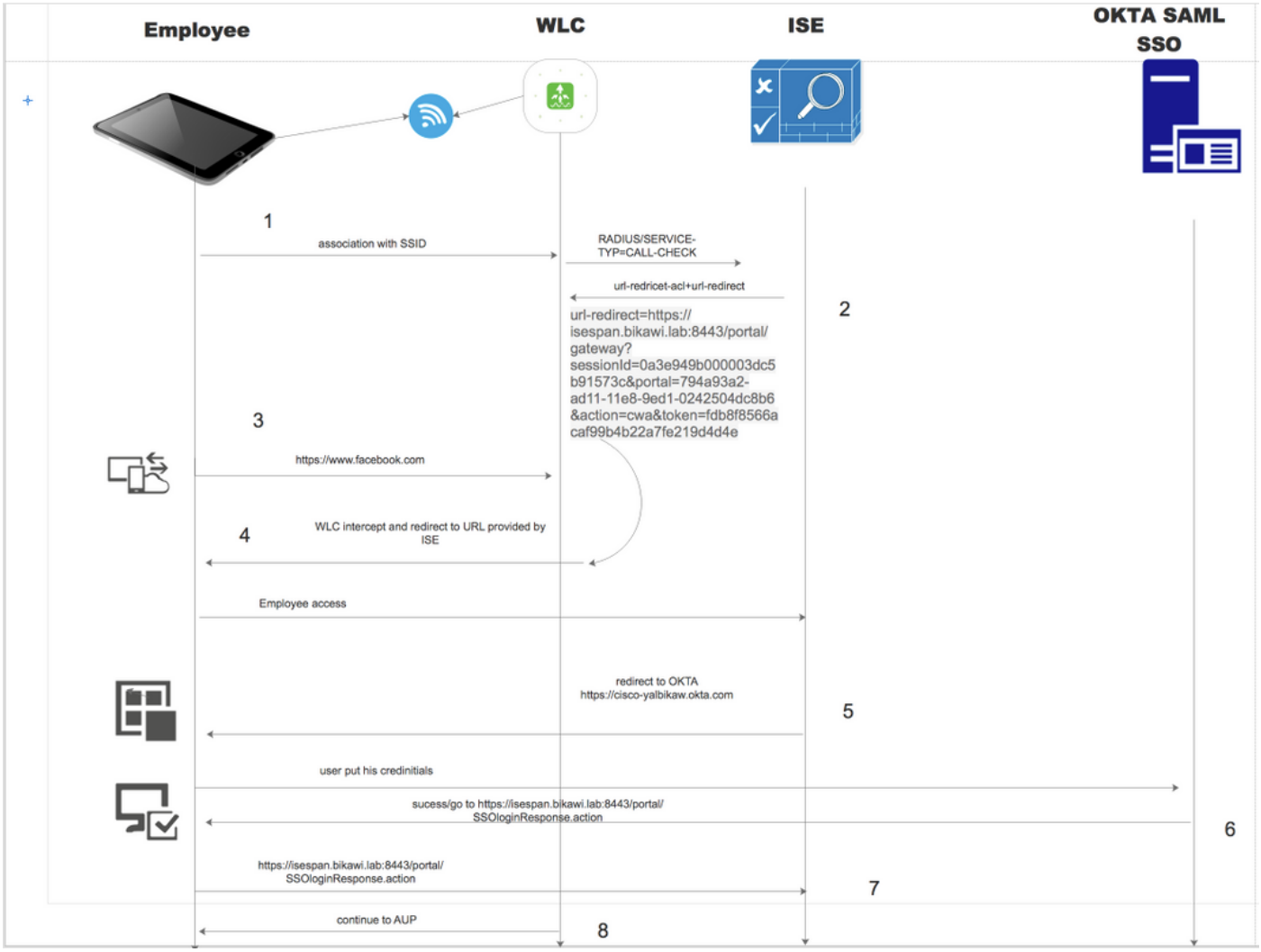
OAuth2やOpenIDなどのSSOを実装するプロトコルがいくつかあります。ISEはSAMLを使用します。

SAMLは、XMLベースのフレームワークで、ビジネスエンティティ間でのSAMLアサーションの使用と交換を安全に記述します。標準では、これらのアサーションを要求、作成、使用、および交換するための構文とルールについて説明します。

ISEはSP開始モードを使用します。ユーザはゲストポータルにリダイレクトされ、ISEはこれを認証のためにIdPにリダイレクトします。その後、ISEにリダイレクトして戻ります。リクエストが検証され、ユーザはポータルの設定に応じてゲストアクセスまたはオンボーディングを続行します。


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

ネットワーク フロー



1. ユーザはSSIDに接続し、認証はmacフィルタリング(mab)です。

2. ISEは、リダイレクトURLおよびリダイレクトACL属性を含むaccess-acceptで応答します
3. ユーザーがwww.facebook.comにアクセスしようとします。
4. WLCは要求をインターセプトし、ユーザをISEゲストポータルにリダイレクトします。ユーザは従業員アクセスをクリックして、デバイスをSSOクレデンシャルで登録します。
5. ISEは、認証のためにユーザをOKTAアプリケーションにリダイレクトします。
6. 認証に成功すると、OKTAはSAMLアサーション応答をブラウザに送信します。
7. ブラウザがアサーションをISEにリレーします。
8. ISEはアサーション応答を確認し、ユーザが正しく認証されると、AUPに進み、デバイス登録を行います。

SAMLの詳細については、次のリンクを参照してください

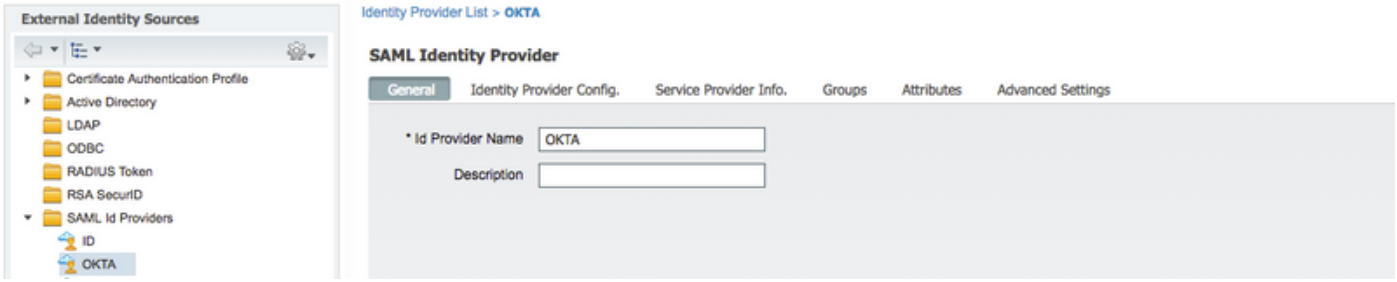
https://developer.okta.com/standards/SAML/

設定

ステップ1:ISEでSAML IDプロバイダーとゲストポータルを設定します。

1.外部アイデンティティソースの準備

ステップ1:[Administration] > **[External Identity Sources] > [SAML id Providers]に移動します。**

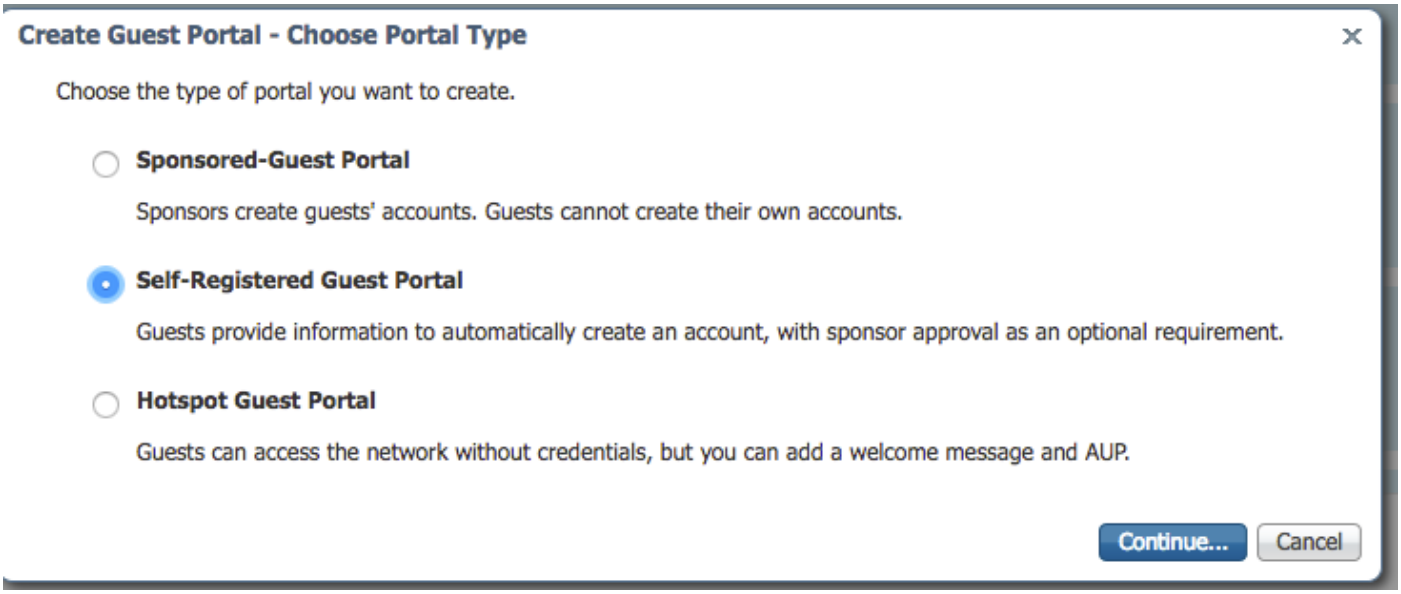


ステップ2:idプロバイダーに名前を割り当て、設定を送信します。

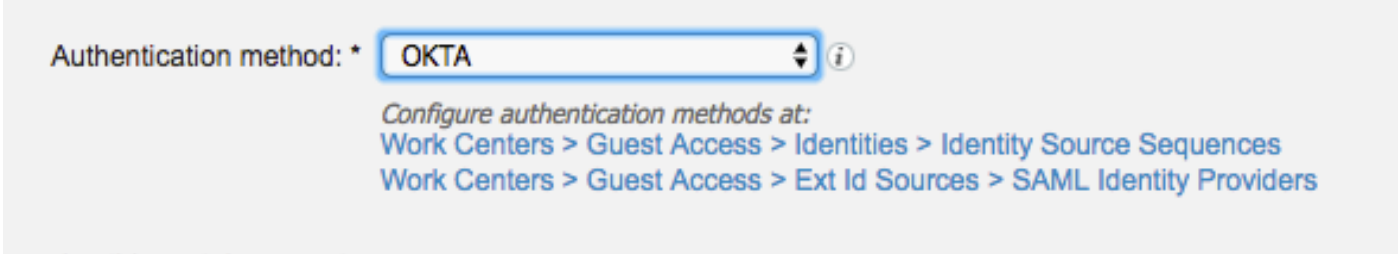
2. SSOのポータルを作成します。

ステップ1：アイデンティティソースとしてOKTAに割り当てられているポータルを作成します。BYOD、デバイス登録、ゲストなどの他の設定は、通常のポータルとまったく同じです。このドキュメントでは、ポータルが従業員の代替ログインとしてゲストポータルにマッピングされます。

ステップ2:[Work Centers] > [**Guest Access] > [Portals & Components]に移動し、**ポータルを作成します。

