

Configurazione del portale per gli utenti guest ISE 2.3 con OKTA SAML SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[SSO federato](#)

[Flusso di rete](#)

[Configurazione](#)

[Passaggio 1. Configurare SAML Identity Provider e Guest Portal su ISE.](#)

[1. Preparare l'origine dell'identità esterna.](#)

[2. Creare il portale per SSO.](#)

[3. Configurare l'accesso alternativo.](#)

[Passaggio 2. Configurare le impostazioni dell'applicazione OKTA e del provider di identità SAML.](#)

[1. Creare l'applicazione OKTA.](#)

[2. Esportare le informazioni SP dal provider di identità SAML.](#)

[3. Impostazioni OKTA SAML.](#)

[4. Esportare i metadati dall'applicazione.](#)

[5. Assegnare gli utenti all'applicazione.](#)

[6. Importare i metadati dall'Idp all'ISE.](#)

[Passaggio 3. Configurazione di CWA.](#)

[Verifica](#)

[Verifica utente finale](#)

[Verifica ISE](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi OKTA](#)

[Risoluzione dei problemi ISE](#)

[Problemi comuni e soluzioni](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come integrare Identity Services Engine (ISE) con OKTA per fornire l'autenticazione Single Sign-On (SAML SSO) Security Assertion Markup Language per il portale guest.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Servizi guest Cisco Identity Services Engine.
- SSO SAML.
- (facoltativo) configurazione del controller WLC (Wireless LAN Controller).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

SSO federato

Un utente all'interno dell'organizzazione può eseguire l'autenticazione una sola volta e quindi accedere a più risorse. Questa identità utilizzata nelle organizzazioni è detta identità federativa.

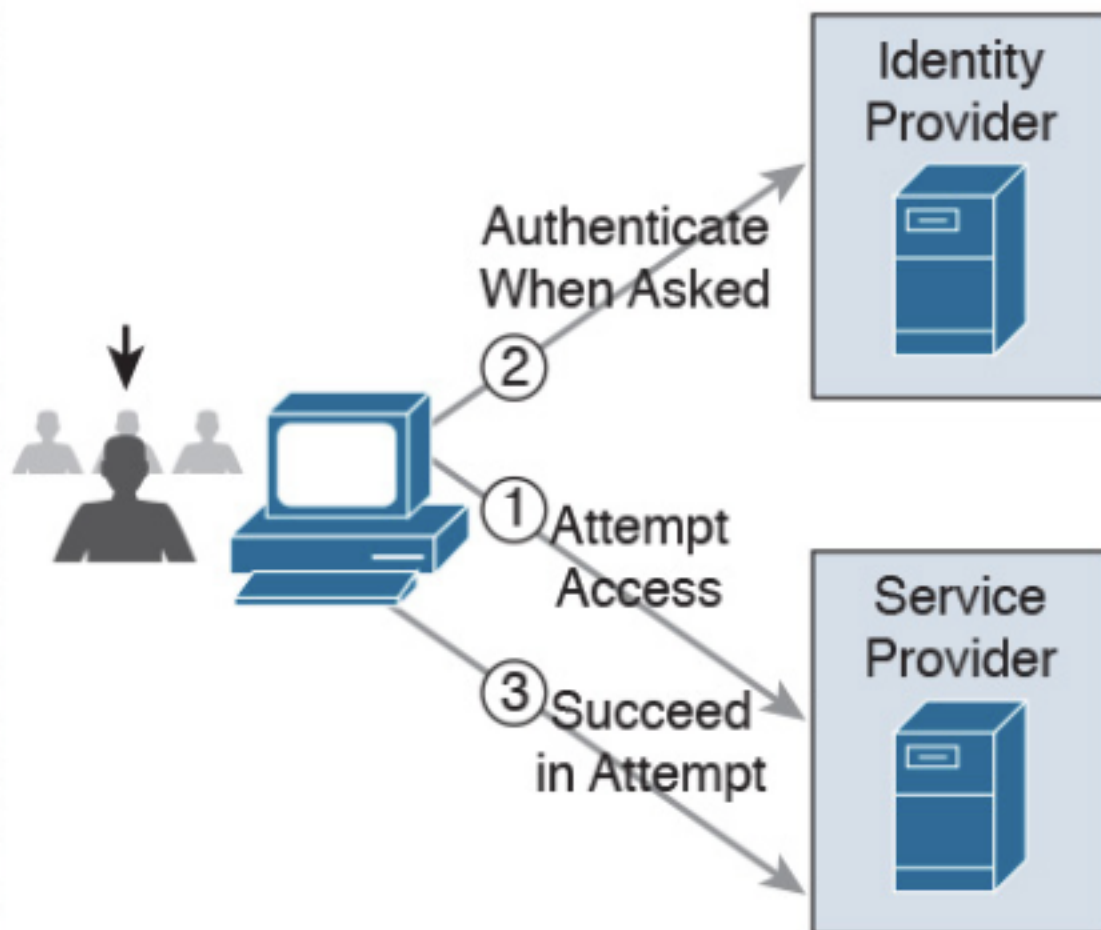
Il concetto di federazione:

- Principio: L'endpoint è rappresentato dall'utente finale (colui che richiede un servizio), in questo caso il browser Web.
- Provider di servizi (SP): chiamato anche relying party (RP), che è il sistema che fornisce un servizio, in questo caso ISE.
- Provider di identità (IdP): che gestisce l'autenticazione, il risultato dell'autorizzazione e gli attributi restituiti all'SP, in questo caso OKTA.
- Asserzione: le informazioni utente inviate da IdP a SP.

Diversi protocolli implementano SSO, ad esempio OAuth2 e OpenID. ISE utilizza SAML.

