

Externe OKTA SSO-Authentifizierung für erweiterten Phishing-Schutz konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Hintergrundinformationen](#)

[Anforderungen](#)

[Konfigurieren](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der externen OKTA SSO-Authentifizierung für die Anmeldung bei Cisco Advanced Phishing Protection.

Voraussetzungen

Administratorzugriff auf das Cisco Advanced Phishing Protection-Portal

Administratorzugriff auf Okta idP.

Selbstsignierte oder CA-signierte (optional) X.509 SSL-Zertifikate im PKCS #12- oder PEM-Format.

Hintergrundinformationen

- Cisco Advanced Phishing Protection ermöglicht die SSO-Anmeldung für Administratoren mit SAML.
- OKTA ist ein Identitätsmanager, der Authentifizierungs- und Autorisierungsdienste für Ihre Anwendungen bereitstellt.
- Cisco Advanced Phishing Protection kann als Anwendung festgelegt werden, die mit OKTA zur Authentifizierung und Autorisierung verbunden ist.
- SAML ist ein XML-basiertes, offenes Standarddatenformat, das es Administratoren ermöglicht, nach der Anmeldung bei einer dieser Anwendungen nahtlos auf einen definierten Satz von Anwendungen zuzugreifen.
- Um mehr über SAML zu erfahren, können Sie auf den folgenden Link zugreifen: [SAML Allgemeine Informationen](#)

Anforderungen

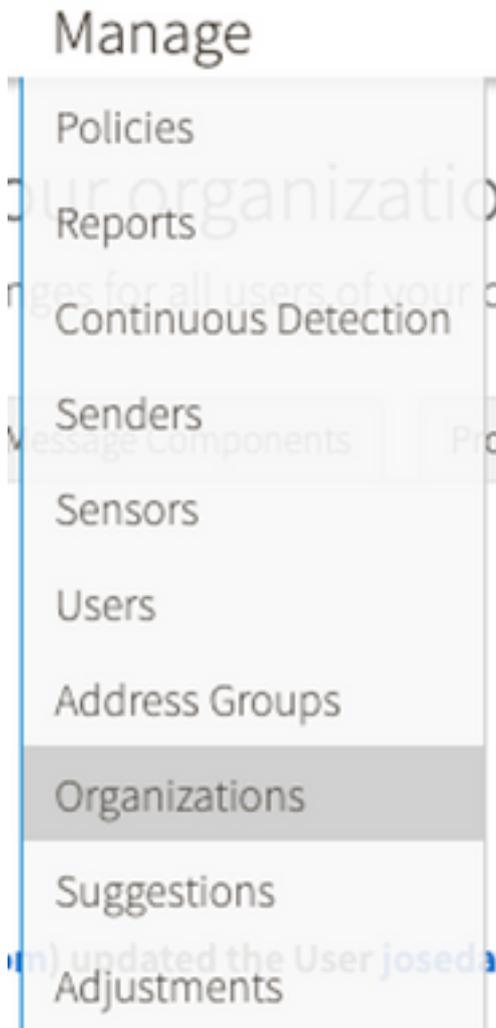
- Cisco Advanced Phishing Protection-Portal

- OKTA-Administratorkonto.

Konfigurieren

Im Cisco Advanced Phishing Protection-Portal:

1. Melden Sie sich bei Ihrem Organisationsportal an, und wählen Sie dann **Verwalten > Organisationen**, wie in der Abbildung dargestellt:



2. Wählen Sie Ihren Organisationsnamen **Organisation bearbeiten**, wie in der Abbildung dargestellt:

Edit Organization

Alter the settings for this organization.



3. Scrollen Sie auf der Registerkarte **Verwaltung** nach unten zu **Benutzerkontoeinstellungen** und wählen Sie unter SSO die Option **Aktivieren** aus, wie im Bild gezeigt:

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. Das nächste Fenster enthält die Informationen, die Sie unter der OKTA SSO-Konfiguration eingeben müssen. Fügen Sie die folgenden Informationen in einen Notizblock ein. Verwenden Sie diese Informationen, um die OKTA-Einstellungen zu konfigurieren:

-Entitäts-ID: apcc.cisco.com

- Assertion Consumer Service: Diese Daten sind auf Ihre Organisation zugeschnitten.

Wählen Sie das benannte **E-Mail**-Format aus, um eine E-Mail-Adresse für die Anmeldung zu verwenden, wie im Bild gezeigt:

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:csa:names:to:SAML_1.1:nameid-format:unspecified
 - urn:csa:names:to:SAML_1.1:nameid-format:emailAddress
 - urn:csa:names:to:SAML_2.0:nameid-format:persistent

5. Minimieren Sie die Cisco Advanced Phishing Protection-Konfiguration zu diesem Zeitpunkt, da Sie zunächst die Anwendung in OKTA einrichten müssen, bevor Sie mit den nächsten Schritten fortfahren.

