

# OKTA SAML SSOによるISE 2.3ゲストポータル の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[フェデレーテッドSSO](#)

[ネットワークフロー](#)

[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](#)

[2. SSOのポータルを作成します。](#)

[3. 代替ログインの設定](#)

[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。](#)

[2. SAML Identity ProviderからSP情報をエクスポートします。](#)

[3. OKTA SAML設定](#)

[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。](#)

[5. アプリケーションへのユーザーの割り当て](#)

[6. IDPからISEへのメタデータのインポート。](#)

[ステップ3: CWAの設定。](#)

[確認](#)

[エンドユーザの検証](#)

[ISEの検証](#)

[トラブルシューティング](#)

[OKTAのトラブルシューティング](#)

[ISEのトラブルシューティング](#)

[一般的な問題と解決策](#)

[関連情報](#)

## 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。

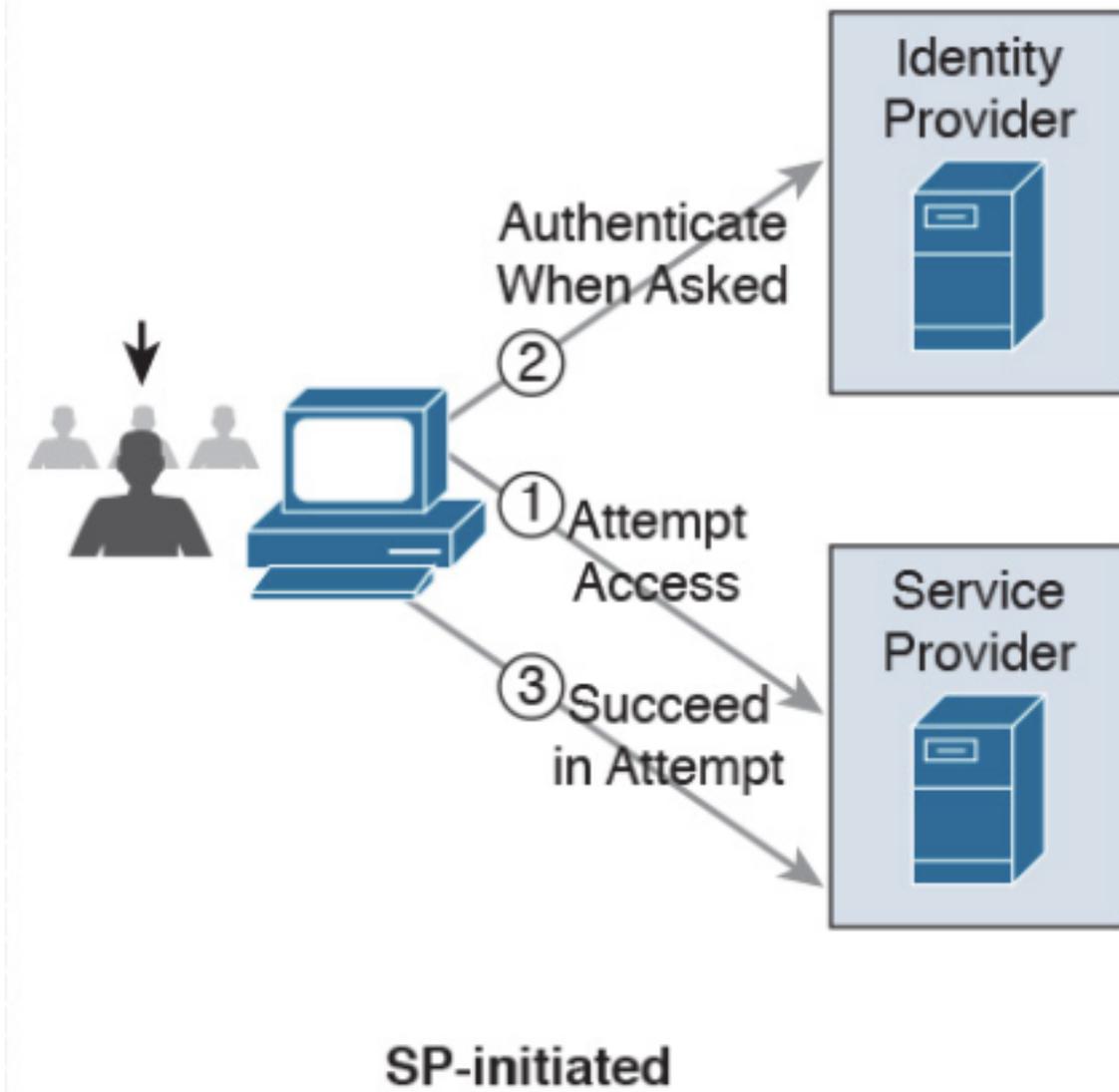
フェデレーションの概念：

- 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。

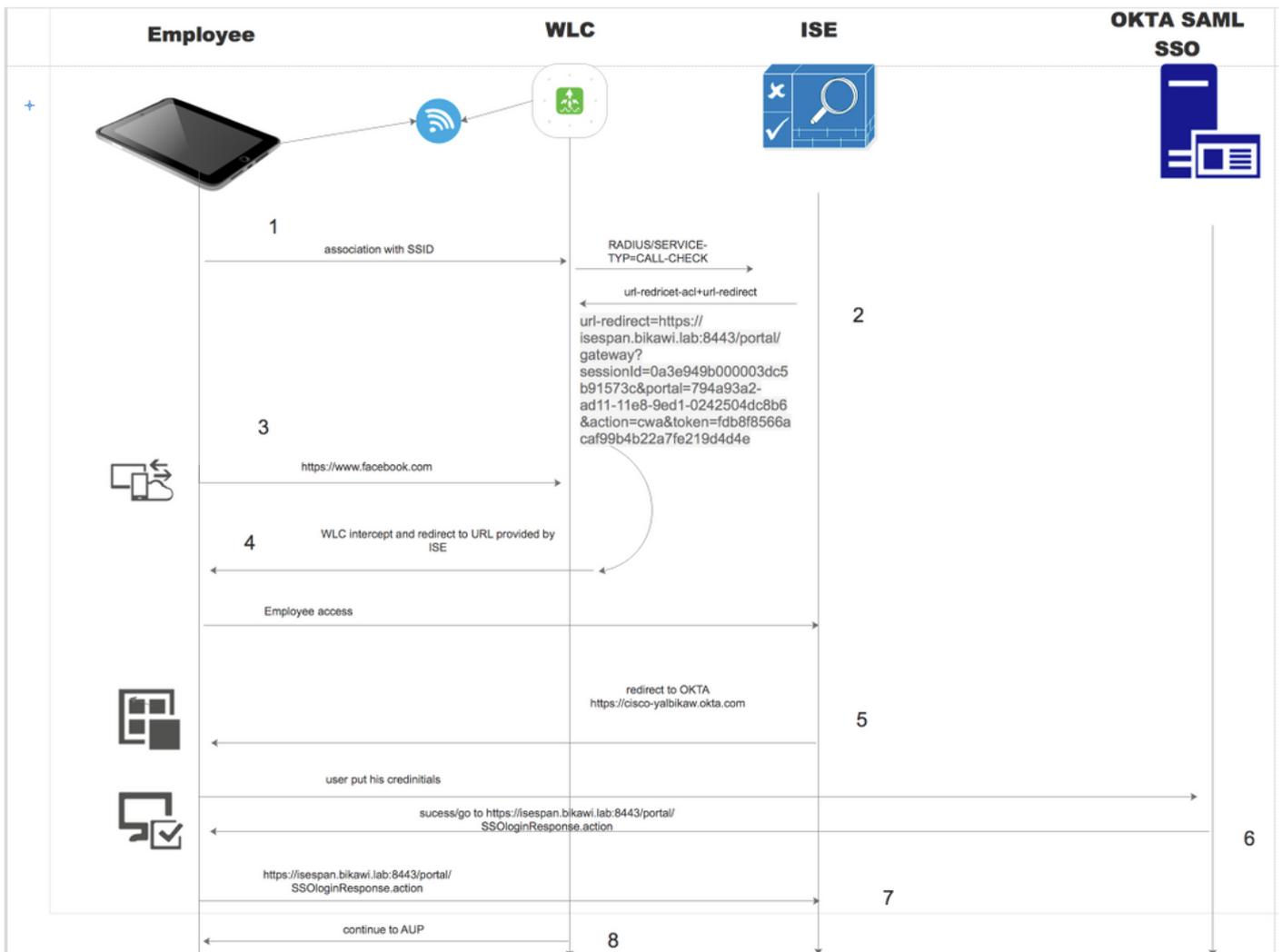
OAuth2やOpenIDなどのSSOを実装するプロトコルがいくつかあります。ISEはSAMLを使用します。

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。



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。

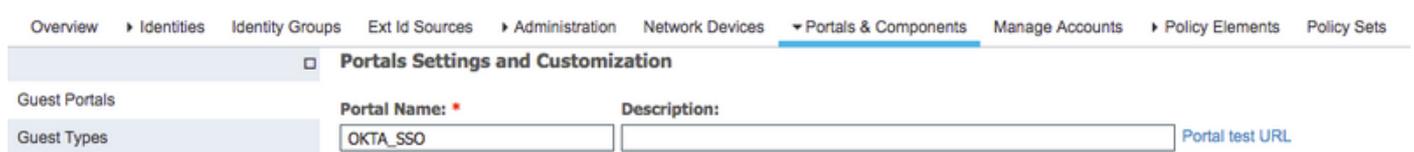
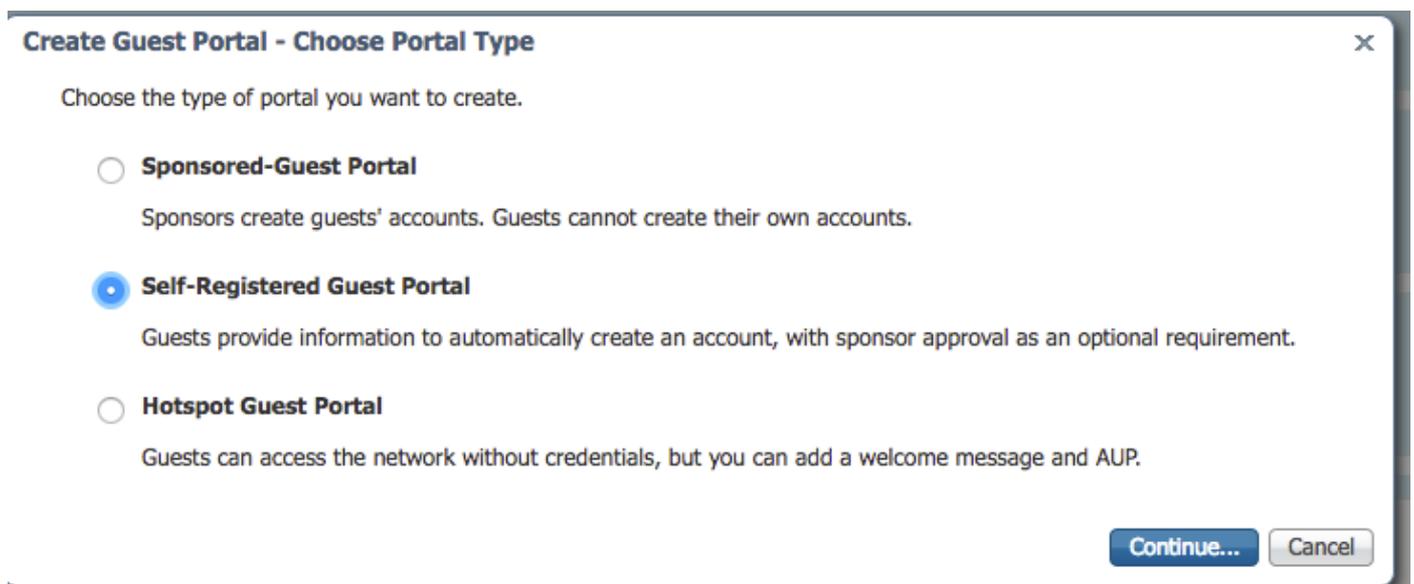