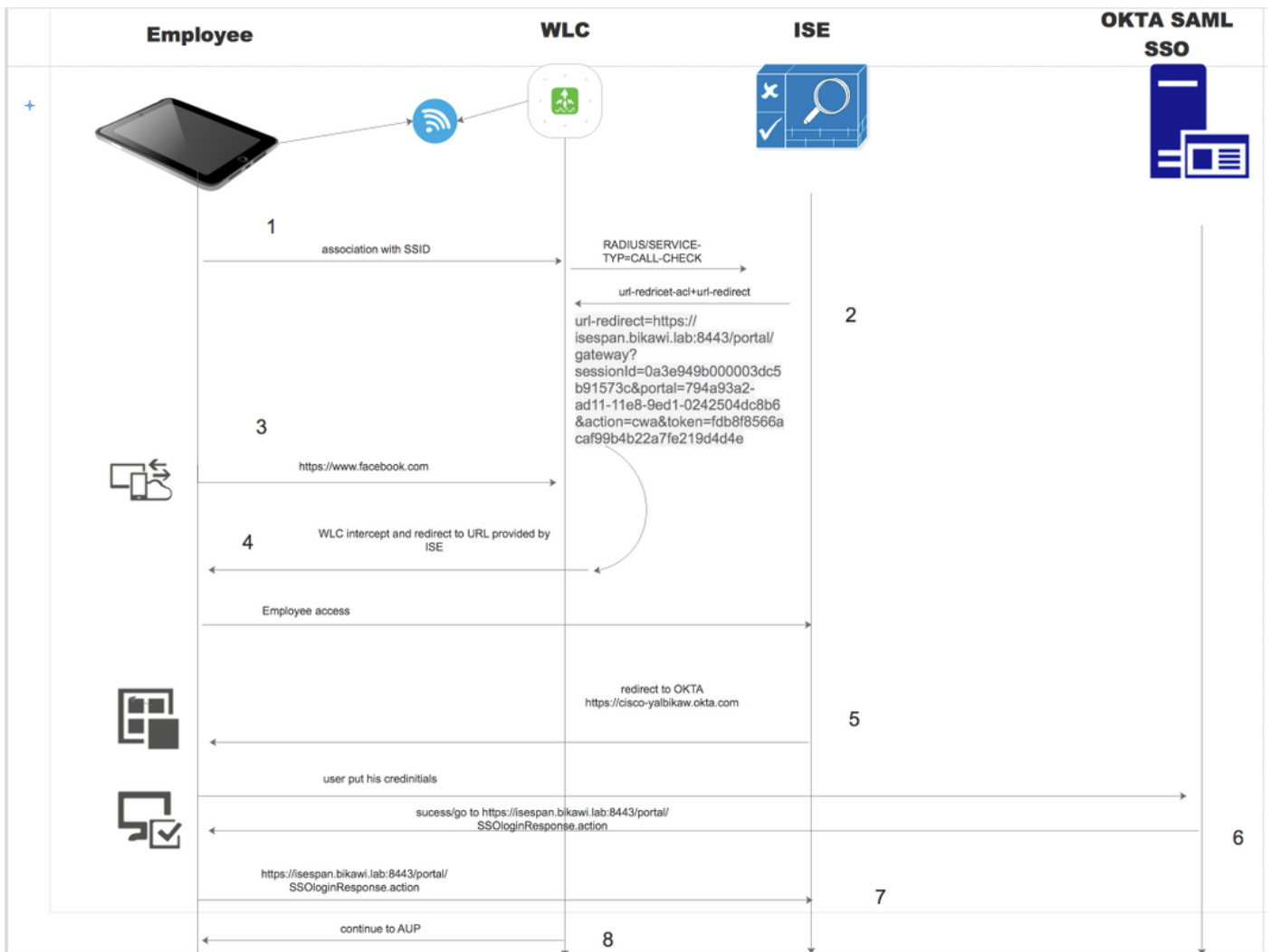
SAML è un framework basato su XML che descrive l'utilizzo e lo scambio di asserzioni SAML in modo sicuro tra entità aziendali. Lo standard descrive la sintassi e le regole per richiedere, creare, utilizzare e scambiare queste asserzioni.

ISE utilizza la modalità SP avviata. L'utente viene reindirizzato al portale guest, quindi ISE lo reindirizza a IdP per l'autenticazione. Dopodiché, il prodotto torna ad ISE. La richiesta viene convalidata e l'utente procede con l'accesso guest o l'avvio, a seconda della configurazione del portale.



SP-initiated

Flusso di rete



1. L'utente si connette al SSID e l'autenticazione è mac filtering (mab).
2. ISE risponde con access-accept contenente gli attributi Redirect-URL e Redirect-ACL
3. L'utente tenta di accedere a www.facebook.com.
4. WLC intercetta la richiesta e reindirizza l'utente al portale guest ISE, facendo clic sull'accesso dei dipendenti per registrare il dispositivo con le credenziali SSO.
5. ISE reindirizza l'utente all'applicazione OKTA per l'autenticazione.
6. Dopo l'autenticazione riuscita, OKTA invia la risposta dell'asserzione SAML al browser.
7. Il browser ritrasmette l'asserzione ad ISE.
8. ISE verifica la risposta all'asserzione e, se l'utente è autenticato correttamente, passa all'AUP e quindi alla registrazione del dispositivo.

Per ulteriori informazioni su SAML, fare clic sul collegamento seguente

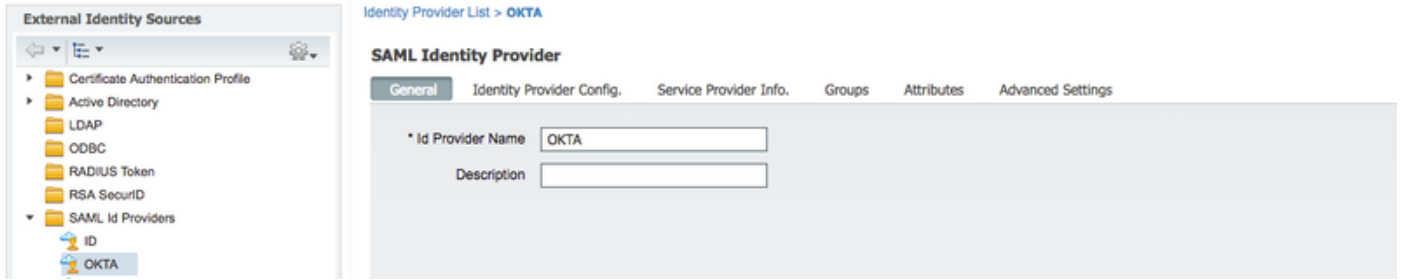
<https://developer.okta.com/standards/SAML/>

Configurazione

Passaggio 1. Configurare SAML Identity Provider e Guest Portal su ISE.

1. Preparare l'origine dell'identità esterna.

Passaggio 1. Passare a **Amministrazione > Origini identità esterne > Provider di ID SAML**.