Unter Okta.

1. Navigieren Sie zum Anwendungsportal, und wählen Sie **Create App Integration** (Anwendungsintegration erstellen) aus, wie in der Abbildung dargestellt:

Applications



2. Wählen Sie **SAML 2.0** als Anwendungstyp, wie in der Abbildung dargestellt:

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. Geben Sie den App-Namen **Advanced Phishing Protection** ein, und wählen Sie **Weiter**, wie im Bild gezeigt:

1 General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel Next

4. Füllen Sie unter den SAML-Einstellungen die Lücken aus, wie in der Abbildung dargestellt:

- URL für einmalige Anmeldung: Dies ist der Assertion Consumer Service von Cisco Advanced Phishing Protection.

- Empfänger-URL: Dies ist die Objektkennung, die von Cisco Advanced Phishing Protection bezogen wird.

- Format der Namens-ID: als nicht angegeben.

- Anwendungsbenutzername: E-Mail, bei der der Benutzer aufgefordert wird, seine E-Mail-Adresse bei der Authentifizierung einzugeben.

- Anwendungsbenutzername aktualisieren auf: Erstellen und aktualisieren

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](#)

Blättern Sie nach unten zu **Gruppenattribut-Anweisungen (optional)**, wie in der Abbildung dargestellt:

Geben Sie die nächste Attributanweisung ein:

- Name: gruppe
- Namensformat: Nicht angegeben.
- Filter: "Equals" und "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"/>

Wählen Sie Weiter aus.

5. Wenn Sie Okta um Hilfe gebeten werden, um zu verstehen, wie Sie diese Anwendung konfiguriert haben, geben Sie bitte den entsprechenden Grund für die aktuelle Umgebung ein, wie im Bild gezeigt:

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](#)

Wählen Sie **Beenden**, um mit dem nächsten Schritt fortzufahren.

6. Wählen Sie die Registerkarte **Assignments (Aufgaben)** und dann **Assign > Assign to Groups (Zuordnen zu Gruppen)**, wie im Bild gezeigt:

General **Sign On** **Import** **Assignments**

Assign **Convert assignments**

Assign to People

Assign to Groups

Groups

7. Wählen Sie die OKTA-Gruppe, d. h. die Gruppe mit den autorisierten Benutzern, um auf die Umgebung zuzugreifen.

8. Wählen Sie **Anmelden**, wie im Bild gezeigt:

General **Sign On** **Import** **Assignments**

9. Blättern Sie nach unten und nach rechts, und geben Sie die Option **SAML-Installationsanweisungen anzeigen** ein, wie in der Abbildung dargestellt:

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. Speichern Sie auf einem Notizblock die nächsten Informationen, die erforderlich sind, um das Cisco Advanced Phishing Protection-Portal aufzurufen, wie im Bild gezeigt:

- Single-Sign-On-URL des Identitätsanbieters
- Identifizieren Sie einen Provider (nicht erforderlich für Cisco Advanced Phishing Protection, aber obligatorisch für andere Anwendungen).
- X.509-Zertifikat.

