为SMA最终用户隔离配置Okta SAML SSO

目录

简介

本文档介绍如何将Okta配置为Cisco安全邮件SMA最终用户隔离访问的SAML 2.0身份提供程序。

先决条件

- 产品:思科安全邮件安全管理设备(SMA)
- 功能：最终用户隔离区(EUQ)的SAML SSO
- 标识提供程序：Okta(SAML 2.0)
- 适用于：在虚拟或硬件平台上提供EUQ访问的SMA部署。用环境中的值替换示例主机名和端口。
- 版本上下文：此过程适用于支持SAML for EUQ的SMA版本。验证已安装版本中的可用字段和菜单选项。

注意：本文档重点介绍SMA EUQ SAML配置。当SMA无法生成自签名证书时，仅引用ESA生成证书。

要求

开始之前，请确认您拥有：

- 对SMA Web界面的管理访问。
- 在Okta中创建创建SAML 2.0应用和分配用户或组的管理权限。

- SMA服务提供商配置的证书和私钥。自签名证书对于测试是允许的。
- 可访问的SMA EUQ完全限定域名(FQDN)和最终用户可以从浏览器访问的端口。
- SMA SAML断言URL和SP实体ID值(在创建SP条目后，从System Administration > SAML)。
- Okta中分配给Okta应用程序的用户帐户。
- 目录同步用户（如果您的部署使用目录集成）。

注意：Okta是第三方身份提供程序。本文档提供示例配置以供客户参考。

使用的组件

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最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

