

ISE 2.3 Guest Portal met OKTA SAML configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Federale SSO](#)

[Netwerkstroom](#)

[Configureren](#)

[Stap 1. Configureer de SAML Identity Provider en Guest portal op ISE.](#)

[1. Maak een externe identiteitsbron klaar.](#)

[2. Maak een portal voor SSO.](#)

[3. Alternatieve aanmelding configureren](#)

[Stap 2. Configuratie van OKTA-toepassing en van SAML-identiteitsproviders.](#)

[1. Maak OKTA-toepassing.](#)

[2. ExportSP-informatie van SAML Identity Provider.](#)

[3. Instellingen OKTA SAML.](#)

[4. metagegevens uit de toepassing exporteren.](#)

[5. Gebruikers aan de applicatie toewijzen.](#)

[6. Metagegevens importeren van IP naar ISE.](#)

[Stap 3. CWA-configuratie.](#)

[Verifiëren](#)

[Verificatie van eindgebruikers](#)

[ISE-verificatie](#)

[Problemen oplossen](#)

[OKTA-probleemoplossing](#)

[ISE-probleemoplossing](#)

[Gemeenschappelijke problemen en oplossingen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe Identity Services Engine (ISE) moet worden geïntegreerd in OKTA om een Security Assertion Markup Language Single Sign-On (SAML SSO) verificatie te maken voor het gastportaal.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Gastservices van Cisco Identity Services Engine
- SAML SSO.
- (optioneel) configuratie van draadloze LAN Controller (WLC).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine 2.3.0.298
- OKTA SAML SSO-toepassing
- Cisco 5500 draadloze controller versie 8.3.14.0
- Lenovo Windows 7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Federale SSO

Een gebruiker binnen een organisatie kan één keer authenticeren en dan toegang tot meerdere bronnen hebben. Deze identiteit die door organisaties wordt gebruikt wordt gefedereerd genoemd.

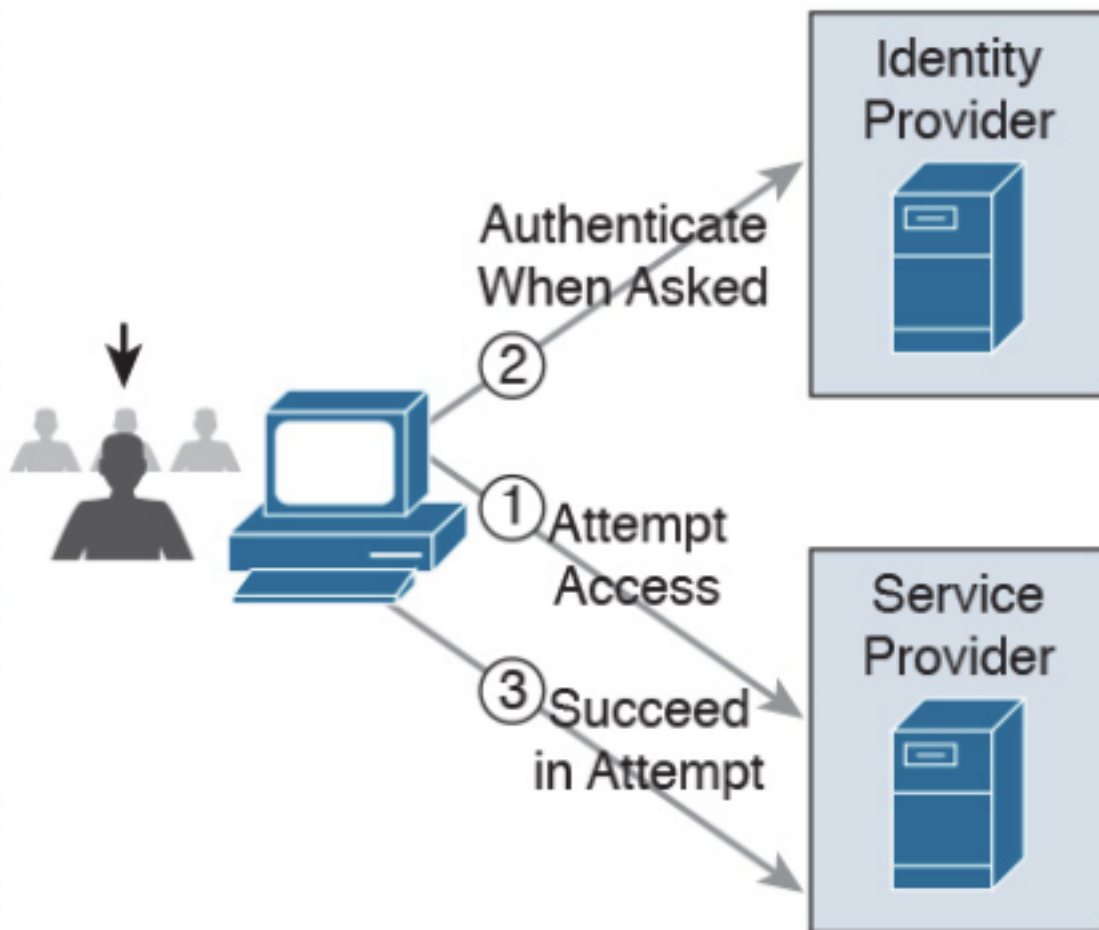
Het concept federatie:

- Beginsel: Eindgebruiker (degene die om een service vraagt), webbrowser, in dit geval, is het eindpunt.
- Serviceprovider: soms een relying Party (RP) genoemd, het systeem dat een dienst verleent, in dit geval ISE.
- Identiteitsaanbieder (IDP): die de echtheidscontrole, het autorisatieresultaat en de eigenschappen beheren die teruggestuurd worden naar SP, in dit geval OKTA.
- Verklaring: de gebruikersinformatie die door IDP naar SP wordt verzonden.

Verschillende protocollen implementeren SSO's zoals OAuth2 en OpenID. ISE gebruikt SAML.

