

OKTA SAML عم 2.3 ISE فيض لخدم نيوكت SSO

تايتو تحملا

[عم دق م لا](#)

[عم ساس ال ا تاب ل ط ت م لا](#)

[تاب ل ط ت م لا](#)

[عم دخت س م لا تانوك م لا](#)

[عم ساس ا تامول عم](#)

[سا و سا داختا](#)

[عم ك ب ش ل ق ف د ت](#)

[نيوك ت ل ا](#)

[ISE. ىلع فيض ل ا لخدمو SAML عم يوه رفوم نيوك ت 1. عم و ط خ ل ا](#)

[1. عم ي ج ر ا خ ل ا عم يوه ل ا ر د ص م دا د ع ا .](#)

[2. ب ت ك م ل ا ب ص ا خ ل خدم ا ش ن ا .](#)

[3. ل ي د ب ل و خ د ل ي ج س ت ن ي و ك ت .](#)

[SAML عم يوه رفومو OKTA ق ي ب ط ت ا دا د ع ا ن ي و ك ت 2. عم و ط خ ل ا](#)

[1. OKTA ق ي ب ط ت ا ش ن ا .](#)

[2. SAML عم يوه رفوم ن م SP تامول عم ر ي د ص ت .](#)

[3. OKTA SAML ا دا د ع ا .](#)

[4. ق ي ب ط ت ل ا ن م ف ي ر ع ت ل ا ت ا ن ا ي ب ر ي د ص ت .](#)

[5. ق ي ب ط ت ل ل ن ي م د خ ت س م ن ي ي ع ت .](#)

[ت ا ع ا ص ا ل ل ل ق ت س م ل ا د ع م ل ا ل ا ا ي ل خ ا د ن ي د ر ش م ل ا ن م عم ي ف ص و ت ا ن ا ي ب د ا ر ي ت س ا - 6](#)

[ل ي ك ش ت 3.cwa عم و ط خ](#)

[عم ح ص ل ا ن م ق ق ح ت ل ا](#)

[ي ئ ا ه ن ل ا م د خ ت س م ل ا ن م ق ق ح ت ل ا](#)

[ISE ن م ق ق ح ت ل ا](#)

[ا ه ا ل ص ا و ا ط ا خ ا ل ا ف ا ش ك ت س ا](#)

[ا ه ا ل ص ا و OKTA ا ط ا خ ا ف ا ش ك ت س ا](#)

[ا ه ا ل ص ا و ISE ا ط ا خ ا ف ا ش ك ت س ا](#)

[عم ك ر ت ش م ل ا ل و ل ح ل ا و ا ي ا ض ق ل ا](#)

[عم ل ص ت ا ذ ت ا م و ل عم](#)

عم دق م لا

عم دق م لا ري فوتل، OKTA عم Identity Services Engine (ISE) ل م ا ك ت عم ي ف ي ك د ن ت س م ل ا ا ذ ه ح ض و ي ف و ي ض ل ا عم ب ا و ب ل (SAML SSO) ن ا م ا ل ا د ي ك ا ت عم غ ل ل ي دا ح ا ل ا ل و خ د ل ا ل ي ج س ت

عم ساس ال ا تاب ل ط ت م لا

[تاب ل ط ت م لا](#)

ةةللاتل عيضاوملاب ةفرعم كلدل نوكت ناب Cisco يصوت:

- Cisco نم ةيوهال تامدخ كرحم فويض تامدخ.
- وس لماس.
- (WLC) ةيكلسالل (LAN) ةيولحملا ةكبشلل في مكلحتلا ةدحو نيوك (يراي تخ).

ةمدختسملل تانوكملا

ةةللاتل ةيداملل تانوكملا وجماربلل تارادصلل دلل دننتسملل اذو في ةدراولل تامولعملل دننتست:

- Identity Services Engine 2.3.0.298
- OKTA SAML SSO قيبطت
- Cisco 5500 Wireless Controller، رادصلل 8.3.141.0
- Windows 7 نم Lenovo ليعششتلل ماطن

ةصاخ ةيلعمل ةئيبل في ةدووملا ةزهجال نم دننتسملل اذو في ةدراولل تامولعملل عاشنل مت تناك اذا. (يضارثفا) حوسم نيوك تب دننتسملل اذو في ةمدختسملل ةزهجال عيمج تادب رملل لمتحملل ريثاتلل كلمهف نم دكأتف، ليعششتلل دي قكتك تشبش.

ةيساسا تامولعمل

سإ و سا داخلا

ةددعتم دراوم دلل لوصولل هنكمي م، ةدحاو ةرم ةقداصلل ةسسؤملا لخاد ممدختسملل نكمي ةدحوملا ةيوهال تاموظنملا ربع ةمدختسملل ةيوهال هذو يمسو.

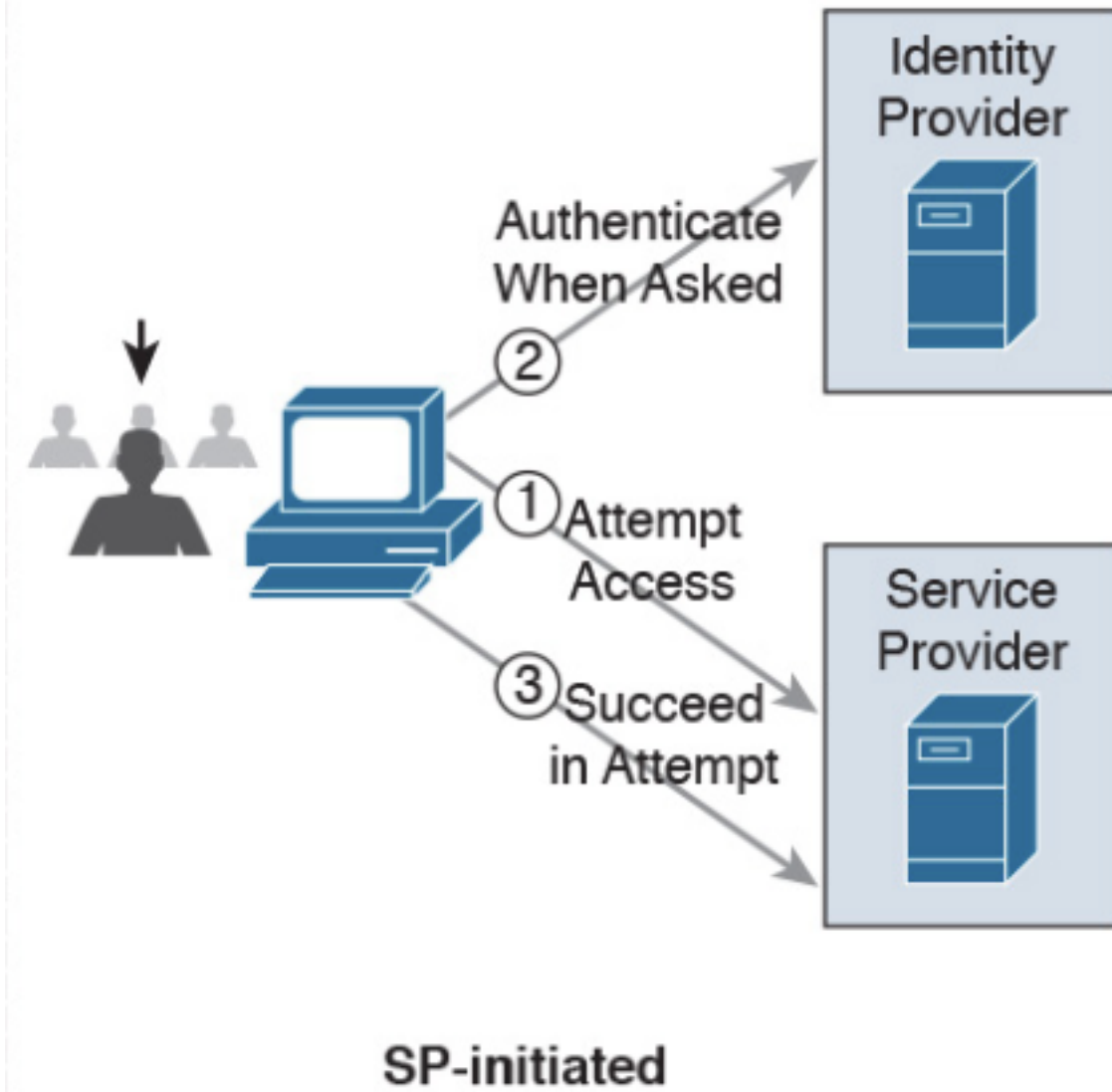
داختاللا موهم:

