生成和添加安装安全终端私有云3.x及更高版本所需的证书

目录

简介

本文档介绍生成证书的过程，每次全新安装安全控制台私有云时必须上传这些证书，或者更新已安装的证书服务。

先决条件

要求

本文档中的信息基于以下软件和硬件版本：

- Windows Server 2008

- CentOS 7/8
- 安全控制台虚拟私有云3.0.2（以后）
- OpenSSL 1.1.1

使用的组件

Cisco 建议您了解以下主题：

- Windows Server 2008（以后）
- 安全控制台私有云安装
- 公用密钥基础结构
- OpenSSL
- Linux CLI

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

引入安全控制台私有云3.X后，以下所有服务都需要主机名和证书/密钥对：

- 管理门户
- 身份验证（私有云3.X中的新功能）
- 安全控制台
- 处置服务器
- Disposition Server — 扩展协议
- 处置更新服务
- Firepower 管理中心

本文档将讨论生成和上传所需证书的快速方法。您可以根据组织策略调整每个参数，包括散列算法、密钥大小和其他参数，并且生成这些证书的机制可能与此处详细介绍的内容不匹配。

> **警告**：下面提到的步骤可能因您的CA服务器配置而异。预期您选择的CA服务器已调配，并且配置已完成。以下技术说明仅介绍生成证书的示例，思科TAC不参与任何类型的证书生成和/或CA服务器问题的故障排除。

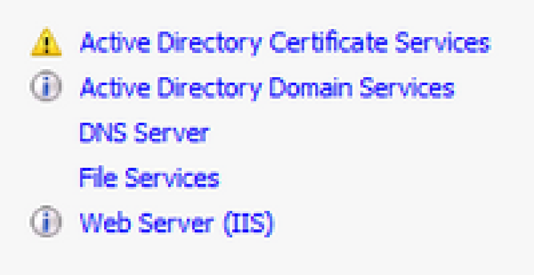
证书创建

在Window服务器上生成证书

确保在Windows Server上安装并配置以下角色。

- Active Directory证书服务
- 证书颁发机构
- 证书颁发机构Web注册
- 在线响应器
- 证书注册Web服务
- 证书注册策略Web服务

- Active Directory 域服务
- DNS Servers
- Web服务器(IIS)



⚠ Active Directory Certificate Services

ⓘ Active Directory Domain Services

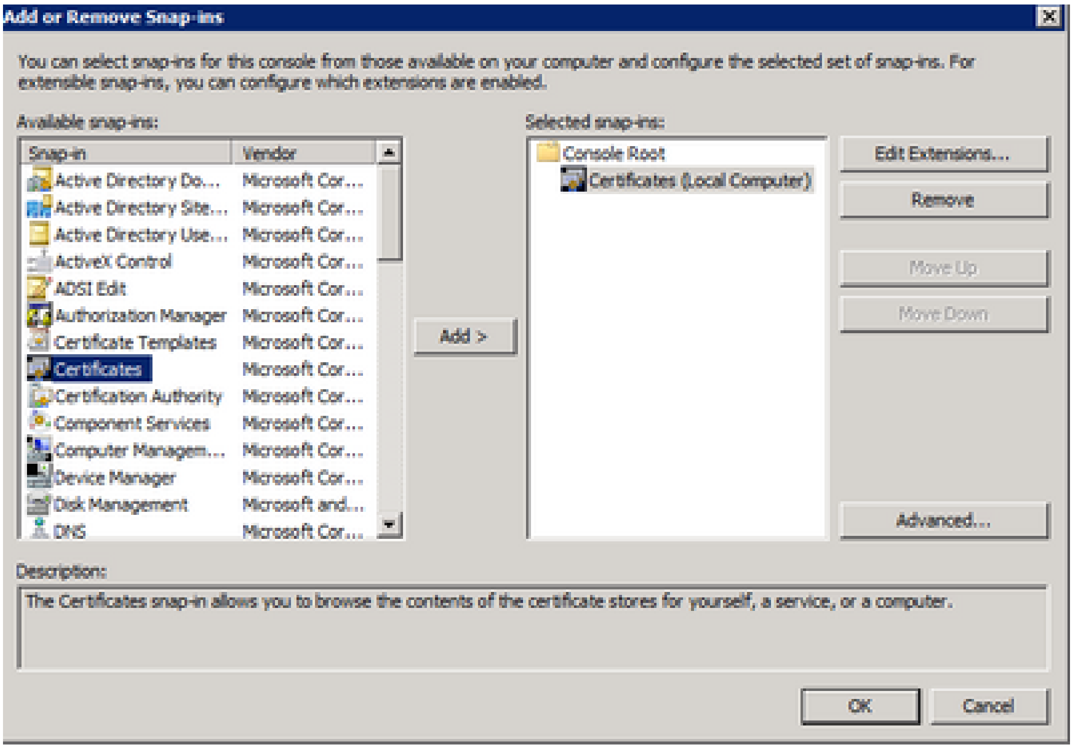
DNS Server

File Services

ⓘ Web Server (IIS)

生成证书签名请求(CSR)

步骤1:导航到MMC控制台，然后添加计算机帐户的证书管理单元，如下图所示。



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...

Selected snap-ins:

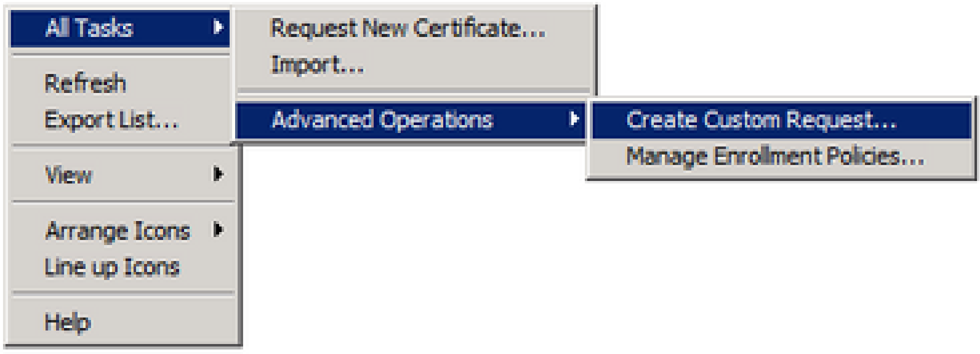
Console Root
  Certificates (Local Computer)

Description:

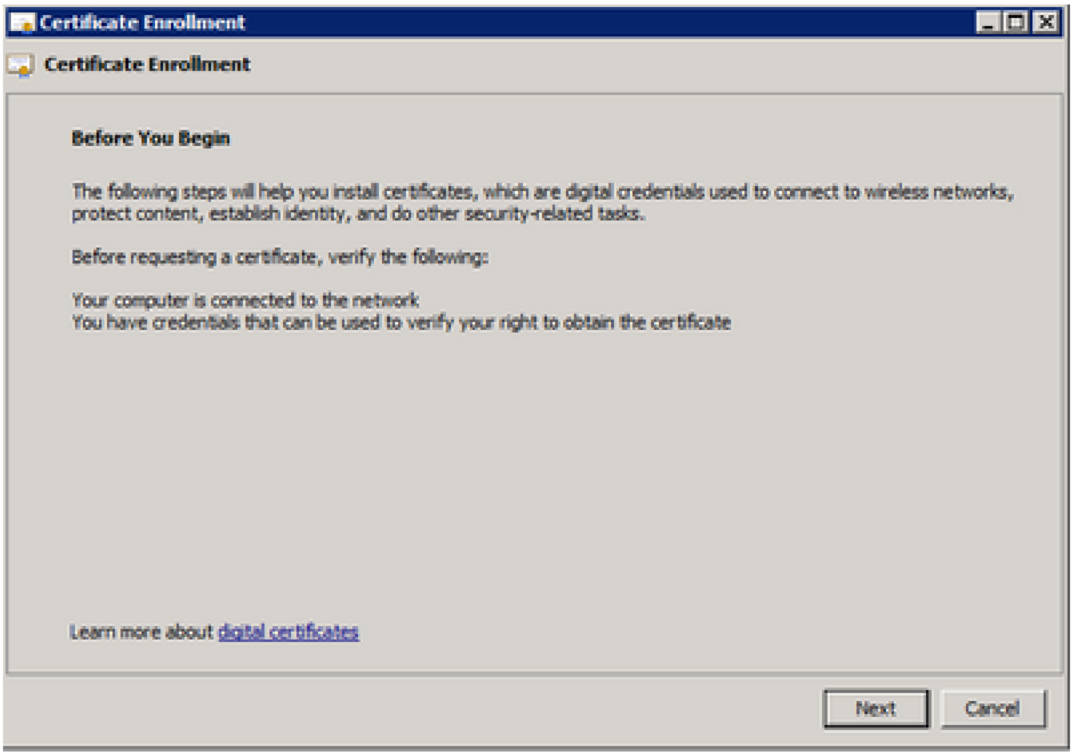
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

第二步：向下钻取**证书（本地计算机）>个人>证书。**

第三步：右键单击空白区域，然后选择**所有任务>高级操作>创建自定义请求。**



第四步：在“登记”窗口中选择**下一步。**



Before You Begin

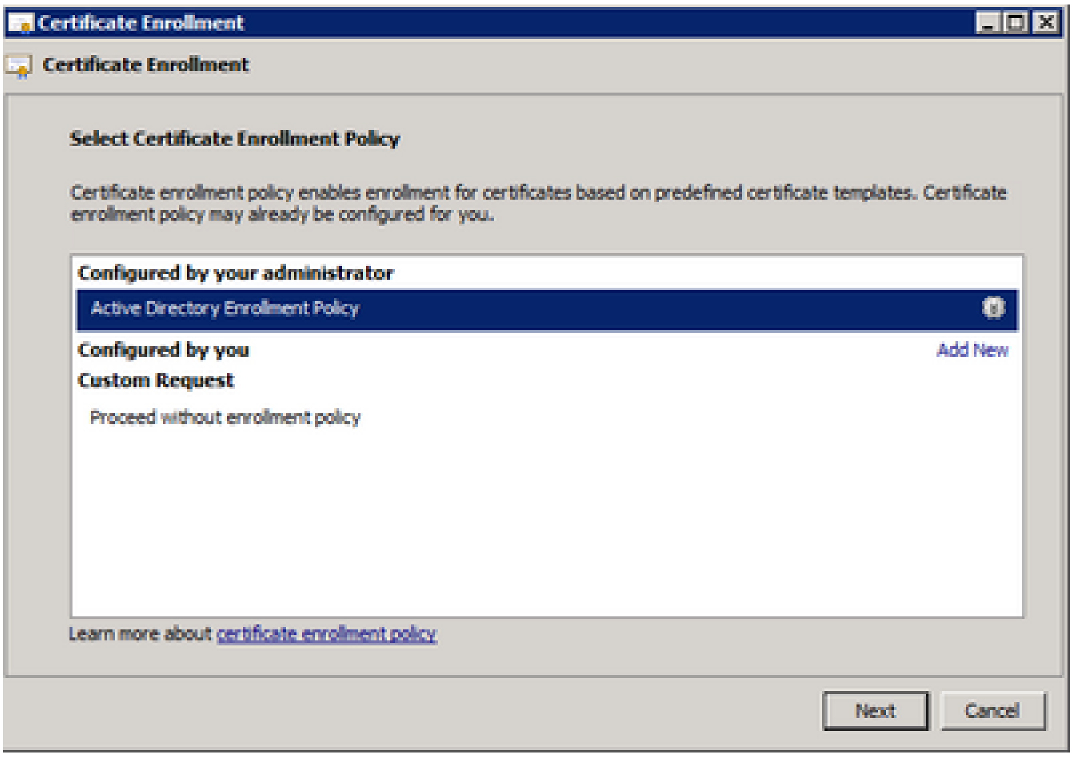
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Learn more about digital certificates

第五步：选择证书注册策略，然后选择**下一步**。



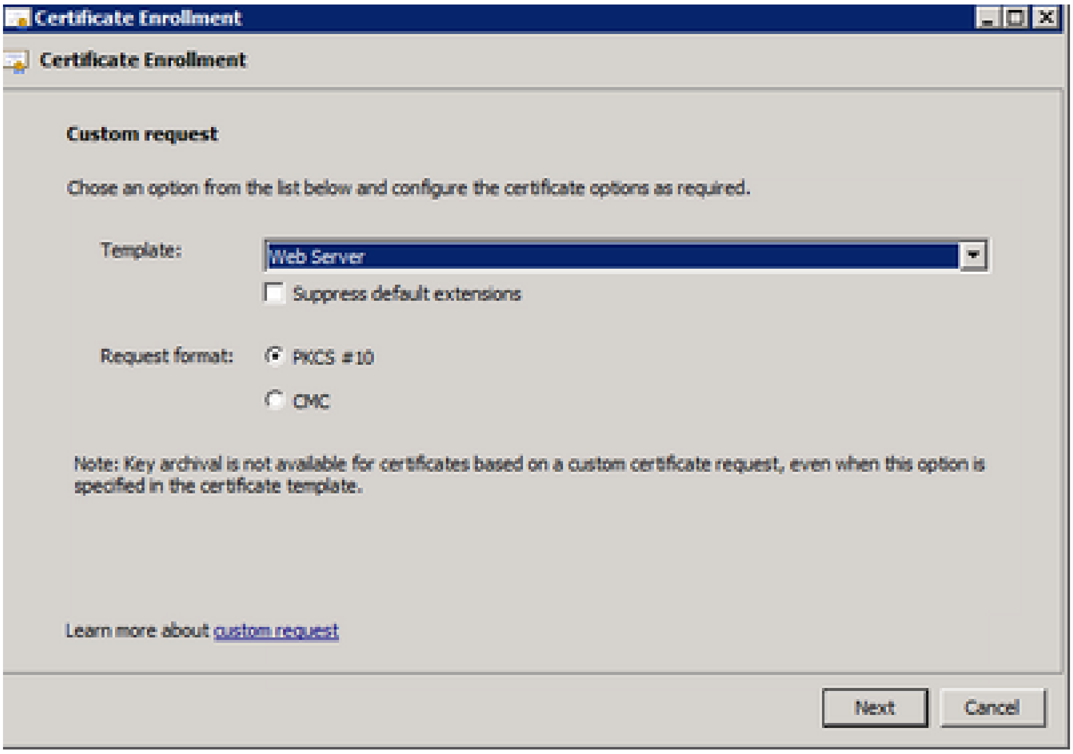
Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator
Active Directory Enrollment Policy
Configured by you
Custom Request
Proceed without enrollment policy

