配置OKTA SSO外部身份验证以实现高级网络钓鱼保护

目录

简介

本文档介绍如何配置OKTA SSO外部身份验证以登录思科高级网络钓鱼防护。

先决条件

管理员有权访问思科高级网络钓鱼防护门户。

Okta idP的管理员访问权限。

自签名或CA签名（可选）PKCS或PEM格式的X.#12 SSL证书。

背景信息

- 思科高级网络钓鱼防护允许管理员使用SAML启用SSO登录。
- OKTA是一个身份管理器，为您的应用提供身份验证和授权服务。
- 思科高级网络钓鱼防护可以设置为连接到OKTA进行身份验证和授权的应用。
- SAML是基于XML的开放标准数据格式，使管理员能够在登录到其中某个应用程序后，无缝访问一组定义的应用程序。
- 要了解有关SAML的更多信息，您可以访问下一个链接:SAML一般信息

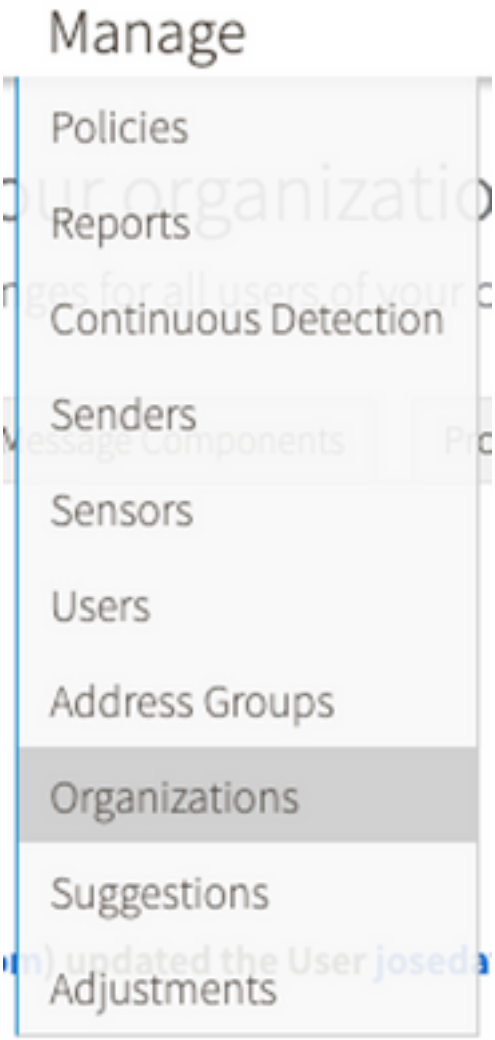
要求

- 思科高级网络钓鱼防护门户。
- OKTA管理员帐户。

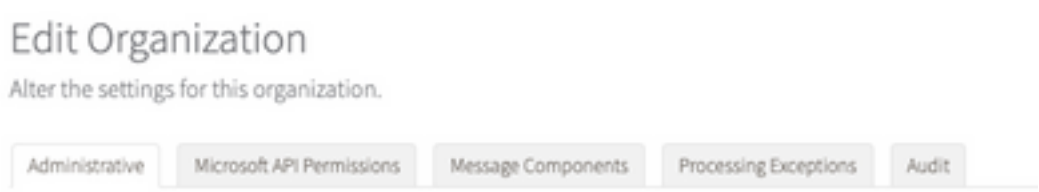