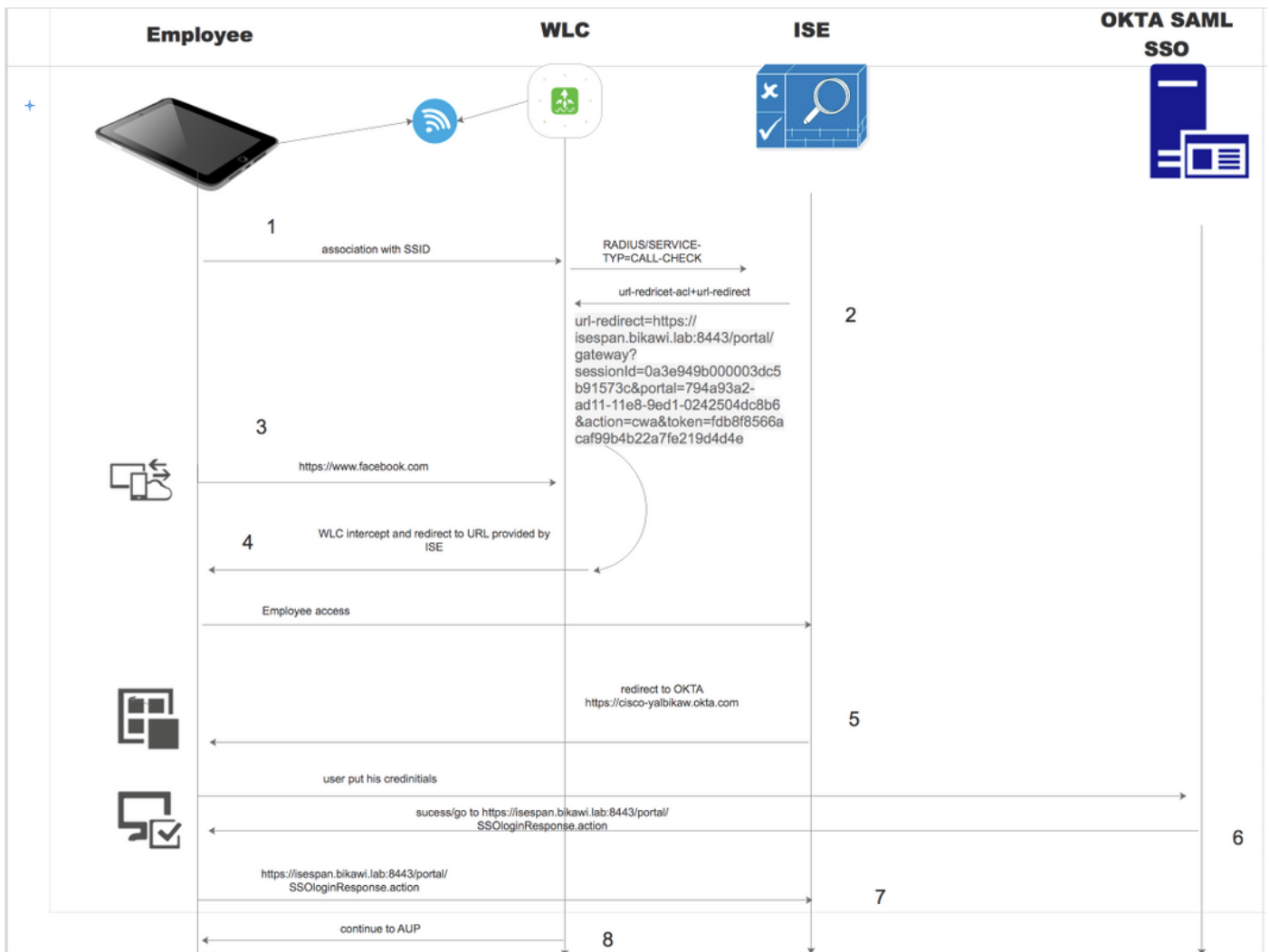
SAML is een XML-gebaseerd kader dat het gebruik en de uitwisseling van SAML-beweringen op veilige wijze tussen zakelijke entiteiten beschrijft. De standaard beschrijft de syntaxis en de regels om deze beweringen aan te vragen, te maken, te gebruiken en te ruilen.

ISE gebruikt SP geïnitieerde modus. De gebruiker wordt naar het portal voor schoonmaken verwezen en ISE stuurt het naar IDP om het te bevestigen. Daarna gaat het terug naar ISE. Het verzoek wordt gevalideerd, en de gebruiker gaat, afhankelijk van de configuratie van de portal, verder met de toegang tot of het instappen van een gast.



SP-initiated

Netwerkstroom



1. De gebruiker sluit zich aan op SSID en de authenticatie is mac filteren (mab).
2. ISE antwoordt terug met toegang-accepteert dat eigenschappen Redirect-URL en Redirect-ACL bevat
3. Gebruiker probeert toegang te krijgen tot www.facebook.com.
4. WLC intercepteert het verzoek en stuurt de gebruiker terug naar het ISE gastportaal, de gebruiker klikt op de werknemerstoegang om het apparaat met SSO geloofsbriefen te registreren.
5. ISE wijst de gebruiker terug naar OKTA-toepassing voor authenticatie.
6. Na succesvolle authenticatie stuurt OKTA de SAML-aanmaningsreactie naar de browser.
7. browser geeft de aanname terug aan ISE.
8. ISE verifieert de assertiereactie en als de gebruiker correct geauthentiseerd is, gaat deze naar de AUP en dan met apparaatregistratie.

Controleer de onderstaande link voor meer informatie over SAML

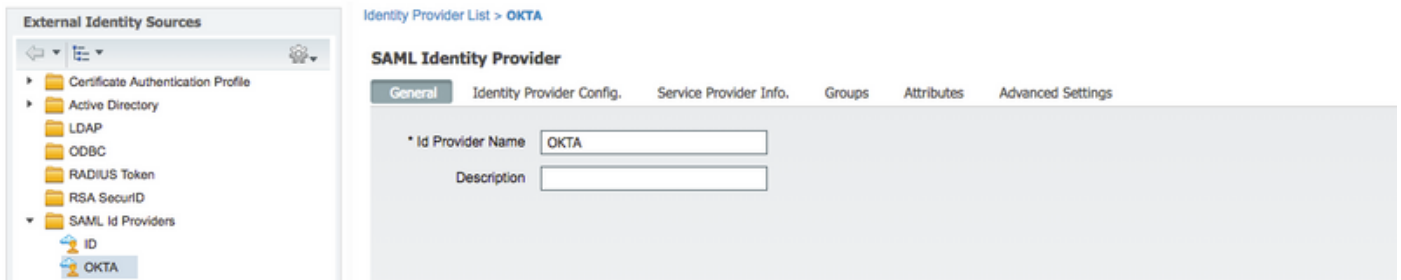
<https://developer.okta.com/standards/SAML/>

Configureren

Stap 1. Configureer de SAML Identity Provider en Guest portal op ISE.