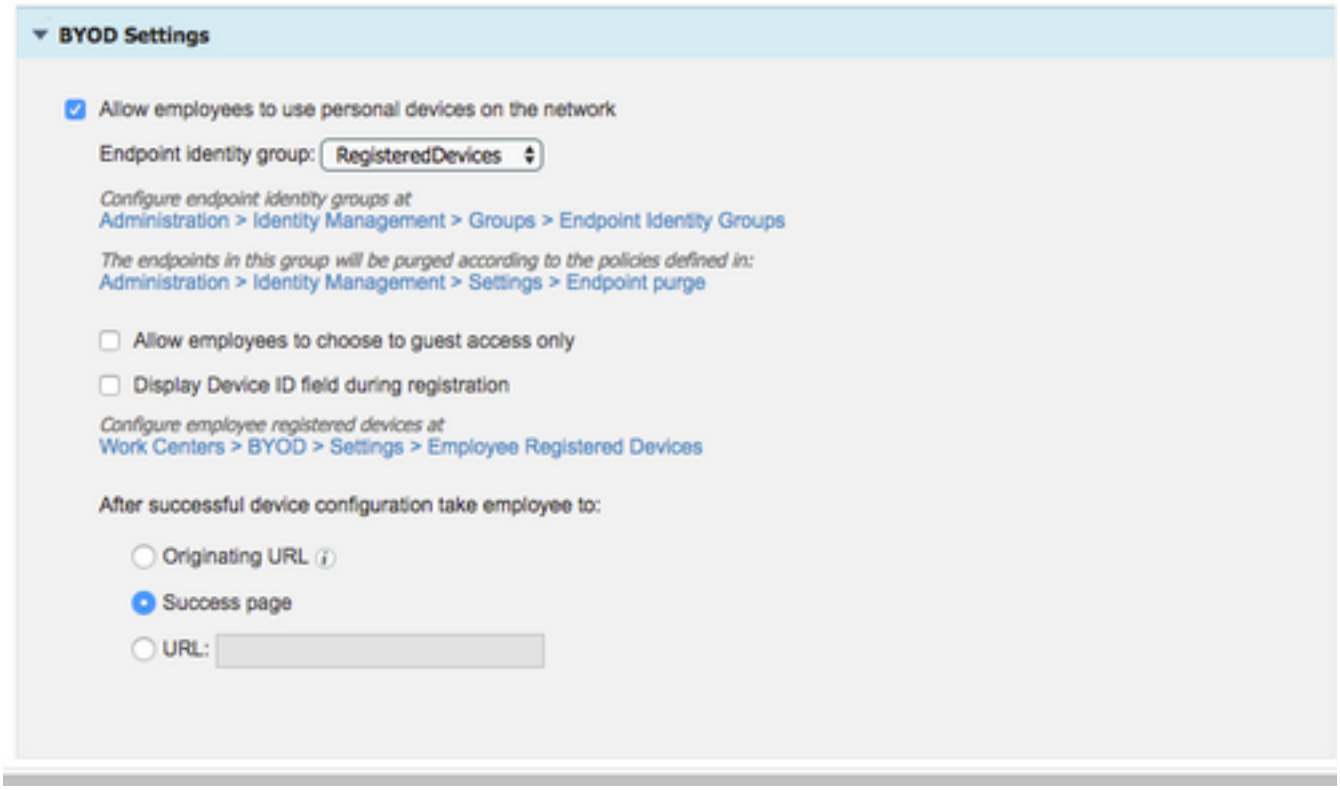


ステップ3：以前に設定したIDプロバイダーをポイントする認証方法を選択します。

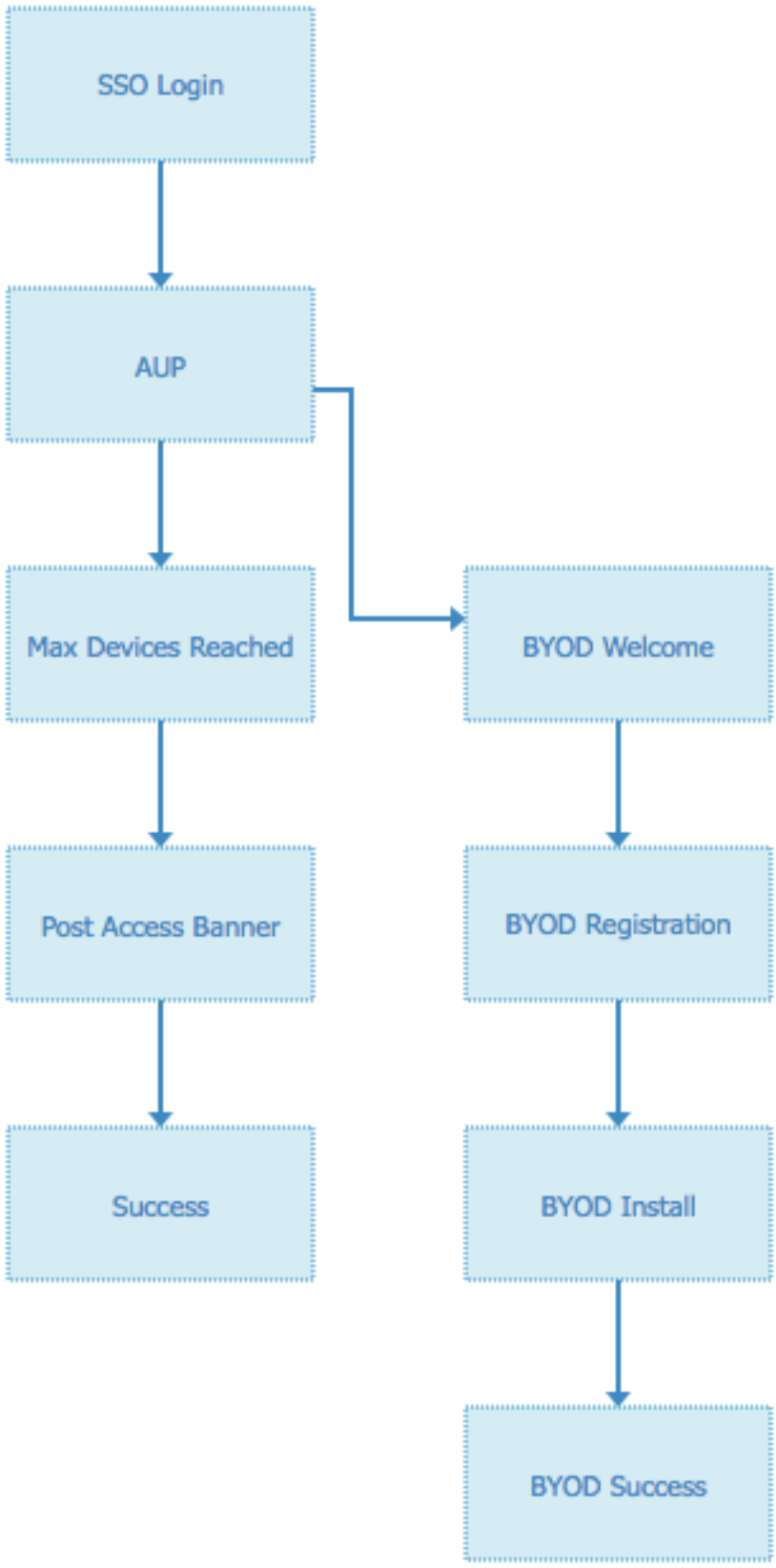


ステップ4：認証方式として[OKTA identity source]を選択します。

（オプション）BYOD設定を選択します。



ステップ5:BYODでポータル設定を保存します。フローは次のようになります。



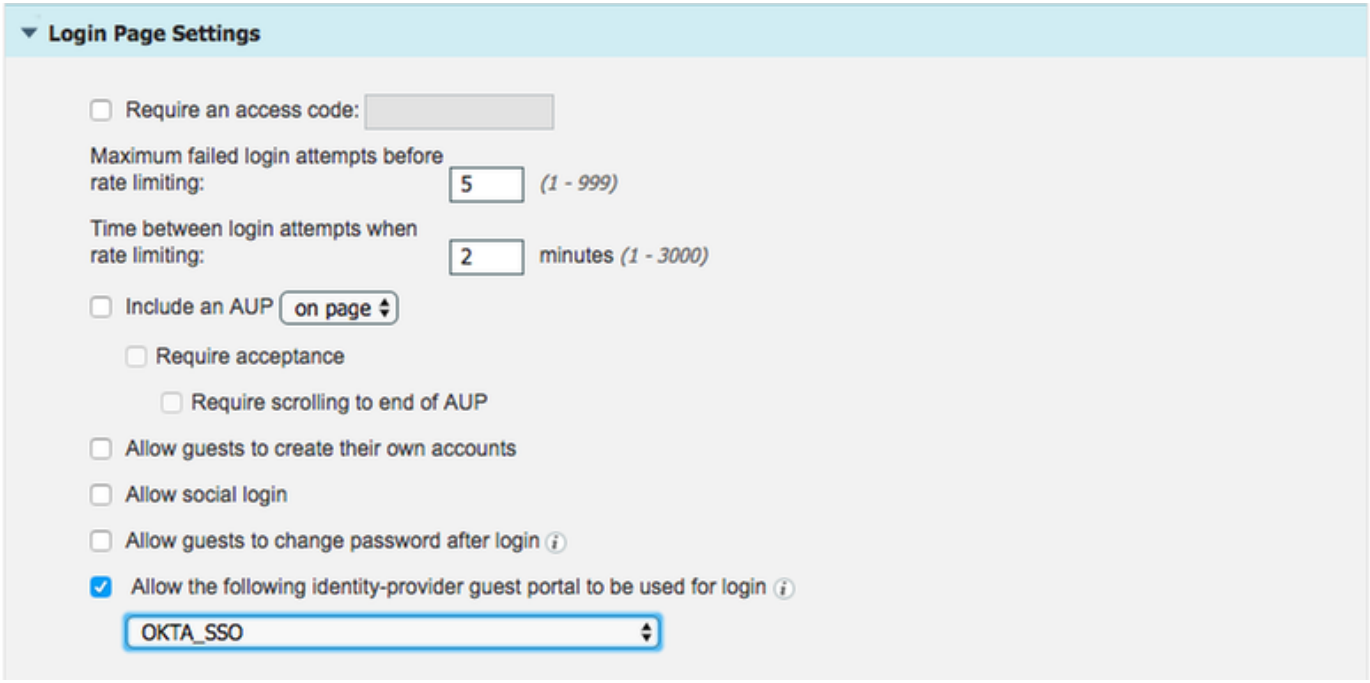
3.代替ログインの設定

注：代替ログインを使用していない場合は、この部分をスキップできます。

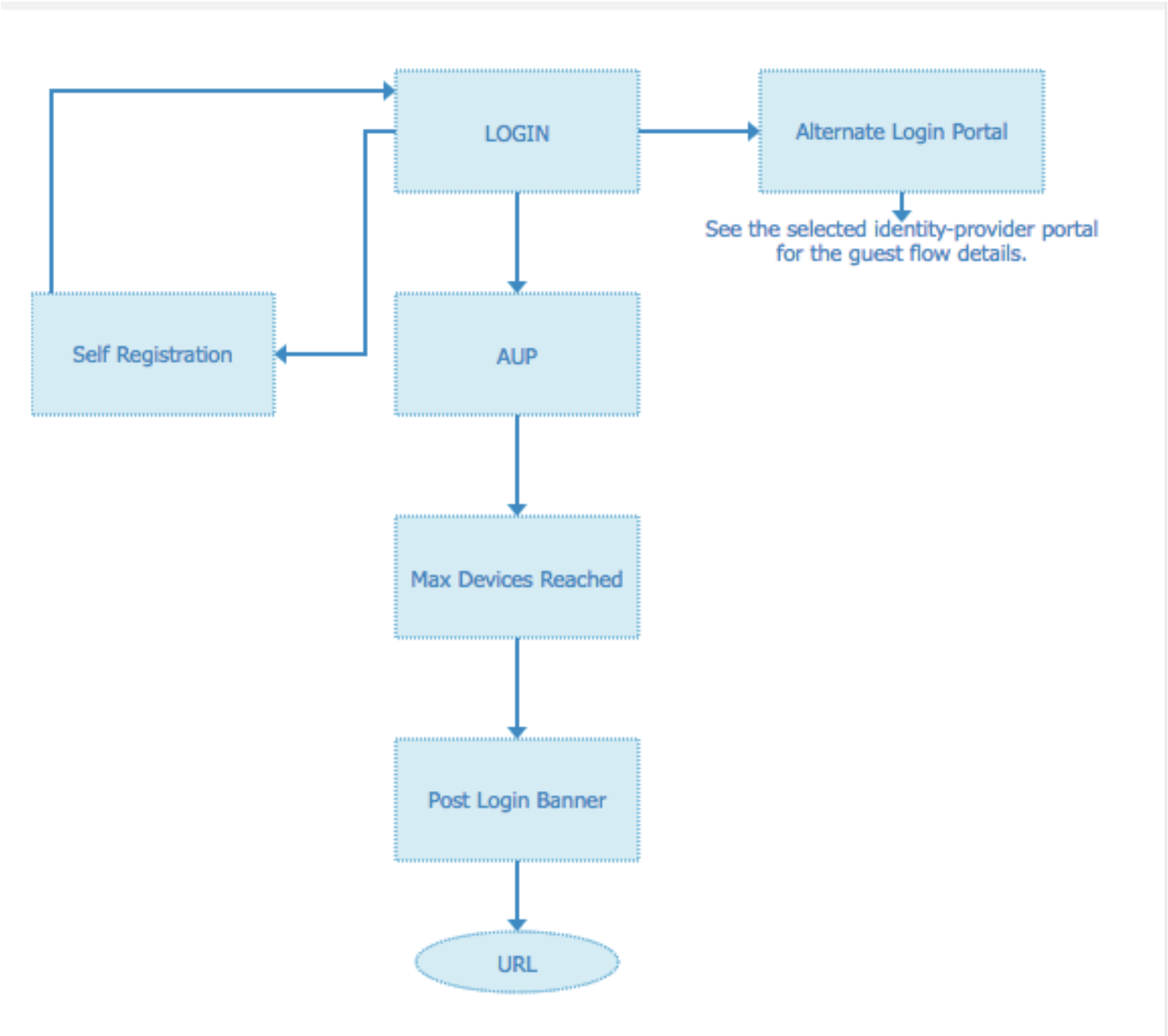
自己登録ゲストポータル、またはゲストアクセス用にカスタマイズされたその他のポータルに移

