SSL 證書 - Cisco

證書安裝指南

webnic
accelerate your business

請選擇您的版本

Cisco ISE SSL 安裝指南

Cisco ACS 3.2 SSL 安裝指南

Cisco Secure ACS 4.2 SSL 安裝指南

使用命令行界面安裝 Cisco ASA 5000 SSL 證書指南

Cisco ASA 5510 SSL 證書安裝指南

Cisco ASA 5520 SSL 安裝指南

Cisco ISE SSL 安裝指南

步驟 1：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

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

3. 把文件存檔為 SSLCert.cer。

步驟 2：下載 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

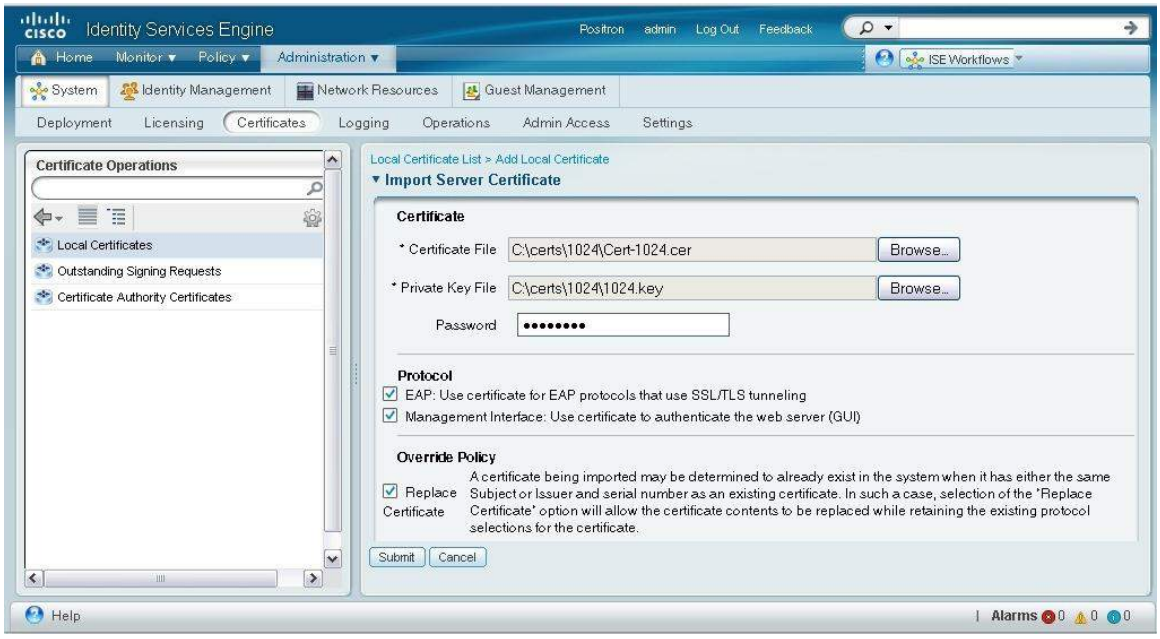
   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.cer。

步驟 3：安裝 SSL 證書

1. 選擇 Administration > System > Certificates。
2. 從 Certificate Operations 導航窗格中，點擊 Local Certificates。

   注：要把本地證書導入輔助節點，請選擇 Administrative > System > Server Certificate。
3. 選擇 Add > Import。
4. Import Local Server Certificate 頁面將會顯示如下：



5. 點擊 Browse 選擇證書文件，以及運行您客戶瀏覽器的系統的私鑰。
6. 如果私鑰已被加密，輸入密碼解密。
7. 在 Protocol 頁面：
   - 點選 EAP 複選框以使用此證書的 EAP 協議以確認 Cisco ISE 節點。
   - 點選 Management Interface 複選框以使用此證書驗證 Web 服務器（GUI）。