- هذه في، بيولل حفصتم، (ةمدخل بلطي يذلا ممدختسملل) يئاهنل ممدختسملل: أدبملا ةياهنل ةطقن وه، ةلاخل.
- هذه في، ةمدخل رفوي يذلا ماطنل وهو، (RP) لوعملا فرطلل انايحأ يسمي (SP) ةمدخلل دوزم ISE، ةلاخل.
- اهل سارل متي يتل تامسلاو ليوختللا جئاتنو ةقداصلل ريدي يذلا (IdP) ةيوهال رفوم OKTA، ةلاخل هذه في SP، دلل ىرخأ ةرم.
- SP دلل IdP ةطساوب ةل سرمل ممدختسملل تامولعمل: ديكأتللا.

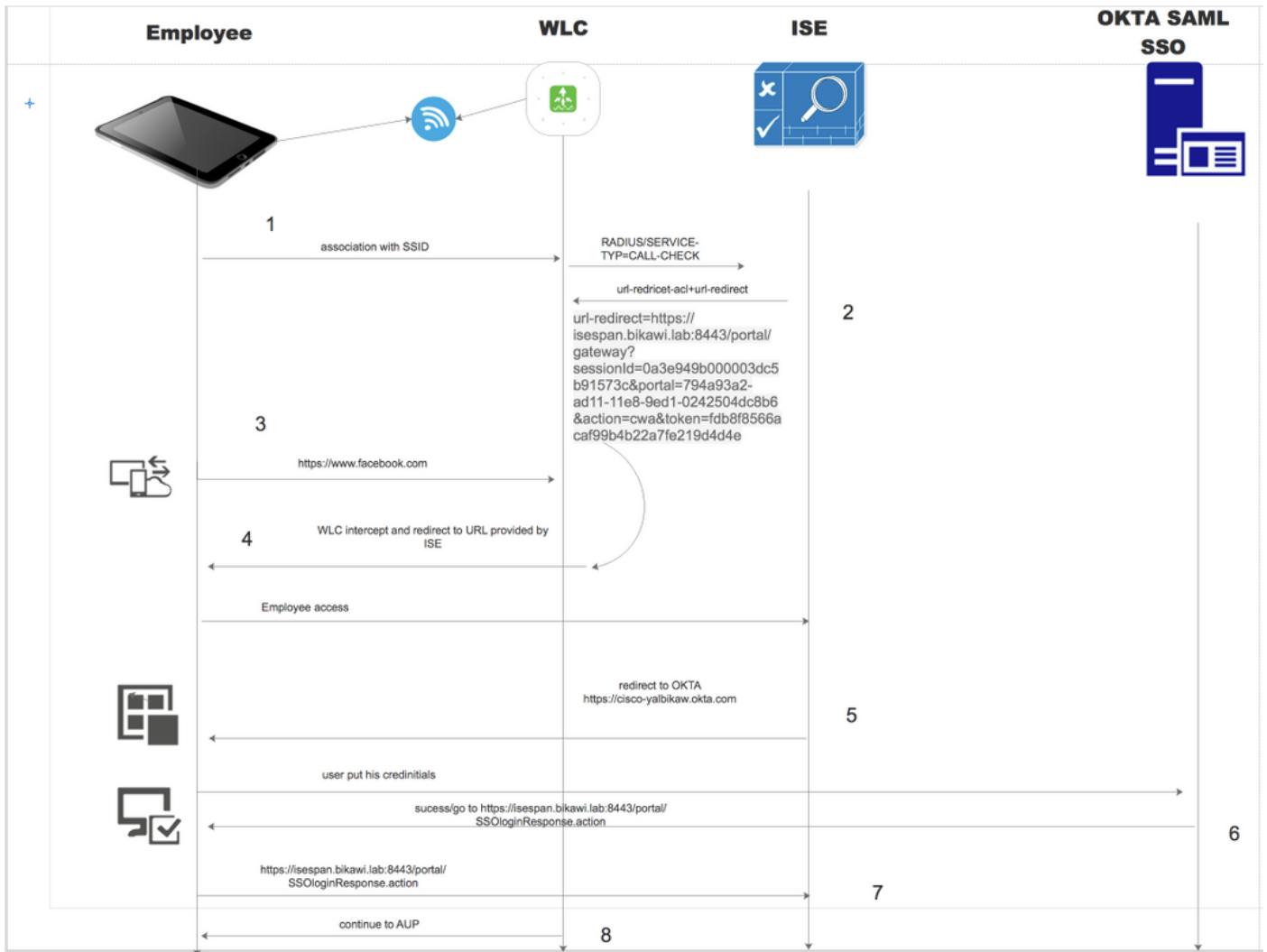
ISE ممدختسي OpenID و OAuth2 لثم SSO ريرياعم قيبطت تالوكتو ربلل نم دي دعلل موقت SAML.

