# Externe OKTA SSO-Authentifizierung für erweiterten Phishing-Schutz konfigurieren

## Inhalt



## 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

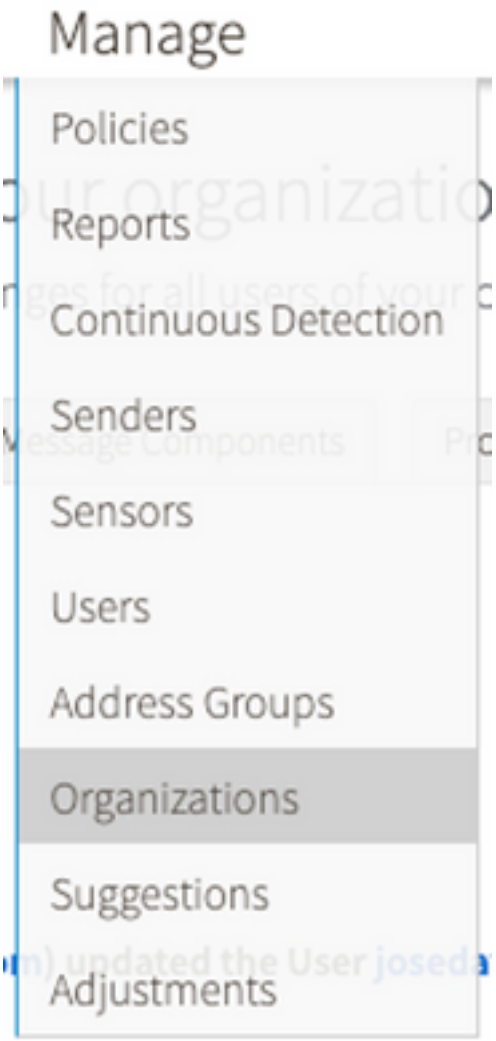
- Cisco Advanced Phishing Protection-Portal

- OKTA-Administratorkonto.

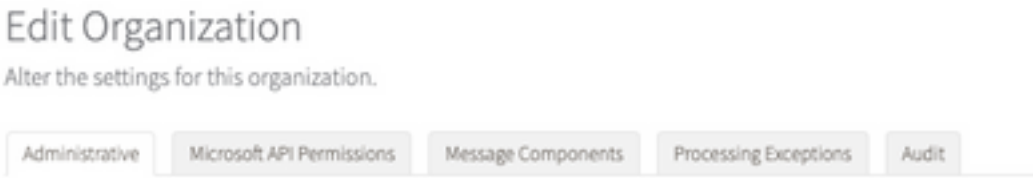
# Konfigurieren

**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:




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


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.

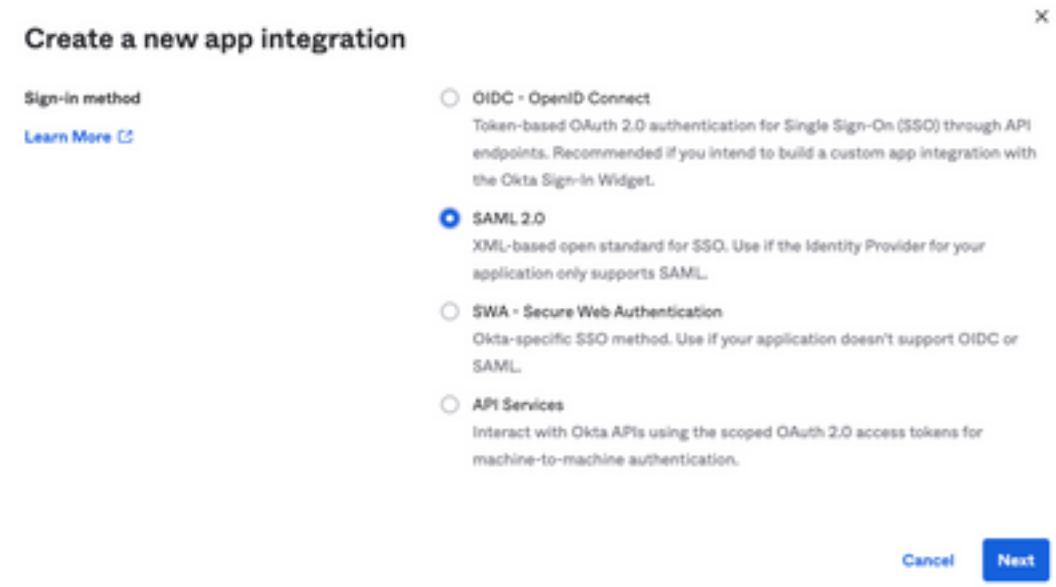
Wählen Sie das benannte E-**Mail-**Format aus, um eine E-Mail-Adresse für die Anmeldung zu verwenden, wie im Bild gezeigt:


