

SSL 证书 - Cisco

证书安装指南

请选择您的版本

[Cisco ISE SSL 安装指南](#)

[Cisco ACS 3.2 SSL 安装指南](#)

[Cisco Secure ACS 4.2 SSL 安装指南](#)

[使用命令行界面安装 Cisco ASA 5000 SSL 证书指南](#)

[Cisco ASA 5510 SSL 证书安装指南](#)

[Cisco ASA 5520 SSL 安装指南](#)

Cisco ISE SSL 安装指南

步骤 1: 获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

3. 把文件存档为 SSLCert.cer。

步骤 2: 下载 Intermediate CA 证书

1. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

2. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.cer。

步骤 3: 安装 SSL 证书

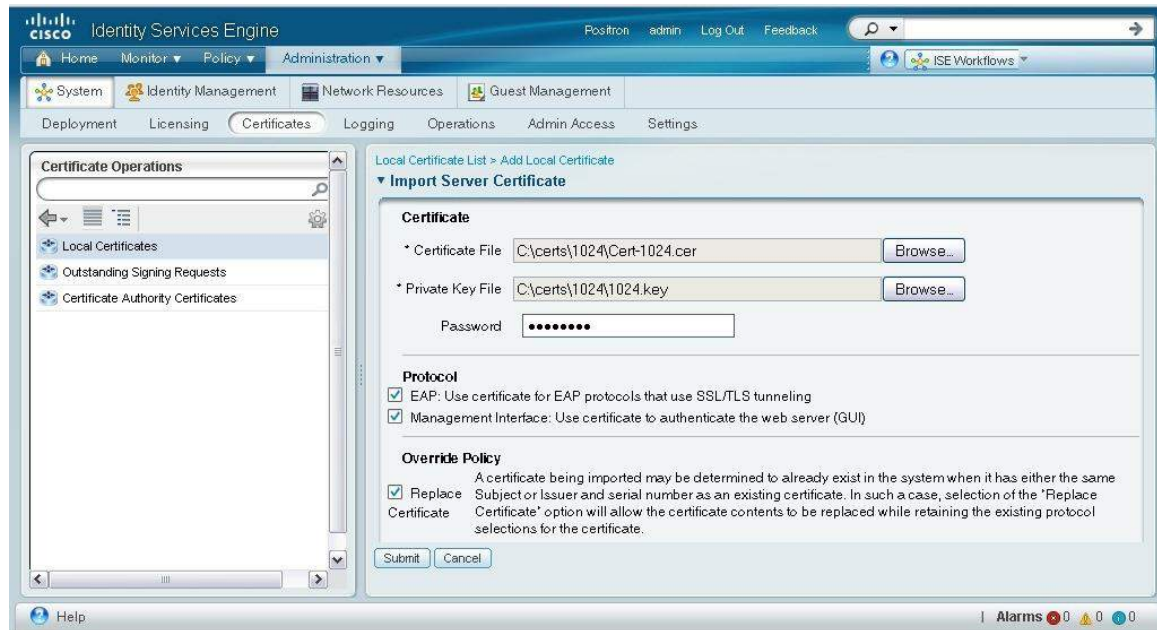
1. 选择 Administration > System > Certificates。
2. 从 Certificate Operations 导航窗格中，点击 Local Certificates。

注：要把本地证书导入辅助节点，请选择 **Administrative > System > Server**

Certificate。

3. 选择 **Add > Import。**

4. **Import Local Server Certificate** 页面将会显示如下：



5. 点击 **Browse** 选择证书文件，以及运行您客户浏览器的系统的私钥。

6. 如果私钥已被加密，输入密码解密。

7. 在 **Protocol** 页面：

- 点选 **EAP** 复选框以使用此证书的 **EAP** 协议以确认 **Cisco ISE** 节点。
- 点选 **Management Interface** 复选框以使用此证书验证 **Web 服务器（GUI）**。

注：如你已点选 **Management Interface**，确保在 **CN** 栏里的 **Certificate Subject** 填上证书的完全域名，否则流程将会失败。

