



证书

- [证书的要求和前提条件](#)，第 1 页
- [Cisco Secure Firewall Threat Defense VPN 证书准则和限制](#)，第 1 页
- [管理 威胁防御 证书](#)，第 2 页
- [使用自签注册安装证书](#)，第 5 页
- [使用 EST 注册安装证书](#)，第 6 页
- [使用 SCEP 注册安装证书](#)，第 7 页
- [使用手动注册安装证书](#)，第 7 页
- [使用 PKCS12 文件安装证书](#)，第 8 页
- [排除 威胁防御 证书问题](#)，第 9 页
- [证书的历史记录](#)，第 10 页

证书的要求和前提条件

支持的域

任意

用户角色

管理员

网络管理员

Cisco Secure Firewall Threat Defense VPN 证书准则和限制

- 如果 PKI 注册对象与某个设备关联并要安装在该设备上，证书注册过程将立即开始。对于自签名和 SCEP 注册类型，此过程将自动执行；它不需要任何额外的管理员操作。手动证书注册需要管理员操作。
- 注册完成后，设备上会出现一个信任点，其名称与 证书注册对象相同。在配置 VPN 身份验证方法时会使用此信任点。

- 威胁防御设备支持使用 Microsoft 证书颁发机构 (CA) 服务和思科自适应安全设备 (ASA) 和思科 IOS 路由器中提供的 CA 服务的证书注册。
- 威胁防御 设备无法配置为证书颁发机构 (CA)。

跨域和设备进行证书管理的准则

- 证书注册可以在子域或父域中完成。
- 当从父域执行注册时，证书注册对象也需要在同一个域中。如果该设备上的信任点在子域中被覆盖，则将在该设备上部署被覆盖的值。
- 当在分叶域中的设备上执行证书注册时，该注册对父域或其他子域是可见的。此外，还可以添加其他证书。
- 当一个叶域被删除时，将自动删除所包含的设备上的证书注册。
- 设备在一个域中注册了证书后，该设备将允许在其他任何域中进行注册。可以在其他域中添加该证书。
- 当您一台设备从一个域移动到另一个域时，还会相应移动证书。您将收到一个警报，要求您删除这些设备上的注册。

管理 威胁防御 证书

有关数字证书的介绍，请参阅[PKI 基础设施和数字证书](#)。

有关用于在托管设备上注册和获取证书的对象说明，请参阅[证书注册对象](#)。

过程

步骤 1 选择设备 > 证书。

您可以看到此屏幕上列出的每个设备的以下列：

- **名称**-列出已经与信任点关联的设备。展开设备可查看关联的信任点列表。
- **域**-显示特定域中注册的证书。
- **注册类型**-显示此信任点使用的注册类型。
- **状态**-提供 **CA 证书** 和 **身份证书** 的状态。当 可用时，您可以通过点击放大镜来查看证书内容。
查看 CA 证书信息时，可以查看颁发 CA 证书的所有证书颁发机构的层次结构。
如果注册失败，点击状态可显示故障消息。
- 点击右侧的 **启用弱密码**，启用证书中的弱密码使用。当您点击切换按钮时，系统会在启用弱密码之前收到警告确认。点击 **是** 以启用弱密码。

注释

当由于弱密码使用导致证书注册失败时，系统会提示您启用弱密码。您可以选择在需要使用弱加密时启用弱密码。

- 附加列列出了用于执行以下任务的图标：
 - **导出证书**-点击以导出并下载证书的副本。您可以选择导出 PKCS12（完整证书链）或 PEM（仅身份证书）格式。
您必须提供密码才能导出 PKCS12 证书格式，以便稍后导入文件。
 - **重新注册证书**-重新注册现有证书。
 - **刷新证书状态**-刷新证书会将 Firepower Threat Defense 设备证书状态同步到 Firepower 管理中心。
 - **删除证书**-删除信任点的所有关联证书。

步骤 2 选择 (+) 添加以关联注册对象，并在设备上安装该注册对象。

在证书注册对象与某个设备关联并安装到该设备后，证书注册过程将立即开始。对于自签名和 SCEP 注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。

注释

在设备上注册证书不会阻止用户界面，并且注册过程将在后台执行，从而使用户能够在其他设备上并行执行证书注册。在同一个用户界面可以监控这些并行操作的进度。各自的图标显示各自的证书注册状态。