注：如你已點選 Management Interface，確保在 CN 欄裡的 Certificate Subject 填上證書的完全域名，否則流程將會失敗。

1. 在 Override Policy 選項，點選 Replace Certificate 以使用替代證書代替現有證書。

   注：如如果證書擁有與現有證書相同發行人和相同的序號，它將會被視為替代證書。此選項是為了更新證書的內容，但保留證書的協議。

2. 點擊提交以導入本地證書。

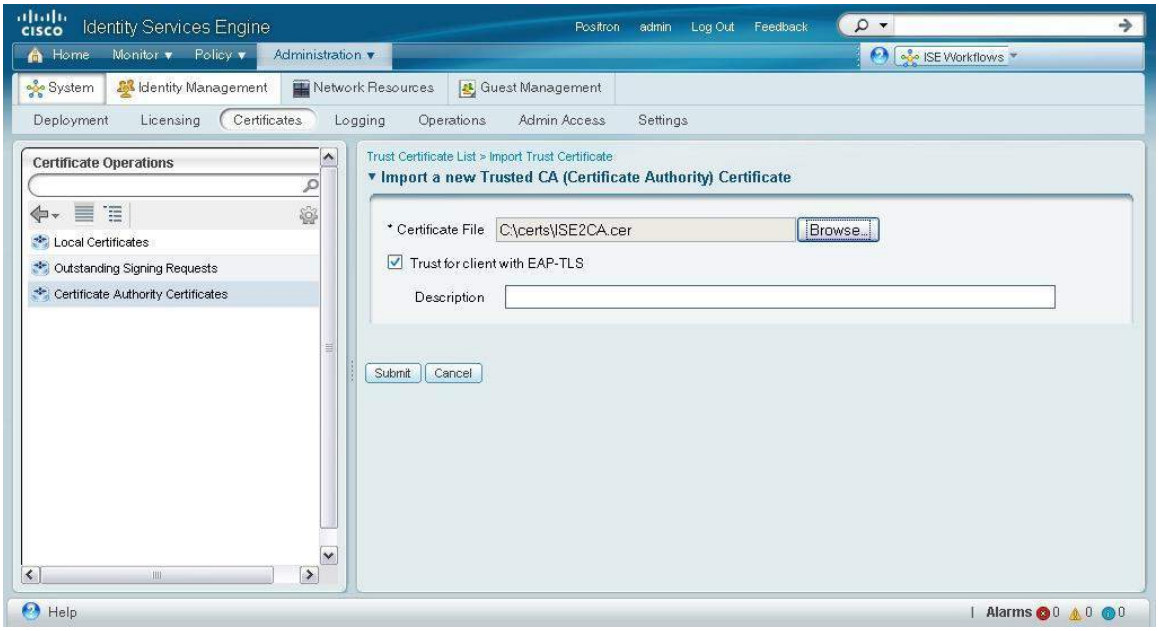
   注：如果你把證書導入你的主要 Cisco ISE 節點，你必須重啟你的輔助 Cisco ISE 節點以連接你的主要 Cisco ISE 節點。請使用命令行頁面（CLI）輸入以下指令以重啟你的輔助節點：

   a. application stop ise

   b. application start ise

步驟 4：安裝 Intermediate CA 證書

1. 選擇 Administration > System > Certificates。
2. 在左則的 Certificate Operations 導航窗格中，點擊 Certificate Authority Certificates。
3. Certificate Authority Certificates 頁面將會出現。
4. 點擊 Add。
5. Import Trusted CA (Certificate Authority) Certificate 頁面將會顯示如下：



6. 點擊 Browse 選擇運行你客戶的瀏覽器的 CA 證書。
7. 如果你要把此證書用於客戶的 EAP-TLS 協議的信任列表，請點選 Trust for client with EAP-TLS 選項。

   注：如果 Trust for client with EAP-TLS 選項已被點選，請確認 keyUsage 擴展已顯示，同時 keyCertSign 已設置，以及 basic constraints 擴展已顯示並把 CA 標誌設定為 true。
8. 加入描述（可選）。
9. 點擊提交以保存 CA 證書。

   注：如果你把證書導入你的主要 Cisco ISE 節點，你必須重啟你的輔助 Cisco ISE 節點以連接你的主要 Cisco ISE 節點。請使用命令行頁面（CLI）輸入以下指令以重啟你的輔助節點：

   a. application stop ise

   b. application start ise

10. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

Cisco ACS 3.2 SSL 安裝指南

步驟 1：下載 Intermediate CA 證書

1. 通過此鏈接下載 **Intermediate CA** 證書。

   選擇和你的 SSL 證書適合的 **Intermediate CA** 證書。

2. 複製 **Intermediate CA** 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 **intermediate.cer**。

步驟 2：安裝 CA 證書

1. 在導航欄裡，點擊 **System Configuration**。
2. 點擊 **ACS Certificate Setup**。
3. 點擊 **ACS Certification Authority Setup**。
4. CiscoSecure ACS 會在 Cerification Authorities Setup 頁面下顯示 CA Operations 列表。
5. 在 CA Certificate 一欄中，輸入你的 CA 證書的**完整路徑**以及**文件名**。
6. 查找並導入 **intermediate.cer**。
7. 點擊**提交**。

