配置最终用户垃圾邮件隔离区的OKTA SSO

目录

简介

本文档介绍如何配置OKTA SSO以登录到安全管理设备的最终用户垃圾邮件隔离区。

先决条件

- 管理员对思科安全管理设备的访问权限。
- OKTA的管理员访问权限。
- 自签名或CA签名（可选）PKCS #12或PEM格式（由OKTA提供）的X.509 SSL证书。

背景信息

思科安全管理设备为使用最终用户垃圾邮件隔离区的最终用户启用SSO登录，并与OKTA集成，OKTA是一种身份管理器，可为您的应用提供身份验证和授权服务。思科最终用户垃圾邮件隔离区可以设置为连接到OKTA进行身份验证和授权的应用，并使用SAML(基于XML的开放标准数据格式，使管理员能够在登录其中一个应用后无缝访问一组定义的应用。

要了解有关SAML的详细信息，请参阅SAML一般信息

组件

- 思科安全管理设备云管理员帐户。
- OKTA管理员帐户。

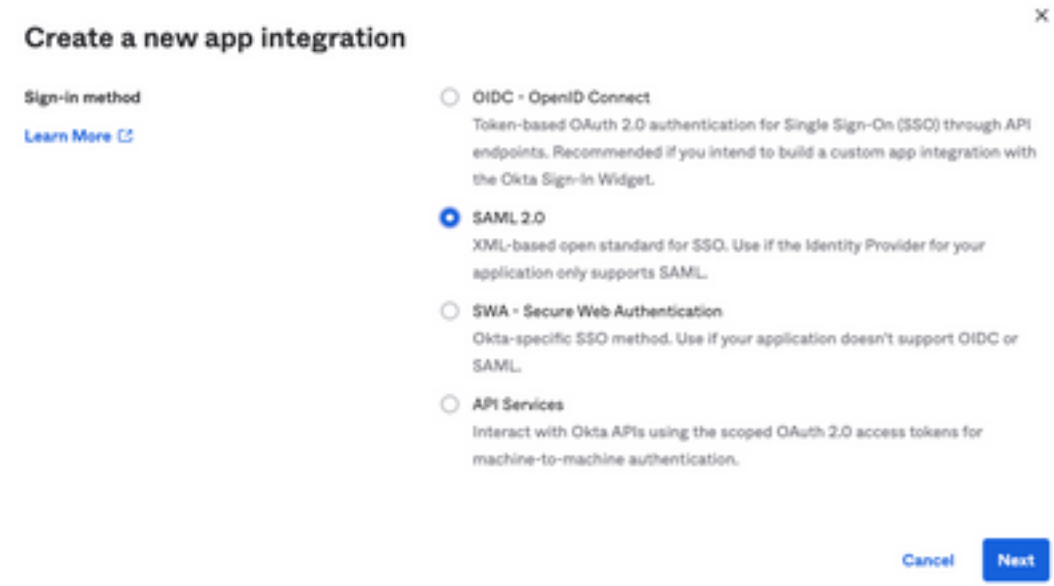
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备都以清除（默认）配置开头。如果网络处于活动状态，请确保您了解任何命令的潜在影响。

