

# 使用OKTA SAML SSO配置ISE 2.3訪客門戶

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[聯合SSO](#)

[網路流量](#)

[設定](#)

[步驟1.在ISE上配置SAML身份提供者和訪客門戶。](#)

[1.準備外部身份源。](#)

[2.為SSO建立門戶。](#)

[3.配置備用登入。](#)

[步驟2.配置OKTA應用程式和SAML身份提供程式設定。](#)

[1.建立OKTA應用程式。](#)

[2.從SAML身份提供程式匯出SP資訊。](#)

[3. OKTA SAML設定。](#)

[4.從應用程式匯出後設資料。](#)

[5.將使用者分配給應用程式。](#)

[6.將後設資料從Idp匯入ISE。](#)

[步驟3.CWA配置。](#)

[驗證](#)

[終端使用者驗證](#)

[ISE驗證](#)

[疑難排解](#)

[OKTA故障排除](#)

[ISE故障排除](#)

[常見問題和解決方案](#)

[相關資訊](#)

## 簡介

本文說明如何將身份服務引擎(ISE)與OKTA整合，以便為訪客門戶提供安全宣告標籤語言單一登入(SAML SSO)身份驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 思科身分識別服務引擎訪客服務。
- SAML SSO。
- ( 可選 ) 無線LAN控制器(WLC)組態。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎2.3.0.298
- OKTA SAML SSO應用程式
- Cisco 5500無線控制器版本8.3.141.0
- 聯想Windows 7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

### 聯合SSO

組織中的使用者可進行一次身份驗證，然後訪問多個資源。跨組織使用的這種身份稱為聯合身份。

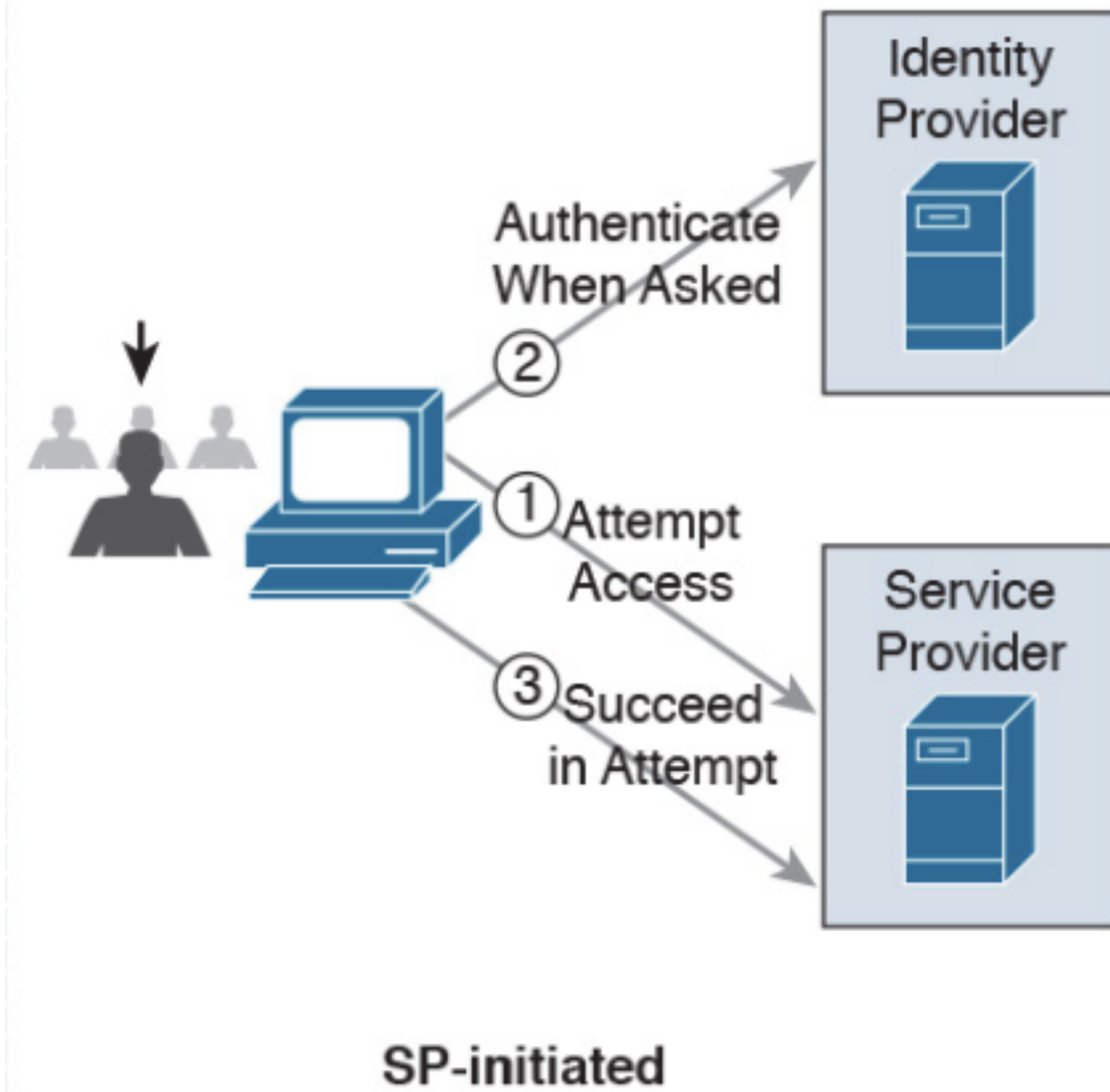
聯邦的概念：

- 原則：終端使用者 ( 請求服務的使用者 )、Web瀏覽器 ( 在本例中 ) 是終端。
- 服務提供商(SP):有時稱為信賴方(RP)，即提供服務的系統，在本例中為ISE。
- 身份提供程式(IdP):管理身份驗證、授權結果以及傳送回SP ( 在本例中為OKTA ) 的屬性。
- 斷言：由IdP傳送到SP的使用者資訊。

