將Cisco VPN 3000集中器配置並註冊到Cisco IOS路由器作為CA伺服器

目錄

簡介

本檔案將說明如何將Cisco IOS®路由器設定為憑證授權單位(CA)伺服器。此外，還說明了如何將Cisco VPN 3000集中器註冊到Cisco IOS路由器，以獲取IPSec身份驗證的根證書和ID證書。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS軟體版本12.3(4)T3的Cisco 2600系列路由器
- Cisco VPN 3030集中器版本4.1.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

生成並匯出證書伺服器的RSA金鑰對

第一步是生成Cisco IOS CA伺服器使用的RSA金鑰對。在路由器(R1)上生成RSA金鑰，如下所示：

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

注意：對於計畫用於證書伺服器的金鑰對(*key-label*)，您必須使用相同的名稱(通過**crypto pki server *cs-label* 命令)。**

匯出生成的金鑰對

然後，需要根據您的配置，將金鑰匯出到非易失性RAM(NVRAM)或TFTP。 在此範例中，使用NVRAM。根據您的實施，您可能希望使用單獨的TFTP伺服器來儲存證書資訊。

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
```

```
Writing file to nvram:cisco1.prv
R1(config)#
```

如果您使用TFTP伺服器，可以重新匯入產生的金鑰對，如下所示：

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

注意：如果不希望金鑰從證書伺服器匯出，請在匯出為不可匯出的金鑰對後將其匯入證書伺服器。因此，不能再次取下金鑰。

驗證生成的金鑰對

您可以通過呼叫**show crypto key mypubkey rsa**命令來驗證生成的金鑰對：

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

在路由器上啟用HTTP伺服器

Cisco IOS CA伺服器僅支援透過簡單憑證註冊通訊協定(SCEP)完成的註冊。 因此，為使這一點成為可能，路由器必須運行內建的Cisco IOS HTTP伺服器。要啟用它，請使用**ip http server**命令：

```
R1(config)#ip http server
```

在路由器上啟用和配置CA伺服器

請按照以下步驟操作。

1. 請務必記住，憑證伺服器必須與您剛才手動產生的金鑰對使用相同的名稱。該標籤與生成的金鑰對標籤匹配：
   ```
   R1(config)#crypto pki server cisco1
   ```

   啟用證書伺服器後，可以使用預配置的預設值或通過CLI指定證書伺服器的功能值。

2. **database url**命令指定CA伺服器的所有資料庫條目的寫入位置。如果未指定此命令，則所有資料庫條目都將寫入快閃記憶體。
```
R1(cs-server)#database url nvram:
```

注意：如果使用TFTP伺服器，則URL需要為**tftp://<ip_address>/directory**。
3. 配置資料庫級別：
```
R1(cs-server)#database level minimum
```

此命令控制儲存在證書註冊資料庫中的資料型別。**Minimum** — 儲存足夠的資訊，以便繼續頒發新證書而不會發生衝突；預設值。**Names** — 除了最小級別中提供的資訊外，每個證書的序列號和主題名稱也包含在內。**Complete** — 除了最小和名稱級別中提供的資訊外，每個已頒發的證書都將寫入資料庫。**注意：**complete關鍵字可生成大量資訊。如果發出，您還需要指定外部TFTP伺服器，以便通過**database url** 命令將資料儲存到其中。
4. 將CA頒發者名稱配置為指定的DN字串。在本示例中，使用了cisco1.cisco.com的CN（通用名稱）、RTP的L（位置）和US的C（國家/地區）：
```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. 指定CA證書或證書的生存期（以天為單位）。有效值範圍為*1天到1825天*。預設CA證書生存期**為3**年，預設證書生存期**為1年**。最大證書生命期*比CA證書*的生命期短1個月。例如：
```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```
6. 定義證書伺服器使用的CRL的生存時間（小時）。最大生存時間值**為336小**時（2週）。 預設值為**168小**時（1週）。
```
R1(cs-server)#lifetime crl 24
```

7. 定義要在證書伺服器頒發的證書中使用的證書撤銷清單分發點(CDP)。URL必須是HTTP URL。例如，伺服器的IP地址是172.18.108.26。
```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