Learn more about certificate enrollment policy

第六步：选择模板作为Web Server，然后选择**下一步**。



Certificate Enrollment

Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template: Web Server

☐ Suppress default extensions

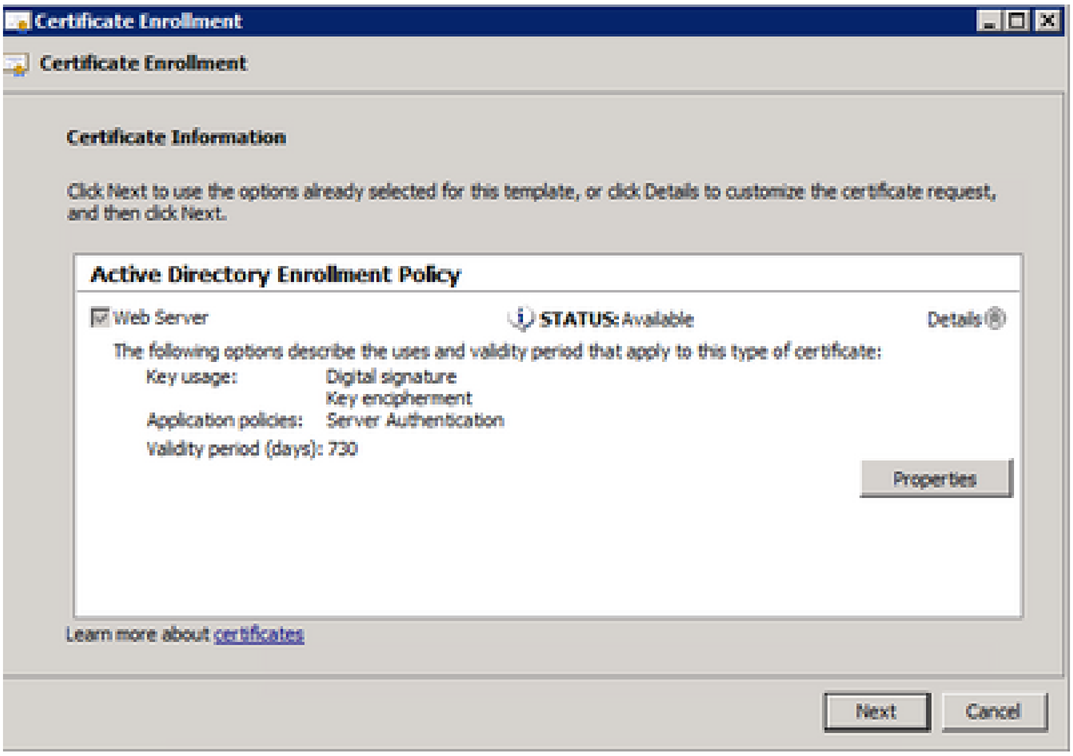
Request format: ● PKCS #10

○ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Learn more about custom request

步骤 7.如果您的“Web服务器”模板已正确配置且可用于注册，则会显示“可用”状态。选择**Details**展开Properties。



Certificate Enrollment

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Active Directory Enrollment Policy

☑ Web Server STATUS: Available Details

The following options describe the uses and validity period that apply to this type of certificate:

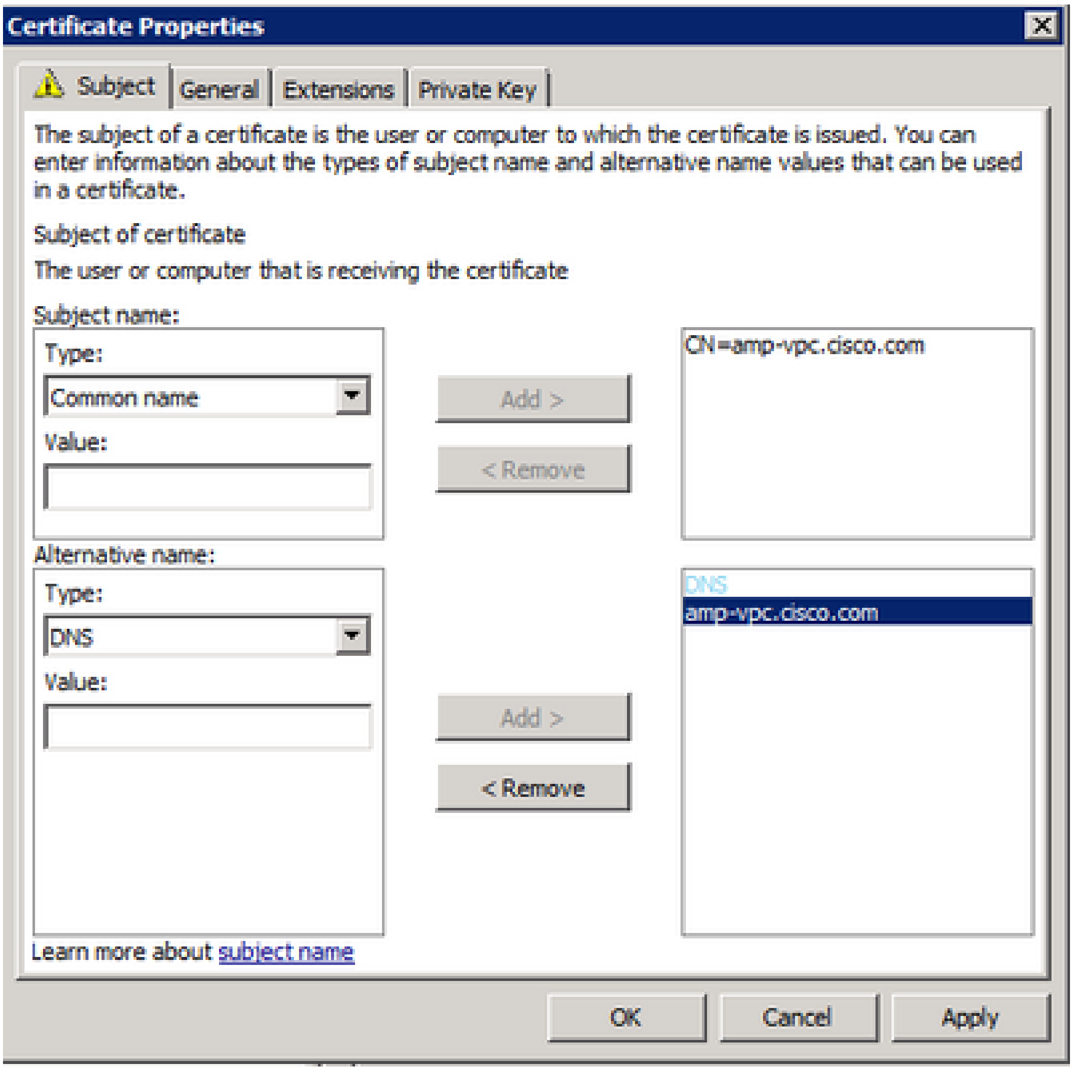
Key usage: Digital signature
Key encipherment