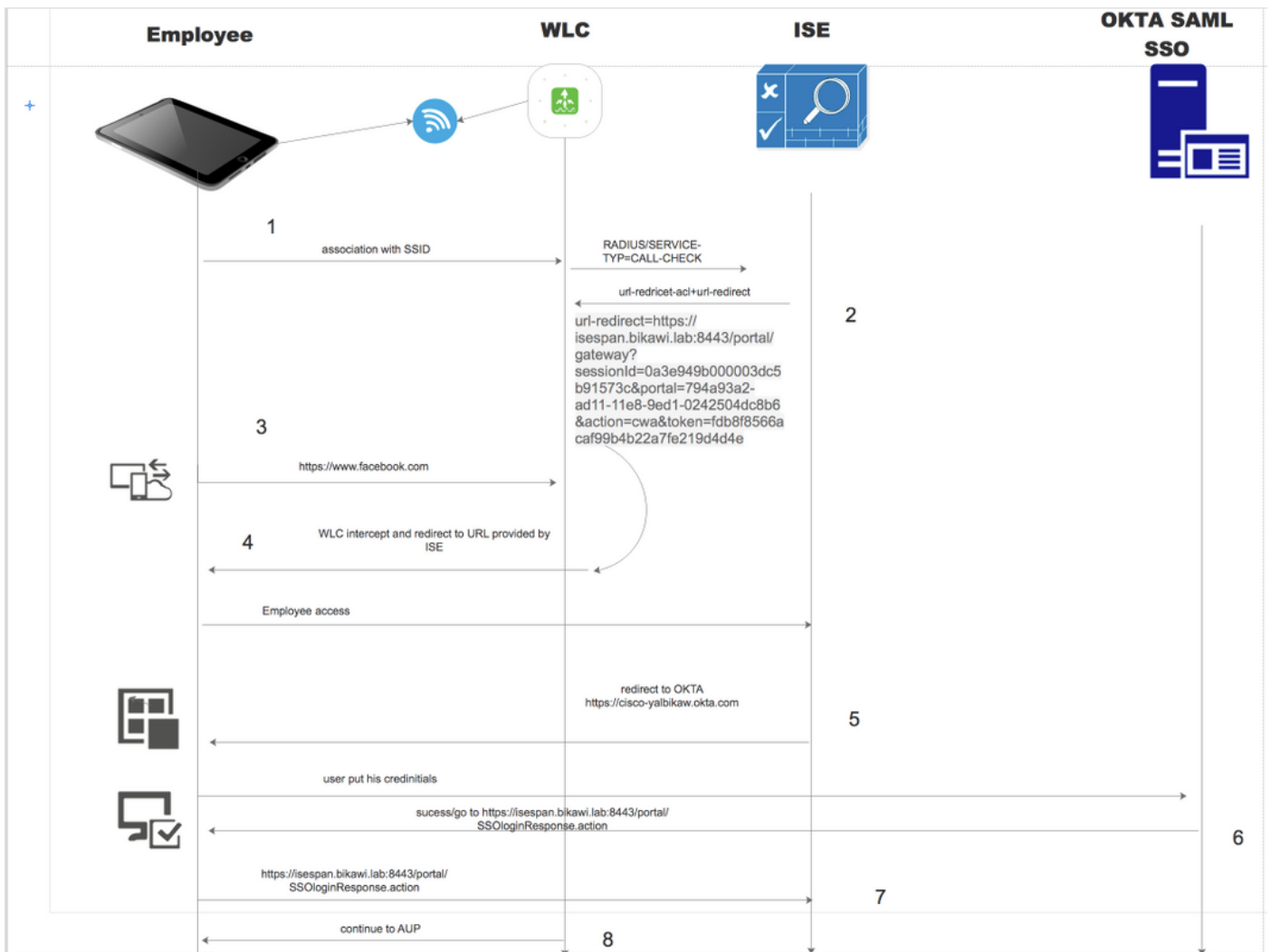
多種協定實現SSO，如OAuth2和OpenID。ISE使用SAML。

SAML是一個基於XML的框架，它描述了業務實體之間以安全方式使用和交換SAML斷言。該標準描述了請求、建立、使用和交換這些斷言的語法和規則。

ISE使用SP啟動模式。使用者被重定向到訪客門戶，然後ISE將其重定向到IdP進行身份驗證。之後，它重定向回ISE。驗證請求後，使用者根據門戶配置繼續訪問或登入。



網路流量



1. 使用者連線到SSID，身份驗證為mac filtering(mab)。
2. ISE使用包含Redirect-URL和Redirect-ACL屬性的訪問接受進行響應
3. 使用者嘗試存取[www.facebook.com](https://www.facebook.com)。
4. WLC攔截請求並將使用者重定向到ISE訪客門戶，使用者點選員工訪問以便使用SSO憑證註冊裝置。
5. ISE將使用者重定向到OKTA應用進行身份驗證。
6. 身份驗證成功後，OKTA將SAML斷言響應傳送到瀏覽器。
7. 瀏覽器將斷言中繼回ISE。
8. ISE驗證斷言響應，如果使用者正確通過身份驗證，它會進入AUP，然後進行裝置註冊。

有關SAML的詳細資訊，請檢視以下連結

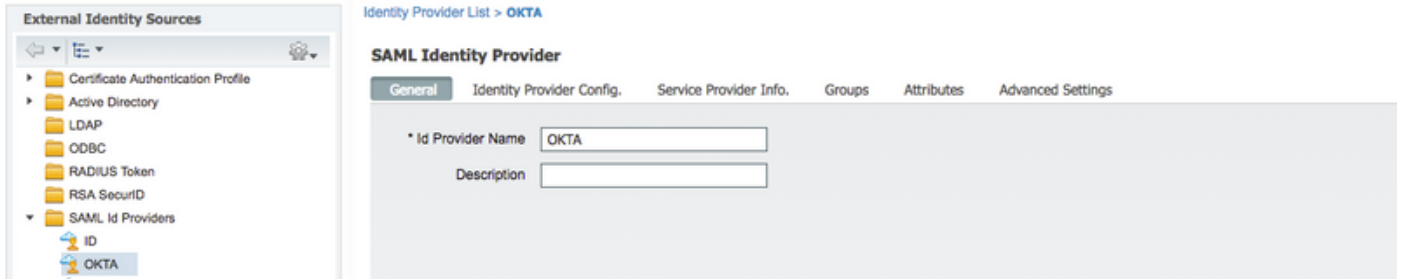
<https://developer.okta.com/standards/SAML/>

