

Configurer le portail invité ISE 2.3 avec OKTA SAML SSO

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[SSO fédérée](#)

[Flux réseau](#)

[Configuration](#)

[Étape 1. Configurez le fournisseur d'identités SAML et le portail invité sur ISE.](#)

[1. Préparer la source d'identité externe.](#)

[2. Créer un portail pour SSO.](#)

[3. Configurez une connexion alternative.](#)

[Étape 2. Configurez les paramètres de l'application OKTA et du fournisseur d'identité SAML.](#)

[1. Créer une application OKTA.](#)

[2. Exporter les informations SP à partir du fournisseur d'identité SAML.](#)

[3. Paramètres SAML OKTA.](#)

[4. Exporter les métadonnées à partir de l'application.](#)

[5. Affecter des utilisateurs à l'application.](#)

[6. Importez des métadonnées depuis Idp vers ISE.](#)

[Étape 3. Configuration CWA](#)

[Vérification](#)

[Vérification de l'utilisateur final](#)

[Vérification ISE](#)

[Dépannage](#)

[Dépannage d'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 SAML (Security Assertion Markup Language Single Sign-On) pour le portail invité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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 SSO OKTA SAML
- 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 de l'organisation peut s'authentifier une fois puis avoir accès à plusieurs ressources. Cette identité utilisée dans toutes les organisations est appelée identité fédérée.

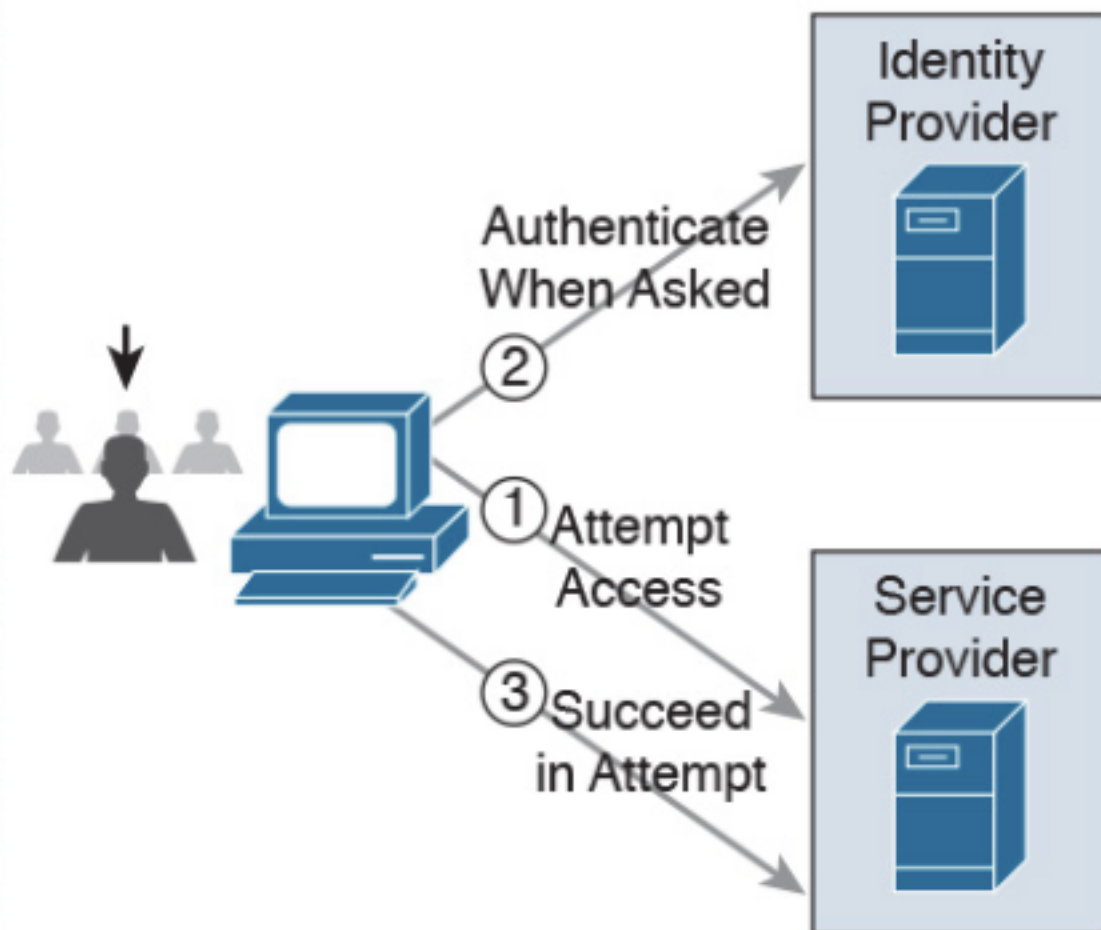
Le concept de fédération :

- Principe : Utilisateur final (celui qui demande un service), navigateur Web, dans ce cas, est le point de terminaison.
- Fournisseur de services (SP) : parfois appelé partie de confiance (RP), qui est le système qui fournit un service, dans ce cas, ISE.
- Fournisseur d'identité (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 IdP au SP.