配置

在思科高级网络钓鱼防护门户下：

1.登录到您的组织门户，然后选择**Manage** > **Organizations**，如图所示：



2.选择您的组织名称**编辑组织**，如图所示：



3.在**管理**选项卡上，向下滚动到**用户帐户设置**，然后在SSO下选择**启用**，如图所示：

4.下一个窗口提供要在OKTA SSO配置下输入的信息。将以下信息粘贴到记事本，使用它来配置OKTA设置：

— 实体ID:apcc.cisco.com

— 断言消费者服务：此数据针对您的组织量身定制。

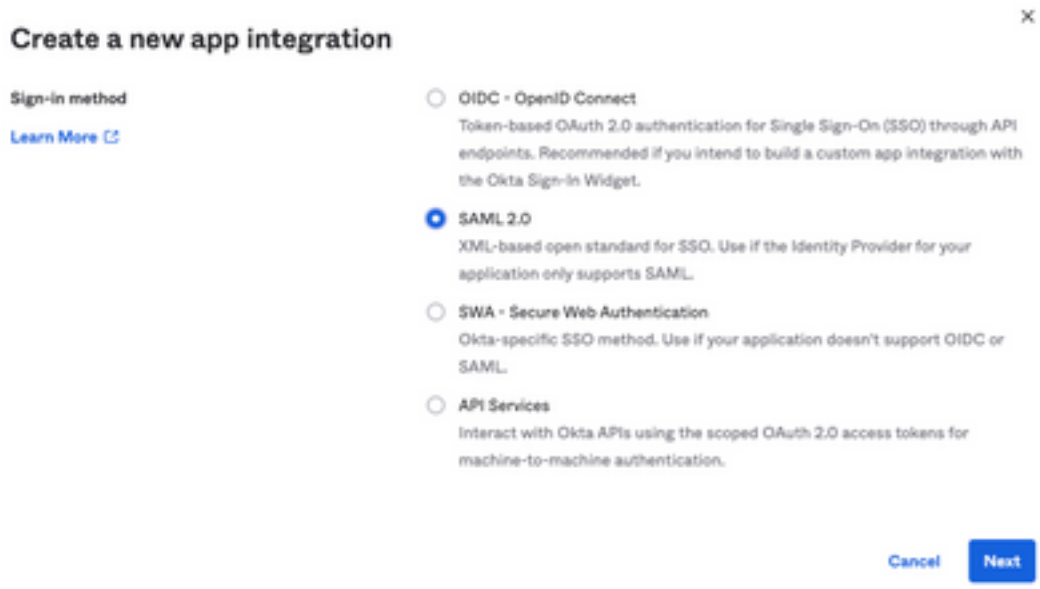
选择指定格式**的电**子邮件，以使用电子邮件地址登录，如图所示：

5.目前尽可能减少思科高级网络钓鱼防护配置，因为您需要首先在OKTA中设置应用程序，然后再继续下一步。

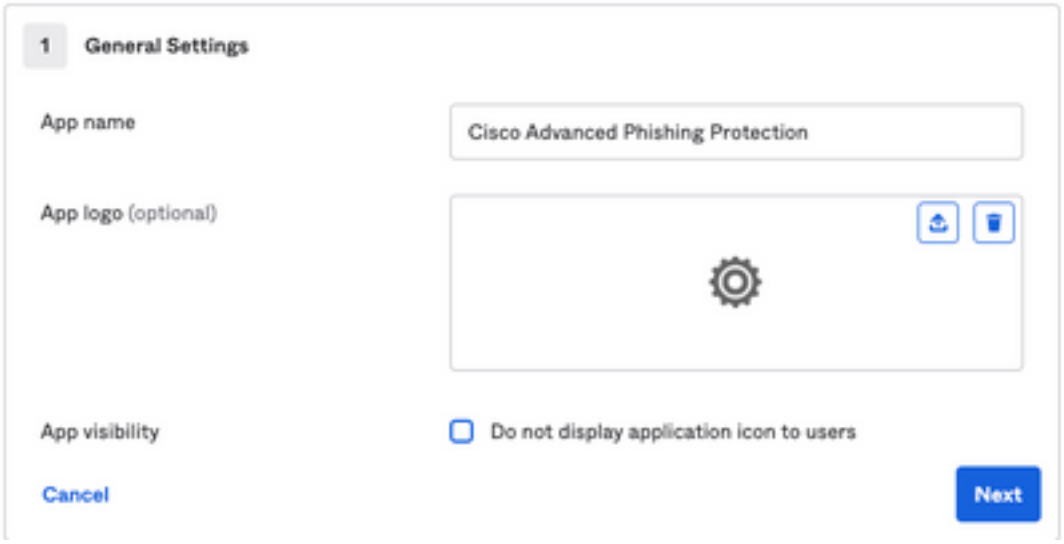
在Okta下。