## 設定

**步驟1.在ISE上配置SAML身份提供者和訪客門戶。**

1.準備外部身份源。

步驟1.導航到**管理>外部身份源> SAML ID提供程式**。

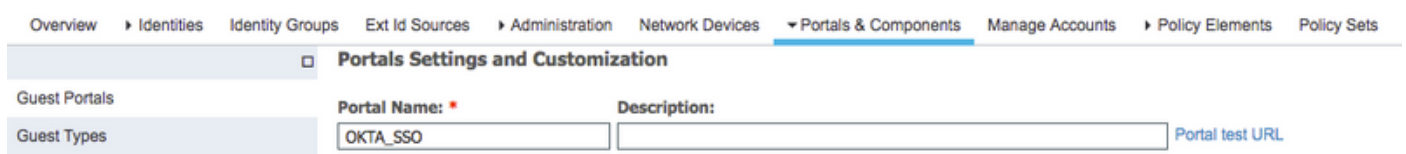
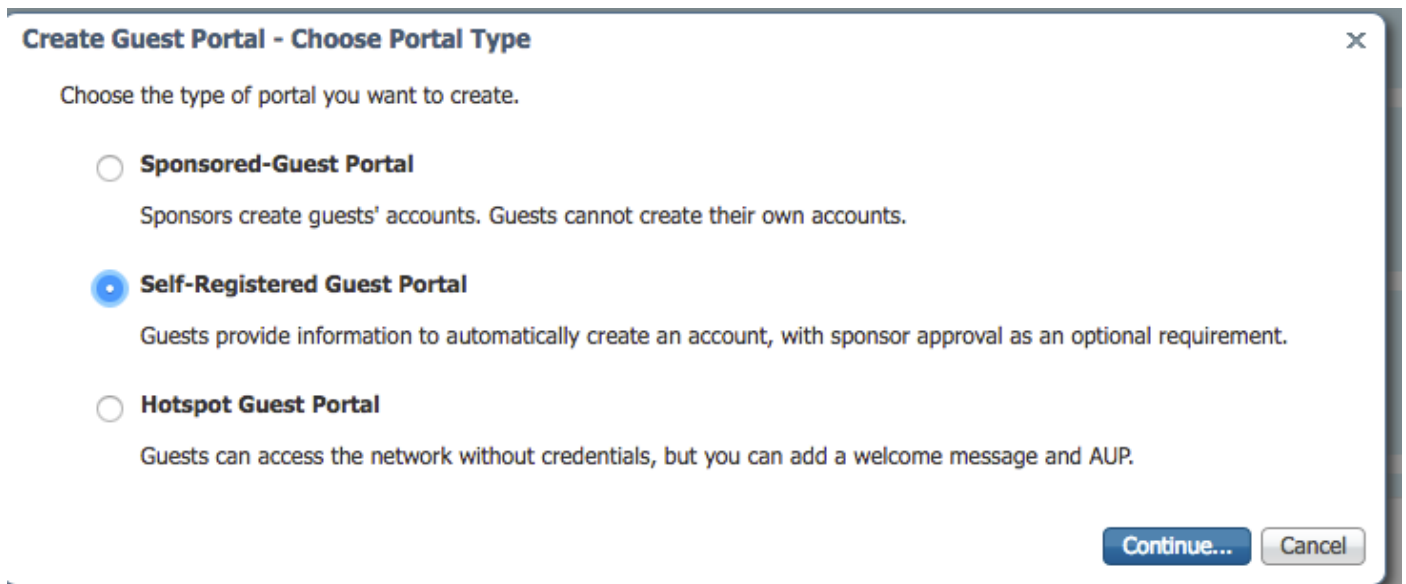


步驟2.為ID提供程式分配名稱並提交配置。

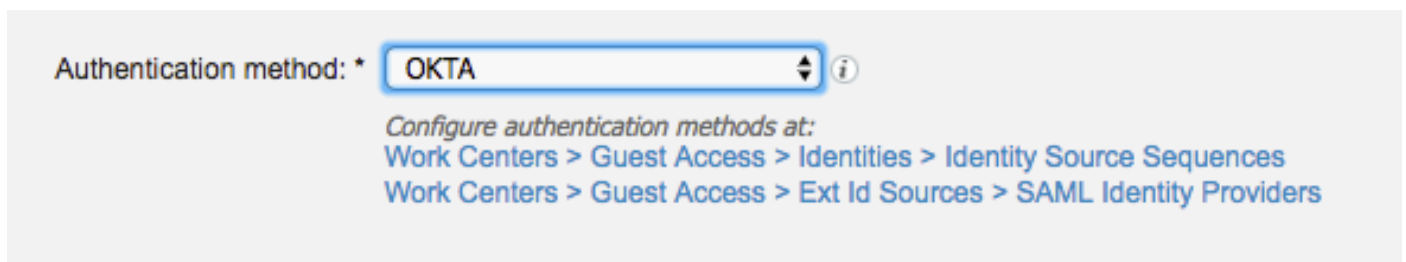
## 2.為SSO建立門戶。

步驟1.建立分配給OKTA作為身份源的門戶。BYOD、裝置註冊、訪客等的任何其他配置與普通門戶完全相同。在本文檔中，門戶被對映到訪客門戶，作為員工的備用登入。

步驟2.導航到**工作中心>訪客訪問>門戶和元件**，然後建立門戶。



步驟3.選擇身份驗證方法以指向之前配置的身份提供程式。



步驟4.選擇OKTA身份源作為身份驗證方法。

( 可選 ) 選擇BYOD設定。

## ▼ BYOD Settings

- 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](#)