動します。

ログインページの設定で、代替ログインポータルを追加します。OKTA_SSO。



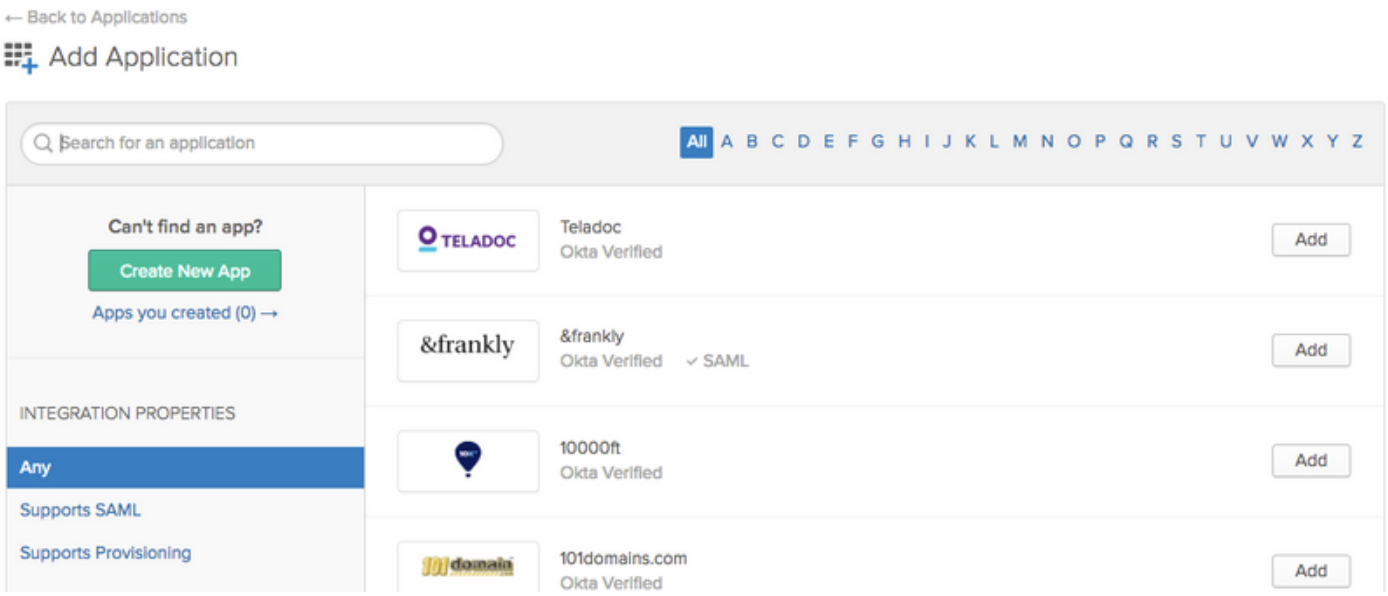
これがポータルフローです。



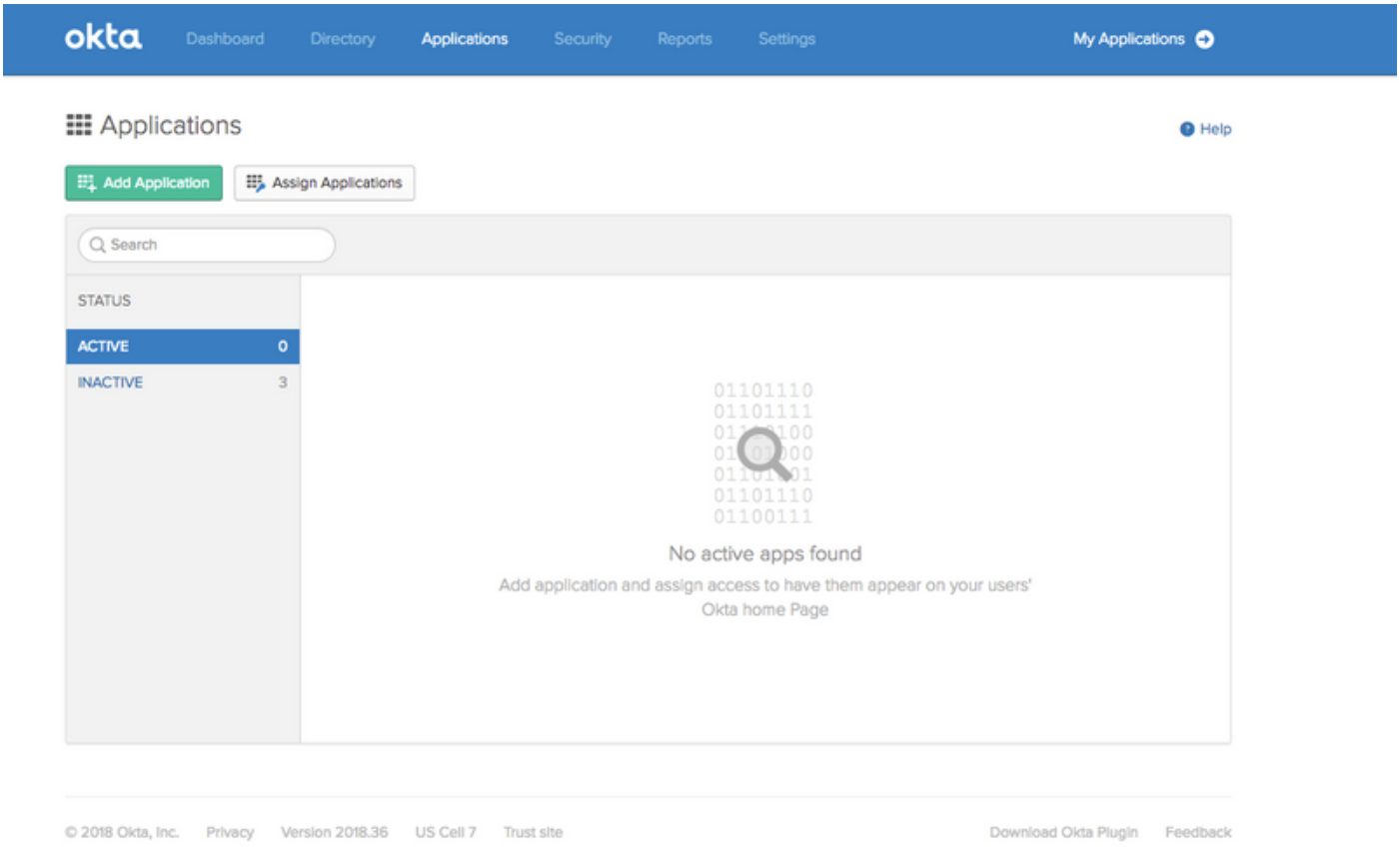
ステップ2:OKTAアプリケーションとSAML IDプロバイダーの設定を行います。