配置

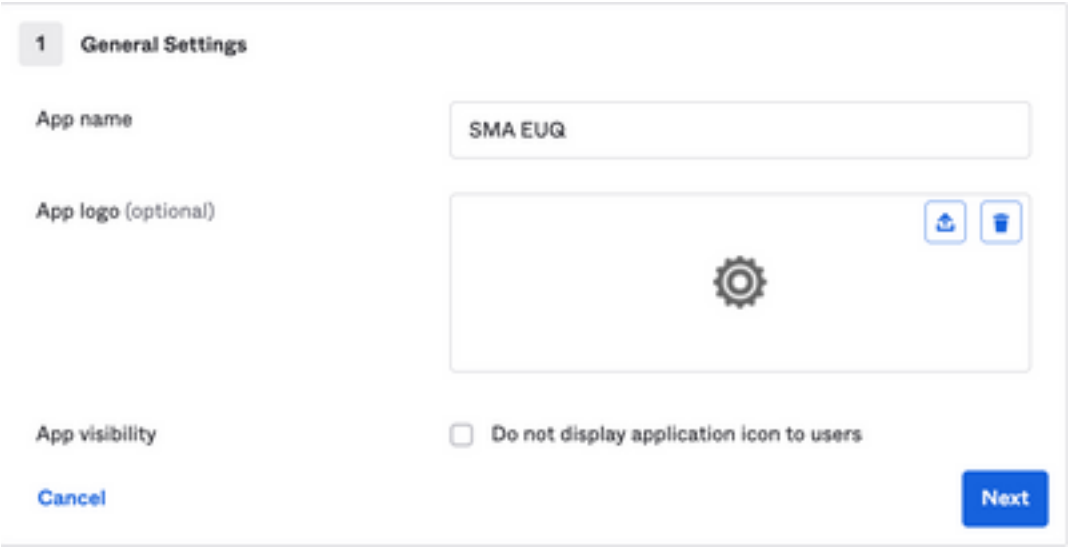
在Okta下。

1.定位至“应用程序”门户，然后选择 Create App Integration ,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 SMA EUQ 选择 Next,如图所示:



4.在 SAML settings，如图所示，填空隙：

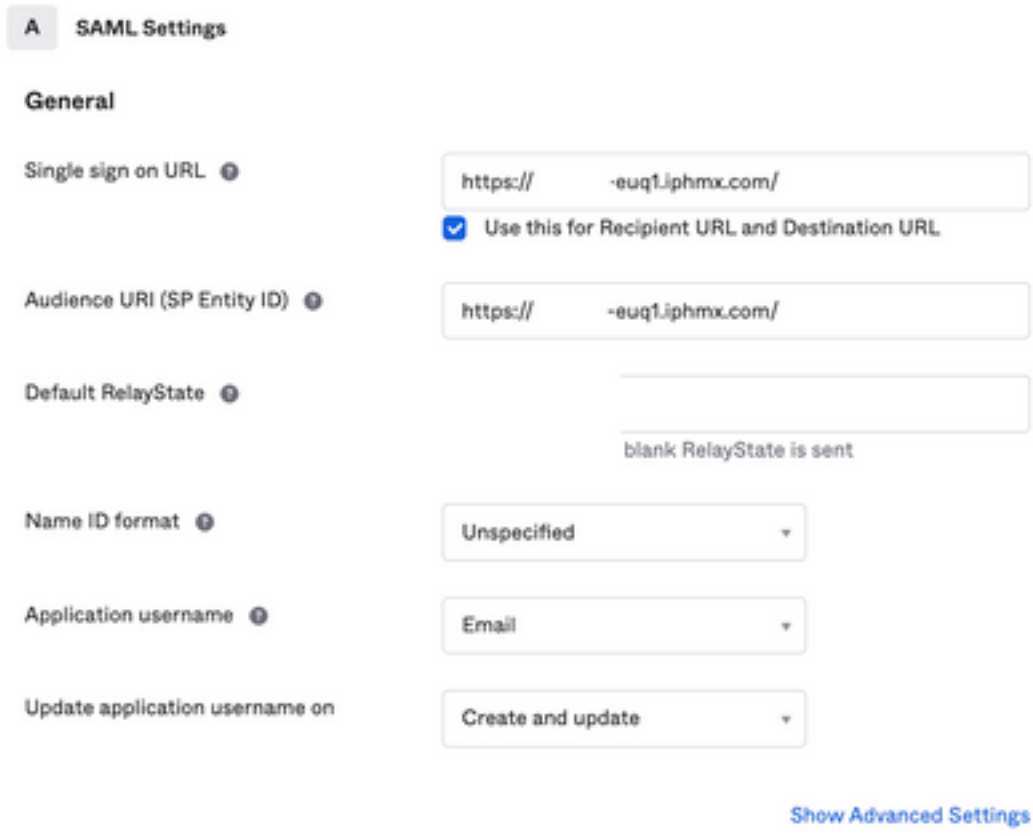
— 单点登录URL：这是从SMA EUQ接口获取的声明使用者服务。

— 受众URI（SP实体ID）：这是从SMA EUQ实体ID获取的实体ID。

— 名称ID格式：保留为未指定。

— 应用用户名：提示用户在身份验证过程中输入其电子邮件地址的电子邮件。

— 更新上的应用程序用户名：创建和更新。



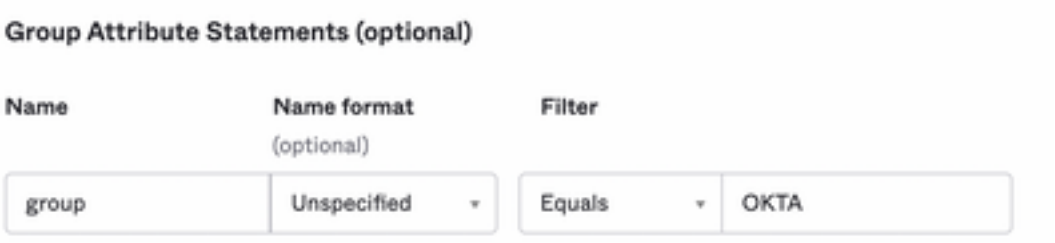
向下滚动到 Group Attibute Statements (optional) ,如图所示:

输入下一个属性语句：

-姓名：group

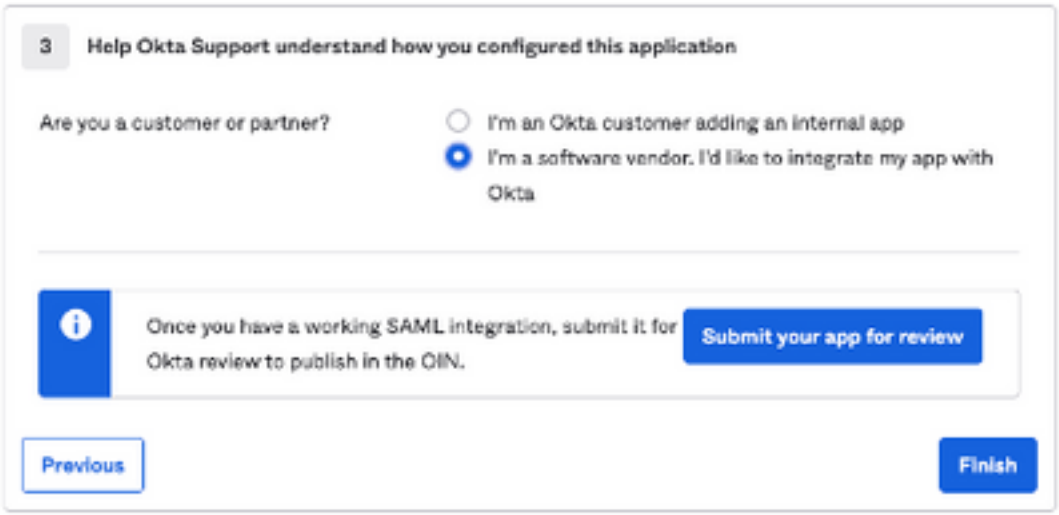
-姓名格式: Unspecified

— 过滤器： Equals 和 OKTA



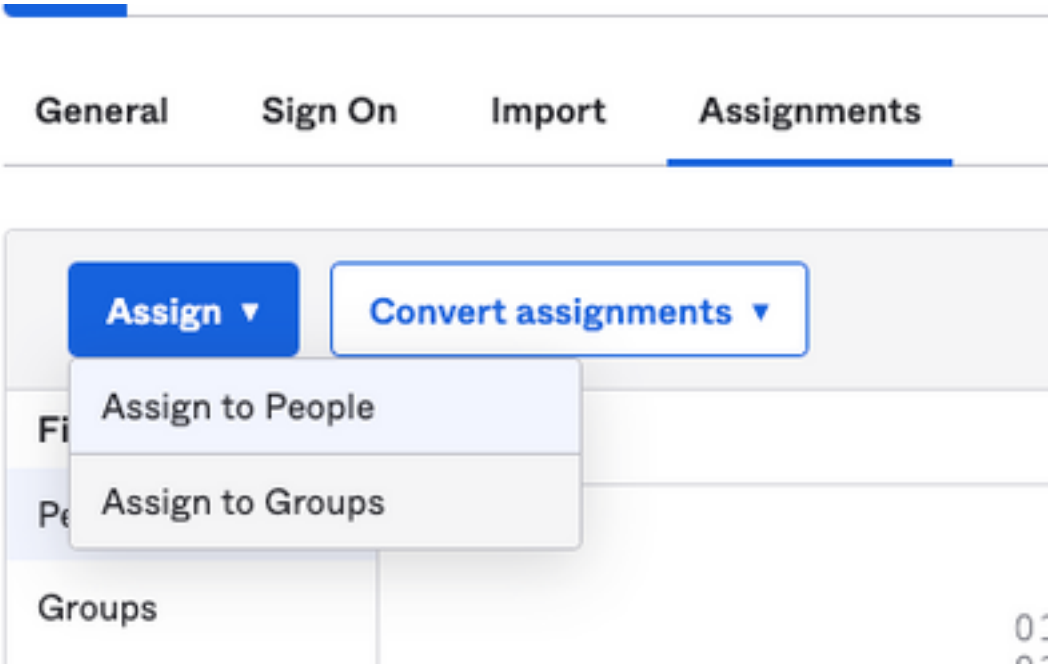
选择 Next .