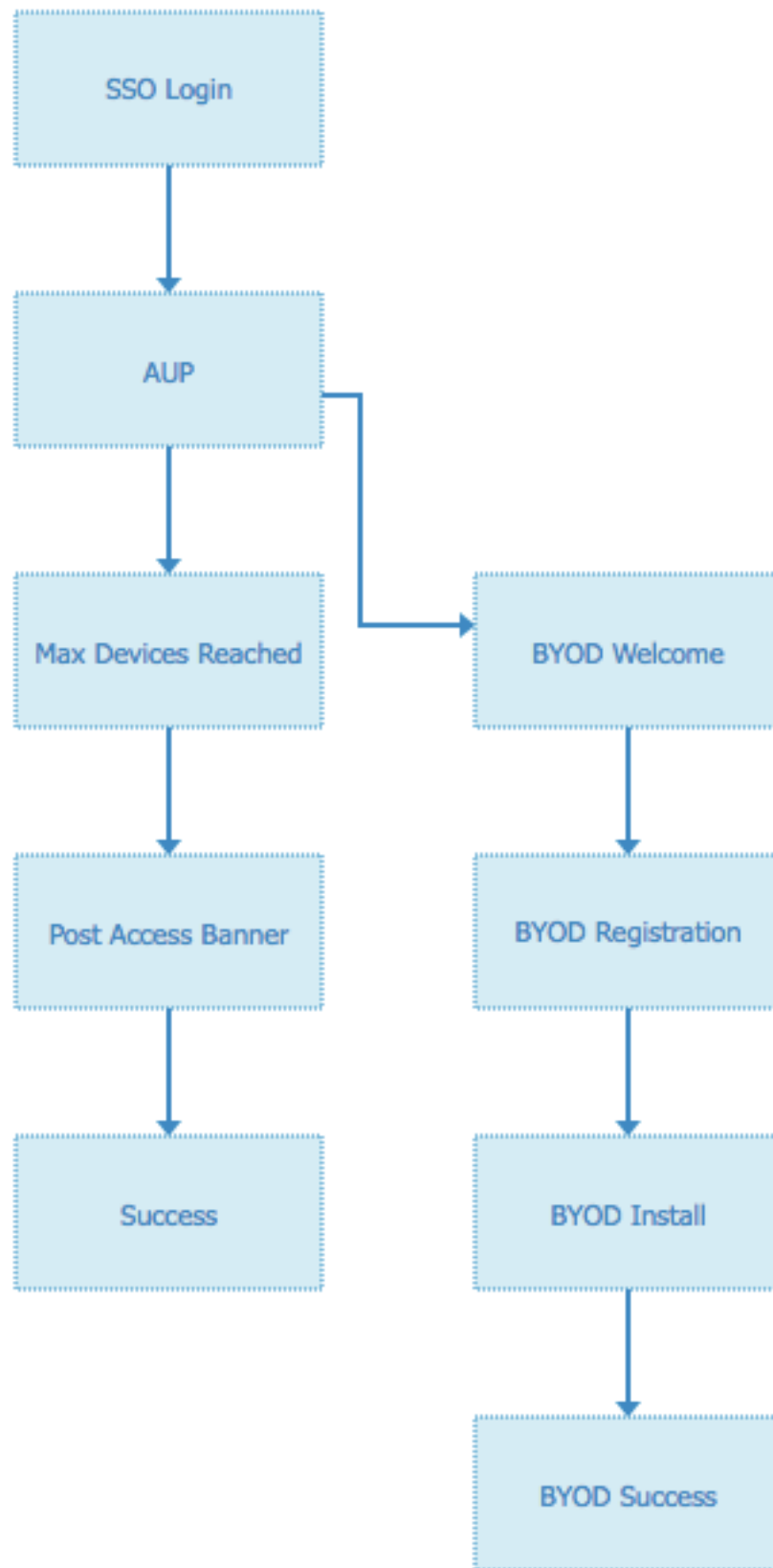
After successful device configuration take employee to:

- Originating URL [\(i\)](#)

- Success page

- URL:

步驟5.儲存門戶配置，使用BYOD時，流程如下所示：



### 3. 配置備用登入。

附註：如果不使用Alternative登入名，可以跳過此部分。

導航到自助註冊訪客門戶或任何其他為訪客訪問定製的門戶。

在登入頁面設定中新增備用登入門戶：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

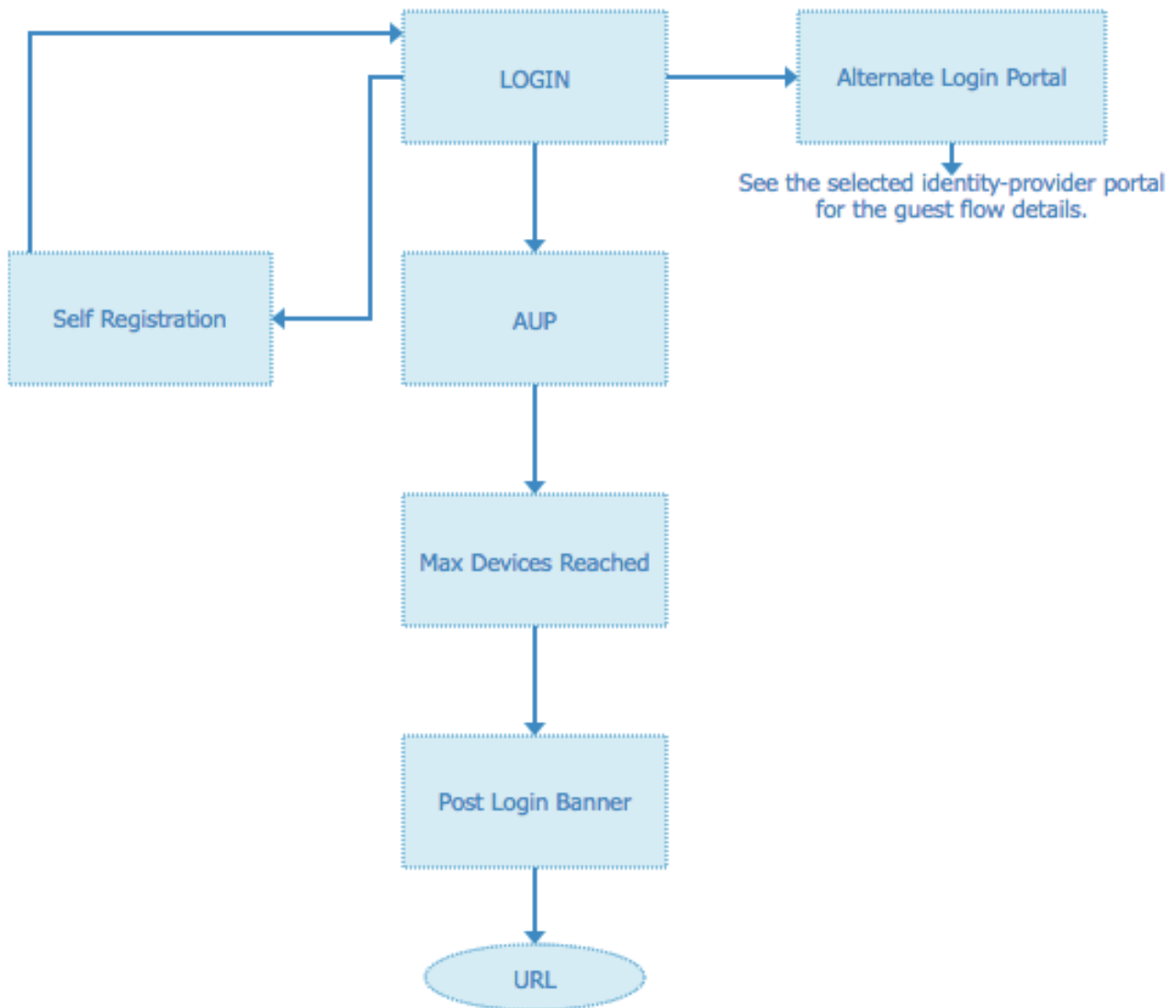
Allow guests to change password after login ⓘ