Application policies: Server Authentication

Validity period (days): 730

Learn more about certificates

步骤 8至少添加CN和DNS属性。可以根据您的安全要求添加其余属性。



Certificate Properties

Subject | General | Extensions | Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=amp-vpc.cisco.com

Alternative name:

Type: DNS

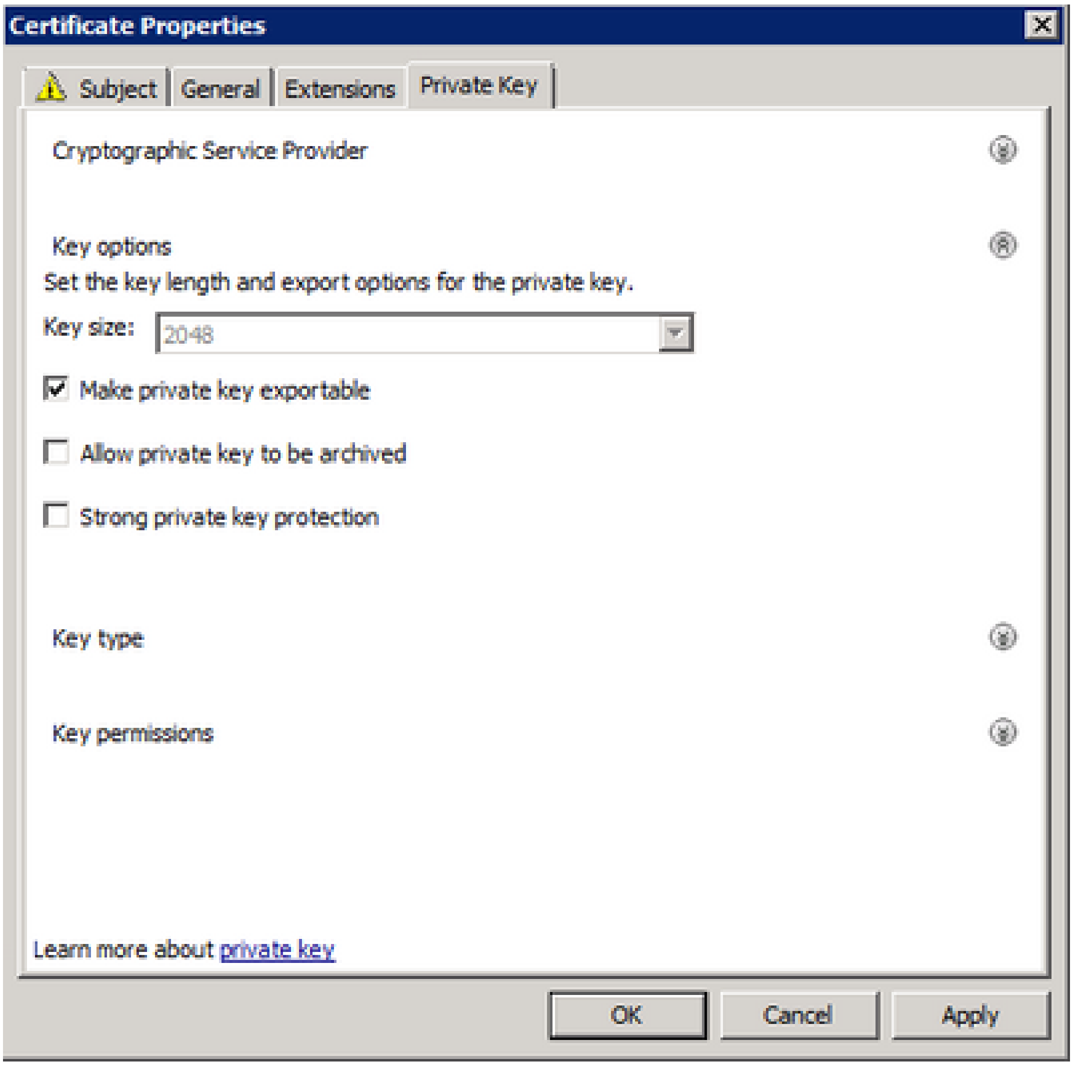
Value:

DNS
amp-vpc.cisco.com

Learn more about subject name

步骤 9或者，在**General**选项卡下提供一个友好名称。

步骤 10选择**Private Key**选项卡，并确保在**Key Options**部分下启用了**Make private key exportable**。



Cryptographic Service Provider

Key options

Set the key length and export options for the private key.