ステップ2: idプロバイダーに名前を割り当て、設定を送信します。

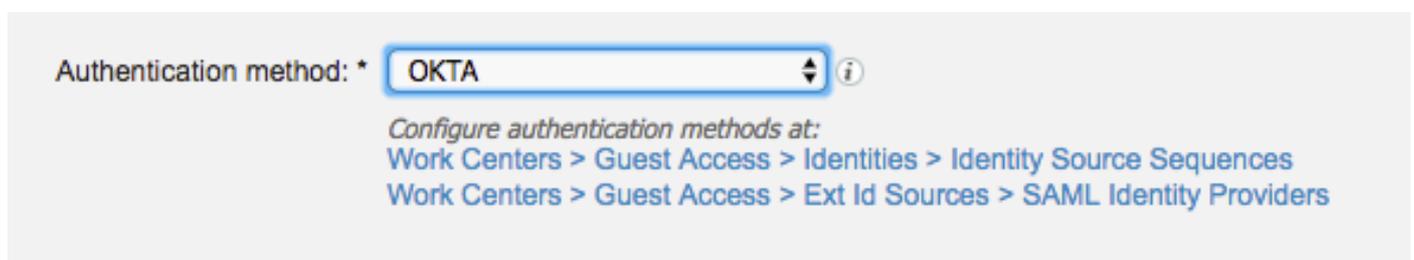
## 2. SSOのポータルを作成します。

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。



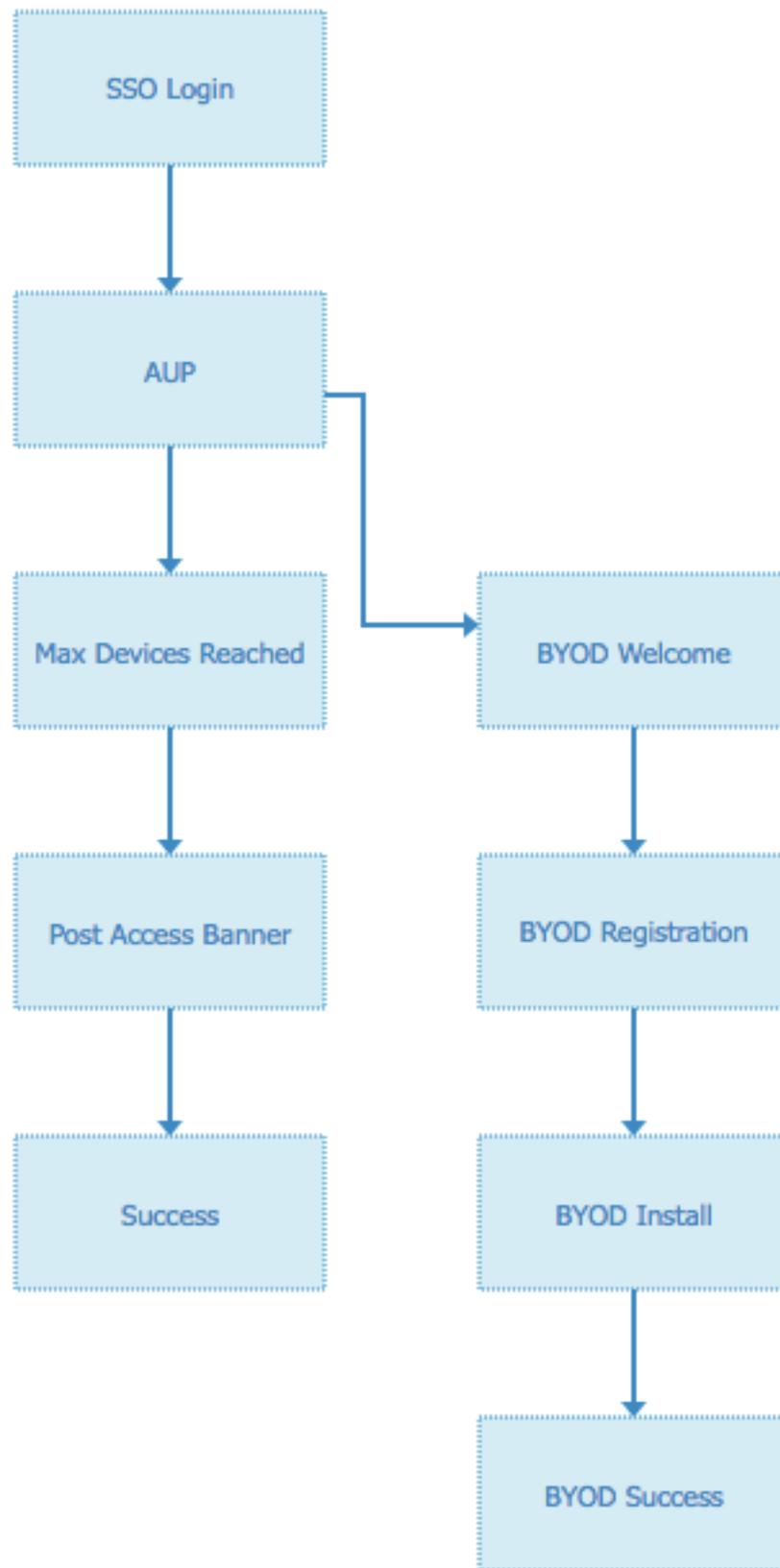
ステップ4: 認証方式として[OKTA identity source]を選択します。

