

OKTA SAML SSO로 ISE 2.3 게스트 포털 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[페더레이션 SSO](#)

[네트워크 흐름](#)

[구성](#)

[1단계. ISE에서 SAML ID 제공자 및 게스트 포털을 구성합니다.](#)

[1. 외부 ID 소스를 준비합니다.](#)

[2. SSO용 포털을 생성합니다.](#)

[3. 대체 로그인을 구성합니다.](#)

[2단계. OKTA 애플리케이션 및 SAML ID 공급자 설정을 구성합니다.](#)

[1. OKTA 응용 프로그램을 만듭니다.](#)

[2. SAML ID 공급자에서 SP 정보를 내보냅니다.](#)

[3. OKTA SAML 설정](#)

[4. 응용 프로그램에서 메타데이터를 내보냅니다.](#)

[5. 애플리케이션에 사용자를 지정합니다.](#)

[6. Idp에서 ISE로 메타데이터를 가져옵니다.](#)

[3단계. CWA 컨피그레이션.](#)

[다음은 확인합니다.](#)

[최종 사용자 확인](#)

[ISE 확인](#)

[문제 해결](#)

[OKTA 문제 해결](#)

[ISE 문제 해결](#)

[일반적인 문제 및 솔루션](#)

[관련 정보](#)

소개

이 문서에서는 ISE(Identity Services Engine)를 OKTA와 통합하여 게스트 포털에 SAML SSO(Security Assertion Markup Language Single Sign-On) 인증을 제공하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services Engine 게스트 서비스.
- SAML SSO입니다.
- (선택 사항) WLC(Wireless LAN Controller) 컨피그레이션.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Identity Services Engine 2.3.0.298
- OKTA SAML SSO 애플리케이션
- Cisco 5500 wireless controller 버전 8.3.141.0
- Lenovo Windows 7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

페더레이션 SSO

조직 내 사용자는 한 번만 인증하면 여러 리소스에 액세스할 수 있습니다. 조직 전체에서 사용되는 이 ID를 페더레이션 ID라고 합니다.

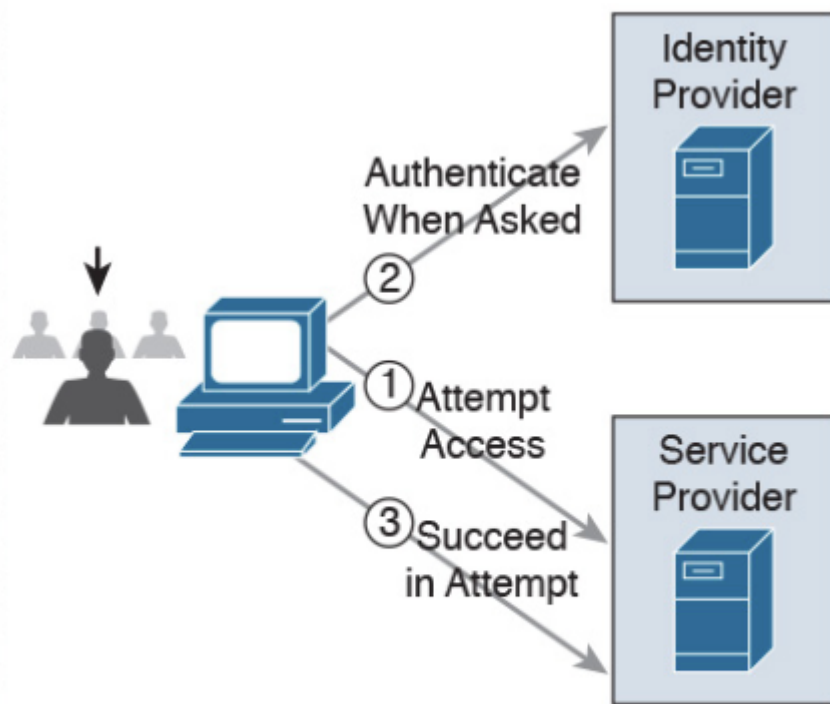
연합의 개념:

- 원칙: 엔드유저(서비스를 요청하는 사용자), 웹 브라우저(이 경우)가 엔드포인트입니다.
- 서비스 공급자(SP): RP(Relying Party)라고도 하며, 이 시스템에서는 ISE가 서비스를 제공합니다.
- IDp(ID 공급자): SP로 다시 전송되는 인증, 권한 부여 결과 및 특성(이 경우 OKTA)을 관리합니다.
- 어설션: IdP에서 SP로 전송한 사용자 정보.

여러 프로토콜에서 OAuth2 및 OpenID와 같은 SSO를 구현합니다. ISE는 SAML을 사용합니다.