1. OKTAアプリケーションを作成します。

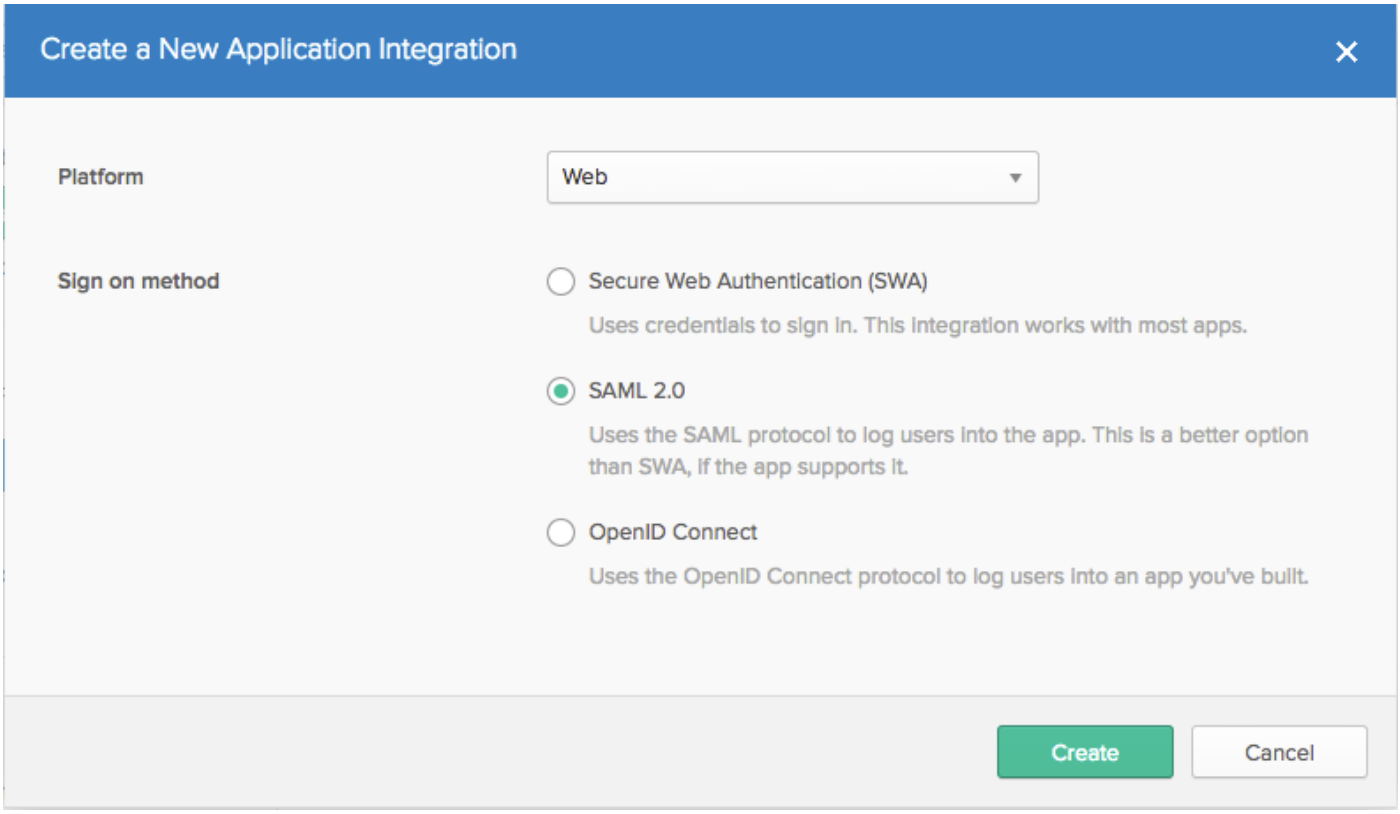
ステップ1：管理者アカウントでOKTA Webサイトにログインします。



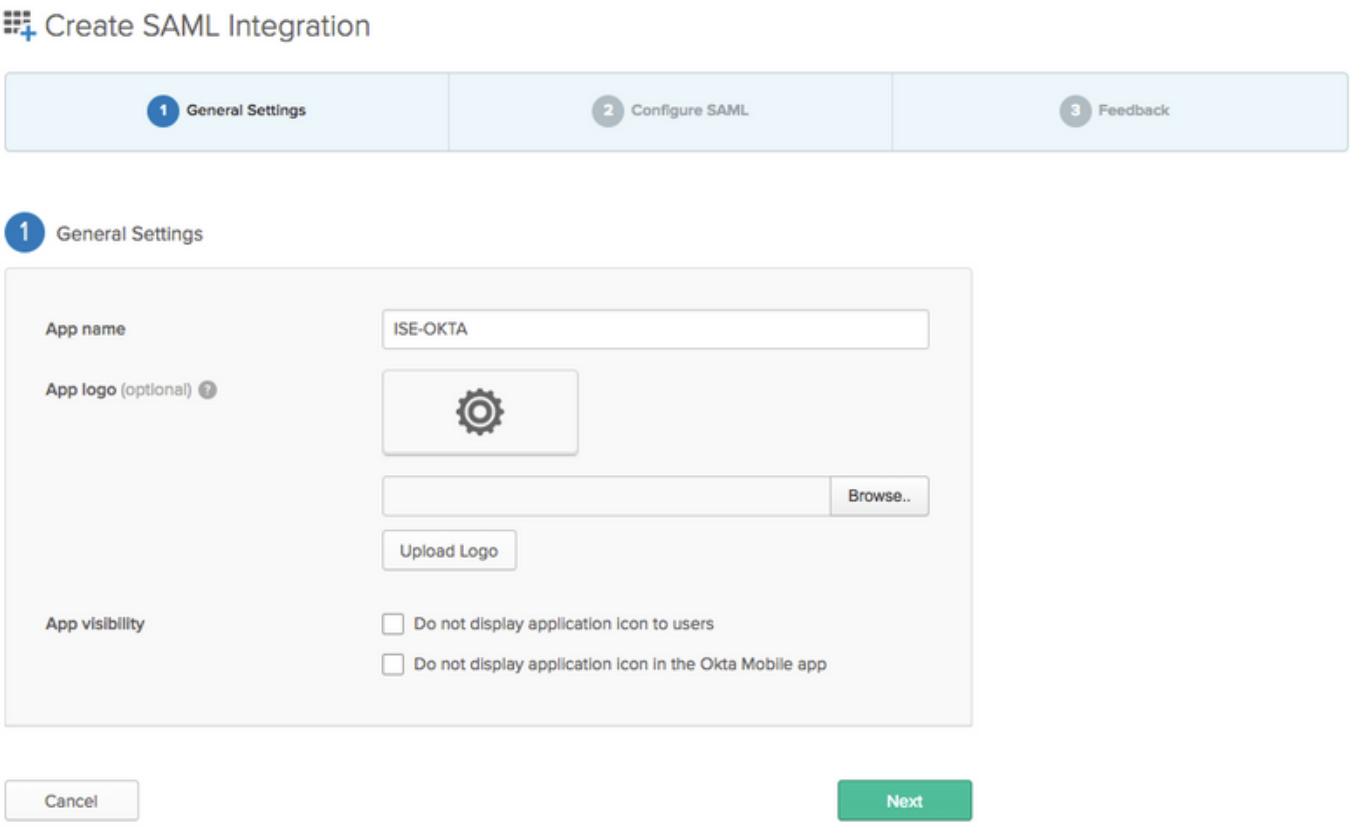
ステップ2:[Add Application]をクリックします。

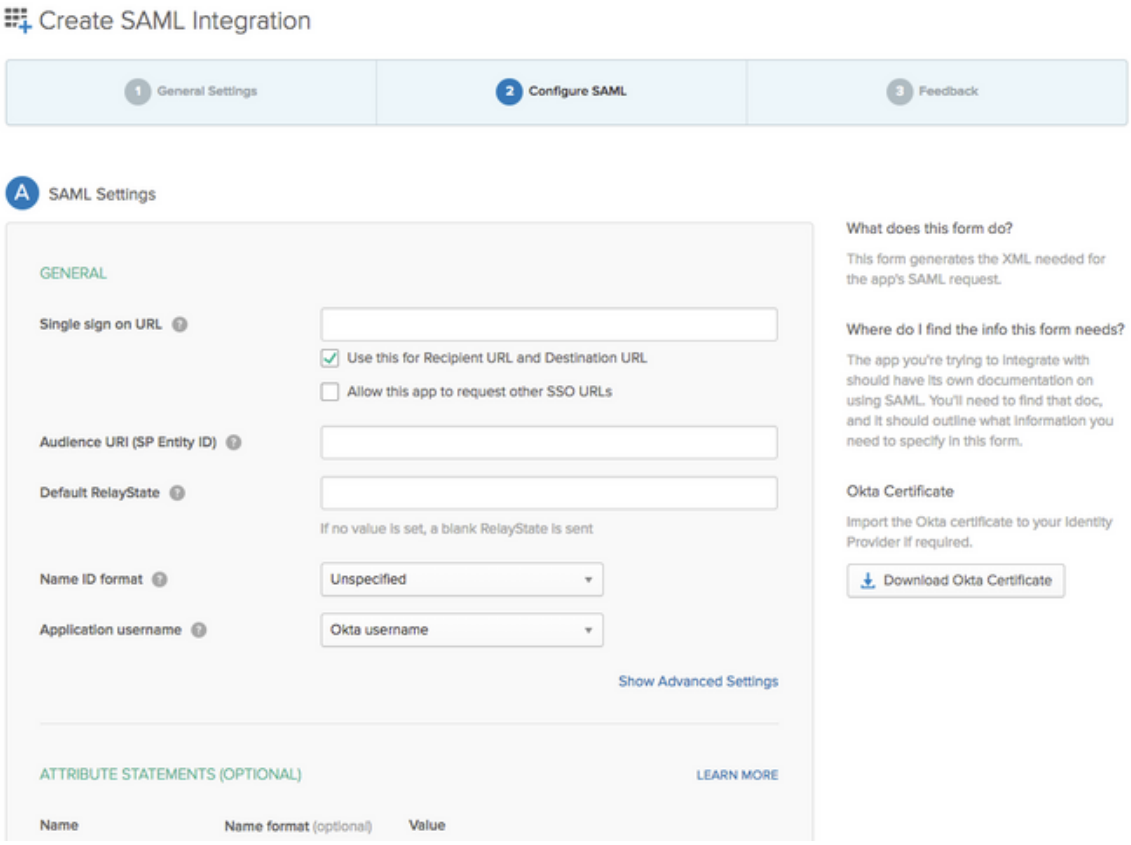


ステップ3：新しいアプリケーションを作成し、SAML2.0を選択します

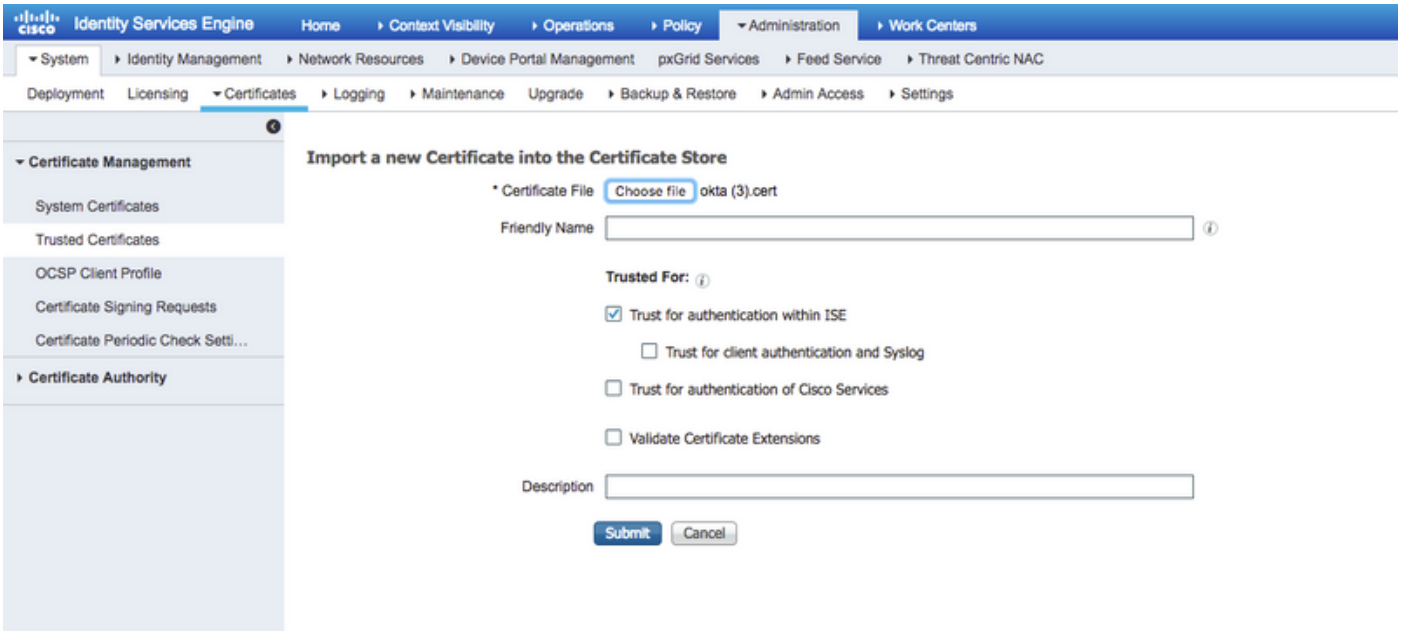

Create a New Application Integration
Platform
Web
Sign on method
Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
OpenID Connect
Uses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

