Configuration du portail invité ISE 2.3 avec OKTA SAML SSO

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - SSO fédérée
  - Flux réseau
- Configurer
  - Étape 1 : configuration du fournisseur d'identité SAML et du portail Invité sur ISE
    - 1. Préparez la source d'identité externe.
    - 2. Créez un portail pour SSO.
    - 3. Configurez une autre connexion.
  - Étape 2 : configuration des paramètres de l'application OKTA et du fournisseur d'identité SAML
    - 1. Créez une application OKTA.
    - 2. Exportez les informations SP du fournisseur d'identité SAML.
    - 3. Paramètres SAML OKTA.
    - 4. Exportez les métadonnées de l'application.
    - 5. Affectez des utilisateurs à l'application.
    - 6. Importez des métadonnées d'Idp vers ISE.
  - Étape 3.Configuration de CWA
- Vérifier
  - Vérification des utilisateurs finaux
  - Vérification ISE
- Dépannage
  - Dépannage OKTA
  - Dépannage ISE
  - Problèmes courants et solutions
- Informations connexes

Introduction

Ce document décrit comment intégrer Identity Services Engine (ISE) avec OKTA, pour fournir l'authentification SSO (Single Sign-On) SAML (Security Assertion Markup Language) pour le portail invité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Services invités Cisco Identity Services Engine.
- SAML SSO.
- (facultatif) Configuration du contrôleur LAN sans fil (WLC).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine 2.3.0.298
- Application OKTA SAML SSO
- Contrôleur sans fil Cisco 5500 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

SSO fédérée

Un utilisateur au sein d'une organisation peut s'authentifier une seule fois, puis accéder à plusieurs ressources. Cette identité utilisée dans plusieurs organisations est appelée identité fédérée.

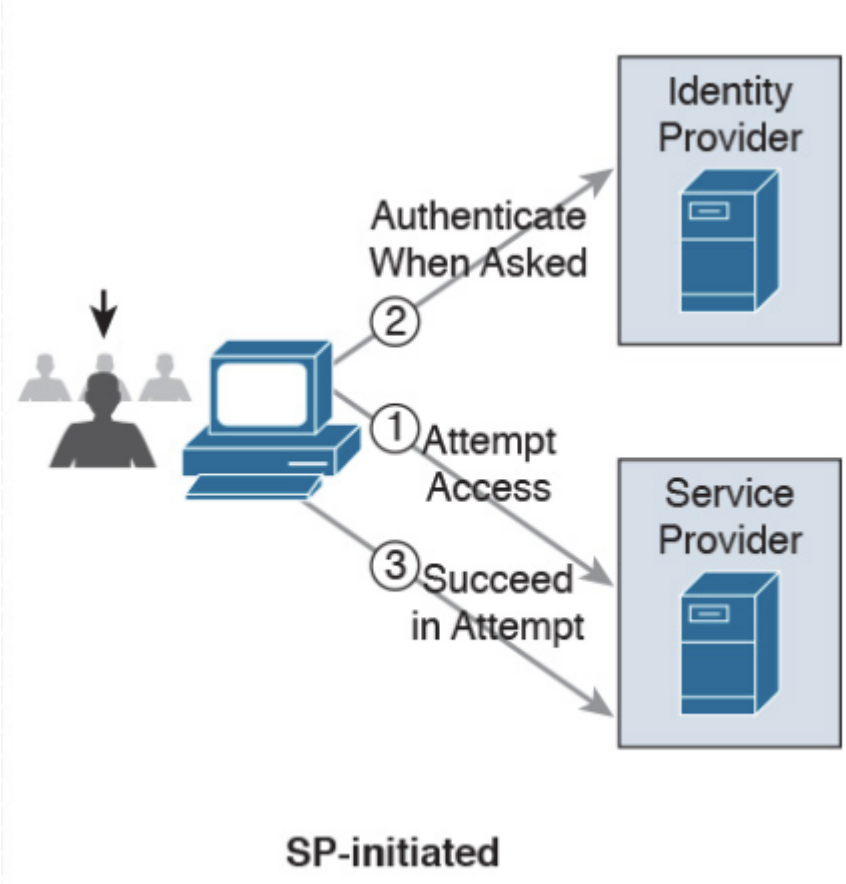
Le concept de fédération :

- Principe : L'utilisateur final (celui qui demande un service), le navigateur Web, dans ce cas, est le terminal.
- Fournisseur de services (SP) : parfois appelé partie de confiance (RP), qui est le système qui fournit un service, dans ce cas, ISE.
- Fournisseur d'identités (IdP) : qui gère l'authentification, le résultat d'autorisation et les attributs qui sont renvoyés au SP, dans ce cas, OKTA.
- Affirmation : les informations utilisateur envoyées par le fournisseur d'identité au fournisseur de services.

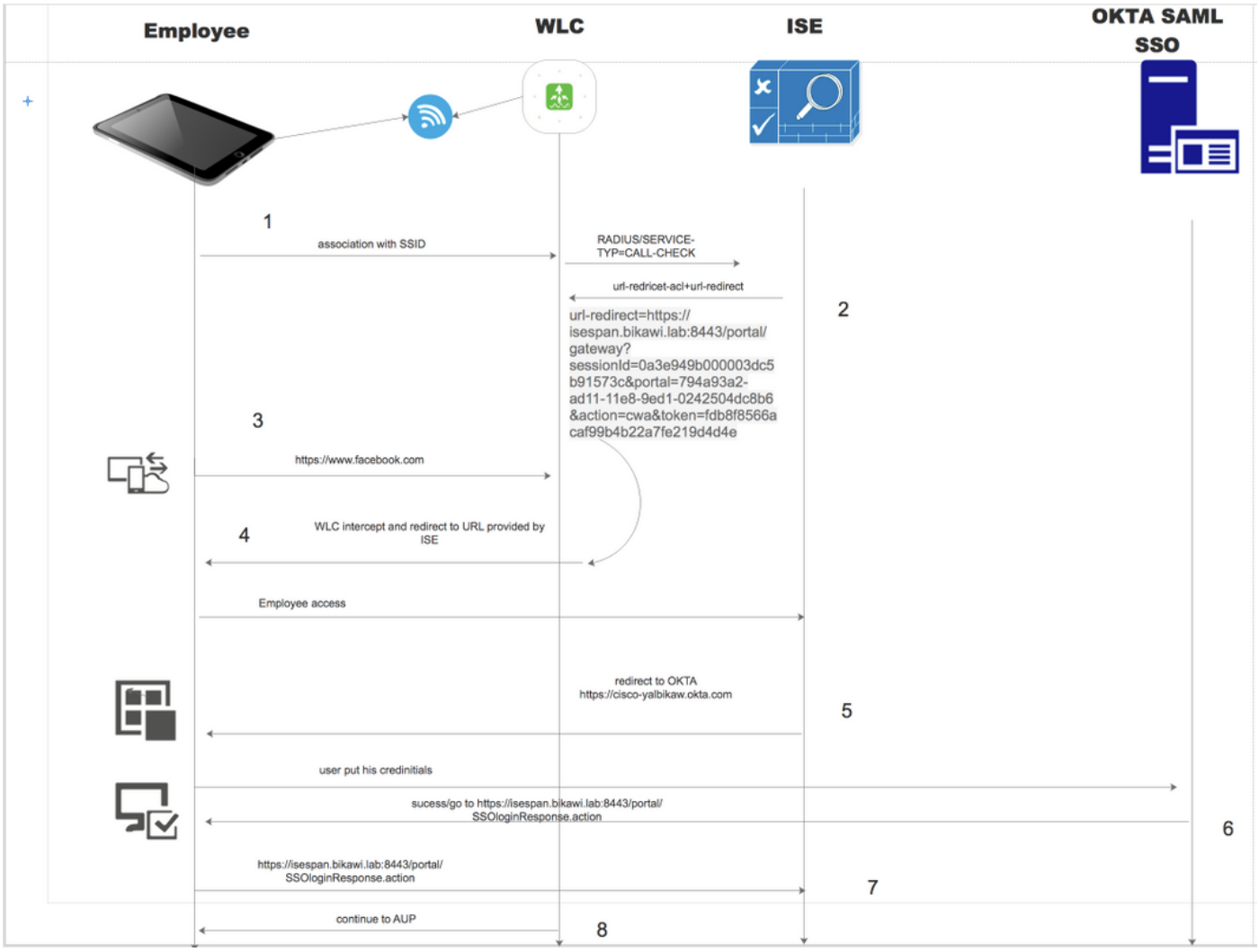
Plusieurs protocoles implémentent SSO, tels qu'OAuth2 et OpenID. ISE utilise SAML.

SAML est un cadre XML qui décrit l'utilisation et l'échange d'assertions SAML d'une manière sécurisée entre des entités commerciales. La norme décrit la syntaxe et les règles pour demander, créer, utiliser et échanger ces assertions.

ISE utilise le mode SP initialisé. L'utilisateur est redirigé vers le portail Invité, puis ISE le redirige vers IdP pour l'authentification. Après cela, il redirige vers ISE. La demande est validée, l'utilisateur procède à l'accès invité ou à l'intégration, en fonction de la configuration du portail.



Flux réseau



1. L'utilisateur se connecte au SSID et l'authentification est mac filtering (mab).

2. ISE répond avec access-accept qui contient les attributs Redirect-URL et Redirect-ACL
3. L'utilisateur tente d'accéder à www.facebook.com.
4. WLC intercepte la demande et redirige l'utilisateur vers le portail invité ISE. L'utilisateur clique sur l'accès des employés afin d'enregistrer le périphérique avec les informations d'identification SSO.
5. ISE redirige l'utilisateur vers l'application OKTA pour authentification.
6. Une fois l'authentification réussie, OKTA envoie la réponse d'assertion SAML au navigateur.
7. Le navigateur renvoie l'assertion à ISE.
8. ISE vérifie la réponse à l'assertion et si l'utilisateur est correctement authentifié, il passe à l'AUP, puis à l'enregistrement du périphérique.

Cliquez sur le lien ci-dessous pour plus d'informations sur SAML

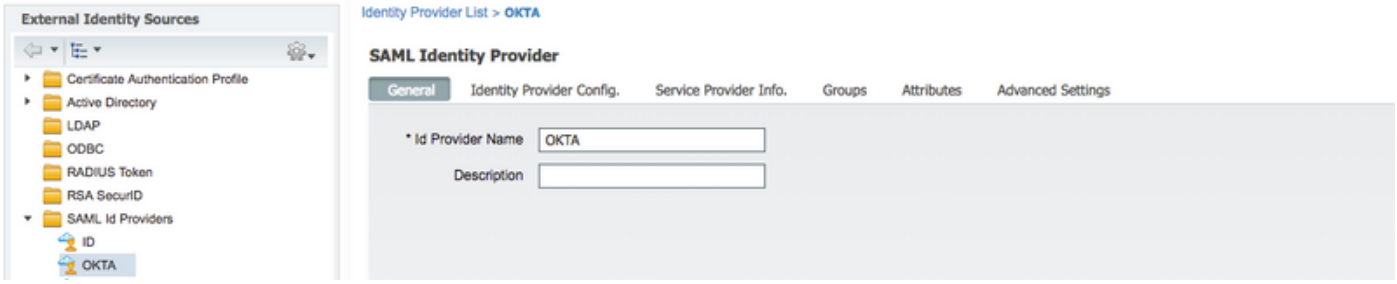
https://developer.okta.com/standards/SAML/

Configurer

Étape 1 : configuration du fournisseur d'identité SAML et du portail Invité sur ISE

1. Préparez la source d'identité externe.

Étape 1. Accédez à Administration > External Identity Sources > SAML id Providers.