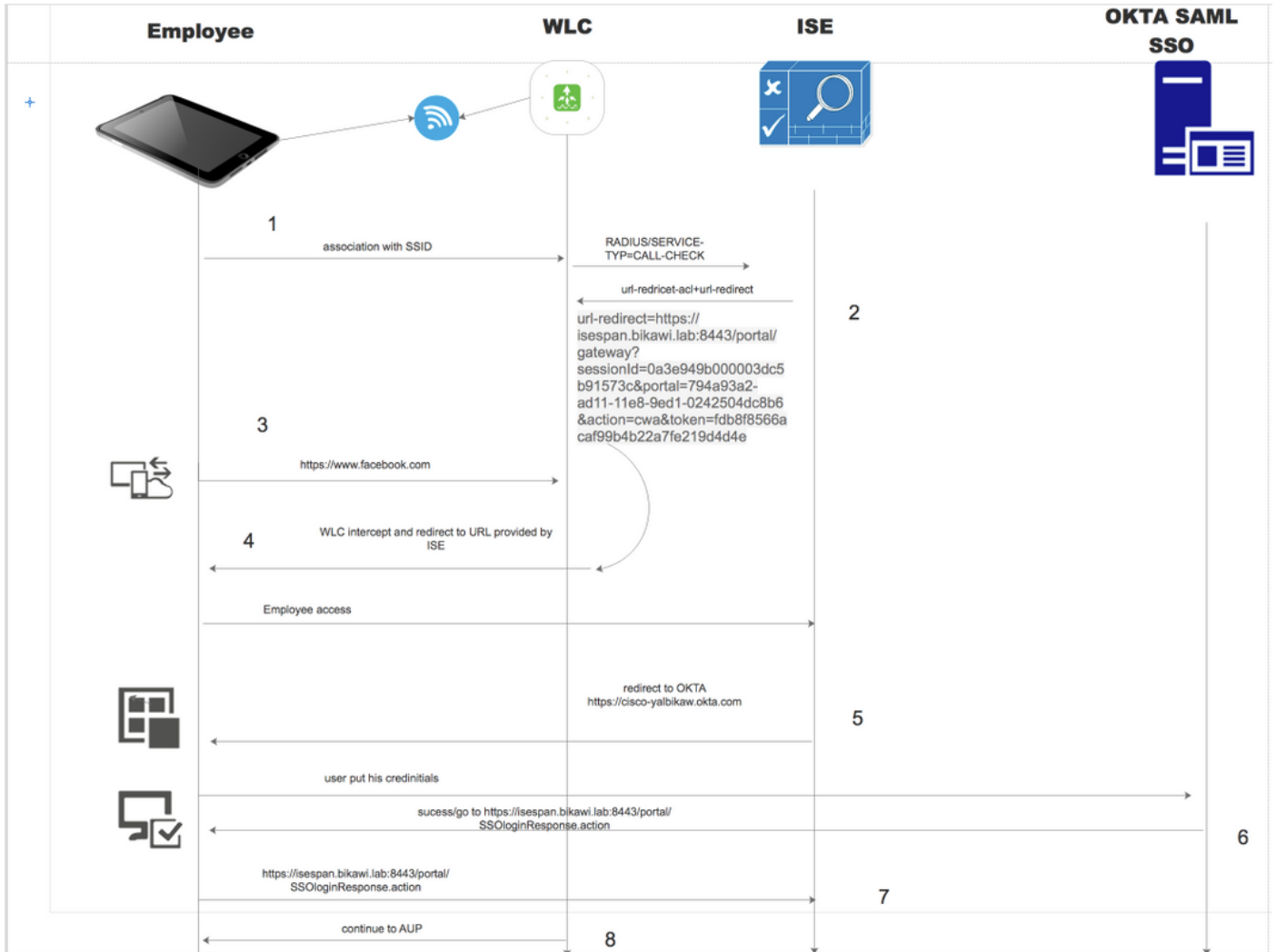
SAML은 XML 기반 프레임워크로서 비즈니스 엔티티 간에 안전하게 SAML 어설션을 사용하고 교환하는 방법을 설명합니다. 표준에서는 이러한 어설션을 요청, 생성, 사용 및 교환하기 위한 구문 및 규칙에 대해 설명합니다.

ISE는 SP 시작 모드를 사용합니다. 사용자가 게스트 포털로 리디렉션된 다음 ISE가 인증을 위해 IdP로 리디렉션합니다. 그런 다음 다시 ISE로 리디렉션됩니다. 요청이 검증되면 사용자는 포털 컨피그레이션에 따라 게스트 액세스 또는 온보딩을 진행합니다.



SP-initiated

네트워크 흐름



1. 사용자는 SSID에 연결되며, 인증은 mab(mac filtering)입니다.

2. ISE는 Redirect-URL 및 Redirect-ACL 특성을 포함하는 access-accept로 응답합니다

3. 사용자가 www.facebook.com에 액세스를 시도합니다.

4. WLC는 요청을 가로채고 ISE 게스트 포털로 사용자를 리디렉션합니다. 사용자는 SSO 자격 증명으로 디바이스를 등록하기 위해 직원 액세스를 클릭합니다.

5. ISE는 인증을 위해 사용자를 OKTA 애플리케이션으로 리디렉션합니다.

6. 인증에 성공하면 OKTA는 SAML assertion 응답을 브라우저로 전송합니다.

7. 브라우저가 어설션을 ISE로 다시 릴레이합니다.

8. ISE는 어설션 응답을 확인하고 사용자가 올바르게 인증되면 AUP로 이동한 다음 디바이스 등록을 진행합니다.

SAML에 대한 자세한 내용은 아래 링크를 참조하십시오

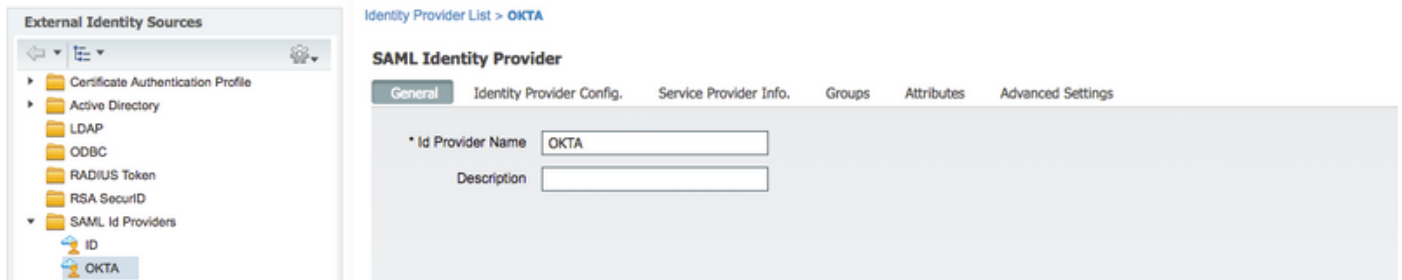
<https://developer.okta.com/standards/SAML/>

구성

1단계. ISE에서 SAML ID 제공자 및 게스트 포털을 구성합니다.

1. 외부 ID 소스를 준비합니다.

1단계. Administration(관리) > External Identity Sources(외부 ID 소스) > SAML ID Providers(SAML ID 제공자)로 이동합니다.