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

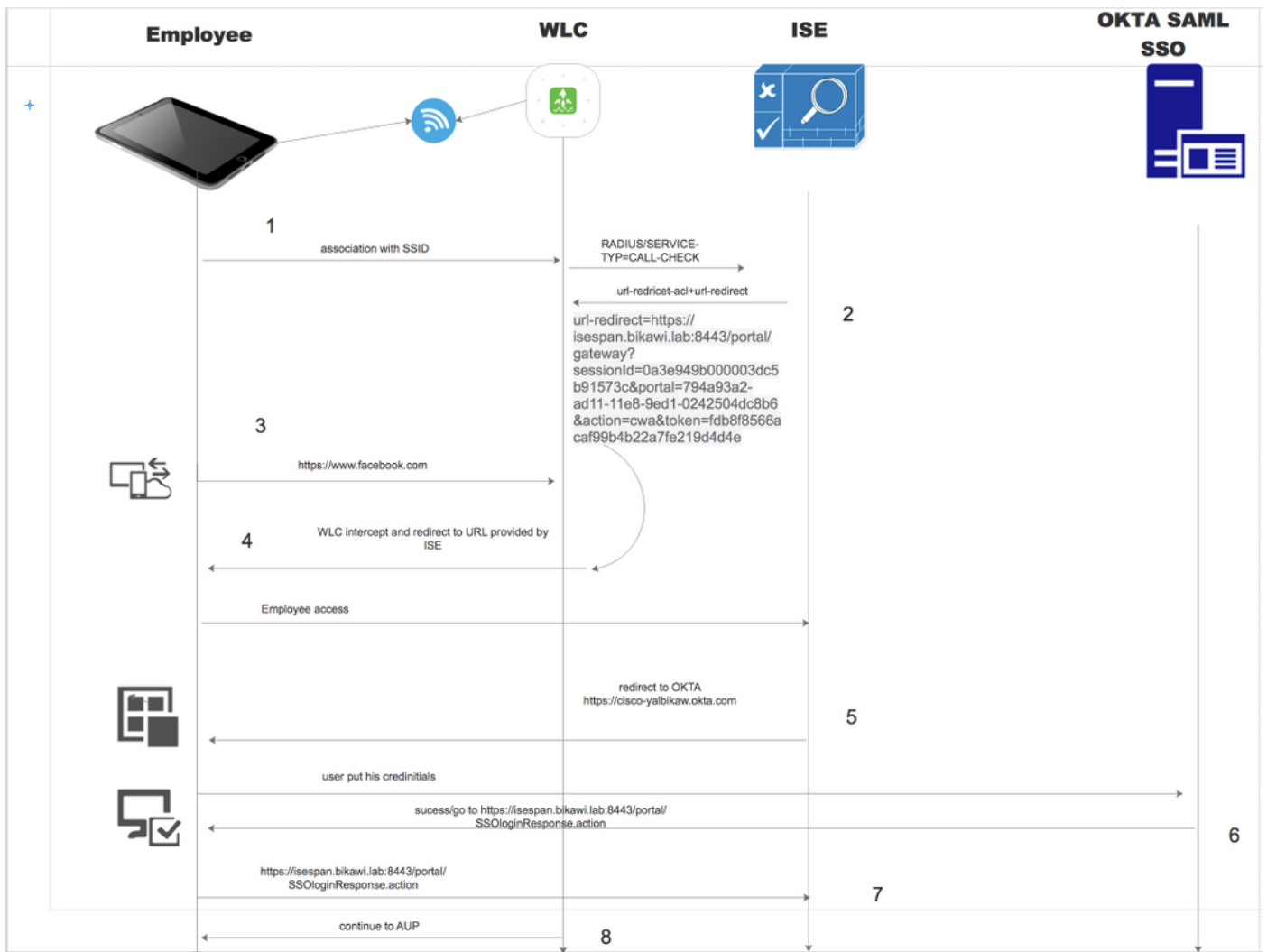
SAML est un cadre XML qui décrit l'utilisation et l'échange d'assertions SAML de manière sécurisée entre les entités commerciales. La norme décrit la syntaxe et les règles pour demander, créer, utiliser et échanger ces assertions.

ISE utilise le mode initié par SP. L'utilisateur est redirigé vers le portail invité, puis ISE le redirige vers IdP pour s'authentifier. Après cela, il redirige vers ISE. La demande est validée, l'utilisateur procède à l'accès invité ou à l'intégration, selon la configuration du portail.



SP-initiated

Flux réseau



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

Pour plus d'informations sur SAML, cliquez sur le lien ci-dessous

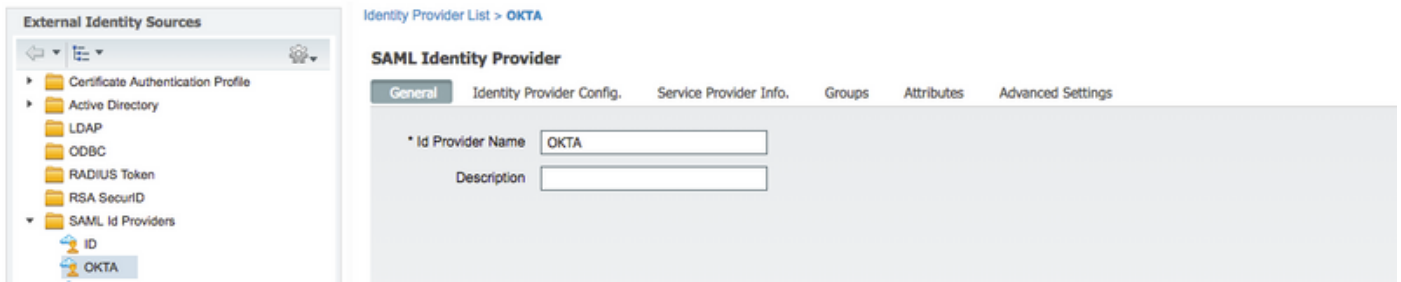
<https://developer.okta.com/standards/SAML/>

Configuration

Étape 1. Configurez le fournisseur d'identités SAML et le portail invité sur ISE.