5.当被要求时 Help Okta to understand how you configured this application ，请输入当前环境的适用原因 ，如图所示：



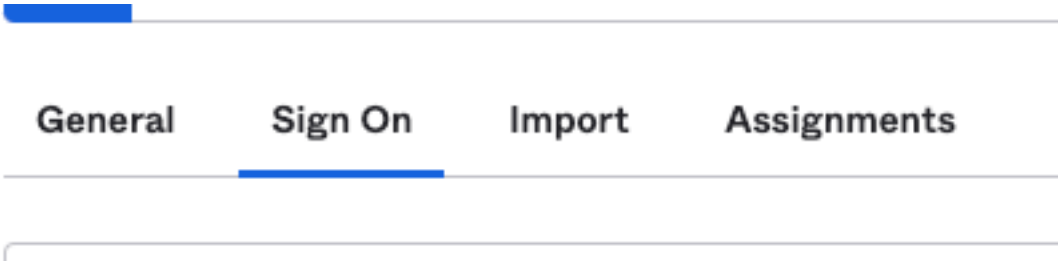
选择 Finish 继续下一步。

6.选择 Assignments 选项卡，然后选择 Assign > Assign to Groups,如图所示:

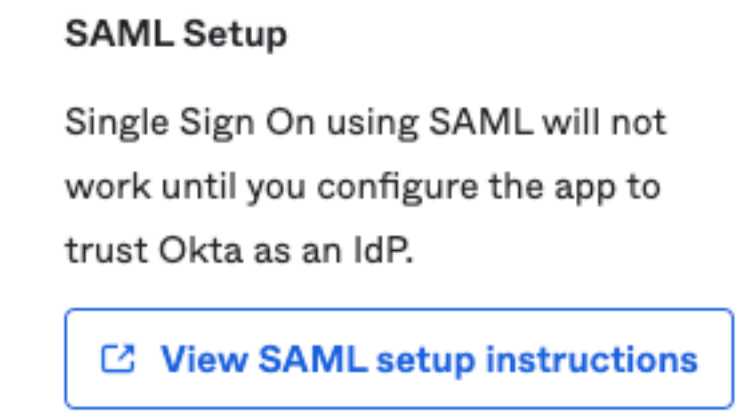


7.选择OKTA组，该组是授权用户访问环境的组

8.选择 Sign On ,如图所示:



9.向下滚动至右角，选择 View SAML setup instructions 选项，如图所示：

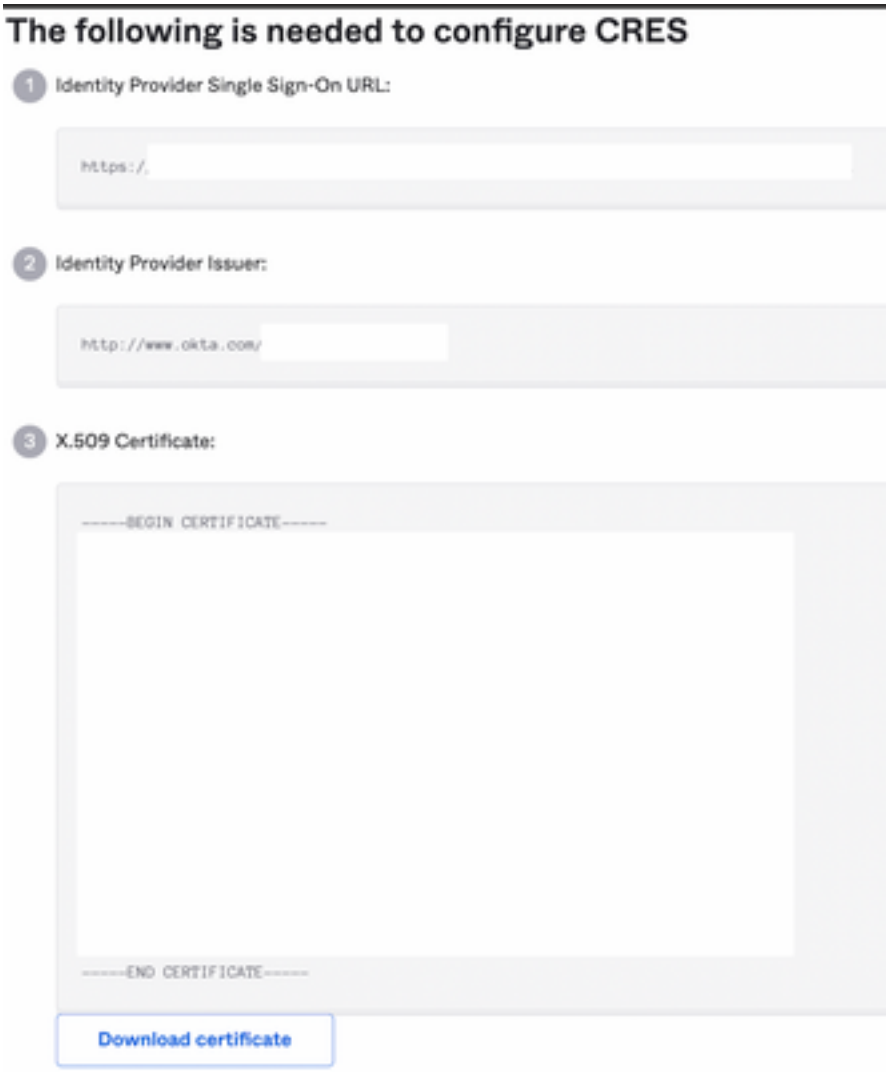


10.将此信息保存到记事本，需要放入 Cisco Security Management Appliance SAML配置，如图所示：

— 身份提供程序单点登录URL

— 身份提供程序颁发者

- X.509证书

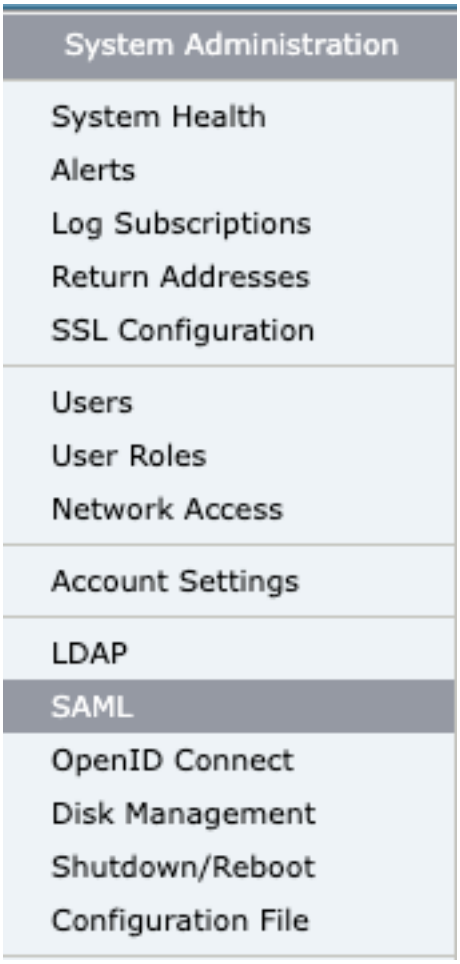


11.完成OKTA配置后，您可以返回思科安全管理设备。

在思科安全管理设备下：

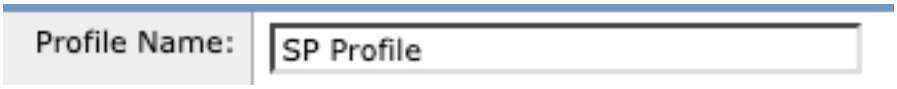
1.以云管理员身份登录思科安全管理设备，如图所示：

2.在 System Administration选项卡中，选择 SAML 选项，如图所示：



3.打开新窗口以配置SAML。低于 SAML for End-User Quarantine，点击 Add Service Provider ,如图所示:

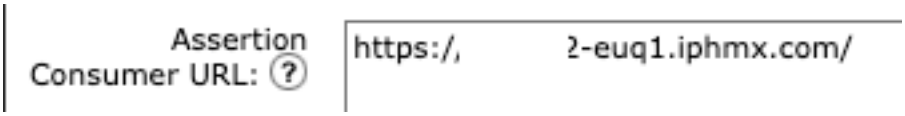
4.不足 Profile Name ，输入服务提供商配置文件的配置文件名，如图所示：



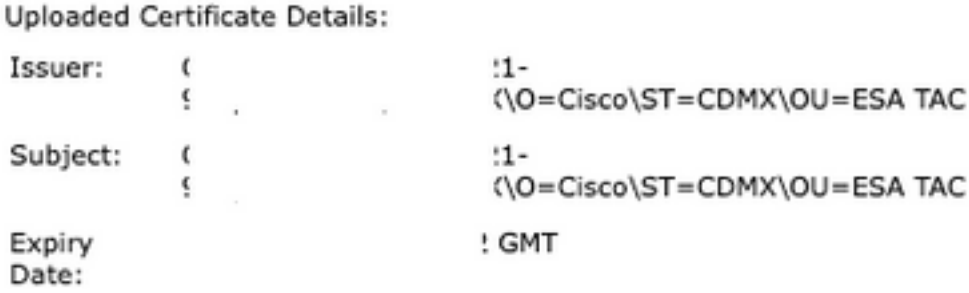
5.对于 Entity ID ,输入服务提供商（在本例中为设备）的全局唯一名称。服务提供商实体ID的格式通常是URI，如图所示：

6.对于 **Name ID Format** ,此字段不可配置。配置身份提供程序时需要此值，如图所示：

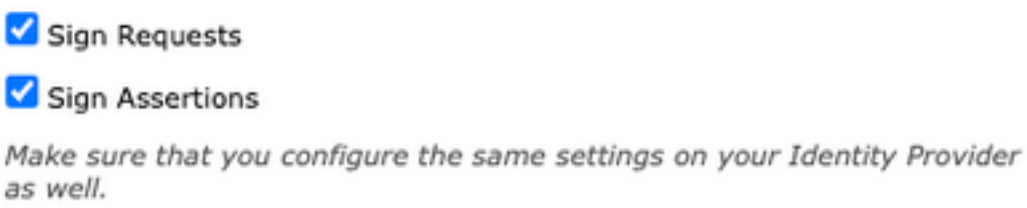
7.对于 **Assertion Consumer URL**，输入身份提供程序在身份验证成功完成后向其发送SAML声明的URL。在本例中，这是垃圾邮件隔离区的URL。



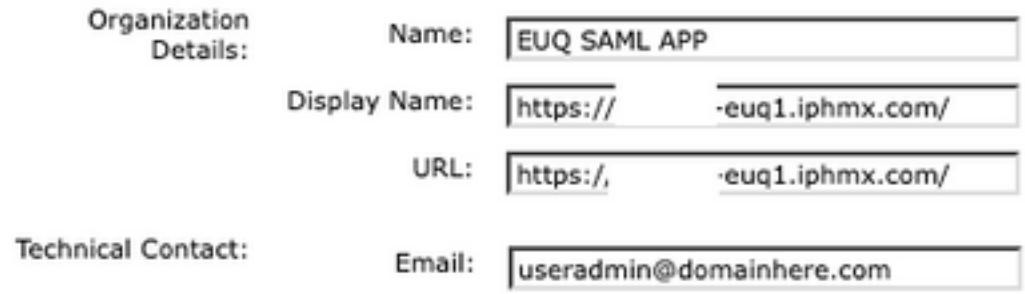
8.对于 SP Certificate ，上传证书和密钥，或上传PKCS #12文件。上传后， Uploaded Certificate Details 如图所示：