步驟 3：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

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

3. 把證書存檔為 **.cer** 文檔。

步驟 4：安裝 SSL 證書

1. 在導航欄裡，點擊 **System Configuration**。
2. 點擊 **ACS Certificate Setup**。
3. 點擊 **Install ACS Certificate**。
4. CiscoSecure ACS 將會顯示 Install ACS Certificate 頁面。
5. 在文件選項中選擇 **Read certificate**，然後在 Certificate 欄中輸入證書文件的**完整路徑**以及**文件名稱**。
6. 在 **Private Key** 欄中，輸入私鑰文件的**完整路徑**以及**文件名稱**。
7. 在 **Private Key Password** 欄中，輸入**私鑰的密碼**。
8. 點擊**提交**。
9. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

Cisco

欲知更多詳情，請瀏覽 Cisco 客服網站。

Cisco Secure ACS 4.2 SSL 安裝指南

步驟 1：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

   證書正文的例子：

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

   [加密數據]

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

3. 把文檔保存為 **SSLCert.cer**。

步驟 2：下載 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 **Intermediate CA** 證書。
2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 **intermediate.cer**。

步驟 3：把證書和 CA 證書複製至 ACS 主機

1. 在 ACS 主機上創建一個 \certs 目錄。
2. 開啟 DOS 命令窗口。
3. 輸入以下指令以創建證書目錄：

   mkdir <selected_drive>:\certs

   注：“selected_drive”即是目前使用的驅動器。

4. 把下列文件（範例）複製至 \certs 目錄。

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

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

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

步驟 4：設置 ACS Certification Authority

1. 你需下載 Root CA 證書以設置 ACS Certification Authority.
2. 在導航欄裡，點擊 System Configuration。

   System Configuration 頁面將會出現。
3. 點擊 ACS Certificate Setup。

   ACS Certificate Setup 頁面將會出現。
4. 點擊 ACS Certification Authority Setup。

ACS Certification Authority 頁面將會顯示如下：

5. 輸入 CA 證書的存檔路徑以及文件名後點擊**提交**。
6. 重啟 ACS。

   選擇 **System Configuration** > **Service Control** 然後點擊 **Restart** 重啟 ACS。

步驟 5：編輯證書信任列表

注：在設置 ACS Certification Authority 後，你必須把 CA 證書加入 ACS 證書信任列表.

1. 在導航欄裡，點擊 **System Configuration.**

   System Configuration 頁面將會開啟。
2. 選擇 **ACS Certificate Setup** > **Edit Certificate Trust List**。

   Edit Certificate Trust List 頁面將會出現。
3. 在證書列表中，點選你已安裝的 CA 證書。
4. 點擊**提交**。
5. 選擇重啟 ACS。

   選擇 **System Configuration** > **Service Control** 然後點擊 Restart 重啟 ACS。

步驟 6：安裝 Intermediate CA 證書

1. 選擇 **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.

   ACS Certification Setup 頁面將會顯示如下：

2. 在 CA certificate file 文字框中，輸入 CA 證書的儲存路徑和文件名；例：

   c:\Certs\ca.cer。

3. 點擊**提交**。

步驟 7：安裝 SSL 證書

1. 在導航欄裡，點擊 **System Configuration**。

   System Configuration 頁面將會出現。

2. 點擊 **ACS Certificate Setup**。

3. 點擊 **Install ACS Certificate**。

   Install ACS Certificate 頁面顯示如下：

4. 選擇 **Read certificate from file** 選項。
5. 在 **Certificate file** 文字框裡，輸入證書的儲存路徑和文件名；例：c:\Certs\server.cer.
6. 在 **Private key file** 文字框裡，輸入主機證書的儲存路徑和文件名；例：c:\Certs\server.pvk.
7. 在 **Private Key password** 文字框裡，輸入私鑰密碼，例：cisco123。
8. 點擊**提交**。
9. ACS 將會顯示證書已成功安裝的消息，然後指示你重啟 ACS 服務。
10. 重啟 ACS。選擇 **System Configuration** > **Service Control** 然後點擊 **Restart** 重啟 ACS。
11. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

使用命令行界面安装 Cisco ASA 5000 SSL 證書指南

步驟 1：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。

2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

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

3. 把證書存檔為 SSLCert.txt。

步驟 2：下載 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.txt。

步驟 3：安裝 Intermediate CA 證書至 Trustpoint

1. 在命令行界面，輸入以下指令：

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

2. 你將會被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself”。
3. 開啟 **intermediate.txt**，把內容複製後粘貼至命令行界面。
4. 確定 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 作為開頭和結尾。

例：

Enter the base 64 encoded certificate.