一般設定


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

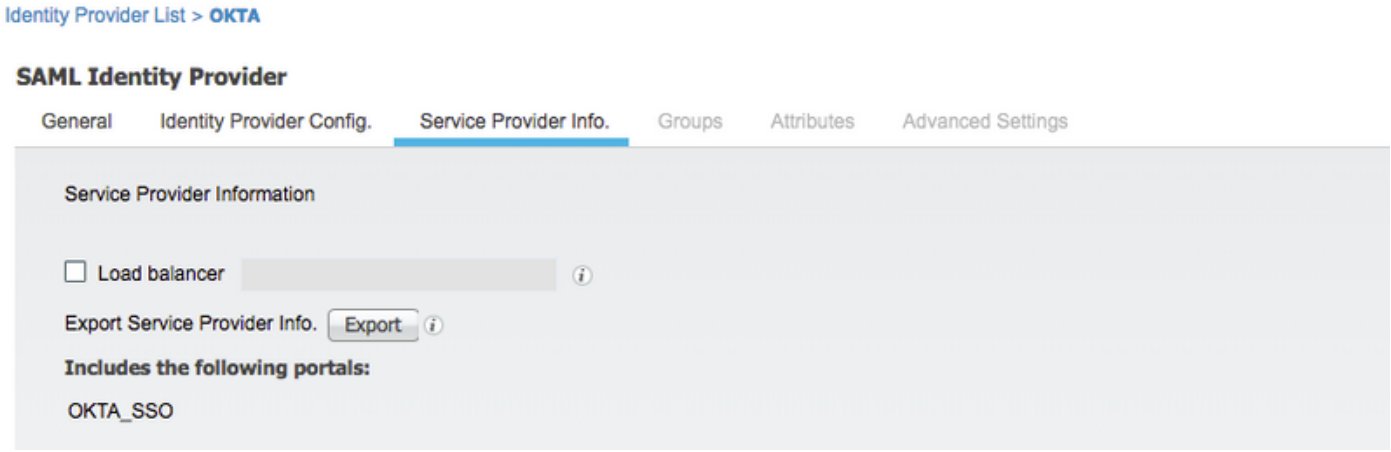


ステップ4：証明書をダウンロードし、ISEの[Trusted Certificates]にインストールします。



2. SAML Identity ProviderからSP情報をエクスポートします。

以前に設定したアイデンティティプロバイダーに移動します。図に示すように、[Service Provider Info]をクリックしてエクスポートします。



エクスポートされたzipフォルダには、XMLファイルとreadme.txtが含まれます

一部のアイデンティティプロバイダーではXMLを直接インポートできますが、この場合は手動でインポートする必要があります。

- シングルサインオンURL（samlアサーション）

```
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エンティティID

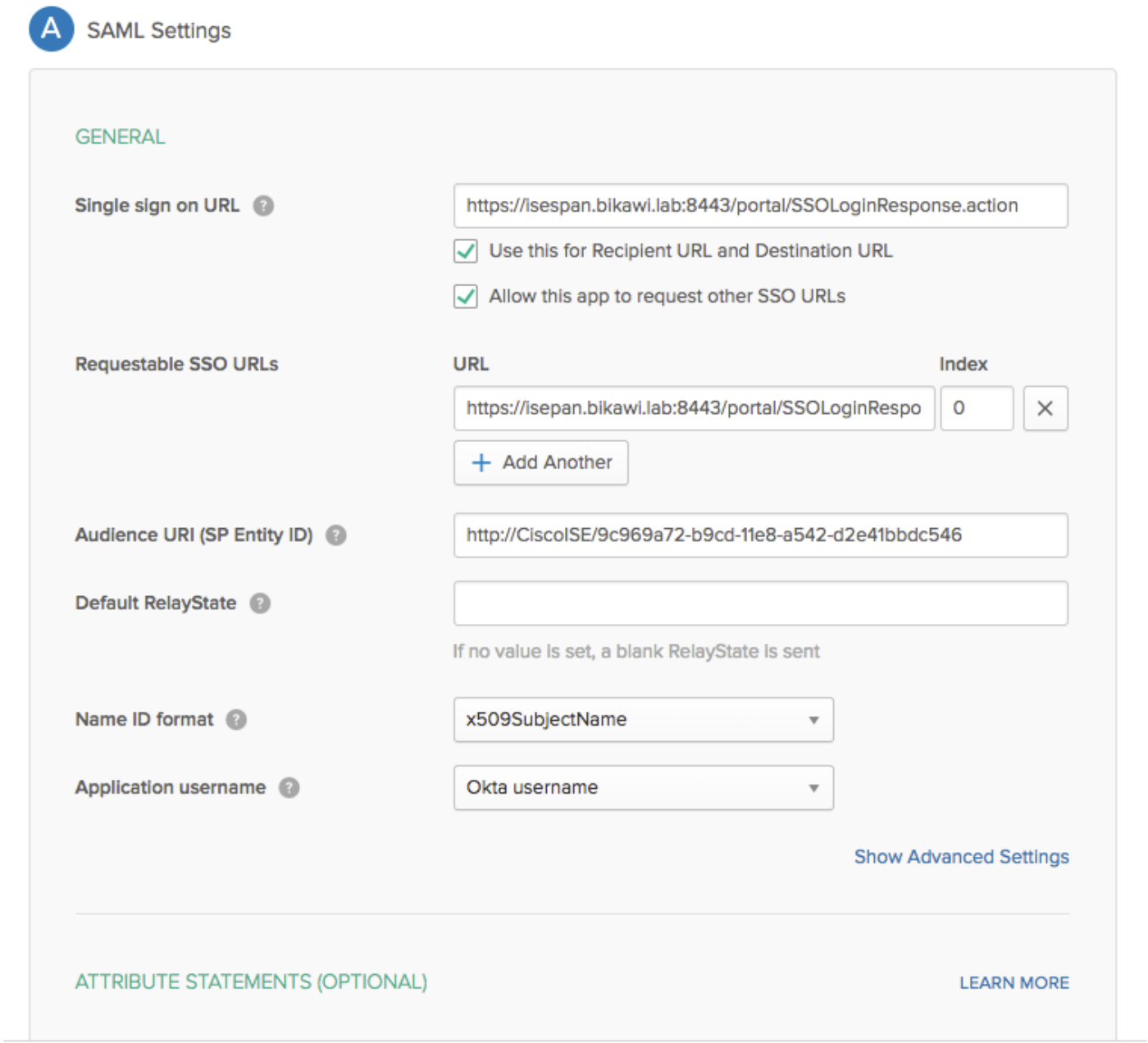
```
entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"
```

IPアドレスおよびFQDN形式で使用可能なSSO URL。

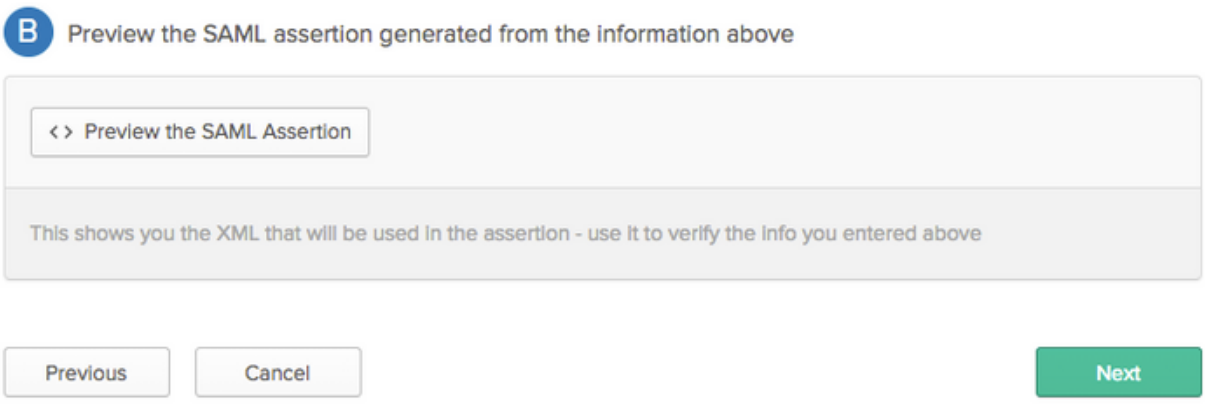
> **注意**：形式の選択は、認可プロファイルのリダイレクト設定によって異なります。static ipを使用する場合は、SSO URLにIPアドレスを使用する必要があります。

3. OKTA SAML設定

ステップ1:SAML設定でこれらのURLを追加します。



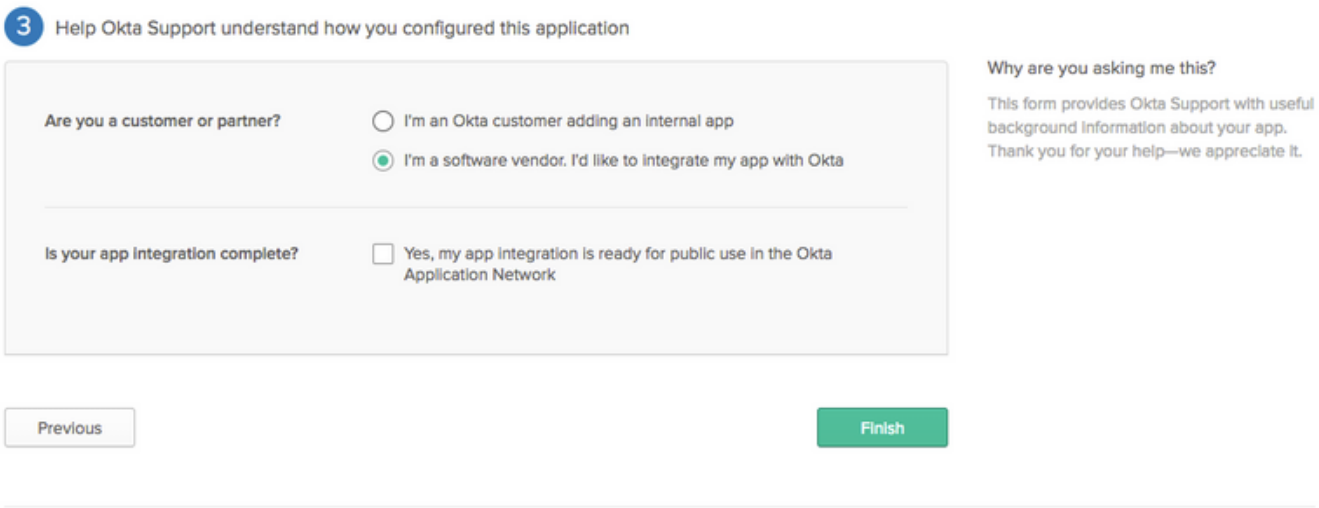
ステップ2：このサービスをホストしているPSNの数に基づいて、XMLファイルから複数のURLを追加できます。名前ID形式とアプリケーションユーザ名は、設計によって異なります。



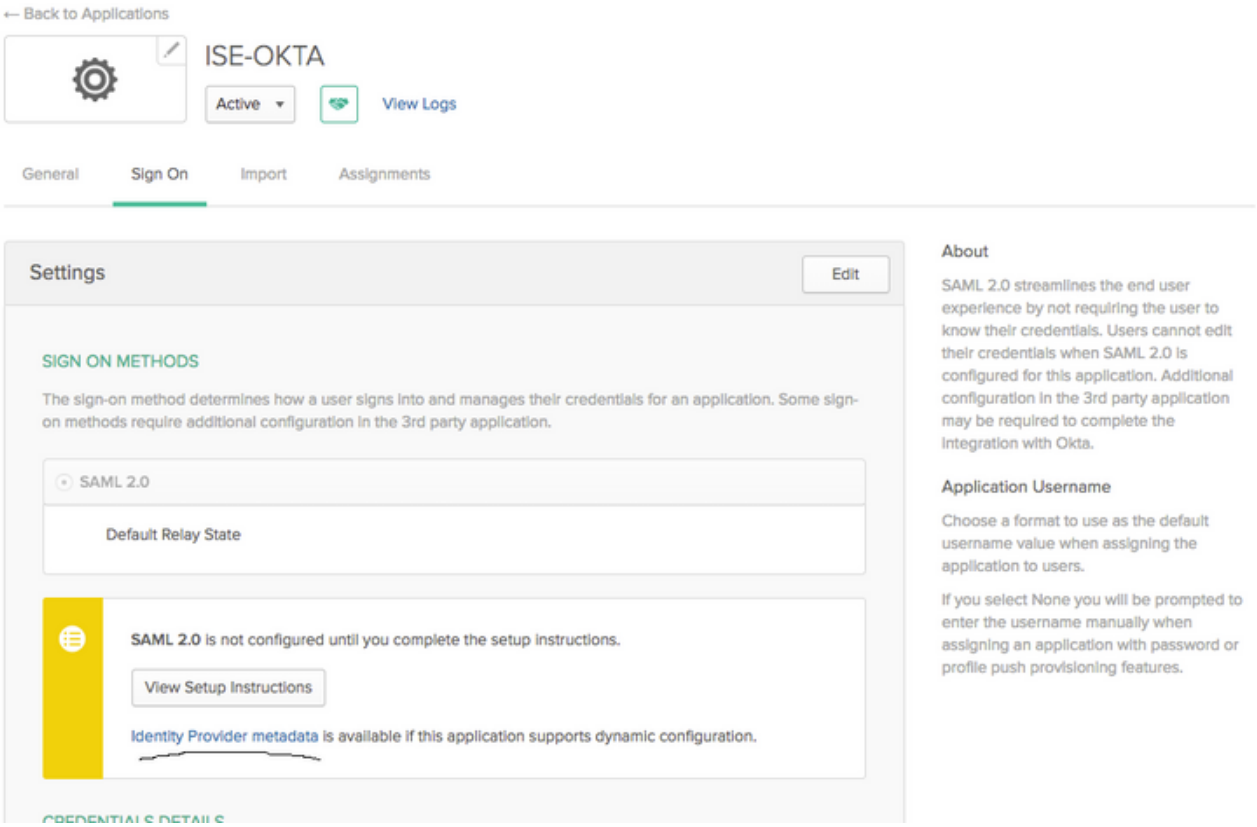

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124"
```

```
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>
```