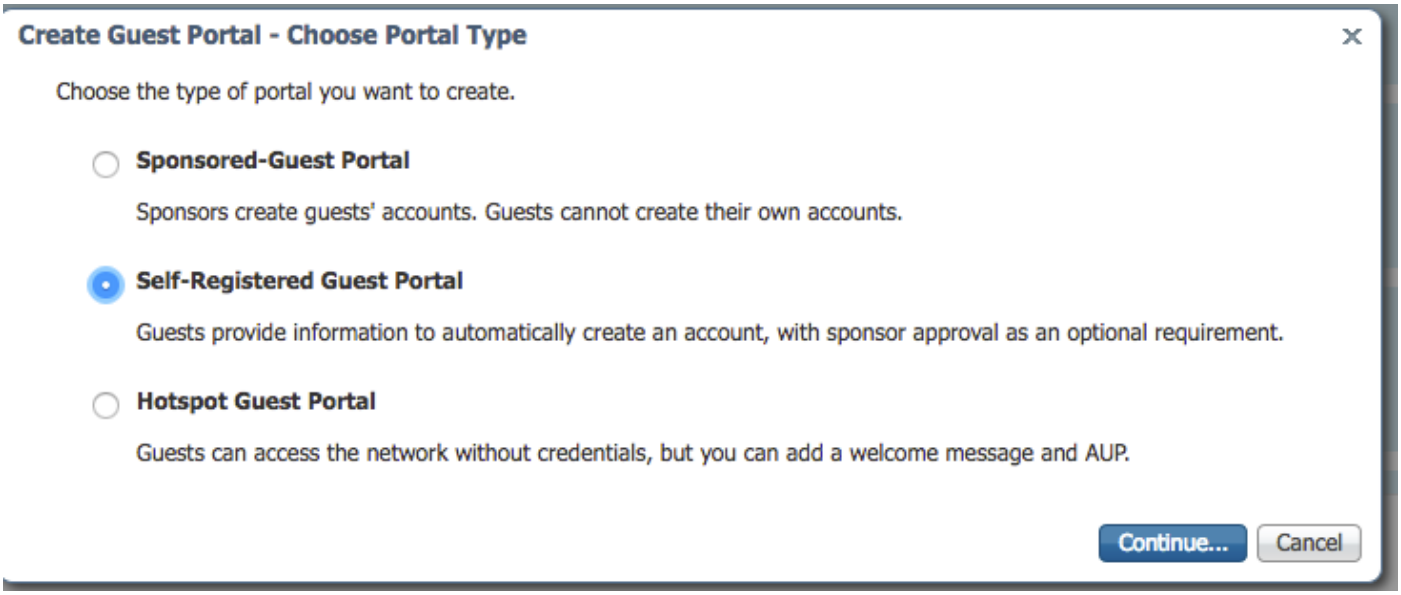


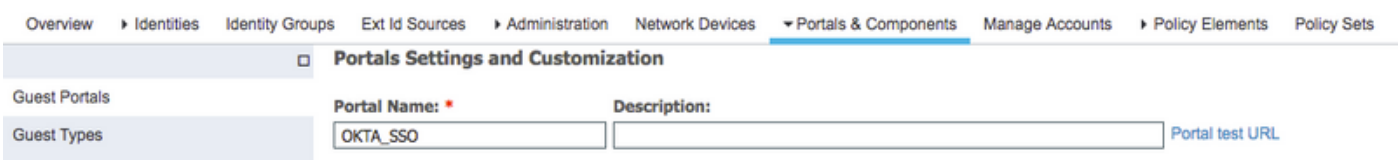
Étape 2 : attribution d'un nom au fournisseur d'ID et envoi de la configuration

2. Créez un portail pour SSO.

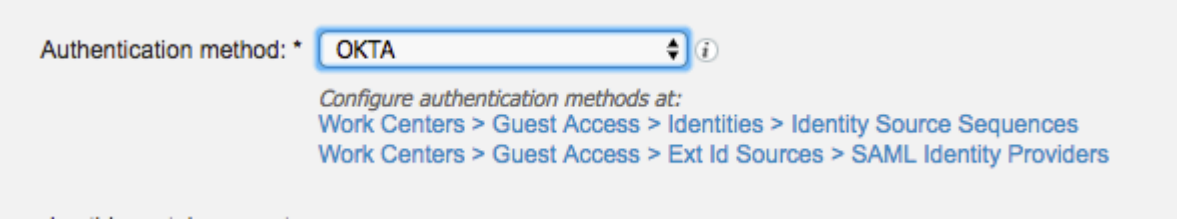
Étape 1 : création du portail attribué à OKTA en tant que source d'identité Toute autre configuration pour le BYOD, l'enregistrement des périphériques, les invités, etc., est exactement la même que pour le portail normal. Dans ce document, le portail est mappé au portail invité comme connexion alternative pour Employé.

Étape 2. Accédez à Work Centers > Guest Access > Portals & Components et créez le portail.



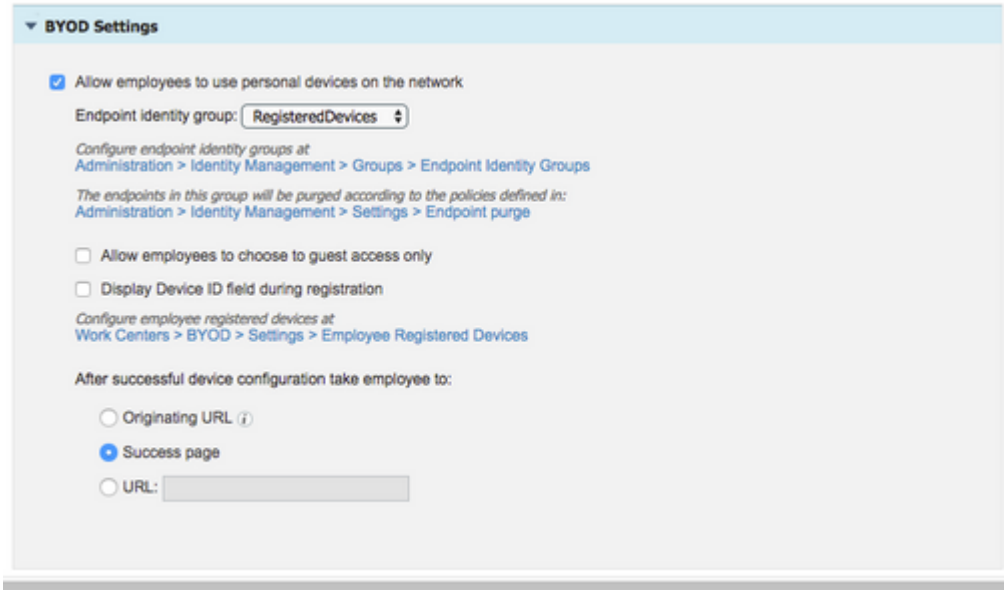


Étape 3. Choisissez la méthode d'authentification pour pointer vers le fournisseur d'identité configuré précédemment.

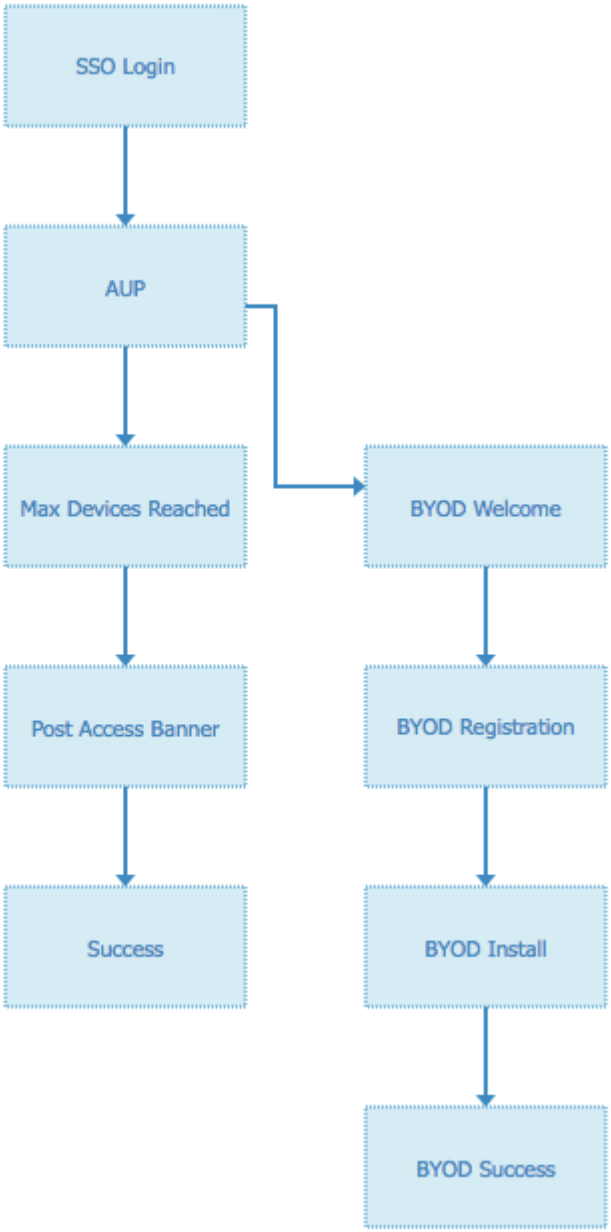


Étape 4. Choisissez la source d'identité OKTA comme méthode d'authentification.

(facultatif) choisissez les paramètres BYOD.



Étape 5. Enregistrez la configuration du portail, avec le BYOD, le flux ressemble à ceci :