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

▼

現在是入口流。





## 步驟2.配置OKTA應用程式和SAML身份提供程式設定。

### 1.建立OKTA應用程式。

步驟1.使用管理員帳戶登入OKTA網站。

← Back to Applications

## Add 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	<a href="#">Add</a>
	&frankly Okta Verified ✓ SAML	<a href="#">Add</a>
	10000ft Okta Verified	<a href="#">Add</a>
	101domains.com Okta Verified	<a href="#">Add</a>

步驟2.按一下Add Application。

okta [Dashboard](#) [Directory](#) [Applications](#) [Security](#) [Reports](#) [Settings](#) [My Applications](#) [Help](#)

### Applications

[Add Application](#) [Assign Applications](#)

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](#)

步驟3.建立新應用，選擇為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

## 常規設定

### 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

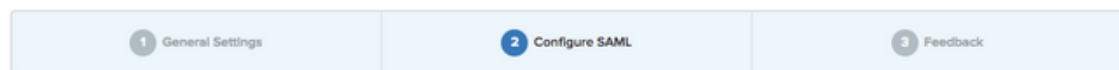


Do not display application icon in the Okta Mobile app

Cancel

Next

## Create SAML Integration



### A SAML Settings

**GENERAL**

Single sign on URL <sup>?</sup>

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

Audience URI (SP Entity ID) <sup>?</sup>

Default RelayState <sup>?</sup>

If no value is set, a blank RelayState is sent

Name ID format <sup>?</sup>

Application username <sup>?</sup>

[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](#)

步驟4. 下載證書並將其安裝在ISE受信任證書中。

Import a new Certificate into the Certificate Store

\* Certificate File

Friendly Name

Trusted For: <sup>?</sup>

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

Description

2. 從SAML身份提供程式匯出SP資訊。

導航到之前配置的身份提供程式。按一下「Service Provider Info」，然後將其匯出，如下圖所示。

### SAML Identity Provider

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

Service Provider Information

Load balancer [?]

Export Service Provider Info. [Export] [?]

Includes the following portals:

OKTA\_SSO

匯出的zip資料夾包含XML檔案和readme.txt



對於某些Identity提供程式，您可以直接匯入XML，但在這種情況下，需要手動匯入XML。

- 單點登入URL ( saml斷言 )

```
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實體ID

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

可用的SSO URL ( IP地址和FQDN格式 )。

**注意：**格式選擇取決於授權配置檔案上的重定向設定，如果使用靜態IP，則應使用SSO URL的IP地址。

### 3. OKTA SAML設定。

步驟1.在SAML設定中新增這些URL。

## 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](#)

步驟2.您可以根據託管此服務的PSN數量從XML檔案中新增多個URL。名稱ID格式和應用程式使用者名稱取決於您的設計。

## 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>
```

步驟3.按一下下一步並選擇第二個選項。

**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.從應用程式匯出後設資料。

← Back to Applications



ISE-OKTA

Active



View Logs

General

Sign On

Import

Assignments

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.

CREDENTIALS DETAIL

### 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.

## 後設資料：

```

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exklrq8loEmedZSf4356">
<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
A1UECAwKQ2FsaWZvcmlkZm9udm90YyYwMjYyOTUwMDA1UEBwNU2FuIEZyYW5jaXNjb2ZlbnMA
SAlUECgwET2t0YTEU
MBIGAlUECwwLU1NPUHJvdmlkZm9udm90YyYwMjYyOTUwMDA1UEBwNU2FuIEZyYW5jaXNjb2ZlbnMA
SAlUECgwET2t0YTEU
AQBKBFglpbmZvZG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNDUzDjE4MDgzMTEwNDQwNDUzZDZlbnMA
SAlUECgwET2t0YTEU
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLEDApTU09Qcm92aW50YyYwMjYyOTUwMDA1UEBwNU2FuIEZyYW5jaXNjb2ZlbnMA
SAlUECgwET2t0YTEU
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9udm90YyYwMjYyOTUwMDA1UEBwNU2FuIEZyYW5jaXNjb2ZlbnMA
SAlUECgwET2t0YTEU
ggEKAoIBAQC1P7DvzVng7wSQWVozgShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8u1Z8HUsOspBECLYcI75gH4rpc2FM4kzZiDbNLb95AW6d1UztC66x42uhRYgduD5+w3/yvdwx
l99upWb6Sdrtnk8cx7AyIJA4E9KK22cv3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjjiadvhCSPdy
+qmMx9eFtZwzN1/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuwjBFHW3Zy7hPEtHgJYQO/7GRK2RzOj
bSZgeAp5Yyytja3NCn9x6FMY5Rppc3HjtG4cjQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dn6YERuV5C5eHUXq3KGul2yIfih7x8EartZ4/wGP/HYUCNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Agle91H6nbdTsz3e5MMSKYGr9HaigGgq4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesyysecPuwQtEqNqt+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>
```