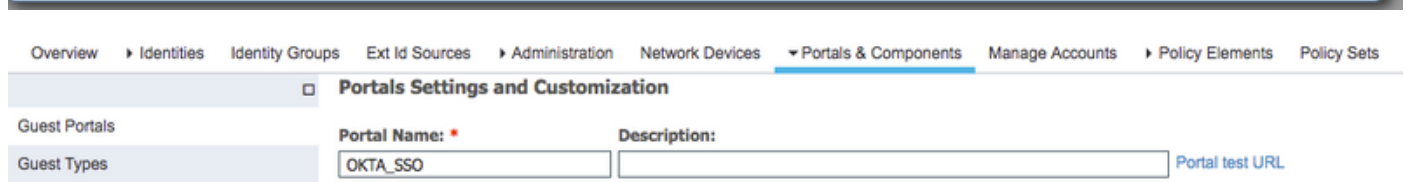
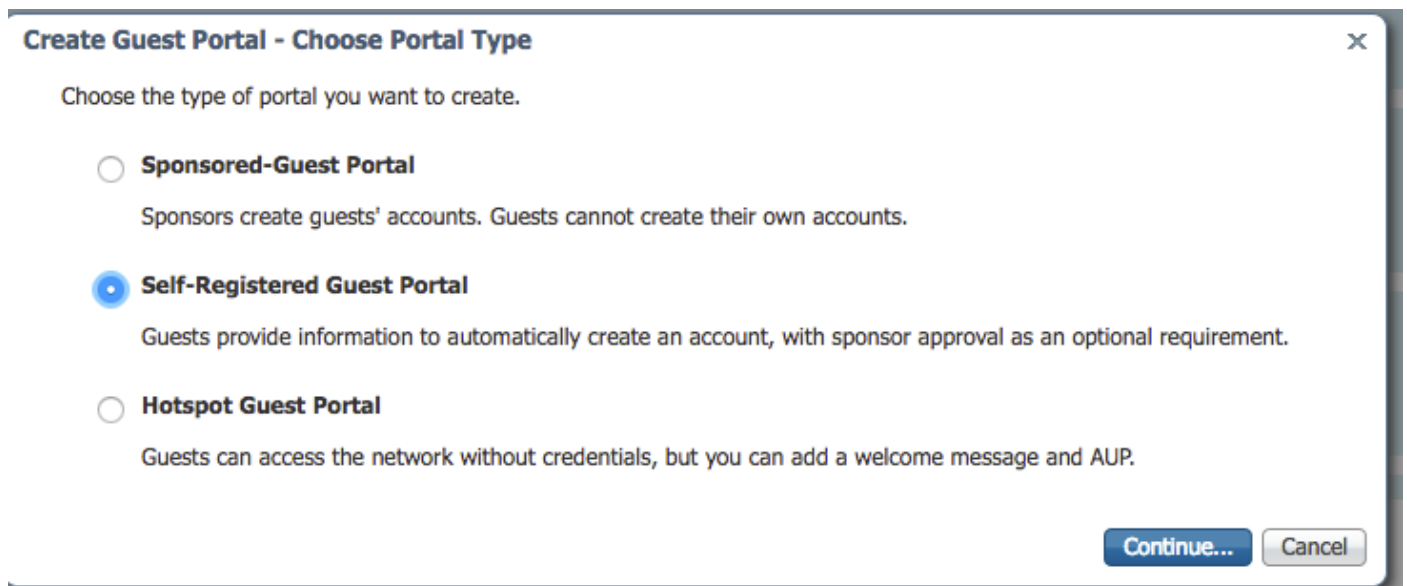


Passaggio 2. Assegnare un nome al provider di ID e sottomettere la configurazione.

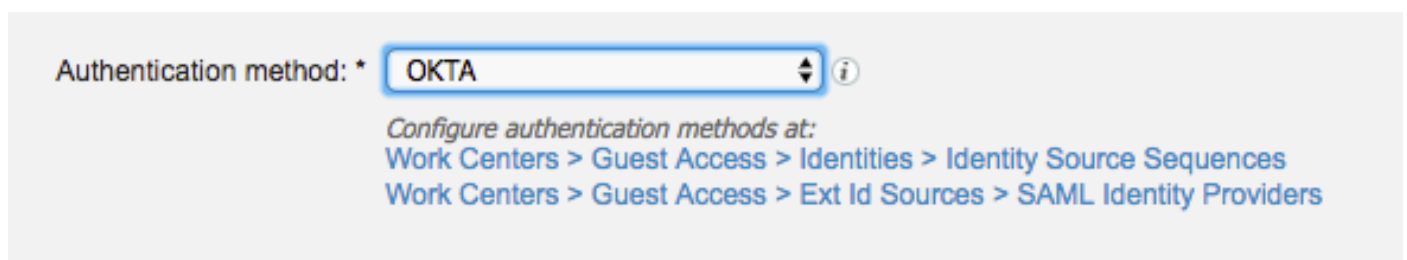
2. Creare il portale per SSO.

Passaggio 1. Creare il portale assegnato a OKTA come origine identità. Qualsiasi altra configurazione per BYOD, registrazione del dispositivo, Guest e così via, è esattamente la stessa del portale normale. In questo documento, il portale viene mappato al portale guest come accesso alternativo per i dipendenti.

Passaggio 2. Passare a **Centri di lavoro > Accesso guest > Portali e componenti** e creare il portale.



Passaggio 3. Scegliere il metodo di autenticazione per puntare al provider di identità configurato in precedenza.



Passaggio 4. Scegliere l'origine di identità OKTA come metodo di autenticazione.

(facoltativo) scegliere le impostazioni BYOD.

▼ 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](#)