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.

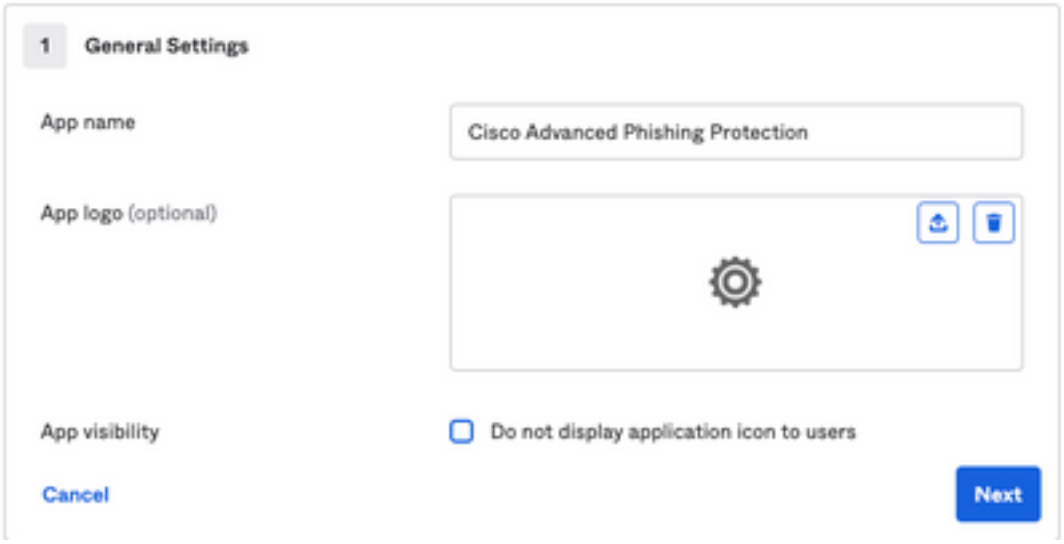
**Unter Okta.**

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


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




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




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

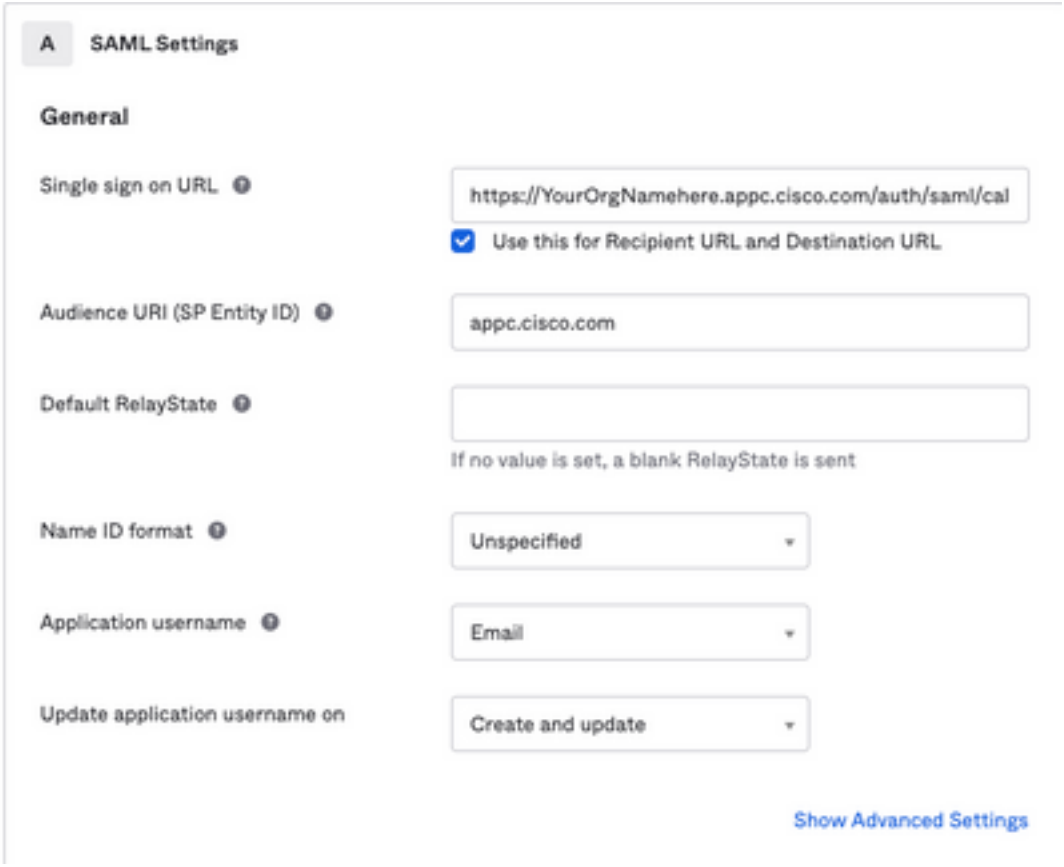
- URL für einmalige Anmeldung: Dies ist der Assertion Consumer Service von Cisco Advanced Phishing Protection.