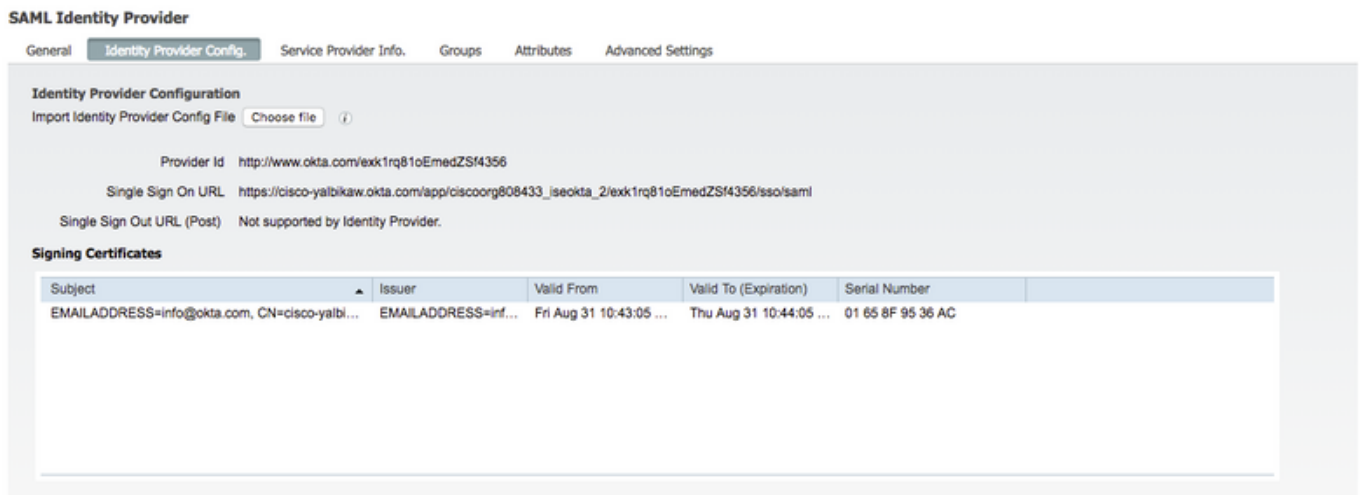
以XML格式儲存檔案。

## 5.將使用者分配給應用程式。

將使用者分配給此應用程式，可以實現AD整合，如中所述：[OKTA活動目錄](#)

## 6.將後設資料從Idp匯入ISE。

步驟1.在SAML Identity Provider下，選擇Identity Provider Config.和Import Metadata。



**SAML Identity Provider**

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

**Identity Provider Configuration**

Import Identity Provider Config File  (?)

Provider Id

Single Sign On URL

Single Sign Out URL (Post)

**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

步驟2.儲存配置。

## 步驟3.CWA配置。

本檔案將說明ISE和WLC的組態。

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

在Redirect-ACL中新增URL。

<https://cisco-yalbikaw.okta.com> /新增應用程式URL

<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.

## 驗證

測試門戶並驗證您是否能夠訪問OKTA應用程式

Portal Name: \*

Description:

OKTA\_SSO

[Portal test URL](#)



#### Portal Behavior and Flow Settings

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



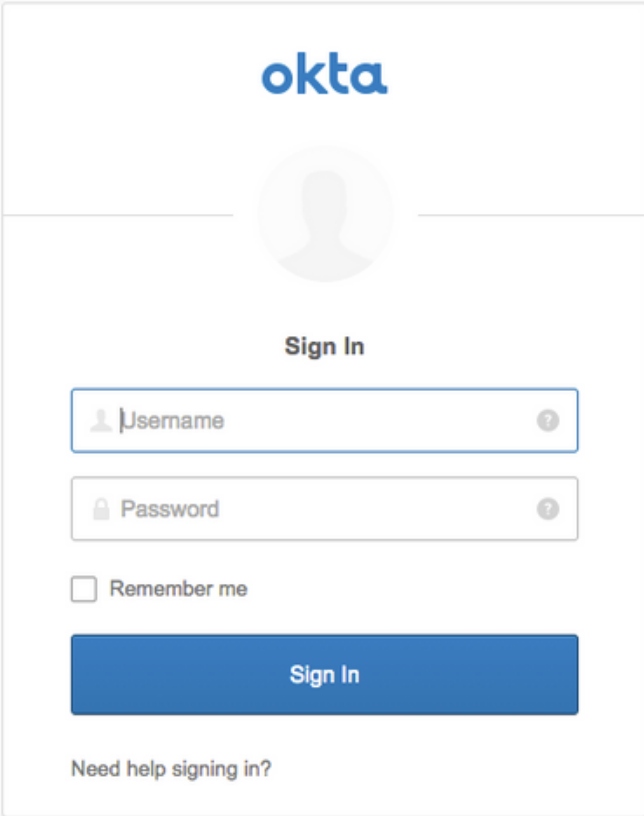
#### Portal Page Customization

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

步驟1. 按一下門戶測試，然後您應該重定向到SSO應用程式。

## 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. Below it is a placeholder for a user profile picture. The main heading is "Sign In". There are two input fields: "Username" and "Password", each with a question mark icon to its right. Below the password field is a checkbox labeled "Remember me". A large blue "Sign In" button is positioned below the checkbox. At the bottom of the form, there is a link that says "Need help signing in?"

步驟2. 檢查與<application name>的資訊連線

步驟3. 如果您輸入憑證時可能看到錯誤的saml請求，這未必表示此時組態錯誤。

## 終端使用者驗證



The image shows a web browser window displaying the Cisco Guest Portal. The address bar shows a URL starting with "https://campus.bkarelab@44.5/portal/PortalSetup.action?portal=794a93a2-ad15-11e8-9ed1-0242504acdb6&sessionid=0a3e949e000002c15eb0036e0...". The page header includes the Cisco logo and "Guest Portal". The main content area is titled "Sign On" and "Sign on for guest access". It contains two input fields: "Username:" and "Password:". Below these fields is a blue "Sign On" button. Underneath the button is a link that says "Or register for guest access". At the bottom, there is a section titled "You can also login with" followed by a "Microsoft account" link with a user icon.

before 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.