1. Maak een externe identiteitsbron klaar.

Stap 1. Navigeer naar **Administratie > Externe Identiteitsbronnen > SAML ID Providers**.

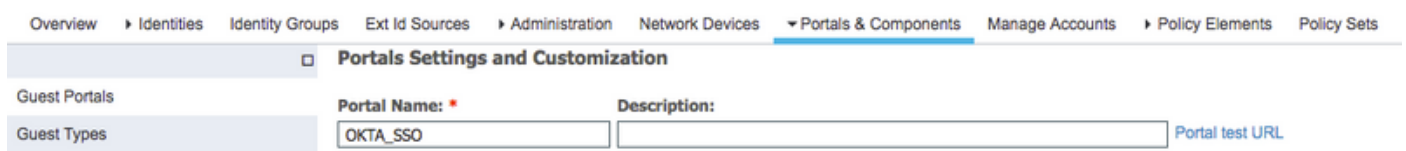
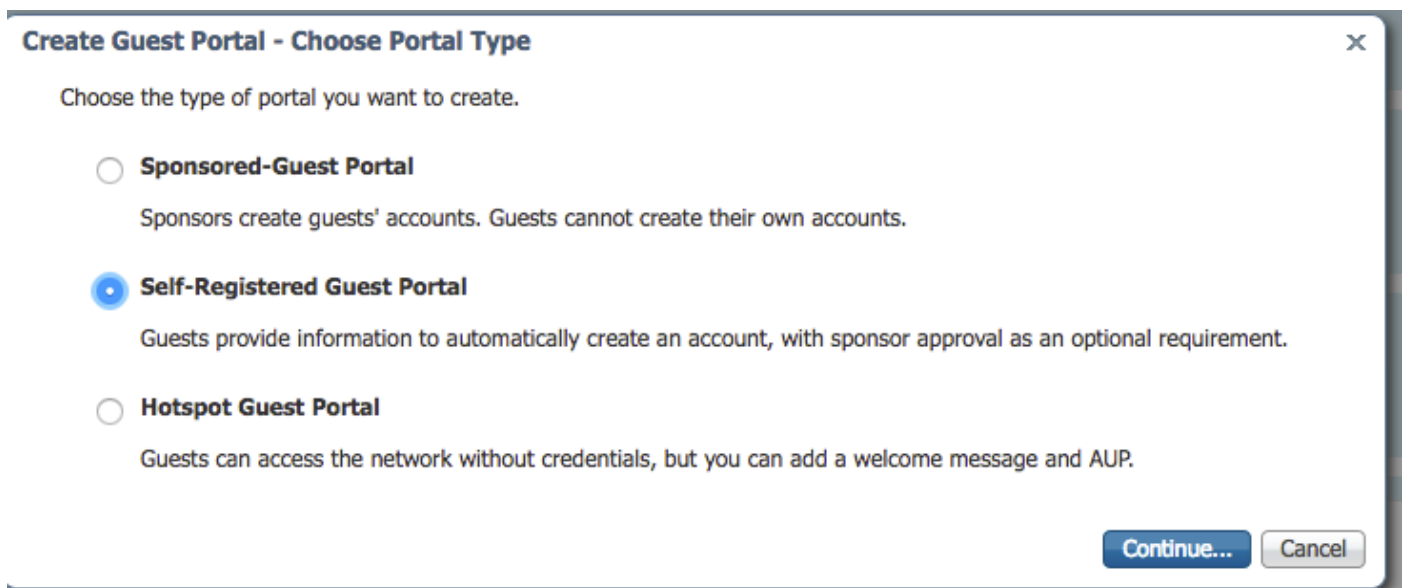


Stap 2. Wijs een naam aan de leverancier toe en breng de configuratie naar voren.

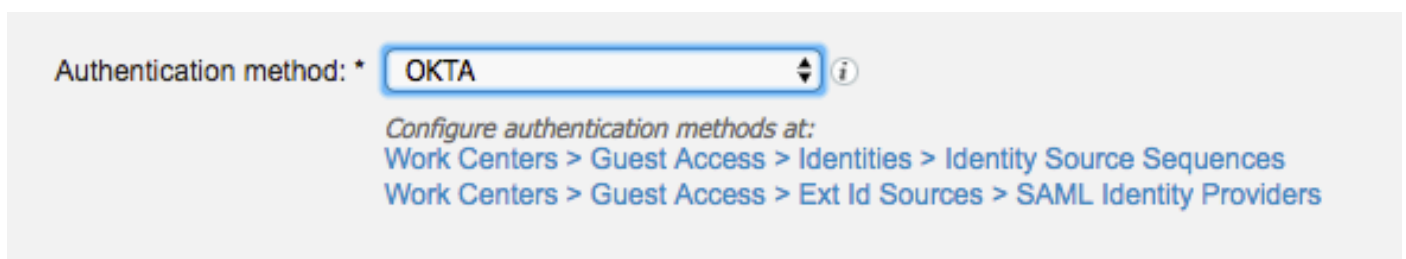
2. Maak een portal voor SSO.

Stap 1. Maak het portaal dat aan OKTA is toegewezen als identiteitsbron. Elke andere configuratie voor BYOD, apparaatregistratie, Guest, enz. is precies hetzelfde als voor een normaal portaal. In dit document wordt de portal in kaart gebracht bij de portal, omdat het een andere inlognaam is voor werknemer.

Stap 2. Navigeer naar **werkcentra > Toegang voor gasten > Portals & Componenten** en maak het portal aan.



Stap 3. Kies de authenticatiemethode om naar de eerder geconfigureerde Identity Provider te wijzen.

