

Konfigurieren des ISE 2.3-Gastportals mit OKTA SAML SSO

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Federated SSO](#)

[Netzwerkfluss](#)

[Konfigurieren](#)

[Schritt 1: Konfigurieren von SAML Identity Provider und Guest Portal auf der ISE](#)

[1. Erstellen einer externen Identitätsquelle.](#)

[2. Portal für SSO erstellen.](#)

[3. Konfigurieren der alternativen Anmeldung](#)

[Schritt 2: Konfigurieren der Einstellungen für die OKTA-Anwendung und den SAML Identity Provider](#)

[1. Erstellen einer OKTA-Anwendung.](#)

[2. Exportieren von SP-Informationen vom SAML Identity Provider.](#)

[3. OKTA SAML-Einstellungen.](#)

[4. Exportieren von Metadaten aus der Anwendung.](#)

[5. Weisen Sie der Anwendung Benutzer zu.](#)

[6. Importieren von Metadaten aus IP in ISE](#)

[Schritt 3.CWA-Konfiguration.](#)

[Überprüfen](#)

[Endbenutzerverifizierung](#)

[ISE-Verifizierung](#)

[Fehlerbehebung](#)

[OKTA-Fehlerbehebung](#)

[ISE-Fehlerbehebung](#)

[Häufige Probleme und Lösungen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Identity Services Engine (ISE) in OKTA integriert wird, um eine Single Sign-On (SAML SSO)-Authentifizierung (Security Assertion Markup Language Single Sign-On) für das Gastportal bereitzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Gastservices der Cisco Identity Services Engine.
- SAML SSO.
- (optional) Konfiguration des Wireless LAN Controllers (WLC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Identity Services Engine 2.3.0.298
- OKTA SAML SSO-Anwendung
- Cisco 5500 Wireless Controller Version 8.3.141.0
- Windows 7

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Federated SSO

Ein Benutzer innerhalb der Organisation kann sich einmalig authentifizieren und dann auf mehrere Ressourcen zugreifen. Diese Identität, die unternehmensübergreifend verwendet wird, wird als "föderierte Identität" bezeichnet.

Das Verbundkonzept:

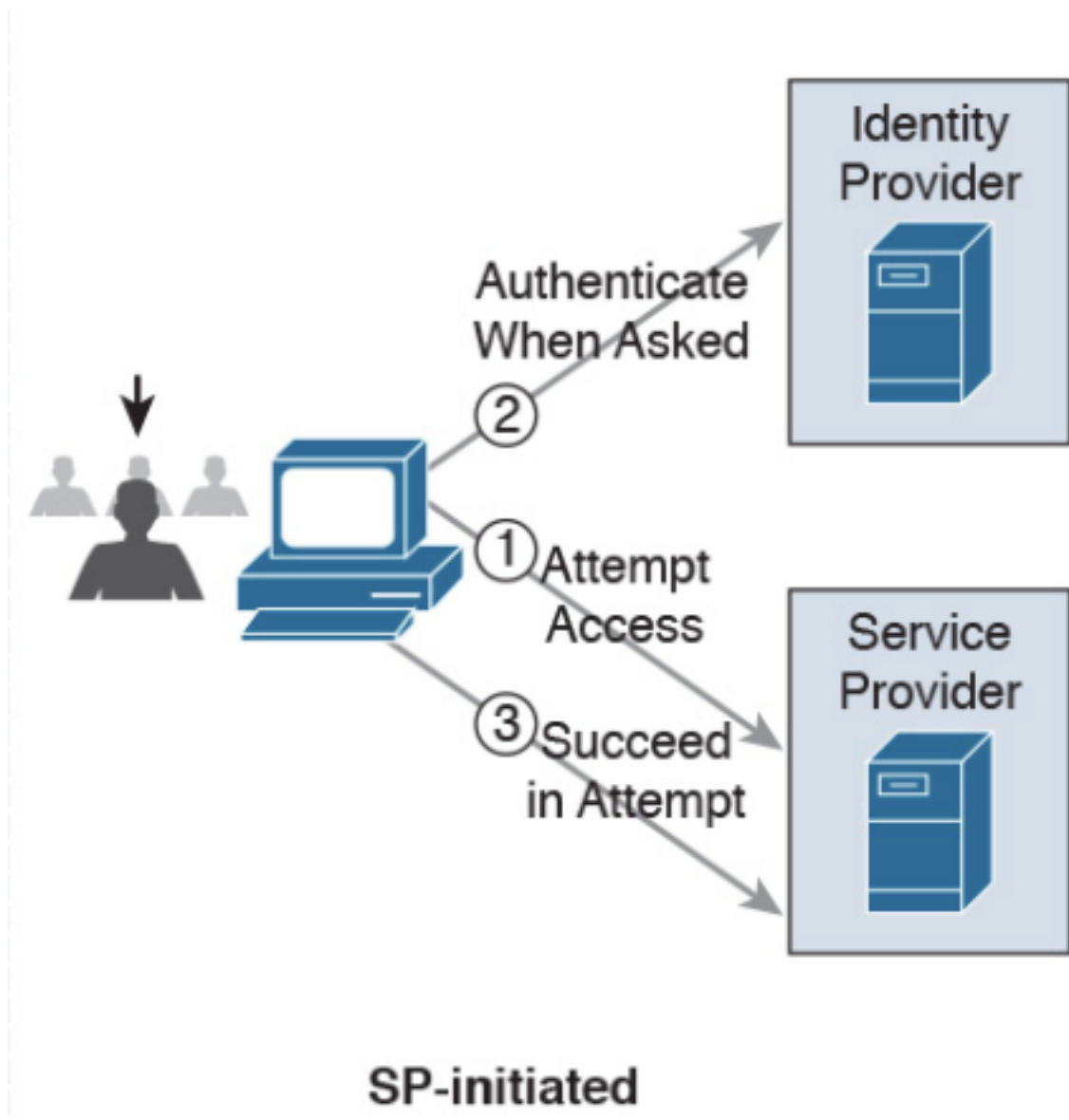
- Grundsatz: Endbenutzer (der einen Service anfordert), in diesem Fall Webbrowser, ist das Endgerät.
- Service Provider: manchmal auch als Relying Party (RP) bezeichnet, d. h. das System, das einen Service bereitstellt, in diesem Fall ISE.
- Identitätsanbieter (IdP): , das die Authentifizierungs-, Autorisierungsergebnisse und Attribute verwaltet, die an SP, in diesem Fall OKTA, zurückgesendet werden.
- Assertion: die Benutzerinformationen, die von IdP an SP gesendet wurden.