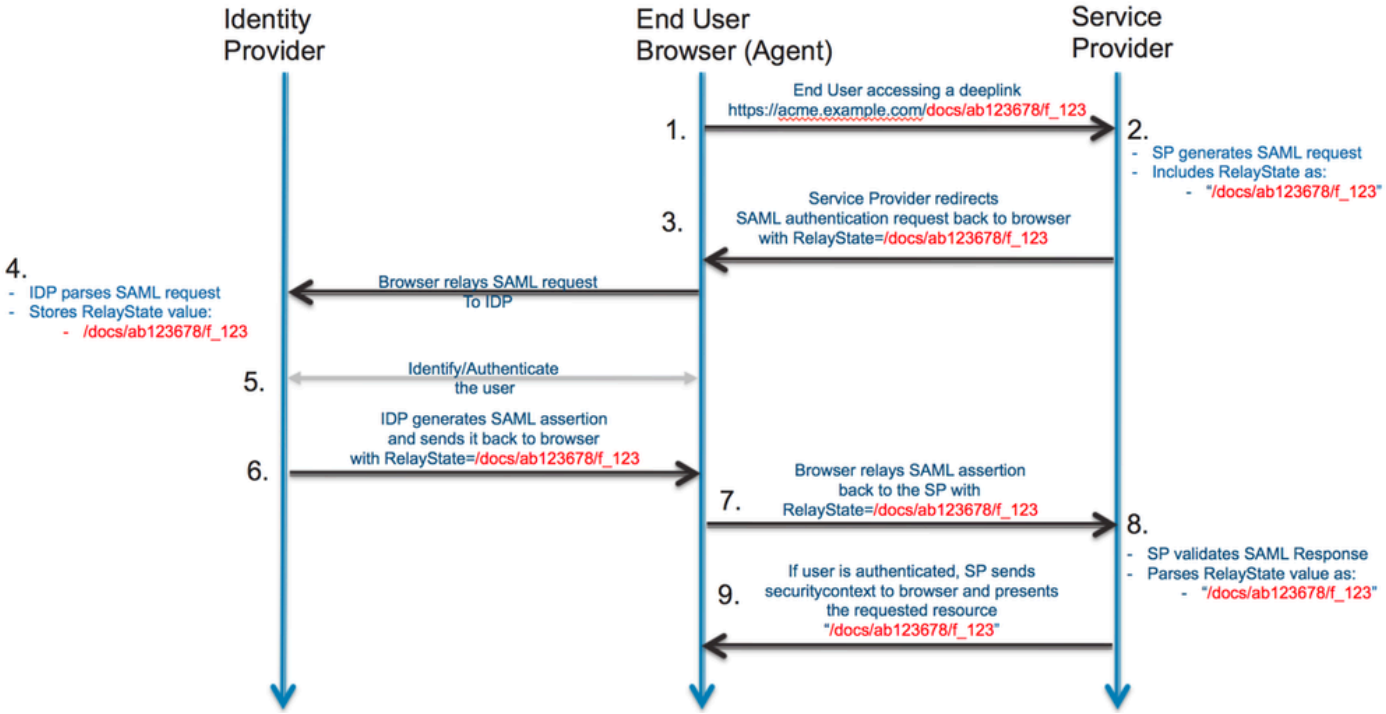
背景信息

目标是为垃圾邮件隔离区门户配置单点登录(SSO)，以便用户被重定向到Okta进行身份验证，如果Okta中启用了多重身份验证(MFA)，则完成多重身份验证(MFA)，然后返回到SMA EUQ门户。本文档仅适用于SMA。当SMA无法生成自签名证书时，思科安全邮件网关（以前称为邮件安全设备[ESA]）仅用于证书生成。