( オプション ) BYOD設定を選択します。

The screenshot shows a configuration page titled "BYOD Settings". It contains several sections:

- Allow employees to use personal devices on the network:** This checkbox is checked. Below it, the "Endpoint identity group" is set to "RegisteredDevices" via a dropdown menu. There are two links: "Configure endpoint identity groups at Administration > Identity Management > Groups > Endpoint Identity Groups" and "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:** This checkbox is unchecked.
- Display Device ID field during registration:** This checkbox is unchecked. Below it is a link: "Configure employee registered devices at Work Centers > BYOD > Settings > Employee Registered Devices".
- After successful device configuration take employee to:** This section has three radio button options:
  - Originating URL (i) (unchecked)
  - Success page (checked)
  - URL: (unchecked, with an empty text input field next to it)

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。

▼ 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

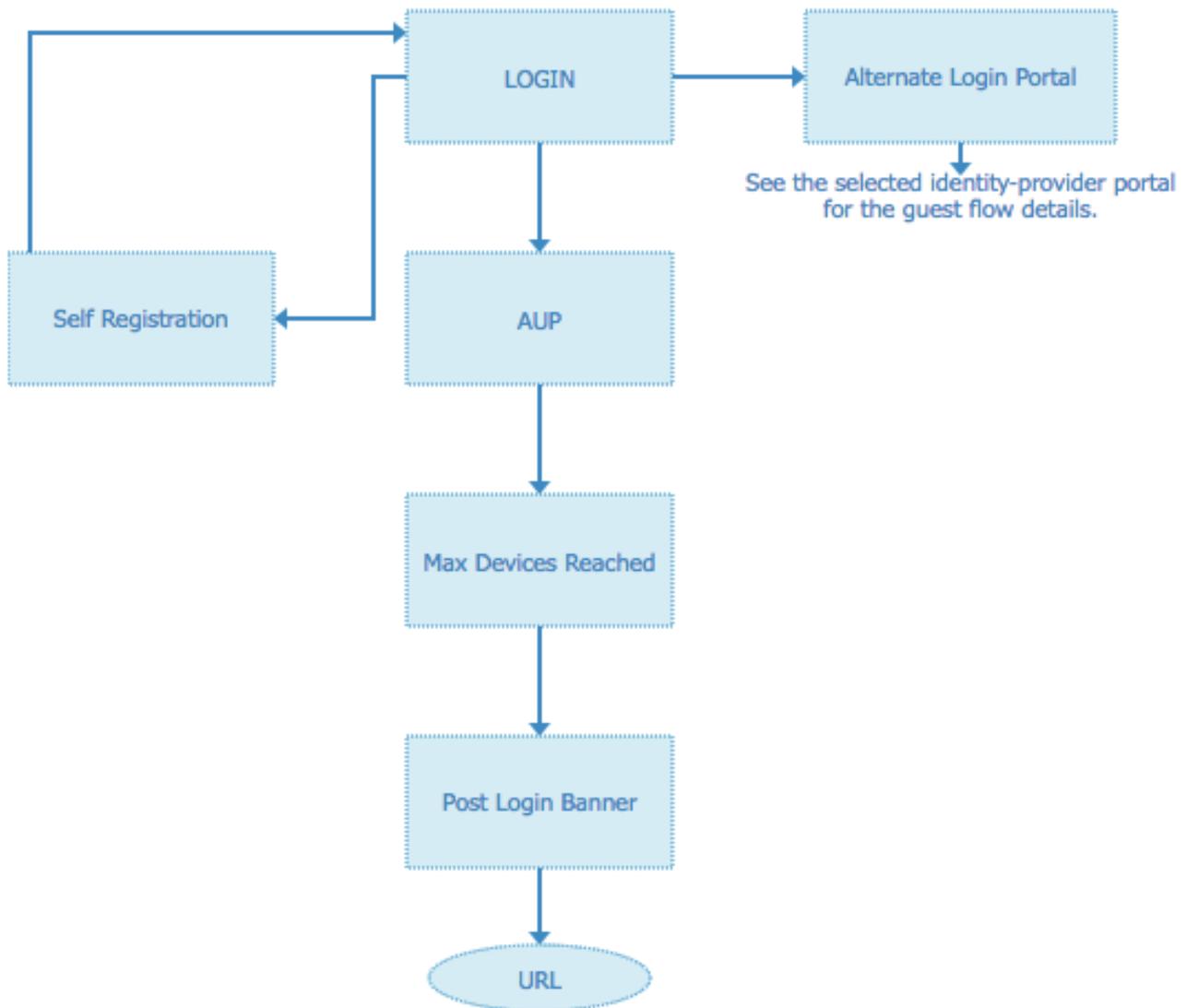
Allow social login

Allow guests to change password after login ⓘ

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

⌵

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。

← 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

ステップ2:[Add Application]をクリックします。

okta Dashboard Directory Applications Security Reports Settings My Applications

Applications Help

Add Application Assign Applications

Q Search

STATUS

ACTIVE	0
INACTIVE	3

01101110  
01101111  
01101100  
01101000  
01101101  
01101110  
01100111

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

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

## 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?

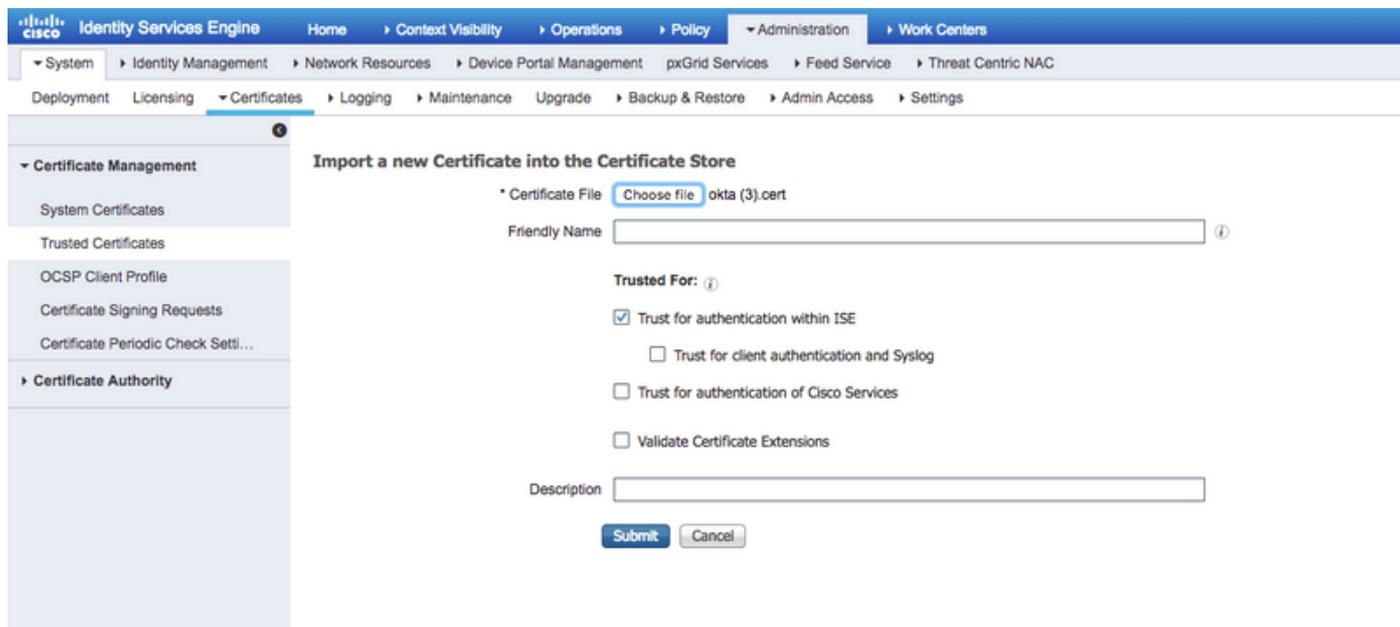
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

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。

### SAML Identity Provider

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