1.定位至“应用程序”门户，然后选择**创建应用程序集成**，如图所示：

2.选择**SAML 2.0**作为应用类型，如图所示：



3.输入应用名称**高级网络钓鱼**保护，然**后选**择**Next**，如图所示：



4.在SAML设置下，填补空白，如图所示：

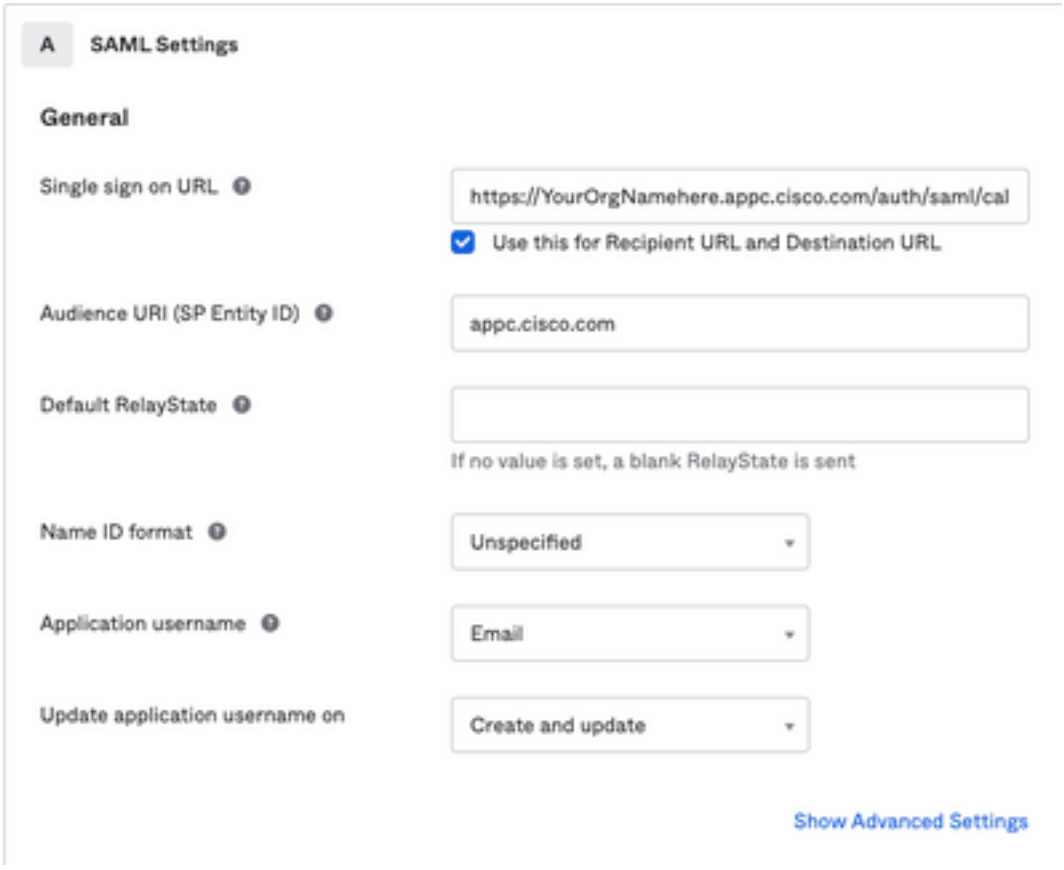
— 单点登录URL:这是从思科高级网络钓鱼防护获取的断言消费者服务。

— 收件人URL:这是从思科高级网络钓鱼防护获取的实体ID。

— 名称ID格式：将其保留为“未指定”(Unspecified)。

— 应用程序用户名：电子邮件，提示用户在身份验证过程中输入其电子邮件地址。

— 更新应用程序用户名：创建和更新。



向下滚动到**Group Attribute Statements(可选)**，如图所示：

输入下一个属性语句：

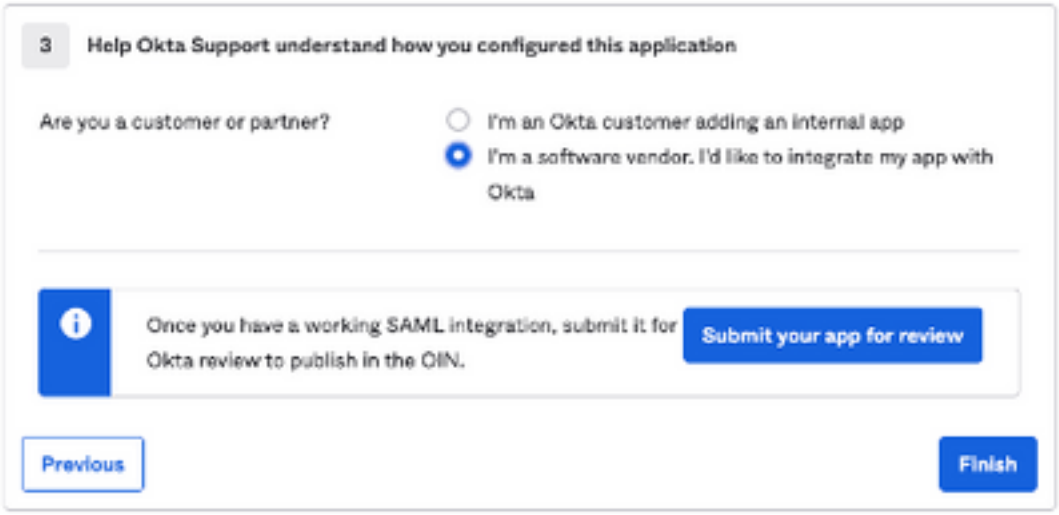
-姓名 :组

-姓名格式:未指定。

— 过滤器：“等于”和“OKTA”