问题：用户必须使用SAML SSO和可选MFA通过Okta向SMA垃圾邮件隔离区门户进行身份验证。

分辨率：将SMA配置为服务提供商，在Okta中配置SAML应用，将Okta IdP设置导入SMA，在Okta中分配用户，并验证访问。

SAML流：



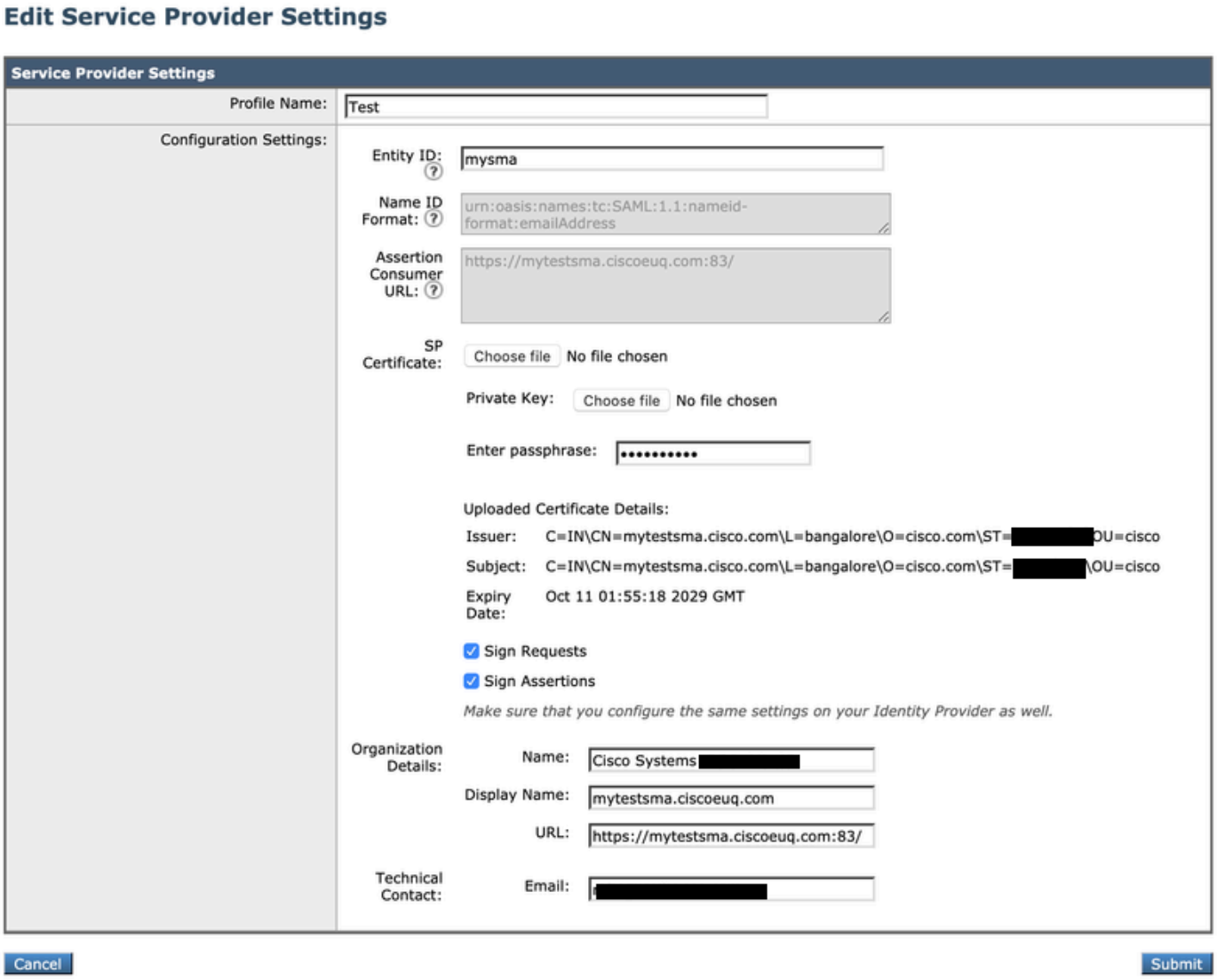
配置

在SMA设备上配置服务提供商(SP)

要将SMA配置为EUQ访问的SAML服务提供商，请完成以下步骤：

1. 登录到SMA Web界面。
2. 导航到系统管理> SAML。
3. 选择添加服务提供商。
4. 在Service Provider Entity ID中，输入实体ID，您也可以在数据库中配置。
5. 验证是否已为EUQ接口填充Name ID Format和Assertion Consumer Service(ACS) URL。
6. 在SP证书中，上传证书以签署SAML请求。