Service Provider Information

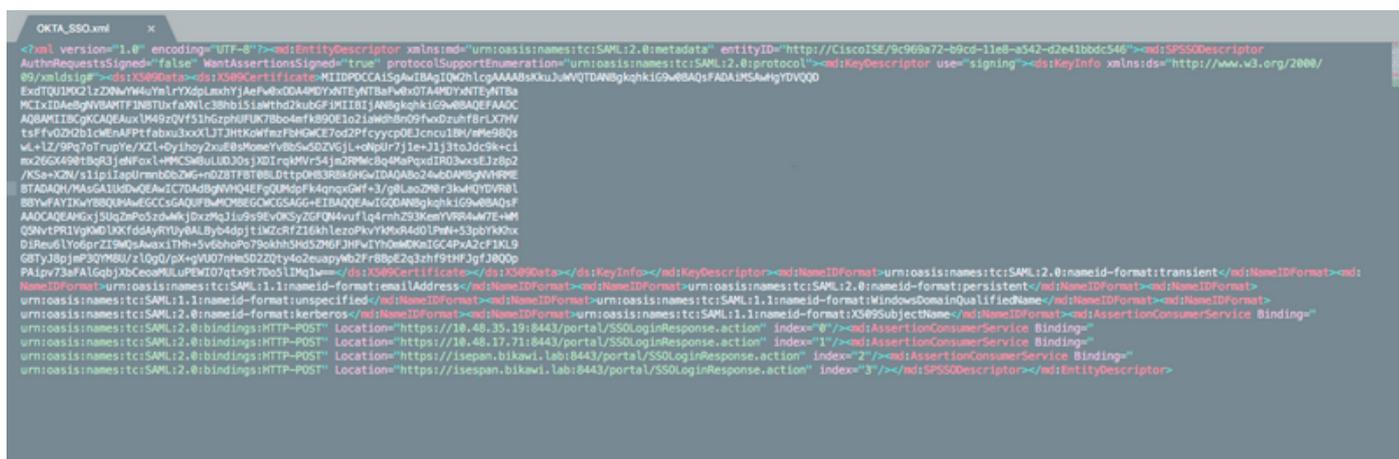
Load balancer

Export Service Provider Info.

Includes the following portals:

OKTA\_SSO

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://isespan.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。

## 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://lspan.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](#)

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ー名は、設計によって異なります。

## 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</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。

**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.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。

**Settings** Edit

**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

**SAML 2.0**

Default Relay State

**SAML 2.0 is not configured until you complete the setup instructions.**

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

**About**

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

**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
A1UECAwKQ2FsaWZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXlhbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFglpbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNV0XDTI4MDgzMTEwNDQwNVowZyZyxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEjEXMBUGA1UEAwwOY2l2Y28tZWFlsYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC1P7DvzVng7wSQWVOzGShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8u1Z8HUsOspBECLYcI75gH4rpc2FM4kzZiDbNLb95AW6dlUztC66x42uhRYgduD5+w3/yvdwx
l99upWb6Sdrtnk8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgJYQO/7GRK2RzOj
bSZgeAp5Yyytja3NCn9x6FMY5Rppc3HjtG4cJQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dN6YERuV5C5eHUXq3KGul2yIfih7x8EartZ4/wGP/HYucNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdTsz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesysecPuWQtEqNqt+MyZnlCurJ0e+JTvKYH1dSWapM1dzqoX
OzyF7yiId9KPP6I4Ndc+BXe1dA8imneYy5MH7/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。

