为ESA/SMA SAML SSO生成和配置自签名证书

目录

简介

本文档介绍如何为安全断言标记语言(SAML)服务提供商(SP)配置创建自签名证书。

先决条件

使用本文档为邮件安全设备(ESA)和安全管理设备(SMA)上的安全声明标记语言(SAML)2.0单点登录(SSO)服务提供商(SP)配置生成自签名证书。

要求

方法1(ESA Web UI):Web UI中的ESA管理访问以及管理证书的权限。

方法2（OpenSSL命令）：OpenSSL已安装，可从命令行获取。

Windows 窗口版本:安装OpenSSL。

macOS、Linux或Unix:OpenSSL通常在默认情况下或通过操作系统软件包管理器提供。

使用的组件

没有特定的硬件和软件要求。

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

本文档适用于使用安全声明标记语言(SAML)2.0单点登录(SSO)的邮件安全设备(ESA)和安全管理设备(SMA)部署。SAML SP配置需要安全套接字层(SSL)证书才能进行服务提供商设置。证书可以来自内部证书工具、证书颁发机构(CA)或自签名证书。

问题

ESA和SMA的一些SAML SP部署中需要自签名证书。本文档介绍如何创建证书和私钥，以及如何使用密码短语对私钥进行加密（可选）。

分辨率

- 在Windows上，安装OpenSSL for Windows。在线提供一些教程，其中包含有关如何执行此操作的说明。
- 在Unix、macOS和Linux上，OpenSSL通常在默认情况下可用。
- 当ESA已管理证书且必须导出证书以供SAML SP使用时，请使用ESA Web UI方法。
- 当必须直接从命令行创建证书和密钥对时，请使用OpenSSL命令方法。