注意：SMA无法生成自签名证书。您还可以在ESA上生成证书，并将其导出以在SMA上使用。

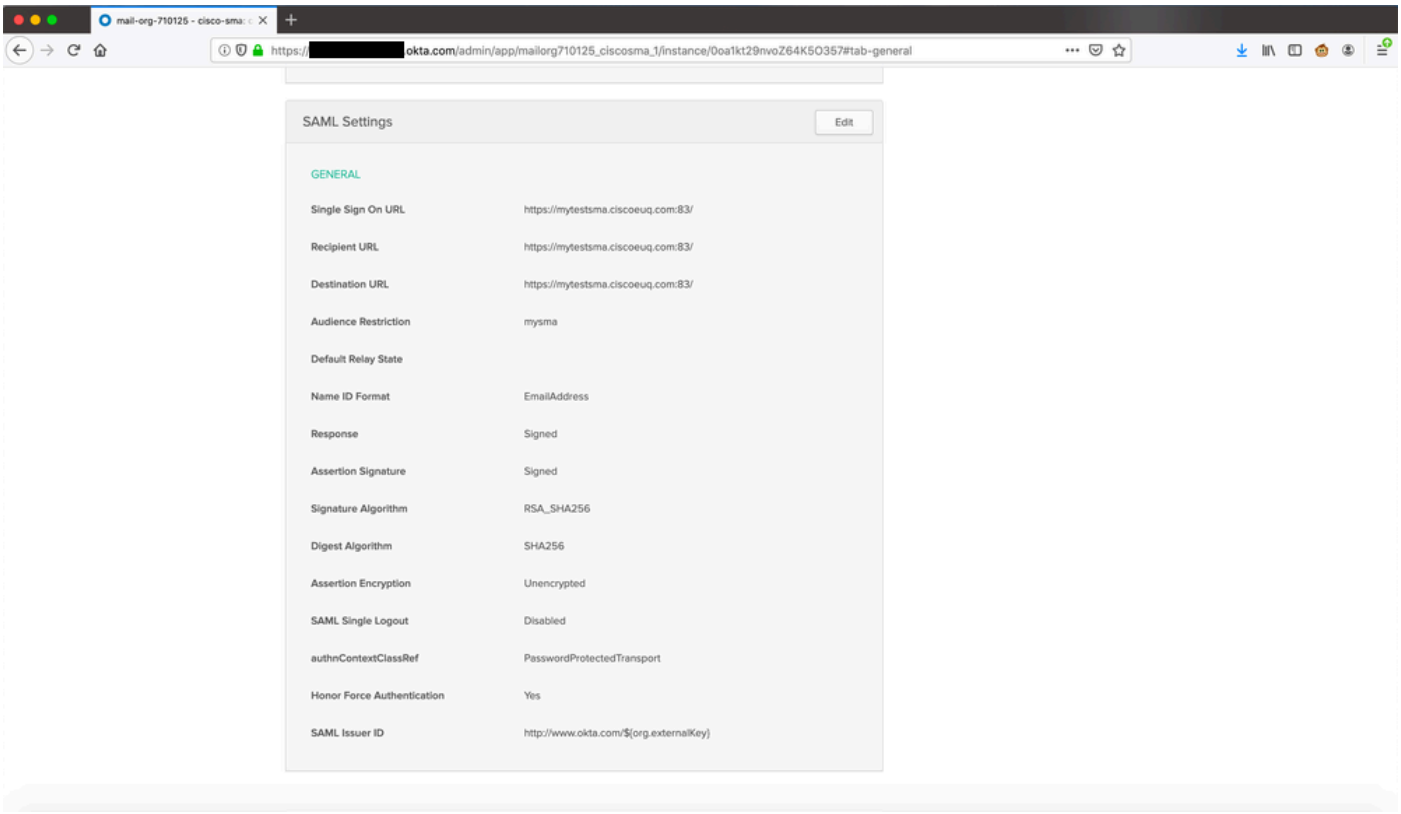


GUI中的服务提供商设置

在Okta中配置SAML应用

要在Okta中为SMA EUQ访问创建SAML 2.0应用程序，请完成以下步骤：

1. 以管理员身份登录Okta。
2. 导航到应用>应用，然后选择创建应用集成。
3. 选择SAML 2.0，然后选择下一步。
4. 输入App name，例如SMA EUQ，然后选择Next。
5. 在单点登录URL中，从SMA服务提供商设置输入SMA ACS URL。
6. 在受众URI（SP实体ID）中，输入在SMA上配置的相同实体ID。
7. 对于名称ID格式，请选择EmailAddress。
8. 对于Application username，请为您的部署选择适当的Okta用户名格式。
9. 完成向导，然后打开新应用程序并复制IdP metadata XML文件或metadata URL。