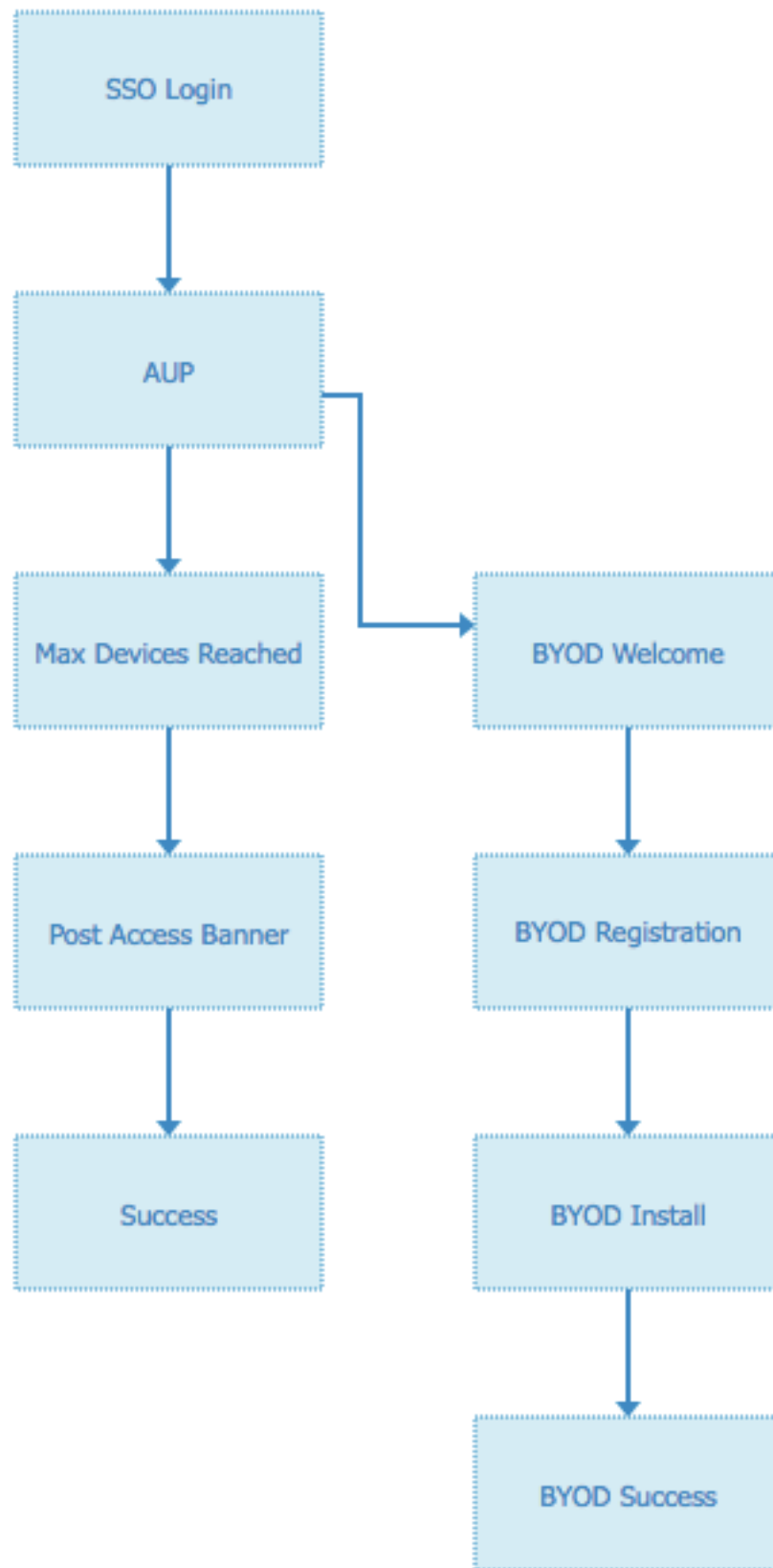


Stap 4. Kies de OKTA-bron als een authenticatiemethode.

(optioneel) kies de BYOD-instellingen.

The screenshot shows the 'BYOD Settings' configuration page. At the top, there is a header 'BYOD Settings' with a dropdown arrow. Below this, the first option is 'Allow employees to use personal devices on the network', which is checked with a blue square. Underneath this option, there is a label 'Endpoint identity group:' followed by a dropdown menu showing 'RegisteredDevices'. Below the dropdown, there are two lines of instructional text: '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'. The next two options are 'Allow employees to choose to guest access only' and 'Display Device ID field during registration', both of which are unchecked. Below these, there is another line of instructional text: 'Configure employee registered devices at Work Centers > BYOD > Settings > Employee Registered Devices'. The final section is 'After successful device configuration take employee to:', which has three radio button options: 'Originating URL' (with an information icon), 'Success page' (which is selected), and 'URL:' followed by an empty text input field.

Stap 5. Save the portal Configuration, met BYOD ziet de stroom er als volgt uit:



3. Alternatieve aanmelding configureren

Opmerking: U kunt dit onderdeel overslaan als u de inlognaam voor alternatief niet gebruikt.

Navigeren in naar de selfregistration Guest Portal of een ander portal dat aangepast is voor

gastentoeegang.

Als u een loginpagina-instellingen wilt toevoegen, kunt u ook een andere inlogportal toevoegen: 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