- 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



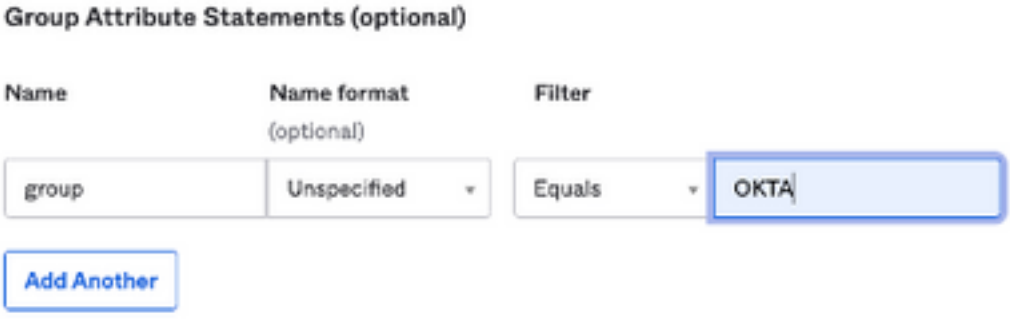

Blättern Sie nach unten zu **Gruppenattribut-Anweisungen (optional**), wie in der Abbildung dargestellt:

Geben Sie die nächste Attributanweisung ein:

-Name: gruppe

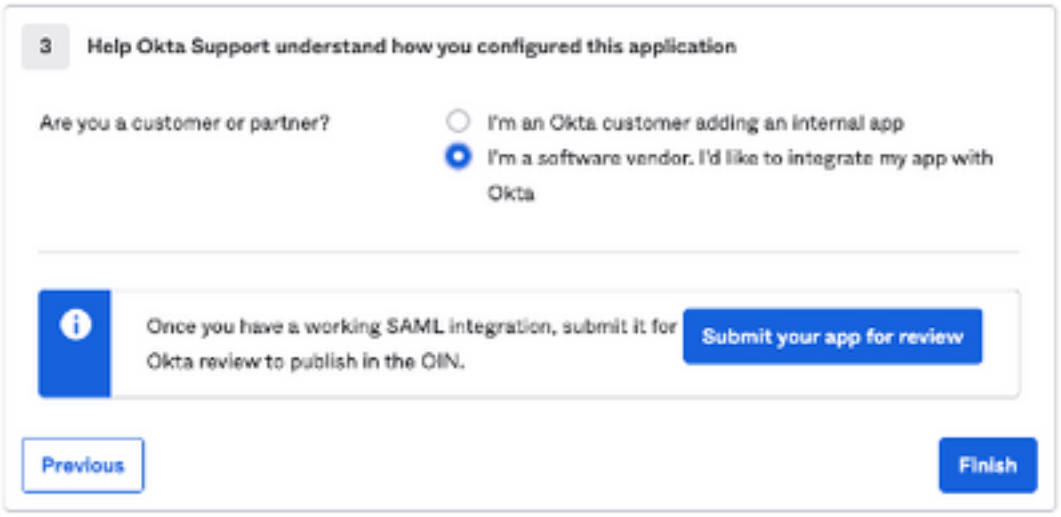
- Namensformat: Nicht angegeben.