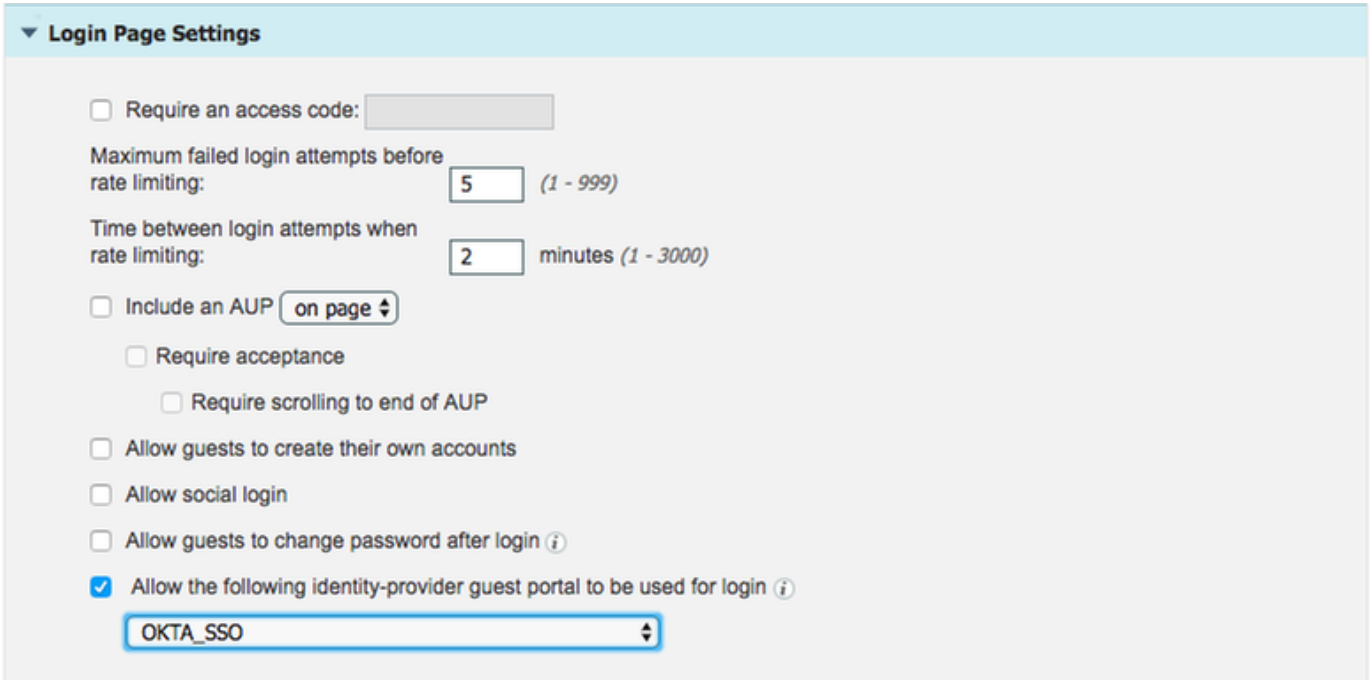


3. Configurez une autre connexion.

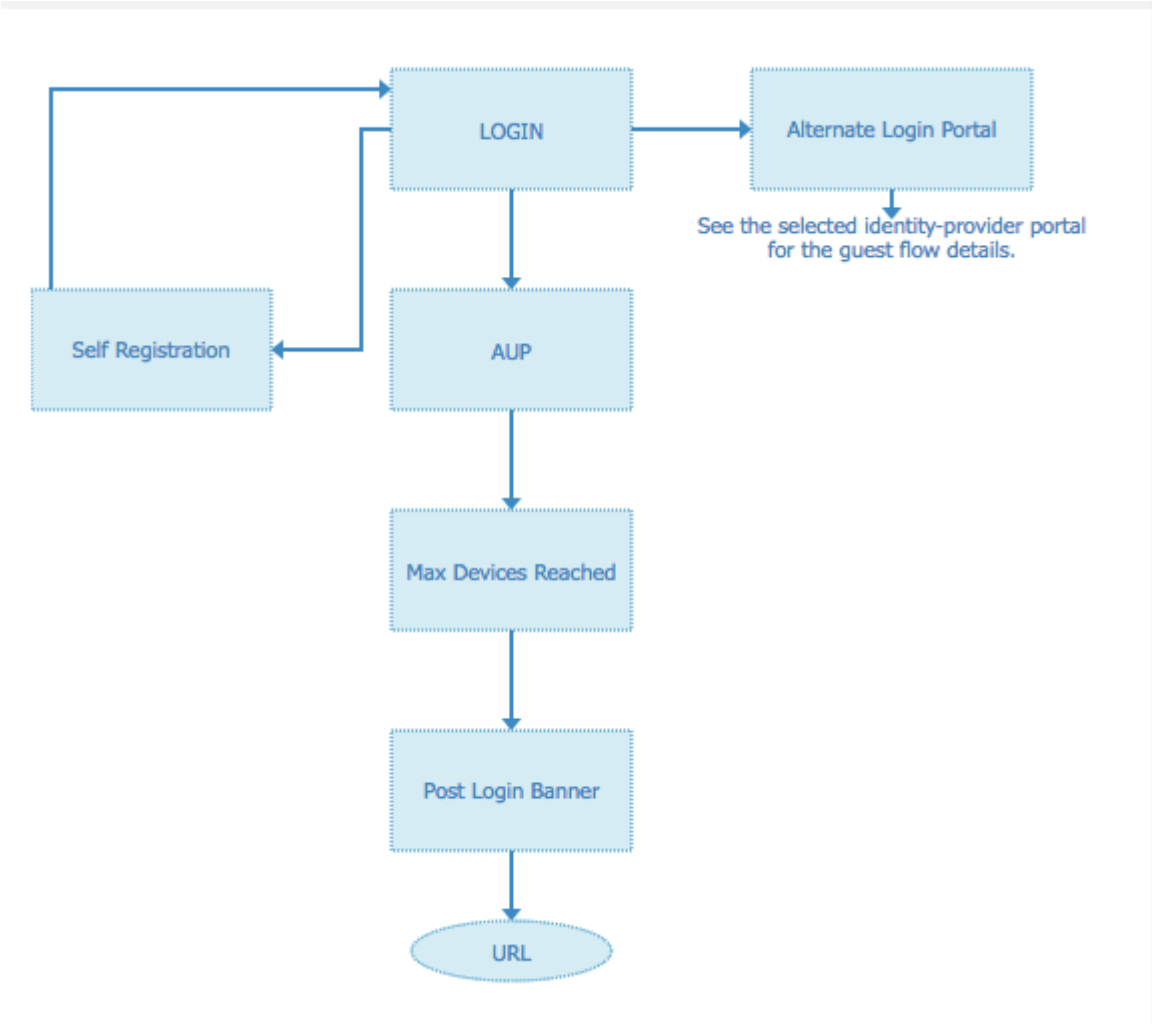
Remarque : Vous pouvez ignorer cette partie si vous n'utilisez pas la connexion alternative.

Accédez au portail d'auto-inscription Guest Portal ou à tout autre portail personnalisé pour l'accès invité.

Dans les paramètres de la page de connexion, ajoutez le portail de connexion alternatif : OKTA_SSO.



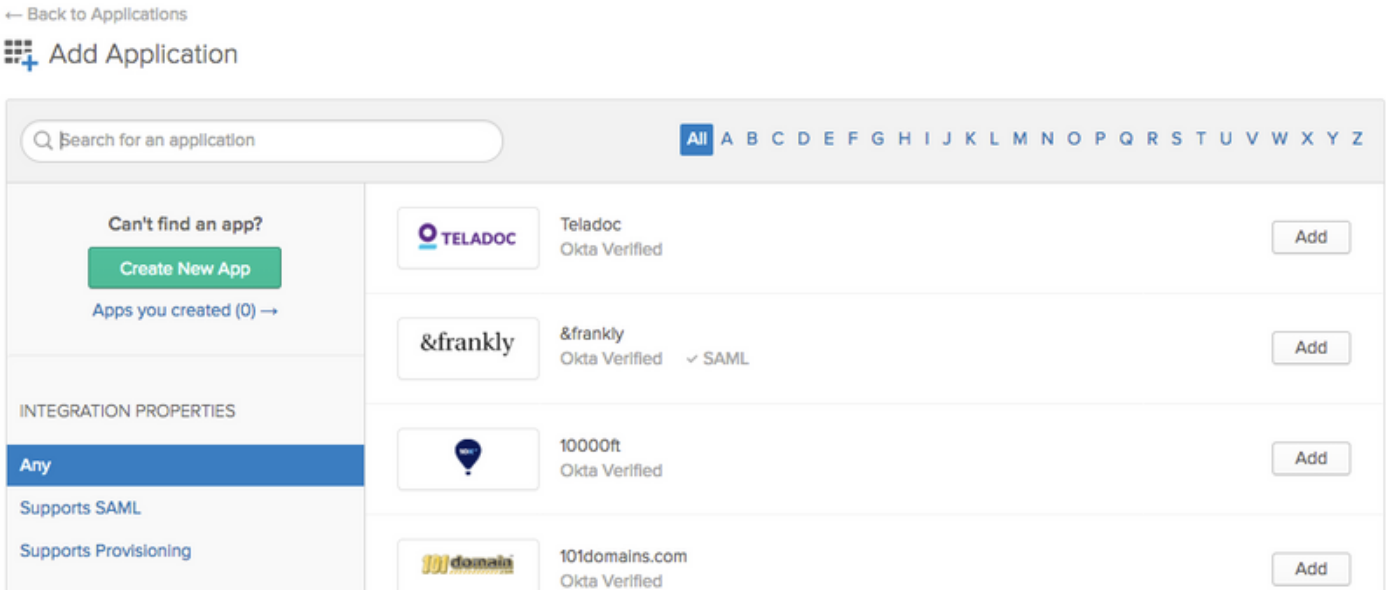
Voici le flux du portail maintenant.



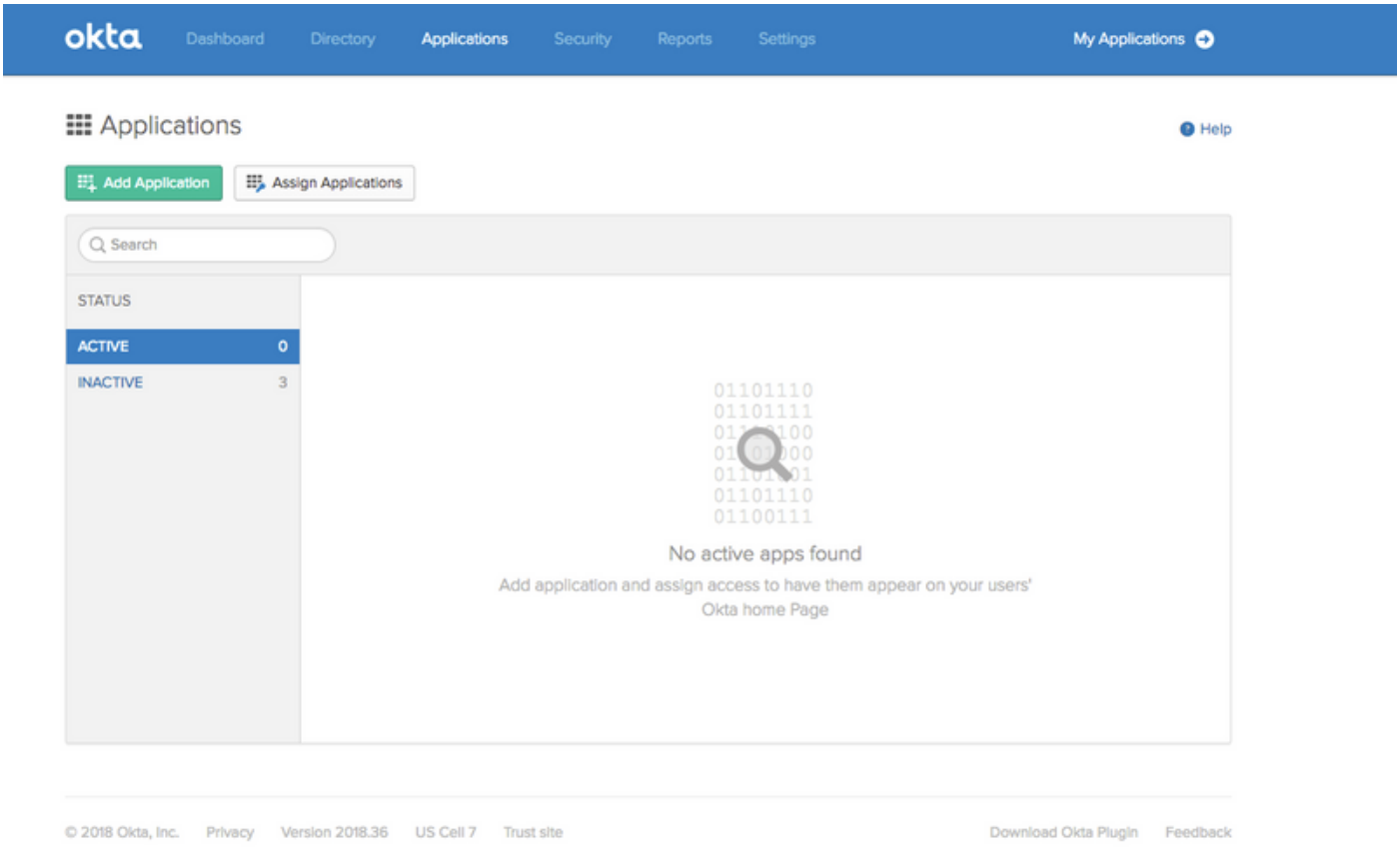
Étape 2 : configuration des paramètres de l'application OKTA et du fournisseur d'identité SAML