Mehrere Protokolle implementieren SSO, z. B. OAuth2 und OpenID. Die ISE verwendet SAML.

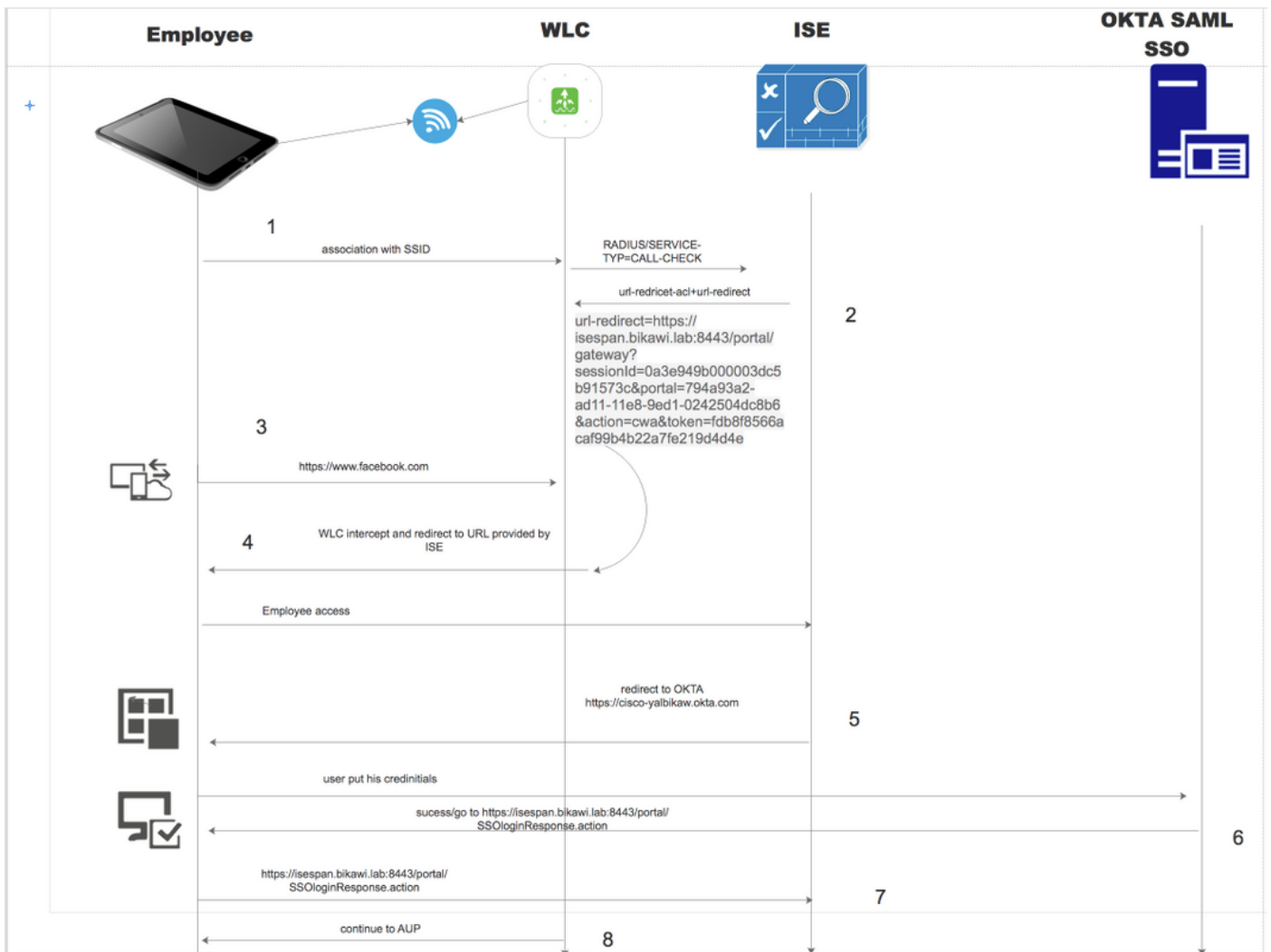
SAML ist ein XML-basiertes Framework, das die sichere Verwendung und den sicheren Austausch von SAML-Assertionen zwischen Geschäftseinheiten beschreibt. Der Standard beschreibt die Syntax und die Regeln, um diese Assertionen anzufordern, zu erstellen, zu verwenden und auszutauschen.

Die ISE verwendet den SP-initiierten Modus. Der Benutzer wird zum Gastportal umgeleitet, und die ISE leitet ihn zur Authentifizierung an IDP weiter. Danach wird wieder zur ISE umgeleitet. Die Anfrage wird validiert, und der Benutzer erhält je nach Portalkonfiguration Gastzugriff oder

Onboarding.



Netzwerkfluss



1. Der Benutzer stellt eine Verbindung mit der SSID her, und die Authentifizierung ist MAC-Filterung (MAB).
2. Die ISE antwortet mit Access-Accept, das die Attribute Redirect-URL und Redirect-ACL enthält.
3. Benutzer versucht, auf www.facebook.com zuzugreifen.
4. WLC fängt die Anforderung ab und leitet den Benutzer zum ISE-Gastportal weiter. Der Benutzer klickt auf den Mitarbeiterzugriff, um das Gerät mit SSO-Anmeldeinformationen zu registrieren.
5. Die ISE leitet den Benutzer zur Authentifizierung an die OKTA-Anwendung weiter.
6. Nach erfolgreicher Authentifizierung sendet OKTA die SAML Assertion-Antwort an den Browser.
7. Browser leitet die Assertion zurück zur ISE.
8. Die ISE überprüft die Assertionsantwort, und wenn der Benutzer ordnungsgemäß authentifiziert wurde, geht er zum AUP und dann bei der Geräteregistrierung über.