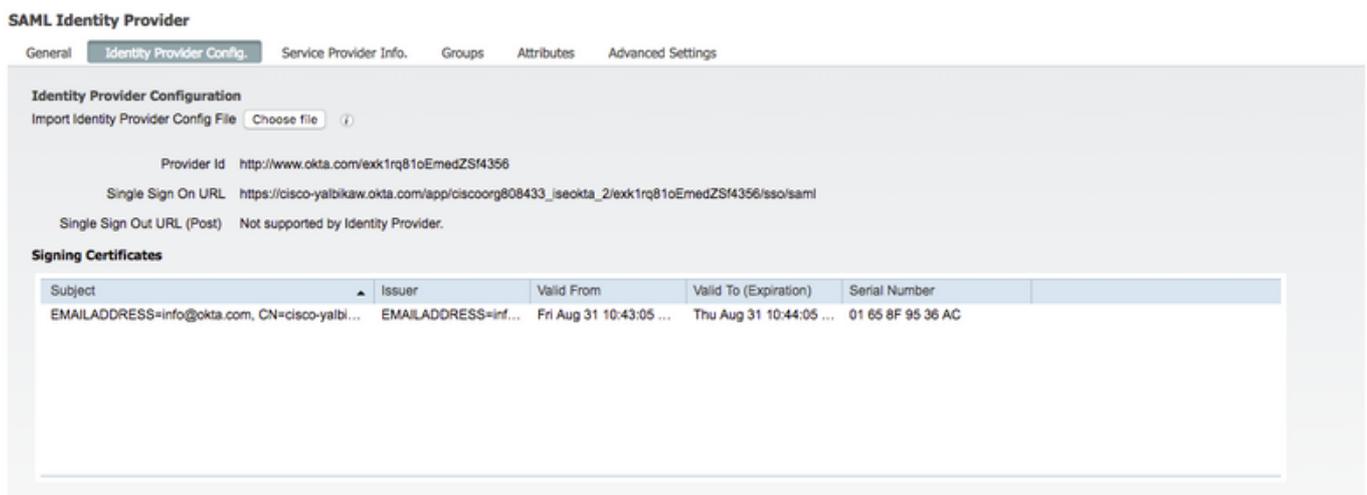
## 5. アプリケーションへのユーザーの割り当て

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>

[REDIRECT-ACL](#)

IPv4

- Remove
- Clear Counters
- Add-Remove URL

### Foot Notes

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

## 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

Portal Name: \*  Description:  [Portal test URL](#)



**Portal Behavior and Flow Settings**  
Use these settings to specify the guest experience for this portal.

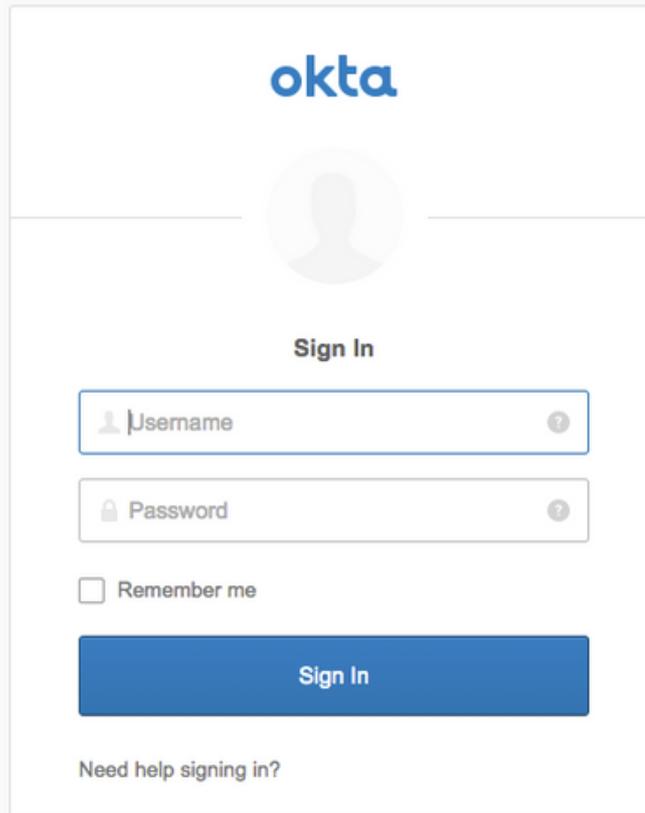


**Portal Page Customization**  
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

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。

## Connecting to

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



The image shows the Okta sign-in interface. At the top is the 'okta' logo in blue. Below it is a grey silhouette of a person's head and shoulders. Underneath the silhouette is the text 'Sign In'. There are two input fields: the first is labeled 'Username' with a person icon on the left and a question mark icon on the right; the second is labeled 'Password' with a lock icon on the left and a question mark icon on the right. Below these fields is a checkbox labeled 'Remember me'. At the bottom of the form is a large blue button with the text 'Sign In'. Below the button is the text 'Need help signing in?'.

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

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

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.



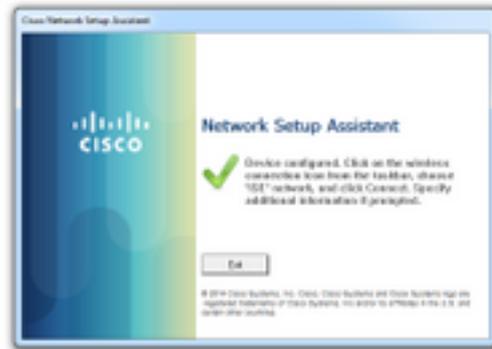
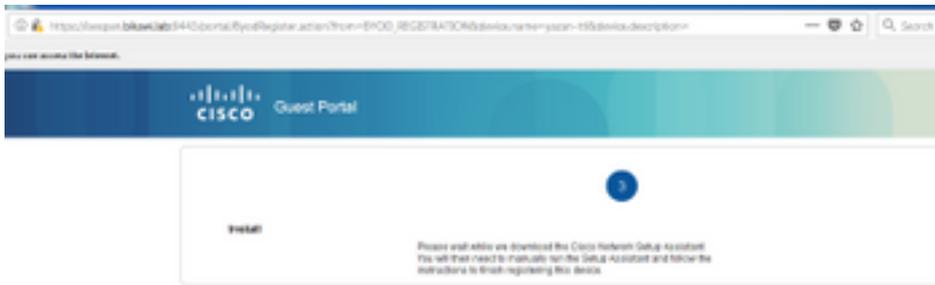
**Acceptable Use Policy**