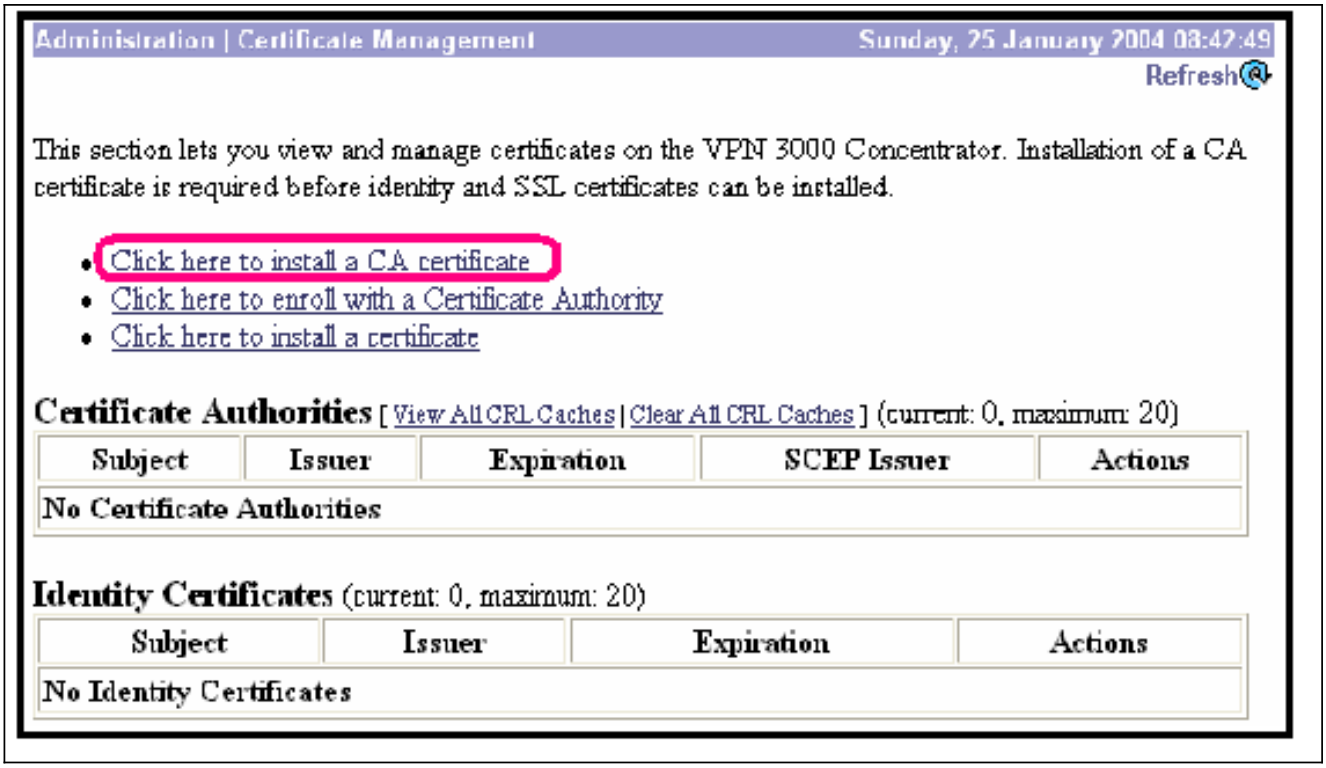
8. 發出**no shutdown**命令以啟用CA伺服器。
```
R1(cs-server)#no shutdown
```