Key size: 2048

☑ Make private key exportable

□ Allow private key to be archived

□ Strong private key protection

Key type

Key permissions

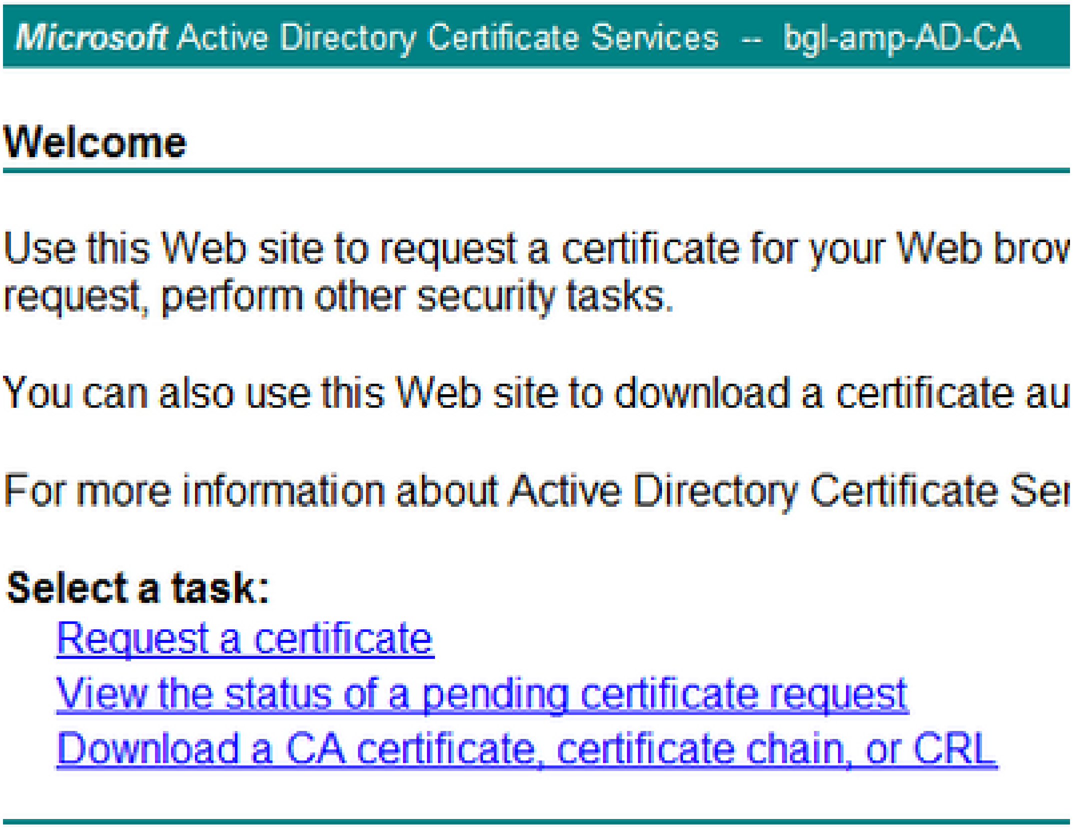
Learn more about private key

步骤 11最后，选择**OK**。这必须引导您进入Certificate Enrollment对话框，从中可以选择**Next**。

步骤 12浏览到保存提交到CA服务器进行签名的.req文件的位置。

向CA提交CSR并生成证书

步骤1:导航到您的MS AD证书服务网页（如下所示），然后选择**Request a Certificate**。



Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

Welcome

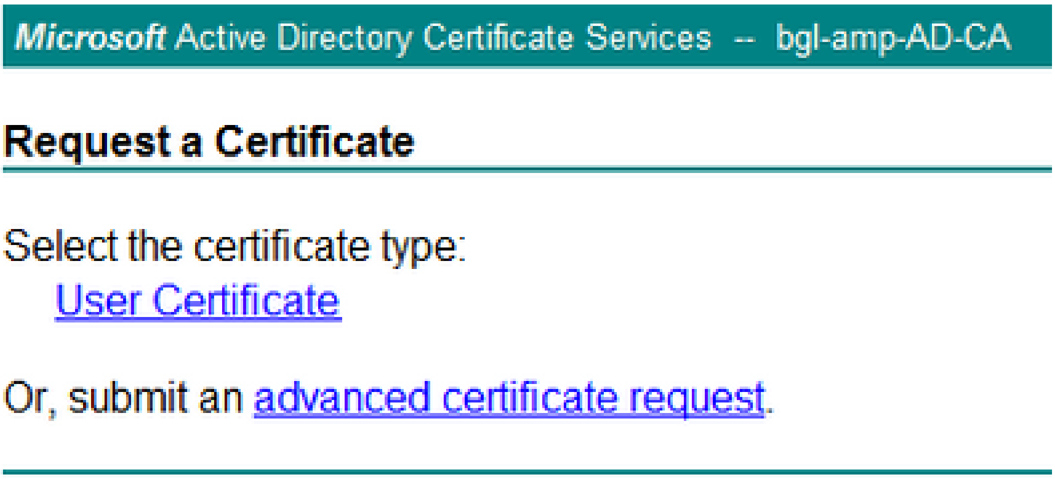
Use this Web site to request a certificate for your Web brov
request, perform other security tasks.

You can also use this Web site to download a certificate au

For more information about Active Directory Certificate Ser

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

第二步：选择**advanced certificate request链**接。



Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

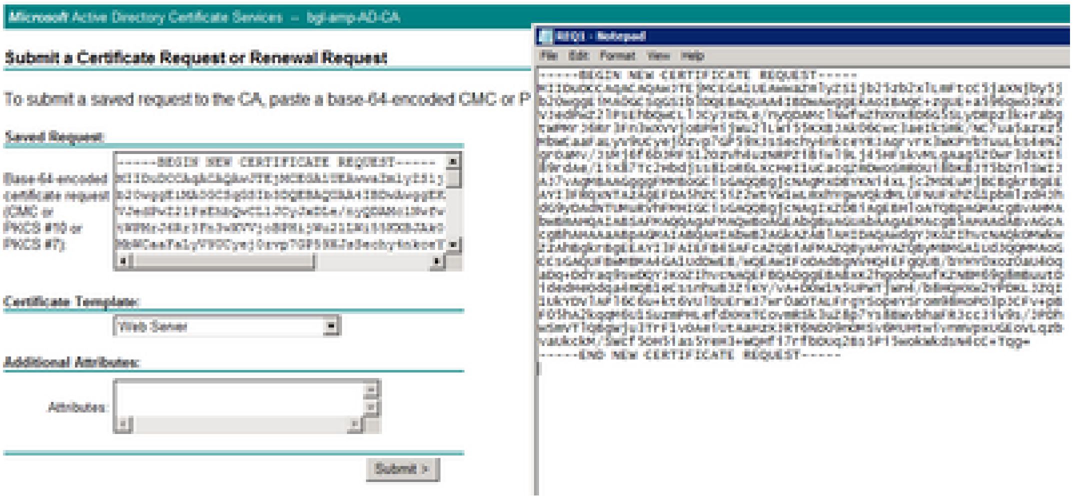
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

第三步：选择**Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file，或选择submit a renewal request by using a base-64-encoded PKCS #7 file**。