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



## 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。

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

## トラブルシューティング

### 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。

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](#)

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。

← 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 "00a7e81b031c201f9356" and target.type eq "AppInstance" Advanced Filter / Reset Filters



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"> <li>▶ Actor: OKTA-TEST@cisco.com OKTA (id: 00a22b031c201f9356)</li> <li>▶ Client: FIREFOX on Windows 7 Computer from [REDACTED]</li> <li>▶ Event: successful user authentication.sso (id: W1a2c01e11Mh2noJGtDgAABQ)</li> <li>▶ Request: ISE-OKTA (id: 00a7e81b031c201f9356) AppInstance</li> <li>▶ Target: OKTA-TEST@cisco.com OKTA (id: 00a22b031c201f9356) AppUser</li> </ul> <span style="float: right;"><a href="#">Expand All</a></span>			

## 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

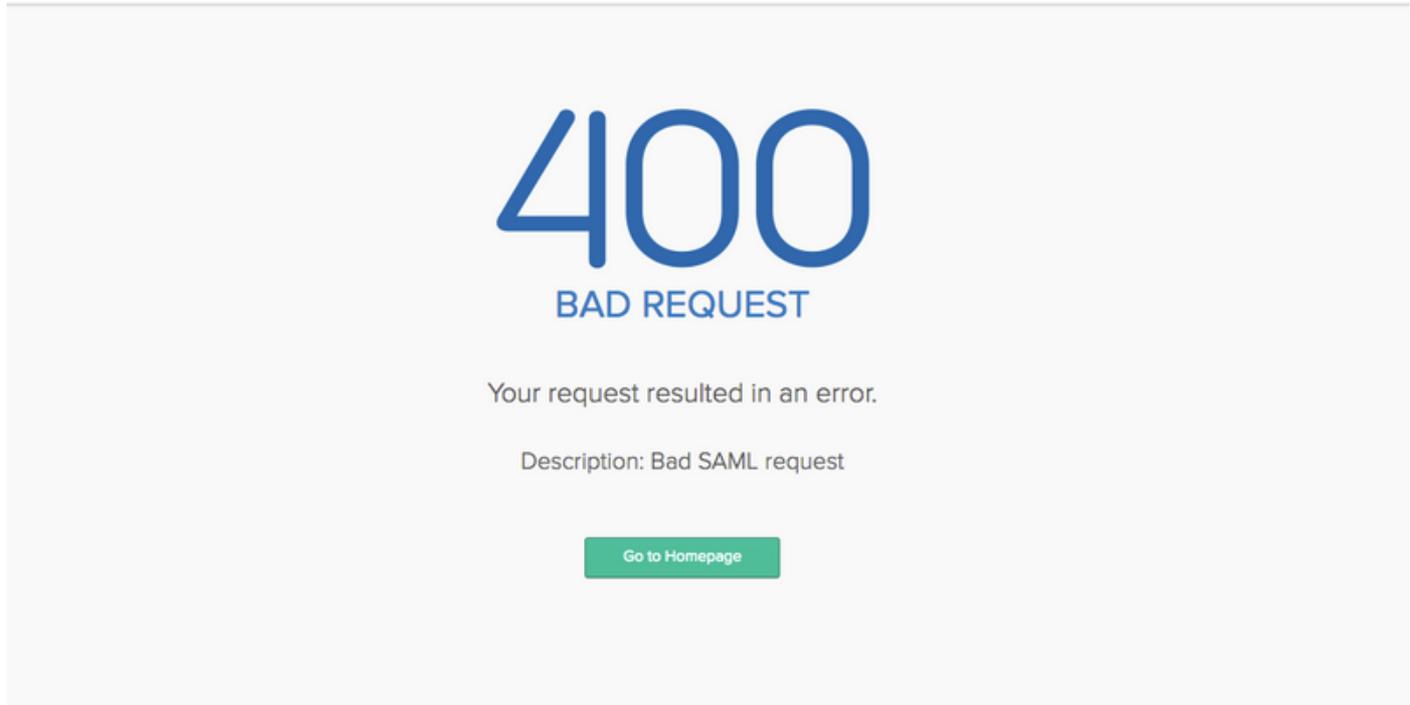
[Administration] > [System] > [Logging] > [Debug Log Configuration]に移動します。レベルをDEBUGに有効にします。

