

# Configura autenticazione esterna OKTA SSO per protezione anti-phishing avanzata

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Informazioni generali](#)

[Requisiti](#)

[Configurazione](#)

[Verifica](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna OKTA SSO per l'accesso a Cisco Advanced Phishing Protection.

## Prerequisiti

Accesso come amministratore al portale Cisco Advanced Phishing Protection.

Accesso come amministratore a Okta idP.

Certificati SSL X.509 autofirmati o firmati dalla CA (facoltativi) in formato PKCS #12 o PEM.

## Informazioni generali

- Cisco Advanced Phishing Protection consente di abilitare l'accesso SSO per gli amministratori che utilizzano SAML.
- OKTA è un programma di gestione delle identità che fornisce servizi di autenticazione e autorizzazione alle applicazioni.
- Cisco Advanced Phishing Protection può essere impostata come applicazione connessa a OKTA per l'autenticazione e l'autorizzazione.
- SAML è un formato di dati standard aperto basato su XML che consente agli amministratori di accedere senza problemi a un set definito di applicazioni dopo aver eseguito l'accesso a una di tali applicazioni.
- Per ulteriori informazioni su SAML, è possibile accedere al collegamento seguente: [SAML Informazioni generali](#)

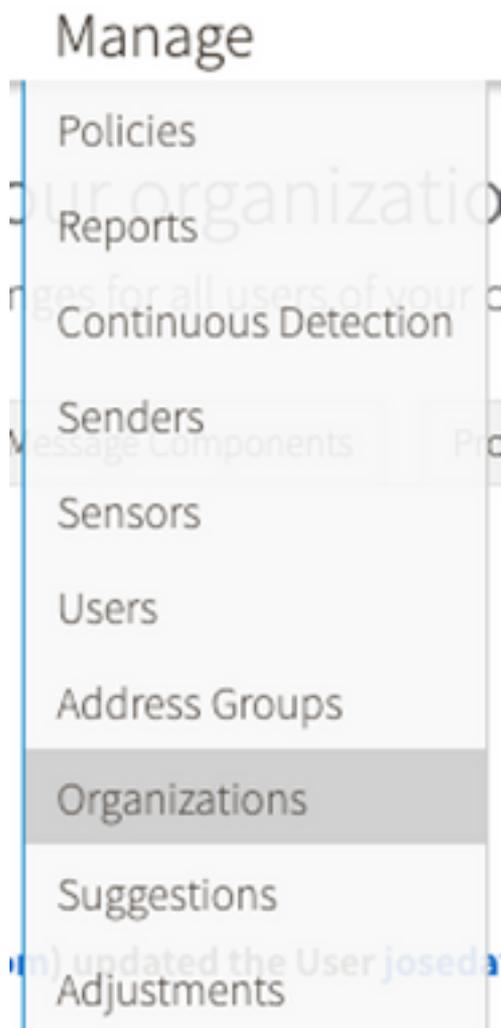
## Requisiti

- Portale Cisco Advanced Phishing Protection.
- Account amministratore OKTA.

# Configurazione

In Cisco Advanced Phishing Protection Portal:

1. Accedere al portale dell'organizzazione, quindi selezionare **Gestisci > Organizzazioni**, come mostrato nell'immagine:



2. Selezionare il nome dell'organizzazione, **Modifica organizzazione**, come mostrato nell'immagine:

## Edit Organization

Alter the settings for this organization.



3. Nella scheda **Amministrativo**, scorrere fino a **Impostazioni account utente** e selezionare **Abilita** in SSO, come mostrato nell'immagine:

## User Account Settings

Single Sign-On:

If Single Sign-On is enabled for the users in an organization, some of the following settings may be overridden by the Identity Provider used for authentication. Refer to the documentation for the Identity Provider for specific settings regarding failed login attempts and password policy.

4. La finestra successiva fornisce le informazioni da inserire nella configurazione di OKTA SSO. Incollare in un blocco note le informazioni seguenti, utilizzarle per configurare le impostazioni OKTA:

-ID entità: apcc.cisco.com

- Assertion Consumer Service: questi dati sono personalizzati in base all'organizzazione.

Selezionare il formato di **posta elettronica** denominato per utilizzare un indirizzo di posta elettronica per l'accesso, come mostrato nell'immagine:

## Single Sign-On Configuration

Follow the steps below to configure Cisco APP to use your organization's Single Sign-On solution. Upon completion, all users in your organization will receive an email with instructions to complete account setup to use Single Sign-On to authenticate with Cisco APP.

