# 配置安全Web设备GUI证书

## 目录


简介

先决条件

- 要求
- 使用的组件

Web用户界面证书

修改Web界面证书的步骤

从命令行测试证书

常见错误

- 错误PKCS#12格式无效
- 天数必须是一个整数
- 证书验证错误
- 密码无效
- 证书尚未生效

从CLI重新启动GUI服务

相关内容


## 简介

本文档介绍为安全网络设备(SWA)管理Web界面配置证书的步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- SWA管理。

Cisco 建议您：

- 已安装物理或虚拟SWA。
- 对SWA图形用户界面(GUI)的管理访问。

- 对SWA命令行界面(CLI)的管理访问。

### 使用的组件

本文档不限于特定的软件和硬件版本。

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。

## Web用户界面证书

首先，选择要用于SWA管理Web用户界面(Web UI)的证书类型。

默认情况下，SWA使用思科设备演示证书：

- CN =思科设备演示证书
- O =思科系统公司
- L =圣荷西
- S =加利福尼亚
- C =美国

您可以在SWA中创建自签名证书，也可以导入由内部证书颁发机构(CA)服务器生成的自签名证书。

生成证书签名请求(CSR)时，SWA不支持包括主题备用名称(SAN)。 此外，SWA自签名证书也不支持SAN属性。要使用具有SAN属性的证书，您必须自己创建并签署证书，确保证书包含必要的SAN详细信息。生成此证书后，您可以将其上传到要使用的SWA。此方法允许您指定多个主机名、IP地址或其他标识符，为您的网络环境提供更大的灵活性和安全性。

---

注意：证书必须包含私钥，并且必须是PKCS#12格式。

---

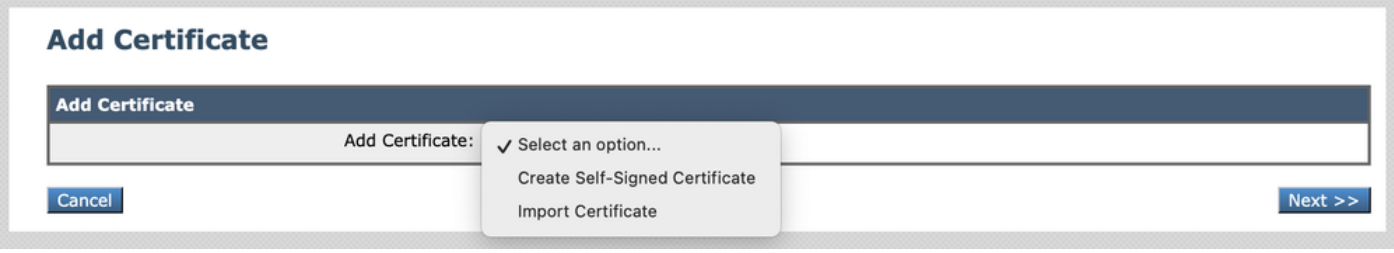
## 修改Web界面证书的步骤

步骤1.登录到GUI并从顶部菜单中选择Network。

步骤2.选择证书管理。

第3步：从Appliance Certificates中选择Add Certificate。

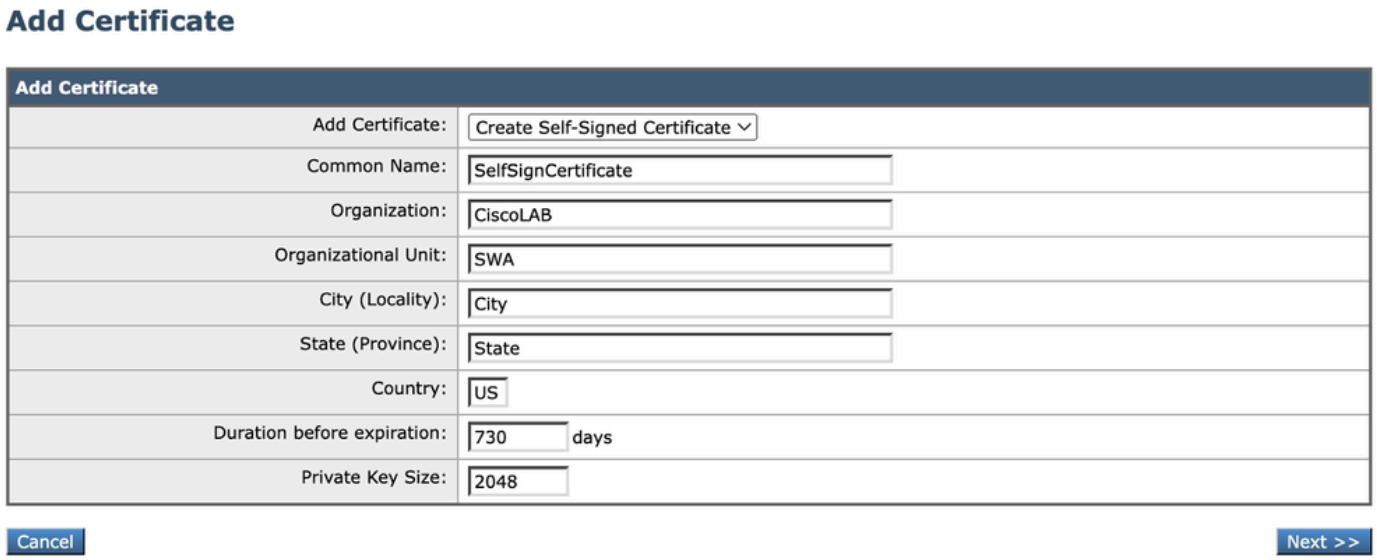
第4步：选择Certificate Type（Self Signed Certificate或Import Certificate）。