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。



400  
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

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

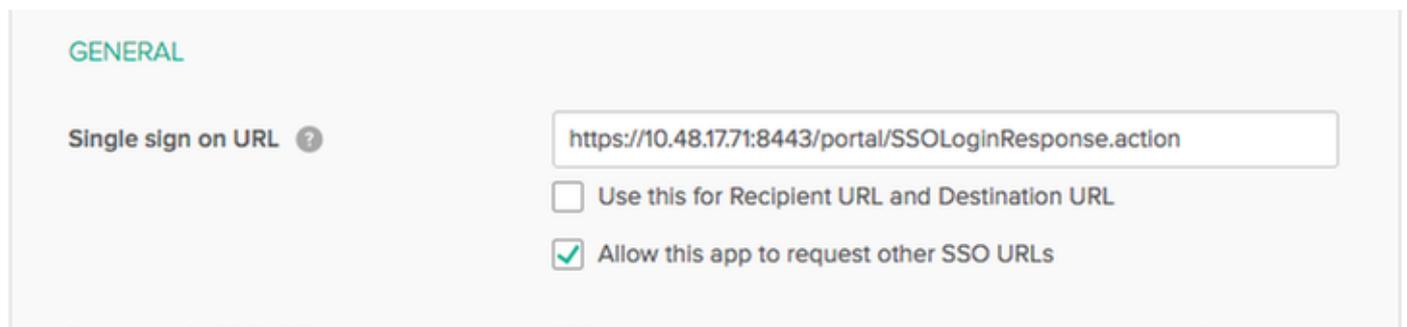
```
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][  
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:  
SSOLoginTransitionResult:
```

```
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/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrgZKmv0  
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0SltA0Vxv1CPwo1hGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bzilld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%2BVyWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnCh3jF  
Fo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n8m0x%2BAQ%3D%3D&RelayState=\_9c969a72-b9cd-11e8-a542-d2e41bbdc546\_DELIMITERportal  
alId\_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546\_SEMIportalSessionId\_EQUALS6770f0a4-bc86-4565-940a-  
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%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0SltA0Vxv1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bzilld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVcEbfk6XdcnITsIPtot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnCh3jFfo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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

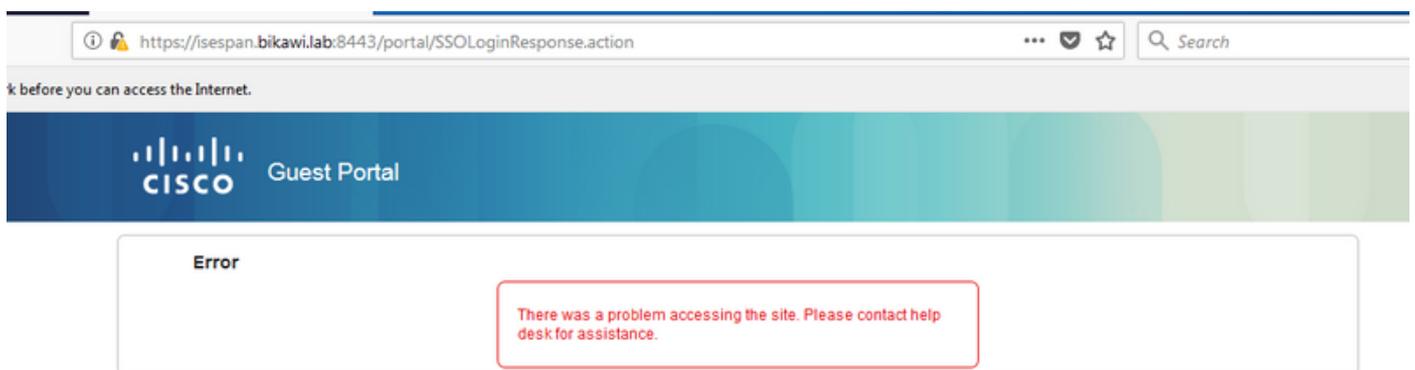
ISEがユーザをIDPにリダイレクトしました。ただし、ISEへの応答はなく、不正なSAML要求が表示されます。OKTAが以下のSAML要求を受け入れていないことを確認します。

```
https://cisco-  
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPiBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0  
OdAH6IDHs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0S1taB0Vxv1CPwolhGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvEcbfkb6XdcnITsIPtot64oM%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  
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

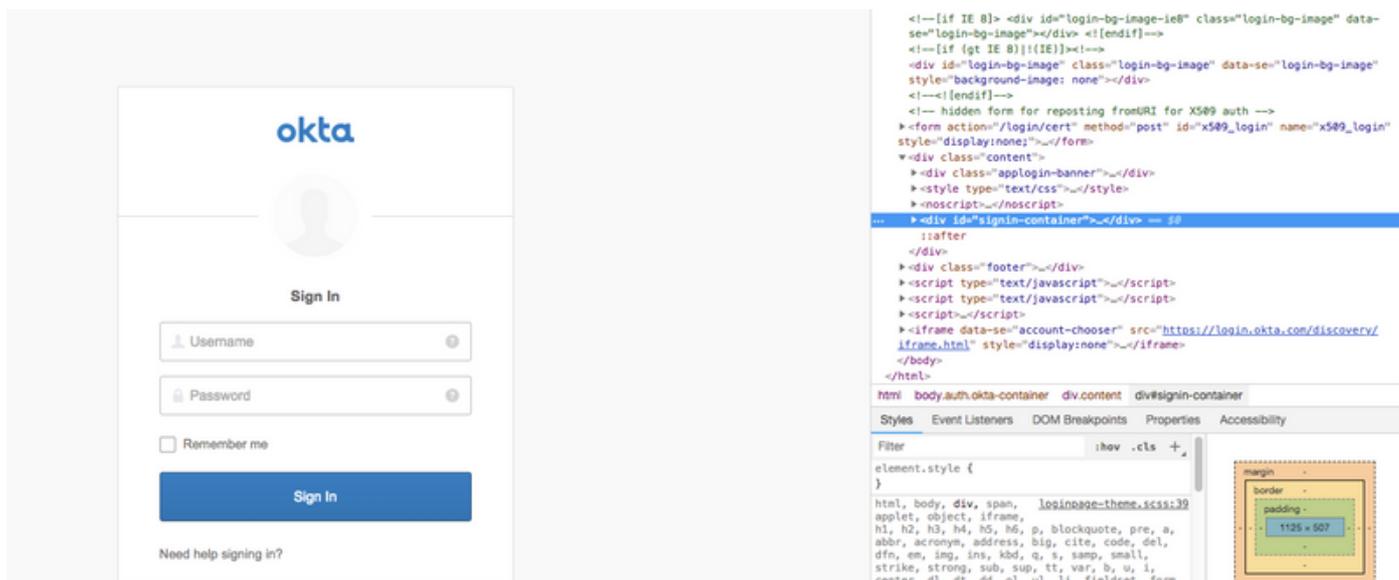
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][  
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or  
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not  
contain ma
```

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>