第四步：通过记事本打开以前保存的.req文件(CSR)的内容。复制内容并粘贴到此处。确保证书模板被选为Web**服务器**



Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or P

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
[illegible]
-----END NEW CERTIFICATE REQUEST-----
```

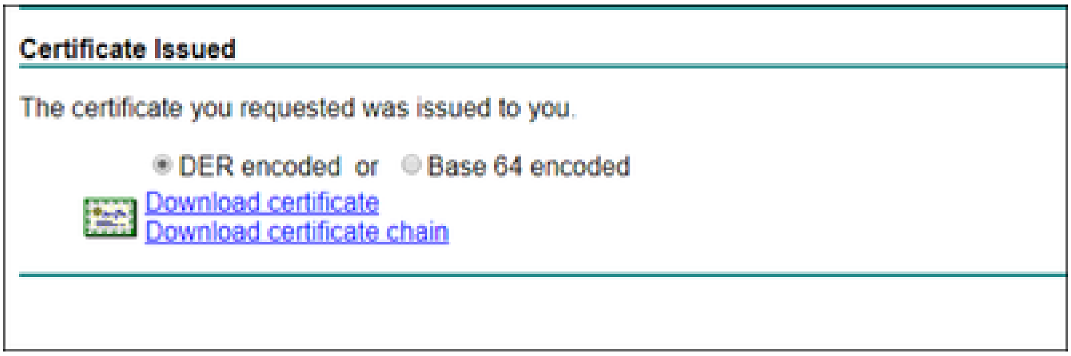
Certificate Template: Web Server

Additional Attributes:

Attributes:

第五步：最后，选择**Submit**。

第六步：此时，您必须能够下载**证书**，如图所示。



Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

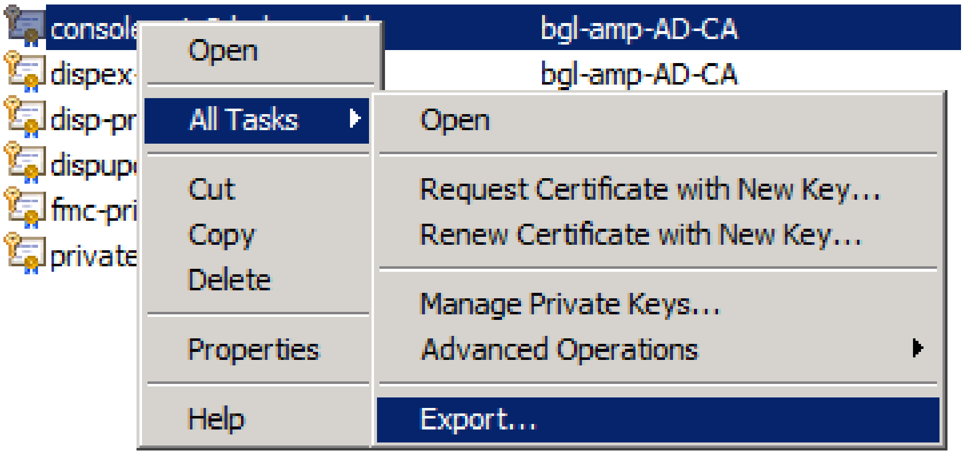
导出私钥并转换为PEM格式

步骤1:通过打开.cer文件并选择**安装证书**，将证书安装到证书存储区。

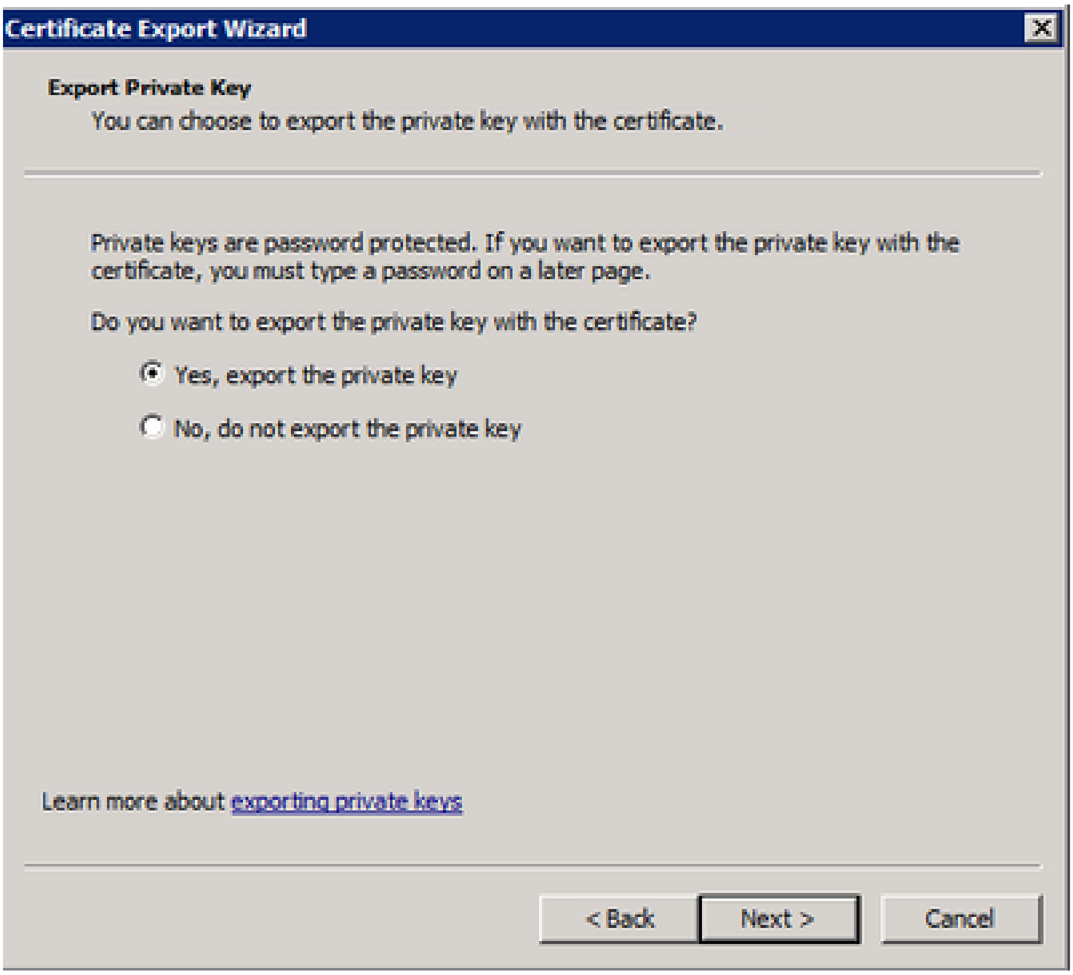
第二步：导航到之前选择的MMC管理单元。

第三步：导航到安装证书的商店。

第四步：右键单击正确的证书，选择**所有任务>导出。**



第五步：在证书导出向导中，确认导出私钥，如图所示。



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

第六步：输入密码，然后选择**Next**将私钥保存到磁盘上。

步骤 7.这会以.PFX格式保存私钥，但是，需要将其转换为.PEM格式才能将其用于安全终端私有云。

步骤 8安装OpenSSL库。

步骤 9打开命令提示符窗口，并切换到安装OpenSSL的目录。

步骤 10运行以下命令提取私钥并将其保存到新文件：（如果PFX文件与存储OpenSSL库的路径不同，则必须指定确切路径以及文件名）

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

步骤 11现在运行以下命令来提取公共证书并将其保存到新文件：

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

在Linux服务器上生成证书(Strict SSL check DISABLED)

注意:严格TLS检查验证证书是否符合Apple的TLS要求。有关详细信息，请参阅管理员指南。

确保您尝试生成所需证书的Linux服务器安装了OpenSSL 1.1.1库。验证此操作以及下面列出的过程是否可能与您运行的Linux发行版不同。此部分已编档，在CentOS 8.4服务器上完成。

生成自签名RootCA

步骤1:生成根CA证书的私钥。

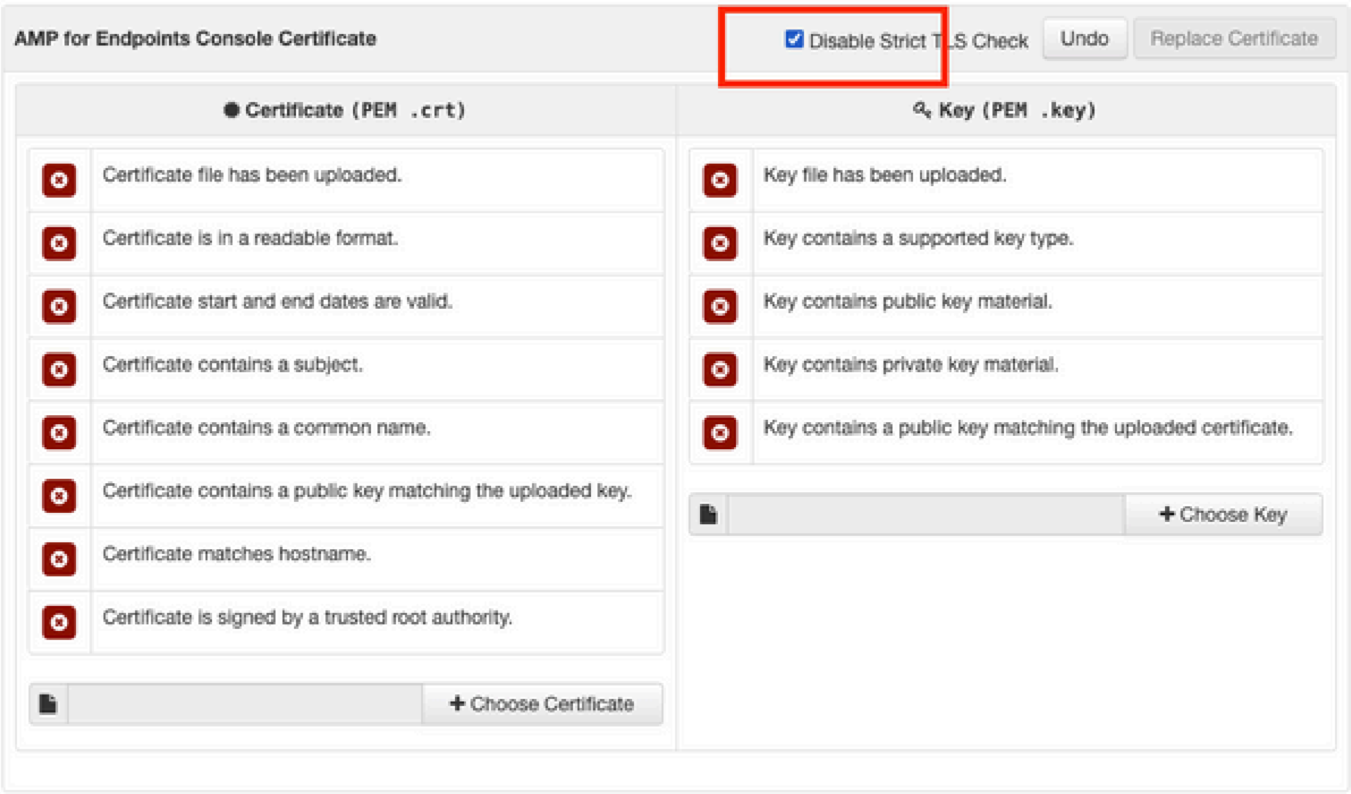
```
openssl genrsa -out
```

第二步：生成CA证书。

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

为每个服务生成证书

根据DNS名称条目为身份验证、控制台、性质、性质扩展、更新服务器、Firepower管理中心(FMC)服务创建证书。您需要为每个服务（身份验证、控制台等）重复以下证书生成过程。



AMP for Endpoints Console Certificate

☑ Disable Strict TLS Check

● Certificate (PEM .crt)

⊗ Certificate file has been uploaded.
⊗ Certificate is in a readable format.
⊗ Certificate start and end dates are valid.
⊗ Certificate contains a subject.
⊗ Certificate contains a common name.
⊗ Certificate contains a public key matching the uploaded key.
⊗ Certificate matches hostname.
⊗ Certificate is signed by a trusted root authority.

Key (PEM .key)

⊗ Key file has been uploaded.
⊗ Key contains a supported key type.
⊗ Key contains public key material.
⊗ Key contains private key material.
⊗ Key contains a public key matching the uploaded certificate.

生成私钥