8. 在 **Override Policy** 选项，点选 **Replace Certificate** 以使用替代证书代替现有证书。

注：如如果证书拥有与现有证书相同发行人和相同的序号，它将会被视为替代证书。此选项是为了更新证书的内容，但保留证书的协议。

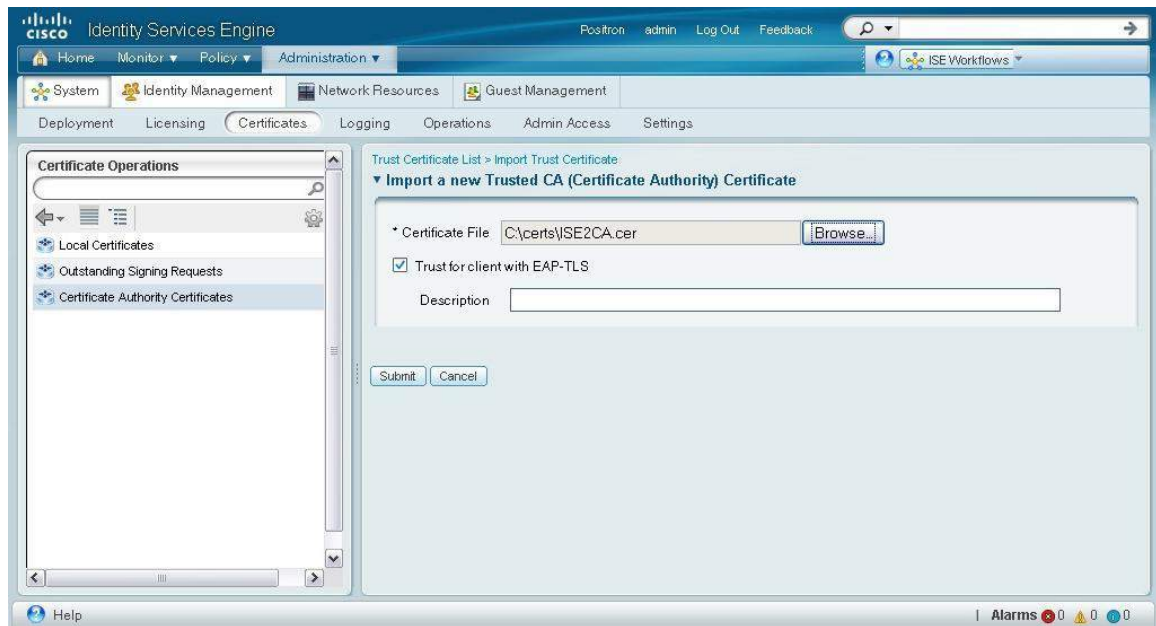
9. 点击提交以导入本地证书。

注：如果你把证书导入你的主要 Cisco ISE 节点，你必须重启你的辅助 Cisco ISE 节点以连接你的主要 Cisco ISE 节点。请使用命令行页面（CLI）输入以下指令以重启你的辅助节点：

- a. application stop ise
- b. application start ise

步骤 4：安装 Intermediate CA 证书

1. 选择 **Administration > System > Certificates**。
2. 在左则的 **Certificate Operations** 导航窗格中，点击 **Certificate Authority Certificates**。
3. **Certificate Authority Certificates** 页面将会出现。
4. 点击 **Add**。
5. **Import Trusted CA (Certificate Authority) Certificate** 页面将会显示如下：



6. 点击 Browse 选择运行你客户的浏览器的 CA 证书。
7. 如果你要把此证书用于客户的 EAP-TLS 协议的信任列表，请点选 Trust for client with EAP-TLS 选项。

注：如果 Trust for client with EAP-TLS 选项已被点选，请确认 keyUsage 扩展已显示，同时 keyCertSign 已设置，以及 basic constraints 扩展已显示并把 CA 标志设定为 true。

8. 加入描述（可选）。
9. 点击提交以保存 CA 证书。

注：如果你把证书导入你的主要 Cisco ISE 节点，你必须重启你的辅助 Cisco ISE 节点以连接你的主要 Cisco ISE 节点。请使用命令行页面（CLI）输入以下指令以重启你的辅助节点：

- a. application stop ise
- b. application start ise

10. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

Cisco ACS 3.2 SSL 安装指南

步骤 1：下载 Intermediate CA 证书

3. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

4. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.cer。

步骤 2：安装 CA 证书

1. 在导航栏里，点击 System Configuration。
2. 点击 ACS Certificate Setup。
3. 点击 ACS Certification Authority Setup。
4. CiscoSecure ACS 会在 Cerification Authorities Setup 页面下显示 CA Operations 列表。
5. 在 CA Certificate 一栏中，输入你的 CA 证书的完整路径以及文件名。
6. 查找并导入 intermediate.cer。
7. 点击提交。

步骤 3：获取 SSL 证书

4. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
5. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

6. 把证书存档为 .cer 文档。

步骤 4：安装 SSL 证书

1. 在导航栏里，点击 **System Configuration**。
2. 点击 **ACS Certificate Setup**。
3. 点击 **Install ACS Certificate**。
4. CiscoSecure ACS 将会显示 **Install ACS Certificate** 页面。
5. 在文件选项中选择 **Read certificate**，然后在 **Certificate** 栏中输入证书文件的完整路径以及文件名称。
6. 在 **Private Key** 栏中，输入私钥文件的完整路径以及文件名称。
7. 在 **Private Key Password** 栏中，输入私钥的密码。
8. 点击提交。
9. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

Cisco

欲知更多详情，请浏览 [Cisco 客服网站](#)。

Cisco Secure ACS 4.2 SSL 安装指南

步骤 1: 获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

3. 把文档保存为 SSLCert.cer。

步骤 2: 下载 Intermediate CA 证书

5. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

6. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.cer。

步骤 3: 把证书和 CA 证书复制至 ACS 主机

1. 在 ACS 主机上创建一个 \certs 目录。
2. 开启 DOS 命令窗口。
3. 输入以下指令以创建证书目录：

```
mkdir <selected_drive>:\certs
```

注：“selected_drive”即是目前使用的驱动器。

4. 把下列文件（范例）复制至 \certs 目录。

ACS-1.nac.cisco.com.cer (server SSL certificate)

ACS-1.PrivateKey.txt (server certificate private key)

ca.nac.cisco.com.cer (CA certificate)

步骤 4：设置 ACS Certification Authority

1. 你需[下载 Root CA 证书](#)以设置 ACS Certification Authority.