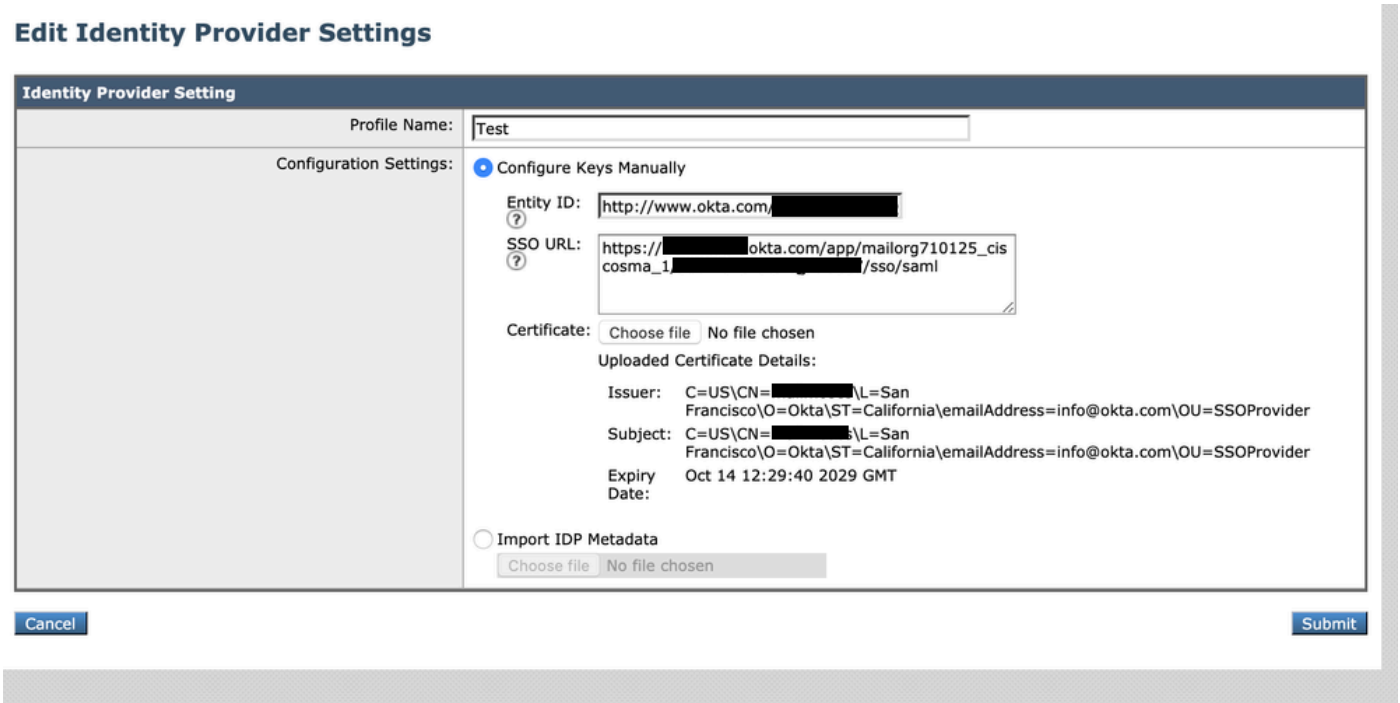


查看Okta门户

在SMA设备上配置身份提供程序(IdP)

要在SMA上将Okta配置为身份提供程序(IdP)，请完成以下步骤：

1. 登录到SMA Web界面。
2. 导航到系统管理> SAML。
3. 在Identity Provider Settings下，从上一节导入Okta IdP元数据，或手动输入值。