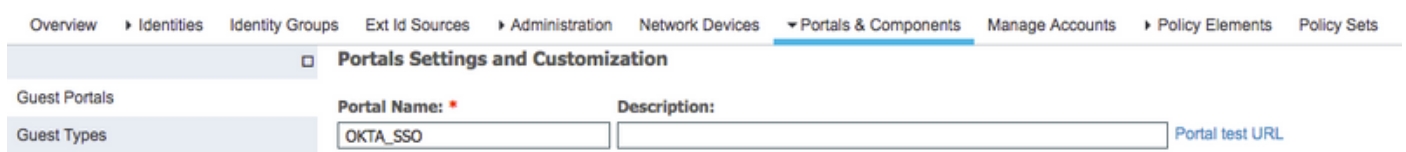
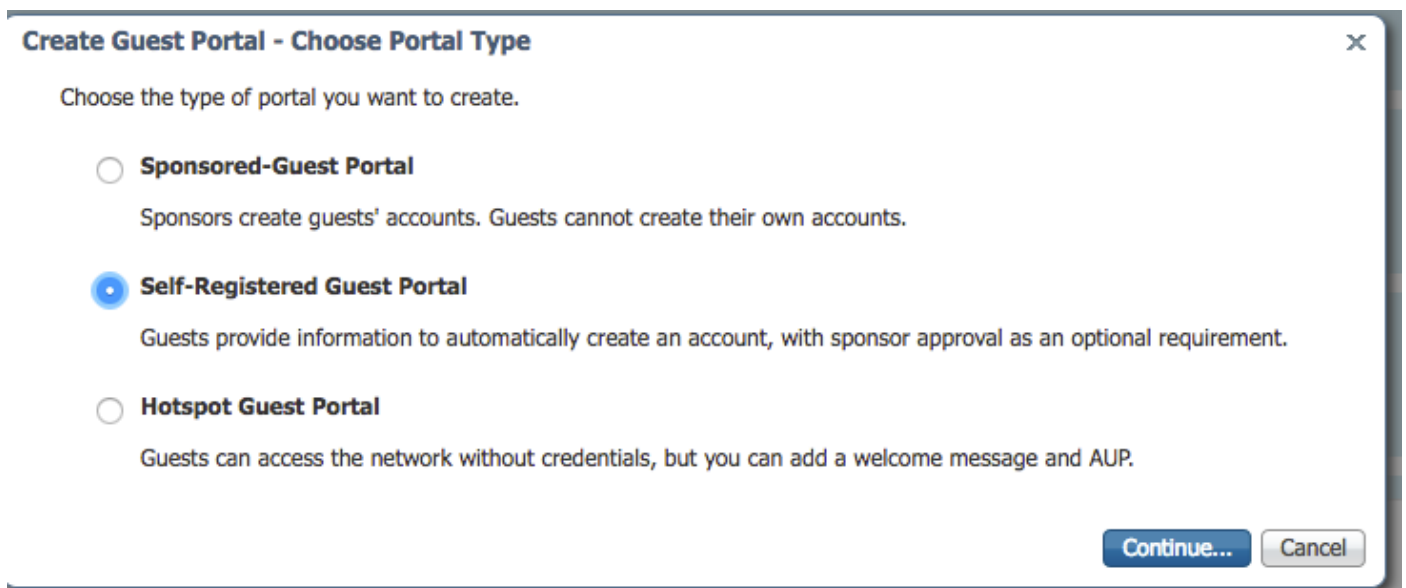


2단계. ID 공급자에 이름을 지정하고 구성을 제출합니다.

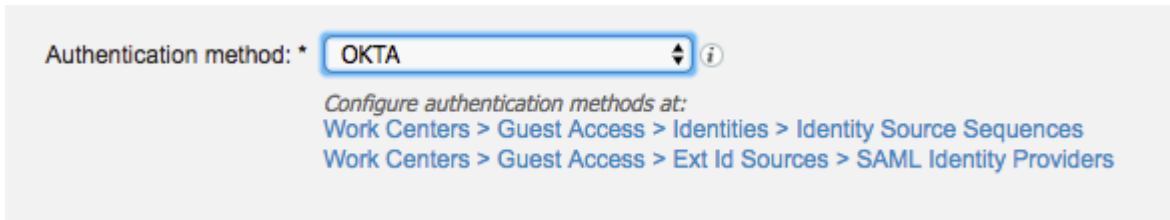
2. SSO용 포털을 생성합니다.

1단계. OKTA에 ID 소스로 할당된 포털을 생성합니다. BYOD, 디바이스 등록, 게스트 등에 대한 기타 모든 컨피그레이션은 일반 포털과 정확히 동일합니다. 이 문서에서 포털은 직원의 대체 로그인으로 게스트 포털에 매핑 됩니다.

2단계. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소)로 이동하여 포털을 생성합니다.

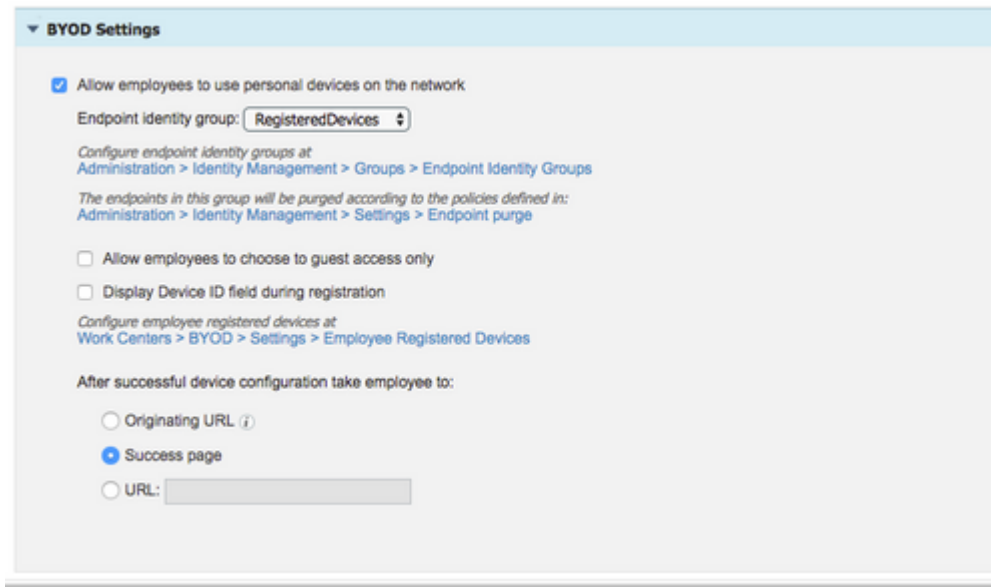


3단계. 이전에 구성한 ID 제공자를 가리키려면 인증 방법을 선택합니다.