Über den unten stehenden Link erhalten Sie weitere Informationen zu SAML.

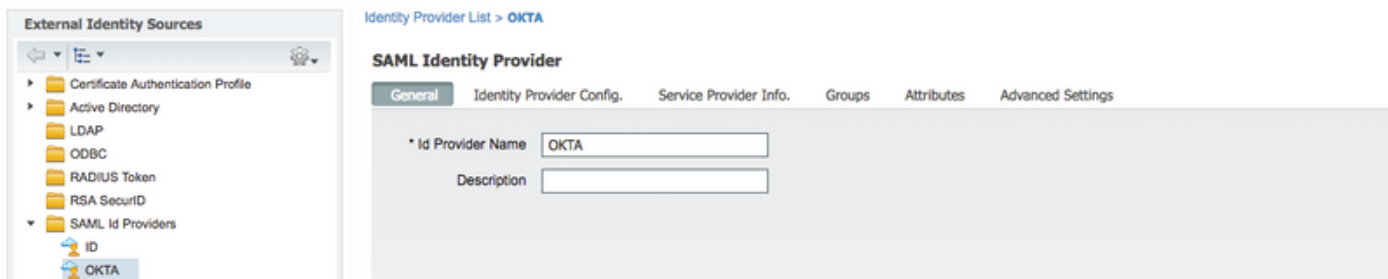
<https://developer.okta.com/standards/SAML/>

Konfigurieren

Schritt 1: Konfigurieren von SAML Identity Provider und Guest Portal auf der ISE

1. Erstellen einer externen Identitätsquelle.

Schritt 1: Navigieren Sie zu **Administration > External Identity Sources > SAML id Providers**.

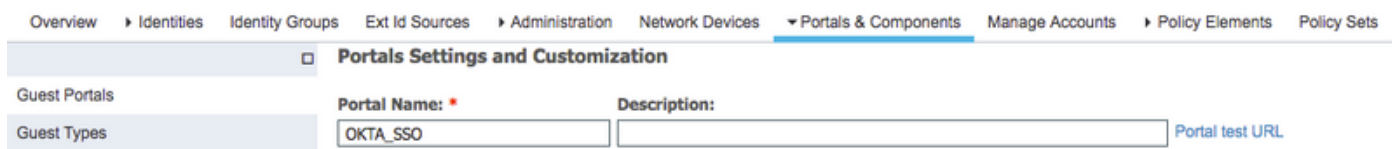
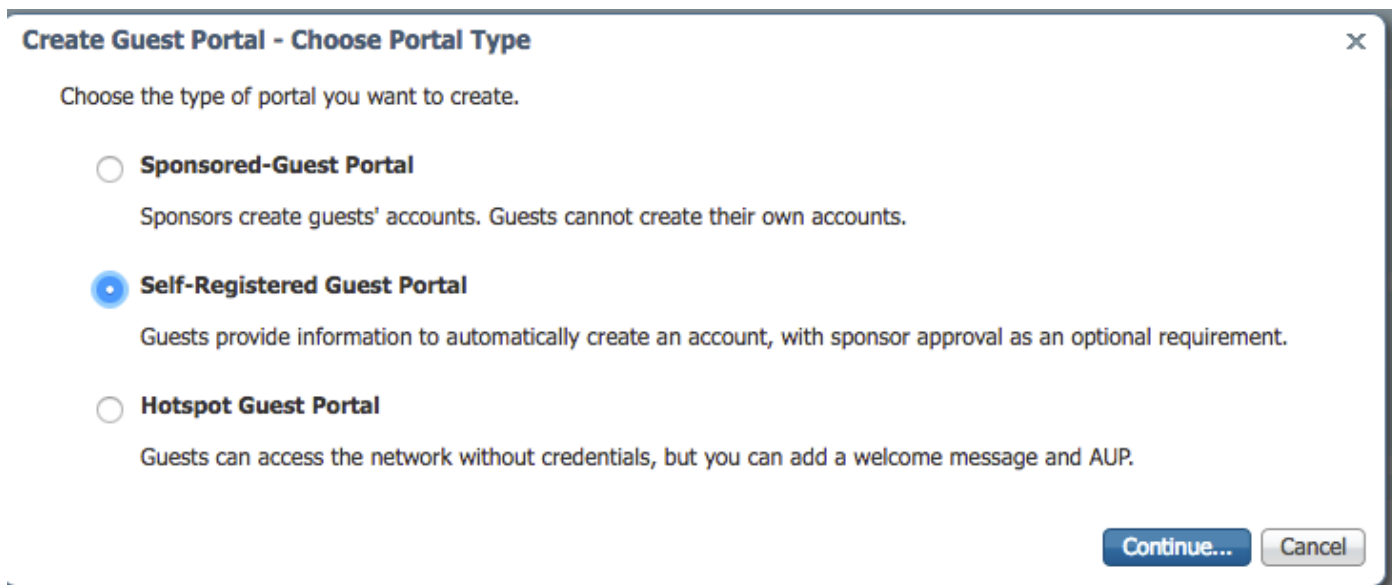


Schritt 2: Weisen Sie dem ID-Anbieter einen Namen zu, und senden Sie die Konfiguration.

2. Portal für SSO erstellen.

Schritt 1: Erstellen Sie das Portal, das der OKTA als Identitätsquelle zugewiesen ist. Alle anderen Konfigurationen für BYOD, Geräteregistrierung, Gast usw. entsprechen exakt den Einstellungen für das normale Portal. In diesem Dokument wird das Portal dem Gastportal als alternative Anmeldung für Mitarbeiter zugeordnet.