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

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

MIIE0DCCBDmgAwIBAgIQJQzo4DBhLp8rifcFTXz4/TANBgkqhkiG9w0BAQUFADBf

MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAs

T

LkNsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw

HhcNMDYxMTA4MDAwMDAwWhcNMjExMTA3MjM1OTU5WjCByjELMAkGA1UEBhMCVV

Mx

FzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVz

dCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZv

ciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAz

IFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEi

MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudLO07cfLw8

RRy7K+D+KQL5VwijZIUVJ/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70Pb

ZmIVYc9gDaTY3vjgw2IIPVQT60nKWVSFJuUrjxuf6/WhkcIzSdhDY2pSS9KP6HBR

TdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQGBO+QueQA5N06tRn/

Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNH

iDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/NIeWiu5T6CUVAgMB

AAGjggGbMIIBlzAPBgNVHRMBAf8EBTADAQH/MDEGA1UdHwQqMCgwJqAkoCKGIGh0

dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA4GA1UdDwEB/wQEAwIBBjA9

BgNVHSAENjA0MDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVy

aXNpZ24uY29tL2NwczAdBgNVHQ4EFgQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMwbQYI

KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGg

QU

j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t

L3ZzbG9nby5naWYwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi

8v

b2NzcC52ZXJpc2lnbi5jb20wPgYDVR0lBDcwNQYIKwYBBQUHAwEGCCsGAQUFBwMC

BggrBgEFBQcDAwYJYIZIAYb4QgQBBgpghkgBhvhFAQgBMA0GCSqGSIb3DQEBBQUA

A4GBABMC3fjohgDyWvj4IAxZiGIHzs73Tvm7WaGY5eE43U68ZhjTresY8g3JbT5K

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 證書，你將會被提示是否接受證書，回答 ”Yes”。

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

   提交後，系統將會顯示：

   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. 開啟 Trustpoint，並以以下命令安裝二級證書：

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

7. 你將會被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself”。

步驟 4：安裝 SSL 證書

1. 為了使用命令行頁面，你必須輸入以下指令：

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

2. 你將會被提示 “Enter the base 64 encoded CA certificate. End with the word “quit” on a line by itself”。
3. 開啟在步驟 1 創建的 SSLCert.txt，把內容髮複製後粘貼至命令行頁面。
4. 確定 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 作為開頭和結尾。

   注：以下證書只作為參考，並非真正證書。

   證書裡的完全限定域名（FQDN）：<你證書裡的 Common Name>

   Enter the base 64 encoded certificate.

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

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

   MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0BAQUFADCB

   yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQ

   L

   EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV

   BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz

   L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl

   cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox

   CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH

UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQFVFNXRUIx
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20wgZ8wDQY
J
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgryosBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2lnbi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAv
Bggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYD
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQFVFNXRUIx
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYIKwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5KJY
G
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FSewy8MAIY

rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td

0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O

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

quit

INFO: Certificate successfully imported

ciscoasa(config)#

步驟 5：設置使用你的 SSL 證書的接口的 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)#

步驟 6：驗證證書和證書鏈

1. 輸入以下指令驗證你剛剛安裝的證書：

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

你也可以使用 Symantec 的證書檢查工具。

Cisco ASA 5510 SSL 證書安裝指南

步驟 1：下載 Root CA 證書和 Intermediate CA 證書

注：若使用 Cisco ASDM 6.3 或 6.1，你必須在生成 RSA 密鑰之前安裝 Root 和 Intermediate CA 證書。

1. 點擊此下載 Root CA 證書。
2. 點擊此下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

步驟 2：安裝 Root CA 證書

1. 在 ASDM 裡，點擊 Configuration > Device Management。
2. 點擊 Certificate Management > CA Certificates。
3. 點擊“Add”。
4. 點擊 Paste Certificate in PEM Format > 把 Root CA 證書粘貼至文字框裡。
5. 點擊安裝證書。

   對話框將會出現，顯示證書已成功安裝。

步驟 3：安裝 Intermediate CA 證書

1. 在 ASDM 裡，點擊 **Configuration > Device Management**。
2. 點擊 **Certificate Management > CA Certificates**。
3. 點擊“**Add**”。
4. 點擊 **Paste Certificate in PEM Format** > 把 Intermediate CA 證書粘貼至文字框裡。
5. 點擊**安裝證書**。