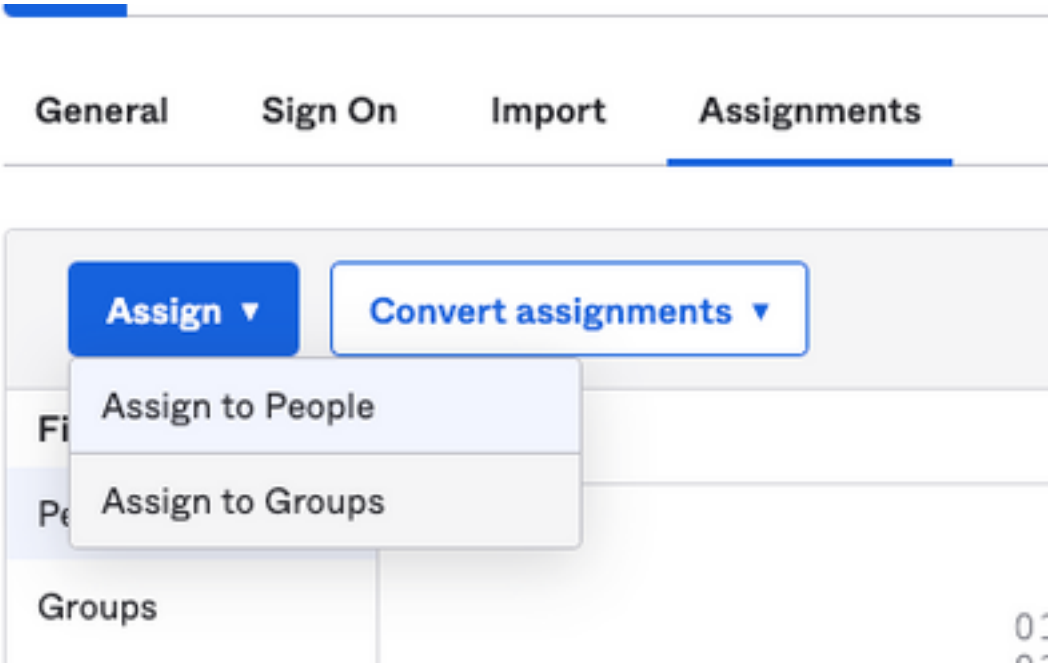
选择 Next（下一步）。

5.当要求帮助Okta了解如何配置此应用程序时，请输入当前环境的适用原因，如图所示：



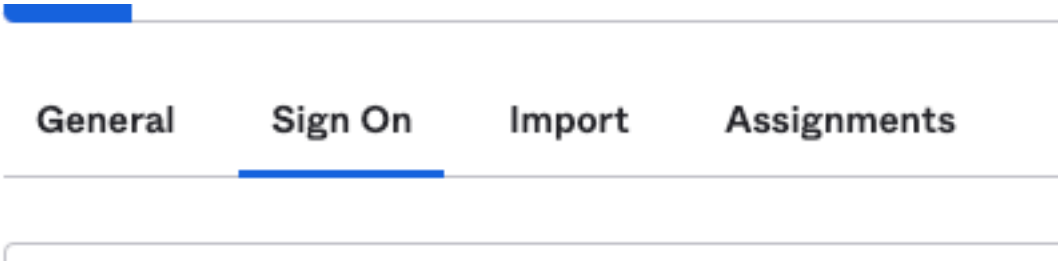
选择**Finish**继续下一步。

6.选择**分配**标签，然后选择**分配 > 分配到组**，如图所示：

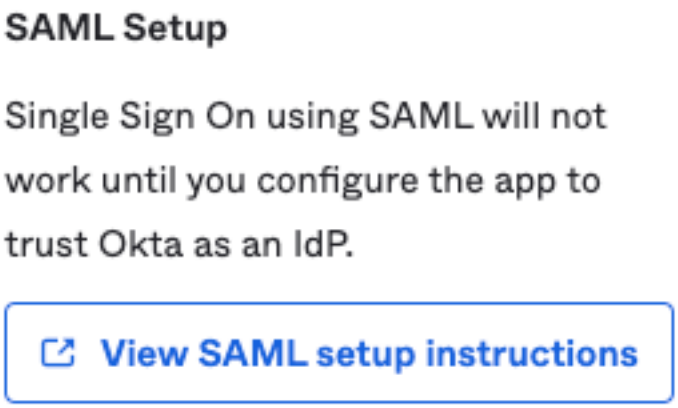