- Filter: "Equals" und "OKTA"



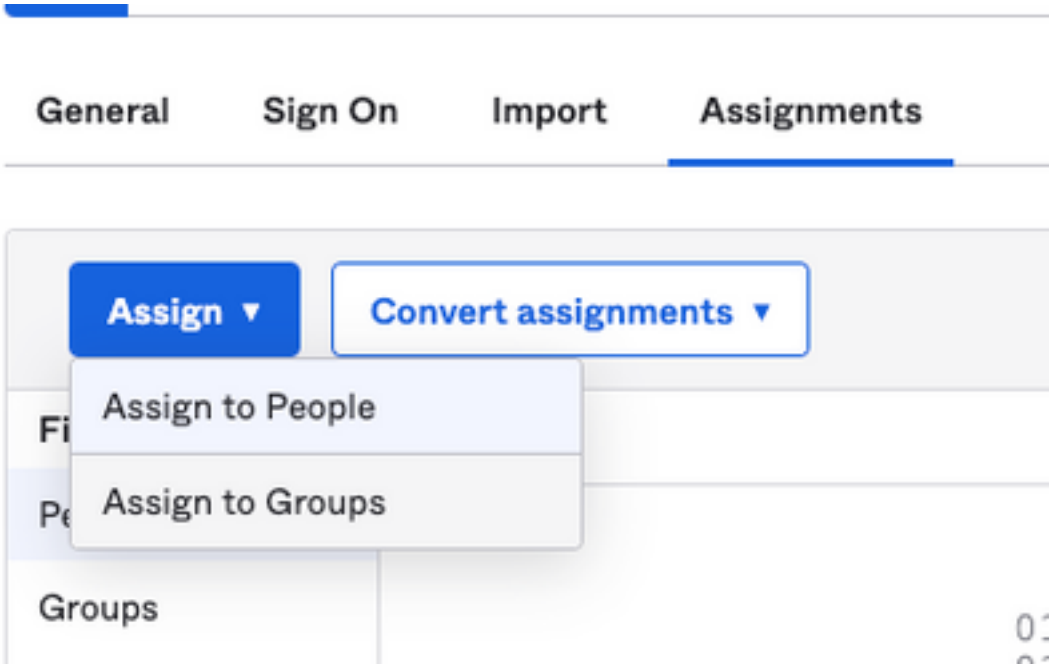

Wählen Sie Weiter aus.

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:



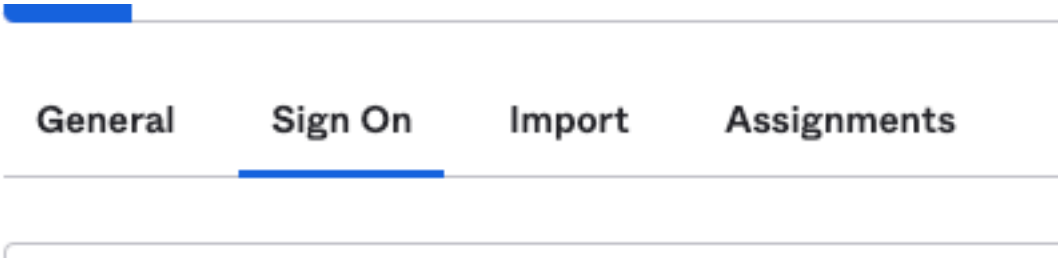

Wählen Sie **Beenden**, um mit dem nächsten Schritt fortzufahren.