   對話框將會出現，顯示證書已成功安裝。

步驟 4：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

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

3. 把文件存檔為 **SSLCert.pem**。

步驟 5：安裝 SSL 證書

1. 點擊 **Configuration > Device Management**。
2. 點擊 **Certificate Management > Identify Certificates**。

3. 選擇你所創建的標識（逾期日期將會顯示為 Pending）。
4. 點擊“**安裝**”。
5. 點擊 Paste the certificate data in base-64 format > 把證書複製並粘貼至文件筐。
6. 點擊“**安裝證書**”。

   對話框將會出現，顯示證書已成功安裝。

步驟 6：激活 SSL 證書

1. 點擊 Configuration > Device Management。
2. 展開 Advanced，然後展開 SSL Settings。
3. 在 Certificates 選項下，選擇終結 WebVPN 的界面。
4. 選擇“**編輯**”。
5. 在 Certificate 的列表中，選擇你剛安裝的 SSL 證書。
6. 點擊“**OK**”。
7. 點擊“**應用**”。
8. 你的證書應該已在你的 ASA 裡激活。
9. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

Cisco ASA 5520 SSL 安裝指南

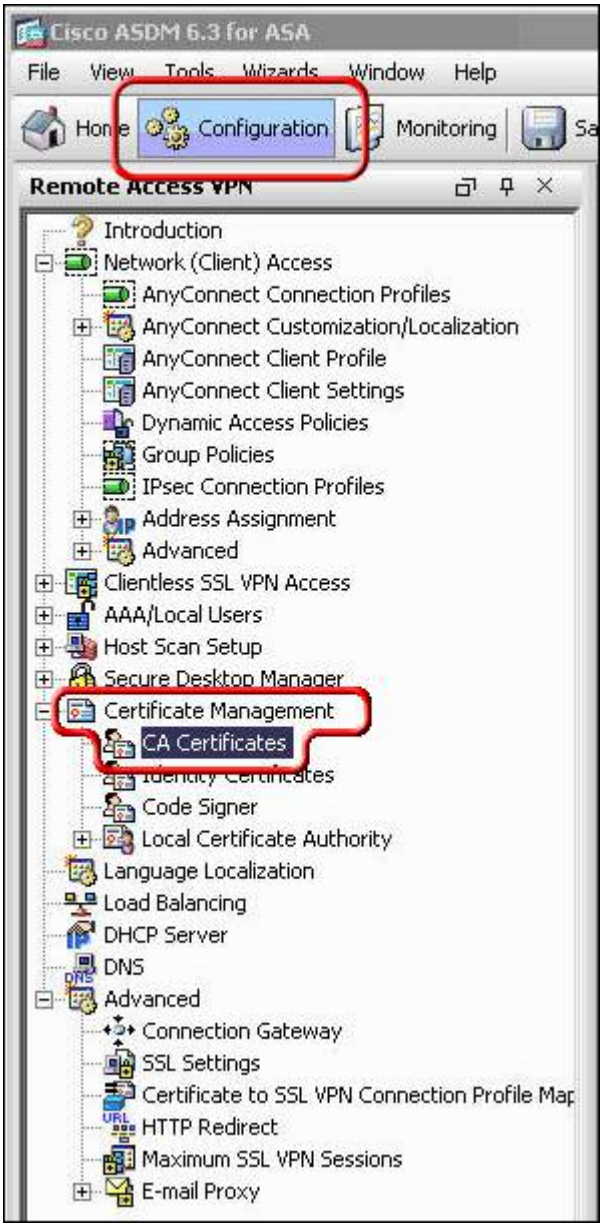
步驟 1：下載 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