相关主题

[使用自签注册安装证书](#)，第 5 页

[使用 SCEP 注册安装证书](#)，第 7 页

[使用手动注册安装证书](#)，第 7 页

[使用 PKCS12 文件安装证书](#)，第 8 页

自动更新 CA 捆绑包

您可以将管理中心设置为通过 CLI 命令自动更新 CA 证书。默认情况下，当您安装或升级到版本 7.0.5 时，CA 证书会自动更新。



注释

在仅 IPv6 部署中，CA 证书的自动更新可能会失败，因为某些思科服务器不支持 IPv6。在这种情况下，请使用 **configure cert-update run-now force** 命令强制更新 CA 证书。

过程

步骤 1 使用 SSH 登录 FMC CLI，或者打开 VM 控制台（如果是虚拟的）。

步骤 2 您可以验证本地系统中的 CA 证书是否是最新的：

configure cert-update test

此命令将本地系统上的 CA 捆绑包与最新的 CA 捆绑包（来自思科服务器）进行比较。如果 CA 捆绑包是最新的，则不会执行连接检查，并且会显示测试结果，如下所示：

示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

如果 CA 捆绑包已过期，则对下载的 CA 捆绑包执行连接检查，展示结果。

示例：

当连接检查失败时：

```
> configure cert-update test
Test failed, not able to fully connect.
```

示例：

当连接检查成功时，或者 CA 捆绑包已经是最新的：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

步骤 3 （可选）要立即更新 CA 捆绑包，请执行以下操作：

configure cert-update run-now

示例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

执行此命令时，将验证 CA 证书（来自思科服务器）以进行 SSL 连接。如果其中一台思科服务器的 SSL 连接检查失败，该流程也会终止。

示例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

要在连接失败的情况下继续更新，请使用 **force** 关键字。

示例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

步骤 4 如果您不希望自动更新 CA 捆绑包，请禁用配置：

```
configure cert-update auto-update disable
```

示例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

步骤 5 要重新启用 CA 捆绑包的自动更新：

```
configure cert-update auto-update enable
```

示例：

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

当您为 CA 证书启用自动更新时，系统将每天在系统定义的时间执行更新流程。

步骤 6 （可选）显示 CA 证书的自动更新状态。

```
show cert-update
```

示例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

使用自签注册安装证书

过程

步骤 1 在设备 > 证书屏幕上，选择添加，以打开添加新证书对话框。

步骤 2 从设备下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“自签名”类型的证书注册对象。
- 点击 (+)，以添加新的证书注册对象，请参阅[添加证书注册对象](#)。

步骤 4 按添加开始自动自签名注册过程。

对于自签名注册类型的信任点，**CA 证书** 状态将始终显示，因为托管设备会充当自己的 CA，而不需要 CA 证书来生成自己的身份证书。

身份证书 (Identity Certificate) 状态会在设备创建自己的自签身份证书时由“进行中” (InProgress) 转变为“可用” (Available)。

步骤 5 点击放大镜可查看为此设备创建的自签身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用 EST 注册安装证书

开始之前



注释 使用 EST 注册创建托管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。



注释 不支持 EST 在证书过期时自动注册设备的功能。

过程

步骤 1 在 **设备 > 证书** 屏幕上，点击 **添加** 以打开 **添加新证书** 对话框。

步骤 2 从设备下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从 **认证登记** 下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+) 添加新证书注册对象**，请参阅[添加证书注册对象](#)。

步骤 4 点击 **添加** 以在设备上注册证书。

身份证书 将在设备使用 EST 从指定的 CA 获取其身份证书后从 **进行中** 转变为 **可用**。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

使用 SCEP 注册安装证书

开始之前



注释 使用 SCEP 注册创建托管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

过程

步骤 1 在设备 > 证书屏幕上，选择添加，以打开添加新证书对话框。

步骤 2 从设备下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 SCEP 类型的证书注册对象。
- 点击 (+)，以添加新的证书注册对象，请参阅[添加证书注册对象](#)。

步骤 4 按安装，以开始自动注册过程。

对于 SCEP 注册类型信任点，CA 证书状态将在从 CA 服务器获取 CA 证书并安装在设备上后，从“进行中”过渡到“可用”。

身份证书将在设备使用 SCEP 从指定的 CA 获取其身份证书后从进行中转变为可用。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用手动注册安装证书

过程

步骤 1 在设备 > 证书屏幕上，选择添加，以打开添加新证书对话框。

步骤 2 从设备下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“手动”类型的证书注册对象。
- 点击 (+)，以添加新的证书注册对象，请参阅[添加证书注册对象](#)。

步骤 4 按添加，以开始注册过程。

步骤 5 使用 PKI CA 服务器执行适当的活动，以获取身份证书。

- a) 点击 **身份证书** 警告图标以查看和复制 CSR。
- b) 使用 PKI CA 服务器执行适当的活动，以使用此 CSR 获取身份证书。

此活动完全独立于 Cisco Secure Firewall Management Center 或托管设备。完成后，您将获得托管设备的身份证书。您可以将其放置在文件中。