2. 在导航栏里，点击 **System Configuration**。

System Configuration 页面将会出现。

3. 点击 **ACS Certificate Setup**。

ACS Certificate Setup 页面将会出现。

4. 点击 **ACS Certification Authority Setup**。

ACS Certification Authority 页面将会显示如下：



5. 输入 CA 证书的存档路径以及文件名后点击提交。
6. 重启 ACS。

选择 **System Configuration > Service Control** 然后点击 **Restart** 重启 ACS。

步骤 5：编辑证书信任列表

注：在设置 ACS Certification Authority 后，你必须把 CA 证书加入 ACS 证书信任列表。

1. 在导航栏里，点击 **System Configuration**。

System Configuration 页面将会开启。

2. 选择 **ACS Certificate Setup > Edit Certificate Trust List**。

Edit Certificate Trust List 页面将会出现。

3. 在证书列表中，点选你已安装的 CA 证书。
4. 点击提交。
5. 选择重启 ACS。

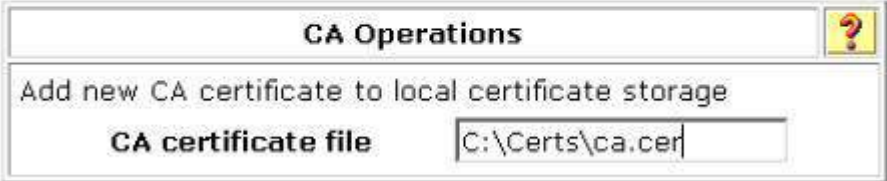
选择 **System Configuration > Service Control** 然后点击 **Restart** 重启 ACS。

步骤 6：安装 Intermediate CA 证书

1. 选择 **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**。

ACS Certification Setup 页面将会显示如下：

ACS Certification Authority Setup



CA Operations ?	
Add new CA certificate to local certificate storage	
CA certificate file	C:\Certs\ca.cer

2. 在 CA certificate file 文字框中，输入 CA 证书的储存路径和文件名；例：

c:\Certs\ca.cer。

3. 点击提交。

步骤 7：安装 SSL 证书

1. 在导航栏里，点击 System Configuration。

System Configuration 页面将会出现。

2. 点击 ACS Certificate Setup。

3. 点击 Install ACS Certificate。

Install ACS Certificate 页面显示如下：



Install new certificate

☒ Read certificate from file

Certificate file C:\Certs\server.cer

☐ Use certificate from storage

Certificate CN

Private key file C:\Certs\server.pvk

Private key password ****

4. 选择 Read certificate from file 选项。
5. 在 Certificate file 文字框里，输入证书的储存路径和文件名；例：c:\Certs\server.cer.
6. 在 Private key file 文字框里，输入主机证书的储存路径和文件名；例：
c:\Certs\server.pvk.
7. 在 Private Key password 文字框里，输入私钥密码，例：cisco123。
8. 点击提交。

9. ACS 将会显示证书已成功安装的消息，然后指示你重启 ACS 服务。
10. 重启 ACS。选择 **System Configuration > Service Control** 然后点击 **Restart** 重启 ACS。
11. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

使用命令行界面安装 Cisco ASA 5000 SSL 证书指南

步骤 1: 获取 SSL 证书

7. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
8. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

9. 把证书存档为 SSLCert.txt。

步骤 2: 下载 Intermediate CA 证书

7. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

8. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.txt。

步骤 3: 安装 Intermediate CA 证书至 Trustpoint

1. 在命令行界面，输入以下指令：

```
ciscoasa(config)#crypto ca authenticate <Trustpoint name>.Trustpoint
```

2. 你将会被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself” 。
3. 开启 `intermediate.txt`，把内容复制后粘贴至命令行界面。
4. 确定 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 作为开头和结尾。

例：

Enter the base 64 encoded certificate.