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

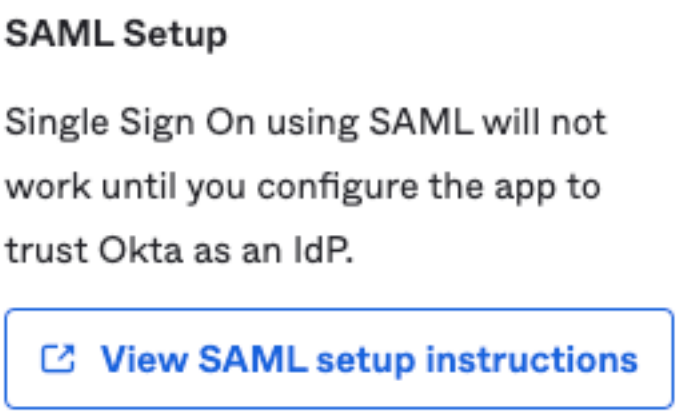



7. Wählen Sie die OKTA-Gruppe, d. h. die Gruppe mit den autorisierten Benutzern, um auf die Umgebung zuzugreifen.

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




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

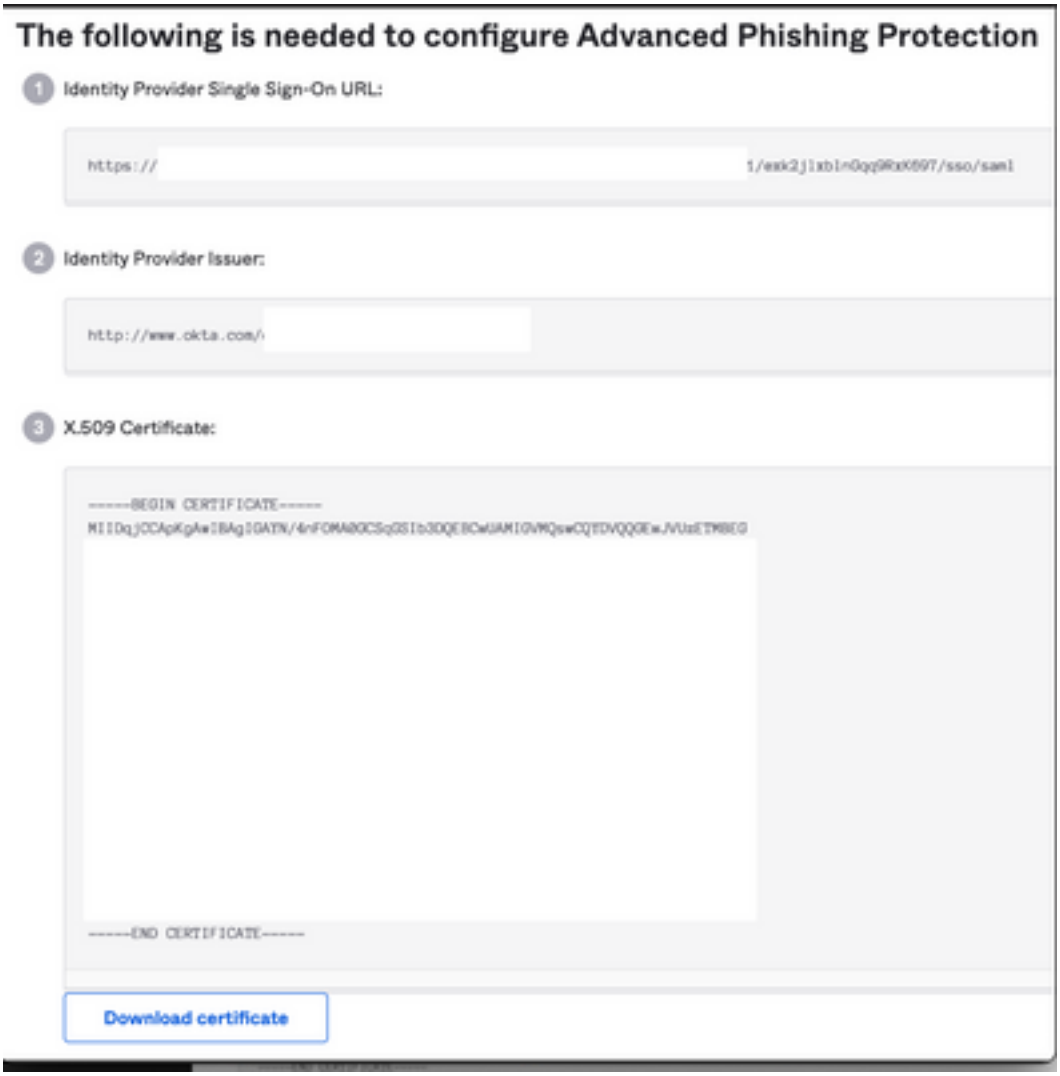



9. Speichern Sie auf einem Notizblock die nächsten Informationen, die erforderlich sind, um das Cisco Advanced Phishing Protection-Portal aufzurufen, wie im Bild gezeigt:

- Single-Sing-On-URL des Identitätsanbieters