1. Créez une application OKTA.

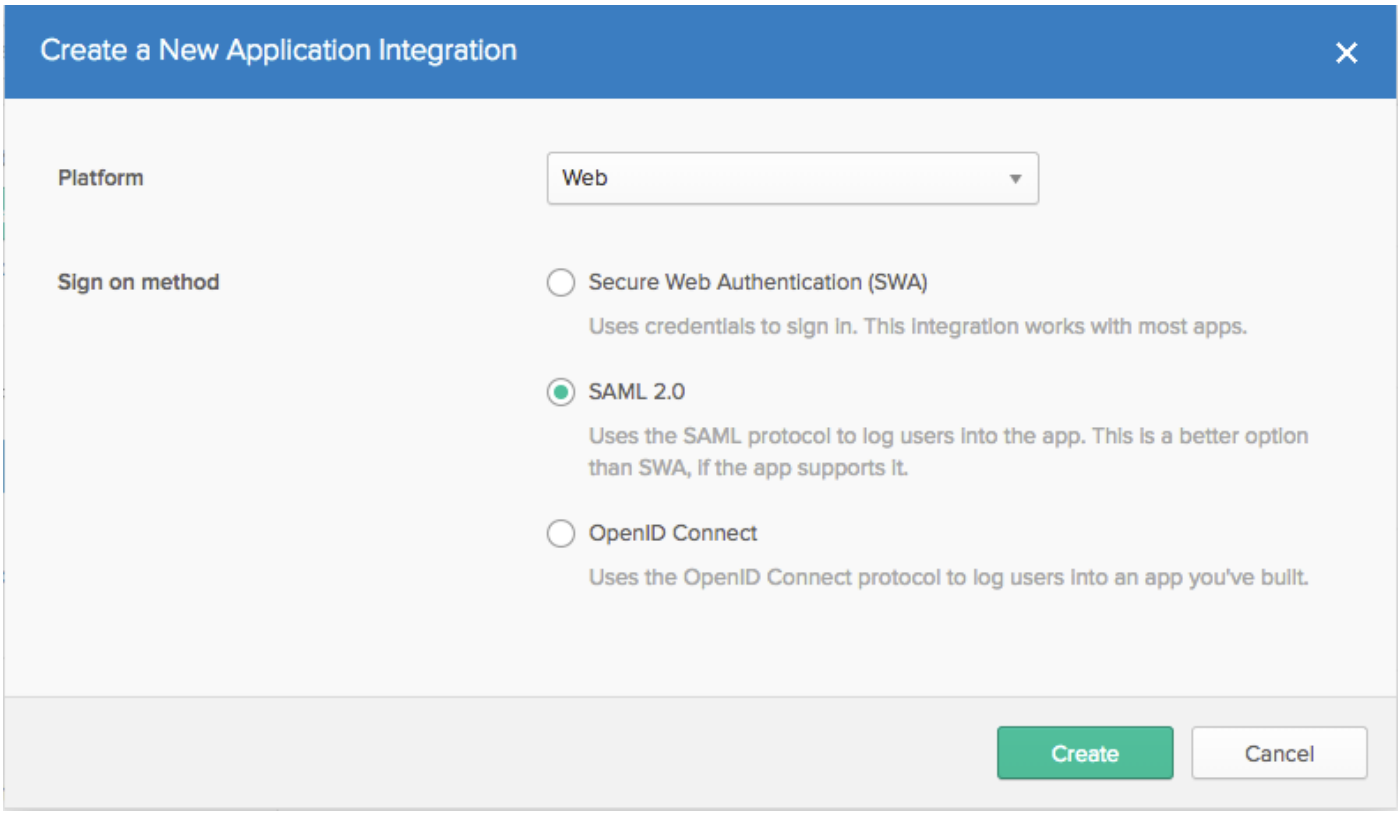
Étape 1. Connectez-vous au site Web OKTA avec un compte d'administrateur.



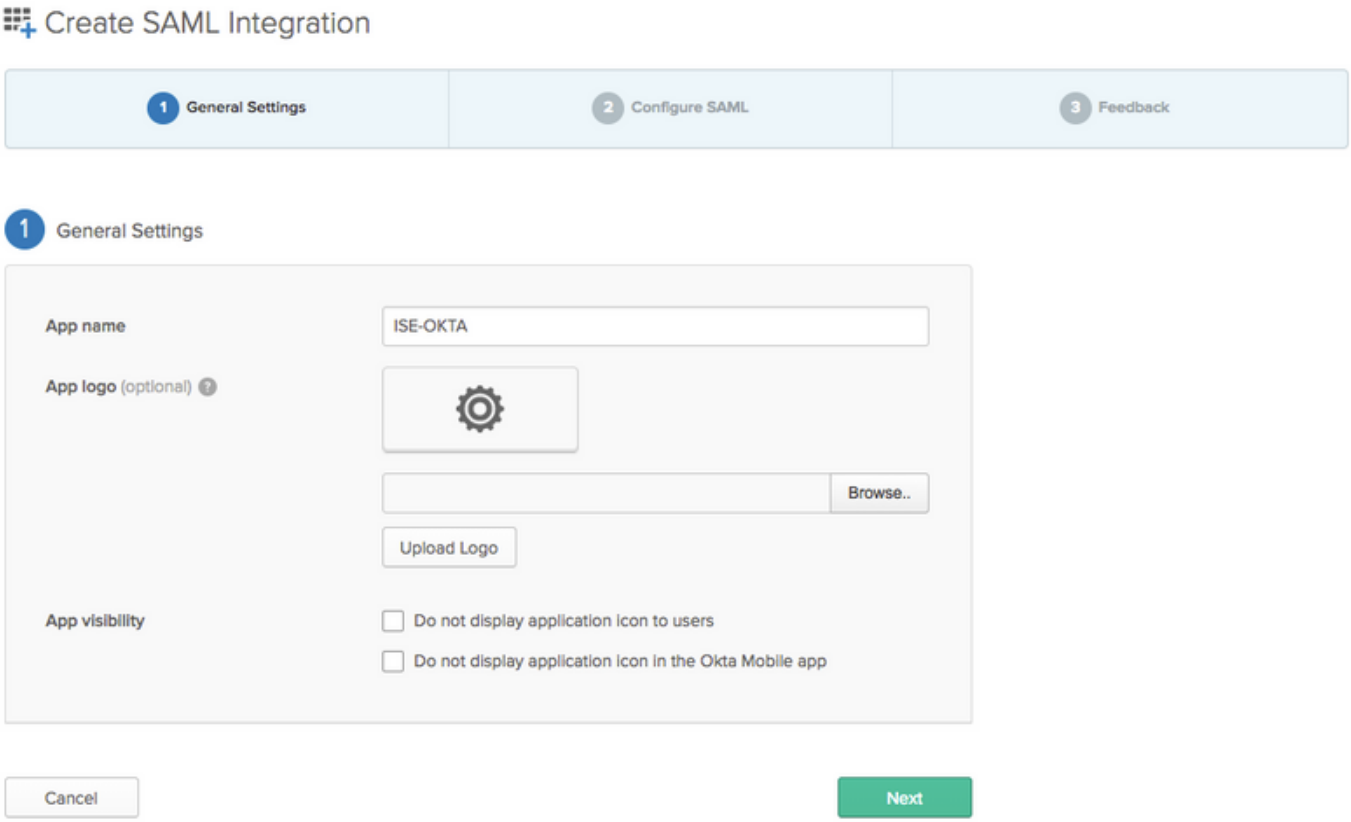
Étape 2. Cliquez sur Add Application.