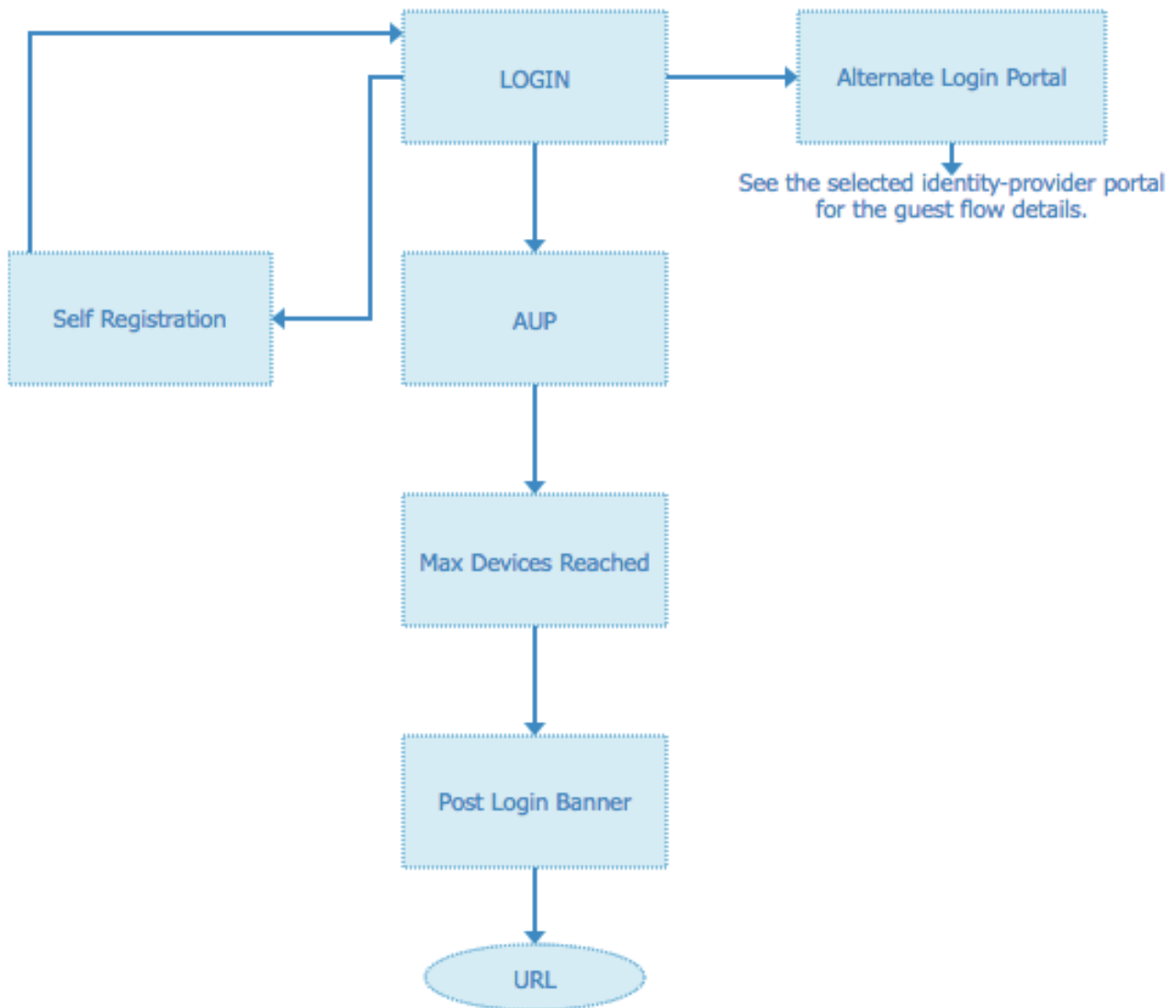
Allow guests to create their own accounts

Allow social login

Allow guests to change password after login ⓘ

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

Dit is nu de poortstroom.



Stap 2. Configuratie van OKTA-toepassing en van SAML-identiteitsproviders.

1. Maak OKTA-toepassing.

Stap 1. Meld u aan bij de OKTA-website met een beheeraccount.

← 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

Step 2. Klik op Add Application.

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

Step 3. Maak een nieuwe app, kies deze om SAML2.0 te zijn

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

Algemene instellingen

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

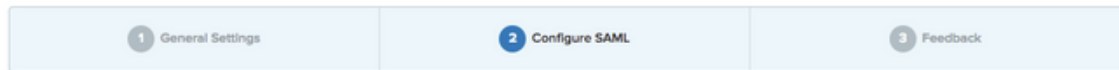


Do not display application icon in the Okta Mobile app

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](#)

Stap 4. Download het certificaat en installeer het in ISE Trusted Certificates.

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. ExportSP-informatie van SAML Identity Provider.

Navigeer naar de eerder gevormde Identity Provider. Klik op **Service Provider Info** en voer deze uit, zoals in de afbeelding.

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

De geëxporteerde zip-map bevat XML-bestand en **readme.txt**

```

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
ActiveRequestsSigned="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/
Export10KQZLz2NwYw4YelrY0pLxshjAeFv8y00AMdYNTeYNTBaPw8OTA4NDYdNTEyNTBa
MCDXIDe8gNvBMTFFINBTUxfaw1c3hb151amhd2kubGFJHTIBIjANBqkqhkiG9w0BAQ0FAAOC
AQ8AMITBCKCAQEAuxUM49zQVf51hGzphUFUK7Bbo4mf890E1o21amdh8n09FwDzuHf8rLX7W
tsFfv0Zb1cWEnAFPTfabxu3ooXLTJHTKofmzF8GwCE7od2PfCyycoEJcncu1Bh/mfe980s
vL+1Z/Pq7oTrupYe/XZLHdyIhoy2xuE8sMomeYvB85w5DZVgJL+nPur7j1e+31j3toJdc9k+c1
mx26X49RtBqR3jehFoxL+PMCS8buLU0J0sJdInqMvV54jnzR9Mc9WspQxdIR03wxsEJzBpZ
7X5s+2M/s1p1IapIjrmtdo3K6h0Z2FT8T8BLDtp0B3R8K9wIDMqA8o2w4dV8y8YH9E
BTADQh/MASGA11dWQEAWLCTDAdBvWQHEFg0L8pFk4enoxGf+3/p8LaoZ9h3h4WdYV8L
BBYvAYIXWY8BQKAwEGCCsGAQJFBNwCHBEGOMCGSAGG+EIBA00EAUIG00ANBqkqhkiG9w0BAQ0F
AAOCQAQEAHxj5UgZpPozdWkkjDxzMoj1u9s9EvOKSyzGFQ4vuf1q4rh293KevYVR84w7E+HM
QSNvEPRI1Vg0MDLKKfddAyRtUy8ALBy64dpjt1KZcRfZ1Bkhlez0PkVYK6R4d01PnH+53pbYK9hx
D1Reu6LYo6prZI9MqsAwax1THh+5v6h0Po79okhhSHdsZM6FJHFwTYh0mDkaIGC4PxA2CF1KL9
GBYj8pJmP3YMBU/zloy0/pX+gVU07nHed02Z0ty4o2eupYwBzFr88pE2g3zhf9THfJgFJ00Op
PALpV38FAIGqbXbCeoAMULPEKID7q1xstD05LIHQ1e==</ds:KeyInfo?></md:KeyDescriptor><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient?></md:NameIDFormat><md:
NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress?></md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent?></md:NameIDFormat><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:WindowsDomainQualifiedName?></md:NameIDFormat><md:NameIDFormat
urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos?></md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName?></md:NameIDFormat><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.48.35.19:8443/portal/SSOLoginResponse.action" index="0"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.48.17.71:8443/portal/SSOLoginResponse.action" index="1"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action" index="2"/><md:AssertionConsumerService Binding="
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action" index="3"/></md:SPSSODescriptor></md:EntityDescriptor>
    
```

Voor sommige aanbieders van Identiteiten kun je XML direct importeren, maar in dit geval moet het handmatig importeren.