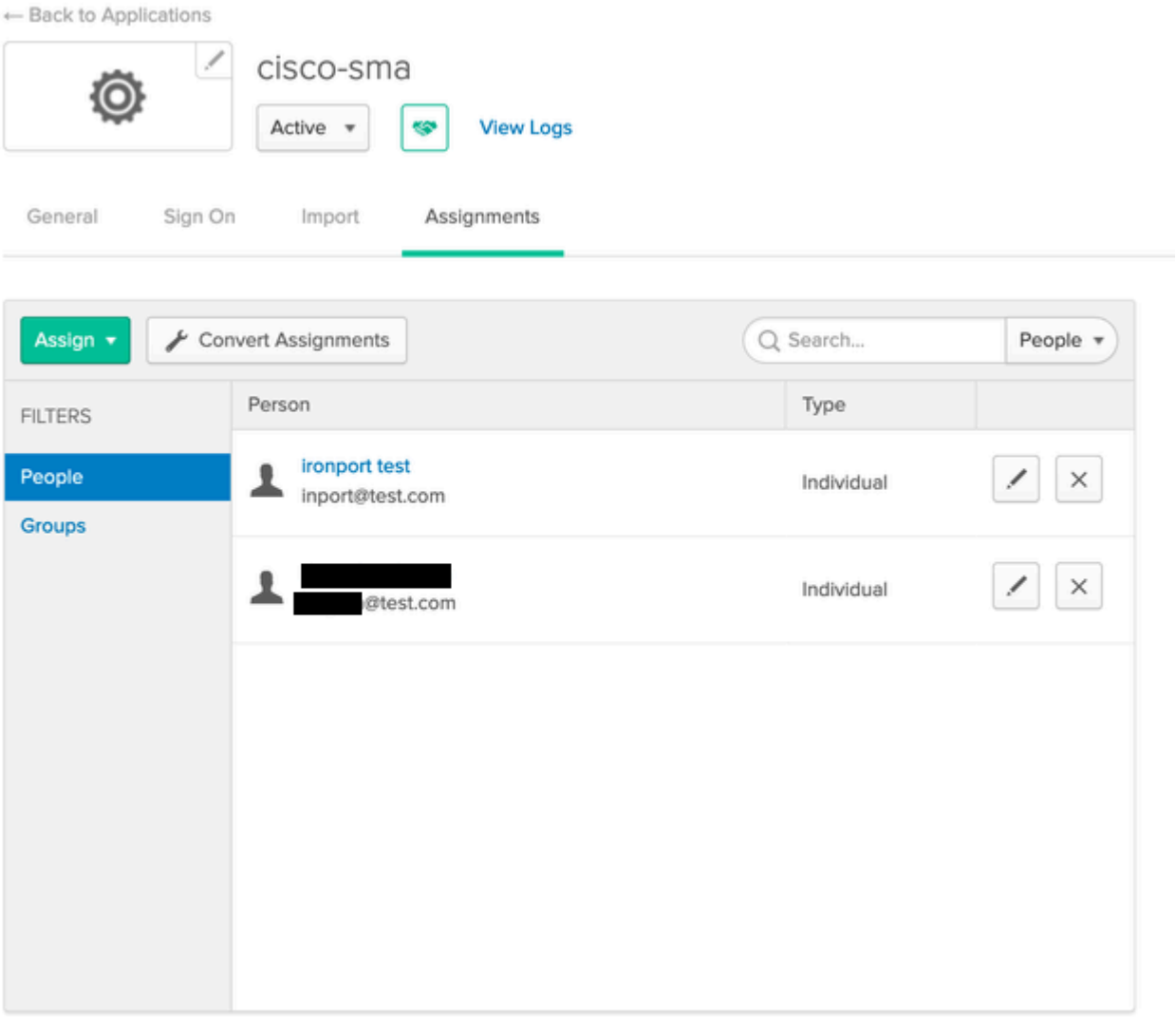


SMA GUI中的IdP配置文件设置

将用户分配到Okta应用程序

要允许用户通过Okta向SMA EUQ进行身份验证，请向Okta应用分配用户或组：

1. 在Okta中，打开您创建的应用程序。
2. 导航到分配>人员，然后选择分配。
3. 选择每个用户旁边的Assign，然后选择Done。



在Okta门户中分配用户

注意：您可以手动分配用户，从Active Directory同步用户，或者使用Okta支持的另一个目录集成。