1. Préparer la source d'identité externe.

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

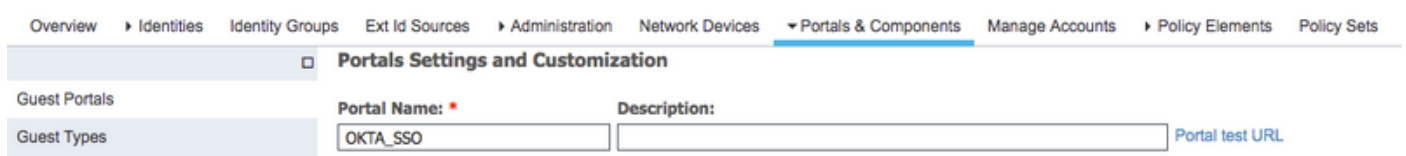
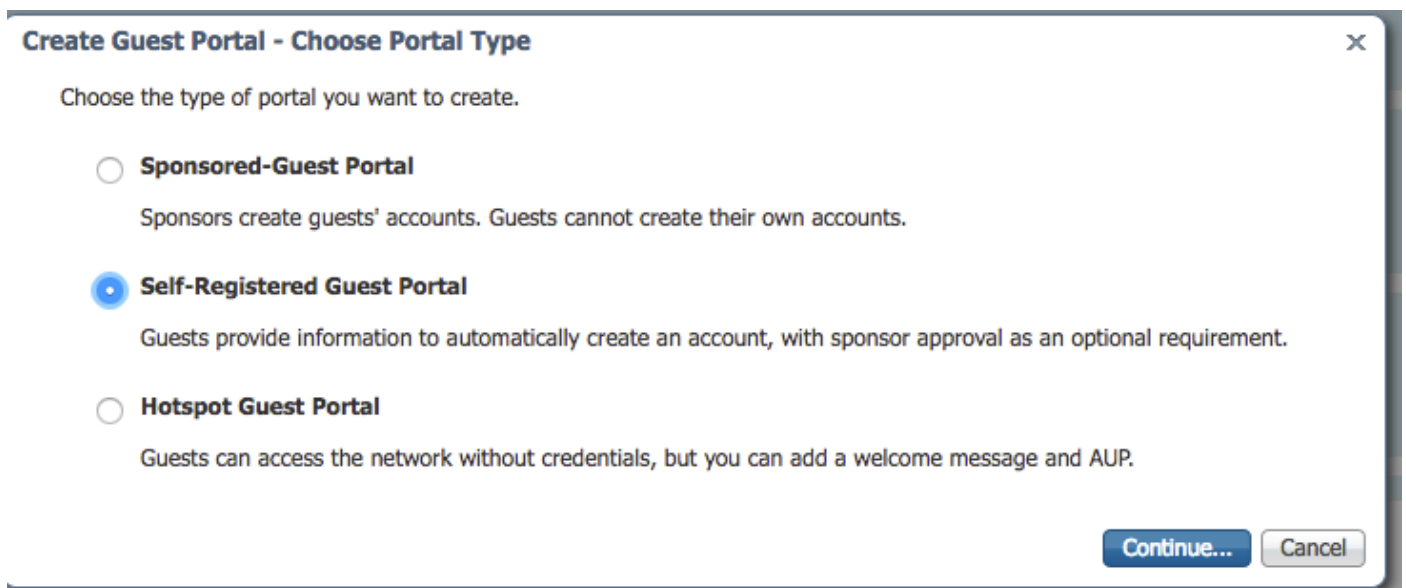


Étape 2. Attribuez un nom au fournisseur d'ID et envoyez la configuration.

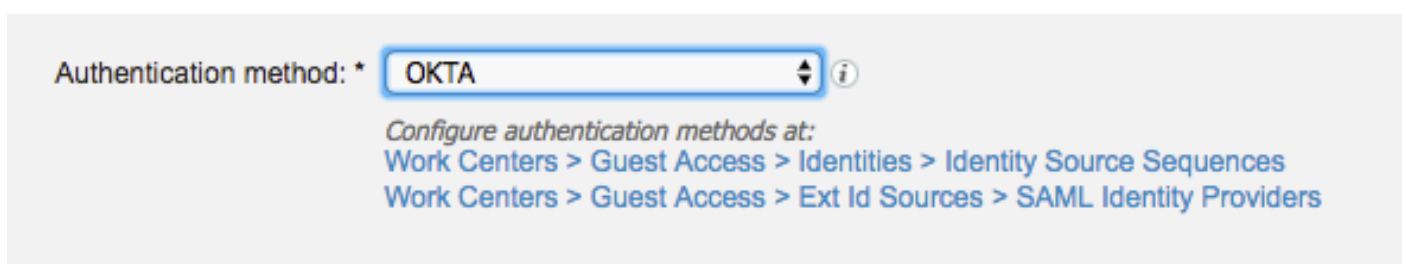
2. Créer un portail pour SSO.

Étape 1. Créez le portail affecté à OKTA comme source d'identité. Toute autre configuration pour le BYOD, l'enregistrement des périphériques, l'invité, 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 **Centres de travail > Accès invité > Portails et composants** et créez le portail.