Schritt 2: Navigieren Sie zu **Work Center > Guest Access > Portals & Components (Arbeitscenter > Gastzugriff > Portale & Komponenten)**, und erstellen Sie das Portal.



Schritt 3: Wählen Sie die Authentifizierungsmethode aus, um auf den zuvor konfigurierten Identitätsanbieter zu verweisen.

Authentication method: * **OKTA** ⓘ

Configure authentication methods at:
[Work Centers > Guest Access > Identities > Identity Source Sequences](#)
[Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers](#)

Schritt 4: Wählen Sie OKTA-Identitätsquelle als Authentifizierungsmethode aus.

(Optional) Wählen Sie die BYOD-Einstellungen aus.

▼ **BYOD Settings**

Allow employees to use personal devices on the network

Endpoint identity group: **RegisteredDevices**

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](#)

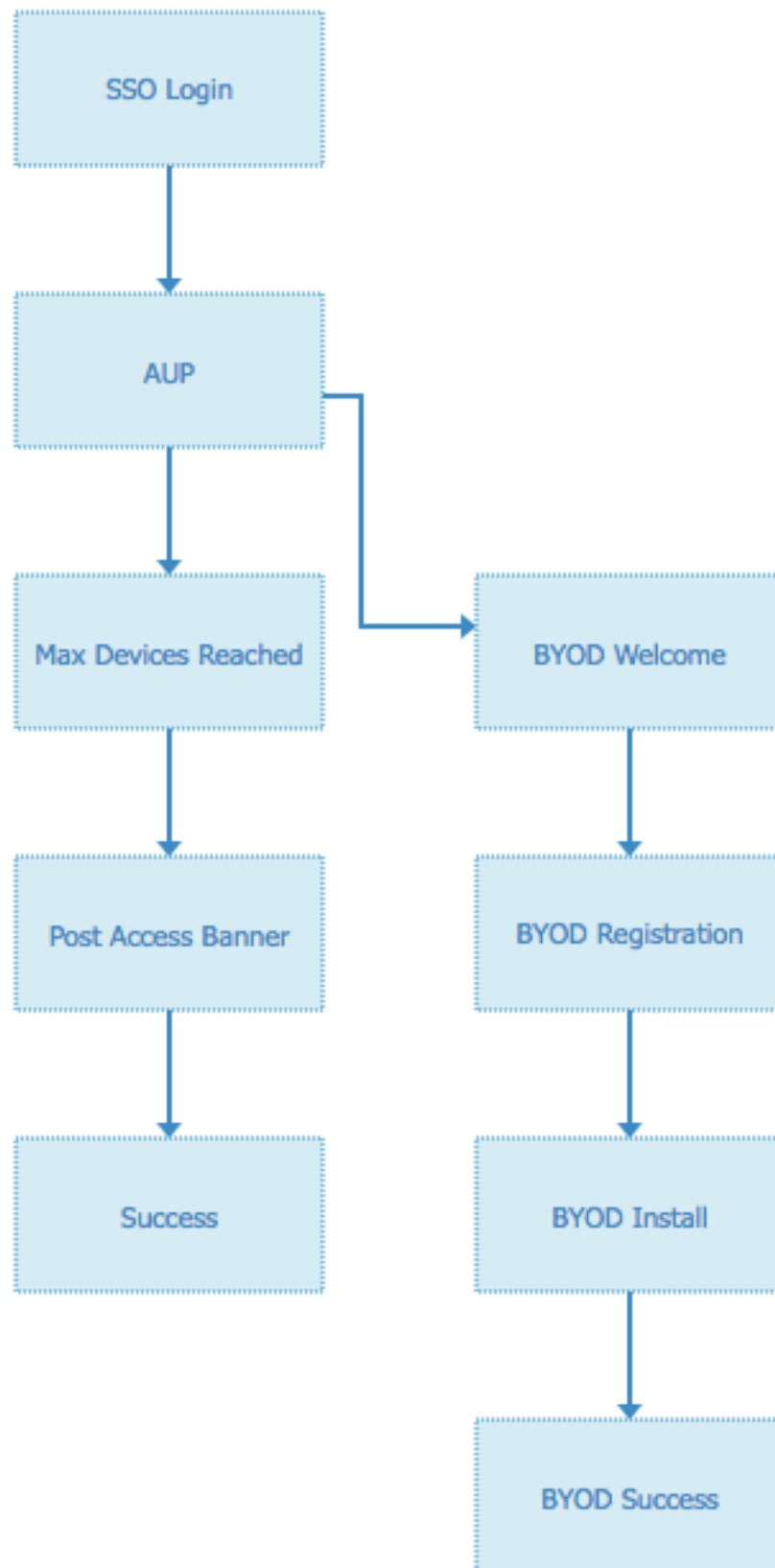
After successful device configuration take employee to:

Originating URL ⓘ

Success page

URL:

Schritt 5: Speichern Sie die Portalkonfiguration. Bei BYOD sieht der Ablauf wie folgt aus:



3. Konfigurieren der alternativen Anmeldung

Hinweis: Sie können diesen Teil überspringen, wenn Sie nicht die alternative Anmeldung verwenden.

Navigieren Sie zum Portal für Gastbenutzer zur Selbstregistrierung oder zu einem anderen Portal, das für den Gastzugriff angepasst wurde.