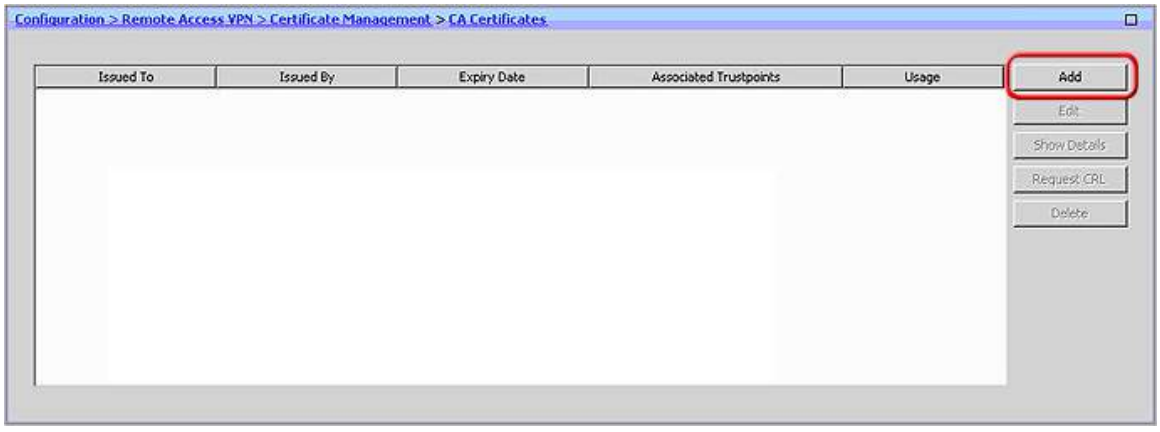
   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.crt。

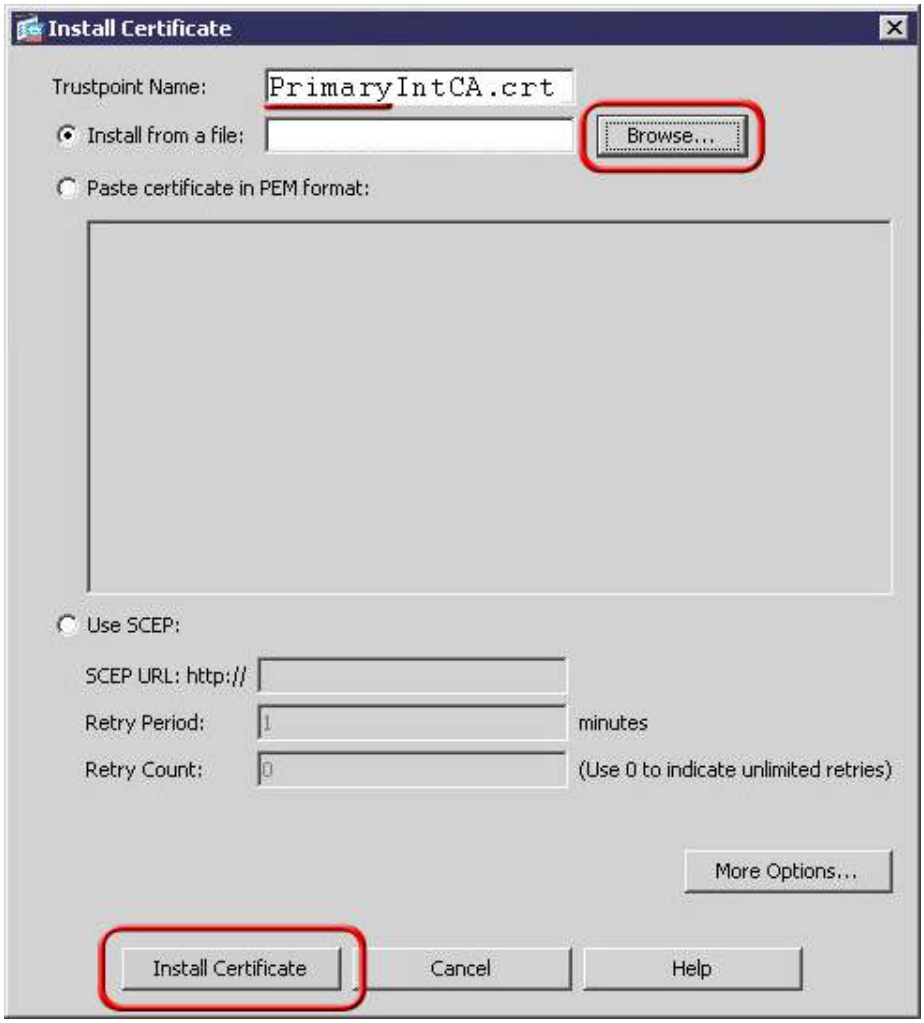
3. 開啟 Cisco ASDM 面板，在 Remote Access VPN 的窗格里，在 Configuration 選項下，展開 Certificate Management 然後點擊 CA Certificates.