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



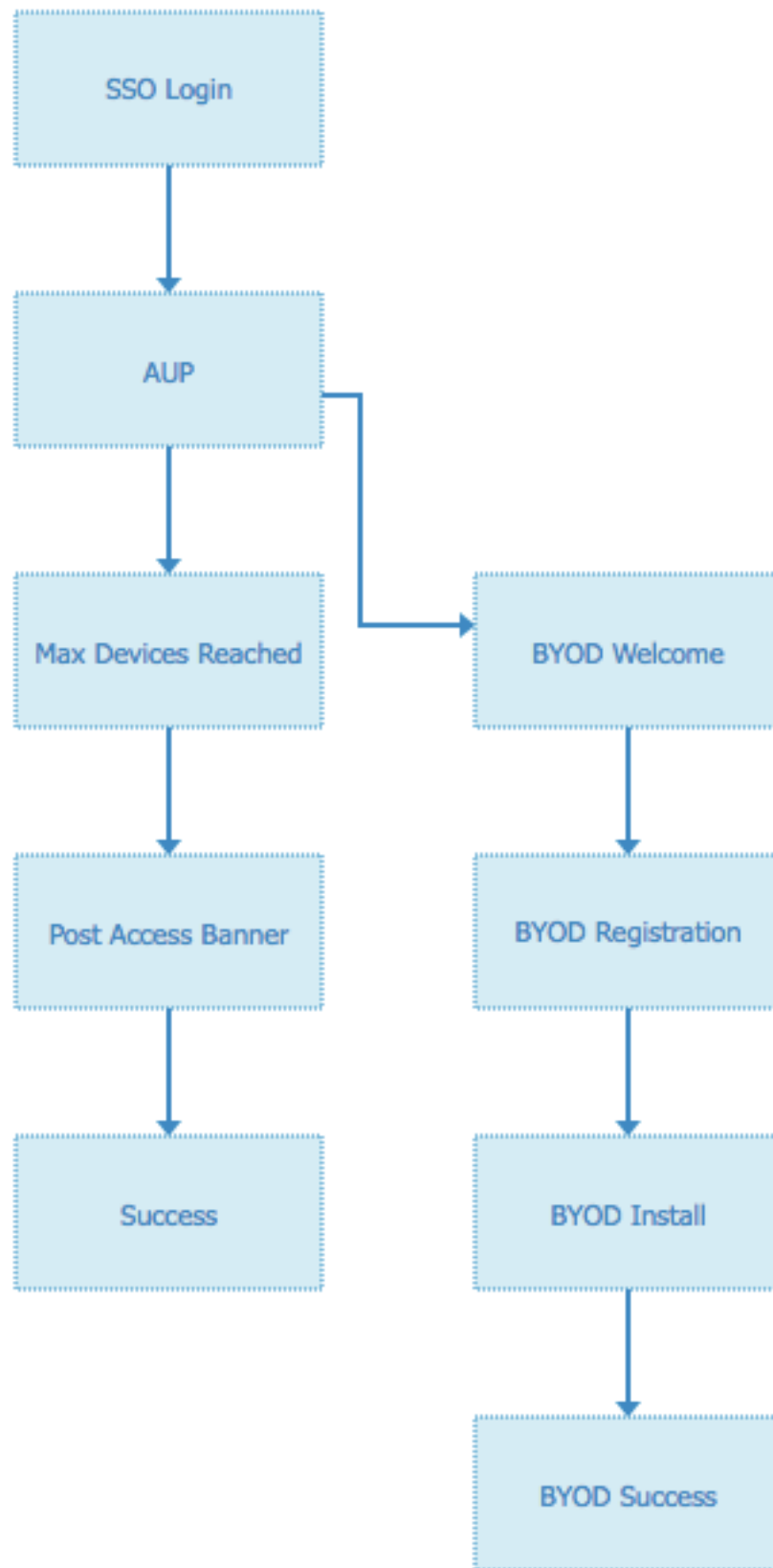
Étape 4. Sélectionnez la source d'identité OKTA comme méthode d'authentification.

(facultatif) sélectionnez les paramètres BYOD.

The screenshot shows the 'BYOD Settings' configuration page. At the top, there is a section titled 'BYOD Settings' with a dropdown arrow. Below this, there are several configuration options:

- Allow employees to use personal devices on the network
 - Endpoint identity group:
 - Configure endpoint identity groups at [Administration > Identity Management > Groups > Endpoint Identity Groups](#)
 - The endpoints in this group will be purged according to the policies defined in: [Administration > Identity Management > Settings > Endpoint purge](#)
- Allow employees to choose to guest access only
- Display Device ID field during registration
 - Configure employee registered devices at [Work Centers > BYOD > Settings > Employee Registered Devices](#)
- After successful device configuration take employee to:
 - Originating URL (i)
 - Success page
 - URL:

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



3. Configurez une connexion alternative.

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

Accédez au portail invité d'auto-inscription 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.

▼ Login Page Settings

Require an access code:

Maximum failed login attempts before rate limiting: (1 - 999)

Time between login attempts when rate limiting: minutes (1 - 3000)