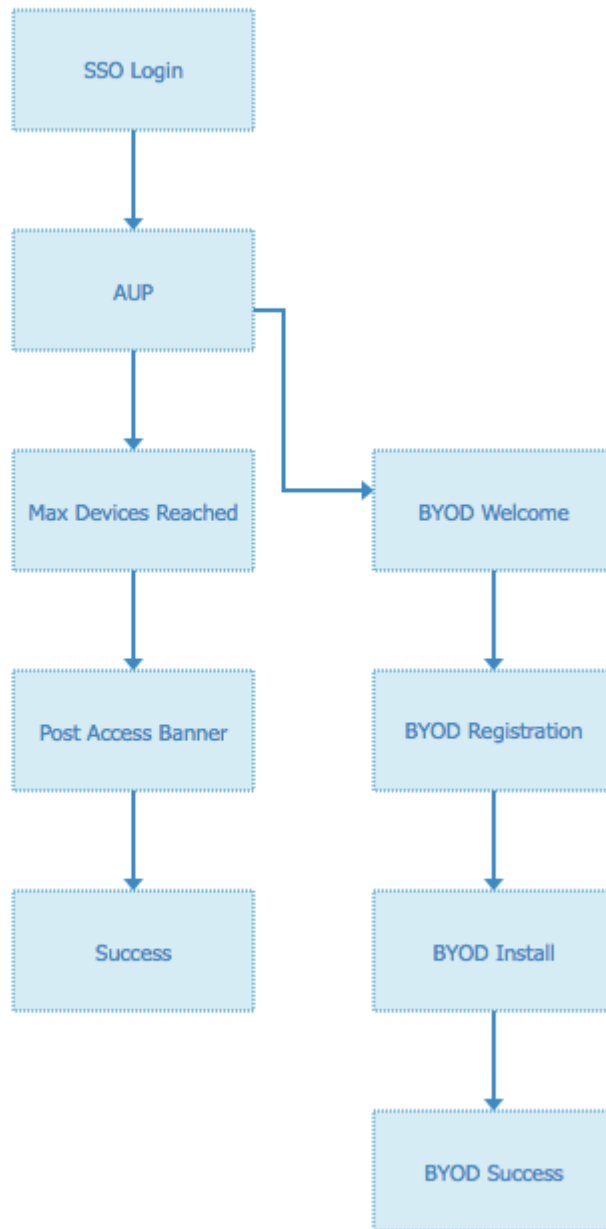


4단계. 인증 방법으로 OKTA ID 소스를 선택합니다.

(선택 사항) BYOD 설정을 선택합니다.



5단계. 포털 컨피그레이션을 저장하고 BYOD를 사용하면 다음과 같은 흐름이 표시됩니다.



3. 대체 로그인을 구성합니다.



참고: 대체 로그인을 사용하지 않는 경우 이 부분을 건너뛸 수 있습니다.

셀프 등록 게스트 포털 또는 게스트 액세스를 위해 사용자 지정된 다른 포털로 이동합니다.

로그인 페이지 설정에서 대체 로그인 포털을 추가합니다. OKTA_SSO입니다.

▼ 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 on page ▾

☐ Require acceptance

☐ Require scrolling to end of AUP

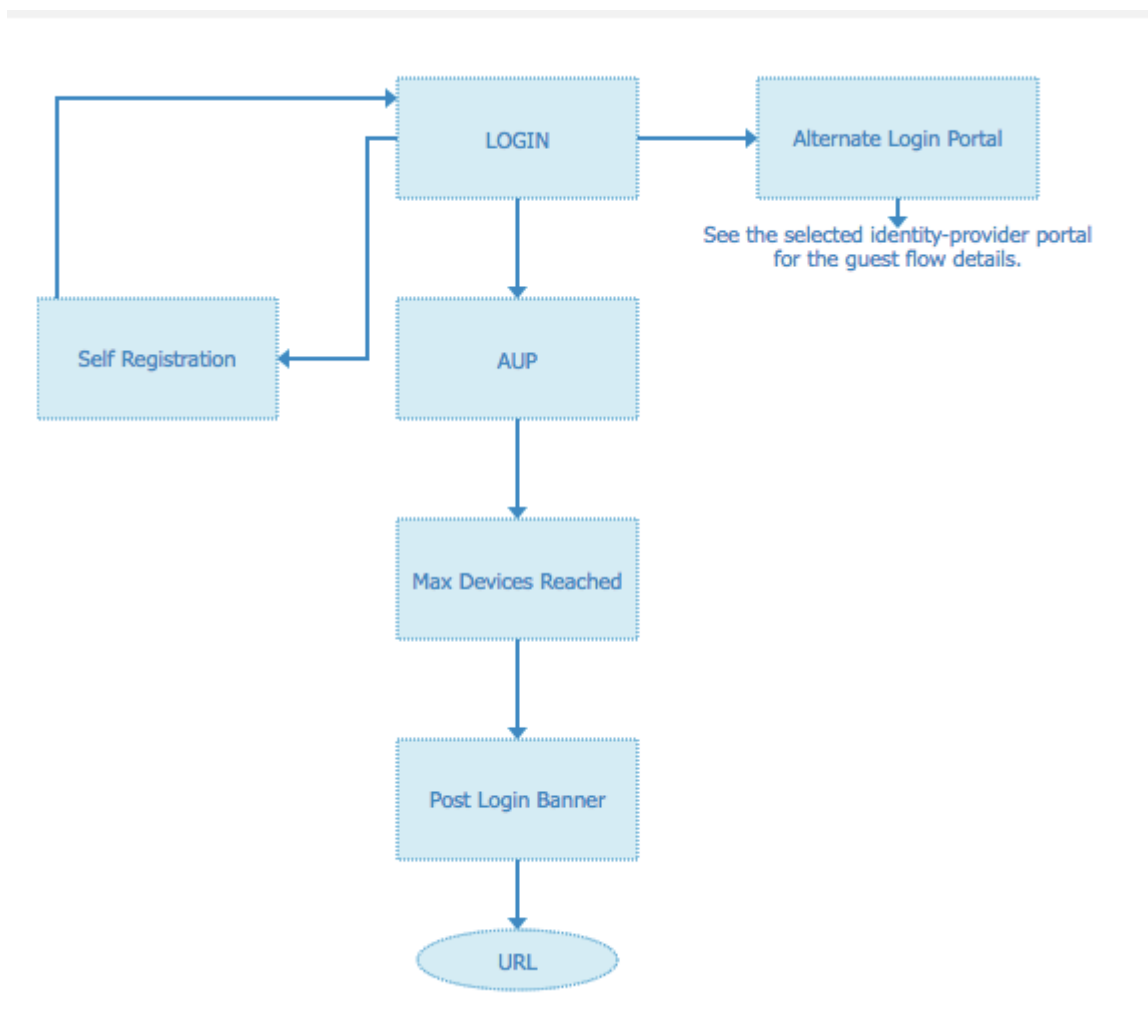
☐ Allow guests to create their own accounts

☐ Allow social login

☐ Allow guests to change password after login ⓘ

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

이것은 포털 흐름입니다.