ةنم آقيرطب اهل دابو SAML تاديكات مادختسلا فصي XML دلل دننتسي لمع راطل وه SAML تاديكاتللا هذه بلطب ةصاخلا دعاوقلاو ةغايصلل راي عملل فصي. ةيراجتلل تانايكلل نيب اهل دابو اهمادختساو اهئاشنل و.

موقمي م، Guest لخدم دلل ممدختسملل هيحوت ةداغ ممت. هوذب مت يذلا SP عضو ISE ممدختسي ققحتللا مت. ISE دلل هيحوتللا دي عي هنل، كلذ دعبو. ةقداصلل IDP دلل لهيحوت ةداغاب ISE دلل هجاردل وافيصلل دلل لوصولل ةيلعمل في ممدختسملل يضمي و، بلطللا ةحص نم ةبوابلل نيوكتل اقفو، تنرتنللا.



ةكبشلا قفدت



1. MAC (MAB) في صفت يه قداصم لاو، SSID، ب مدختسم لا لصتي.

2. هيجوت لا دواعل URL ناوع تامس لىع يوتحت يتلا لوصول لوبق ةزي م ب ISE بيجتسي و (ACL) لوصول ي ف مكحتلا ةمئاقو

3. www.facebook.com لى لوصول مدختسم لا لواحي.

4. مدختسم لا رقنيو، ISE فيض لخدم لى مدختسم لا هيجوت ديعتو بلطال WLC ضرعتت. SSO دامتعا تانايب مادختساب زاهال ليجستل فظوم لا لوصول لىع

5. قداصم لا ل OKTA قيبطت لى مدختسم لا هيجوت دواعل ISE موقتي.

6. ضرعتسم لا لى SAML ديكأت ةباجتسا ل OKTA لسري، ةحجانلا قداصم لا دع ب.

7. ISE لى ديكأتال اعجار ب ضرعتسم لا موقتي.

8. هنا ف، حيحص لكش ب مدختسم لا قداصم تمت اذاو ديكأتال ةباجتسا لى ISE ققحتي. زاهال ليجست ب م ث AUP لى لقتني.

SAML لوح تامولعمل نم ديزم لىع لوصول هاندأ طابترال اعجار

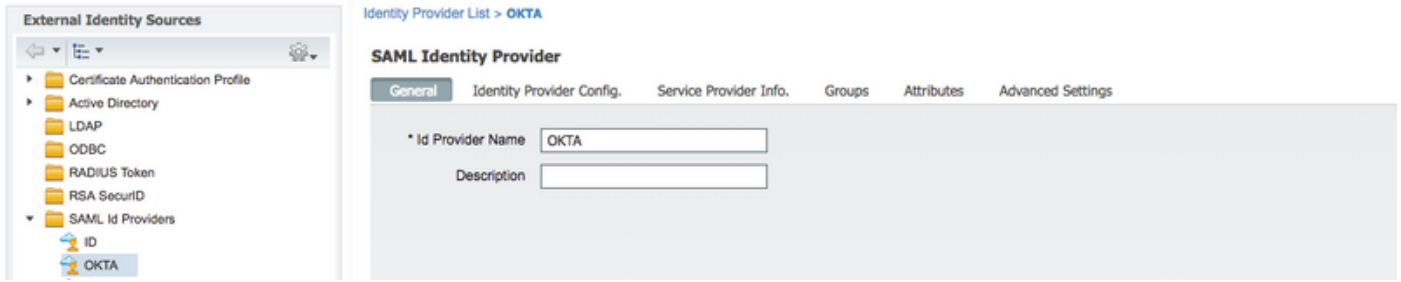
<https://developer.okta.com/standards/SAML/>

نيوكتلا

ISE لىع فيضال لخدم و SAML ةيوه رفوم نيوكت 1. ةوطخلال

1. ةجراخلال ةيوهال ردصم دادعلا.