Cisco ASDM 6.3 for ASA
File View Tools Wizards Window Help
Home Configuration Monitoring
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Setup
Secure Desktop Manager
Certificate Management
CA Certificates
Code Signer
Local Certificate Authority
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to SSL VPN Connection Profile Map
HTTP Redirect
Maximum SSL VPN Sessions
E-mail Proxy

4. 點擊 Add 鍵


Configuration > Remote Access VPN > Certificate Management > CA Certificates
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
Add
Edit
Show Details
Request CRL
Delete

5. 為證書選擇一個 Trustpoint Name（如：intermediate.crt），然後選擇 Install from a file 選項，按 Browse 查找 intermediate.crt。點擊安裝證書。



你將會看到證書列在你所選擇的 Trustpoint Name 下。

步驟 2：安裝 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

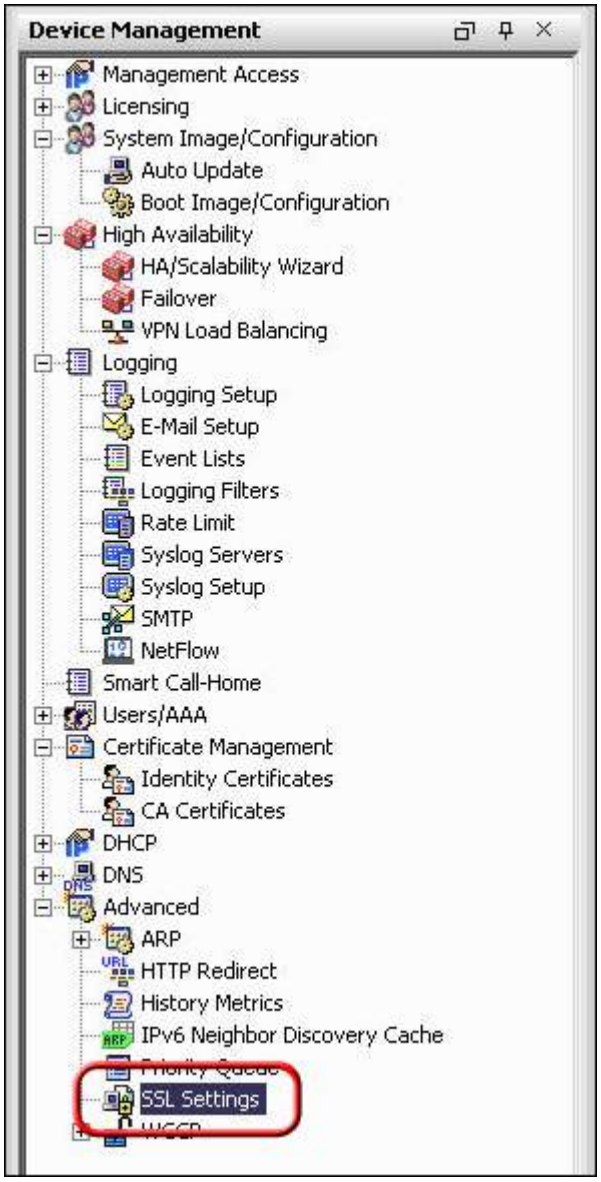
-----END CERTIFICATE-----

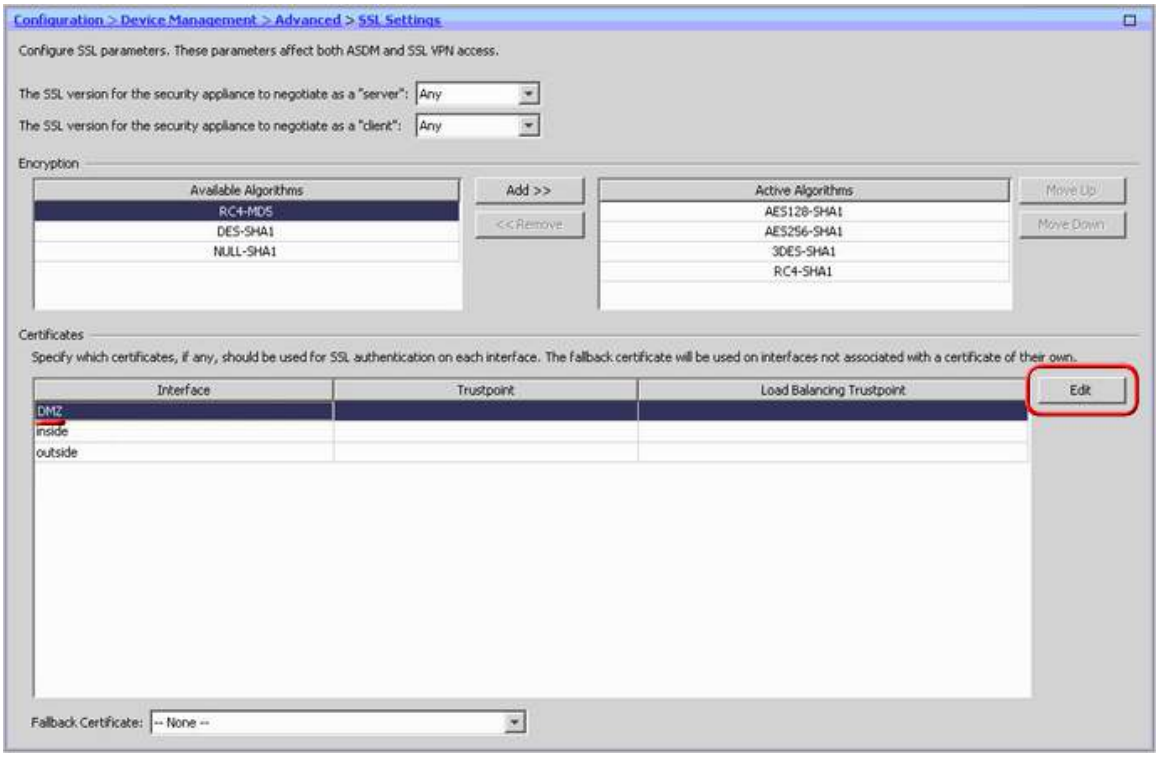
3. 把證書存檔為 .txt 文檔。
4. 根據 Cisco 的命名規則，把證書文檔更改為 .crt 格式。