End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIIE0DCCBDmgAwI`BAglQJQzo4DBhLp8r`ifcFTXz4/TANBgkqhkiG9w0BAQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOV`mVyaVNpZ24s`lEluYy4xNzA1BgNVBAs
T
LkNsYXNzIDMgUHVibGljIFByaW1hc`nkqQ2VydGlmaWNhdGl`vb`iBBdXRob3JpdHkw`
HhcNMDYxMTA4MDAwMDAwWhcNMjExMTA3MjM1OTU5WjCBYjELMAkGA1UEBhMCV
Mx
FzAVBgNVBAoTDlZlcm`lTaWduLCBJbmMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVz`
dCBOZX`R3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZv`
ciBhdX`Rob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDdGFzcyAz`
IFB1Ym`xpYyBQcmItYXJ5IEIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEi`
MA0GCSqGS`Ib3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAglKXo1nmAMqudLO07cfLw8`
RRy7K+D+KQL5V`wijZIUVJ/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70Pb`
ZmIVYc9gDaTY3`vjgw2IIPVQT60nKWVSfJuUrjxuf6/WhkclzSdhDY2pSS9KP6HBR`

TdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9Kil8q8ckmcY5fQGBO+QueQA5N06tRn/
Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNH
iDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/NleWiu5T6CUVAgMB
AAGjggGbMIIBlZAPBgNVHRMBAf8EBTADAQH/MDEGA1UdHwQqMCgwJqAkoCKGIGh0
dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA4GA1UdDwEB/wQEAwIBBjA9
BgNVHSAENjA0MDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVy
aXNpZ24uY29tL2NwczAdBgNVHQ4EFgQUf9Nlp8Ld7LvwMANzQzn6Aq8zMTMwbQYI
KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGg
QU
j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nby5naWYwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBzABhhhodHRwOi
8v
b2NzcC52ZXJpc2lnbi5jb20wPgYDVR0lBDcwNQYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDAwYJYIZIAYb4QgQBbgpghkgBhvhFAQgBMA0GCSqGSib3DQEBBQUA
A4GBABMC3fjohgDyWvj4lAxZiGIHzs73Tvm7WaGY5eE43U68ZhjTresY8g3JbT5K
lCDDPLq9ZVTGr0SzEK0saz6r1we2uIFjxfleLuUqZ87NMwwq14lWAYmfs77oOghZ
tOxFNfeKW/9mz1Cvxm1XjRl4t7mi0VfqH5pLr7rJjhJ+xr3/
-----END CERTIFICATE-----
quit

Manually pasted certificate into CLI.

INFO: Certificate has the following attributes:

Fingerprint: 32 f3 08 82 62 2b 87 cf 88 56 c6 3d b8 73 df 08 53 b4 dd 27

5. 一旦提交 **Intermediate CA** 证书，你将会被提示是否接受证书，回答 ” Yes” 。

Do you accept this certificate? [yes/no]: **yes**

提交后，系统将会显示：

Trustpoint <name of Trustpoint> is a subordinate CA and

holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported

ciscoasa(config)#

ciscoasa(config-ca-trustpoint)# **exit**

6. 开启 Trustpoint，并以以下命令安装二级证书：

ciscoasa(config)#**crypto ca authenticate <Trustpoint name>.Trustpoint**

7. 你将会被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself” 。

步骤 4：安装 SSL 证书

1. 为了使用命令行页面，你必须输入以下指令：

```
ciscoasa(config)#crypto ca import <Trustpoint name>.Trustpoint certificate
```

2. 你将会被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself” 。
3. 开启在步骤 1 创建的 `SSLCert.txt`，把内容发复制后粘贴至命令行页面。
4. 确定 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 作为开头和结尾。

注：以下证书只作为参考，并非真正证书。

证书里的完全限定域名 (FQDN) : <你证书里的 Common Name>

Enter the base 64 encoded certificate.

End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVWMxZzAVBgNVBAoTDIzlcm1TaWduLCBJbmMuMTAwLgYDVQQQ
L
EydGb3IgVGZzdCBQdXJwb3NlcyBPbm55LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAStOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNI
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox
CzAJBgNVBAYTAiVTRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2l2Y28gU3lzdGVtczEOMAwGA1UECxQFVFNXRUIx
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90

ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjb20wgZ8wDQY

J

KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRIJeJKCrQ/9kER2JQ

9UOkUP3mVPZJtYN63ZxDwACeyNb+lildKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R

IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgryosBMMazg

5IcLhgSpAgMBAAGjggHXMIIBozAJBgNVHRMEAjaAMAsGA1UdDwQEAwIFoDBDBgNV

HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJLLWNybc52ZXJpc2lnbi5jb20v

U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAv

Bggr

BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYD

UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECmQVFNXRUIx

Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDov

L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzACHjZodHRwOi8vU1ZSU2VjdXJl

LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYIKwYBBQUH

AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5KJY

G

DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n

bzEuZ2lmMA0GCSqGS1b3DQEBBQUAA4IBAQAnym4GVThPlyL/9ylDBd8N7/yW3Ov3

blirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNNDomn4xRXQTUDD8q86ZiKyMIj

XM2VCmcHSajmMMRyjpydxfk6CldDMtMGotCavRHD9Tl2tvwgrBock/v/54o02lkB

SmLzVV7crlYJEUhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FSewy8MAIY

rtab5F+oiTc5xGy8w7NARAFNgFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td

0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O

-----END CERTIFICATE-----

quit

INFO: Certificate successfully imported

ciscoasa(config)#

步骤 5：设置使用你的 SSL 证书的接口的 Trustpoint

1. 使用以下指令更新 Trustpoint:

```
ciscoasa(config)#ssl trust-point <Trustpoint name>.Trustpoint outside
```

```
ciscoasa(config)#wr mem
```

Building configuration...

Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08

8808 bytes copied in 3.630 secs (2936 bytes/sec)

[OK]

```
ciscoasa(config)#
```

步骤 6：验证证书和证书链

1. 输入以下指令验证你刚刚安装的证书:

```
ciscoasa(config)#show crypto ca certificates
```

2. 你也可以使用 Symantec 的[证书检查工具](#)。

Cisco ASA 5510 SSL 证书安装指南

步骤 1：下载 Root CA 证书和 Intermediate CA 证书

注：若使用 Cisco ASDM 6.3 或 6.1，你必须在生成 RSA 密钥之前安装 Root 和 Intermediate CA 证书。

1. [点击此下载 Root CA 证书](#)。
2. [点击此下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

步骤 2：安装 Root CA 证书

1. 在 ASDM 里，点击 Configuration > Device Management。
2. 点击 Certificate Management > CA Certificates。
3. 点击 “Add” 。
4. 点击 Paste Certificate in PEM Format > 把 Root CA 证书粘贴至文字框里。
5. 点击安装证书。

对话框将会出现，显示证书已成功安装。

步骤 3：安装 Intermediate CA 证书

1. 在 ASDM 里，点击 Configuration > Device Management。
2. 点击 Certificate Management > CA Certificates。
3. 点击 “Add” 。
4. 点击 Paste Certificate in PEM Format > 把 Intermediate CA 证书粘贴至文字框里。

5. 点击安装证书。

对话框将会出现，显示证书已成功安装。

步骤 4：获取 SSL 证书

10. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

11. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

12. 把文件存档为 SSLCert.pem。

步骤 5：安装 SSL 证书

1. 点击 Configuration > Device Management。
2. 点击 Certificate Management > Identify Certificates。
3. 选择你所创建的标识（逾期日期将会显示为 Pending）。
4. 点击“安装”。
5. 点击 Paste the certificate data in base-64 format > 把证书复制并粘贴至文件筐。
6. 点击“安装证书”。

对话框将会出现，显示证书已成功安装。

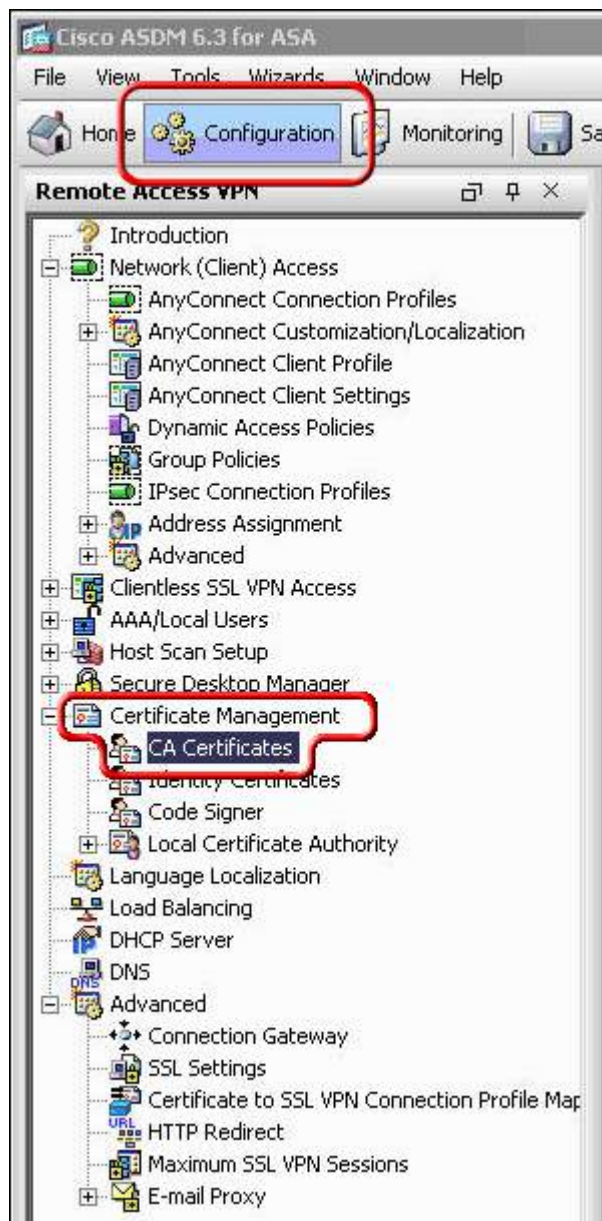
步骤 6：激活 SSL 证书

1. 点击 **Configuration > Device Management**。
2. 展开 **Advanced**，然后展开 **SSL Settings**。
3. 在 **Certificates** 选项下，选择终结 **WebVPN** 的界面。
4. 选择“编辑”。
5. 在 **Certificate** 的列表中，选择你刚安装的 SSL 证书。
6. 点击“OK”。
7. 点击“应用”。
8. 你的证书应该已在你的 ASA 里激活。
9. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