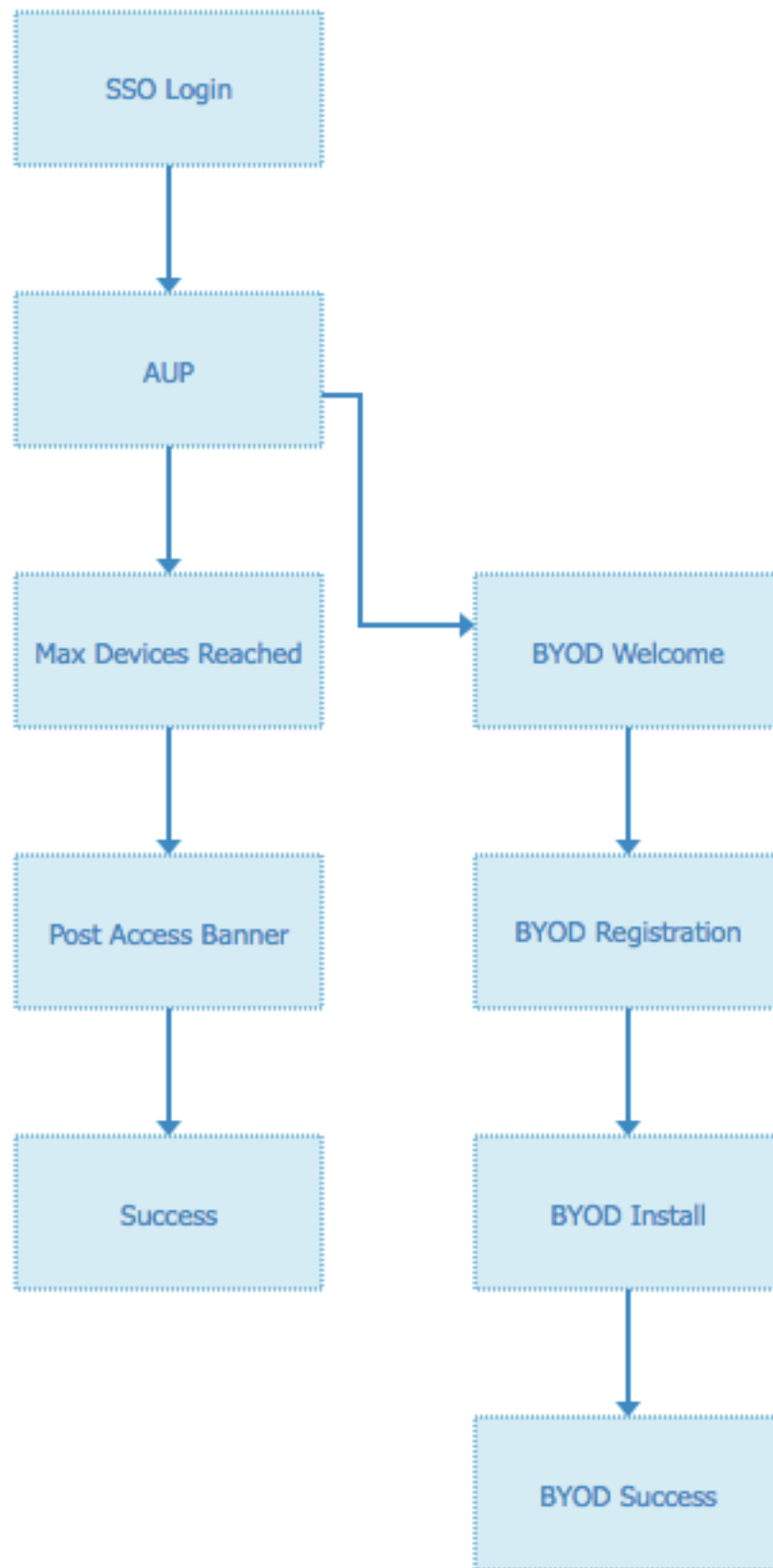
After successful device configuration take employee to:

Originating URL (i)

Success page

URL:

Passaggio 5. Salvare la configurazione del portale, con BYOD il flusso avrà il seguente aspetto:



3. Configurare l'accesso alternativo.

Nota: È possibile ignorare questa parte se non si utilizza il login alternativo.

Passare al portale guest di registrazione automatica o a qualsiasi altro portale personalizzato per

l'accesso guest.

Nelle impostazioni della pagina di accesso, aggiungere il portale di accesso alternativo: 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

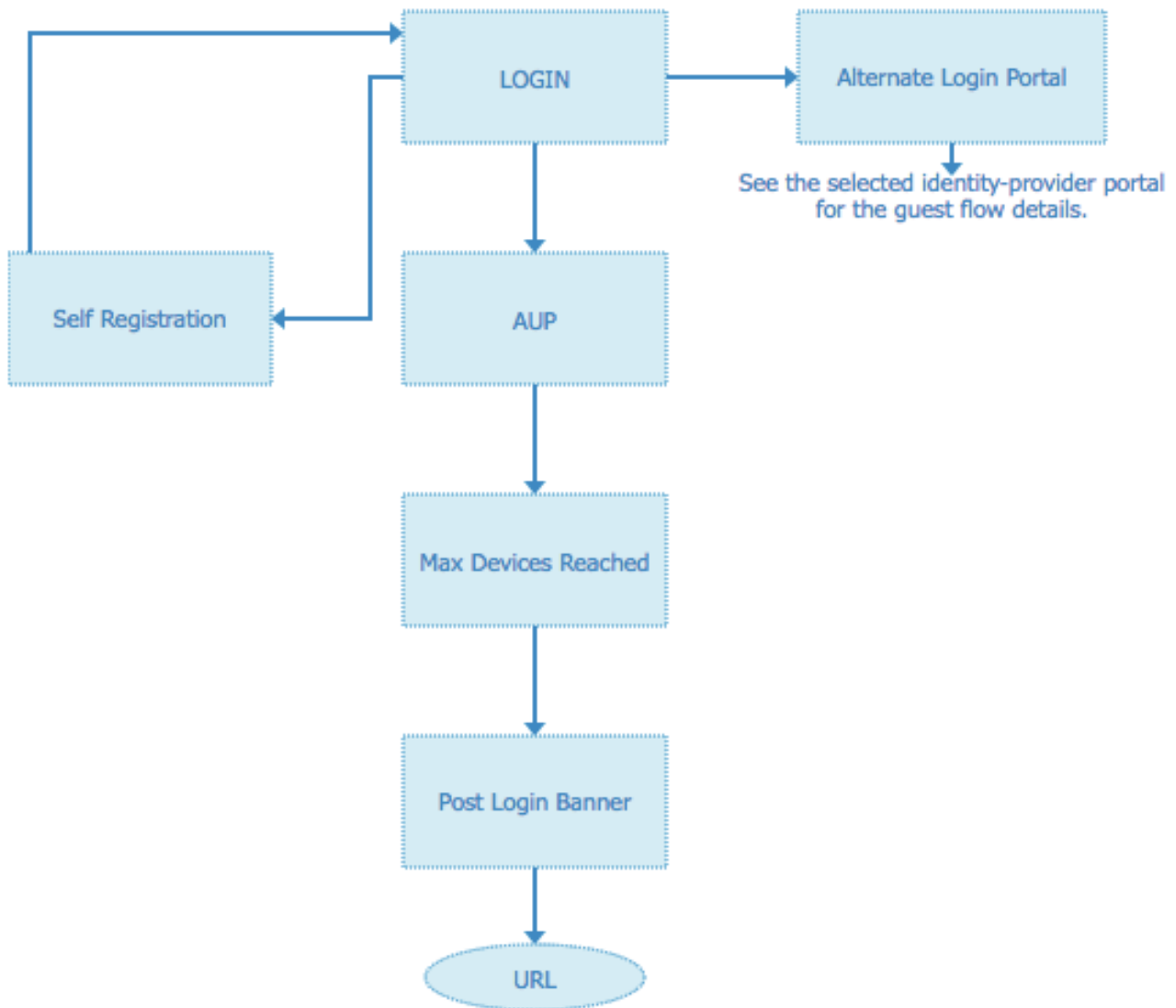
Allow social login

Allow guests to change password after login ⓘ

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

▼

Questo è il flusso del portale ora.



Passaggio 2. Configurare le impostazioni dell'applicazione OKTA e del provider di identità SAML.

1. Creare l'applicazione OKTA.

Passaggio 1. Accedere al sito Web OKTA con un account amministratore.

← 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

Passaggio 2. Fare clic su Aggiungi applicazione.