SAML ID. ڀرفوم > ڏيڃراڃال ڏي وهال رداصم > ڏرادال ڀل لڃتنا 1. ڏوطڃال

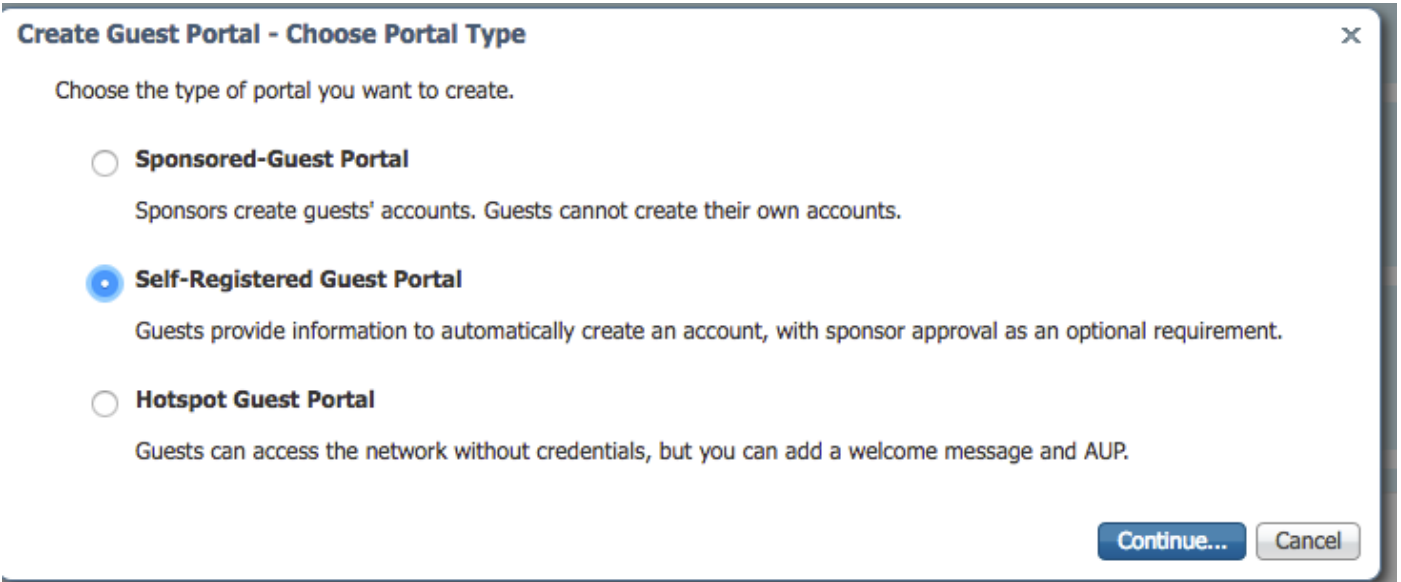


ڀني وڃتا ل لسراو فرعمال رفوم ل مسا ڀني عتب مق 2. ڏوطڃال

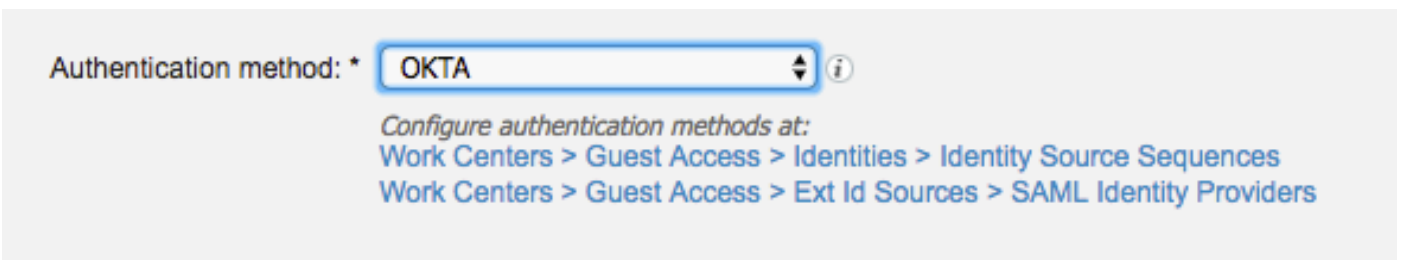
2. بڃتا م ل ا ب صاڃ لڃدم عاشن ا.

ل رخا ڀني وڃتا ڀا. ڏي وه رداصم ڪ OKTA ڀل ڀني عتب مت ڀي ڏال لڃدمال عاشن ا ب مق 1. ڏوطڃال ڀي ڏال لڃدمال ل ڏس ڀل ل اڃال وه ام ڪ امامت هس فن وه، ڃل Guest ...، ڏزه ا ل لڃست، BYOD، فظوم ل ل وڃد ل لڃست ل لڃد ڪ فڀض ل لڃدمال لڃل لڃدمال ڀني عتب متي، دن تس مال اڏه ڀي ف.

ڏابو ڀل عاشن ا ب مق و تان و ڪم و تاباوب > فڀض ل ل و ص و > ل عمال زڪارم ڀل لڃتنا 2. ڏوطڃال



اڃب سم هني وڃتا مت ڀي ڏال ڏي وهال رفوم ڀل ڀراش ا ل ل ڏقداصم ل بول سا رتڃا 3. ڏوطڃال



ڏقداصم ڏقڀرط ڪ OKTA ڏي وه رداصم رتڃا 4. ڏوطڃال

BYOD تاداداعا رتخأ (يراي تخا)

▼ 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](#)

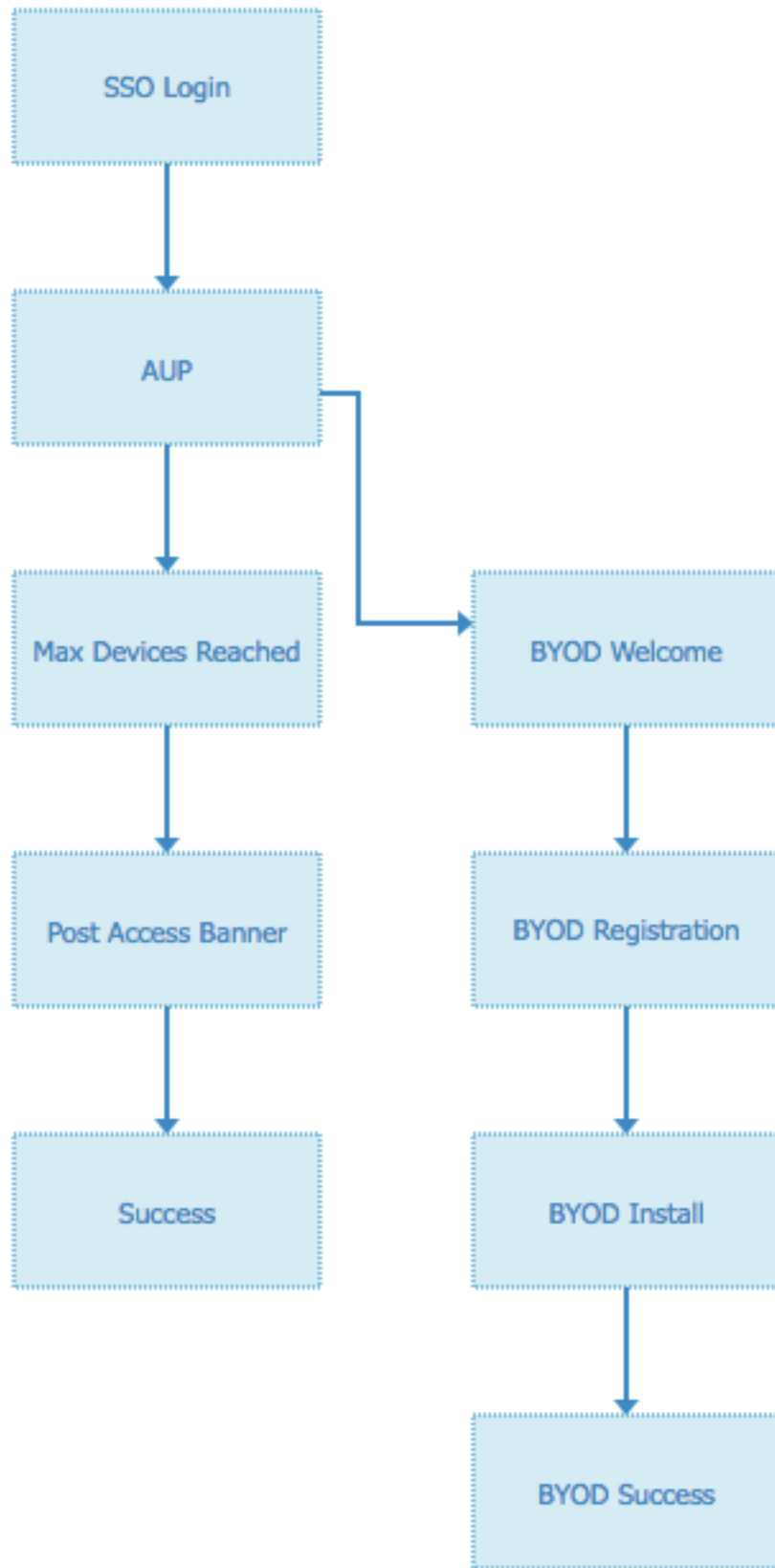
After successful device configuration take employee to:

Originating URL (i)

Success page

URL:

يولي امك قفدتلا ودبي BYOD مادختساب، لخدملا نيوكت ظفح 5 ةوطخلا



3. لېډب لوڅد لېجسټ نېوكت.