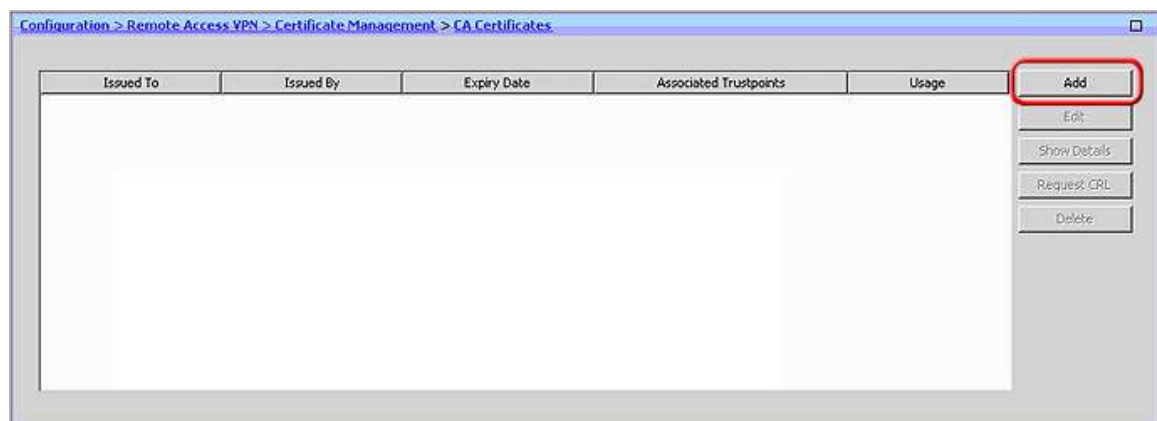
Cisco ASA 5520 SSL 安装指南

步骤 1: 下载 Intermediate CA 证书

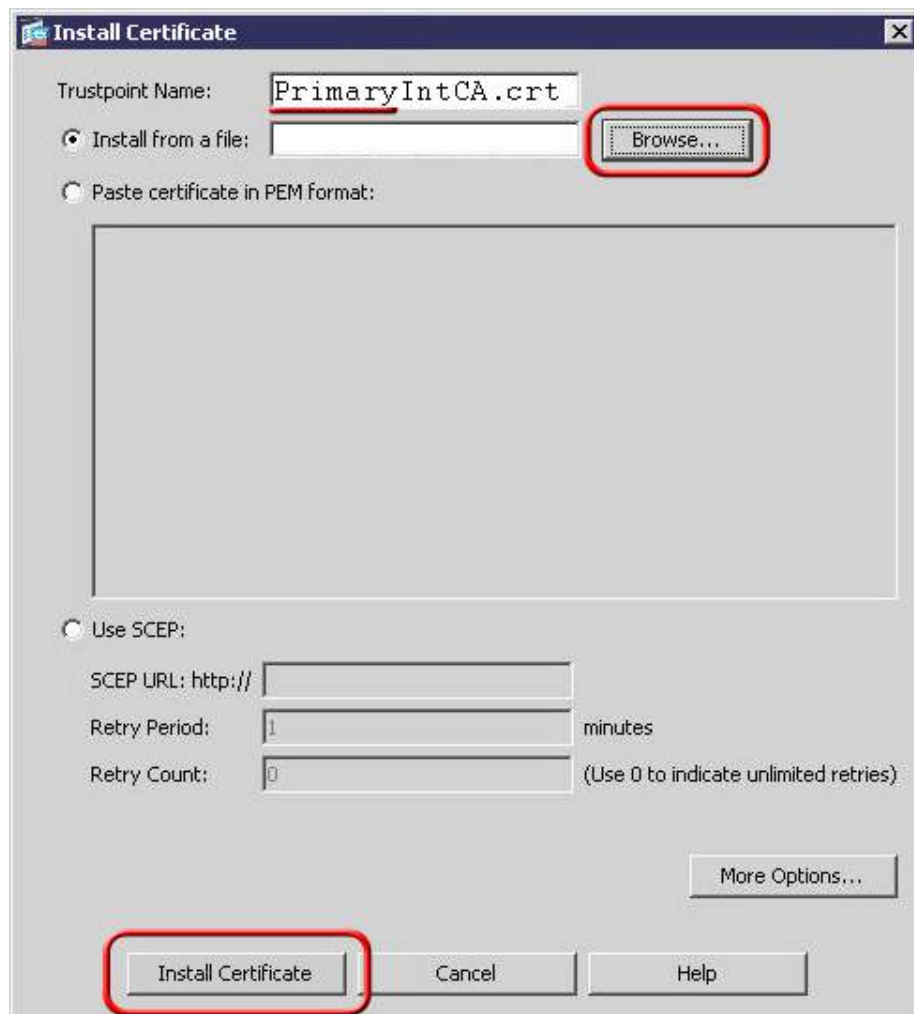
9. [通过此链接下载 Intermediate CA 证书](#)。选择和你的 SSL 证书适合的 Intermediate CA 证书。
10. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.crt。
11. 开启 Cisco ASDM 面板，在 Remote Access VPN 的窗格里，在 Configuration 选项下，展开 Certificate Management 然后点击 CA Certificates.