方法 1：在ESA Web UI中创建和导出自签名证书

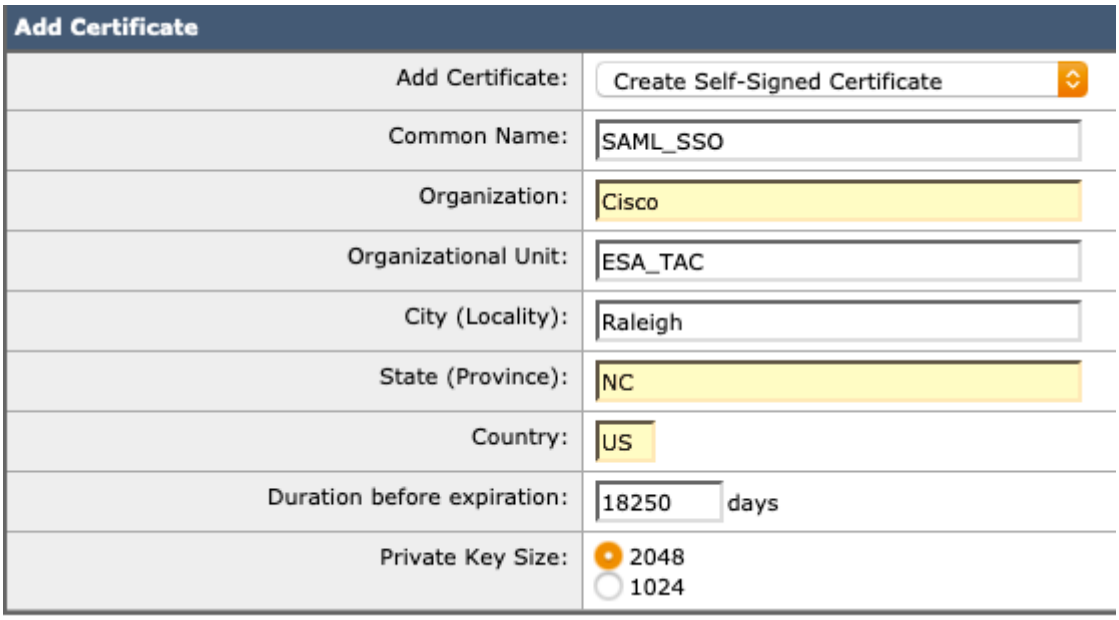
当ESA已管理证书且必须导出证书以供SAML SP使用时，请使用此方法。

创建证书。

1.在ESA Web UI中，导航到网络>证书。选择Add Certificate，然后选择Create Self-Signed Certificate。

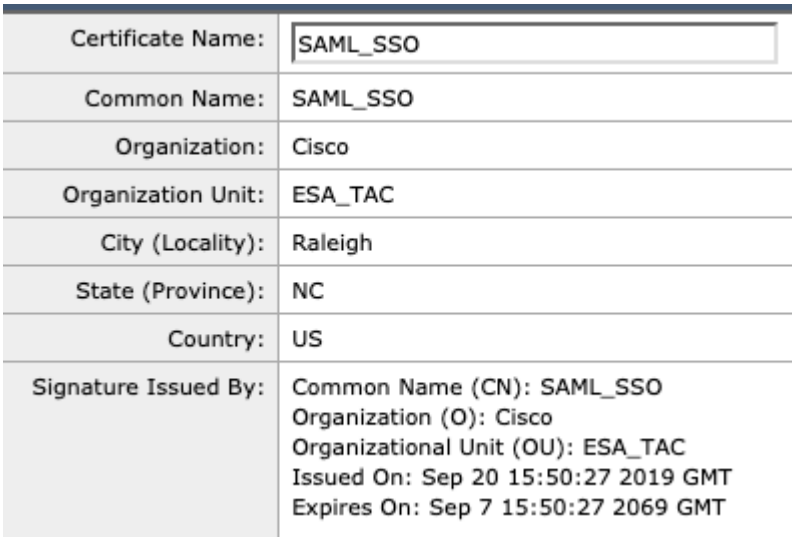
2.输入模板字段:公用名称、组织、组织单位、城市、州、国家/地区和持续时间(1-18250天)。

3.将私钥大小设置为2048。



完成自签名证书模板

4.提交证书，审核结果，然后选择提交更改。



配置后查看

导出证书。

1.在ESA Web UI中，导航到网络>证书>导出证书。

2.选择要导出的证书，创建口令，选择导出，然后将文件保存到目录。

注意：用于管理的SAML SSO可以导入PKCS#12(PFX)证书。如果不需要私钥加密，则其余转换步骤是可选的。

转换证书。

导出的证书采用PKCS#12/PFX格式，需要转换为隐私增强邮件(PEM)。

运行此OpenSSL命令将PFX文件转换为PEM格式。

<#root>

openssl

```
 pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes
```

<#root>

openssl

```
 pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes
```

编辑内容并将输出拆分为两个文件。

1.新转换的文件需要进行细微编辑。

2.在文本编辑器中打开两个空白文件，并将它们命名为<name>.crt和<name>.key。

----- 3.从转换的文件复制BEGIN CERTIFICATE-----至-----END CERTIFICATE-----部分。

4.将内容粘贴到<name>.crt文件中，然后保存。

----- 5.从转换后的文件中复制BEGIN PRIVATE KEY-----至-----END PRIVATE KEY-----部分。

6.将内容粘贴到<name>.key文件中，然后保存它。

7.现在可以将证书和密钥加载到配置的SAML SP部分。

方法 2：使用OpenSSL命令创建自签名证书和密钥对

当必须直接从命令行创建证书和密钥对时，请使用此方法。

创建证书和密钥对。

在Unix、Linux或macOS命令行界面中运行OpenSSL命令。将domain替换为所需的名称。

<#root>

openssl

 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt

在创建过程中，将显示所列字段的提示。

在命令运行的目录中生成两个文件：saml_ssl.crt和saml_ssl.key。

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

加密私钥(可选；配置不需要)。

注意：请勿重复使用示例密码。此密钥仅用于示例目的。

此OpenSSL命令采用未加密的私钥(unencrypted.key)并输出加密的密钥(encrypted.key):

<#root>

openssl

rsa -des3 -in unencrypted.key -out encrypted.key

<#root>

openssl

rsa -des3 -in saml_sso.key -out saml_secure.key

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

证书和密钥已准备好用于SAML SSO SP或垃圾邮件SSO SP设置。

相关信息

思科邮件安全设备 — 最终用户指南

思科内容安全管理设备 — 最终用户指南

思科网络安全 — 最终用户指南

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）。