Fügen Sie bei den Einstellungen der Anmeldeseite das alternative Anmeldeportal hinzu: 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

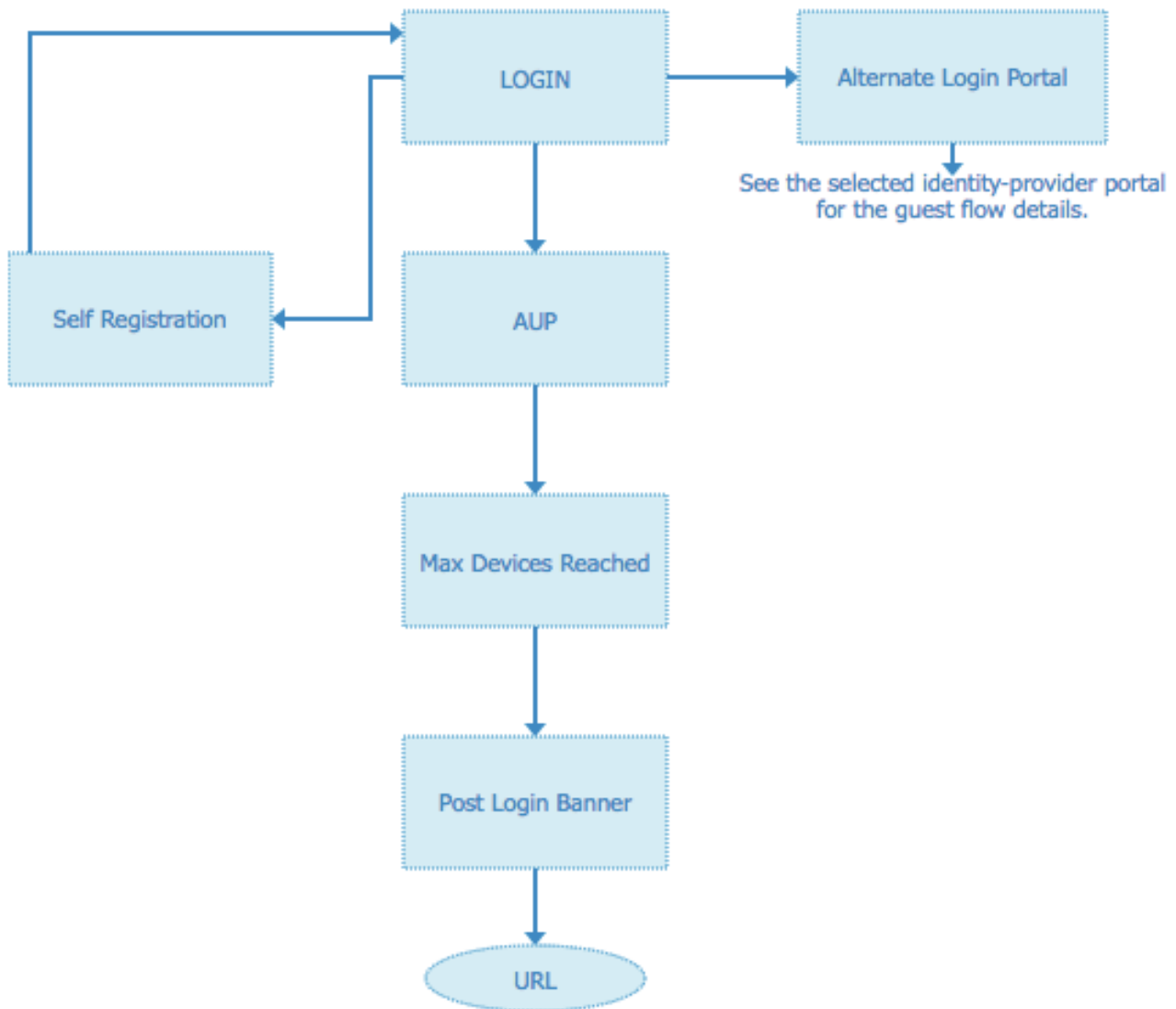
Allow guests to create their own accounts

Allow social login

Allow guests to change password after login ⓘ

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

Dies ist jetzt der Portalfluss.



Schritt 2: Konfigurieren der Einstellungen für die OKTA-Anwendung und den SAML Identity Provider

1. Erstellen einer OKTA-Anwendung.

Schritt 1: Melden Sie sich auf der OKTA-Website mit einem Administratorkonto an.

← 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

Schritt 2: Klicken Sie auf Anwendung hinzufügen.

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

Applications

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

STATUS	
ACTIVE	0
INACTIVE	3

01101110
01101111
01101100
01101000
01101101
01101110
01100111

No active apps found
Add application and assign access to have them appear on your users' Okta home Page

© 2018 Okta, Inc. [Privacy](#) [Version 2018.36](#) [US Cell 7](#) [Trust site](#) [Download Okta Plugin](#) [Feedback](#)

Schritt 3: Neue Anwendung erstellen, SAML2.0 auswählen

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

Allgemeine Einstellungen

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

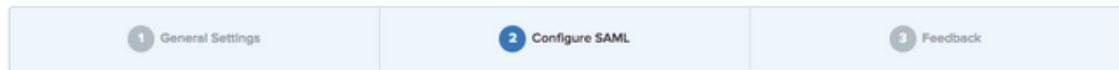


Do not display application icon in the Okta Mobile app

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](#)

Schritt 4: Laden Sie das Zertifikat herunter und installieren Sie es 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. Exportieren von SP-Informationen vom SAML Identity Provider.

Navigieren Sie zum zuvor konfigurierten Identitätsanbieter. Klicken Sie auf **Service Provider Info**, und exportieren Sie sie, wie im Bild gezeigt.

Schritt 1: Fügen Sie diese URLs in den SAML-Einstellungen hinzu.

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.bikawilab: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](#)

Schritt 2: Sie können mehr als eine URL aus der XML-Datei hinzufügen, abhängig von der Anzahl der PSNs, die diesen Dienst hosten. Das Namens-ID-Format und der Anwendungsbenutzername hängen vom Design ab.