在Okta中配置MFA（可选）

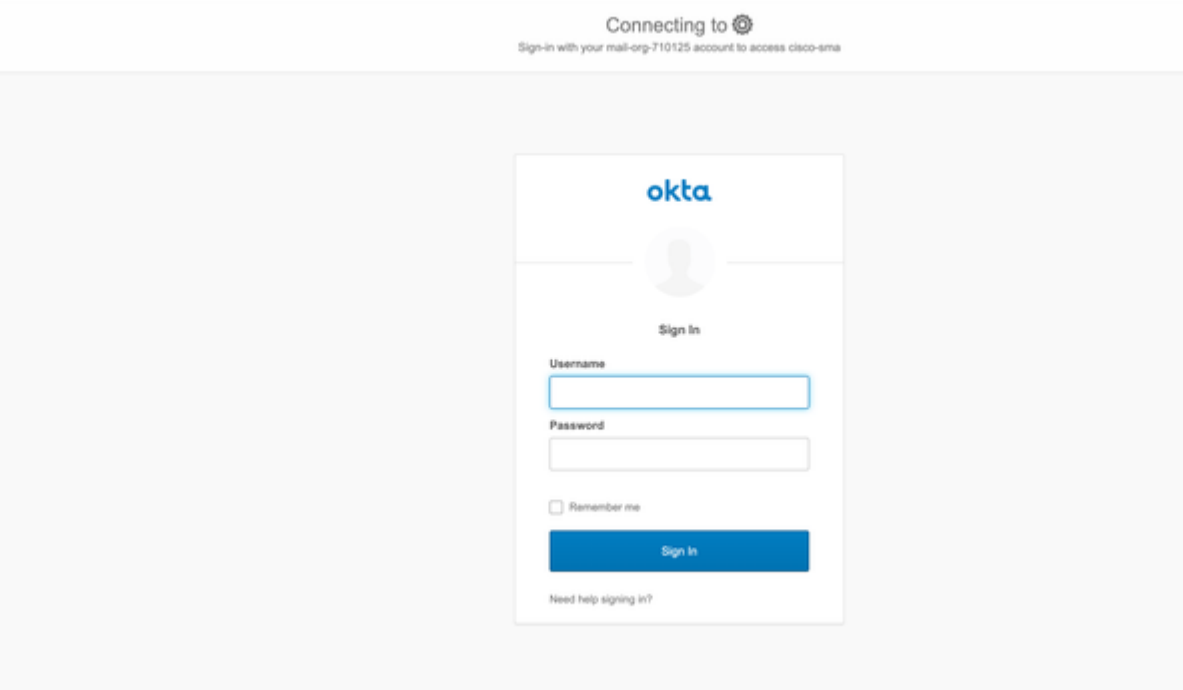
如果要对EUQ访问进行多因素身份验证(MFA)，请在Okta中为应用配置MFA策略：

1. 在Okta Admin中，导航到Security > Authentication。
2. 配置所需的因素（例如Okta Verify、Google Authenticator或SMS），并将策略应用于SMA EUQ应用。