- Identifizieren Sie einen Provider (nicht erforderlich für Cisco Advanced Phishing Protection, aber obligatorisch für andere Anwendungen).

- X.509-Zertifikat.



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

**Im Cisco Advanced Phishing Protection-Portal:**

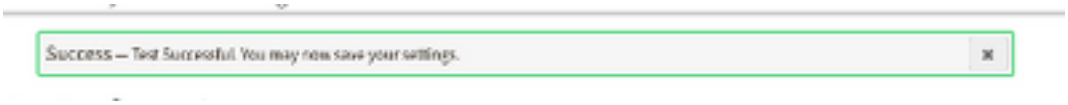
1. Geben Sie unter Name bezeichner Format die folgenden Informationen ein:

- 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.

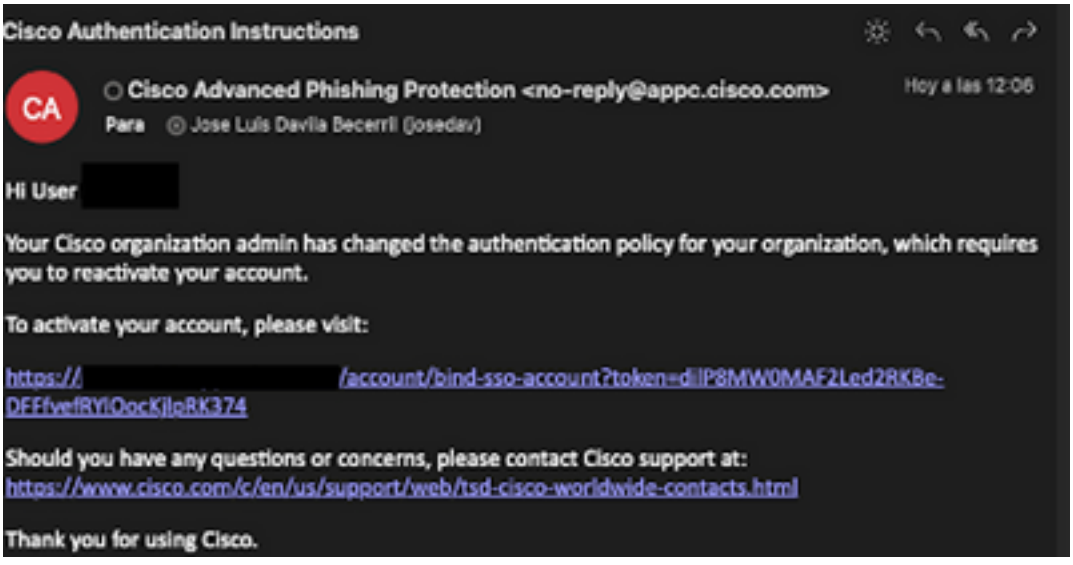
Wenn die Konfiguration keine Fehler enthält, wird der Eintrag Test Successful angezeigt, und die Einstellungen können jetzt gespeichert werden, wie im Bild gezeigt:



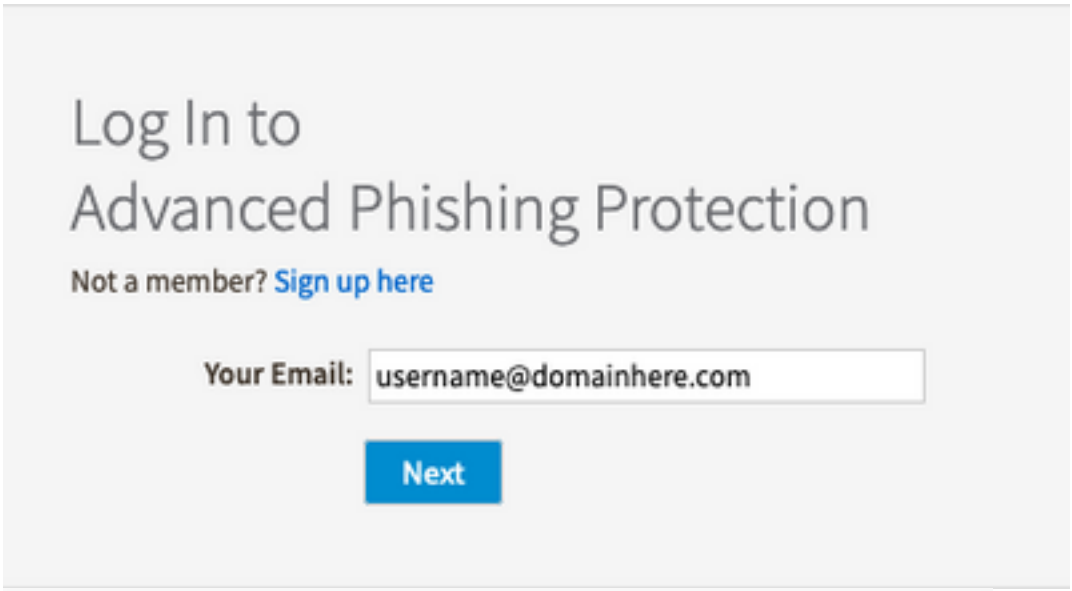

3. Einstellungen speichern

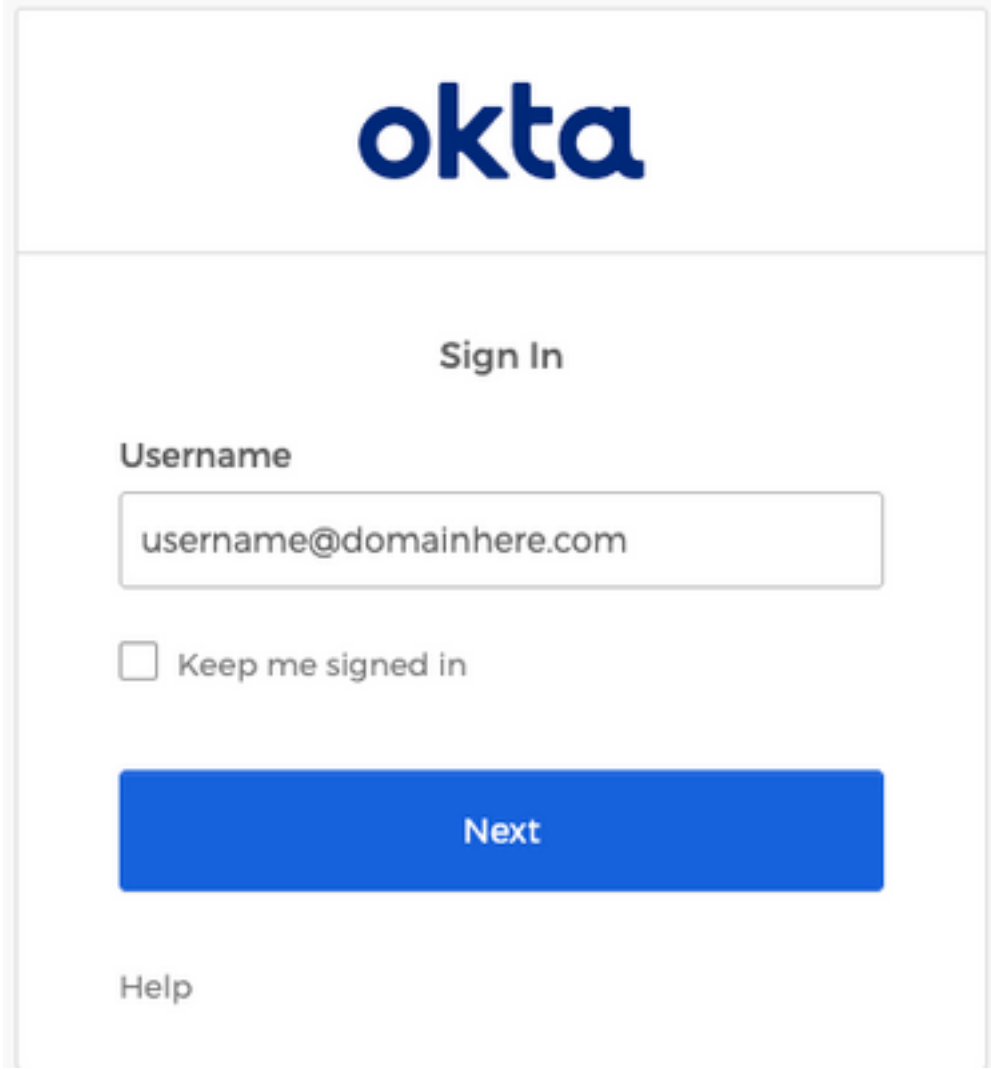
# Überprüfung

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:

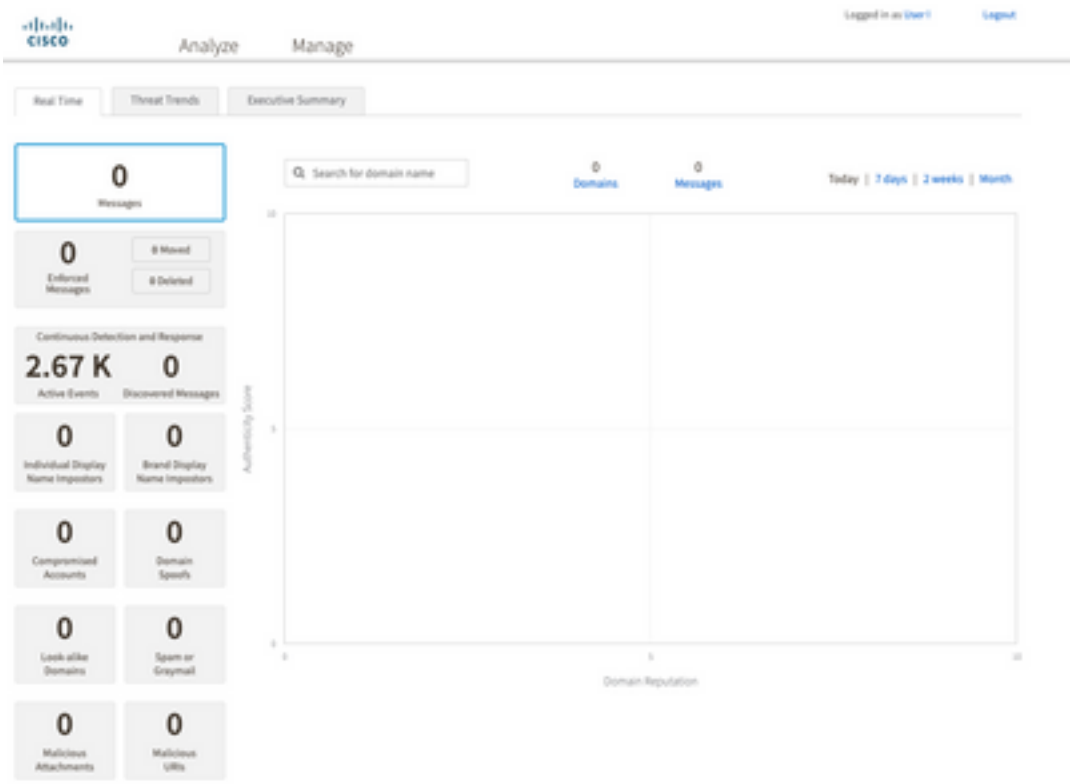



2. Wenn das Konto aktiviert ist, geben Sie Ihre E-Mail-Adresse ein und dann werden Sie zur OKTA-Anmelde-Website weitergeleitet, um sich anzumelden, wie im Bild gezeigt:




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.