9.对于 Sign Requests and Sign Assertions ，如果要对SAML请求和断言进行签名，请选中这两个复选框。如果选择选中这些选项，请确保在OKTA上配置相同的设置，如图所示：

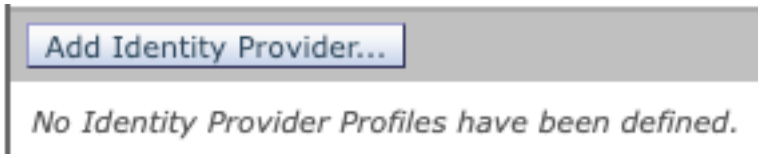


10.对于 Organization Details，输入组织的详细信息，如图所示：



11. Submit 和 Commit 更改后再继续配置 Identity Provider Settings .

12.不足 SAML ，单击 Add Identity Provider,如图所示:



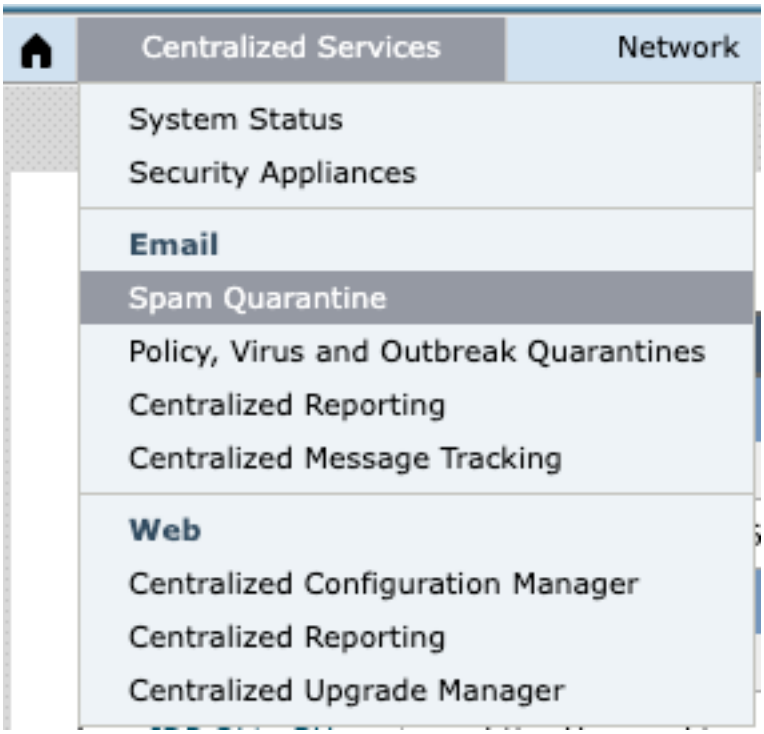
13.不足 Profile Name: 输入身份提供程序配置文件的名称，如图所示：

14.选择 Configure Keys Manually 并输入以下信息，如图所示：

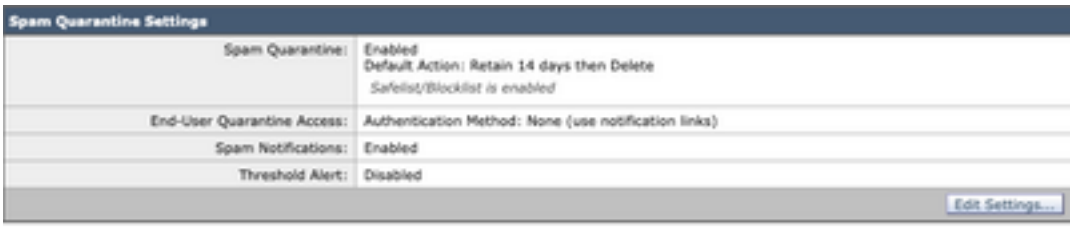
- 实体ID：身份提供程序实体ID用于唯一标识身份提供程序。它通过上述步骤中的OKTA设置获得。
- SSO URL:SP应向其发送SAML身份验证请求的URL。它通过上述步骤中的OKTA设置获得。
- 证书：由OKTA提供的证书。

15. Submit 和 Commit 更改以继续SAML登录激活。

16.不足 Centralized Services > Email ，单击 Spam Quarantine,如图所示:



17.不足 Spam Quarantine - > Spam Quarantine Settings ，单击 Edit Settings ，as shown in the image:



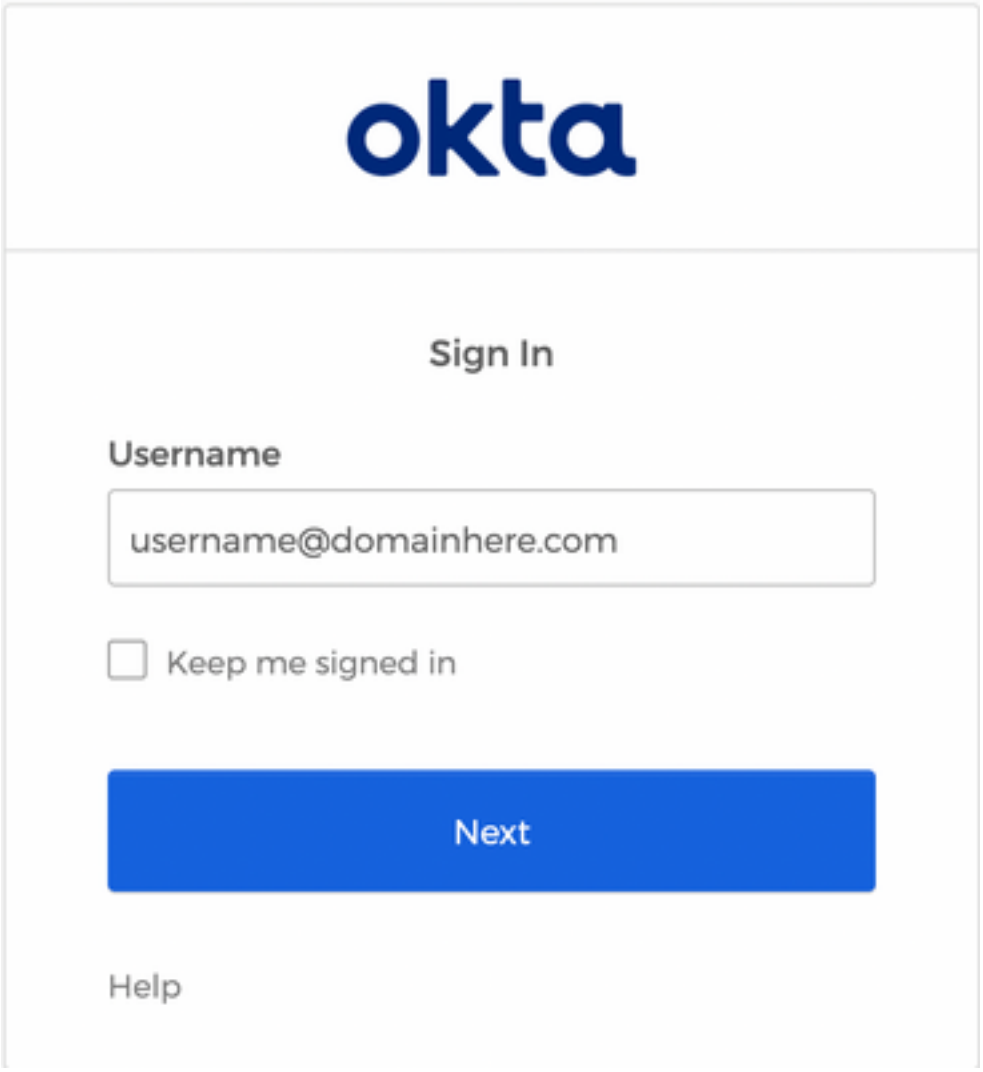
18.向下滚动到 End-User Quarantine Access > End-User Authentication ,选择 SAML 2.0 ,如图所示:

19. Submit 和 Commit 为启用SAML身份验证的更改 **End User Spam Quarantine** .

验证

1.在任何Web浏览器中，输入公司的最终用户垃圾邮件隔离区的URL，如图所示：

2.打开一个新窗口以继续OKTA身份验证。使用**OKTA凭证**登录，如图所示：



3.如果身份验证成功， End User Spam Quarantine 为登录用户打开垃圾邮件隔离区的内容，如图所示：

现在，最终用户可以使用OKTA凭证访问最终用户垃圾邮件隔离区。.

相关信息

Cisco Secure Email and Web Manager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）。