لېډبال لوڅدال لېجسټ مډختسټ نكت مل اذا عزالا اذه ي طخت كنكمي: **ةظحالم**

فويضلال لولل وصلولل صصخم رخآ لخدم يا وأ "يتاذلال لېجسټلال فيضة بابو" لى لقتنا

OKTA_SSO: ةل يدبلا لوخدلا ليجست ةباوب ةفاضاب مق ،لوخدلا ليجست ةحفص تاداعإ يف

▼ 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

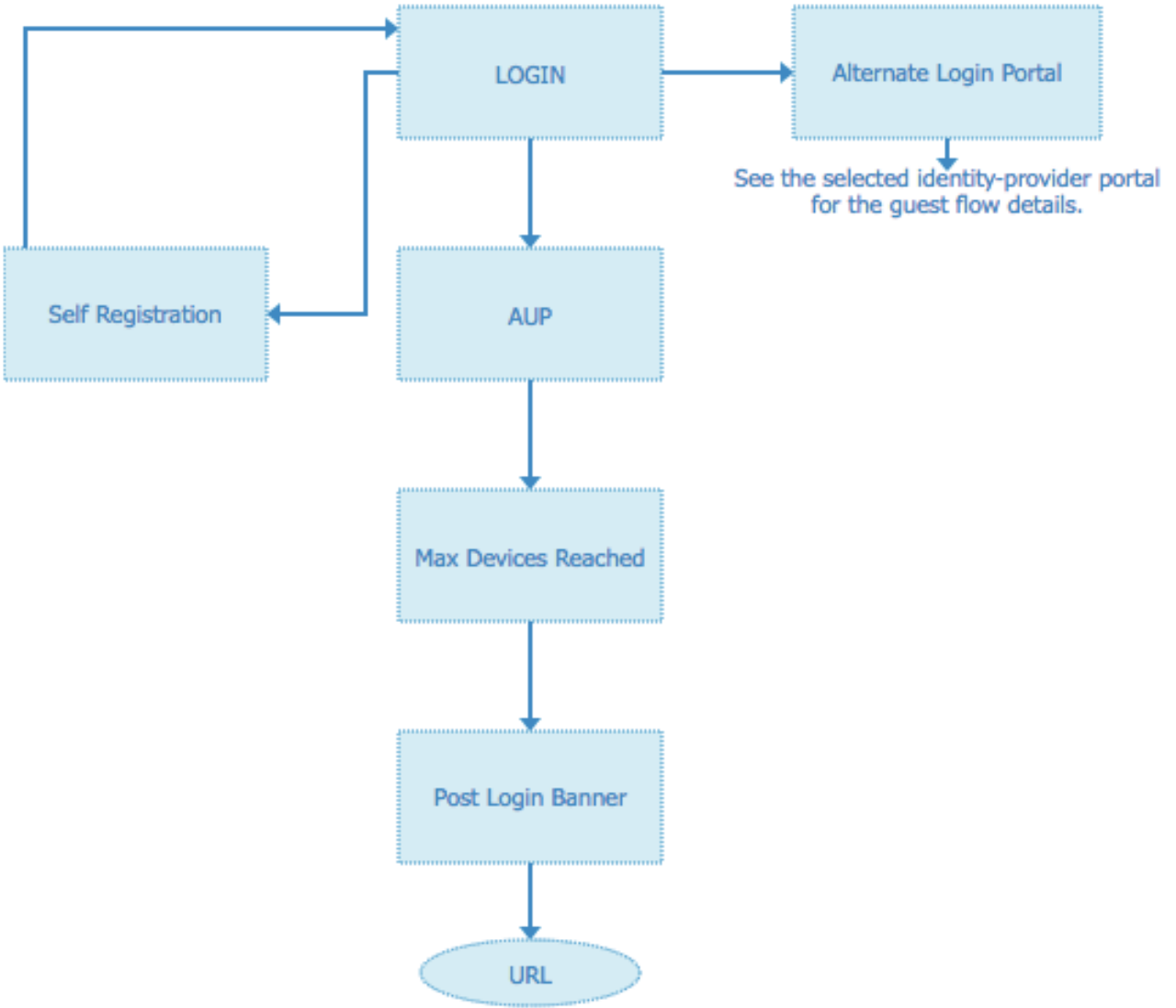
Allow social login

Allow guests to change password after login ⓘ

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

▼

نآلا ةباوبلا قفدت وه اذه.



SAML ةي وه رفوم و OKTA قي بطت ا اداع | ني وكت . 2 ة و ط خ ل ا

1. OKTA قي بطت ء اش ن | .

ل. لوؤسم باسح ما د خ ت سا ب بي و ل ا ي ل ع OKTA ع قوم ي ل ا لو خ د ل ا ل ي ج س ت . 1 ة و ط خ ل ا

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

قېبىتاتە فاضل قوف رونا 2. ةوطخل

okta Dashboard Directory Applications Security Reports Settings My Applications ↻

Applications

Help

[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

3. ةوطخل SAML2.0 نوكل هرتخ، دىج قېبىتاتە عاشن

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

مراجعة الإعدادات

+

 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

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](#)

ةقووثوم ال ISE تاداهش يف اهتېبثتو ةداهشلا لېزنتب مق 4. ةوطخال

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

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. SAML ةيوه رفوم نم SP تامولعم ريڊصت.

اهريڊصتو ةمدخال دوزم تامولعم قوف رقنا. اقېسم هنېوكت مت يذلا ةيوهال رفوم ىل لقتنا، ةروصلال يف حضورم وه امك.

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

XML وreadme.txt فلم ىلع ردصملا zip دلجم يوتحي

```
OKTA_SSO.xml
<?xml version="1.0" encoding="UTF-8" ?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://CiscoISE/9c969a72-b9cd-11e8-a542-d2e41bbdc546" ?>
  <md:SPSSODescriptor
    AuthnRequestsSigned="false"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    ?>
    <md:KeyDescriptor use="signing" ?>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/
        ...
      </ds:KeyInfo>
    </md:KeyDescriptor>
    ...
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

ىلإ جاتيحي ،ةلاجال هذه في نكل ،ةرشابم XML داريتسا كنكمي ةيوهلا ىرفوم ضعبل ايودي داريتسالا .

- SAML دي كأت) يداجال لوخدلا لىجستل URL ناوع

```
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"
```

- سايك فرعم SP

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

FQDN قىسنتو IP ناوع في رفوتم SSO ل URL ناوع

،لىوختلا فيرعت فلم ىلع هيچوتلا ةداع| تاداع| ىلع قيسىنتلا ديدجت دمتعي :ريذحت ،URL ناوع ل IP ناوع مادختسا كيلىع بجي في ،كيكياتسا نكاس ip مدختست تنك اذا ةعوسم لابل صاخلا .

3. تاداع| OKTA SAML.

SAML تادادع|ىل ع هذه URL نيوانع فضا 1. ةوطخال

A 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

X

+ Add Another

Audience URI (SP Entity ID) ?

http://CiscoISE/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

PSN نيوانع ددع ىل ادا نسا ، XML فلم نم دحاو URL ناو نع نم رثك اة فاضا كنكمي 2. ةوطخال ىل ع قىب طتال مدختسم مساو مسالا فرعم قىسنت دمتعي . ةمدخال هذه فىضتست ىتال ك صاخال ميمصتال

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="2018-09-21T15:47:03.790Z" 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>
```

3. يثا لرايخ لرتخا ويلي لالتا رقا .