- Enkelvoudige aanmelding URL (kleine bewering)

```

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"
    
```

- ID SP-entiteit

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

De SSO-URL is beschikbaar in ip-adres en FQDN-indeling.

Voorzichtig: De selectie van de bestandsindeling is afhankelijk van de instellingen voor het doorsturen van een autorisatieprofiel. Als u statische ip gebruikt, moet u het IP-adres voor de SSO-URL gebruiken.

3. Instellingen OKTA SAML.

Stap 1. Voeg deze URL's toe op SAML-instellingen.

A SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Requestable SSO URLs

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

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

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

Stap 2. U kunt meer dan één URL van het XML bestand toevoegen, gebaseerd op het aantal PSN's dat deze service ontvangt. Naam en gebruikersnaam zijn afhankelijk van uw ontwerp.

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>
```

Stap 3. Klik op Volgende en kies de tweede optie.

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. metagegevens uit de toepassing exporteren.

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.

metagegevens:

```
<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>
MIIDrDCCApSgAwIBAgIGAWWP1TasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMmBQA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXl1hbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFg1pbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNVoXDTE4MDgzMTEwNDQwNVowZyZyXzAj
BgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEXMBUGA1UEAwwOY2l1zY28teWFsYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC1P7DvzVng7wSQWVOzGShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8u1Z8HUsOspBECLyCI75gH4rpc2FM4kzZiDbNLb95AW6d1Uztc66x42uhRYgduD5+w3/yvdwx
199upWb6SdrtnwK8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgYQO/7GRK2RzOj
bSZgeAp5YyytjA3Ncn9x6FMY5Rppc3HjtG4cjQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dn6YERuV5C5eHUXq3KGul2yI fiH7x8EartZ4/wGP/HYUCNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdtsz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQonRz7au0Uo9sInH6rWG+eOesysecPuWQtEqNqt+MyZn1CurJ0e+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>
```

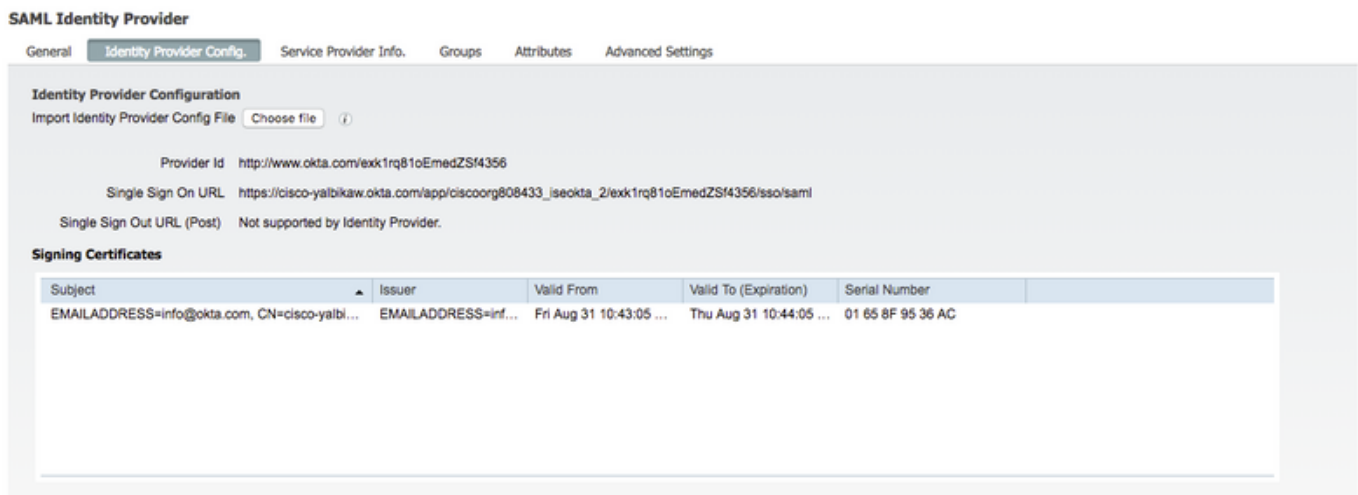
Sla het bestand in XML-indeling op.

5. Gebruikers aan de applicatie toewijzen.

Er is een manier om gebruikers aan deze toepassing toe te wijzen. De toepassing wordt uitgelegd in: [okta-actieve fabriek](#)

6. Metagegevens importeren van IP naar ISE.

Stap 1. Onder **SAML Identity Provider**, selecteer **Identity Provider Config.** en Importeer metagegevens.



SAML Identity Provider

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

Identity Provider Configuration

Import Identity Provider Config File (i)

Provider Id

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-yalbl...	EMAILADDRESS=inf...	Fri Aug 31 10:43:05 ...	Thu Aug 31 10:44:05 ...	01 65 8F 95 36 AC

Stap 2. Bewaar de configuratie.

Stap 3. CWA-configuratie.

Dit document beschrijft de configuratie voor ISE en WLC.

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

Voeg URLs in Redirect-ACL toe.

<https://cisco-yalbikaw.okta.com> / voeg uw toepassing-URL toe

<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.

Verifiëren

Test het portal en controleer of u de OKTA-toepassing kunt bereiken

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

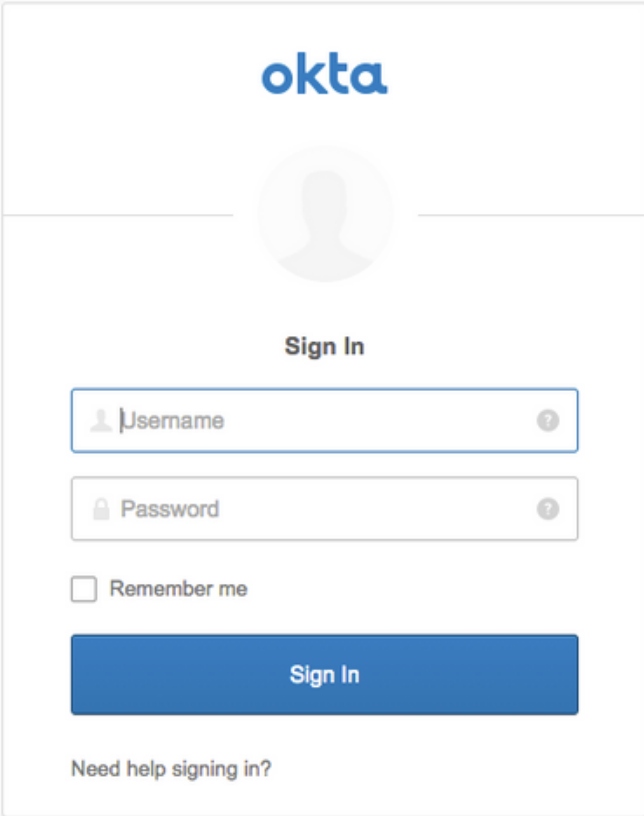
 **Portal Behavior and Flow Settings**
Use these settings to specify the guest experience for this portal.

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

Stap 1. Klik op de portal-test, dan moet u naar de SSO-toepassing worden teruggestuurd.

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 small 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?".

Stap 2. Controleer de **informatieverbinding op <toepassingsnaam>**

Stap 3. Als u de aanmeldingsgegevens invoert die u een slecht verzoek ziet, betekent dit niet noodzakelijkerwijs dat de configuratie op dit punt fout is.

Verificatie van eindgebruikers

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

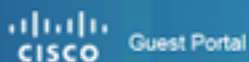
[Need help signing in?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



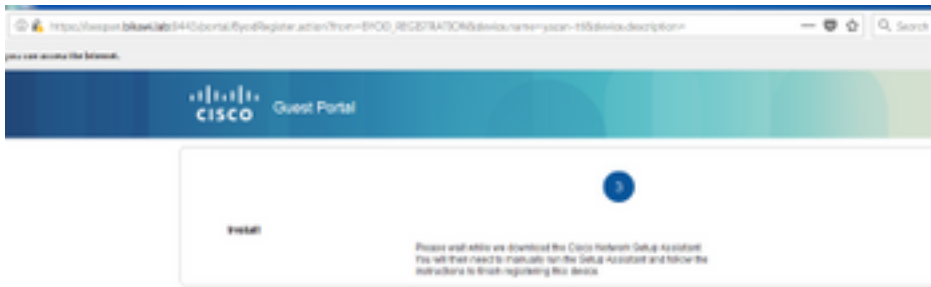
Acceptable Use Policy

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-verificatie

Controleer het levensbestand om de authenticatiestatus te controleren.

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

Problemen oplossen

OKTA-probleemoplossing

Stap 1. Controleer de logbestanden in het tabblad **Rapporten**.

ISE-probleemoplossing

Er zijn twee logbestanden om te controleren

- ise-psc.log
- gastarts

Navigeer naar **Administratie > Systeem > Vastlegging > Logconfiguratie > Debug Log configuratie**. Schakel het niveau in op DEBUG.

SAML	ise-psc.log
Guestaccess	gastarts
Portal	gastarts

In de tabel wordt de component debug en het corresponderende logbestand weergegeven.

Gemeenschappelijke problemen en oplossingen

Scenario 1. Slecht verzoek van SAML.



400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

Deze fout is generiek, controleer de logbestanden om de stroom te controleren en specificeer de kwestie. Op ISE gaste.log:

ISE# toont loggingstoepassing voor.log | laatste 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:
```