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>
```

Schritt 3: Klicken Sie auf Weiter und wählen Sie die zweite Option aus.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

Is your app integration complete?

Yes, my app integration is ready for public use in the Okta Application Network

Previous
Finish

Why are you asking me this?

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

4. Exportieren von Metadaten aus der Anwendung.

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.

Metadaten:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exk1rq81oEmedZSf4356">
<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIDrDCCApSgAwIBAgIGAWWPlTasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFzAVBgNVBAMMDmNpc2NvLXl1hbGJpa2F3MRwwGgYJKoZIhvcN
AQkBFg1pbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNVoXDTE4MDgzMTEwNDQwNVowgZyxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEXMBUGA1UEAwwOY2l1zY28teWFsYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC1P7DvzVng7wSQWVOzGShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8u1Z8HUsOspBECLyCI75gH4rpc2FM4kzZiDbNLb95AW6d1Uztc66x42uhRYgduD5+w3/yvdwx
199upWb6Sdrtnk8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgYQO/7GRK2RzOj
bSZgeAp5YyytjA3Ncn9x6FMY5Rppc3HjtG4cjQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dn6YERuV5C5eHUXq3KGul2yI fiH7x8EartZ4/wGP/HYUCNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdTsz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesysecPuWQtEqNqt+MyZnlCurJ0e+JTvKYH1dSvapM1dzqoX
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>
```

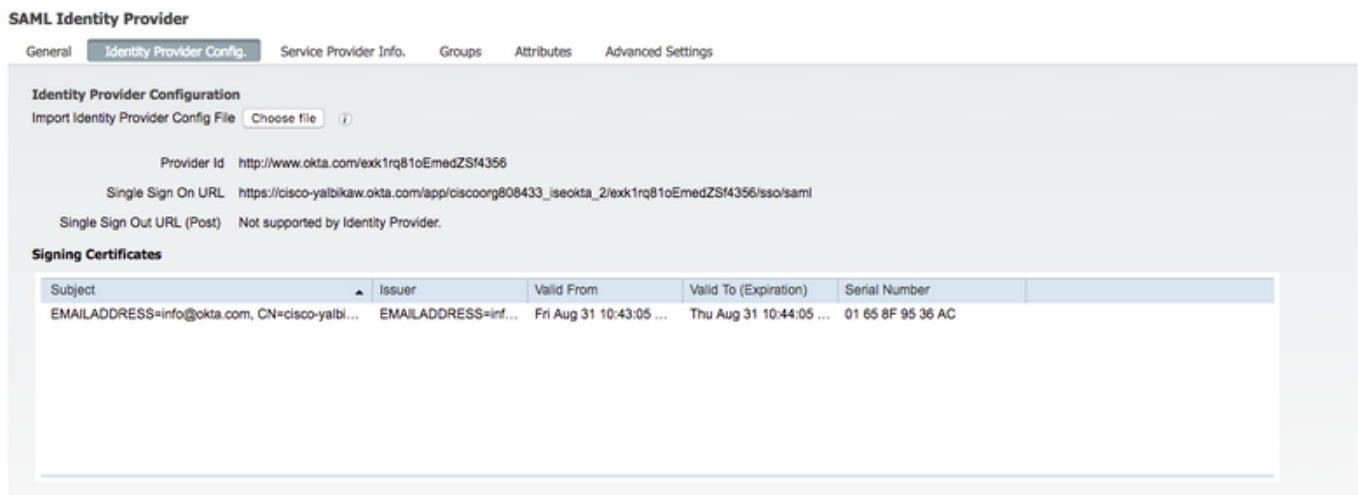
Speichern Sie die Datei im XML-Format.

5. Weisen Sie der Anwendung Benutzer zu.

Weisen Sie dieser Anwendung Benutzer zu, gibt es eine Möglichkeit für die AD-Integration, wie in beschrieben: [okta-aktives Verzeichnis](#)

6. Importieren von Metadaten aus IP in ISE

Schritt 1: Wählen Sie unter **SAML Identity Provider** die Option **Identity Provider Config** aus. und Metadaten importieren.



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

Schritt 2: Speichern Sie die Konfiguration.

Schritt 3. CWA-Konfiguration.

Dieses Dokument beschreibt die Konfiguration für ISE und WLC.

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

Fügen Sie URLs in der Umleitungsliste hinzu.

<https://cisco-yalbikaw.okta.com> / Anwendungs-URL hinzufügen

<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.

Überprüfen

Testen Sie das Portal, und überprüfen Sie, ob Sie die OKTA-Anwendung erreichen können.

Portal Name: *

Description:

OKTA_SSO

[Portal test URL](#)



Portal Behavior and Flow Settings

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



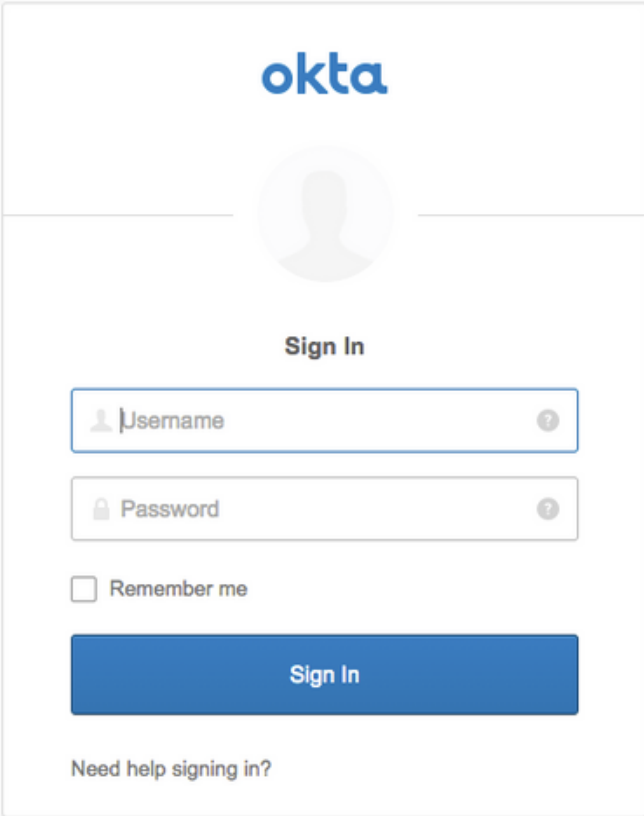
Portal Page Customization

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

Schritt 1: Klicken Sie auf den Portaltest, und Sie sollten zur SSO-Anwendung umgeleitet werden.