Include an AUP

Require acceptance

Require scrolling to end of AUP

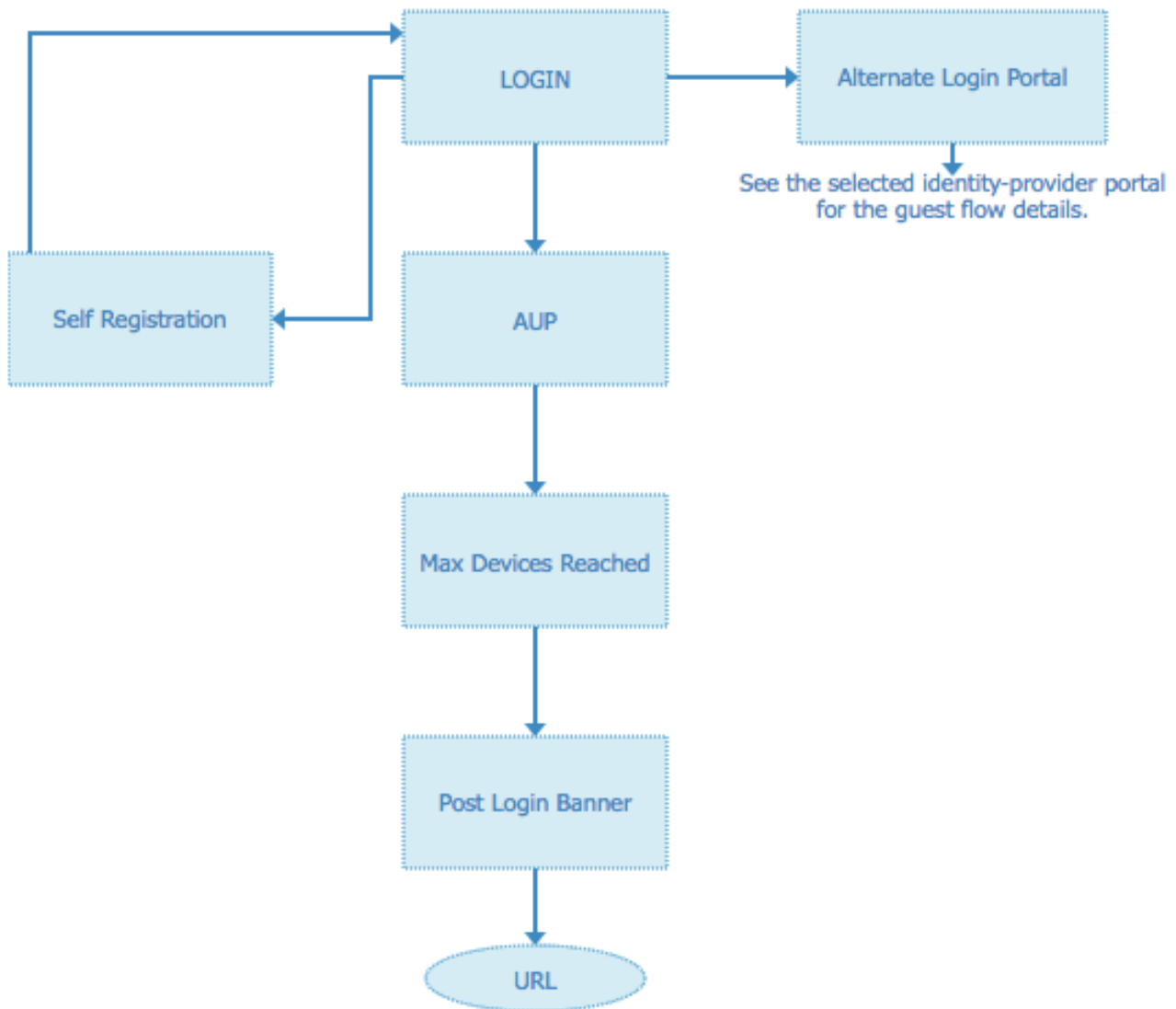
Allow guests to create their own accounts

Allow social login

Allow guests to change password after login ⓘ

Allow the following identity-provider guest portal to be used for login ⓘ

Voici le flux du portail maintenant.



Étape 2. Configurez les paramètres de l'application OKTA et du fournisseur d'identité SAML.

1. Créer une application OKTA.

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

← Back to Applications

Add Application

Search for an application

All A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Can't find an app?
Create New App
Apps you created (0) →

INTEGRATION PROPERTIES

Any
Supports SAML
Supports Provisioning

	Teladoc Okta Verified	Add
	&frankly Okta Verified ✓ SAML	Add
	10000ft Okta Verified	Add
	101domains.com Okta Verified	Add

Étape 2. Cliquez sur Ajouter une application.

okta Dashboard Directory Applications Security Reports Settings My Applications

Applications Help

Add Application Assign Applications

Q Search

STATUS

ACTIVE	0
INACTIVE	3

No active apps found
Add application and assign access to have them appear on your users' Okta home Page

© 2018 Okta, Inc. Privacy Version 2018.36 US Cell 7 Trust site Download Okta Plugin Feedback

Étape 3. Créer une nouvelle application, sélectionnez-la 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

Paramètres généraux

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

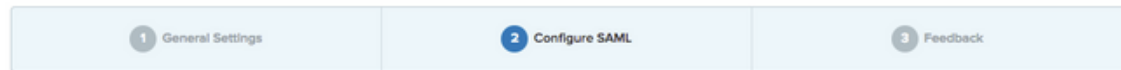


Do not display application icon in the Okta Mobile app

Cancel

Next

Create SAML Integration



A SAML Settings

GENERAL

Single sign on URL

Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
------	------------------------	-------

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

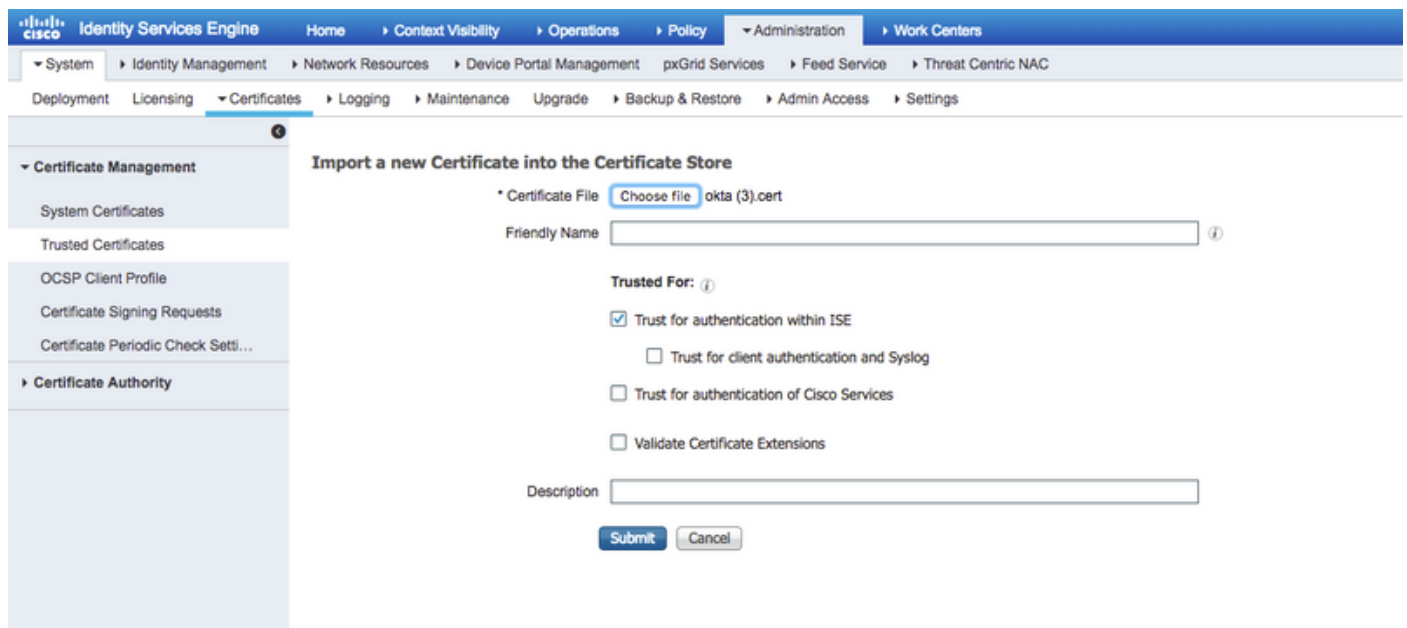
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