ステップ3:[next]をクリックし、2番目のオプションを選択します。



4.アプリケーションからメタデータをエクスポートします。



メタデータ:

```
<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>
```

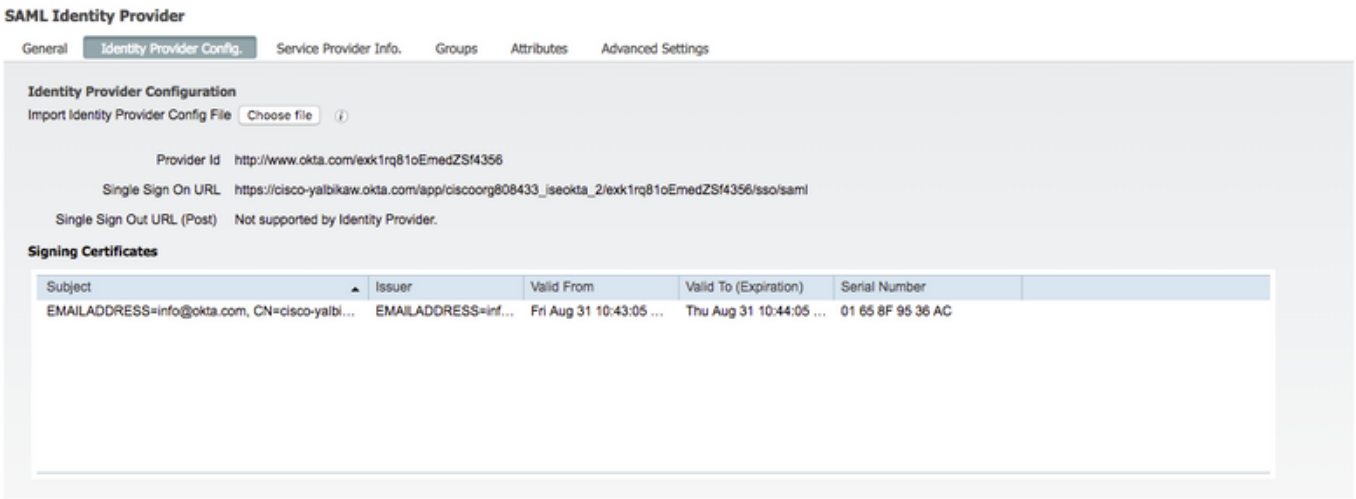
ファイルをXML形式で保存します。

5.アプリケーションへのユーザーの割り当て

このアプリケーションにユーザを割り当てます。AD統合には次の説明を参照してください。
okta-activeディレクトリ

6. IDPからISEへのメタデータのインポート。

ステップ1:[SAML Identity Provider]で、**[Identity Provider Config]**を選択し、**[**Import Metadata]を選択します。



ステップ 2：設定を保存します。

ステップ3:CWAの設定。

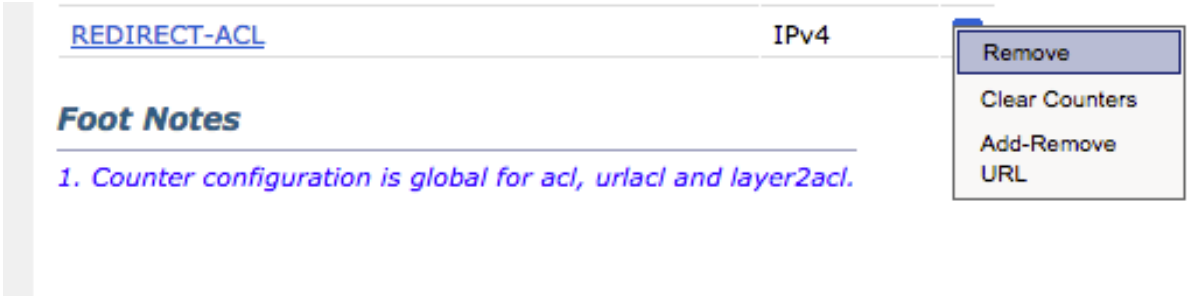
このドキュメントでは、ISEとWLCの設定について説明します。

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

Redirect-ACLにURLを追加します。

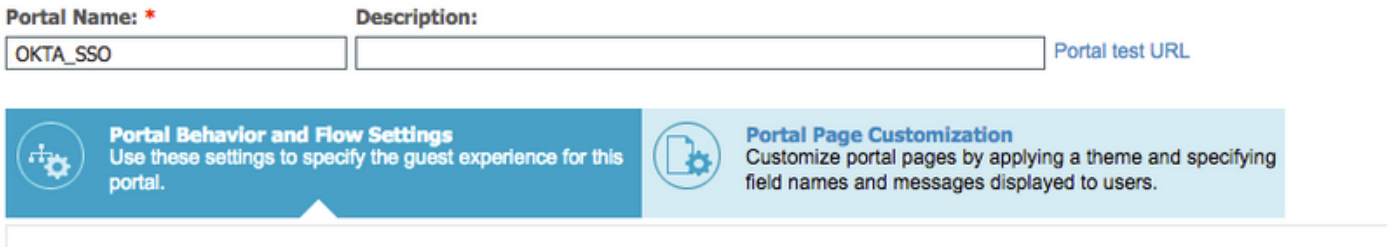
https://cisco-yalbikaw.okta.com /アプリケーションURLの追加