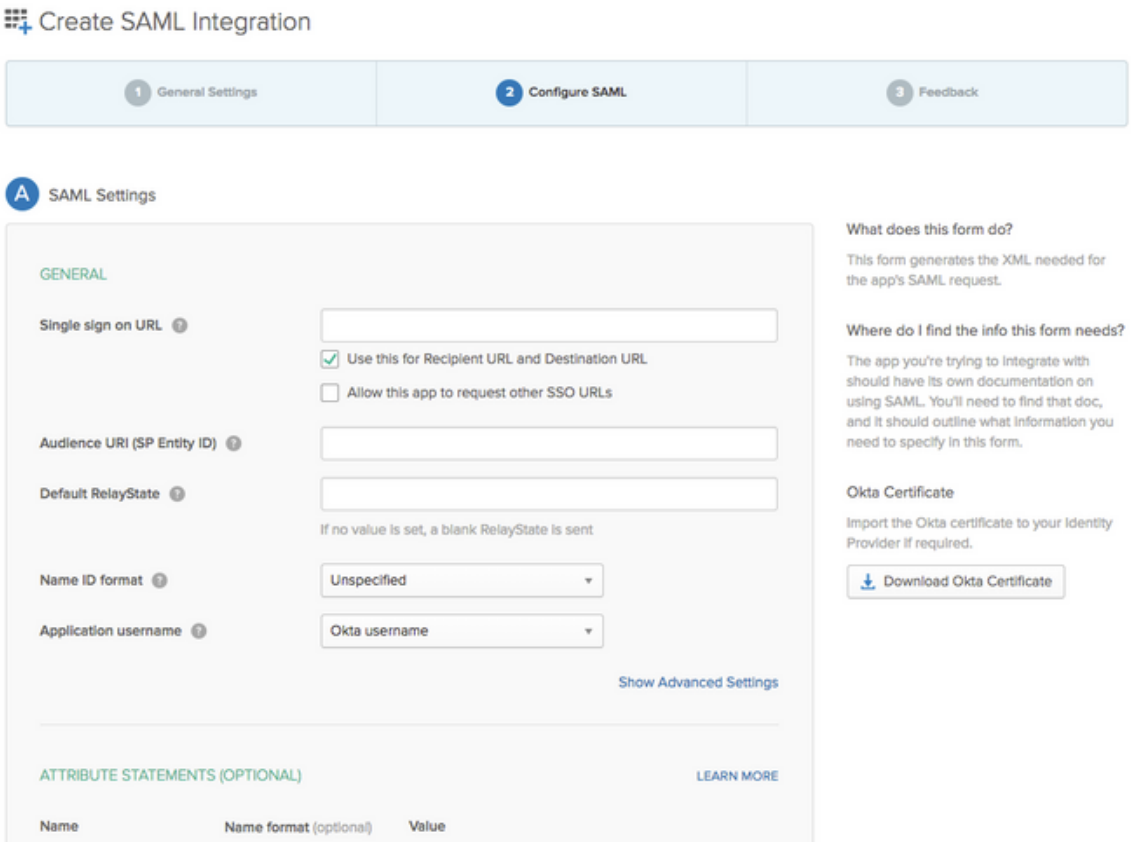


Étape 3. Créez une nouvelle application, choisissez-la SAML2.0

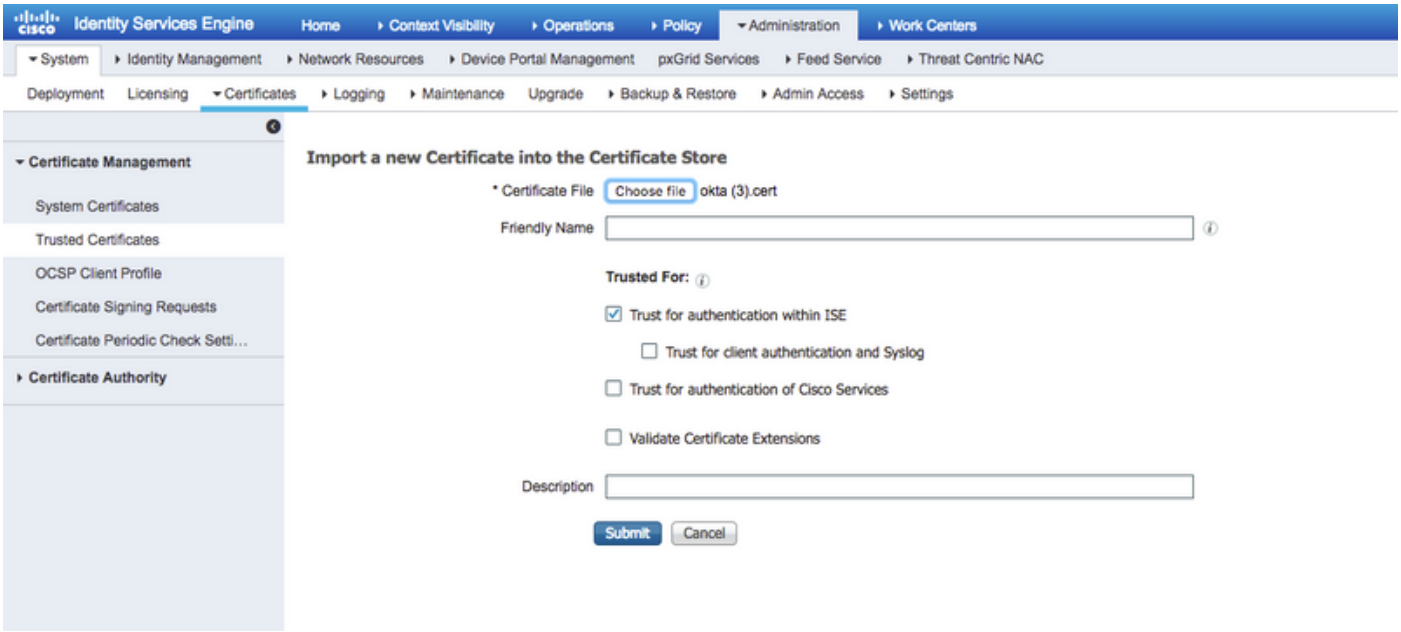


Paramètres généraux



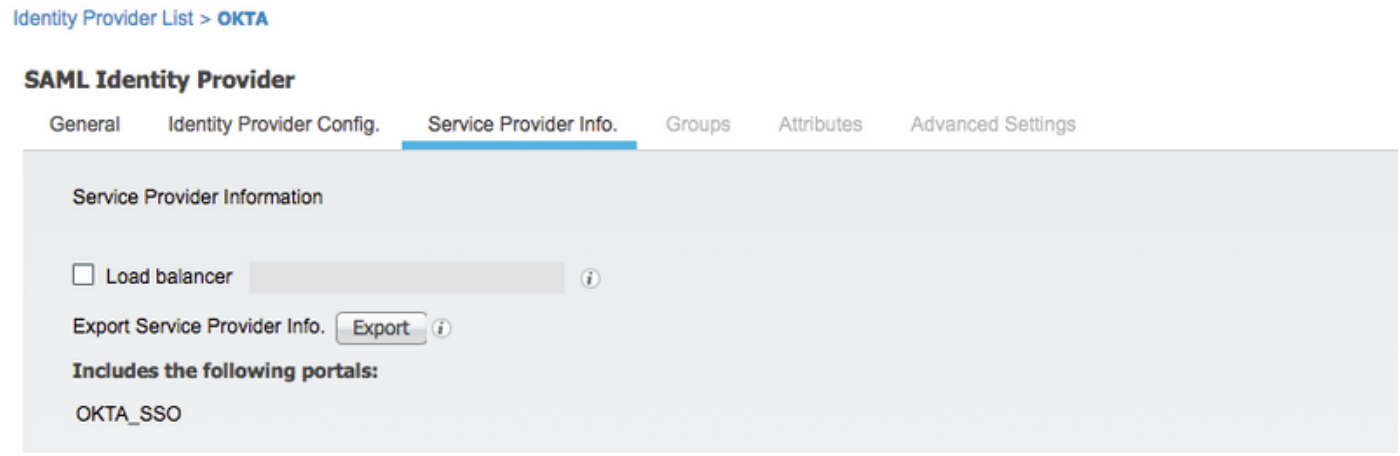


Étape 4. Téléchargez le certificat et installez-le dans les certificats de confiance ISE.



2. Exportez les informations SP du fournisseur d'identité SAML.

Accédez au fournisseur d'identité précédemment configuré. Cliquez sur Service Provider Info et exportez-le, comme indiqué dans l'image.



Le dossier zip exporté contient un fichier XML et le fichier readme.txt



Pour certains fournisseurs d'identités, vous pouvez importer le code XML directement, mais dans ce cas, il doit être importé manuellement.

- URL d'authentification unique (petite 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"
```

- ID d'entité SP

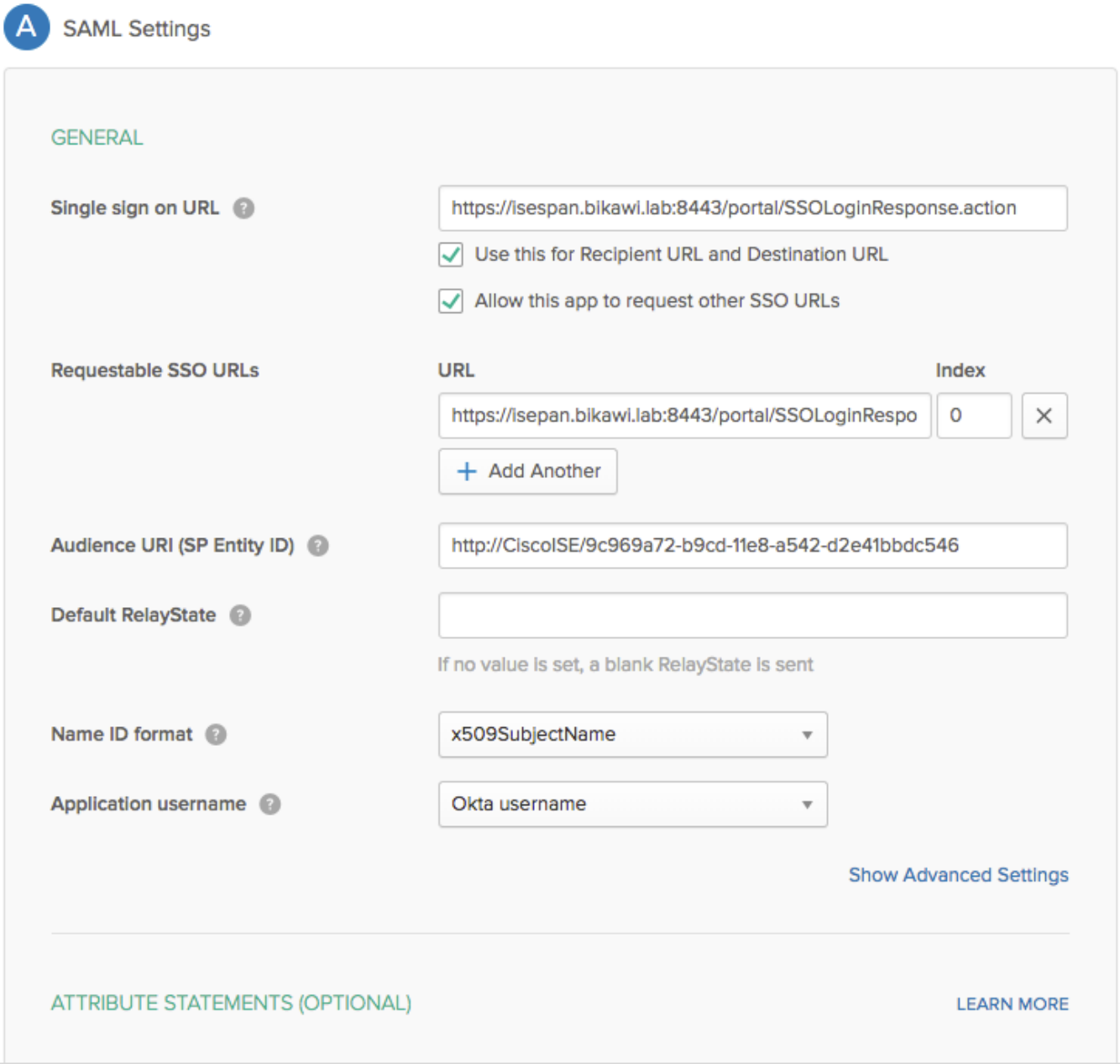
```
entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546"
```

L'URL SSO est disponible au format adresse IP et nom de domaine complet.

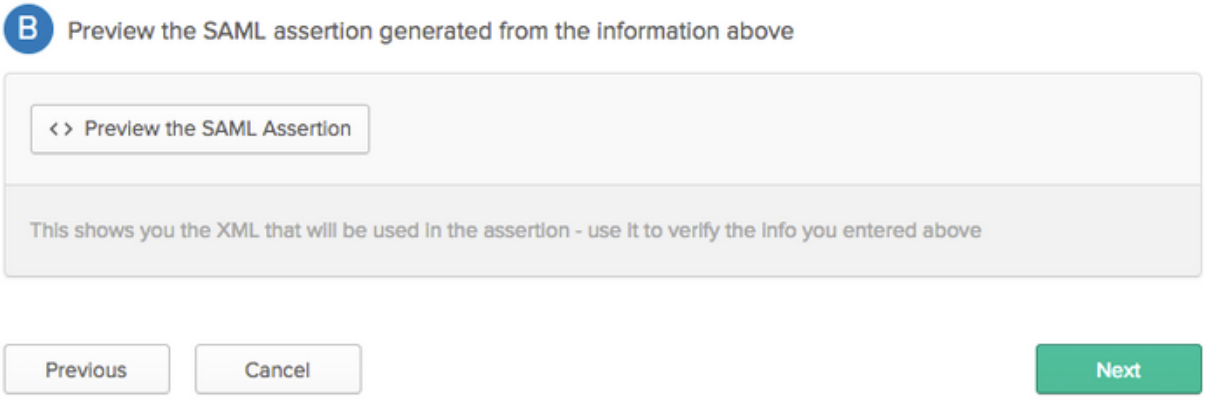
⚠ Mise en garde : La sélection du format dépend des paramètres de redirection du profil d'autorisation. Si vous utilisez l'adresse IP statique, vous devez utiliser l'adresse IP de l'URL SSO.

3. Paramètres SAML OKTA.

Étape 1 : ajout de ces URL dans les paramètres SAML

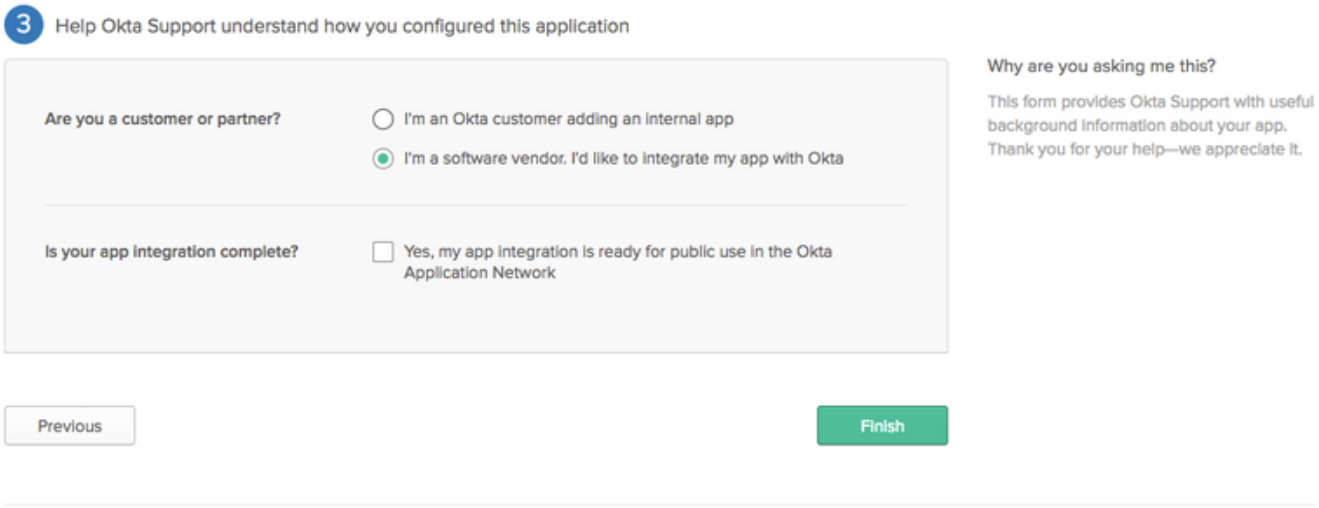


Étape 2. Vous pouvez ajouter plusieurs URL à partir du fichier XML, en fonction du nombre de PSN hébergeant ce service. Le format de l'ID de nom et le nom d'utilisateur de l'application dépendent de votre conception.

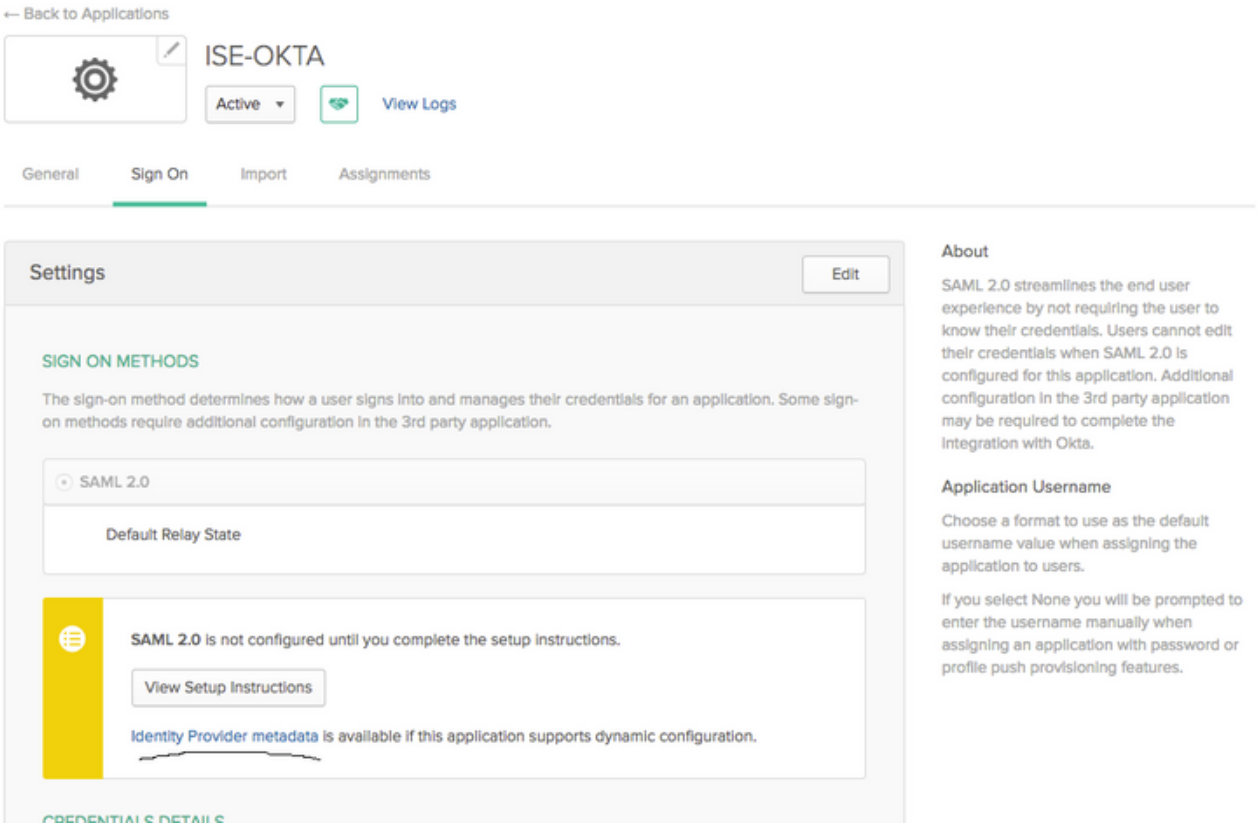