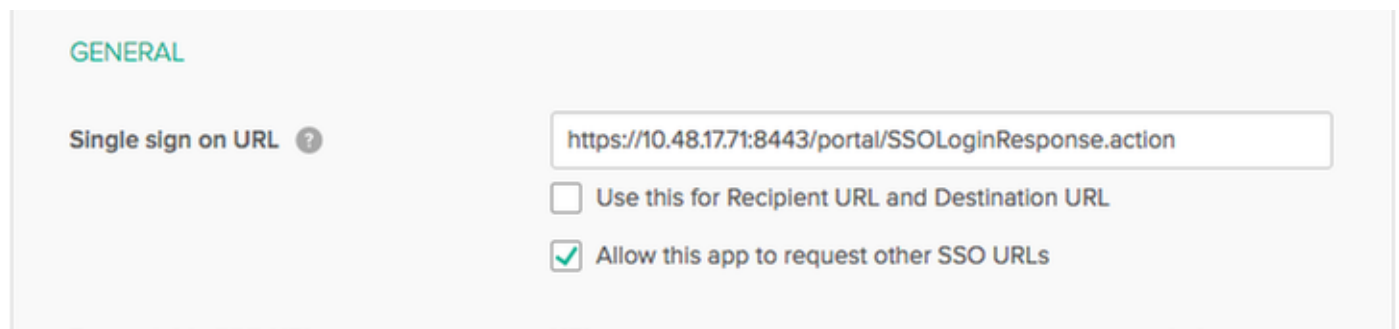
```
Portal Name: OKTA_SSO  
Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546  
Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
```


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/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoEuyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHhloiuQcIeJo1WVnFVI29qDGjrzGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElvECbfk6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fBlQnC
h3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%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_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%2Fn0NKi%2FZRoEuyPu95j9%2FzJ
OOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHhloiuQcIeJ
o1WVnFVI29qDGjrzGZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bizl1d%2Fv8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DECriw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElvECbfk6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1z
X6nmngdq3YIO37q9fBlQnCh3jf072v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWl
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

ISE heeft de gebruiker met succes omgeleid naar IDP. Er verschijnt echter geen reactie op ISE en het slechte SAML verzoek. Identificeer dat OKTA ons SAML-verzoek hieronder niet accepteert, is het verzoek.

```
https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDd3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BvYWK391X5TI%
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmngdq3YIO37q9fB1QnC
h3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n
8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERport
alId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-
940a-
b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_DELIMITERis espan.bikawi.lab
```

Controleer de aanvraag opnieuw en misschien zijn er wijzigingen aangebracht.