2단계. OKTA 애플리케이션 및 SAML ID 공급자 설정을 구성합니다.

1. OKTA 응용 프로그램을 만듭니다.

1단계. 관리자 계정으로 OKTA 웹사이트에 로그인합니다.

[← Back to Applications](#)

[Add Application](#)

Search for an application

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

INTEGRATION PROPERTIES

Any
Supports SAML
Supports Provisioning

Application	Status	Integration Type	Action
Teladoc	Okta Verified		Add
&frankly	Okta Verified	✓ SAML	Add
10000ft	Okta Verified		Add
101domains.com	Okta Verified		Add

2단계. Add Application을 클릭합니다.

okta Dashboard Directory Applications Security Reports Settings My Applications

Applications

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

Q Search

STATUS	Count
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

3단계. 새 앱을 만들고 SAML2.0으로 선택합니다.

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

일반 설정

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

1 General Settings
2 Configure SAML
3 Feedback

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

Unspecified

Application username

Okta 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

4단계. 인증서를 다운로드하고 ISE Trusted Certificates에 설치합니다.

Cisco Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers

System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC

Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings

Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settl...
Certificate Authority

Import a new Certificate into the Certificate Store

Certificate File
Choose 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

Submit
Cancel

2. SAML ID 공급자에서 SP 정보를 내보냅니다.

이전에 구성한 ID 공급자로 이동합니다. 이미지에 표시된 대로 Service Provider Info(서비스 제공자 정보)를 클릭하고 내보냅니다.

 주의: 형식 선택은 권한 부여 프로파일의 리디렉션 설정에 따라 달라집니다. 고정 ip를 사용하는 경우 SSO URL에 ip 주소를 사용해야 합니다.

3. OKTA SAML 설정

1단계. SAML 설정에 해당 URL을 추가합니다.

SAML Settings

GENERAL

Single sign on URL ?

https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action

☒ Use this for Recipient URL and Destination URL

☒ Allow this app to request other SSO URLs

Requestable SSO URLs

URL	Index
https://isespan.bikawi.lab:8443/portal/SSOLoginRespo	0

+ Add Another

Audience URI (SP Entity ID) ?

http://CiscoSE/9c969a72-b9cd-11e8-a542-d2e41bbdc546

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

x509SubjectName

Application username ?

Okta username

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

2단계. 이 서비스를 호스팅하는 PSN의 수에 따라 XML 파일에서 URL을 두 개 이상 추가할 수 있습니다. 이름 ID 형식 및 애플리케이션 사용자 이름은 설계에 따라 달라집니다.

B Preview the SAML assertion generated from the information above

< > Preview the SAML Assertion

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

Previous

Cancel

Next

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id127185945833795871212409124" IssueInstant="2018-09-21T15:52:03.823Z"
  <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://i
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2018-09-21T15:42:03.823Z" NotOnOrAfter="2018-09-21T15:52:03.823Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2018-09-21T15:47:03.790Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

3단계. 다음을 클릭하고 두 번째 옵션을 선택합니다.

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

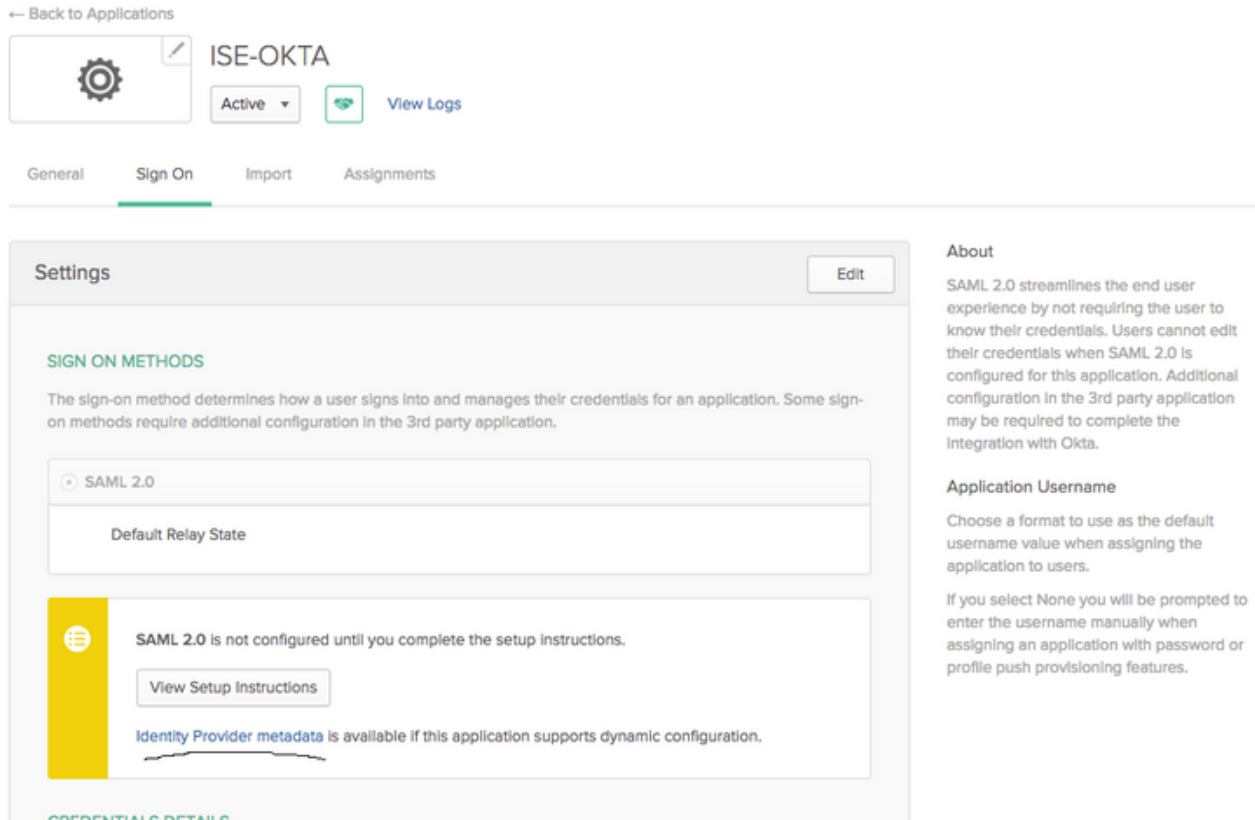
Why are you asking me this?