```
openssl genrsa -out
```

将<YourServiceName.key>替换为要创建为Auth-Cert.key的新密钥文件名

生成 CSR

```
openssl req -new \
-subj '/CN=
-key
```

更换 <YourServiceName.key>使用当前（或新）证书KEY文件，例如Auth-Cert.key

将<YourServiceName.csr>替换为要创建的CSR文件名，例如Auth-Cert.crt

生成证书

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

将<YourServiceName.csr>替换为实际（或新）证书CSR，例如Auth-Cert.csr

将<YourRootCAName.pem>替换为实际（或新）的PEM文件名RootCAName.pem

使用当前（或新）证书KEY文件（例如Auth-Cert.key）替换<YourServiceName.key>

使用要创建的文件名（例如Auth-Cert.crt）替换<YourServiceName.crt>

在Linux服务器上生成证书（启用严格SSL检查）

注意:严格TLS检查验证证书是否符合Apple的TLS要求。有关详细信息，请参阅管理员指南。

生成自签名RootCA

步骤1:生成根CA证书的私钥。

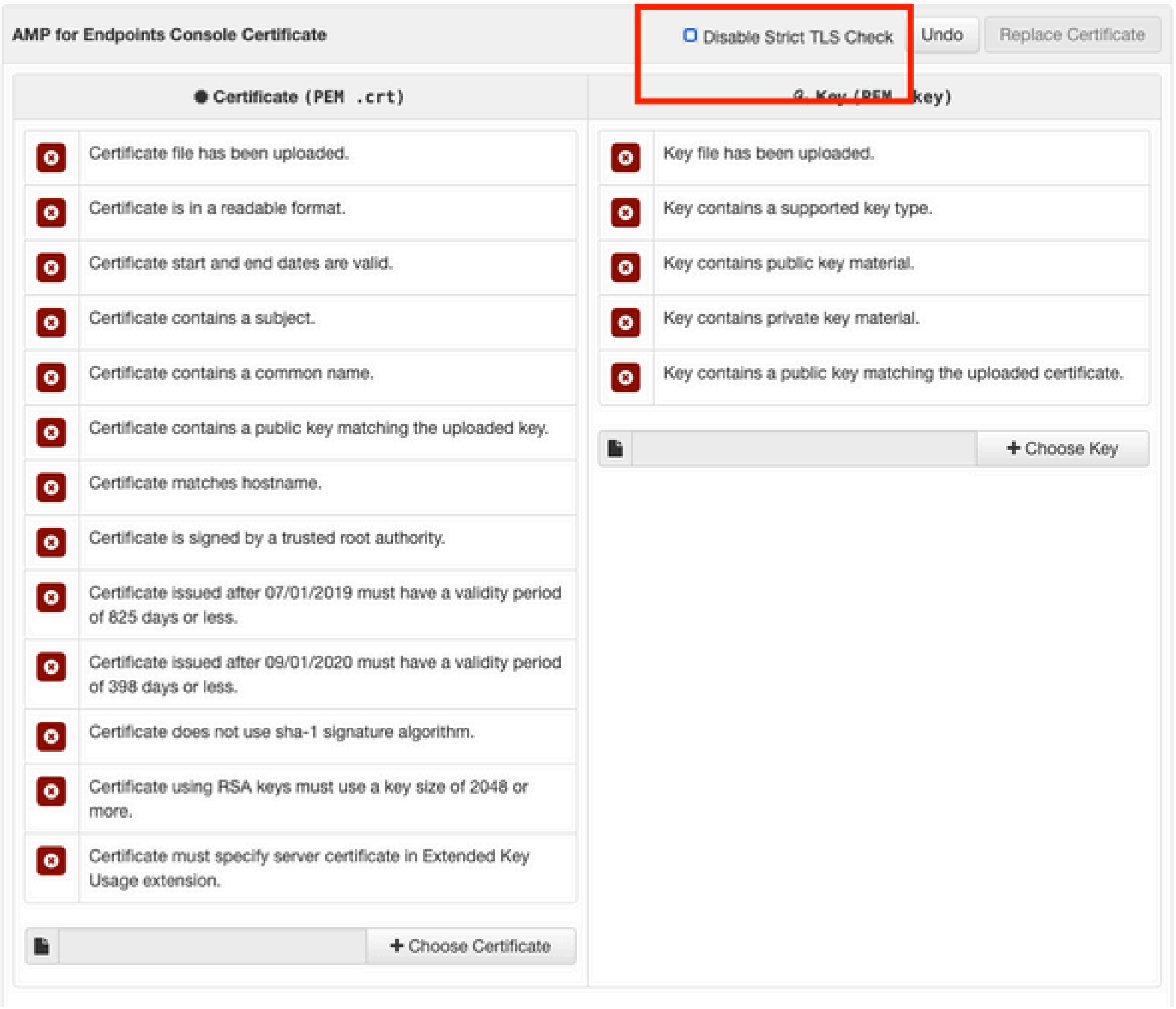
```
openssl genrsa -out
```

第二步：生成CA证书。

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

为每个服务生成证书

根据DNS名称条目为身份验证、控制台、性质、性质扩展、更新服务器、Firepower管理中心(FMC)服务创建证书。您需要为每个服务（身份验证、控制台等）重复以下证书生成过程。



AMP for Endpoints Console Certificate

□ Disable Strict TLS Check

● Certificate (PEM .crt)
Certificate file has been uploaded.
Certificate is in a readable format.
Certificate start and end dates are valid.
Certificate contains a subject.
Certificate contains a common name.
Certificate contains a public key matching the uploaded key.
Certificate matches hostname.
Certificate is signed by a trusted root authority.
Certificate issued after 07/01/2019 must have a validity period of 825 days or less.
Certificate issued after 09/01/2020 must have a validity period of 398 days or less.
Certificate does not use sha-1 signature algorithm.
Certificate using RSA keys must use a key size of 2048 or more.
Certificate must specify server certificate in Extended Key Usage extension.

Key (PEM .key)
Key file has been uploaded.
Key contains a supported key type.
Key contains public key material.
Key contains private key material.
Key contains a public key matching the uploaded certificate.

创建扩展配置文件并保存(extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

生成私钥