GENERAL

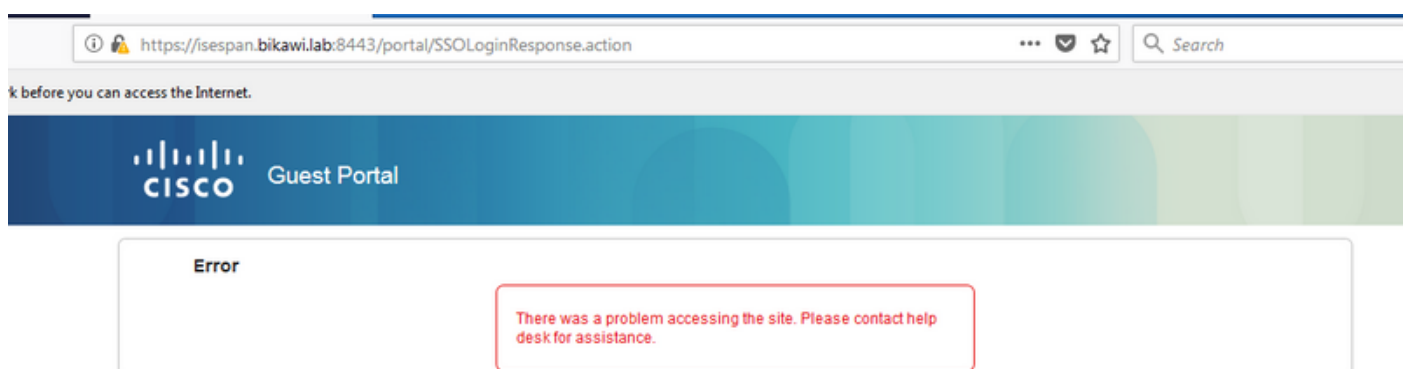
Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

De SSO-URL gebruikt IP-adres, echter, gast stuurt FQDN zoals we in het verzoek boven de laatste regel kunnen zien bevat SEMI_DELIMITER<FQDN> om dit probleem op te lossen en het IP-adres naar FQDN te veranderen op OKTA-instellingen.

Scenario 2. "Er was een probleem bij de toegang tot de site. Neem contact op met de helpdesk om hulp te bieden".



Guest.log

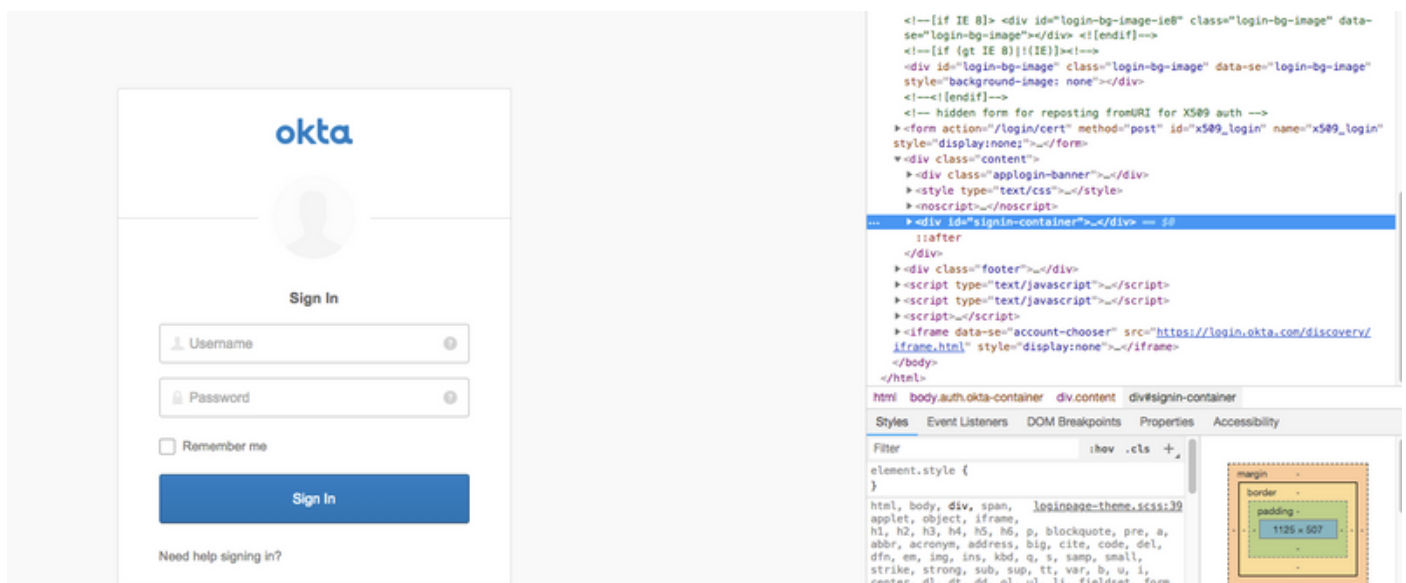
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::: SSO Authentication failed or
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
```

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

Op basis van de blogs meldt ISE dat de verklaring niet juist is. Controleer de OKTA-URI met het publiek of deze overeenkomt met de SP-status om deze op te lossen.

Scenario 3. Wanneer u opnieuw naar de pagina Blanken wijst, wordt de inlogoptie niet weergegeven.

Het hangt af van de omgeving en de poortconfiguratie. In dit soort probleem moet u de OKTA-toepassing controleren en welke URL er voor nodig is om te authenticeren. Klik op de portal test en controleer vervolgens elementen om te controleren welke websites bereikbaar moeten zijn.



In dit scenario zijn slechts twee URL's: toepassingen en inloggen.okta.com - deze moeten op de WLC zijn toegestaan.

Gerelateerde informatie

- <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>