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 profile picture, the text "Sign In" is centered. There are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields have a small question mark icon on the right side. Below the password field 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?".

Schritt 2: Überprüfen Sie die **Informationsverbindung mit <Anwendungsname>**.

Schritt 3: Wenn Sie die Anmeldeinformationen eingeben, die Sie möglicherweise als ungültige Anfrage erhalten, bedeutet dies nicht notwendigerweise, dass die Konfiguration zu diesem Zeitpunkt falsch ist.

Endbenutzerverifizierung

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.



Guest Portal

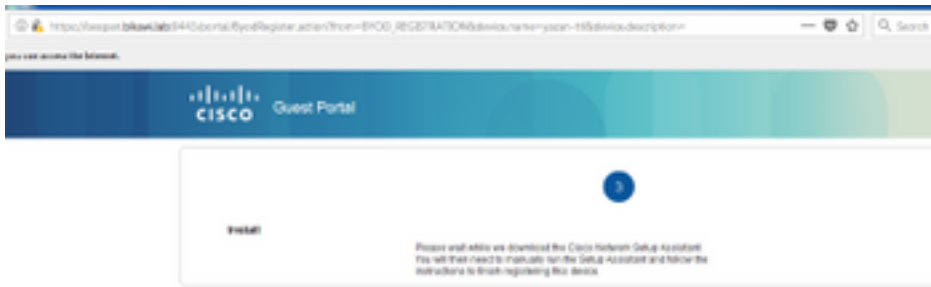
Acceptable Use Policy

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-Verifizierung

Überprüfen Sie die Lebenszyklusprotokolle, um den Authentifizierungsstatus zu überprüfen.

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

Fehlerbehebung

OKTA-Fehlerbehebung

Schritt 1: Überprüfen Sie die Registerkarte Protokolle in **Berichten**.

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

Schritt 2: Auch aus der Anwendungsansicht die zugehörigen Protokolle.

← 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)

Expand All

- Actor: OKTA-TEST@cisco.com OKTA (id: 00a218031c201f9356)
- Client: FIREFOX on Windows 7 Computer from [REDACTED]
- Event: successful user.authentication.sso (id: W1a2c01811Mh2noJGtDgAABQ)
- Request: ISE-OKTA (id: 0ea7e81b031c201f9356) AppInstance
- Target: OKTA-TEST@cisco.com OKTA (id: 0ea218031c201f9356) AppUser

ISE-Fehlerbehebung

Es müssen zwei Protokolldateien überprüft werden.

- ise-psc.log
- guest.log

Navigieren Sie zu **Administration > System > Logging > Debug Log Configuration**. Aktivieren Sie die Ebene zu DEBUG.

SAML	ise-psc.log
Gastzugriff	guest.log
Portal	guest.log

Die Tabelle zeigt die zu debuggende Komponente und die entsprechende Protokolldatei.

Häufige Probleme und Lösungen

Szenario 1. Ungültige SAML-Anforderung.

okta



400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

Dieser Fehler ist allgemein gehalten. Überprüfen Sie die Protokolle, um den Datenfluss zu überprüfen und das Problem zu identifizieren. Auf ISE guest.log:

ISE# show logging application guest.log | Letzte 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:
```

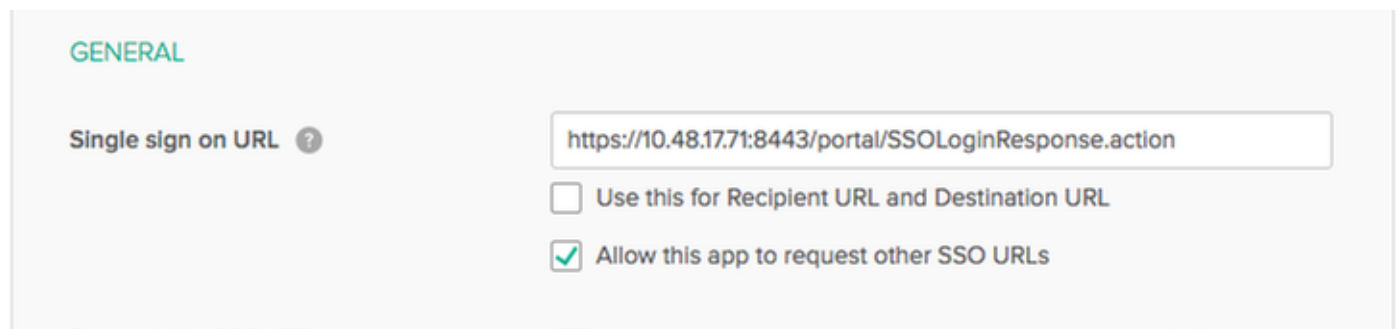
```
Portal Name: OKTA_SSO  
Portal ID: 9c969a72-b9cd-11e8-a542-d2e41bbdc546  
Portal URL: https://isespan.bikawi.lab:8443/portal/SSOLoginResponse.action
```


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%2Biz1ld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u
gJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIPtot64oM%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%2Biz1ld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJ13ugJmM%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DECriw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIP
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 hat den Benutzer erfolgreich an IDP umgeleitet. Es wird jedoch keine Antwort auf die ISE angezeigt, und die SAML-Anfrage ist fehlerhaft. Stellen Sie fest, dass OKTA unsere SAML-Anfrage unten nicht akzeptiert.

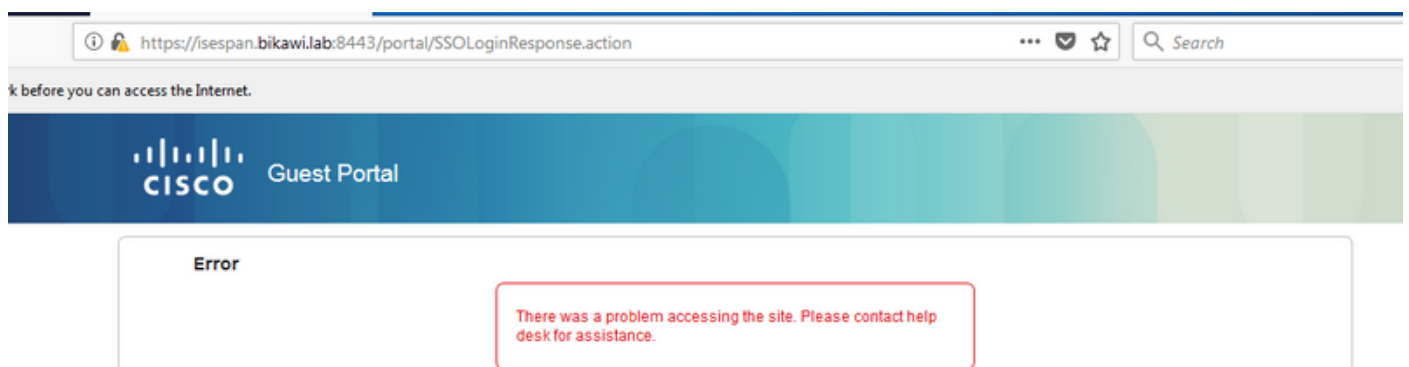
```
https://cisco-  
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHlhOiulyQcIeJo1WVnFVI29qDGjrjGZKmv0  
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0S1taB0Vxv1CPwo1hGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJ13u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTWSpuhEPdHPk79CJe4T6KQRElvECbfkdb6XdcnITsIPtot64oM%2BvYWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fB1QnC  
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
```

Überprüfen Sie jetzt noch einmal die Anwendung, ob Änderungen vorgenommen wurden.



Die SSO-URL verwendet die IP-Adresse. Der Gast sendet jedoch FQDN, wie in der Anfrage oben dargestellt, die letzte Zeile enthält SEMI_DELIMITER<FQDN>, um dieses Problem zu beheben. Ändern Sie die IP-Adresse in den OKTA-Einstellungen in FQDN.

Szenario 2. "Beim Zugriff auf die Website ist ein Problem aufgetreten. Bitte wenden Sie sich an den Helpdesk, um Hilfe zu erhalten."



Guest.log

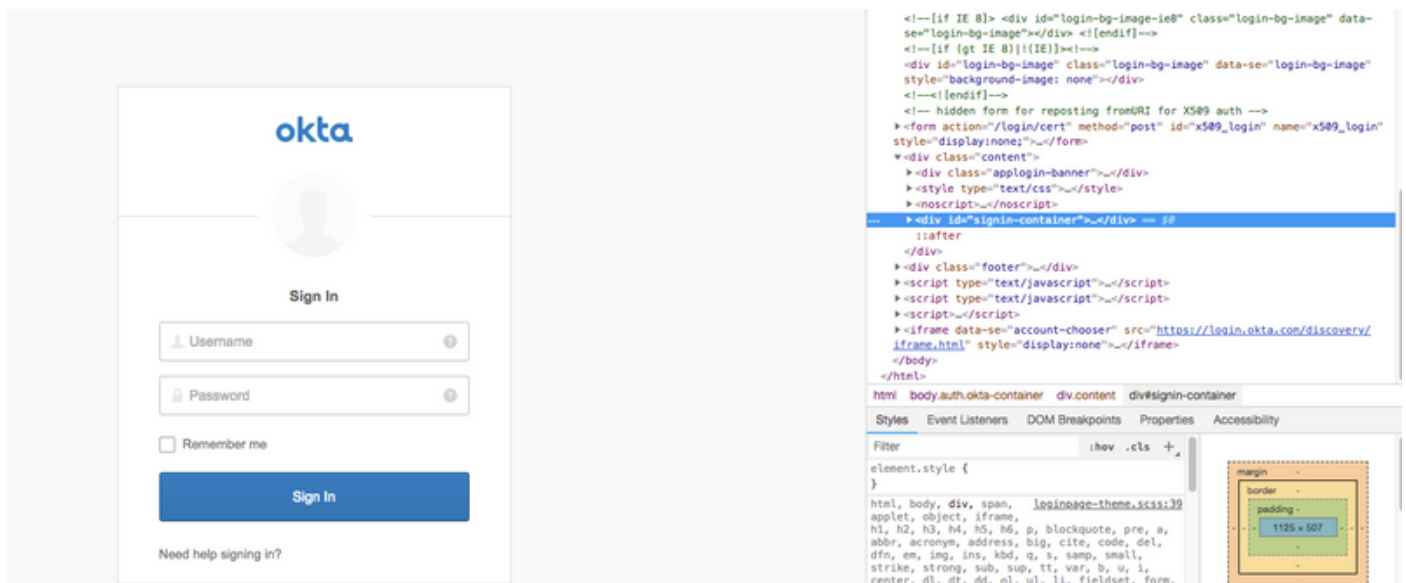
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][  
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::: SSO Authentication failed or  
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not
```

```
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
```

Aus den Protokollen meldet die ISE, dass die Assertion nicht korrekt ist. Überprüfen Sie den OKTA Audience URI, um sicherzustellen, dass er mit dem SP übereinstimmt, um ihn aufzulösen.

Szenario 3. Umgeleitet zur leeren Seite, oder die Anmeldungsoption wird nicht angezeigt.

Dies hängt von der Umgebung und der Portalkonfiguration ab. Bei diesem Problem müssen Sie die OKTA-Anwendung und die URLs überprüfen, die authentifiziert werden müssen. Klicken Sie auf den Portaltest, und überprüfen Sie dann das Element, welche Websites erreichbar sein müssen.



In diesem Szenario gibt es nur zwei URLs: application und login.okta.com - diese sollten auf dem WLC erlaubt sein.

Zugehörige Informationen

- <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>