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](#)

Passaggio 3. Creare una nuova app. Scegliere SAML2.0

Create a New Application Integration



Platform

Web

Sign on method



Secure Web Authentication (SWA)

Uses credentials to sign in. This Integration works with most apps.



SAML 2.0

Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.



OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

Impostazioni generali

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

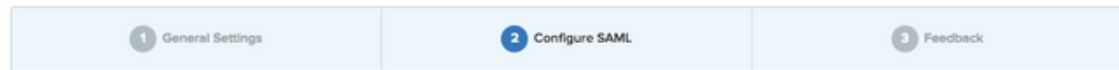


Do not display application icon in the Okta Mobile app

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](#)

Passaggio 4. Scaricare il certificato e installarlo 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. Esportare le informazioni SP dal provider di identità SAML.

Passare al provider di identità configurato in precedenza. Fare clic su **Service Provider Info** (Informazioni provider di servizi) ed esportarlo, come mostrato nell'immagine.

SAML Identity Provider

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

Service Provider Information

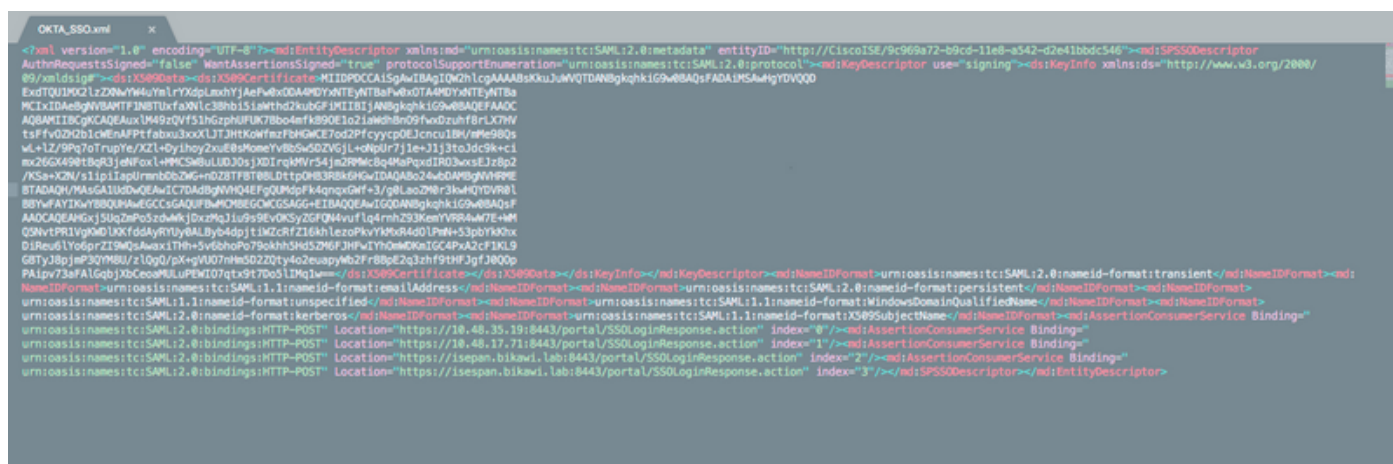
Load balancer

Export Service Provider Info.

Includes the following portals:

OKTA_SSO

La cartella zip esportata contiene il file XML e il file `readme.txt`



Per alcuni provider di identità è possibile importare direttamente il codice XML, ma in questo caso è necessario eseguire l'importazione manualmente.

- URL Single Sign-On (asserzione saml)

```
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 entità SP

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

URL SSO disponibile in formato indirizzo IP e FQDN.

Attenzione: La selezione del formato dipende dalle impostazioni di reindirizzamento nel profilo di autorizzazione. Se si utilizza un indirizzo IP statico, è necessario utilizzare l'indirizzo IP per l'URL SSO.

3. Impostazioni OKTA SAML.

Passaggio 1. Aggiungere gli URL nelle impostazioni SAML.

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"/>
<input type="button" value="+ Add Another"/>		

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](#)

Passaggio 2. È possibile aggiungere più URL dal file XML, in base al numero di PSN che ospitano questo servizio. Il formato ID del nome e il nome utente dell'applicazione dipendono dalla progettazione.

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>
```

Passaggio 3. Fare clic su Avanti e scegliere la seconda opzione.

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. Esportare i metadati dall'applicazione.

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.

Metadati:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exklrq8loEmedZSf4356">
<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIDrDCCApSgAwIBAgIGAWWPlTasMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcmlkZXIzAVBgnVBAMDMNpc2NvLXlhbGJpa2F3MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMB4XDTE4MDgzMTEwNDMwNV0XDTE4MDgzMTEwNDQwNVowgZyxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0w
CwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEjEXMBUGA1UEAwwOY2l2Y28tZWFlYmlr
YXcxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC1P7DvzVng7wSQWVOzGShwn+Yq2U4f3kbVgXWGuM0a7Bk61AUBoq485EQJ1+heB/6x
IMt8ulZ8HUsOspBECLYcI75gH4rpc2FM4kzZiDbNLb95AW6dlUztC66x42uhRYgduD5+w3/yvdwx
l99upWb6Sdrtnk8cx7AyIJA4E9KK22cV3ek2rFTrMEC5TT5iEDsnVzC9Bs9a1SRIjiadvhCSPdy
+qmMx9eFtZwzNl/g/vhS5F/CoC6EfOsFPr6aj/1PBeZuWuWjBFHW3Zy7hPEtHgJYQO/7GRK2RzOj
bSZgeAp5Yyytja3NCn9x6FMY5Rppc3HjtG4cJQS/MQVaJpn/AgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAJUK5zGPZwxECv5dN6YERuV5C5eHUXq3KGul2yIfih7x8EartZ4/wGP/HYUCNCNw3HTh+6T3
oLSAevm6U3ClNELRvG2kG39b/9+ErPG5UkSQSwFekP+bCqd83Jt0kxshYMYHi5FNB5FCTeVbfqRI
TJ2Tq2uuYpSveIMxQmy7r5qFziWOTvDF2Xp0Ag1e91H6nbdtsz3e5MMSKYGr9HaigGgqG4yXHkAs
77ifQOnRz7au0Uo9sInH6rWG+eOesysecPuWQtEqNqt+MyZnlCurJ0e+JTvKYH1dSWapM1dzqoX
OzyF7yiId9KPP6I4Ndc+BXe1dA8imneYy5MH7/nE/g=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</md:NameIDFormat>
<md:NameIDFormat>
```



```
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml" />
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://cisco-
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml" />
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