https://login.okta.com

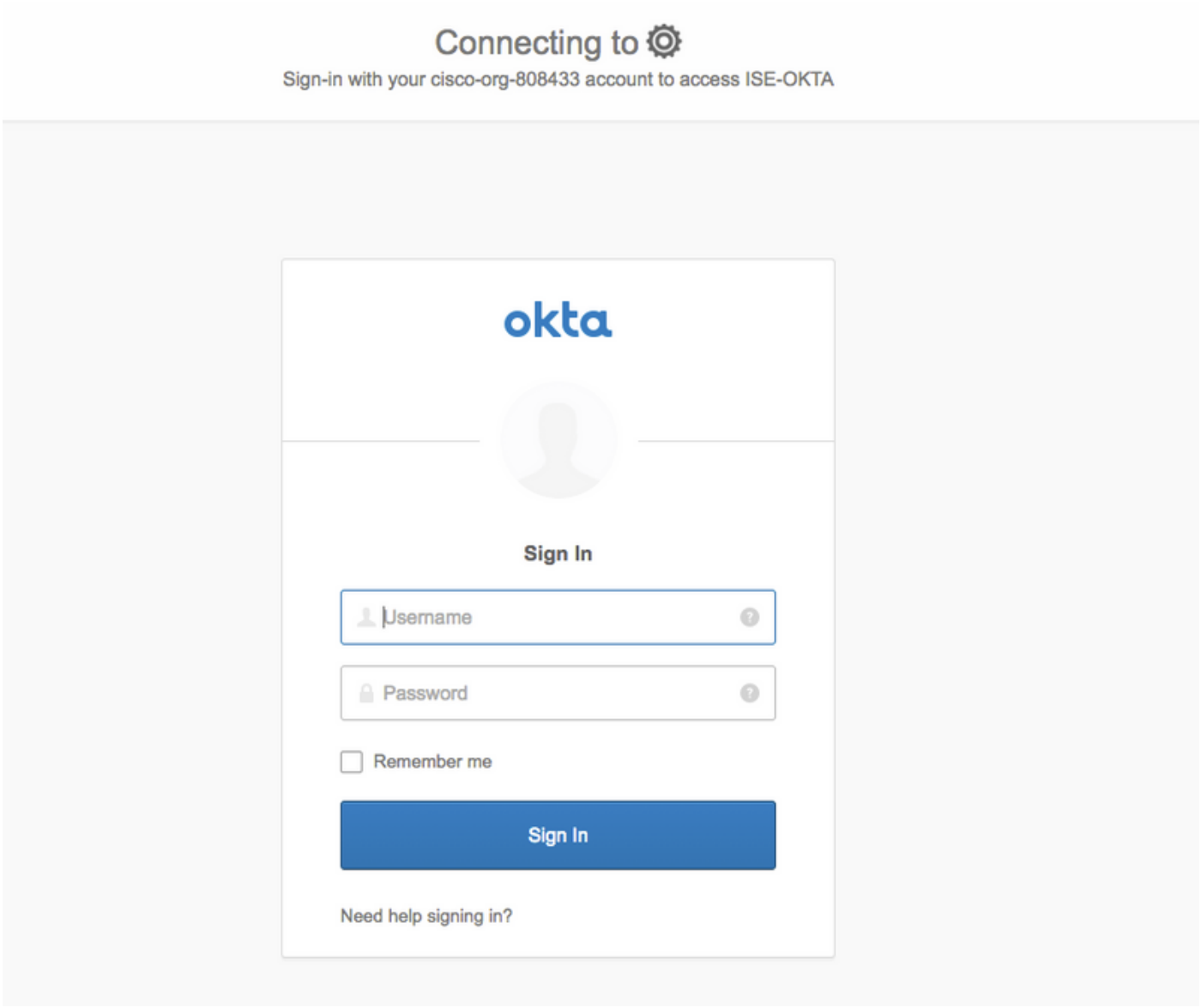


確認

ポータルをテストし、OKTAアプリケーションに到達できるかどうかを確認します



ステップ1：ポータルテストをクリックすると、SSOアプリケーションにリダイレクトされます。

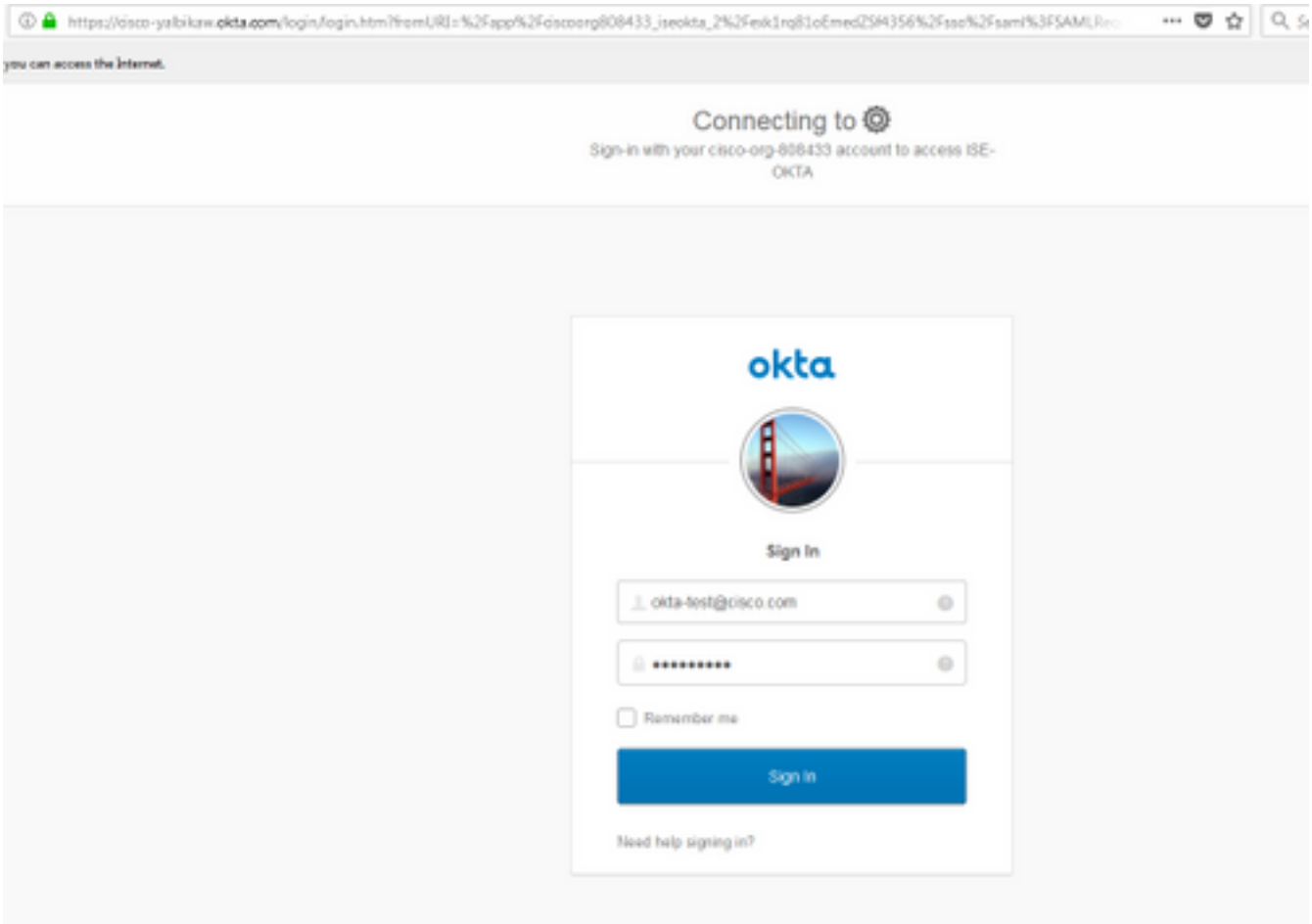


ステップ2: <アプリケーション*名>への情報接続を確認します*

ステップ3：クレデンシャルを入力すると、saml要求が不正である可能性があります。これは、この時点で設定が正しくないことを意味しているとは限りません。

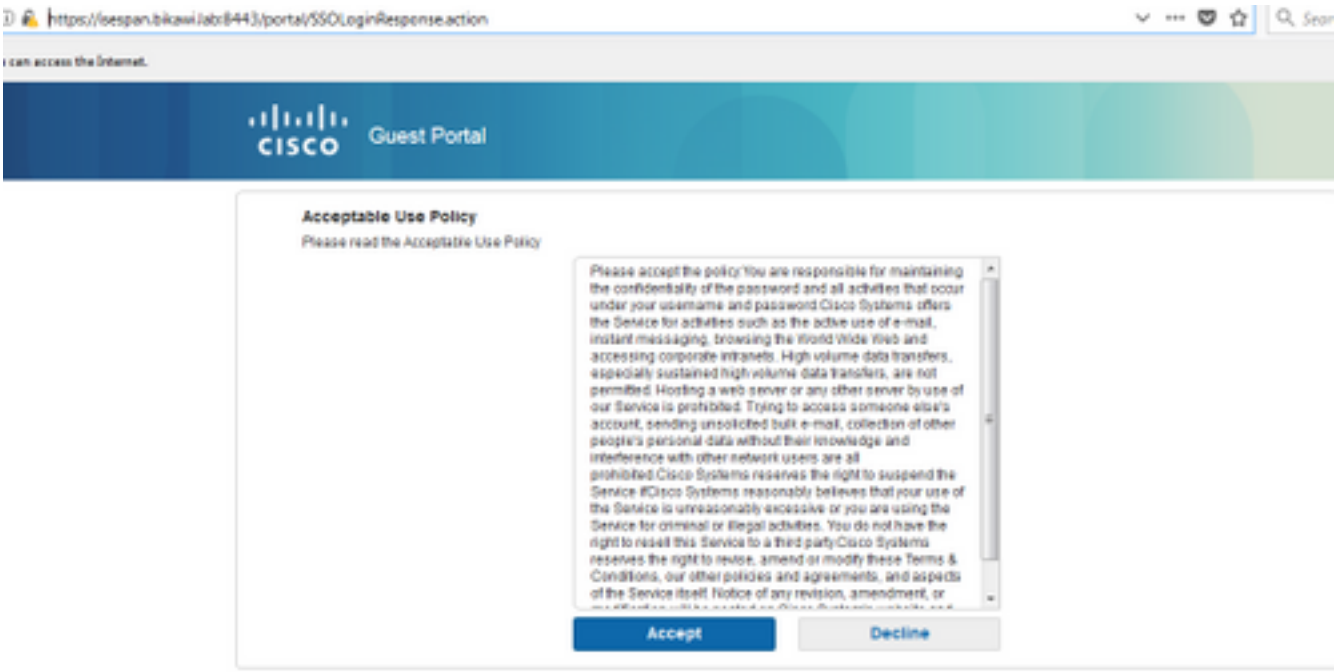
エンドユーザの検証

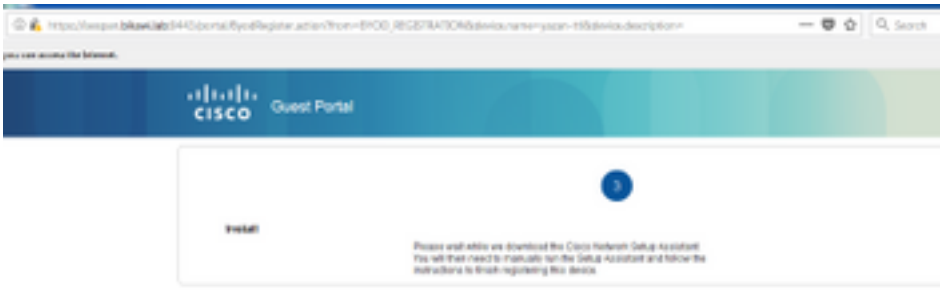

Search
you can access the Internet.
cisco
Guest Portal
Sign On
Sign on for guest access.
Username:
Password:
Sign On
Or register for guest access
You can also login with