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

Previous

Finish

4. 응용 프로그램에서 메타데이터를 내보냅니다.



메타데이터:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk1
<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIDrDCCApSgAwIBAgIGAaWwP1TasMA0GCSqGSIb3DQEBwUAMIGWMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcn5pYTEwMB
</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.com"
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://cisco.com"
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

파일을 XML 형식으로 저장합니다.

5. 애플리케이션에 사용자를 지정합니다.

이 응용 프로그램에 사용자를 할당하면 AD를 통합할 수 있는 방법이 있습니다. 이에 대해서는 다음에서 설명합니다. [옥타 액티브 디렉토리](#)

6. Idp에서 ISE로 메타데이터를 가져옵니다.

1단계. SAML Identity Provider(SAML ID 제공자) 아래에서 Identity Provider Config. 및 Import Metadata(메타데이터 가져오기)를 선택합니다.

SAML Identity Provider

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

Identity Provider Configuration

Import Identity Provider Config File ⓘ

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

Single Sign On URL https://cisco-yalbiokta.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

2단계. 구성을 저장합니다.

3단계.CWA 컨피그레이션.

이 문서에서는 ISE 및 WLC의 컨피그레이션에 대해 설명합니다.

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

Redirect-ACL에 URL을 추가합니다.

<https://cisco-yalbiokta.com> / 애플리케이션 URL 추가

<https://login.okta.com>

REDIRECT-ACL IPv4

Foot Notes

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

Remove
Clear Counters
Add-Remove
URL

다음을 확인합니다.

포털을 테스트하고 OKTA 애플리케이션에 연결할 수 있는지 확인합니다.

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.

1단계. 포털 테스트를 클릭하면 SSO 애플리케이션으로 리디렉션됩니다.

Connecting to 

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





Sign In

Username

Password

☐ Remember me

Sign In

Need help signing in?

2단계. <application name>에 대한 정보 연결 확인

3단계. 자격 증명을 입력하면 잘못된 saml 요청이 표시될 수 있습니다. 그렇다고 해서 현재 컨피그레이션이 잘못된 것은 아닙니다.

최종 사용자 확인

https://sespan.bikawilab.8443/portal/PortalSetup.action?portal=794a03a2-ae01-11e8-9ed1-02425040db06&sessionid=0a3e949a000002c15eb0036e0... you can access the Internet.

 Guest Portal

Sign On

Sign on for guest access.

Username:

Password:

Sign On

[Or register for guest access](#)

You can also sign with

 [Facebook](#)

https://isco-ya.bikawilab.okta.com/login/login.htm?fromURL=%2Fapp%2Fiscoorg808433_iseokta_2%2Fesk1rq81oCmed254356%2Fse%2Fsam%3FSAMLRe... you can access the Internet.

Connecting to 

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





Sign In

okta-test@cisco.com

☐ Remember me

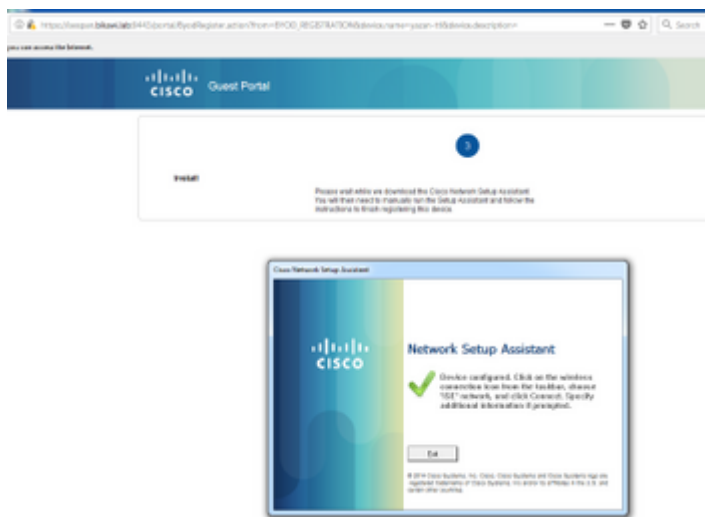
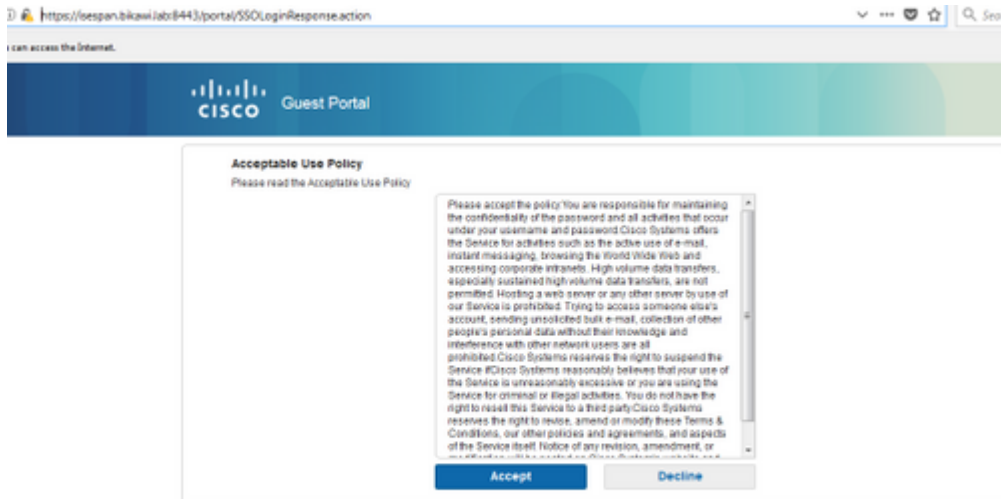
Sign in

Need help signing in?

https://sespan.bikawilab.8443/portal/SSOLoginResponse.action before you can access the Internet.



Signing in to ISE-OKTA



ISE 확인

인증 상태를 확인 하기 위해 수명 로그를 확인 합니다.