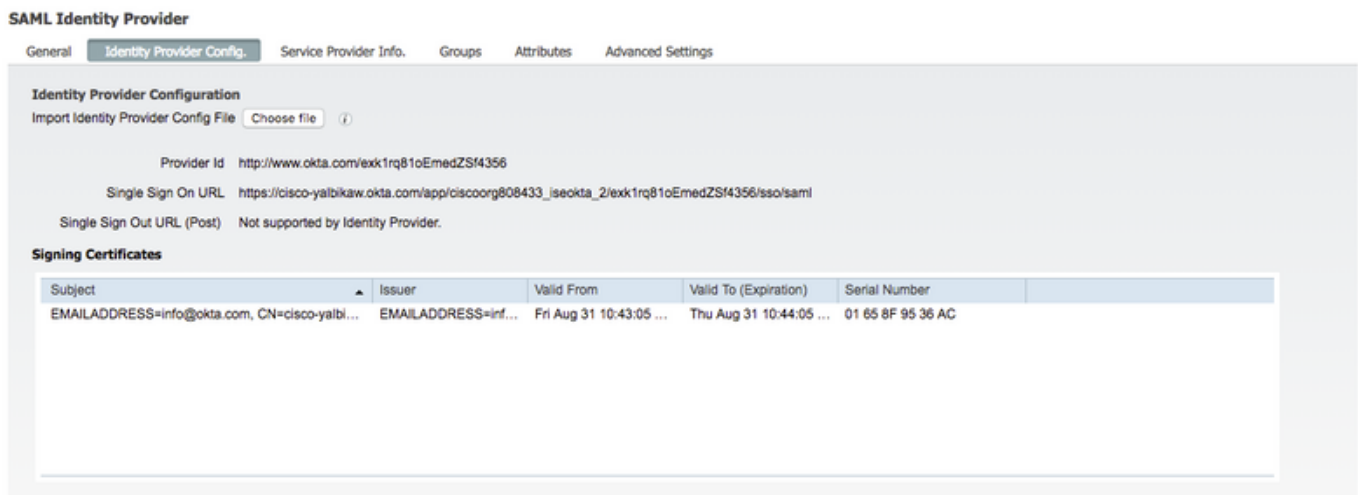
Salvare il file in formato XML.

5. Assegnare gli utenti all'applicazione.

Assegnare gli utenti a questa applicazione, esiste un modo per l'integrazione di AD, come spiegato in: [directory okta-active](#)

6. Importare i metadati dall'Idp all'ISE.

Passaggio 1. In **Provider di identità SAML**, selezionare **Config.** e Importa metadati.



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

Single Sign On URL https://cisco-yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exk1rq81oEmedZSf4356/sso/saml

Single Sign Out URL (Post) Not supported by Identity Provider.

Signing Certificates

Subject	Issuer	Valid From	Valid To (Expiration)	Serial Number
EMAILADDRESS=info@okta.com, CN=cisco-yalbi...	EMAILADDRESS=inf...	Fri Aug 31 10:43:05 ...	Thu Aug 31 10:44:05 ...	01 65 8F 95 36 AC

Passaggio 2. Salvare la configurazione.

Passaggio 3. Configurazione di CWA.

Questo documento descrive la configurazione per ISE e WLC.

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

Aggiungere URL nell'ACL di reindirizzamento.

<https://cisco-yalbikaw.okta.com> / aggiungere l'URL dell'applicazione

<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.

Verifica

Eeguire il test del portale e verificare se è possibile raggiungere l'applicazione OKTA

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

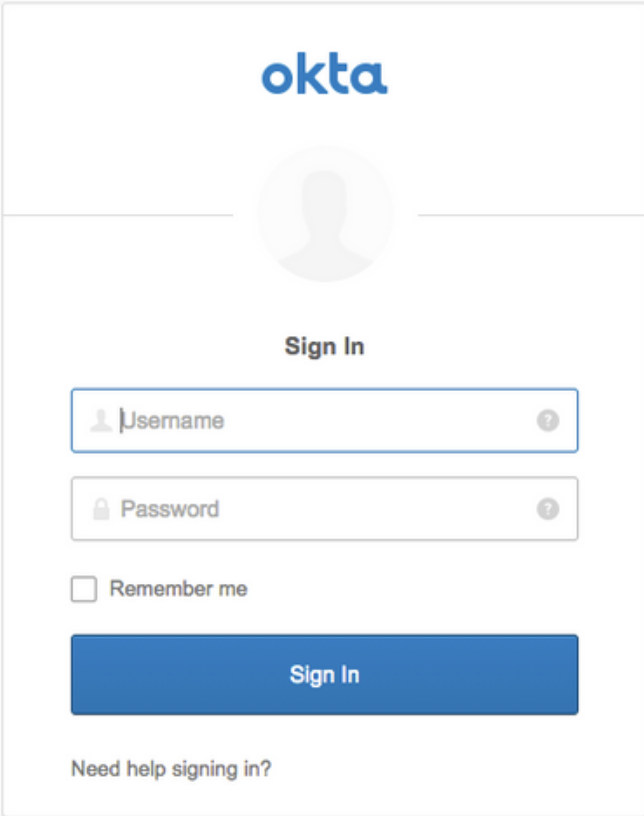
 **Portal Behavior and Flow Settings**
Use these settings to specify the guest experience for this portal.

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

Passaggio 1. Fare clic sul test del portale, quindi reindirizzare all'applicazione SSO.

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. The form contains two input fields: "Username" and "Password". Each field has a small icon on the left (a person icon for the username and a lock icon for the password) and a question mark icon on the right. 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?".

Passaggio 2. Verificare la **connessione** delle informazioni **a <nome applicazione>**

Passaggio 3. Se si immettono le credenziali, è possibile che venga visualizzata una richiesta SAML errata. Ciò non significa necessariamente che a questo punto la configurazione sia errata.

Verifica utente finale

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

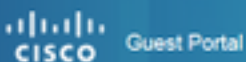
[Need help signing in?](#)

before you can access the Internet.



Signing in to ISE-OKTA

before you can access the Internet.



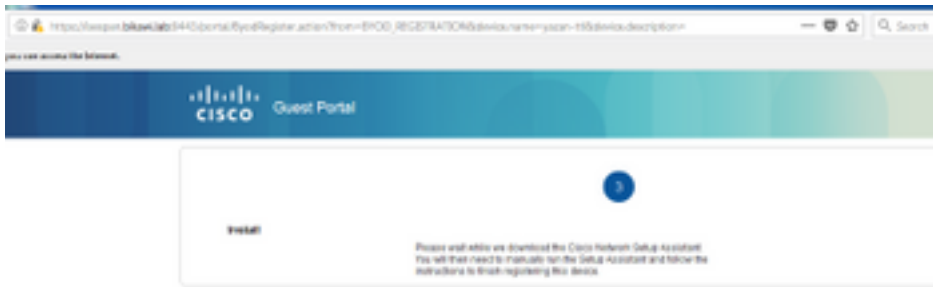
Acceptable Use Policy

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



Verifica ISE

Controllare i registri di durata per verificare lo stato di autenticazione.