7.选择OKTA组，该组是授权用户访问环境的组

8.选择**登录**，如图所示：



9.向下滚动到右角，输入**查看SAML设置说明**选项，如图所示：

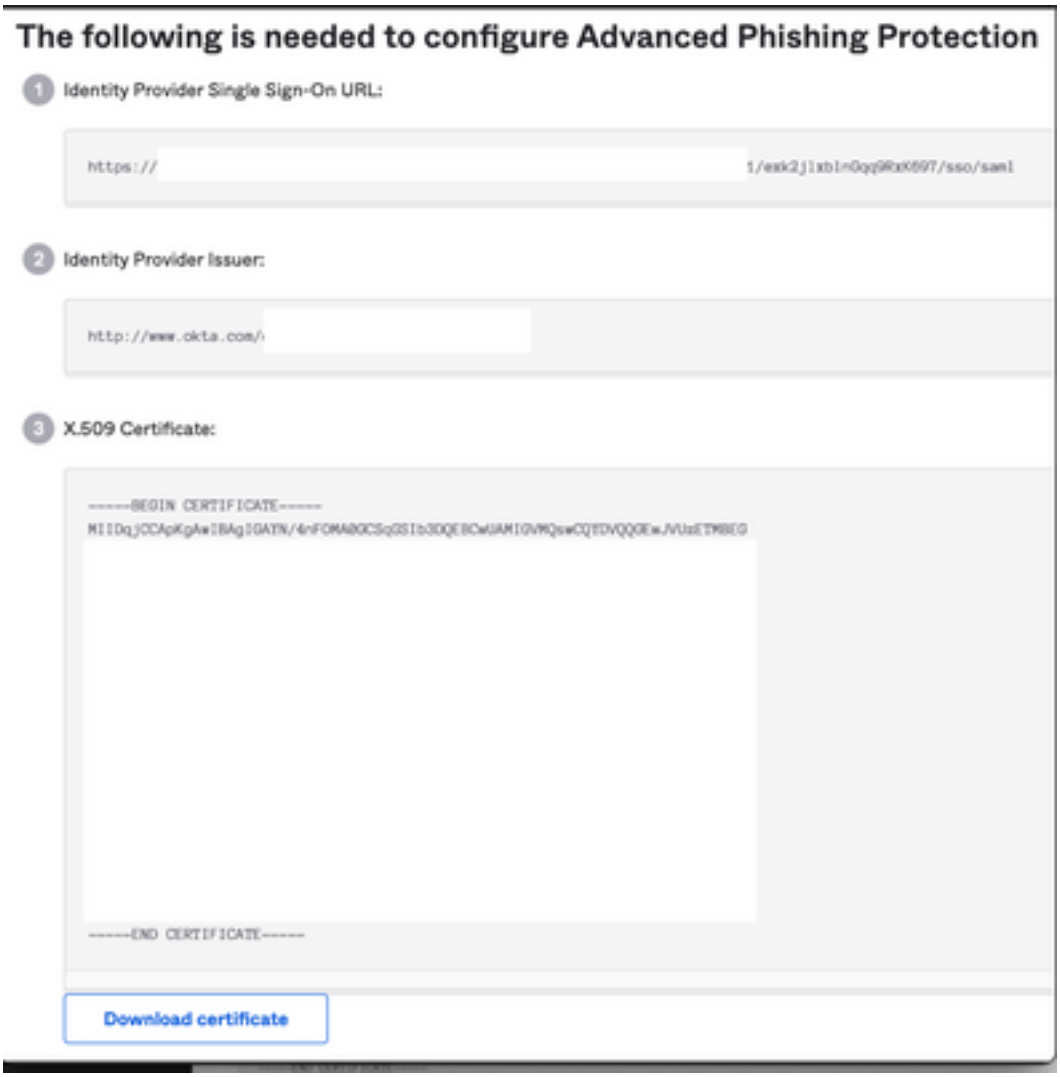


9.将思科高级网络钓鱼防护门户所需的下一个信息保存到记事本，如图所示：

— 身份提供程序单点登录URL。

— 确定提供商颁发者（对于思科高级网络钓鱼防护来说不是必需的，但对于其他应用而言是必需的）。