12. 点击 Add 键



13. 为证书选择一个 Trustpoint Name（如：intermediate.crt），然后选择 Install from a file 选项，按 Browse 查找 intermediate.crt。点击安装证书。



你将会看到证书列在你所选择的 Trustpoint Name 下。

步骤 2：安装 SSL 证书

13. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

14. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

[加密数据]

-----END CERTIFICATE-----

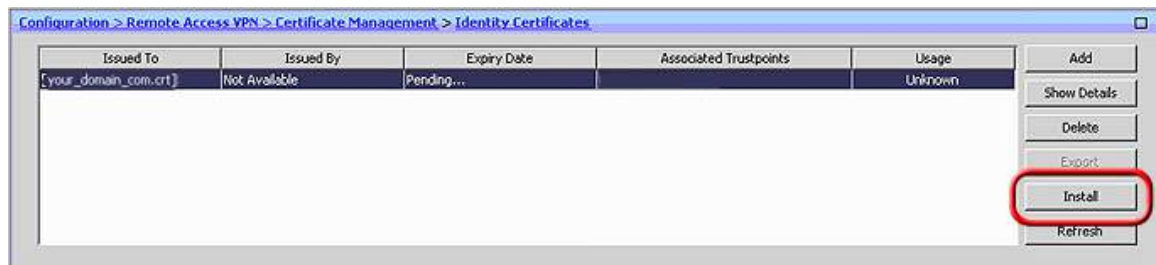
15. 把证书存档为 .txt 文档。

16. 根据 Cisco 的命名规则，把证书文档更改为 .crt 格式。

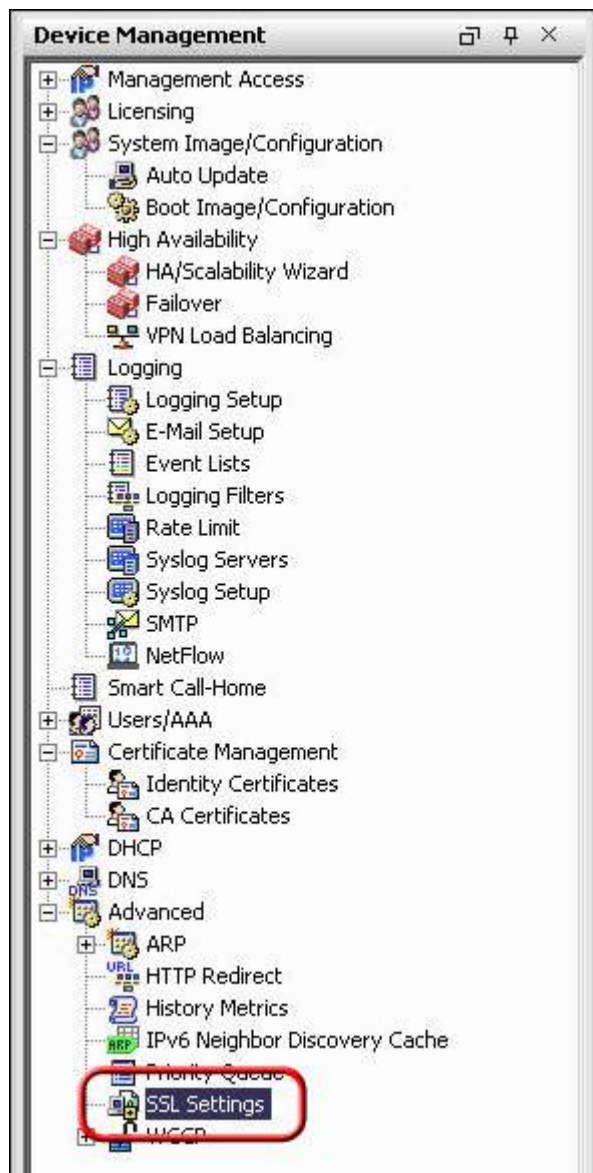
例：public.crt

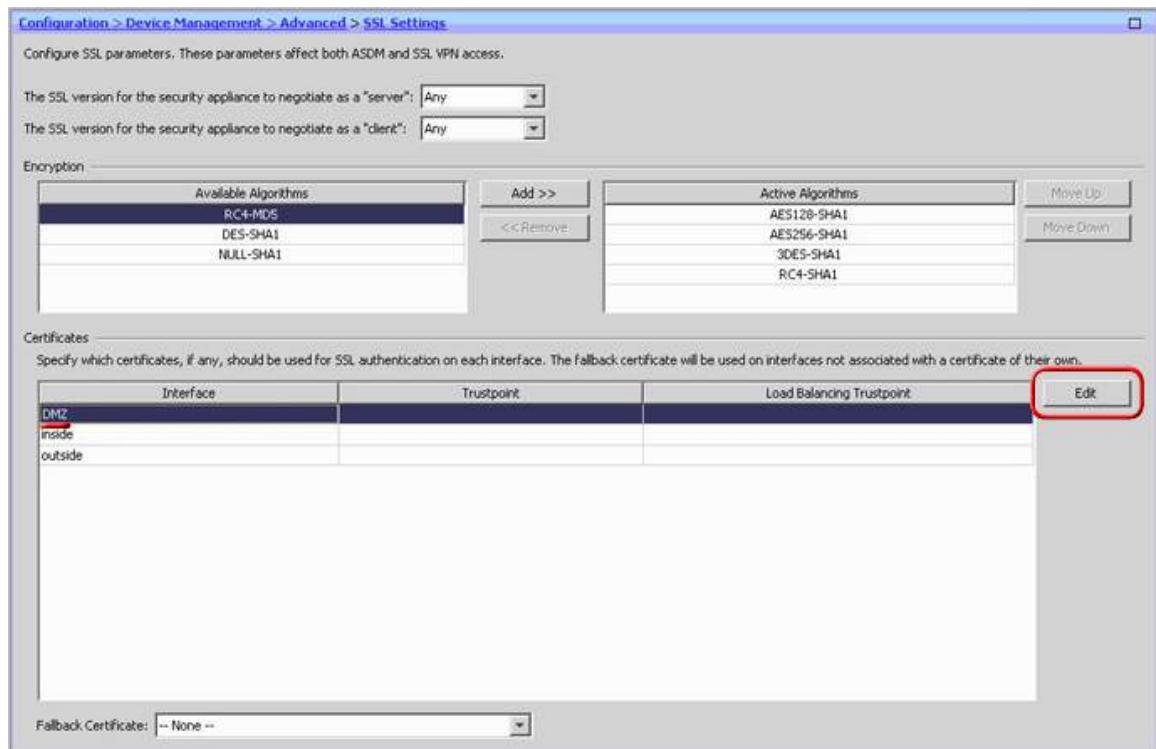