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

Risoluzione dei problemi

Risoluzione dei problemi OKTA

Passaggio 1. Controllare i log nella scheda **Report**.

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

Passaggio 2. Visualizzare anche i log correlati dall'applicazione.

← 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 "0aaf78f031HC20YF356" and target.type eq "AppInstance"



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

Risoluzione dei problemi ISE

Sono disponibili due file registro da controllare

- ise-psc.log
- guest.log

Selezionare **Amministrazione > Sistema > Log > Configurazione log di debug**. Abilitare il livello a DEBUG.

SAML	ise-psc.log
Guestaccess	guest.log
Portale	guest.log

Nella tabella viene illustrato il componente di cui eseguire il debug e il file di log corrispondente.

Problemi comuni e soluzioni

Scenario 1. Richiesta SAML non valida.

okta



400
BAD REQUEST

Your request resulted in an error.

Description: Bad SAML request

[Go to Homepage](#)

Questo errore è generico. Controllare i registri per verificare il flusso e individuare il problema. Su ISE guest.log:

ISE# show logging applicazione guest.log | ultimi 50

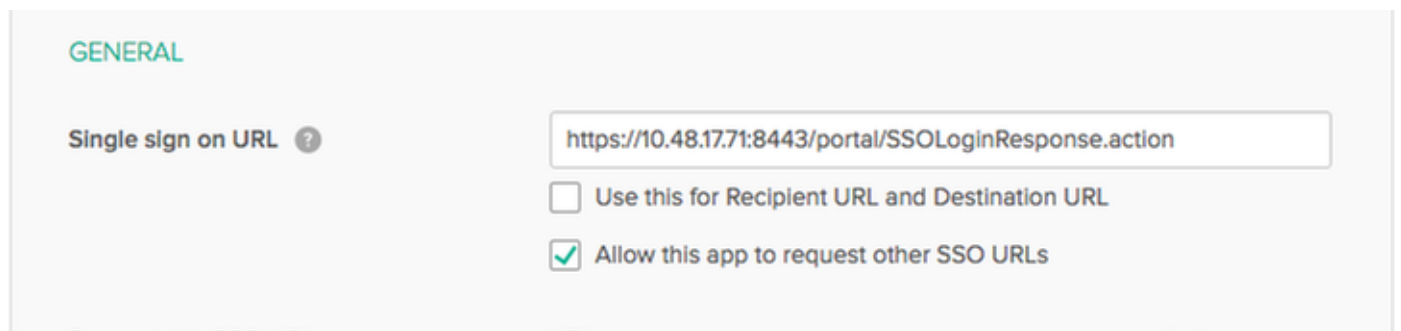
```
2018-09-30 01:32:35,624 DEBUG [https-jsse-nio-10.48.17.71-8443-exec-2][  
cisco.ise.portalwebaction.configmanager.SSOLoginConfigHandler -::- SSOLoginTransitionResult:  
SSOLoginTransitionResult:
```

```
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/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o
wF
Ib%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH
kiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhOiulyQcIeJo1WVnFVI29qDGjrgZKmv0
OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0SltA0Vxv1CPwo1hGtcFepS3HZF3pzS
H04QZ2tLaAPLy2ww9pDwdpHQY%2Bzilld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3u
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo
q7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIPtot64oM%2BVyWK391X5TI%
2B3aGyRWgMzond309NPSMCPq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXElzX6nmngdq3YIO37q9fBlQnC
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_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/exklrq81oEmedZSf4356/sso/saml
?SAMLRequest=nZRdb9owFIb%2FSuT7EJMPIBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2FnONki%2FZRoeUyPu95j9%2FzJ
OOb4672DqCNUJD%2FR5GHkiuKiEfM7Qp7%2FwRupmMDD3VDZnu7ZNcw889GOs5nTTkdJChvZZEUSMMkXQHhOiulyQcIeJ
o1WVnFVI29qDGjrgZKmv0OdAH6IDhs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcrQ0SltA0Vxv
1CPwo1hGtcFepS3HZF3pzSH04QZ2tLaAPLy2ww9pDwdpHQY%2Bzilld%2FvW8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93L
nn1MP%2B6mS6Kq8TFfJl3ugJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iTh
DECriw6Sd5n%2FjMxd3Wzoq7ZAd7DMGYPuTWSVpuhEPdHPk79CJe4T6KQRElVEcbfkb6XdcnITsIP
tot64oM%2BVyWK391X5TI%2B3aGyRWgMzond309NPSMCPq0YDguZsJwlRfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXElz
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

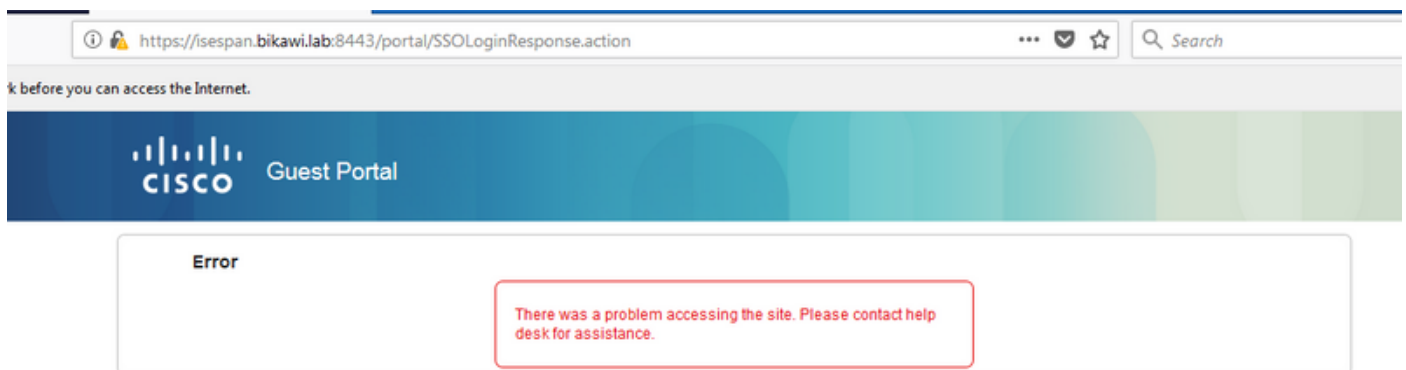
ISE ha reindirizzato l'utente all'IDP. Tuttavia, non verrà inviata alcuna risposta all'ISE e verrà visualizzata una richiesta SAML errata. Indicare che OKTA non accetta la richiesta SAML.