- X.509证书。



10.完成OKTA配置后，您可以返回到思科高级网络钓鱼防护

在思科高级网络钓鱼防护门户下：

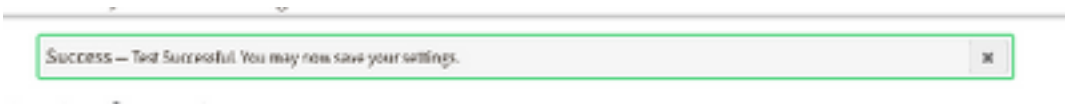
1.使用名称标识符格式，输入以下信息：

- SAML 2.0终端（HTTP重定向）：Okta提供的识别提供程序单点登录URL。

— 公共证书：输入Okta提供的X.509证书。

2.选择**测试设置**以验证配置是否正确

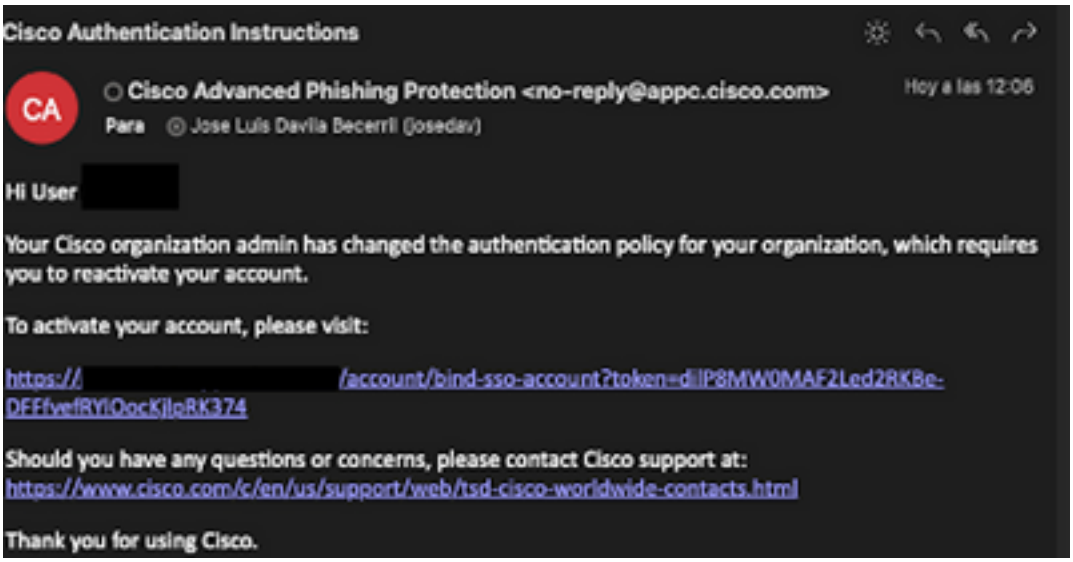
如果配置中没有错误，您将看到“测试成功”条目，现在可以保存设置，如图所示：



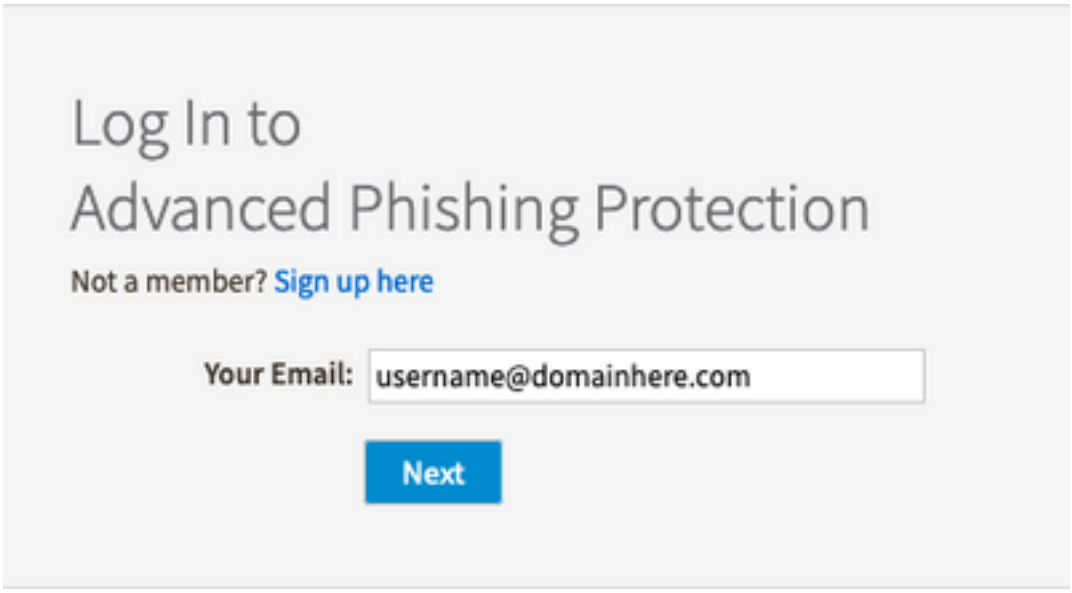
3.保存设置

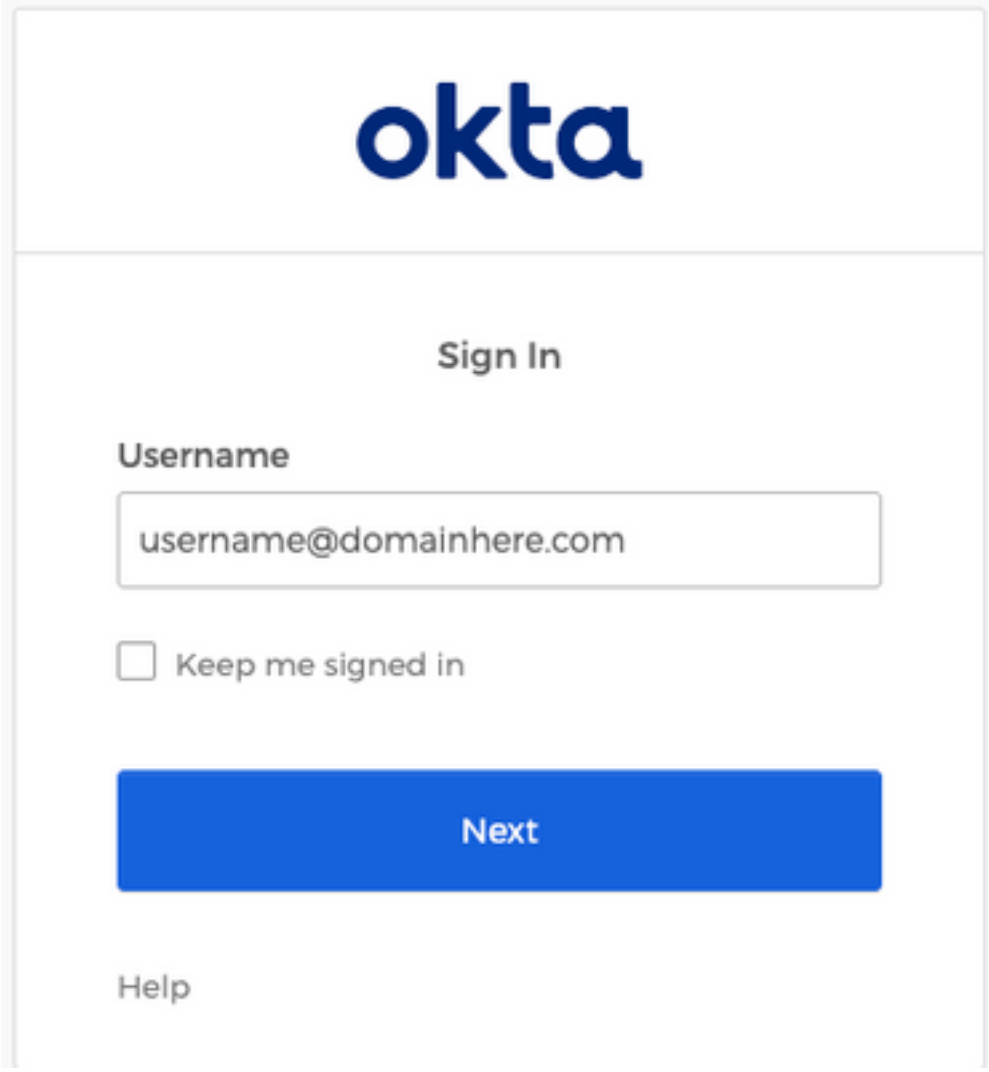
验证

1.对于不使用SSO的任何现有管理员，系统会通过电子邮件通知他们组织的身份验证策略已更改，并要求管理员使用外部链接激活其帐户，如图所示：