图像 — 选择证书类型

第5步：如果选择自签名证书，请使用以下步骤。否则，请跳至步骤6。

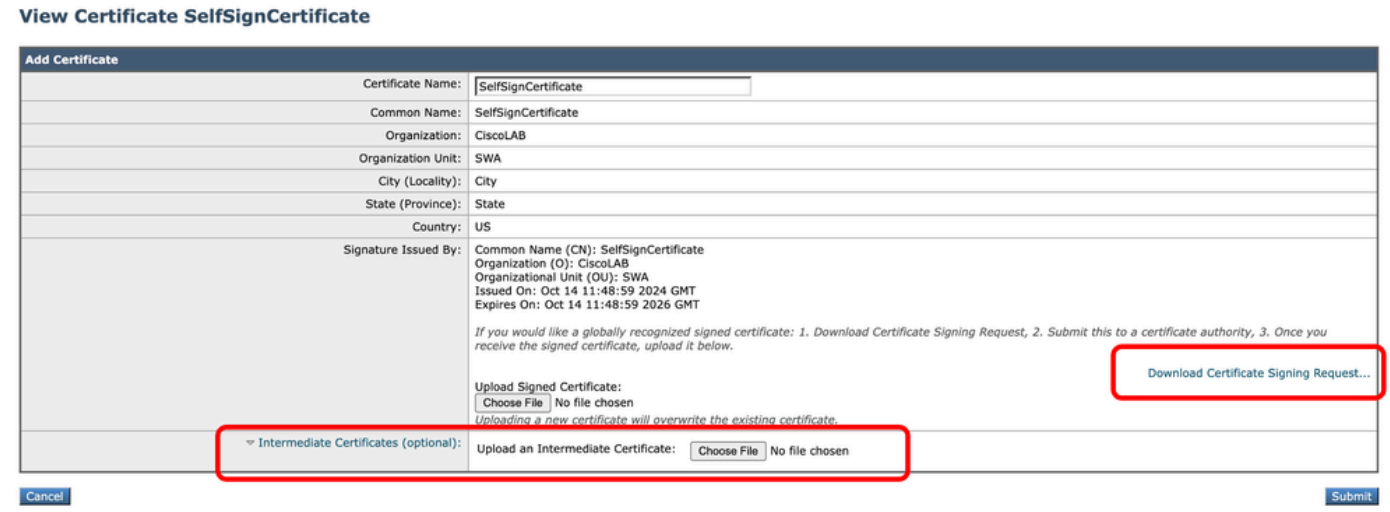
步骤5.1.填写字段。




图像 — 自签名证书详细信息

注意：私钥大小必须在2048到8192范围内。

步骤5.2.单击Next。




图像 — 下载CSR

第5.3步（可选）您可以下载CSR并使用您的组织CA服务器进行签名，然后上传签名证书并提交文件。

---

⚠ 警告：如果要使用CA服务器签署CSR，请确保在签署或上传签名证书之前先提交提交和提交页面。在CSR生成过程中创建的配置文件包含您的私钥。

---

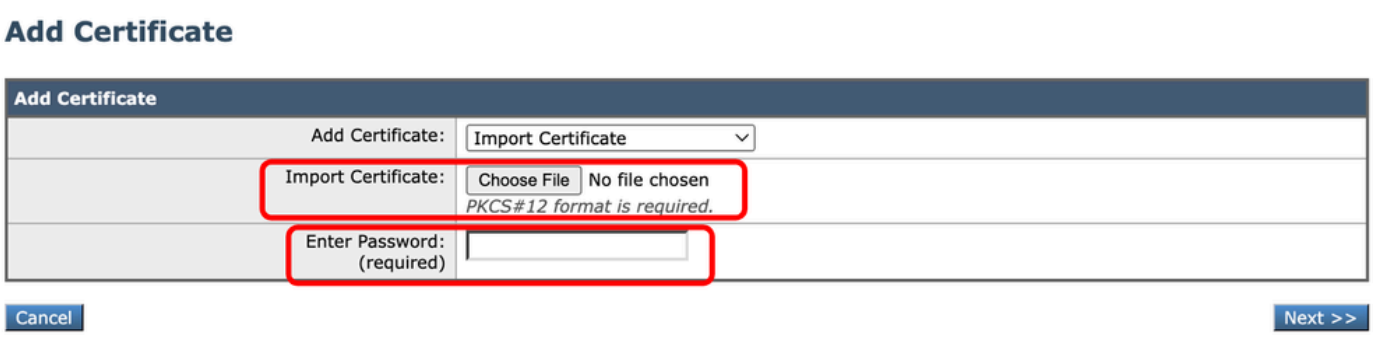
步骤5.4.提交（如果当前自签名证书适用）。

步骤5.5.跳至步骤7。

步骤6.如果选择Import Certificate，请完成以下步骤：

第6.1步：导入证书文件（需要PKCS#12格式）。

步骤6.2.输入证书文件的密码。



图像 — 导入证书

步骤6.3.单击Next。

步骤6.4.提交更改。

步骤7.提交更改。

步骤8.登录到CLI。

步骤9.键入certconfig并按Enter键。

步骤10.键入SETUP。

步骤11.键入Y，然后按Enter键。

注意：更改证书后，当前登录Web用户界面的管理用户可能会遇到连接错误，并且可能会丢失未提交的更改。仅当浏览器未将证书标记为受信任时，才会出现这种情况。

第12步：选择2以从可用证书列表中选择。

步骤13.选择要用于GUI的所需证书的编号。

步骤14.如果您有中间证书并想要添加它们，请键入Y，否则键入N。

注意：如果您需要添加中间证书，则必须以PEM格式粘贴中间证书，并以.（仅点）结尾。

```
SWA_CLI> certconfig

Choose the operation you want to perform:
- SETUP - Configure security certificate and key.
- OCSPVALIDATION - Enable OCSP validation of certificates during upload
- RESTRICTCERTSIGNATURE - Enable restricted signature validation of certificates during upload
- OCSPVALIDATION_FOR_SERVER_CERT - Enable OCSP validation for server certificates
- FQDNVALIDATION - FQDN validation for certificate
[]> SETUP

Currently using the demo certificate/key for HTTPS management access.

When the certificate is changed, administrative users who are currently logged in to the web user inter
occurs only if the certificate is not already marked as trusted by the browser.
```

```
Do you want to continue? [Y]> Y

Management (HTTPS):
Choose the operation you want to perform:
1. PASTE - Copy paste cert and key manually
2. SELECT - select from available list of certificates
[1]> 2

Select the certificate you want to upload
1. SelfSignCertificate
2. SWA_GUI.cisco.com
[1]> 1

Do you want add an intermediate certificate? [N]> N

Successfully updated the certificate/key for HTTPS management access.
```