```
https://cisco-  
yalbikaw.okta.com/app/ciscoorg808433_iseokta_2/exklrq81oEmedZSf4356/sso/saml?SAMLRequest=nZRdb9o  
wF  
Ib%2FSuT7EJMPiBahYpRqkWB1JOxiN5XtHFprwc5sQ%2Bm%2Fn0NKi%2FZRoeUyPu95j9%2FzJOOb4672DqCNUJD%2FR5GH  
kiuKiEfm7Qp7%2FwRupmMDd3VDZnu7ZNcw889Gos5nTTkdJChvZZEUSMMkXQHh1hOiulyQcIeJo1WVnFVI29qDGjrrjGZKmv0  
OdAH6IDHs1osMPVnbGBIEwoBpqOwx8YM%2Bi15NGRnFcRQ0S1taB0Vxv1CPwolhGtcFepS3HZF3pzS  
H04QZ2tLaAPLy2ww9pDwdpHQY%2Biz1ld%2Fvw8inSRz6VQhxn7GKJ%2FHg4Xa%2ByJd5OV93Lnn1MP%2B6mS6Kq8TFfJl3u  
gJMm%2BObfDac4i2msc%2F4aODHySDx0xhTn%2BHtKOIM0mgYnuSaVmJvfpdjGkEapwy3T8iThDecRiw6Sd5n%2FjMxd3Wzo  
q7ZAd7DMGYPuTSWSpuhEPdHPk79CJe4T6KQRElvECbfk6d6XdcnITsIPtot64oM%2BVyWK391X5TI%  
2B3aGyRWgMzond309NPSMCpq0YDguZsJwlrfz4JqdjINL226IsCFfnE9%2Bu1K14C8Xs4TXE1zX6nmmgdq3YIO37q9fBlQnC  
h3jFo72v2xmatdQLUybIhwd4a85ksvOs9qFtIbthcPvmX5YxglvW7vXLUPPSlctE8DdzUpNpWlZ7wL%2B6zyT7uxfgUzOu7n  
8m0x%2BAQ%3D%3D&RelayState=_9c969a72-b9cd-11e8-a542-d2e41bbdc546_DELIMITERport  
alId_EQUALS9c969a72-b9cd-11e8-a542-d2e41bbdc546_SEMIportalSessionId_EQUALS6770f0a4-bc86-4565-  
940a-  
b0f83cbe9372_SEMIradiusSessionId_EQUALS0a3e949b000002c55bb023b3_SEMI_DELIMITERisespan.bikawi.lab  
Controllare nuovamente l'applicazione, se sono state apportate modifiche.
```



L'URL SSO utilizza un indirizzo IP. Tuttavia, il guest sta inviando un FQDN come è possibile vedere nella richiesta sopra l'ultima riga contiene SEMI_DELIMITER<FQDN> per risolvere il problema. Modificare l'indirizzo IP in FQDN nelle impostazioni OKTA.

Scenario 2. "Si è verificato un problema durante l'accesso al sito. Contattare l'helpdesk per assistenza".



Guest.log

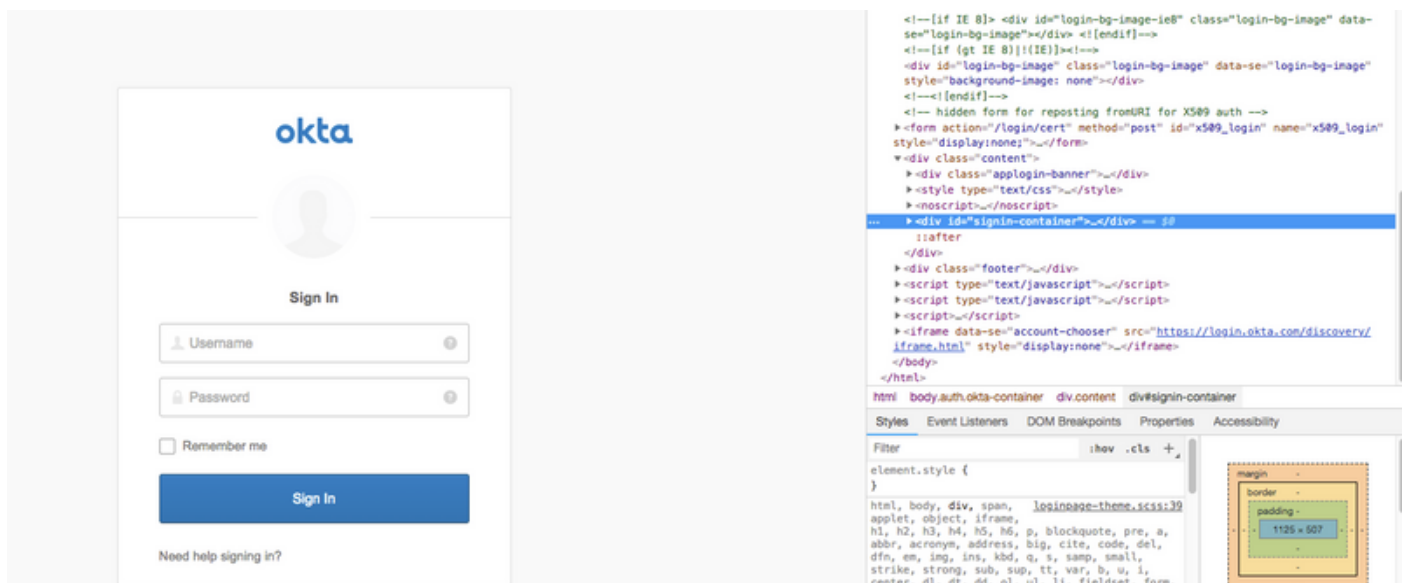
```
2018-09-30 02:25:00,595 ERROR [https-jsse-nio-10.48.17.71-8443-exec-1][  
guestaccess.flowmanager.step.guest.SSOLoginStepExecutor -::- SSO Authentication failed or  
unknown user, authentication result=FAILED, isFailedLogin=true, reason=24823 Assertion does not  
contain ma
```

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

Dai log, ISE segnala che l'asserzione non è corretta. Verificare che l'URI del gruppo di destinatari OKTA corrisponda all'SP per risolverlo.

Scenario 3. Reindirizzato alla pagina vuota oppure l'opzione di accesso non viene visualizzata.

Dipende dall'ambiente e dalla configurazione del portale. In questo tipo di problema è necessario controllare l'applicazione OKTA e quali URL sono necessari per l'autenticazione. Fare clic sul test del portale, quindi esaminare l'elemento per verificare quali siti Web devono essere raggiungibili.



In questo scenario, solo due URL: e login.okta.com - queste dovrebbero essere consentite sul WLC.

Informazioni correlate

- <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>