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/4nFOMA8OC5qGS1b3OQEBCwIAIjOVWQswCQYDVQQGEwAVUudETMBEG
```

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

[Download certificate](#)

10. Nach Abschluss der OKTA-Konfiguration können Sie zu Cisco Advanced Phishing Protection zurückkehren.

Im Cisco Advanced Phishing Protection-Portal:

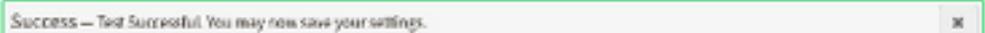
1. Geben Sie unter Name bezeichner Format die folgenden Informationen ein:

- SAML 2.0-Endpunkt (HTTP Redirect): Die von Okta bereitgestellte Identitätsanbieter-Single-Sign-On-URL.

- Öffentliches Zertifikat: Geben Sie das X.509-Zertifikat ein, das von Okta bereitgestellt wird.

2. Wählen Sie **Testeinstellungen**, um die Konfiguration zu überprüfen.

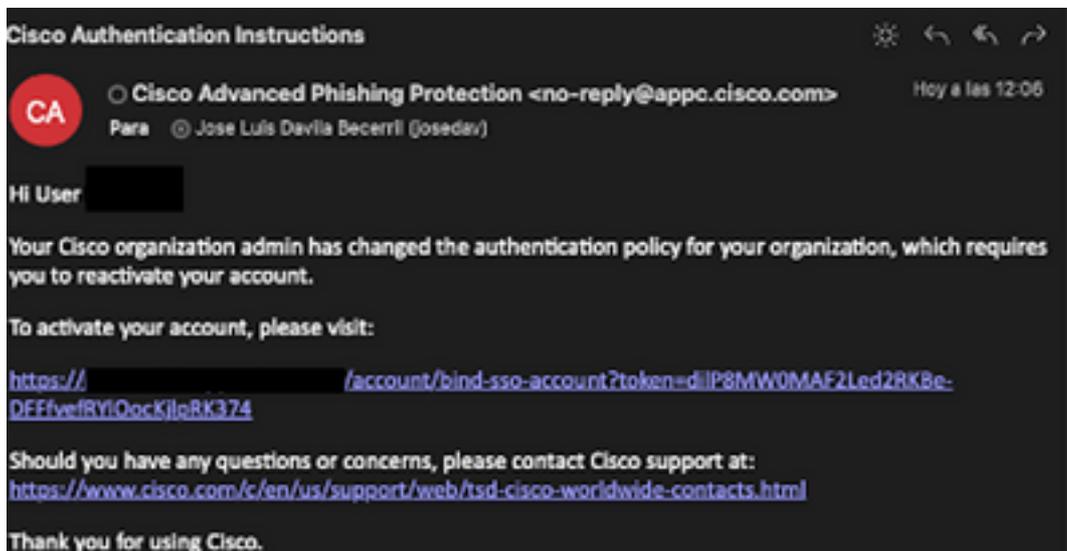
Wenn die Konfiguration keine Fehler enthält, wird der Eintrag Test Successful angezeigt, und die Einstellungen können jetzt gespeichert werden, wie im Bild gezeigt:



3. Einstellungen speichern

Überprüfung

1. Bestehende Administratoren, die SSO nicht verwenden, werden per E-Mail darüber informiert, dass die Authentifizierungsrichtlinie für die Organisation geändert wurde, und die Administratoren werden aufgefordert, ihr Konto über einen externen Link zu aktivieren, wie im Bild gezeigt:



2. Wenn das Konto aktiviert ist, geben Sie Ihre E-Mail-Adresse ein und dann werden Sie zur OKTA-Anmelde-Website weitergeleitet, um sich anzumelden, wie im Bild gezeigt:

Log In to Advanced Phishing Protection

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

Your Email:

[Next](#)

okta

Sign In

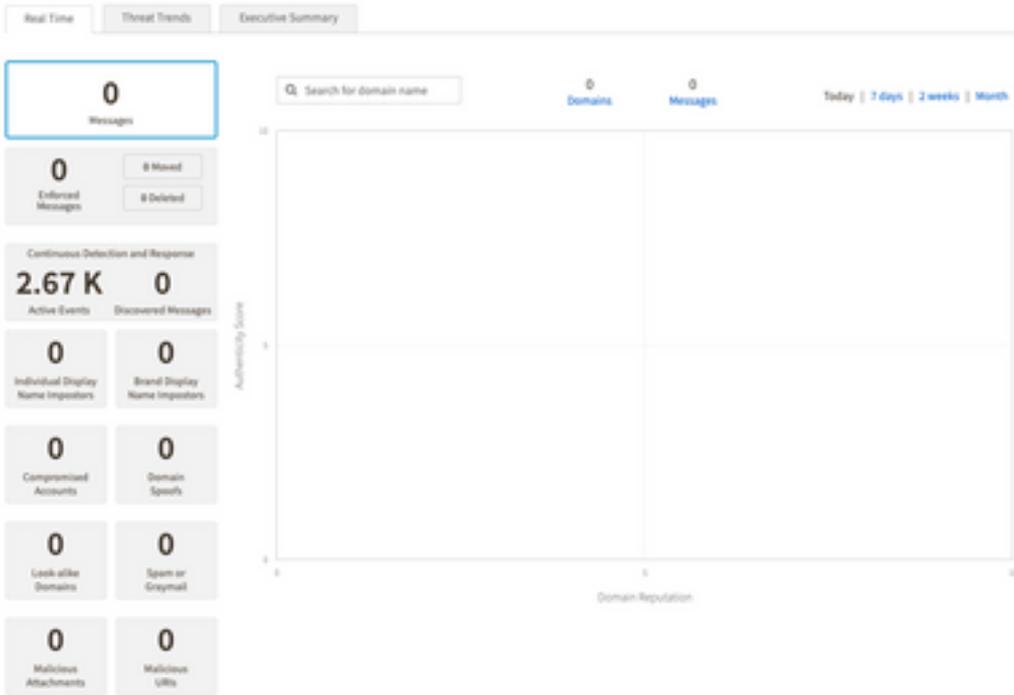
Username

Keep me signed in

[Next](#)

[Help](#)

3. Melden Sie sich nach Abschluss des OKTA-Anmeldevorgangs beim Cisco Advanced Phishing Protection-Portal an, wie im Bild gezeigt:



Zugehörige Informationen

[Cisco Advanced Phishing Protection - Produktinformationen](#)

[Cisco Advanced Phishing Protection - Benutzerhandbuch](#)

[OKTA-Unterstützung](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.