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



Import a new Certificate into the Certificate Store

* Certificate File okta (3).cert

Friendly Name

Trusted For:

Trust for authentication within ISE
 Trust for client authentication and Syslog
 Trust for authentication of Cisco Services
 Validate Certificate Extensions

Description

2. Exporter les informations SP à partir du fournisseur d'identité SAML.

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

Étape 1. Ajoutez ces URL aux paramètres SAML.

A SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Requestable SSO URLs

URL	Index	
<input type="text" value="https://isespan.bikawi.lab:8443/portal/SSOLoginRespo"/>	<input type="text" value="0"/>	<input type="button" value="X"/>

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

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

B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

```
<?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</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

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

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

Is your app integration complete?

Yes, my app integration is ready for public use in the Okta Application Network

Previous
Finish

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

4. Exporter les métadonnées à partir de l'application.


```
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>
```

Enregistrez le fichier au format XML.

5. Affecter des utilisateurs à l'application.

Affecter des utilisateurs à cette application, il existe un moyen d'intégration AD, expliqué dans : [répertoire okta-active](#)

6. Importez des métadonnées depuis Idp vers ISE.

Étape 1. Sous **Fournisseur d'identité SAML**, sélectionnez **Config. fournisseur d'identité.** et Importer des métadonnées.

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups Attributes Advanced Settings

Identity Provider Configuration

Import Identity Provider Config File (i)

Provider Id http://www.okta.com/exk1rq81oEmedZSf4356

Single Sign On URL https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml

Single Sign Out URL (Post) Not supported by Identity Provider.

Signing Certificates

Subject	Issuer	Valid From	Valid To (Expiration)	Serial Number
EMAILADDRESS=info@okta.com, CN=cisco-yalbi...	EMAILADDRESS=inf...	Fri Aug 31 10:43:05 ...	Thu Aug 31 10:44:05 ...	01 65 8F 95 36 AC

Étape 2. Enregistrez la configuration.

Étape 3. Configuration 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>

Ajoutez des URL dans Redirect-ACL.

<https://cisco-yalbikaw.okta.com> / ajoutez votre URL d'application

<https://login.okta.com>

[REDIRECT-ACL](#)

IPv4

Remove

Clear Counters

Add-Remove

URL

Foot Notes

1. Counter configuration is global for acl, urlacl and layer2acl.

Vérification

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

Portal Name: *

Description:

OKTA_SSO

[Portal test URL](#)



Portal Behavior and Flow Settings

Use these settings to specify the guest experience for this portal.



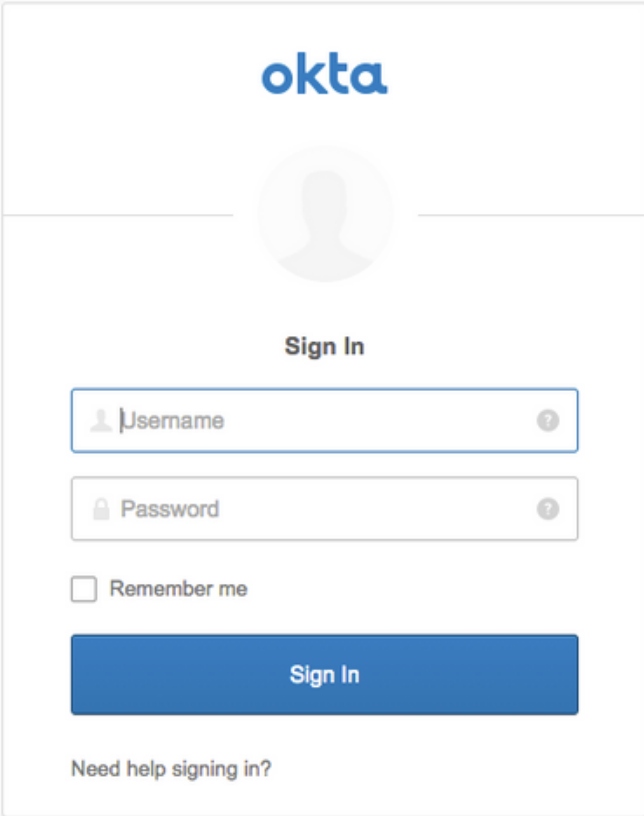
Portal Page Customization

Customize portal pages by applying a theme and specifying field names and messages displayed to users.

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

Connecting to

Sign-in with your cisco-org-808433 account to access ISE-OKTA