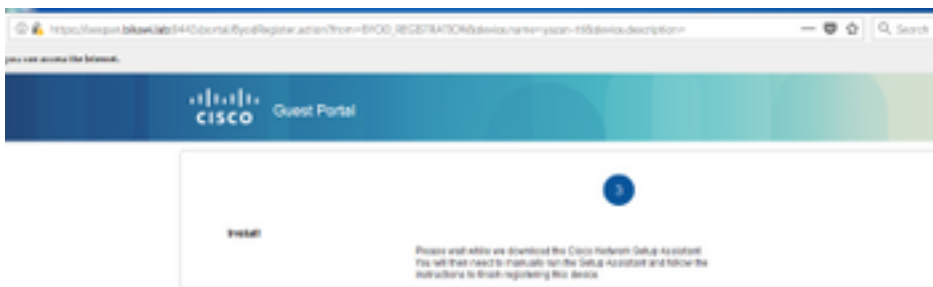
Signing in to ISE-OKTA



**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 usernames 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 modification will be posted on Cisco Systems' website.

**Accept** **Decline**



## ISE驗證

檢查生命日誌以驗證身份驗證狀態。

Sep 30, 2018 12:39:09.514 AM	✓	🔒	okta-test@cisco.c...	3C:A9:F4:34:9F:70				
Sep 30, 2018 12:33:32.640 AM	✓	🔒	3C:A9:F4:34:9F:70	3C:A9:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest	yazan-cpo

## 疑難排解

### OKTA故障排除

步驟1. 檢查Reports頁籤中的日誌。

okta Dashboard Directory Applications Security Reports Settings My Applications

### 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

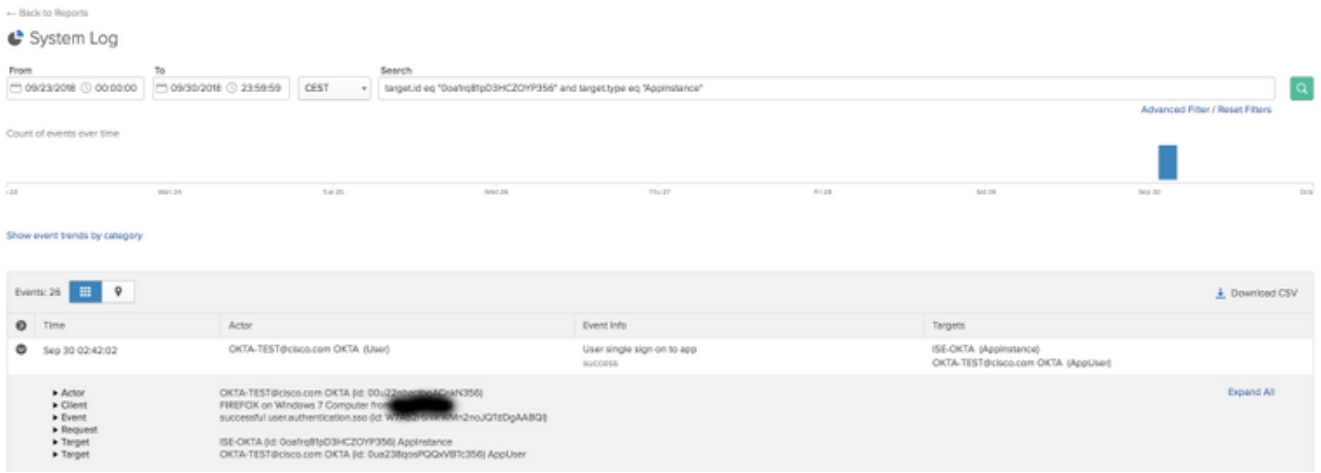
步驟2. 也從應用程式檢視相關日誌。

← Back to Applications

## ISE-OKTA

Active [View Logs](#)

General Sign On Import **Assignments**



## ISE故障排除

有兩個要檢查的日誌檔案

- ise-psc.log
- guest.log

導覽至Administration > System > Logging > Debug Log Configuration。啟用級別以調試。

SAML ise-psc.log  
訪客接入 guest.log  
門戶 guest.log

該表顯示要調試的元件及其相應的日誌檔案。

## 常見問題和解決方案

案例1.錯誤的SAML請求。



# 400

## BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

此錯誤是常見錯誤，請檢查日誌以驗證流並查明問題。在ISE guest.log上：

## ISE# show logging application guest.log |最後50個

```
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:

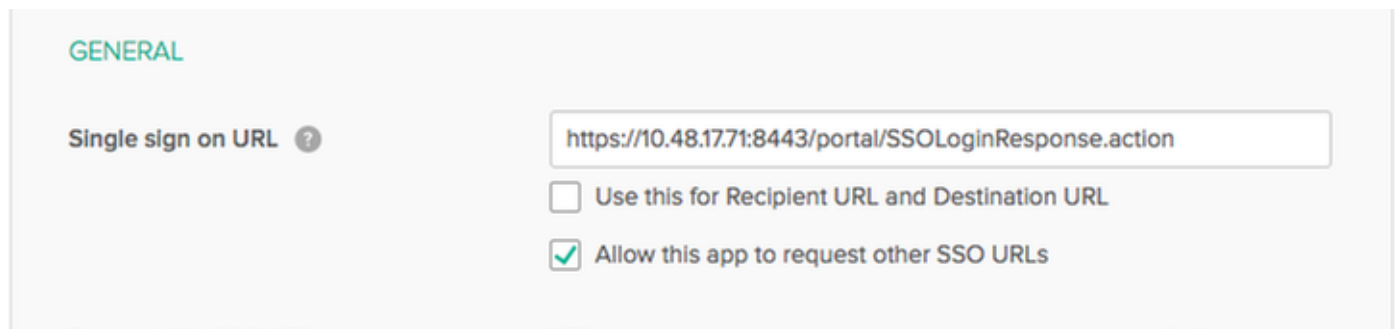
    Portal Name: OKTA_SSO
    Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546
    Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
    Identity Provider: com.cisco.cpm.acs.im.identitystore.saml.IdentityProvider@56c50ab6
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
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%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoEuyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCffne9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnC
h3jFo72v2xmatdQLUyIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoEuyPu95j9%2FzJO
Ob4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJ
o1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DEcRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCffne9%2Bu1K14C8Xs4TXE1z
X6nmngdq3YIO37q9fBlQnCh3jFo72v2xmatdQLUyIhwd4a85ksvOs9qFtIbthcPVMX5YxglvW7vXLUPPSlctE8DdzUpNpWl
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已成功將使用者重定向到IDP。但是，沒有響應ISE並顯示錯誤的SAML請求。請確定OKTA不接受下面我們的SAML請求是請求。

