

# 添加/导入在思科ESA GUI的新建的PKCS-12证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[问题](#)

[解决方法](#)

## 简介

本文描述添加/导入在思科的新建的公钥加密标准(PKCS) #12证书如何给安全工具(ESA) GUI发电子邮件。

## 先决条件

## 要求

Cisco 建议您了解以下主题：

- 思科ESA
- AsyncOS 7.1及以后

## 问题

从AsyncOS 7.1.0及以后，管理/添加在电子邮件设备的GUI的证书是可能的。然而，为此新证书，它必须在PKCS-12格式，因此此需求在接收Certificate Authority (CA)证书以后添加一些额外步骤。

生成PKCS-12证书也要求专用密钥证书。如果从Cisco ESA CLI命令**certconfig**运行证书签名请求(CSR)，您不会接收专用密钥证书。在GUI菜单创建的专用密钥证书(**邮件策略>签署的密钥**)不会有效，当您使用它与CA证书一起生成PKCS-12证书。

## 解决方法

1. 如果您的 workstation 没有它，请安装Openssl应用程序。windows版本可以从[这里](#)下载。保证Visual C++ 2008 Redistributables在Openssl Win32前安装。
2. 请使用一个模板创建脚本生成CSR和专用密钥[此处](#)。脚本如下所示：：**openssl req -新建-**

```
newkey rsa:2048 -节点- test_example.csr - keyout test_example.key - subj  
"/C=AU/ST=NSW/L=Sydney/O= Cisco系统/OU=IronPort/CN=test.example.com"
```

3. 复制和插入脚本到Openssl窗口并且按回车。

```
C:\OpenSSL-Win32\bin>openssl req -新建- newkey rsa:2048 -节点- test_example.csr -  
keyout  
test_example.key - subj "/C=AU/ST=NSW/L=Sydney/O= Cisco系统  
/OU=IronPort/CN=test.example.com"
```

输出：

```
test_example.csr and test_example.key in the C:\OpenSSL-Win32\bin or in the  
'bin' folder where OpenSSL is installed  
test_example.csr = Certificate Signing Request  
example.key = private key
```

4. 请使用.CSR文件为CA证书请求。

5. 一旦接收CA证书，请保存它，当cacert.pem文件。重命名专用密钥文件test\_example.key对test\_example.pem。使用Openssl，现在您能生成PKCS-12证书。

指令：

```
openssl pkcs12 -出口- cacert.p12 -在cacert.pem - inkey test_example.pem
```

如果使用的CA证书和专用密钥正确，Openssl提示您输入出口密码和再证实密码。否则，它建议您使用的证书和密钥不配比并且不能继续进行进程。

输入：

```
cacert.pem = CA certificate  
test_example.pem = private key  
Export password: ironport
```

输出：

```
cacert.p12 (the PKCS#12 certificate)
```

6. 去IronPort GUI菜单，网络>证书。

选择**添加证书**。

选择在**添加身份验证选项的进口证明书**。

选择**选择**并且浏览到PKCS-12生成的证书的位置在步骤5的。

输入您使用使用的同一个密码，当您生成在Openssl的PKCS-12证书(在这种情况下密码是ironport)。

其次选择，并且Next屏幕将显示用于证书的属性详细信息。

选择 **Submit**。

选择**进行更改**。

在这些步骤以后，新证书被添加到证书列出并且可以分配为使用。