The image shows a screenshot of the Okta sign-in interface. At the top, the Okta logo is displayed in blue. Below the logo is a circular placeholder for a user profile picture. Underneath the profile picture, the text "Sign In" is centered. There are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields have a small question mark icon to their right. Below the password field is a checkbox labeled "Remember me". A large blue button with the text "Sign In" is positioned below the checkbox. At the bottom of the form, there is a link that says "Need help signing in?".

Étape 2. Vérifiez la **connexion** d'informations à **<nom de l'application>**

Étape 3. Si vous entrez les informations d'identification, vous risquez de voir une mauvaise demande de type saml, cela ne signifie pas nécessairement que la configuration est erronée à ce stade.

Vérification de l'utilisateur final

You can access the Internet.



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?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



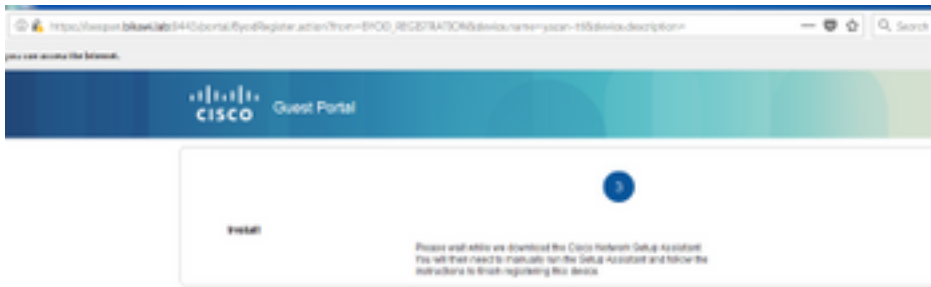
Acceptable Use Policy

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



Vérification ISE

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

Sep 30, 2018 12:39:09.514 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	okta-test@cisco.c...	3C:A8:F4:34:9F:70					
Sep 30, 2018 12:33:32.640 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3C:A8:F4:34:9F:70	3C:A8:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest		yazan-cpp

Dépannage

Dépannage d'OKTA

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

Reports

Help

Okta Usage LAST 30 DAYS

0 users have never signed in 3 users have signed in

[Okta Password Health](#)

Application Usage LAST 30 DAYS

8 apps with unused assignments 2 unused app assignments

[App Password Health](#) [SAML Capable Apps](#)

Auth Troubleshooting

Okta Logins (Total, Failed) Auths Via AD Agent (Total, Failed)

[SSO Attempts](#)

Application Access Audit

[Current Assignments](#)

Multifactor Authentication

[MFA Usage](#) [Yubikey Report](#)

System Log

- Agent Activity
- Application Access
- Application Membership Change
- Authentication Activity
- Policy Activity
- Provisioning Activity
- System Import Activity
- User Account Activity
- User Lifecycle Activity

Étape 2. Également à partir de l'affichage de l'application, les journaux associés.

← Back to Applications



ISE-OKTA

Active



View Logs

General Sign On Import Assignments

← Back to Reports

System Log

From: 09/23/2018 00:00:00 To: 09/30/2018 23:59:59 CEST Search: target.id eq "0ea7e81b031c2019356" and target.type eq "AppInstance"



Show event trends by category

Events: 25 [Download CSV](#)

Time	Actor	Event Info	Targets
Sep 30 02:42:02	OKTA-TEST@cisco.com OKTA (User)	User single sign on to app SUCCESS	ISE-OKTA (AppInstance) OKTA-TEST@cisco.com OKTA (AppUser)
<ul style="list-style-type: none"> Actor: OKTA-TEST@cisco.com OKTA (id: 00a218031c2019356) Client: FIREFOX on Windows 7 Computer from [REDACTED] Event: successful user.authentication.sso (id: W1a2c01911Mh2noJGtDgAABQ) Request: ISE-OKTA (id: 0ea7e81b031c2019356) AppInstance Target: OKTA-TEST@cisco.com OKTA (id: 0ea218031c2019356) AppUser 			

Dépannage ISE

Il y a deux fichiers journaux à vérifier

- 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. Requête SAML incorrecte.

okta



400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

Cette erreur est générique, vérifiez les journaux afin de vérifier le flux et d'identifier le problème.
Sur ISE guest.log :

ISE# show logging application guest.log | 50 dernières

```
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
```

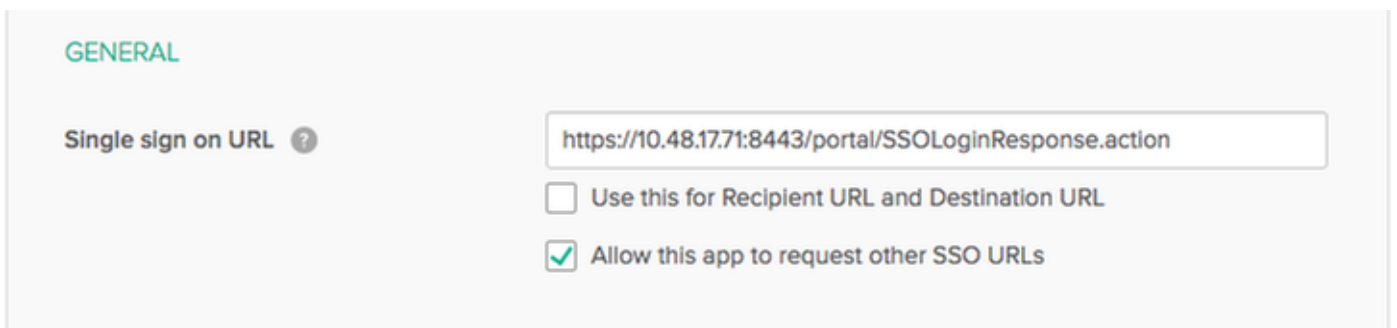