17. 在 Remote Access VPN 下，展开 Certificate Management > Identity Certificates。

选择你在生成 CSR 时创建的标识，逾期日期将会显示为 Pending，点击 **Install**。选择 yourdomain_com.crt 然后点击 **Install Certificate**。一旦完成安装，逾期日期将不会再显示 Pending。

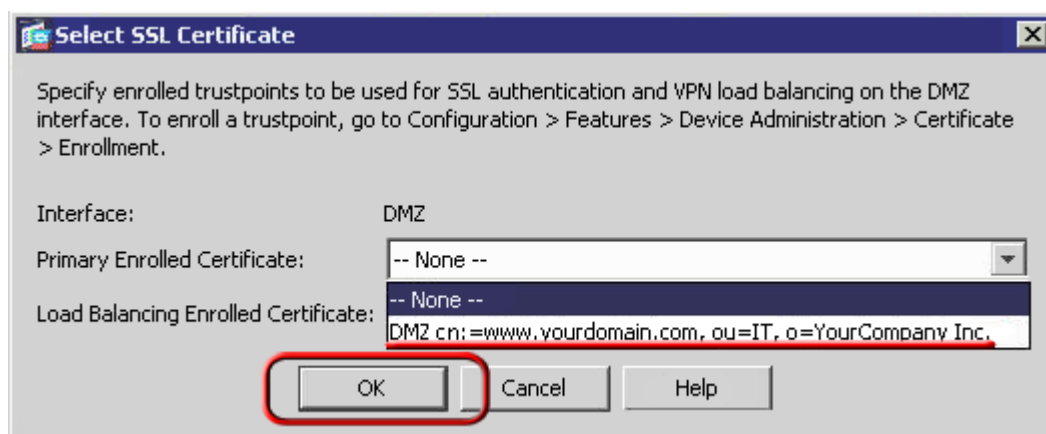


18. 启用你的证书，在左下角，点选 **Advanced > SSL Settings**。然后，选择你要启用 SSL 的借口，然后点击 **Edit**。





19. 在下一页，在菜单选项中的 **Primary Enrolled Certificate** 里选择你的证书然后点击 OK。



20. ASDM 将会在 trustpoint 下显示你的证书。
21. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

Cisco ASA 5520

欲知更多详情，请浏览 [Cisco 客服网站](#)。