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. قيبطتال نم فيرعتال تانايب ريصت .


```
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>
```

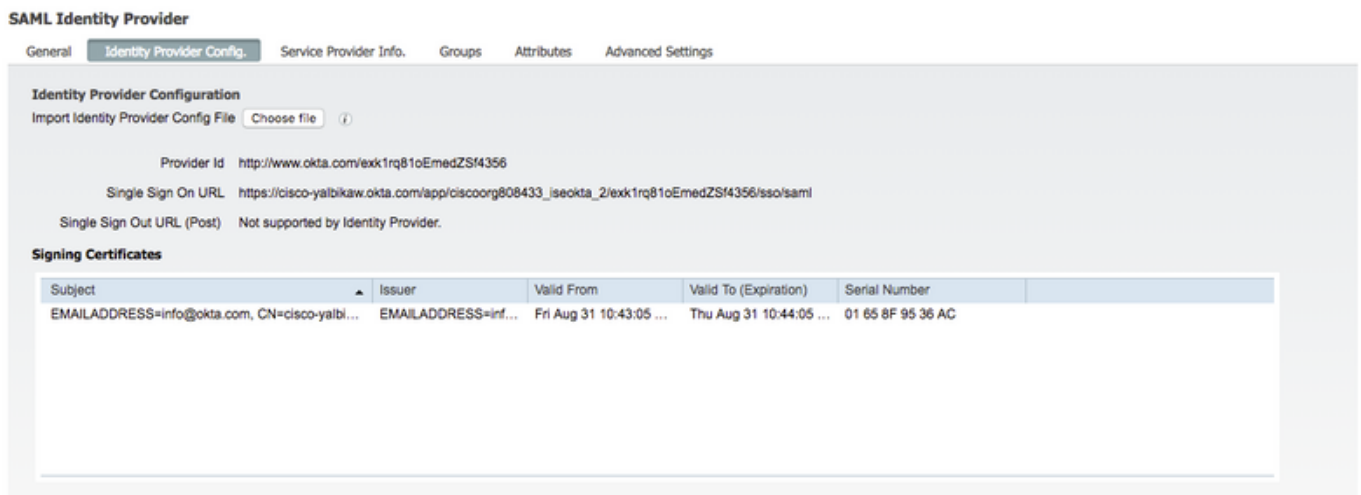
XML قيسنتب ف لمل اظفح.

5. قيبطت ل ل نيمدختسم نيي عت.

تاءاصح ل ل قوتسم ل ده عمل ا ل ا ل خاد نيدرشم ل نم ةي ف ص و تان ا ب داريت سا - 6
 ةي ل و ا ل تان ا ب ل ا دروت سا و Identity Provider Config دح ، SAML Identity Provider تحت 1. ةوطخ ل

تاءاصح ل ل قوتسم ل ده عمل ا ل ا ل خاد نيدرشم ل نم ةي ف ص و تان ا ب داريت سا - 6

ةي ل و ا ل تان ا ب ل ا دروت سا و Identity Provider Config دح ، SAML Identity Provider تحت 1. ةوطخ ل



نيدرشم ل ل اظفح ب مق 2. ةوطخ ل

للي كشت 3.cwa ةوطخ

WLC و ISE ل ليرشم ل ل اظفح و اذ فصي

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

هيجوت ل ل اذ ا ل (ACL) ل و ص و ل ا ب م كحت ل ل ا ةم ئ ا ق ي ف URL نير و ان ع ةفاضا

كب ص ا خ ل ل قيبطت ل ا ب ص ا خ ل ل URL نير و ان ع ةفاضا / <https://cisco-yalbikaw.okta.com>

<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.

ةحصلال نام ققحتلال

OKTA ققبطت ال لوصول ال ع ارداق تنك اذا امم ققحتلال وةباوبال رابتحاب مق

Portal Name: *

Description:

OKTA_SSO

[Portal test URL](#)



Portal Behavior and Flow Settings

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



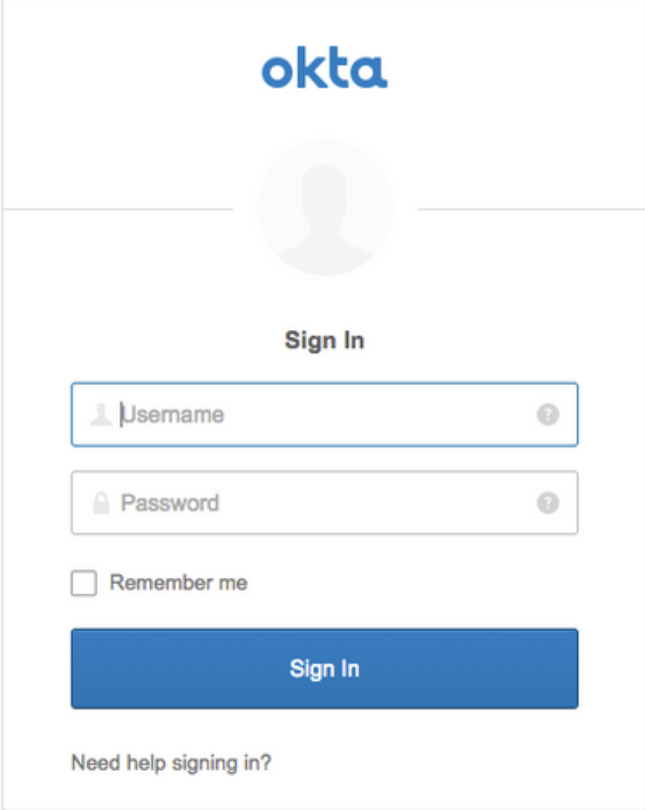
Portal Page Customization

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

SSO ققبطت ال لكهيجوت ةداعل بجي مث ،ةباوبال رابتحل قوف رقنا 1. ةوطخال

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 picture is the text "Sign In". The form contains two input fields: "Username" and "Password", each with a question mark icon to its right. Below these fields 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?".