```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124" IssueInstant=
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://www.okta.com/Issuer<
    <saml2:Subject>
        <saml2:NameID 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>
```

Étape 3. Cliquez sur next et choisissez la deuxième option.



4. Exportez les métadonnées de l'application.



Métadonnées :

```
<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>
```

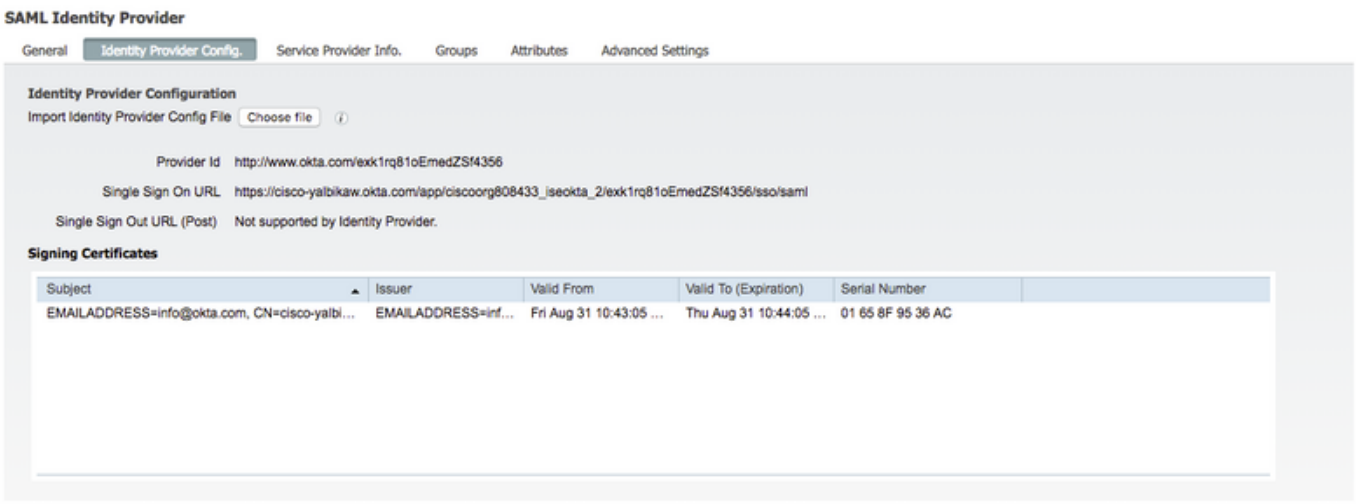
Enregistrez le fichier au format XML.

5. Affectez des utilisateurs à l'application.

Affectez des utilisateurs à cette application, il existe un moyen d'intégrer AD, comme expliqué dans : répertoire octa-actif

6. Importez des métadonnées d'Idp vers ISE.

Étape 1. Sous Fournisseur d'identité SAML, sélectionnez Configuration du fournisseur d'identité et Importer les métadonnées.



Étape 2 : enregistrement de la configuration

Étape 3.Configuration de CWA

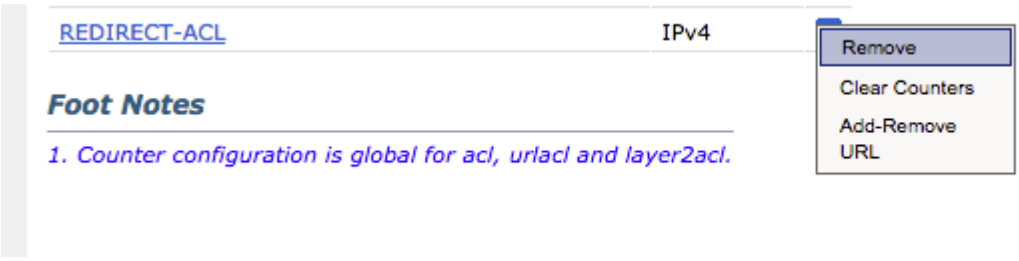
Ce document décrit la configuration pour ISE et WLC.

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

Ajouter des URL dans la liste de contrôle d'accès Redirect.

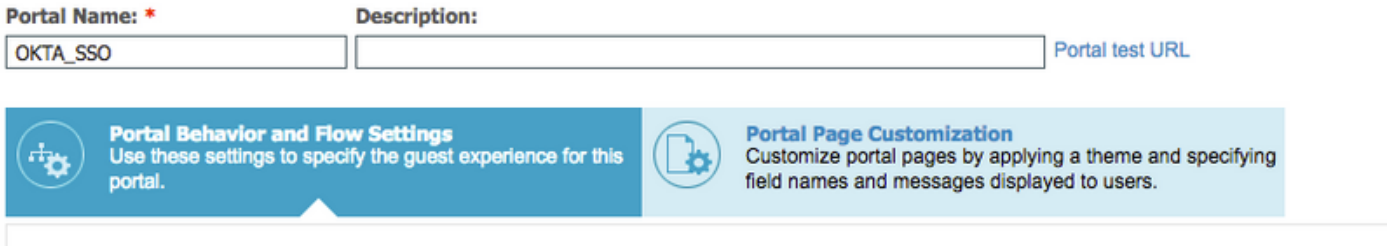
https://cisco-yalbikaw.okta.com / ajouter l'URL de votre application

https://login.okta.com

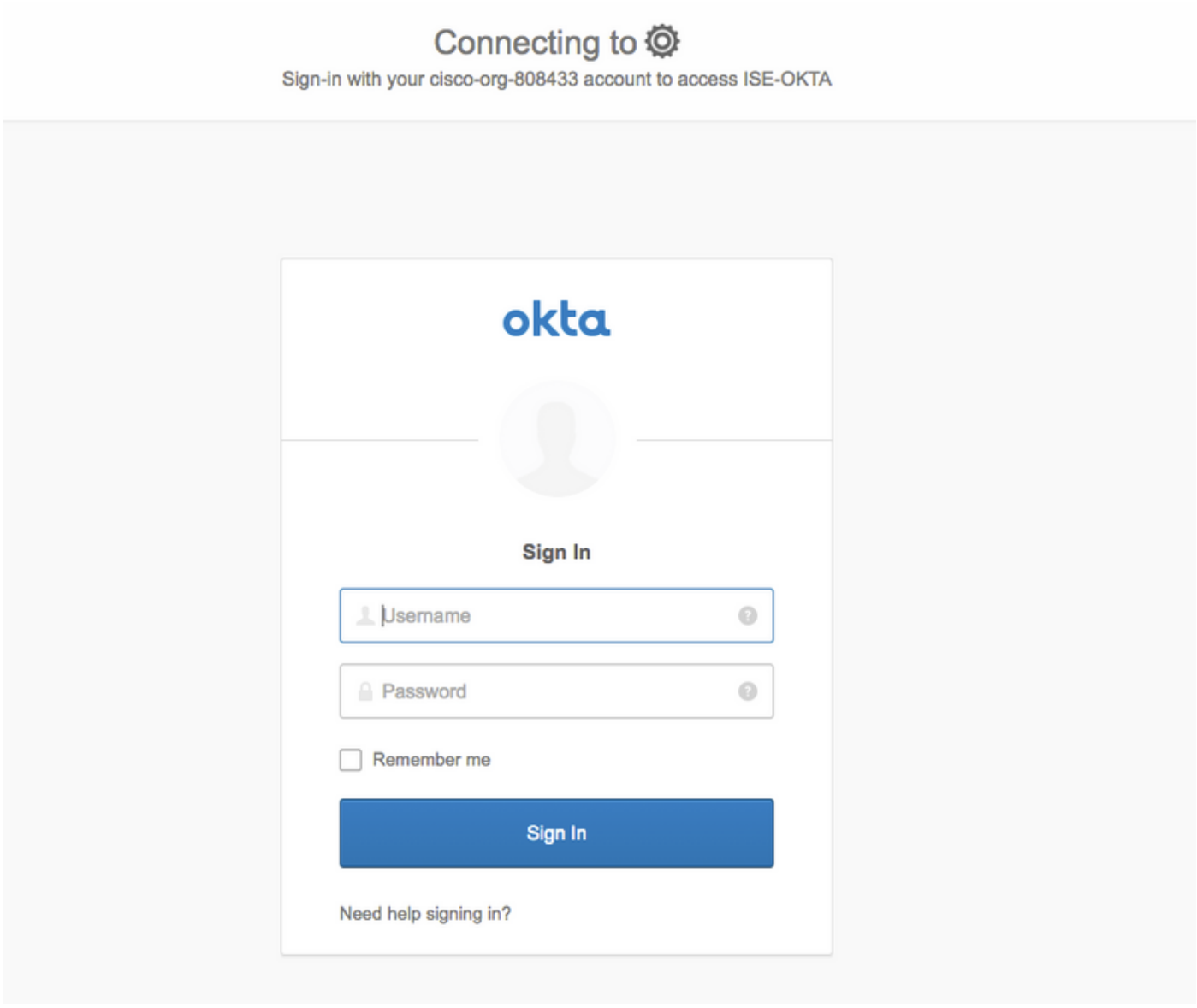


Vérifier

Testez le portail et vérifiez si vous pouvez accéder à l'application OKTA



Étape 1. Cliquez sur le test du portail, puis vous devez être redirigé vers l'application SSO.

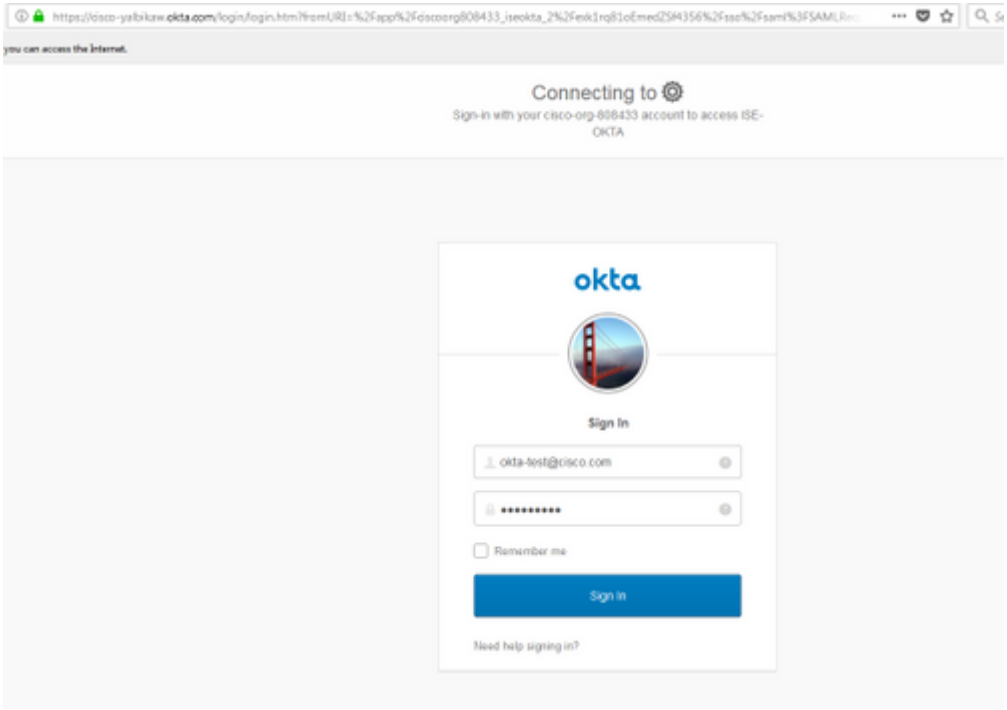