Sep 30, 2018 12:39:09.514 AM	✓	🔒	okta-test@cisco.c...	3CA9:F4:34:9F:70					
Sep 30, 2018 12:33:32.640 AM	✓	🔒	3CA9:F4:34:9F:70	3CA9:F4:34:9F:70	Intel-Device	Default >> M...	Default >> wireless-mab-guest	yazan-cpp	

문제 해결

OKTA 문제 해결

1단계. Reports(보고서) 탭에서 로그를 확인합니다.

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)

SSO Attempts

Auths Via AD Agent (Total, Failed)

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

2단계. 또한 애플리케이션에서 관련 로그를 확인합니다.

← Back to Applications

ISE-OKTA

Active

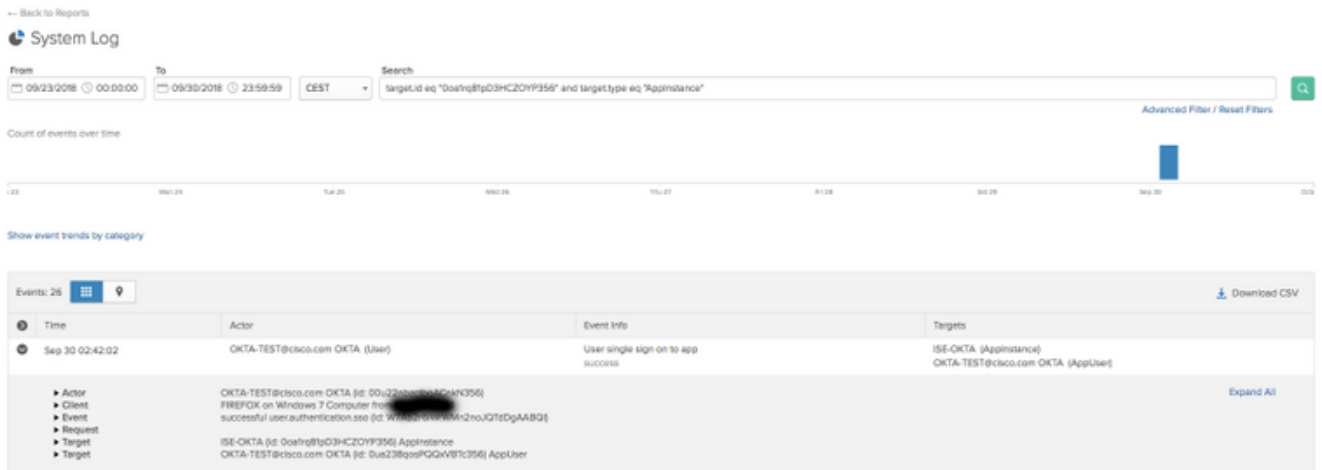
View Logs

General

Sign On

Import

Assignments



ISE 문제 해결

검사할 두 개의 로그 파일이 있습니다.

- ise-psc.log
- guest.log

Administration > System > Logging > Debug Log Configuration으로 이동합니다. DEBUG에 대한 레벨을 활성화합니다.

SAML	ise-psc.log
게스트엑세스	guest.log
포털	guest.log

이 표에서는 디버깅할 구성 요소와 해당 로그 파일을 보여 줍니다.

일반적인 문제 및 솔루션

시나리오 1. 잘못된 SAML 요청입니다.

400

BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

이 오류는 일반적입니다. 로그를 확인하여 흐름을 확인하고 문제를 정확하게 파악하십시오. ISE guest.log에서 다음을 수행합니다.

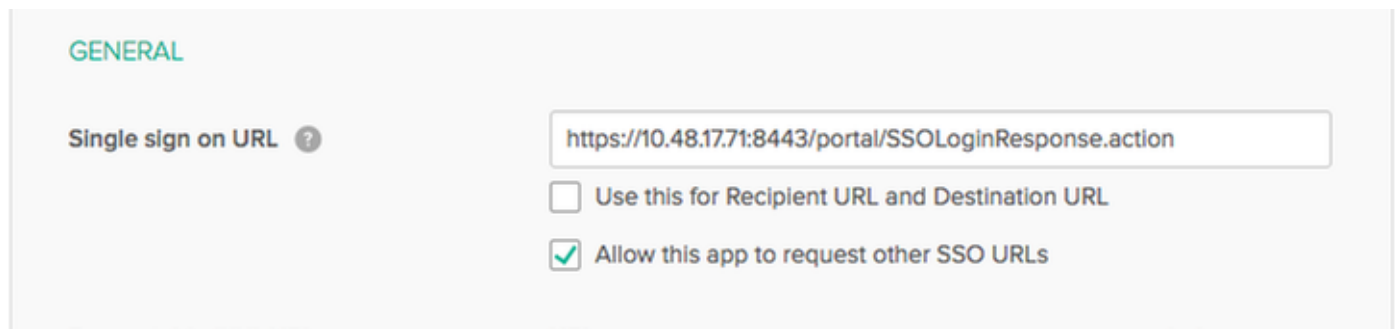
ISE# show logging application guest.log | 지난 50

```
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
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.com
onId=0a3e949b000002c55bb023b3;
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
Ib%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoelUyPu95j9%2FzJ00b4672DqCNUDD%2FR5GHkiuKiEf
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd50V93Lnn1MP%2B6mS6Kq8TFfJ13ugJMM%2B
2B3aGyRWgMzond309NPSMCpq0YDguZsJw1Rfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YI037q9fB1QnCh3jFo72
a1Id_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.uti
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1J0xiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoelUyPu95j9%2FzJ00b4672
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd50V93Lnn1MP%2
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJw1Rfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngd
1bbdc546_DELIMITERportalId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,626 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
2018-09-30 01:32:35,627 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2] [] cisco.ise.portalwebaction.com
```

ISE에서 사용자를 IDP로 리디렉션했습니다. 그러나 ISE에 다시 응답하지 않으며 잘못된 SAML 요청이 나타납니다. OKTA가 아래의 SAML 요청을 수락하지 않음을 확인합니다.

```
https://cisco-yalbi.kaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONKi%2FZRoeUyPu95j9%2FzJ00b4672DqCNUDDJ%2FR5GHkiuKiEfH04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd50V93Lnn1MP%2B6mS6Kq8TFfJ13ugJMm%2B2B3aGyRWgMzond309NPSMCpq0YDguZsJw1Rfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YI037q9fB1QnCh3jFo72a1Id_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-940a-b0f83
```

이제 응용 프로그램을 다시 확인합니다. 변경 사항이 있을 수 있습니다.