```
Identity Provider: com.cisco.cpm.acs.im.identitystore.saml.IdentityProvider@56c50ab6
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- portalSessionInfo:
portalId=9c969a72-b9cd-11e8-a542-d2e41bbdc546;portalSessionId=6770f0a4-bc86-4565-940a-
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/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bzil1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%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_DELIMITERisepan.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/exklrq81oEmedZSf4356/sso/saml
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bzil1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%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_DELIMITERisepan.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 a correctement redirigé l'utilisateur vers le PCI. Cependant, aucune réponse à ISE et la mauvaise demande SAML n'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=nZRdb9o  
wF  
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrjGZKmv0  
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BvYWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fB1QnC  
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_DELIMITERis espan.bikawi.lab
```

Maintenant, vérifiez à nouveau l'application peut-être qu'il ya des changements effectués.



GENERAL

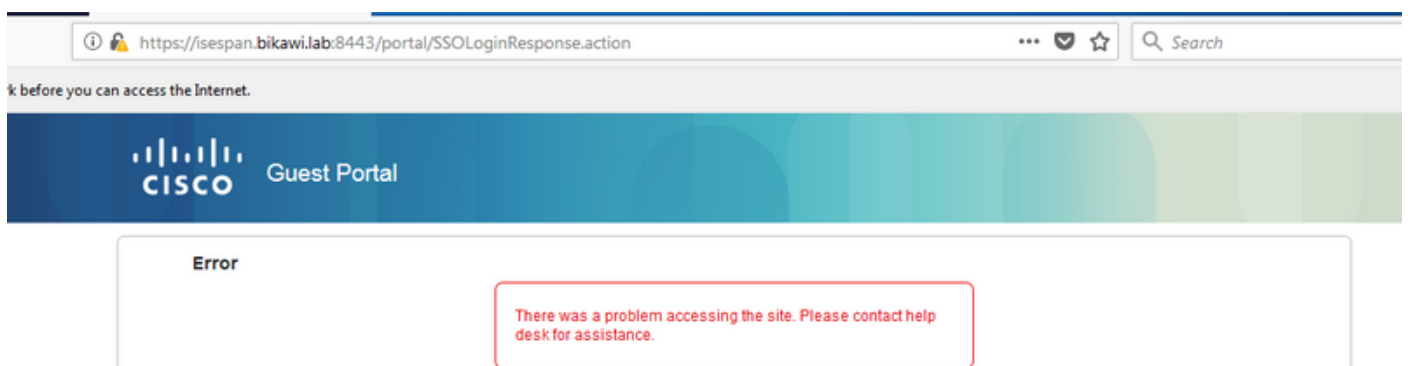
Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

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

Scénario 2. « Un problème s'est produit lors de l'accès au site. Veuillez contacter le service d'assistance 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.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

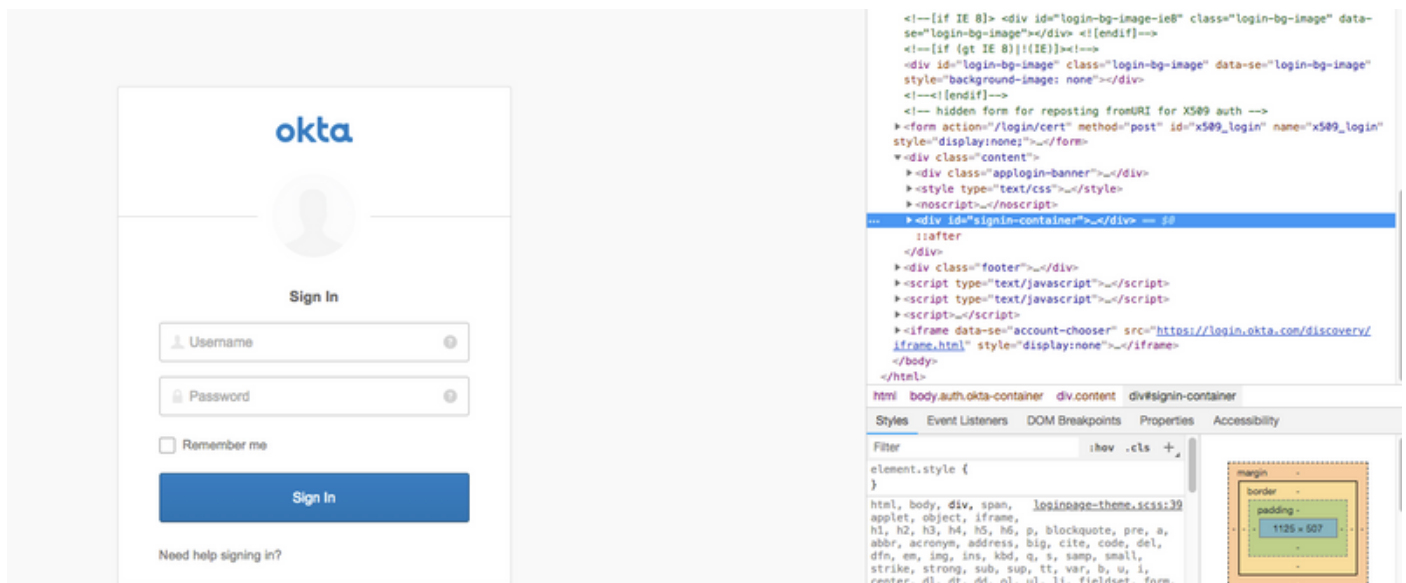
2018-09-30 02:25:00,609 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1]]

guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- Login error with idp

À partir des journaux, ISE signale que l'assertion n'est pas correcte. Vérifiez l'URI de l'audience OKTA 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 type de problème, vous devez vérifier l'application OKTA et l'URL requise 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 : application et login.okta.com - ceux-ci doivent 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>