Étape 2 : vérification de la connexion d'informations à <nom de l'application>

Étape 3. Si vous entrez les informations d'identification et de connexion, une demande d'échantillon incorrecte peut s'afficher, cela ne signifie pas nécessairement que la configuration est incorrecte à ce stade.

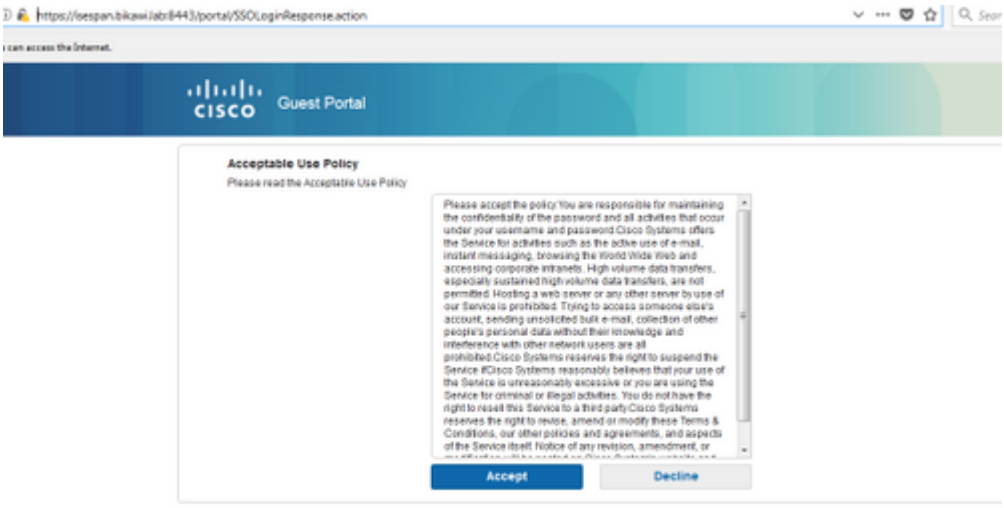
Vérification des utilisateurs finaux

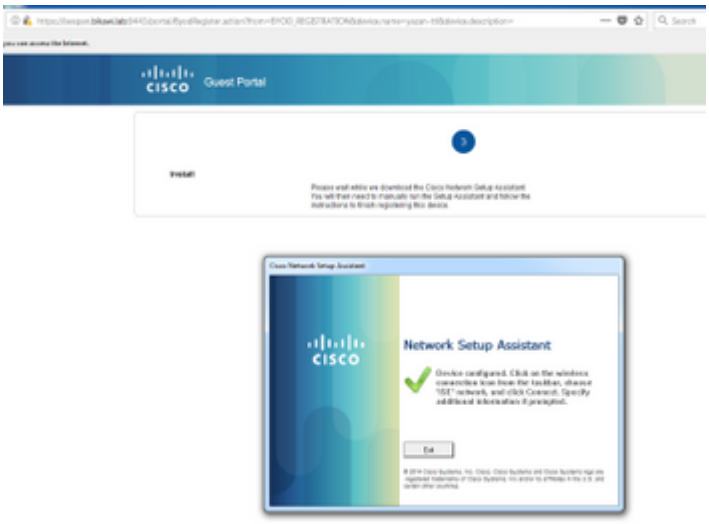






Signing in to ISE-OKTA





Vérification ISE

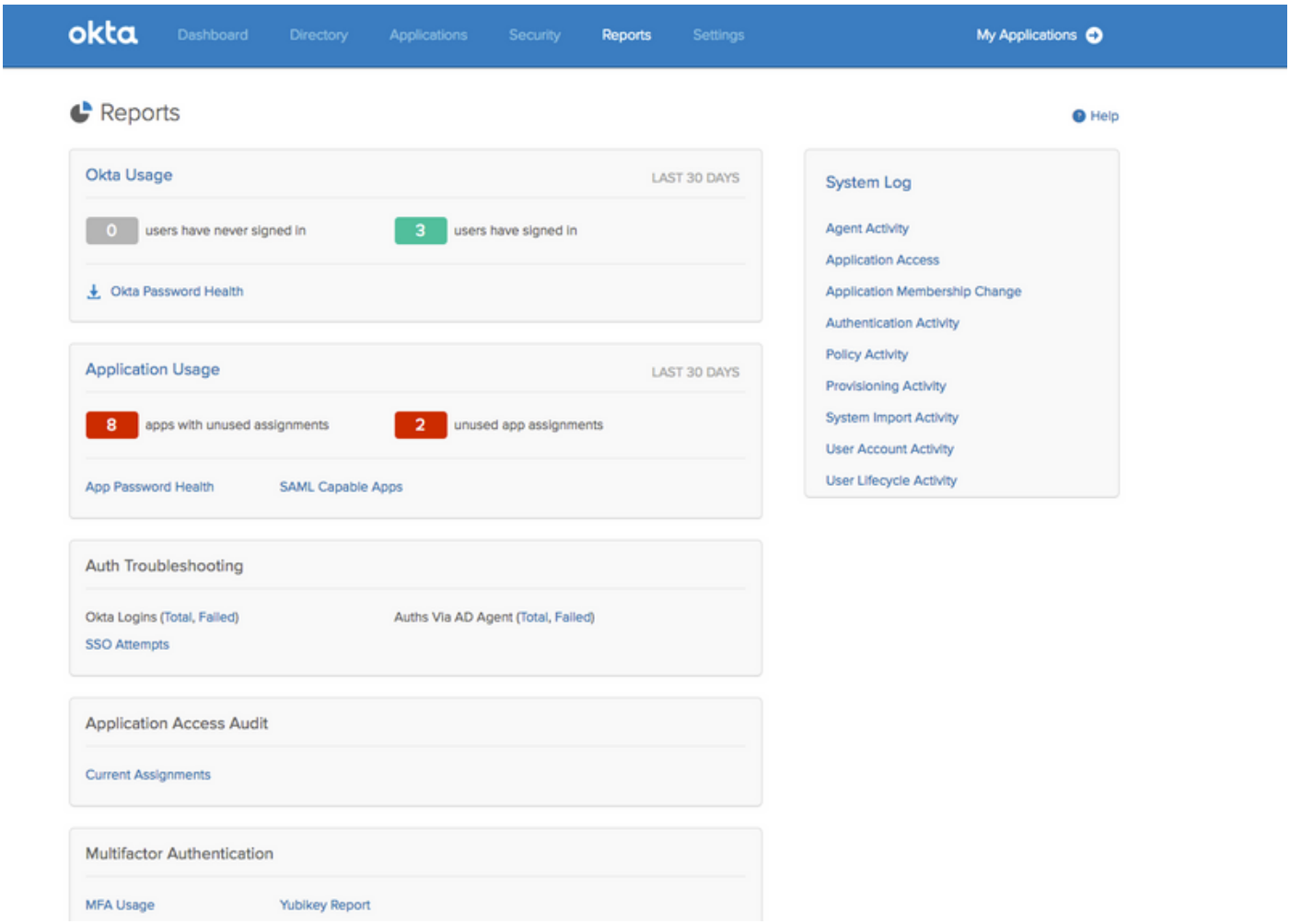
Consultez les journaux de vie pour vérifier l'état de l'authentification.



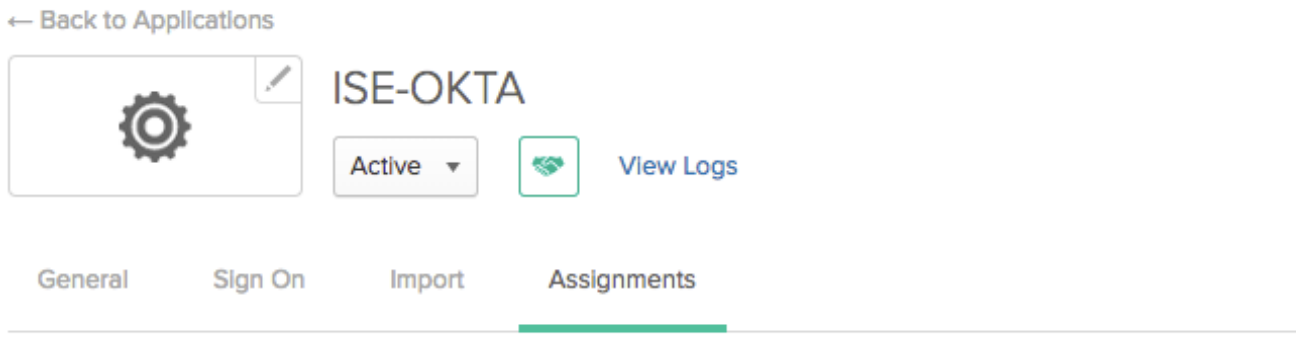
Dépannage

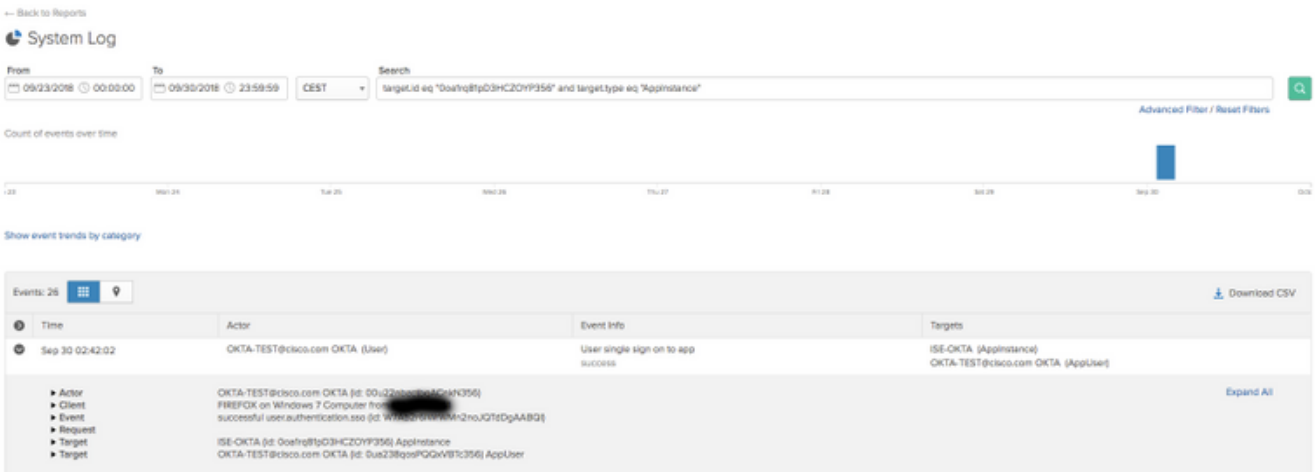
Dépannage OKTA

Étape 1. Vérifiez les journaux dans l'onglet Rapports.



Étape 2. À partir de l’application, affichez également les journaux associés.





Dépannage ISE

Deux fichiers journaux doivent être vérifiés

- ise-psc.log
- guest.log

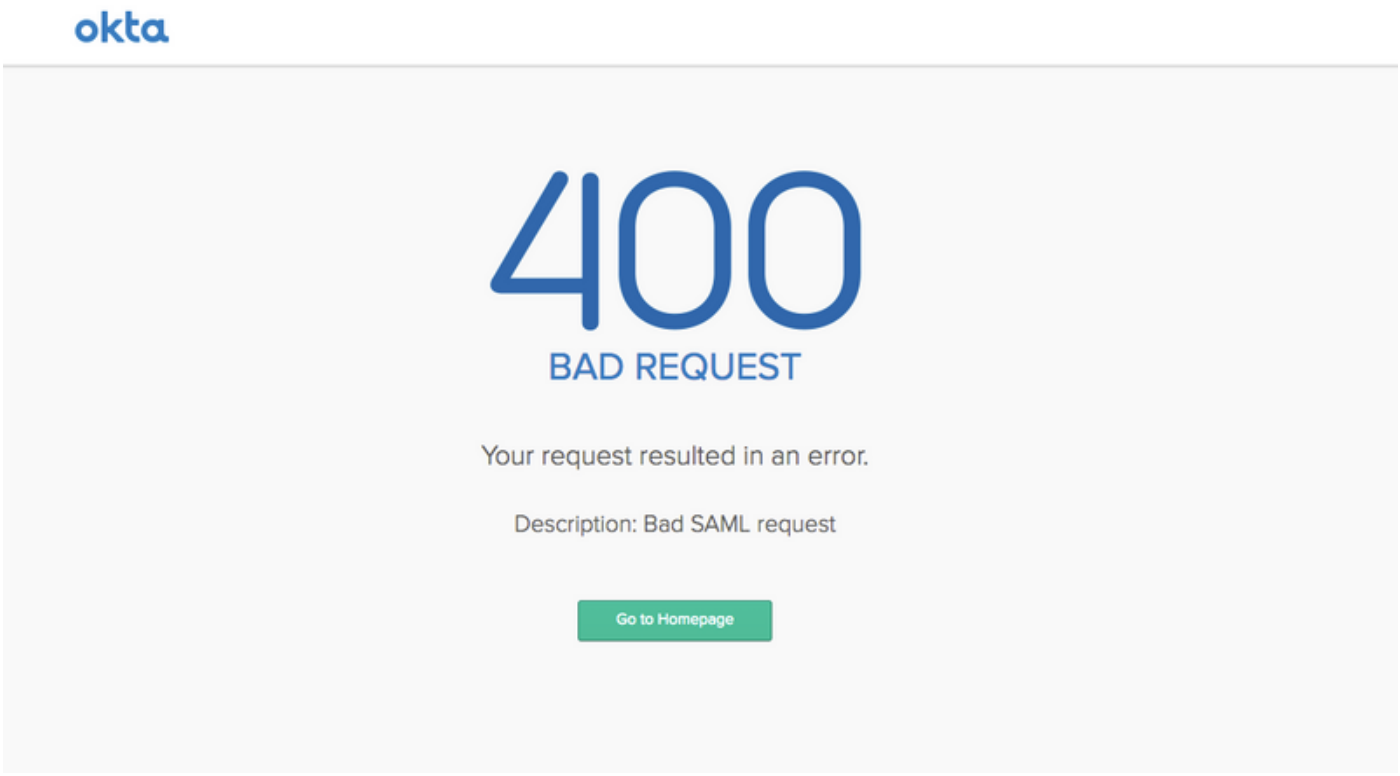
Accédez à Administration > System > Logging > Debug Log Configuration. Activez le niveau DEBUG.

SAML	ise-psc.log
Accès invité	guest.log
Portail	guest.log

Le tableau indique le composant à déboguer et le fichier journal correspondant.

Problèmes courants et solutions

Scénario 1. Demande SAML incorrecte.



Cette erreur est générique. Vérifiez les journaux afin de vérifier le flux et de localiser le problème. Sur ISE guest.log :

ISE# show logging application guest.log | 50 derniers

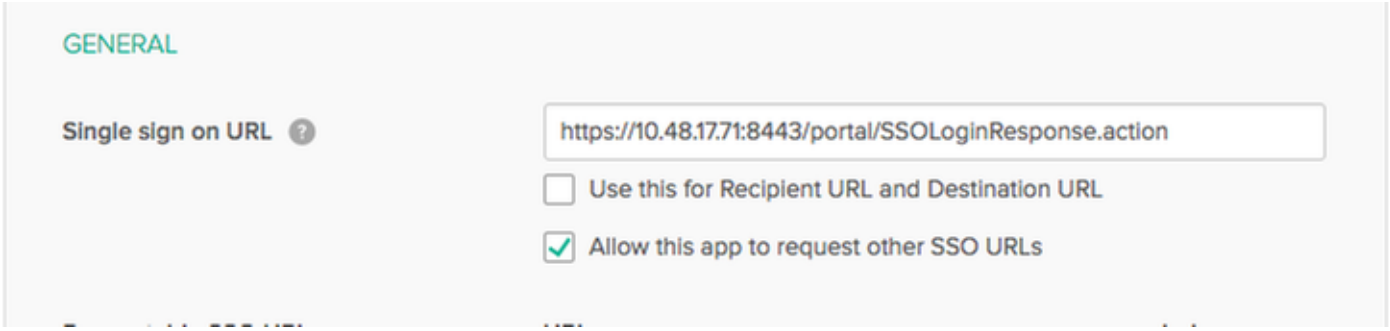
```
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con