You may need the following parameters configured on your Identity Provider:

- Entity ID: apcc.cisco.com
- Assertion Consumer Service (ACS):
  - ✓ urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
  - ✓ urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
  - ✓ urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

5. Ridurre al minimo la configurazione di Cisco Advanced Phishing Protection in questo momento, poiché è necessario impostare prima l'applicazione in OKTA prima di procedere con i passaggi successivi.

Sotto Okta.

1. Passare al portale delle applicazioni e selezionare **Crea integrazione applicazioni**, come mostrato nell'immagine:

## Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2. Selezionare **SAML 2.0** come tipo di applicazione, come mostrato nell'immagine:

## Create a new app integration

X

### Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

3. Immettere il nome dell'app **Advanced Phishing Protection** e selezionare **Avanti**, come mostrato nell'immagine:

1 General Settings

App name

App logo (optional)

App visibility  Do not display application icon to users

Cancel

4. Nelle impostazioni SAML, riempire gli spazi vuoti, come mostrato nell'immagine:

- URL Single Sign-On: Questo è il servizio consumer di asserzione ottenuto da Cisco Advanced Phishing Protection.
- URL destinatario: Questo è l'ID entità ottenuto da Cisco Advanced Phishing Protection.
- Formato ID nome: conservarlo come Non specificato.
- Nome utente applicazione: Email, che richiede all'utente di immettere il proprio indirizzo e-mail nel processo di autenticazione.
- Aggiorna nome utente applicazione in: Crea e aggiorna.

**A SAML Settings**

**General**

Single sign on URL ?   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?   
If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

Scorrere verso il basso fino a **Istruzioni attributi gruppo (facoltativo)**, come mostrato nell'immagine:

Immettere l'istruzione di attributo successiva:

- Nome: group
- Formato nome: Non specificato.
- Filtro: "Uguale a" e "OKTA"

**Group Attribute Statements (optional)**

Name	Name format (optional)	Filter
<input type="text" value="group"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Equals"/> <input type="text" value="OKTA"/>

Selezionare Avanti.

5. Quando viene richiesto a Okta di comprendere come è stata configurata questa applicazione, immettere il motivo applicabile all'ambiente corrente, come mostrato nell'immagine:

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

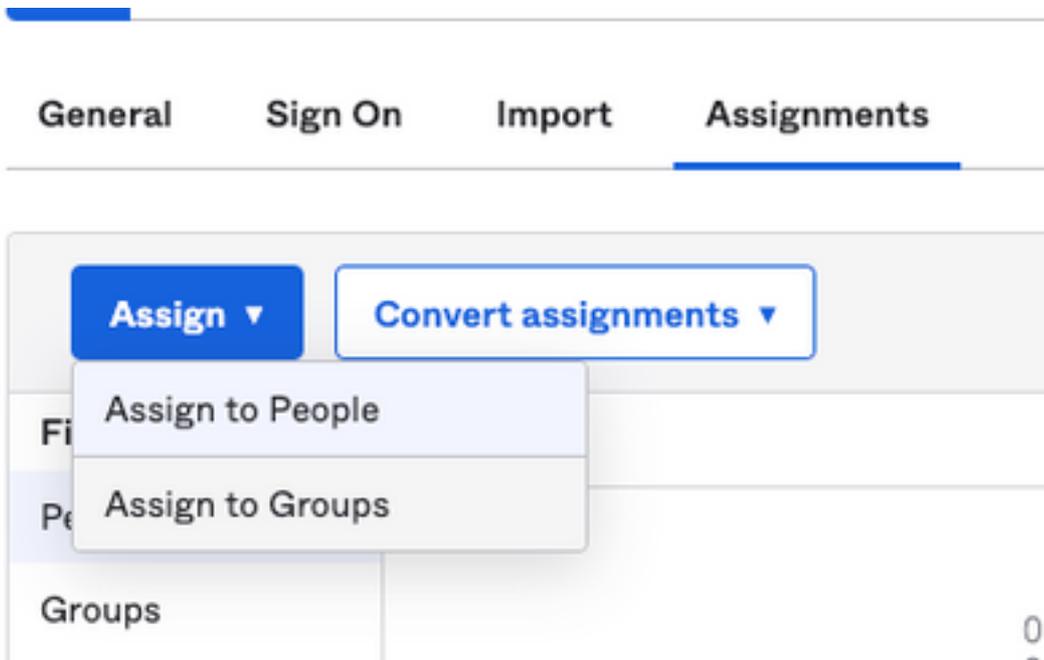
I'm a software vendor. I'd like to integrate my app with Okta

Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

[Previous](#) [Finish](#)

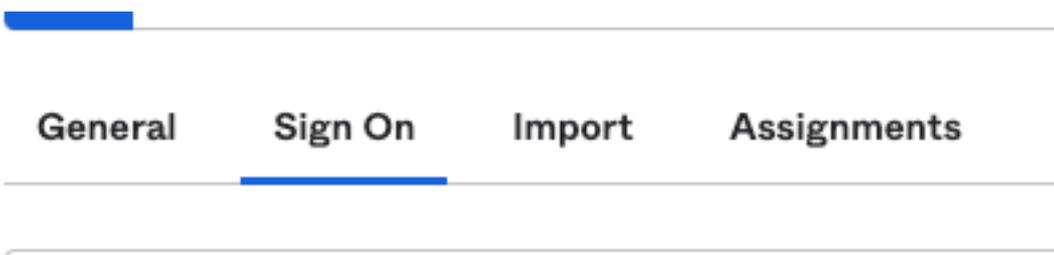
Selezionare **Finish** (Fine) per continuare con il passaggio successivo.

6. Selezionare la scheda **Assegnazioni**, quindi selezionare **Assegna > Assegna a gruppi**, come mostrato nell'immagine:



7. Selezionare il gruppo OKTA, ovvero il gruppo con gli utenti autorizzati ad accedere all'ambiente

8. Selezionare **Sign On** (Accedi), come illustrato nell'immagine:



9. Scorrere verso il basso e verso l'angolo destro, immettere l'opzione **View SAML setup instructions** (Visualizza istruzioni di impostazione SAML), come mostrato nell'immagine:

## SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

9. Salva in un blocco note le informazioni successive, necessarie per l'inserimento nel portale Cisco Advanced Phishing Protection, come mostrato nell'immagine:

- URL Single Sign-On del provider di identità.
- Identificare l'emittente del provider (non richiesto per Cisco Advanced Phishing Protection, ma obbligatorio per altre applicazioni).
- Certificato X.509.

### The following is needed to configure Advanced Phishing Protection

1 Identity Provider Single Sign-On URL:

https://1/eak2j1xb1n0qg9Rk0697/sso/saml

2 Identity Provider Issuer:

http://www.okta.com/

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDqjOCAPkqAwIBAgIIGATN/4nF0MA8OC5qGS1b3OQEBCwIAIjOVWQswCQYDVQQGEwAVUudETMBEG
```