- c) 要完成手动过程，请将获得的身份证书安装到托管设备。

返回到 Cisco Secure Firewall Management Center 对话框，并选择 **浏览身份证书** 以选择身份证书文件。

注释

确保不要选择二进制证书（PKCS12、DER 等）文件，因为 威胁防御 不支持这些文件。

步骤 6 选择 **导入 (Import)** 以导入身份证书。

导入完成时，身份证书状态将为 Available。

步骤 7 点击放大镜可查看此设备的身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用 PKCS12 文件安装证书

过程

步骤 1 转至设备 > 证书屏幕，然后选择添加，以打开添加新证书对话框。

步骤 2 从设备 (Device) 下拉列表中选择预先配置的托管设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 PKCS 类型的证书注册对象。
- 点击 (+) 添加新证书注册对象，请参阅[添加证书注册对象](#)。

步骤 4 按添加 (Add)。

CA 证书和身份证书状态会在其在设备上安装 PKCS12 文件时从 In Progress 变为 Available。

注释

第一次上传 PKCS12 文件时，该文件作为 CertEnrollment 对象的一部分存储在管理中心。对于因密码错误或部署失败导致的任何失败注册，请重试注册 PKCS12 证书，无需再次上传文件。此外，每当您修改证书注册对象以允许覆盖时，都必须更新证书的 **密码** 才能成功注册。PKCS12 文件的大小不应超过 24K。

步骤 5 状态转变为可用 (Available) 后，请点击放大镜查看此设备的身份证书。

下一步做什么

托管设备上的证书（信任点）的名称与 PKCS#12 文件的名称相同。在 VPN 身份验证配置中使用此证书。

排除 威胁防御 证书问题

请参阅 [Cisco Secure Firewall Threat Defense VPN 证书准则和限制](#)，第 1 页 确定您的证书注册环境中的变体是否可能导致问题。然后，考虑以下事项：

- 确保存在从设备到 CA 服务器的路由。

如果在注册对象中给出了 CA 服务器的主机名，请使用 Flex Config 来配置 DNS 以适当方式到达服务器。或者，使用 CA 服务器的 IP 地址。

- 如果您使用的是 Microsoft 2012 CA 服务器，则托管设备不接受默认的 IPsec 模板，必须更改模板。

请参阅您使用 MS CA 文档时的以下步骤来配置工作模板。

1. 复制 IPsec（脱机请求）模板。
2. 在扩展 (Extensions) > 应用策略 (Application policies) 中，请选择 *IP 安全端系统 (IP security end system)*，而不是 *IP 安全 IKE 中间系统 (IP security IKE intermediate)*。
3. 设置权限和模板名称。
4. 添加新模板并更改注册表设置以反映新的模板名称。

- 在管理中心上，您可能会收到与威胁防御设备相关的以下运行状况警报：

代码 - F0853: Description - default Keyring's certificate is invalid, reason: expired

在这种情况下，请使用以下命令在 CLISH CLI 中重新生成默认证书：

```
> system support regenerate-security-keyring default
```

- CA 证书状态中出现一个红色叉，并伴随出现以下错误：

未能配置 CA 证书

解决方案：请参阅[对 FMC 上的证书错误进行故障排除](#)。

- 要检查 .pfx 文件中的证书列表，请使用 `certutil` 或 `openssl` 等工具。您可以查看包含 ID 证书、子 CA 证书和 CA 证书（如有）的整个证书链。

- `certutil -dump cert.pfx`
- `openssl pkcs12 -info -in cert.pfx`

- 会出现以下错误：

需要导入身份证书

解决方案：请参阅[对 FMC 上的证书错误“需要导入身份证书 \(Identity certificate import required\) 进行故障排除”](#)。

证书的历史记录

功能	管理中心最低版本	威胁防御最低版本	详细信息
支持 OCSP 和 CRL IPv6 URL	7.4	任意	您现在可以添加 IPv6 OCSP 和 CRL URL 以进行证书身份验证（吊销检查）。IPv6 地址必须用方括号括起来。
手动注册的增强功能	6.7	任意	您现在无需身份证书即可以仅创建 CA 证书。您也可以在没有任何 CA 证书的情况下生成 CSR，并从 CA 获得身份证书。
PKCS CA 链	6.7	任意	您可以查看和管理颁发证书的证书颁发机构 (CA) 链。您也可以导出证书的副本。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。