   例：**public.crt**
5. 在 **Remote Access VPN** 下，展開 **Certificate Management** > **Identity Certificates**。

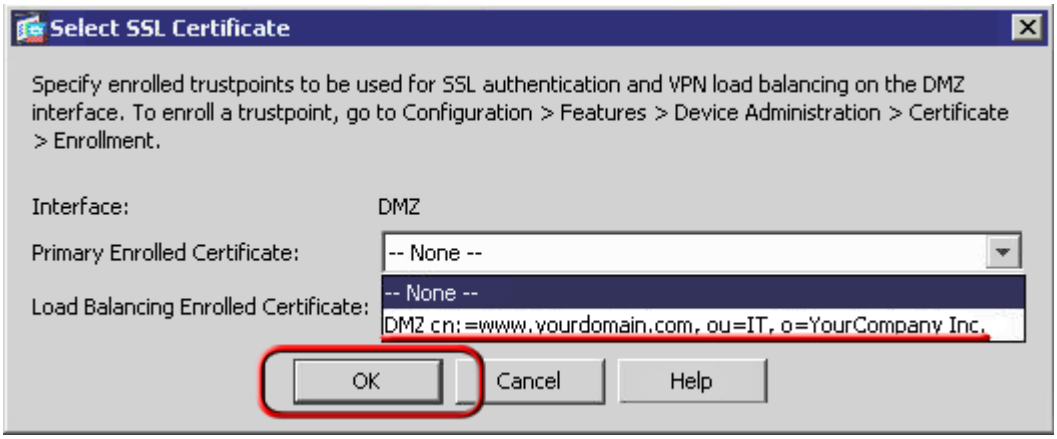
選擇你在生成 CSR 時創建的標識，**逾期日期**將會顯示為 Pending，點擊 **Install**。選擇 **yourdomain_com.crt** 然後點擊 **Install Certificate**。一旦完成安裝，逾期日期將不會再顯示 Pending。

6. 啟用你的證書，在左下角，點選 **Advanced** > **SSL Settings**。然後，選擇你要啟用 SSL 的藉口，然後點擊 **Edit**。


Device Management
Management Access
Licensing
System Image/Configuration
Auto Update
Boot Image/Configuration
High Availability
HA/Scalability Wizard
Failover
VPN Load Balancing
Logging
Logging Setup
E-Mail Setup
Event Lists
Logging Filters
Rate Limit
Syslog Servers
Syslog Setup
SMTP
NetFlow
Smart Call-Home
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discovery Cache
SSL Settings



7. 在下一頁，在菜單選項中的 **Primary Enrolled Certificate** 裡選擇你的證書然後點擊 **OK**。



8. ADSM 將會在 trustpoint 下顯示你的證書。

9. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

Cisco ASA 5520

欲知更多詳情，請瀏覽 Cisco 客服網站。