```
-----END CERTIFICATE-----
```

[Download certificate](#)

10. Dopo aver completato la configurazione dell'OKTA, è possibile tornare a Cisco Advanced Phishing Protection

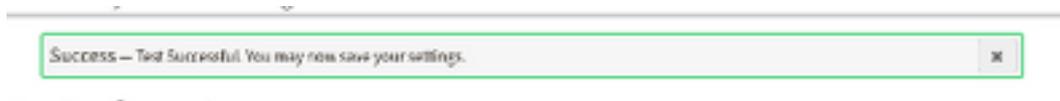
### In Cisco Advanced Phishing Protection Portal:

1. Con il formato identificativo del nome, inserire le informazioni seguenti:

- Endpoint SAML 2.0 (reindirizzamento HTTP): URL Identify Provider Single Sign-On fornito da Okta.
- Certificato pubblico: Immettere il certificato X.509 fornito da Okta.

2. Selezionare **Test Settings** per verificare che la configurazione sia corretta

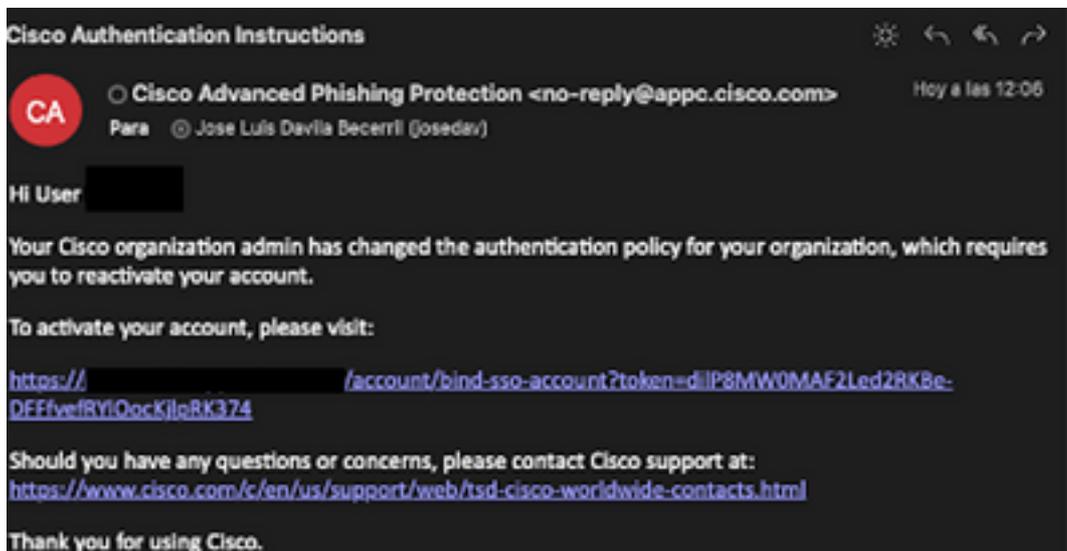
Se non ci sono errori nella configurazione, viene visualizzata una voce Test riuscito e ora è possibile salvare le impostazioni, come mostrato nell'immagine:



3. Salvare le impostazioni

## Verifica

1. Gli amministratori esistenti che non utilizzano SSO vengono informati tramite posta elettronica che il criterio di autenticazione è stato modificato per l'organizzazione e gli amministratori devono attivare il proprio account utilizzando un collegamento esterno, come mostrato nell'immagine:



2. Una volta attivato l'account, immettere l'indirizzo di posta elettronica e quindi reindirizzare l'utente al sito Web di login OKTA per l'accesso, come mostrato nell'immagine:

# Log In to Advanced Phishing Protection

Not a member? [Sign up here](#)

Your Email:

[Next](#)

# okta

## Sign In

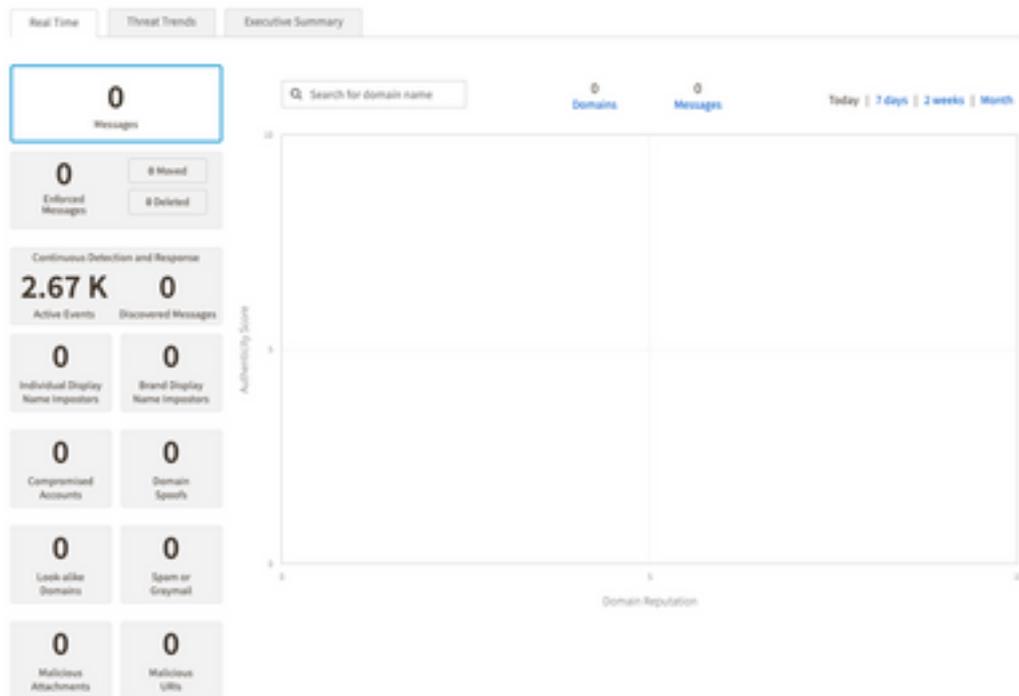
Username

Keep me signed in

[Next](#)

[Help](#)

3. Una volta completato il processo di login OKTA, accedere al portale Cisco Advanced Phishing Protection, come mostrato nell'immagine:



## Informazioni correlate

[Cisco Advanced Phishing Protection - Informazioni sul prodotto](#)

[Cisco Advanced Phishing Protection - Guida per l'utente](#)

[Supporto OKTA](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).