步骤15.键入commit以保存更改。

# 从命令行测试证书

您可以使用openssl命令检查证书：

```
openssl s_client -connect

    :
```

在本示例中，主机名为SWA.cisco.com，管理接口设置为默认值（TCP端口8443）。

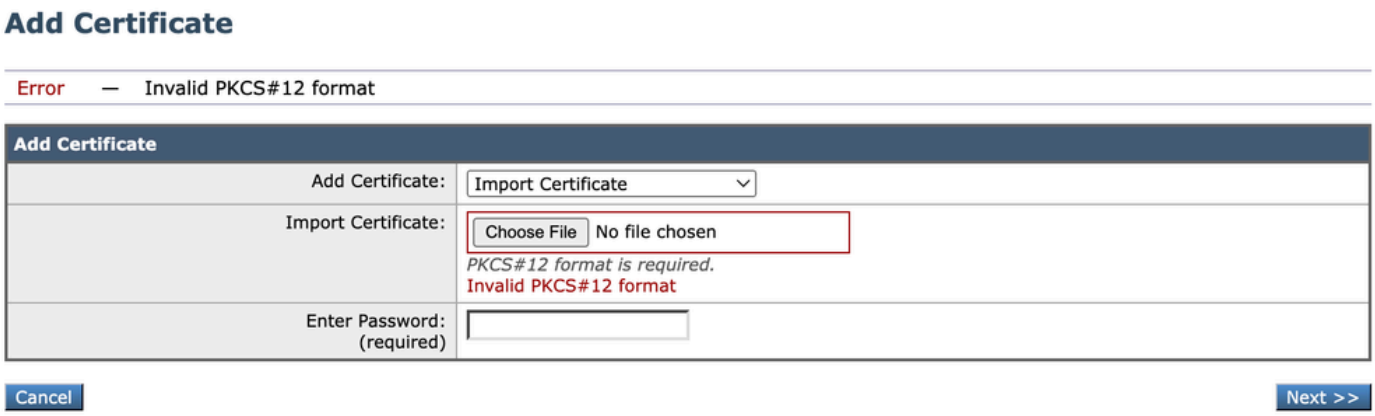
在输出的第二行，您可以看到证书详细信息：

```
openssl s_client -connect SWA.cisco.com:8443
CONNECTED(00000003)
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

# 常见错误

以下是尝试创建或修改GUI证书时可能遇到的一些常见错误。

## 错误PKCS#12格式无效




映像 — PKCS#12格式无效

此错误可能有两个原因：

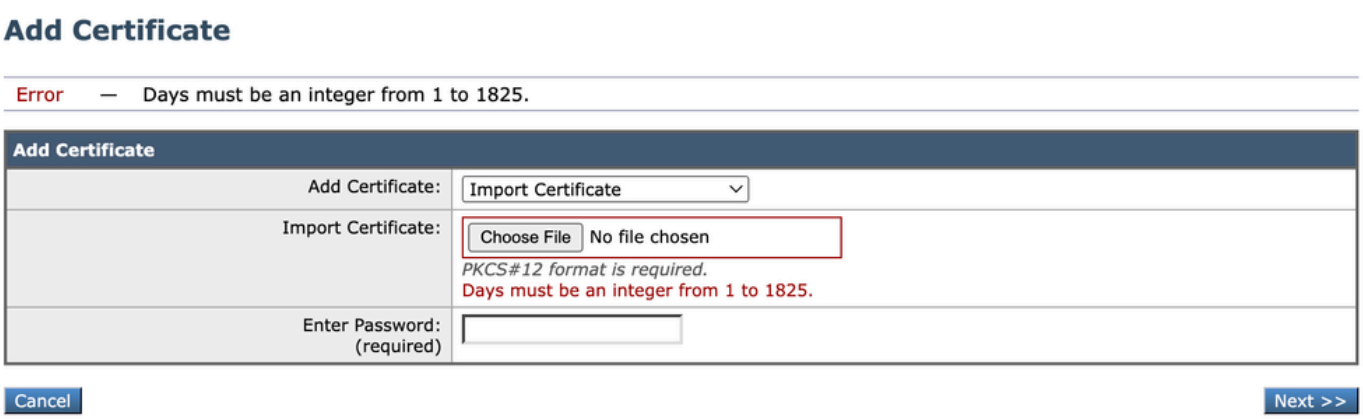
1. 证书文件已损坏且无效。

   尝试打开证书，如果打开时出现错误，您可以重新生成或再次下载证书。

2.以前生成的CSR不再有效。

   生成CSR时，必须确保Submit和Commit更改。原因是注销或更改页面时未保存您的CSR。生成CSR时创建的配置文件包含成功上传证书所需的私钥。此配置文件消失后，私钥也随之消失。因此，必须生成另一个CSR，然后再次将该CSR提供给您的CA。

## 天数必须是一个整数



图像 — 天数必须是整数错误

此错误是由于上载的证书已过期或具有0天有效期。

要解决此问题，请检查证书到期日期并确保您的SWA日期和时间正确。