        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.con
onId=0a3e949b000002c55bb023b3;
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,624 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
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
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.uti
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJOOb4672
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgd
1bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,626 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
2018-09-30 01:32:35,627 DEBUG  [https-jsse-nio-10.48.17.71-8443-exec-2][] cisco.ise.portalwebaction.con
```

ISE a correctement redirigé l'utilisateur vers l'IDP. Cependant, aucune réponse à ISE et la mauvaise requête SAML apparaît. Indiquez que OKTA n'accepte pas notre demande SAML ci-dessous.

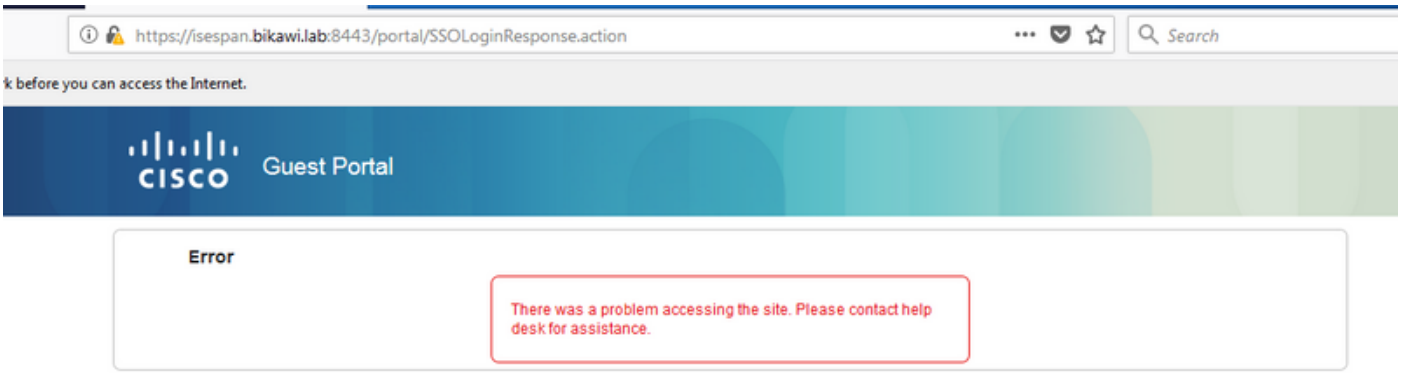
```
https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=
Ib%2FSuT7EJMPIBahYpRqkWBlJOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEf
HO4QZ2tLaAPLy2ww9pDwdpHQY%2Bizlld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3ugJMm%2B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

Vérifiez à nouveau l'application. Des modifications ont peut-être été apportées.



L'URL SSO utilise l'adresse IP, cependant, l'invité envoie un nom de domaine complet (FQDN) comme nous pouvons le voir dans la requête ci-dessus, la dernière ligne contient SEMI_DELIMITER<FQDN> pour résoudre ce problème. Modifiez l'adresse IP en FQDN sur les paramètres OKTA.

Scénario 2. « Un problème est survenu lors de l'accès au site. Veuillez contacter le support technique pour obtenir de l'aide.



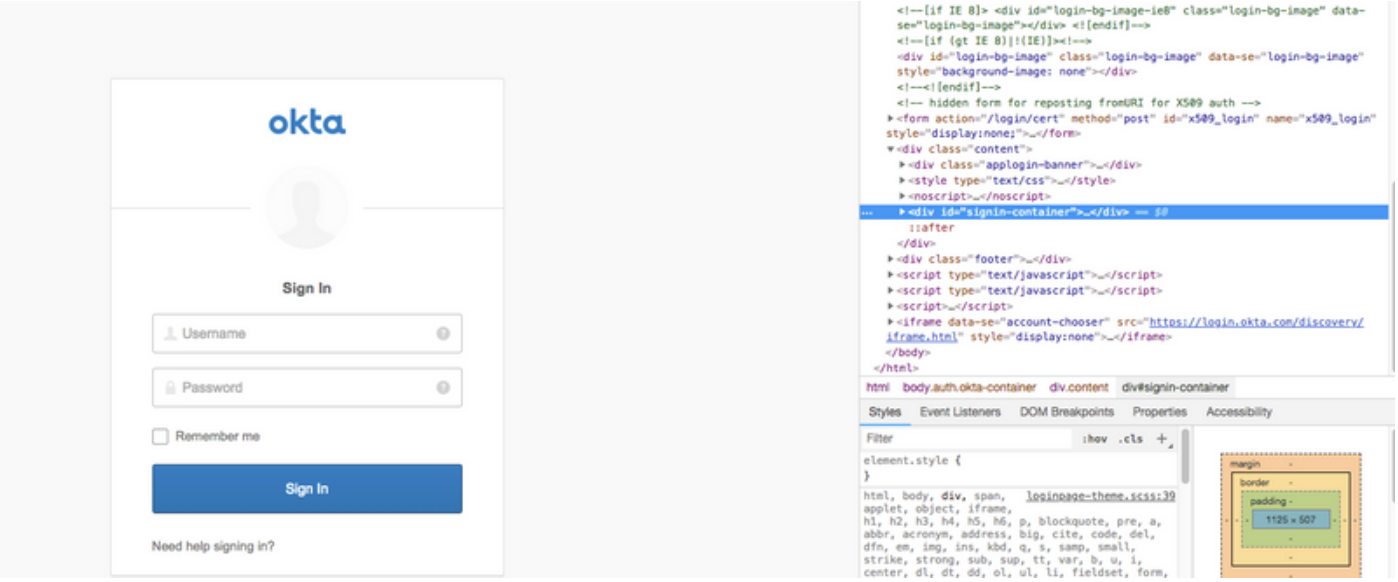
Invité.log

```
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.
```

À partir des journaux, ISE signale que l'assertion est incorrecte. Cochez OKTA Audience URI pour vous assurer qu'il correspond au SP pour le résoudre.

Scénario 3. Redirigé vers la page vide ou l'option de connexion ne s'affiche pas.

Cela dépend de l'environnement et de la configuration du portail. Dans ce genre de problème, vous devez vérifier l'application OKTA et quelle URL est nécessaire pour l'authentification. Cliquez sur le test du portail, puis inspectez l'élément pour vérifier quels sites Web doivent être accessibles.



Dans ce scénario, seulement deux URL : et login.okta.com - ceux-ci devraient être autorisés sur le WLC.

Informations connexes

- 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.