GENERAL

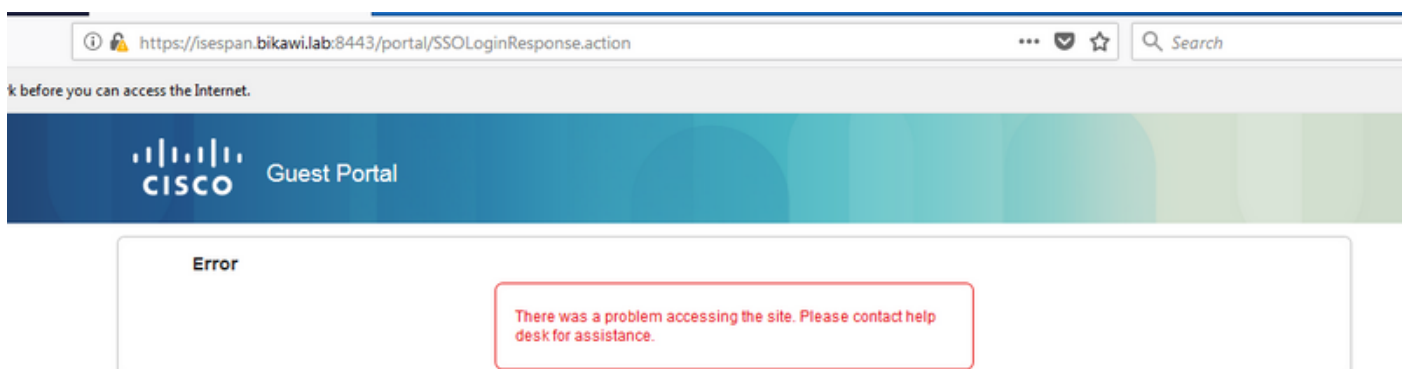
Single sign on URL ?

☐ Use this for Recipient URL and Destination URL

☒ Allow this app to request other SSO URLs

SSO URL이 IP 주소를 사용하지만 게스트가 FQDN을 전송합니다. 마지막 줄에 있는 요청에 나와 있는 것처럼 이 문제를 해결하기 위해 SEMI_DELIMITER<FQDN>을 포함합니다. OKTA 설정에서 IP 주소를 FQDN으로 변경합니다.

시나리오 2. "사이트에 액세스하는 동안 문제가 발생했습니다. 도움이 필요하면 헬프데스크에 문의하십시오."



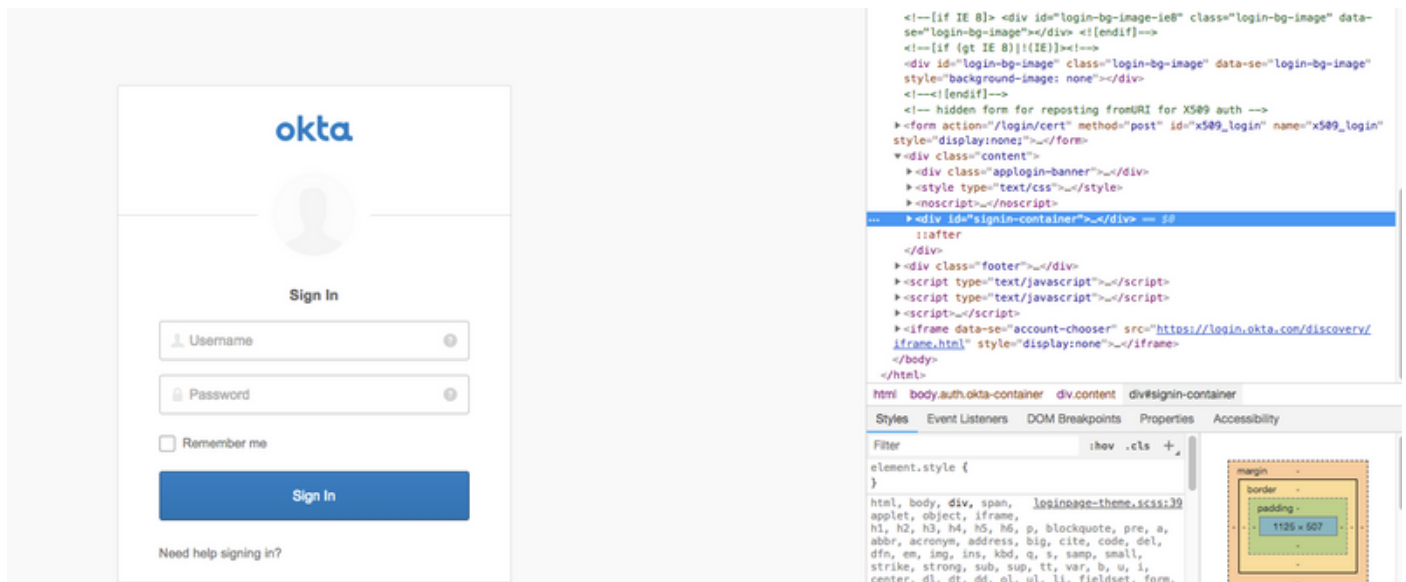
Guest.log

```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][] guestaccess.flowmanager.step.
tching service provider identifier in the audience restriction conditions
2018-09-30 02:25:00,609 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][] guestaccess.flowmanager.step.
```

로그에서 ISE는 Assertion이 올바르지 않음을 보고합니다. OKTA Audience URI(대상 그룹 URI)에서 SP와 일치하는지 확인하여 해결합니다.

시나리오 3. 빈 페이지로 리디렉션되거나 로그인 옵션이 표시되지 않습니다.

환경 및 포털 컨피그레이션에 따라 달라집니다. 이러한 종류의 문제에서는 OKTA 애플리케이션과 인증에 필요한 URL을 확인해야 합니다. 포털 테스트를 클릭한 다음 inspect 요소를 클릭하여 연결할 수 있어야 하는 웹 사이트를 확인합니다.



이 시나리오에서는 두 개의 URL만 애플리케이션 및 login.okta.com - WLC에서 허용되어야 합니다.

관련 정보

- <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>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.