## 证书验证错误

此错误表示根CA或中间CA未添加到SWA中的受信任根证书列表中。要解决此问题，如果您同时使用根CA和中间CA:

1.将根CA上传到SWA，然后提交。

2.上传中间CA，然后重新提交更改。

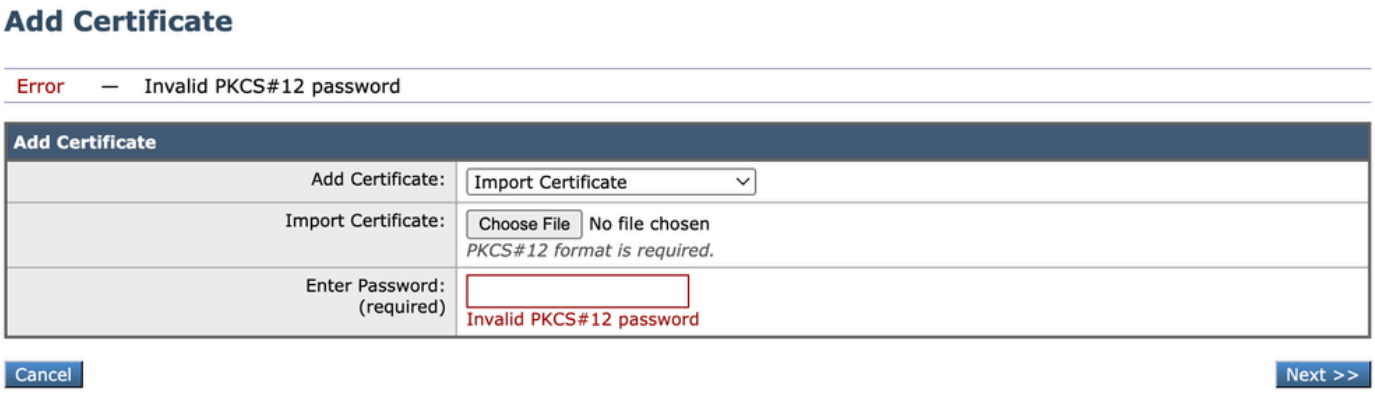
3.上传GUI证书。

---

注意：要上传根或中间CA，请从GUI:网络.在Certificate Management部分中，选择Manage Trusted Root Certificates。在自定义受信任根证书中，点击导入以上传您的CA证书。

---

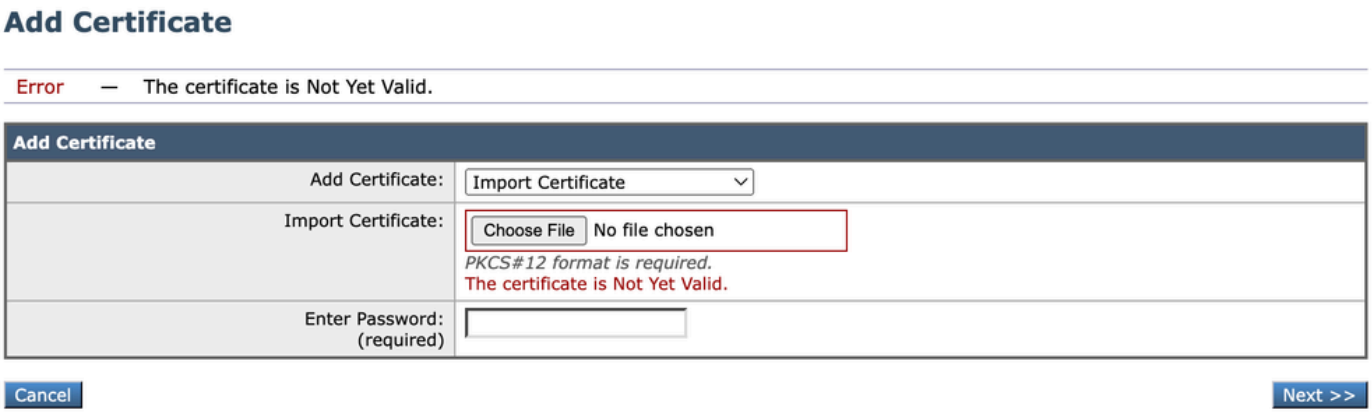
## 密码无效




图像 — 密码无效

此错误表示PKCS#12证书密码不正确。要解决此错误，请键入正确的密码或重新生成证书。

## 证书尚未生效




图像 — 证书尚未生效

1.确保SWA日期和时间正确。

2.检查证书日期，确保“Not Before”日期和时间正确。

---

提示：如果刚刚生成证书，请等待一分钟，然后上传证书。

---

# 从CLI重新启动GUI服务

要重新启动WebUI服务，可以从CLI执行以下步骤：

步骤1.登录CLI。

步骤2.键入diagnostic（这是一个隐藏命令，不会使用TAB自动键入）。

步骤3.选择服务。

步骤4.选择WEBUI。

步骤5.选择RESTART。

# 相关内容

- 思科安全Web设备AsyncOS 15.0用户指南 — GD（通用部署） — 对最终用户进行策略应用分类[思科安全Web设备] — 思科

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）。