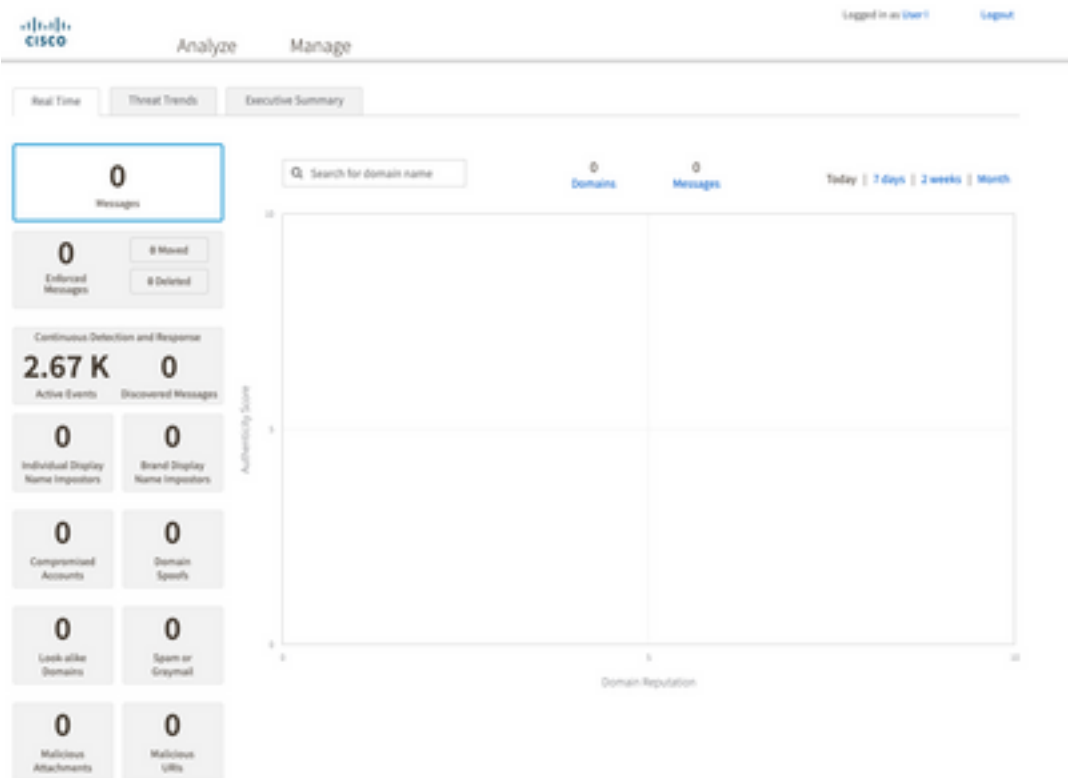


2.激活帐户后，请输入您的电子邮件地址，然后它将您重定向到OKTA登录网站进行登录，如图所示：





3.完成OKTA登录过程后，登录思科高级网络钓鱼防护门户，如图所示：



相关信息

思科高级网络钓鱼防护 — 产品信息

思科高级网络钓鱼防护 — 最终用户指南

OKTA支持

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。