```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exklrq8loEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJ0Ob4672DqCNUDJD%2FR5GH
kiuKiEFM7Qp7%2FwRupmMdd3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1h0iulyQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0Sltab0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDEcRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfk6XdcnITsIPTot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlrFz4JqdjINL226IsCFfnE9%2BulK14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnC
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
現在再次檢查應用程式，可能進行了更改。
```



GENERAL

Single sign on URL ?

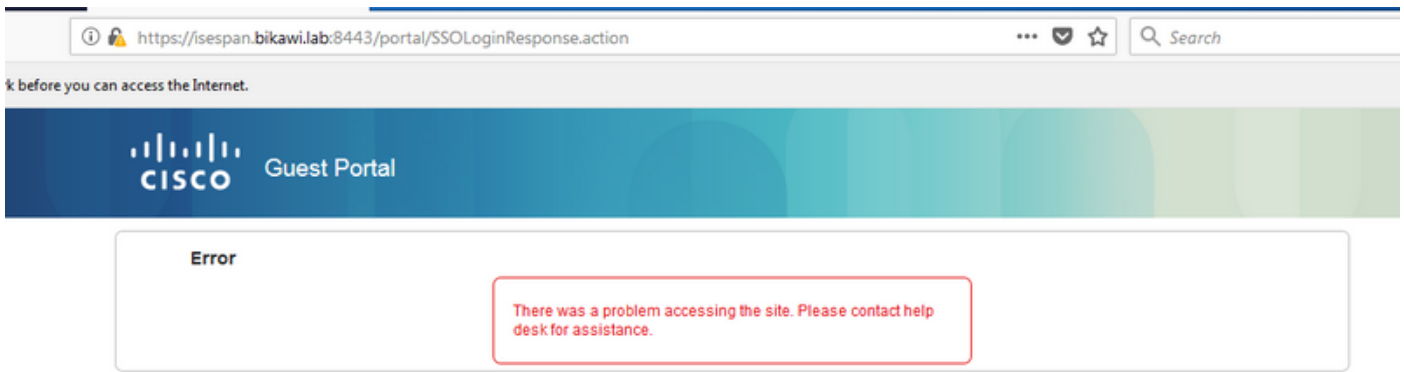
https://10.48.17.71:8443/portal/SSOLoginResponse.action

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

SSO URL使用IP地址，但是，訪客正在傳送FQDN，我們在最後一行上方的請求中看到，包含SEMI\_DELIMITER<FQDN>，要解決此問題，請將IP地址更改為OKTA設定上的FQDN。

場景2. 「訪問站點時出現問題。請聯絡幫助台以獲得幫助」。



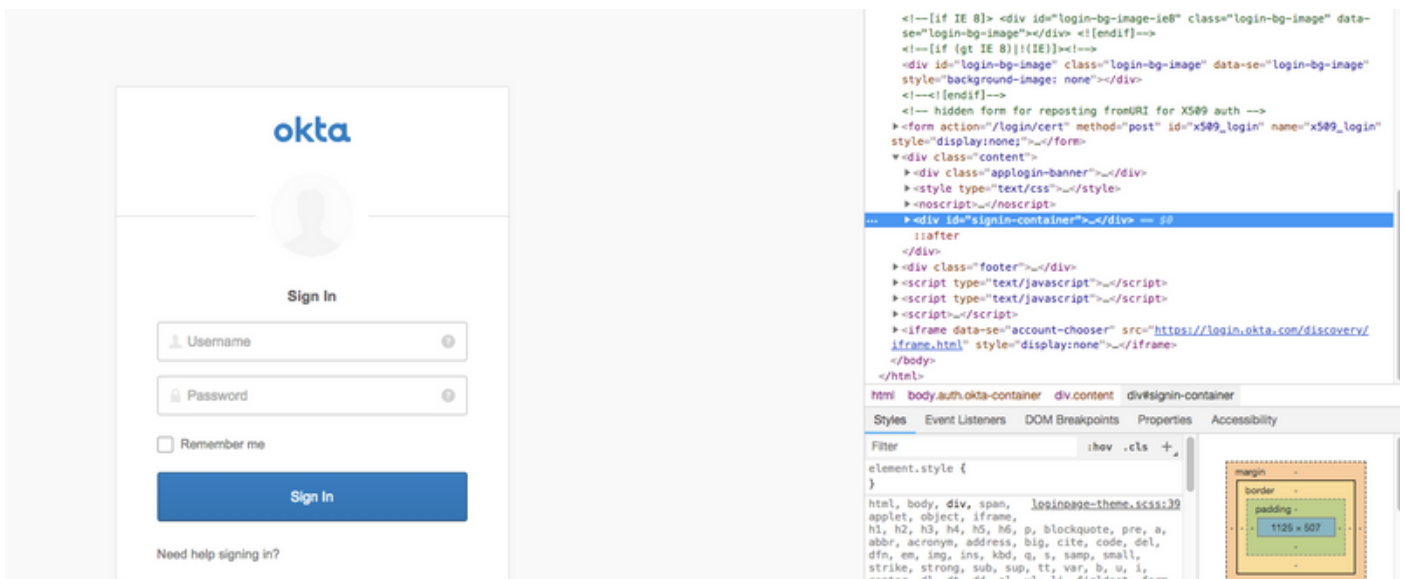
## Guest.log

```
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
```

從日誌中，ISE報告斷言不正確。檢查OKTA受眾URI，確保它與SP匹配以解決此問題。

案例3.已重新導向至「空白」頁面，或登入選項未顯示。

這取決於環境和入口配置。在此類問題中，您需要檢查OKTA應用及其進行身份驗證所需的URL。按一下門戶測試，然後檢查元素以檢查必須訪問的網站。



在此案例中，只有兩個URL:application和login.okta.com — 應該允許在WLC上使用。

## 相關資訊

- <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>