```
openssl genrsa -out
```

用要作为Auth-Cert.key创建的新KEY文件名替换<YourServiceName.key>

生成 CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

更换 <YourServiceName.key>使用当前（或新）证书KEY，例如Auth-Cert.key

使用当前（或新）证书CSR（例如Auth-Cert.csr）替换<YourServiceName.csr>

生成证书

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

使用当前（或新）证书CSR（例如Auth-Cert.csr）替换<YourServiceName.csr>

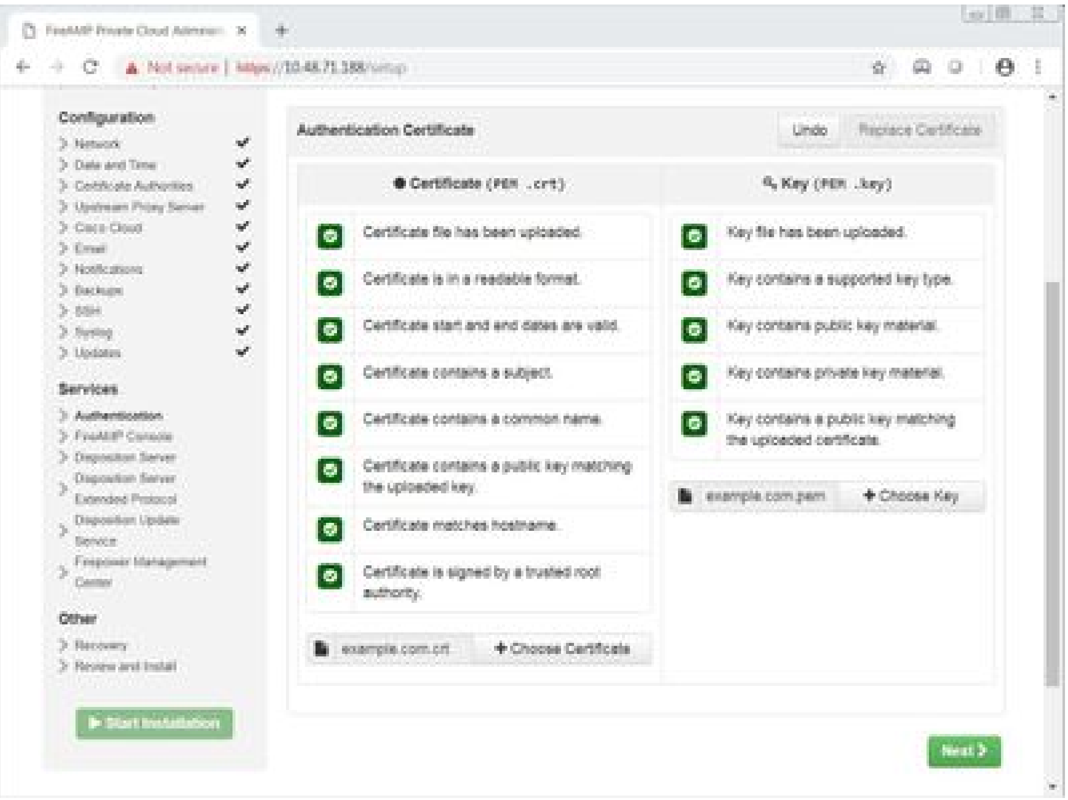
将<YourRootCAName.pem>替换为当前（或新）的PEM文件名RootCAName.pem

使用当前（或新）证书KEY文件（例如Auth-Cert.key）替换<YourServiceName.key>

使用要创建的文件名（例如Auth-Cert.crt）替换<YourServiceName.crt>

将证书添加到安全控制台私有云

步骤1:从上述任一方法生成证书后，上传每个服务的相应证书。如果正确生成，则会启用所有复选标记，如图所示。



Certificate file has been uploaded.

Certificate is in a readable format.

Certificate start and end dates are valid.

Certificate contains a subject.

Certificate contains a common name.

Certificate contains a public key matching the uploaded key.

Certificate matches hostname.

Certificate is signed by a trusted root authority.

example.com.crt

Key file has been uploaded.

Key contains a supported key type.

Key contains public key material.

Key contains private key material.

Key contains a public key matching the uploaded certificate.

example.com.pem

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

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）。