<قېب طتال مس> ب تامول عمل لاصتا نم ققحت 2. ةوطخال

ةرورض لابل ينعي ال اذف ،حيحص ريغ بلط ىرت دق ،دامتعالا تانايب ل اخداب تمق اذا 3. ةوطخال
ةطقنللا هذه يف ئطاخ نيوكتال نا

يئاهنللا مدختسم للا نم ققحتال

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

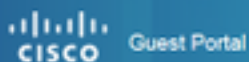
[Need help signing in?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



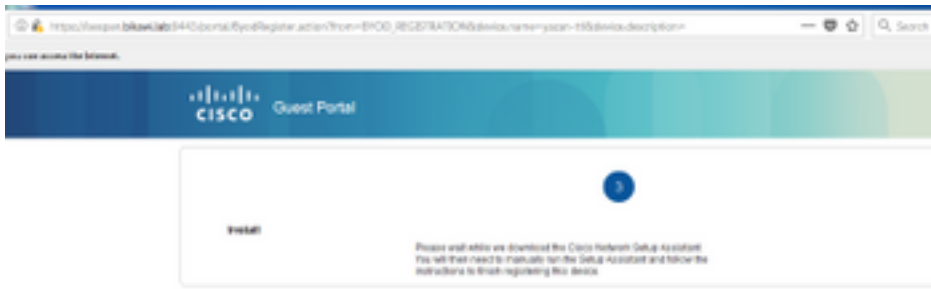
Acceptable Use Policy

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



ISE نم ققحتلا

ةقداصملا ةلاح نم ققحتلل رمعلا تالجس نم ققحت

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

اهحالص او ءاطخ ال فاشكتسا

اهحالص او OKTA ءاطخ ال فاشكتسا

ريراقت بيوبتلا ةمالع يف ةدوجوملا تالجسلا نم ققحت 1. ةوطخل

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

ةلصللا تاذتالجسلا ضرع قيبتطتللا نم اضيأ 2. ةوطخللا

← 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 "0ea7e81b031c201f9356" and target.type eq "AppInstance" [Advanced Filter / Reset Filters](#)

Count of events over time



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: 00a2181b031c201f9356) Client: FIREFOX on Windows 7 Computer from [REDACTED] Event: successful user.authentication.sso (id: W1a2c0181f11Mh2noJGtDgAABQ) Request: [REDACTED] Target: ISE-OKTA (id: 0ea7e81b031c201f9356) AppInstance Target: OKTA-TEST@cisco.com OKTA (id: 00a2181b031c201f9356) AppUser 			

[Expand All](#)

اه حال ص او ISE ءاطخ ا فاش كت س ا

امه ص ح فل ل ج س ل ل ن اف لم ك ان ه

- ise-psc.log
- guest.log

يوت س م ل ا ني ك م ت ب م ق . ءاطخ ا ل ح ح ص ت ل ج س ن ي و ك ت > ل ي ج س ت > م ا ظ ن > ة ر ا د ا ي ل ل ل ق ت ن ا
ءاطخ ا ل ح ح ص ت ي ل ل .

ل م ا س	ise-psc.log
ءاطخ ا ل ح ح ص ت ي ل ل ل و ص و ل ا	guest.log
ة ب ا و ب	guest.log

ه ل ق ب ا ط م ل ا ل ج س ل ا ف ل م و ءاطخ ا ل ح ح ص ت ي ل ل ن و ك م ل ا ل و د ج ل ا ض ر ع ي

ة ك ر ت ش م ل ل و ل ح ل ا و ا ي ا ض ق ل ا

ح ح ص ر ي غ SAML ب ل ط 1. و ي ر ا ن ي س ل ل

okta

400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

ه ا د ص ا ل ا ت ن ي ع و ق ف د ت ل ا ت ق ق د ل o g i n o r d e r t o ل ل ت ص ح ف ، م ا ع ا ط خ ا ذ ه
ISE Guest.log:

ة ن س ن ي س م خ ر خ ا | l o g ل ي ج س ت ل ا ق ي ب ط ت ف ي ض ض ر ع ISE#

```
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
```



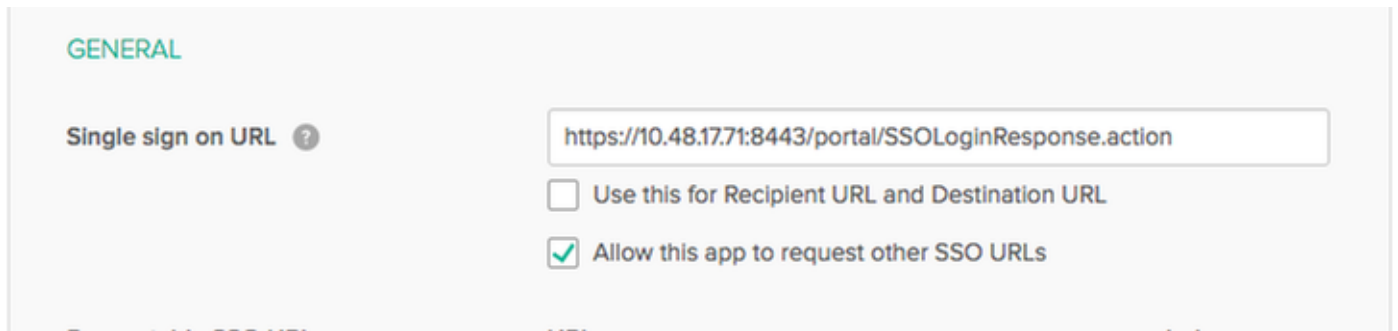
```
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][]
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- portalSessionInfo:
portalId=9c969a72-b9cd-11e8-a542-d2e41bbdc546;portalSessionId=6770f0a4-bc86-4565-940a-
b0f83cbe9372;radiusSessi
onId=0a3e949b000002c55bb023b3;
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%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoEuyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7Zad7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCPq0YDguZsJwlRfz4JqdjINL226IsCffnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnCh3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n
8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERportal
alId_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/exk1rq81oEmedZSf4356/sso/saml
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoEuyPu95j9%2FzJ
OOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJ
o1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DECriw6Sd5n%2FjMxd3Wzoq7Zad7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCPq0YDguZsJwlRfz4JqdjINL226IsCffnE9%2Bu1K14C8Xs4TXE1z
X6nmngdq3YIO37q9fBlQnCh3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWl
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_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
```

بلط رهظي و ISE ل ةباجتس| دجوت ال ،كلذ عم و IDP. ل| مدختس مل ا هي جوت ةداع| ي ف ISE حجن