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



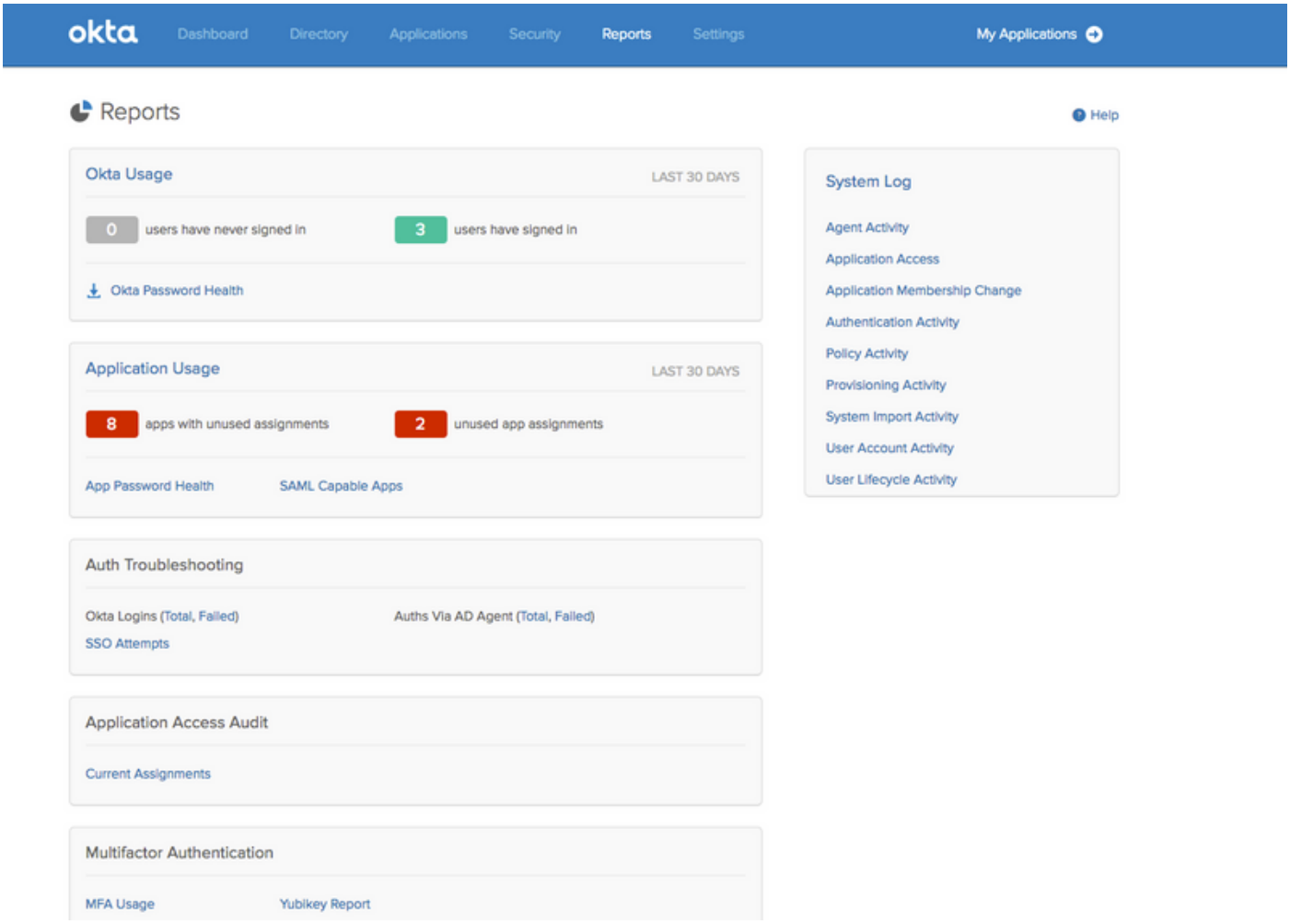
ISEの検証

ライフログを確認して、認証ステータスを確認します。

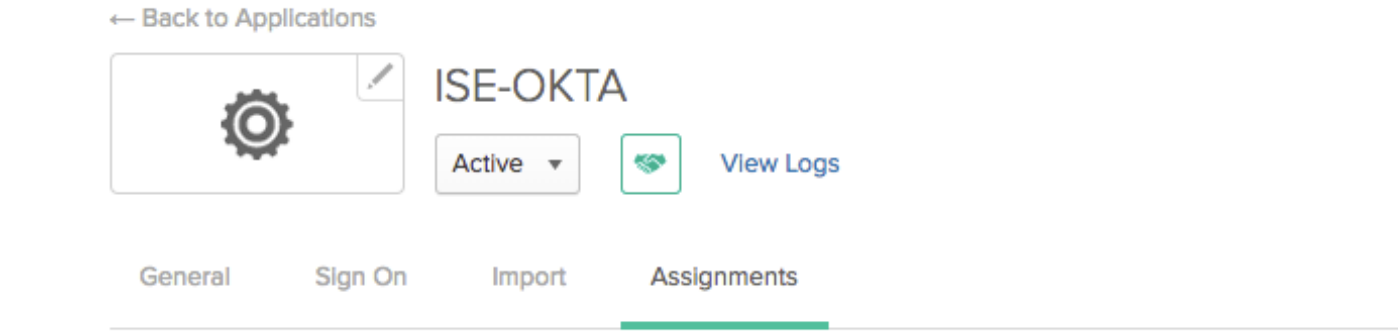
トラブルシュート

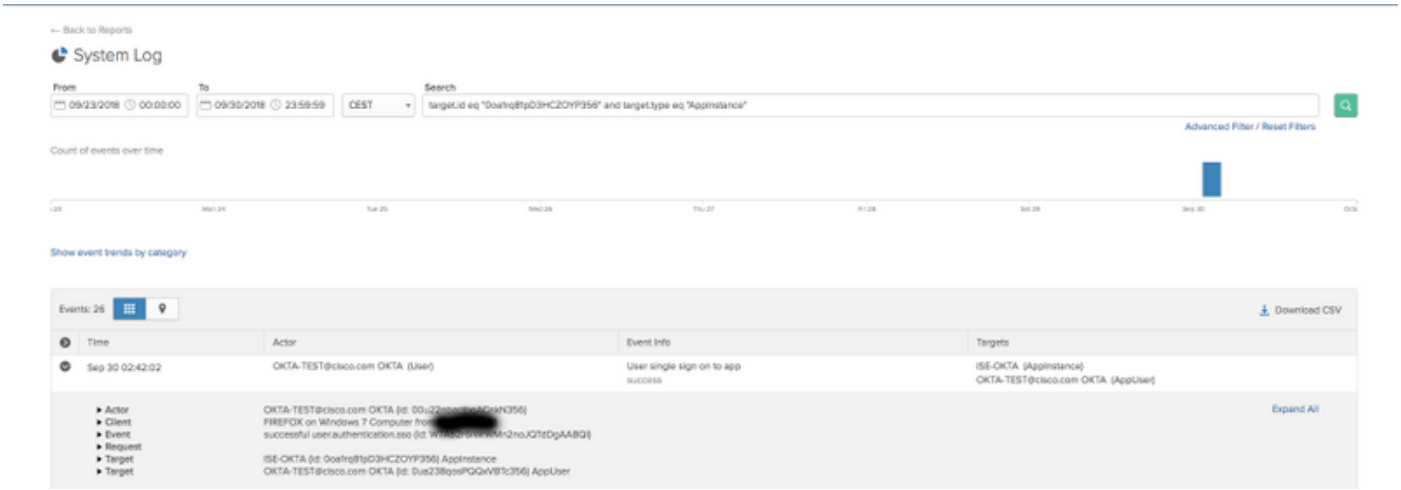
OKTAのトラブルシューティング

ステップ1:[Reports]タブでログを**確認**します。



ステップ2：アプリケーションから関連ログも表示されます。





ISEのトラブルシューティング

確認するログファイルは2つあります

- ise-psc.log
- guest.log

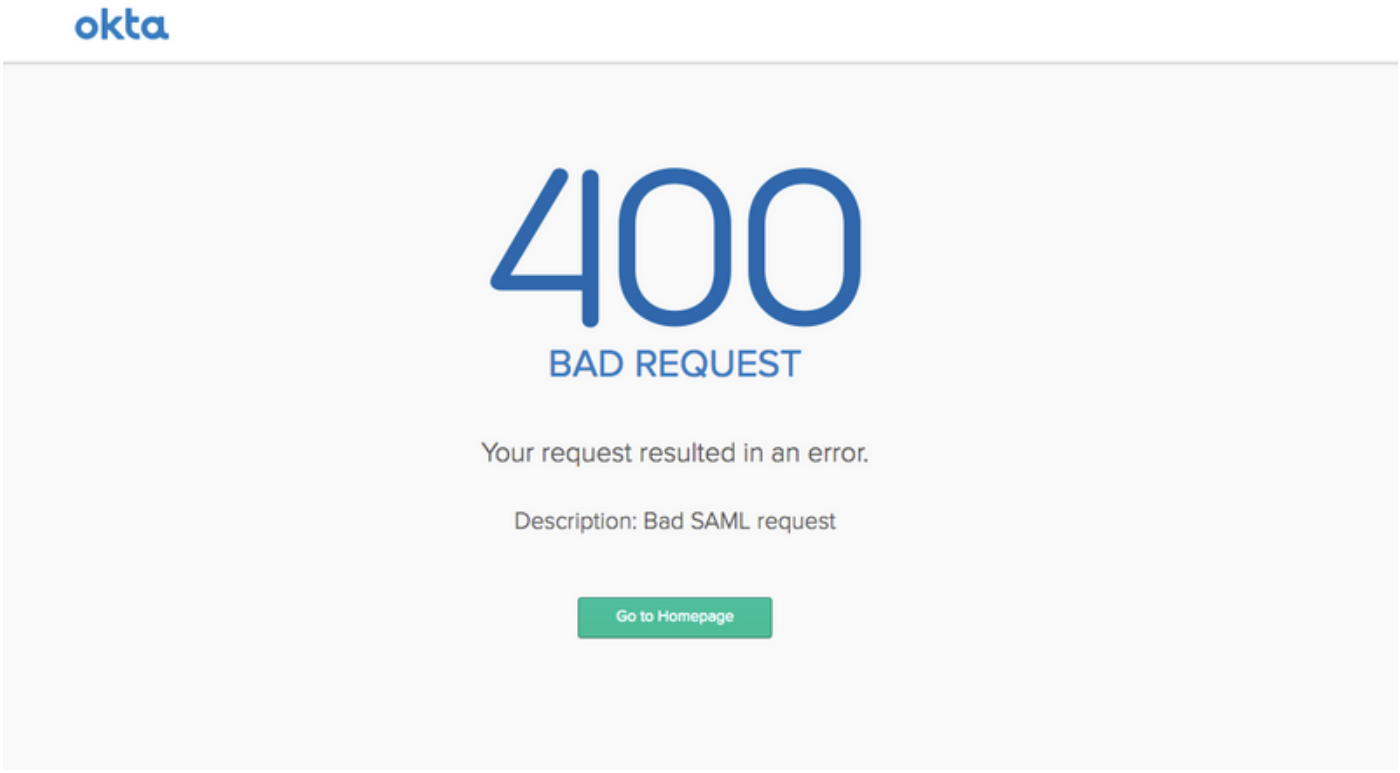
[Administration] > [System] > [Logging] > [Debug Log Configuration]に移動します。レベルをDEBUGに有効にします。

SAML	ise-psc.log
ゲストアクセス	guest.log
ポータル	guest.log

次の表に、デバッグするコンポーネントと、対応するログファイルを示します。

一般的な問題と解決策

シナリオ1.不正なSAML要求。



このエラーは一般的であり、ログをチェックしてフローを確認し、問題を特定します。ISE guest.log:

ISE# show logging application guest.log |過去50

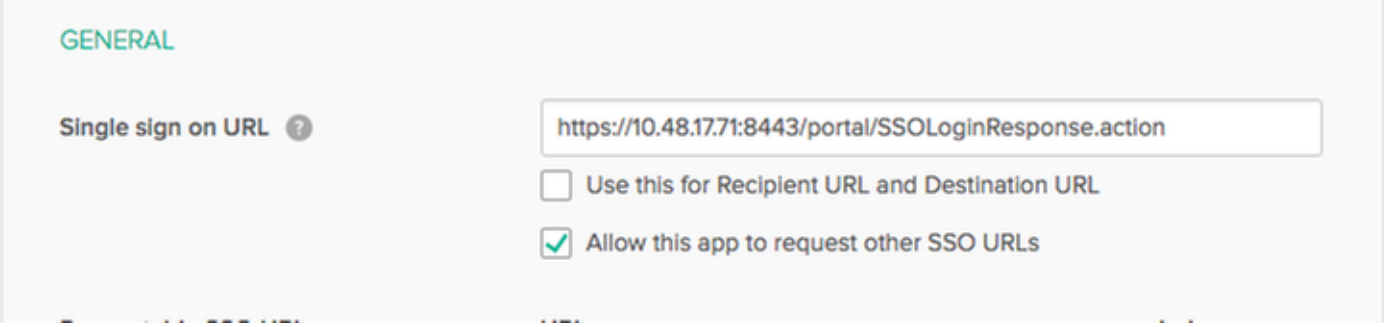
```
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:
SSOLoginTransitionResult:

        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がユーザをIDPにリダイレクトしました。ただし、ISEへの応答はなく、不正なSAML要求が表示されます。OKTAが以下のSAML要求を受け入れていないことを確認します。

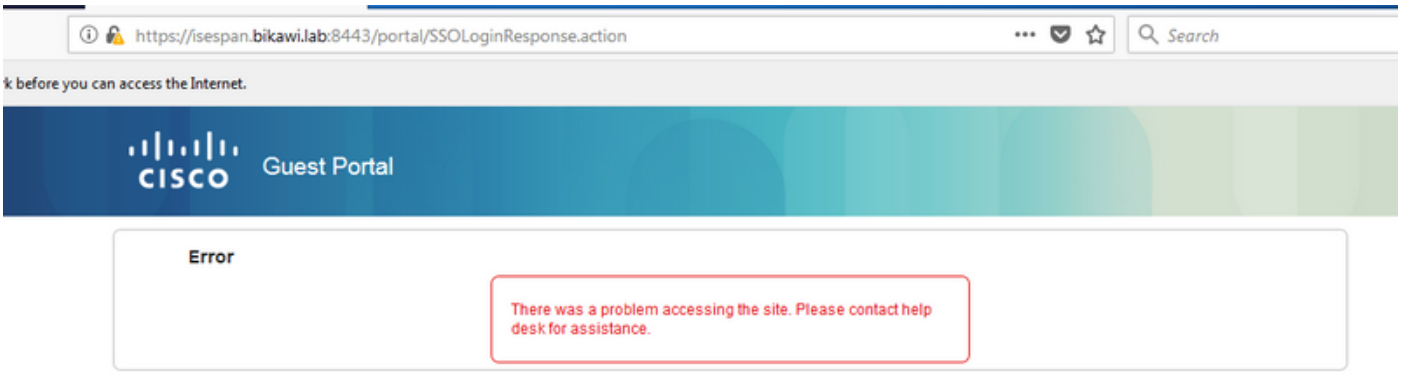
```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9owF
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0SltaB0Vxv1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%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
```

アプリケーションに変更が加えられている可能性があります。



SSO URLはIPアドレスを使用していますが、ゲストはFQDNを送信しています。これは、最後の行の要求にSEMI_DELIMITER<FQDN>が含まれていることが分かるため、この問題を修正するには、IPアドレスをOKTA設定のに変更します。

シナリオ2.「サイトへのアクセスで問題が発生しました。ヘルプデスクにお問い合わせください。」



Guest.log

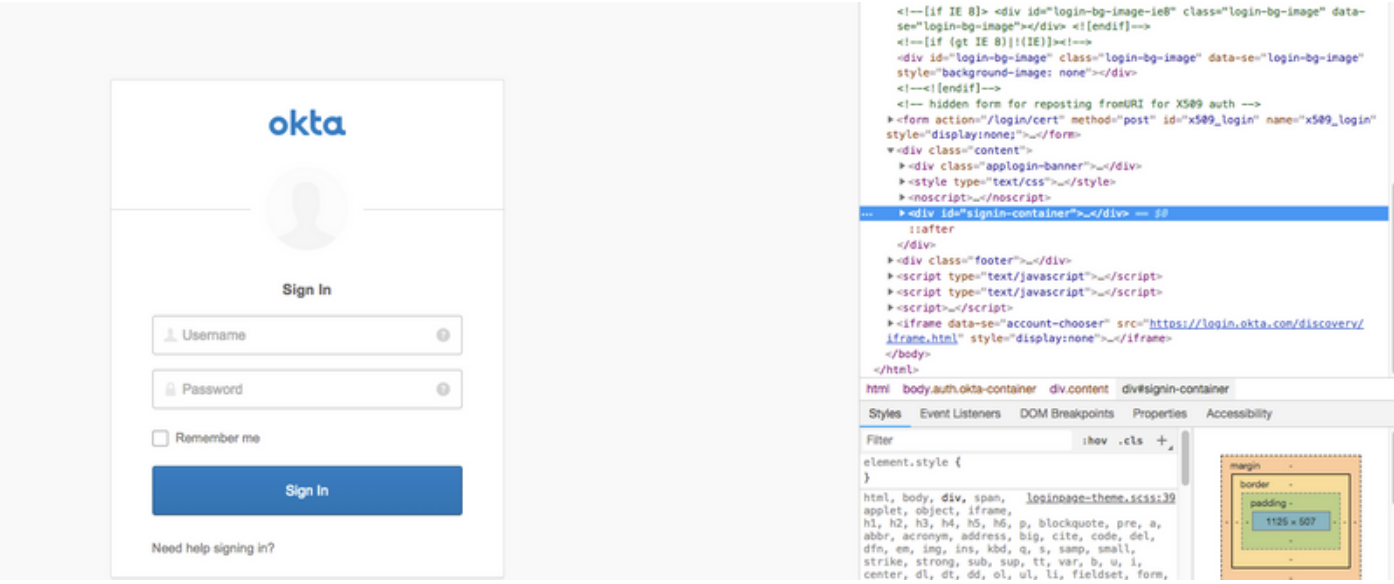
```
2018-09-30 02:25:00,595 ERROR  [https-jsse-nio-10.48.17.71-8443-exec-1][]
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
contain ma
```

```
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
```

ログから、ISEはアサーションが正しくないことを報告します。[OKTA Audience URI]をオンにして、SPと一致していることを確認して解決します。

シナリオ3：空白ページにリダイレクトされるか、ログインオプションが表示されません。

環境とポータルの設定によって異なります。この種の問題では、OKTAアプリケーションと、認証に必要なURLを確認する必要があります。ポータルテストをクリックし、要素を検査して、到達可能にする必要があるWebサイトを確認します。



このシナリオでは、2つのURLのみ：applicationおよびlogin.okta.com：これらはWLCで許可される必要があります。

関連情報

- 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