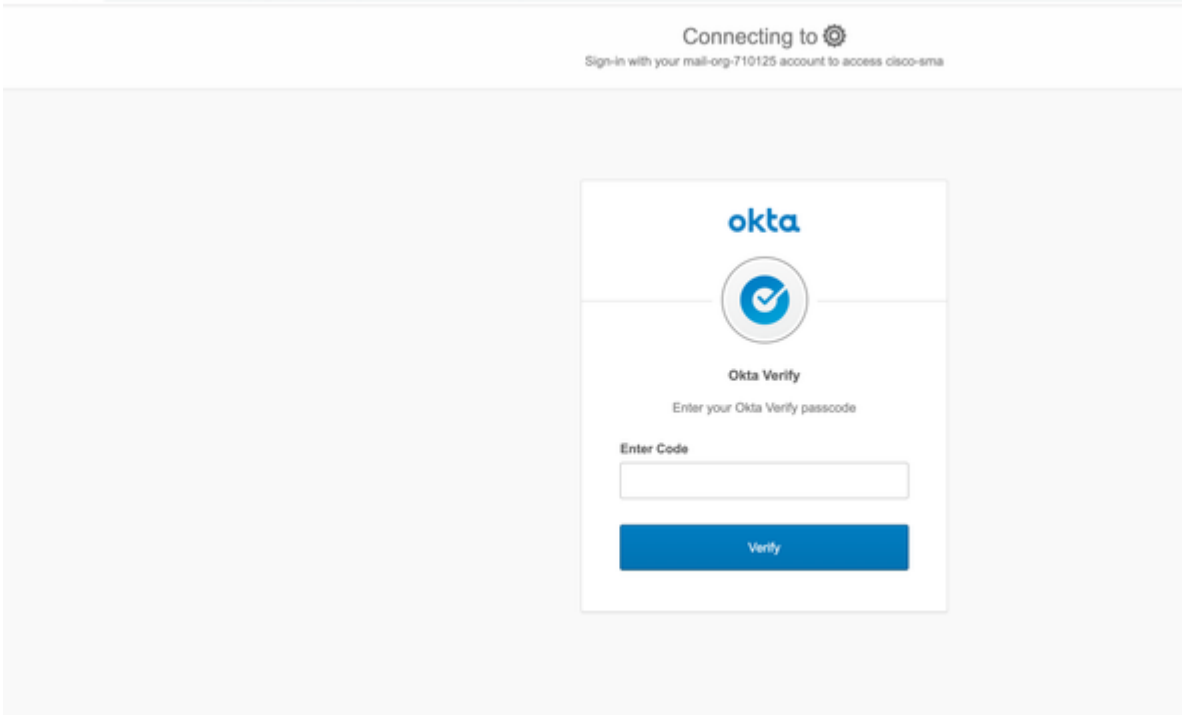
验证SAML登录

预期结果：要验证配置，请完成以下步骤：

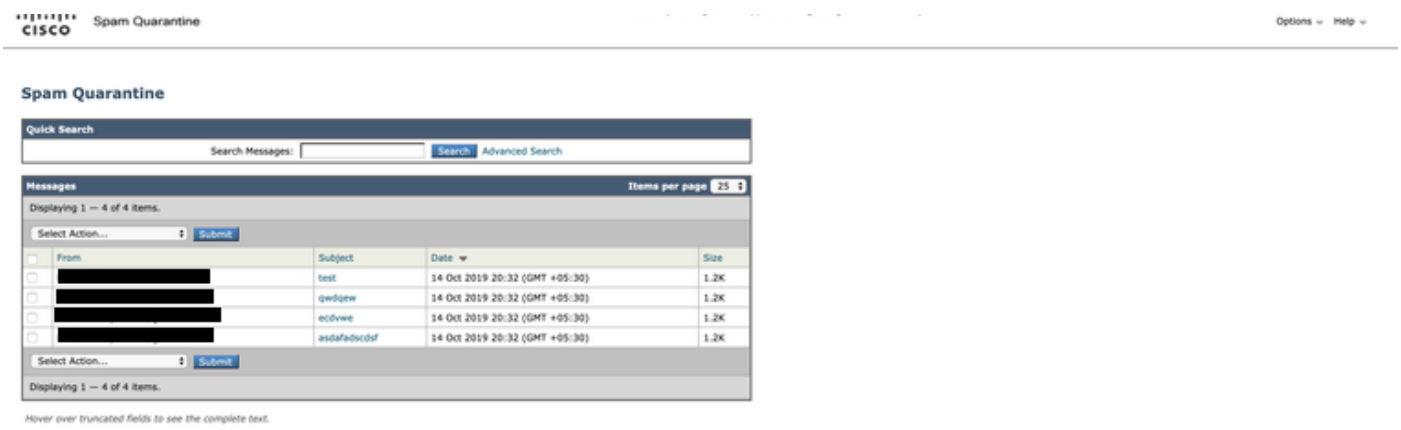
1. 浏览到SMA EUQ URL，例如https://<sma-fqdn>:<port>/。
2. 确认浏览器重定向到Okta进行身份验证。
3. 如果已启用MFA，请完成MFA练习。
4. 确认已重新定向到SMA垃圾邮件隔离区门户并可以访问隔离功能。



使用Okta登录



输入Okta验证代码



使用Okta登录后的垃圾邮件隔离区视图

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）。