بطلال وه هاندأ انب صاخال SAML بطل لبق ي ال OKTA نأ دح .جحص ريغ SAML

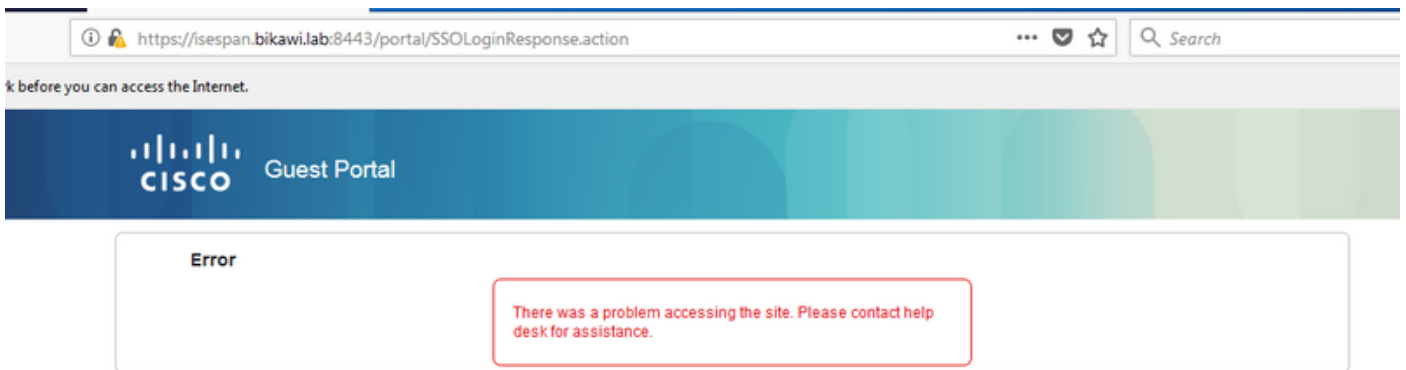
https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9oWFIb%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUDJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1hOiu1yQcIeJo1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0S1taB0Vxv1CPwolhGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2BulK14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnC h3jFo72v2xmatdQLUybIhwd4a85ksvOs9qftIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n8m0x%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

هه لعل تاريخيغ ت عارجا مت ام بر قي بطتال نم ىرخأ قرم نأل ق قح



لاسراب فيضال موق ي ،كلذ عم و ،IP ناوع SSO ىلإ هجوملاب صاخال URL ناوع مدختسي ىلعل يوتحي ريخال رطسلا ىلعلأ دوجومال بطلال ي ف ىرن نأ اننكمي امك FQDN ىلعل FQDN ىلإ IP ناوع ريغيغت ب مق ،ةلكشملا هذه حالصال HALF_DELIMITER<FQDN> OKTA تاداعإ

ةدعاسملا بتكمب لاصتالا جري .عقوملا ىلإ لوصولا ي ف ةلكشم تئدح .2 ويرانيسال ل لوصحلل



Guest.log

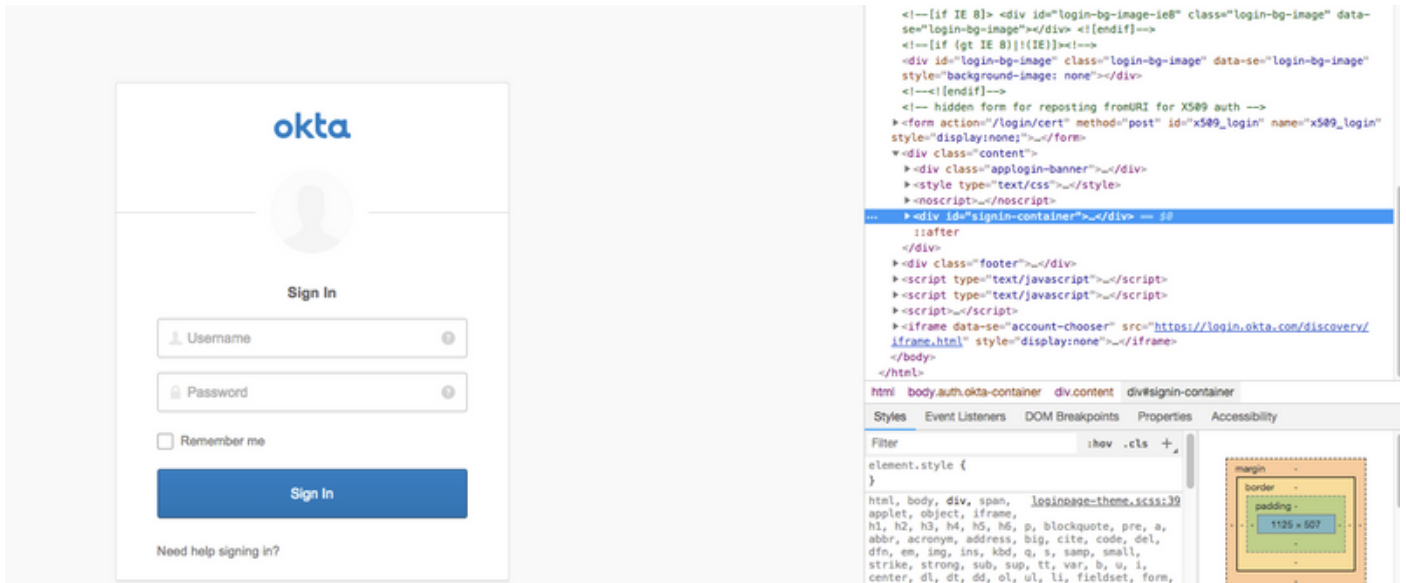
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][ ]
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
contain ma
```

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

نم دكأت OKTA روهمچل URI نم ققحت .جحص ريغ ديكأتال نأب ISE غلبې ،تالچسلا نم
هلحل SP ل هتقباطم .

ل.لخدلا ليجست رايخ رهظي ال وا ،ةغرافال ءحفصلا لىل هيجوتلا ءءاعل تمث 3.ويرانيسلا

نم ققحتي نأ چاتحت ءلكشملا نم عونلا اذه في .ءباوبلا نيوكتو ءئيبلال لىل ءمءتي
صءفب مق مء لءءملا رابءءل قوف رقنا .ءقءاصملا هبلطءي يءلا URL وه امو OKTA قيءبء
ب.بوعقءوم نم هيلال لوصول بءي امم ققءءلل رصنعلا



لىل - login.okta.com و قيءبءءلا :ءقء URL نيوانعب ءامسلا بءي ،ويرانيسلا اذه في
(WLC) ءيكلسالا ءيلاءملا ءكءبءلا في مءءءل رصنع

ءلص ءاءءامولءم

- <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>

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء قء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىلچن إل دن تسمل