注意：僅在完成證書伺服器配置後發出此命令。

配置和註冊Cisco VPN 3000 Concentrator

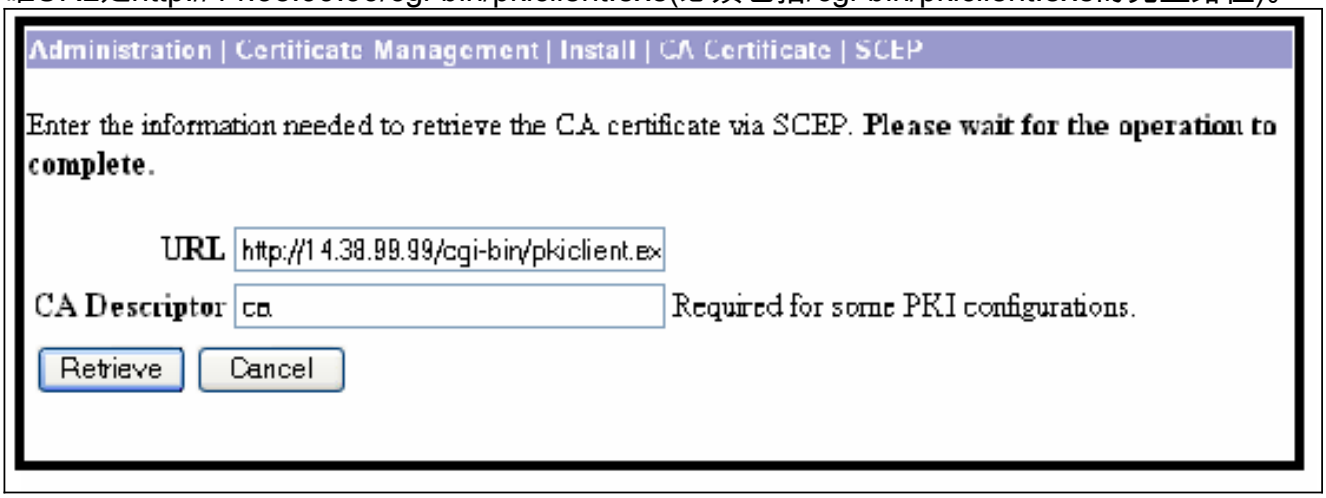
請按照以下步驟操作。

1. 選擇**Administration > Certificate Management**，然後選擇**Click here to install a CA certificate**，以從Cisco IOS CA Server檢索根證書。

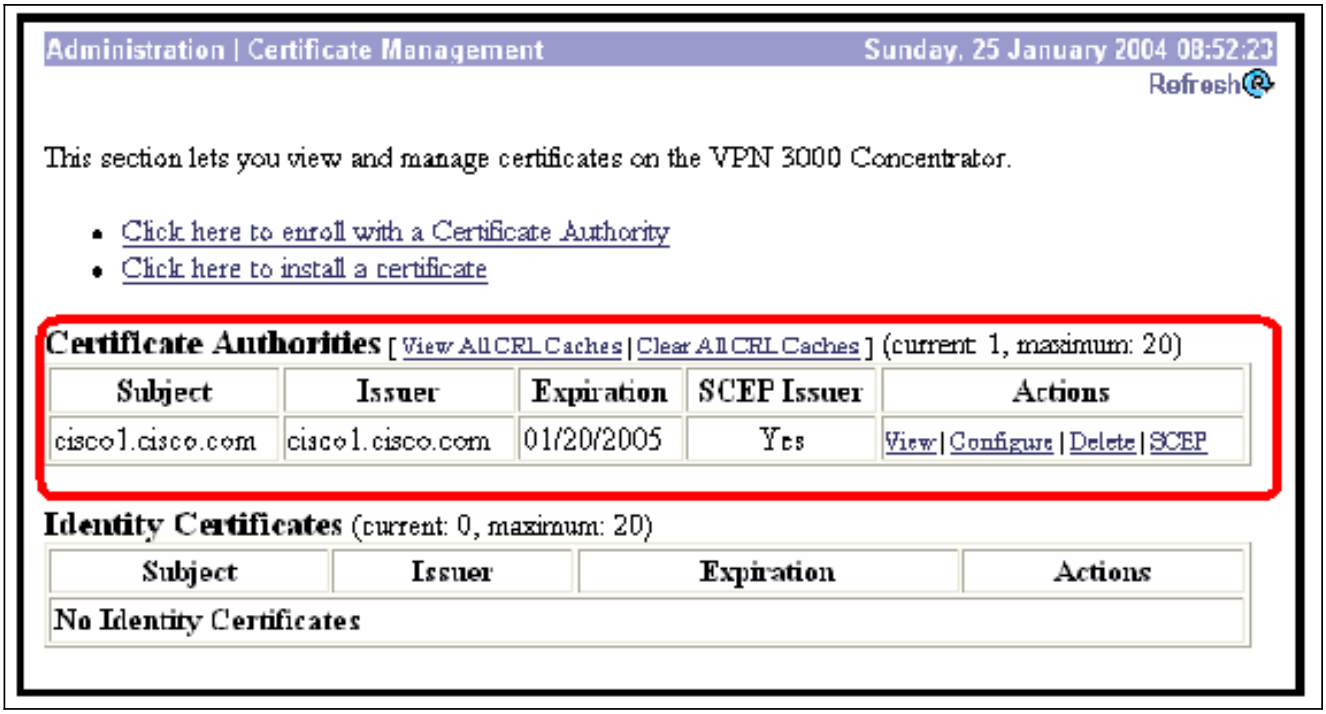


2. 選擇**SCEP**作為安裝方法。

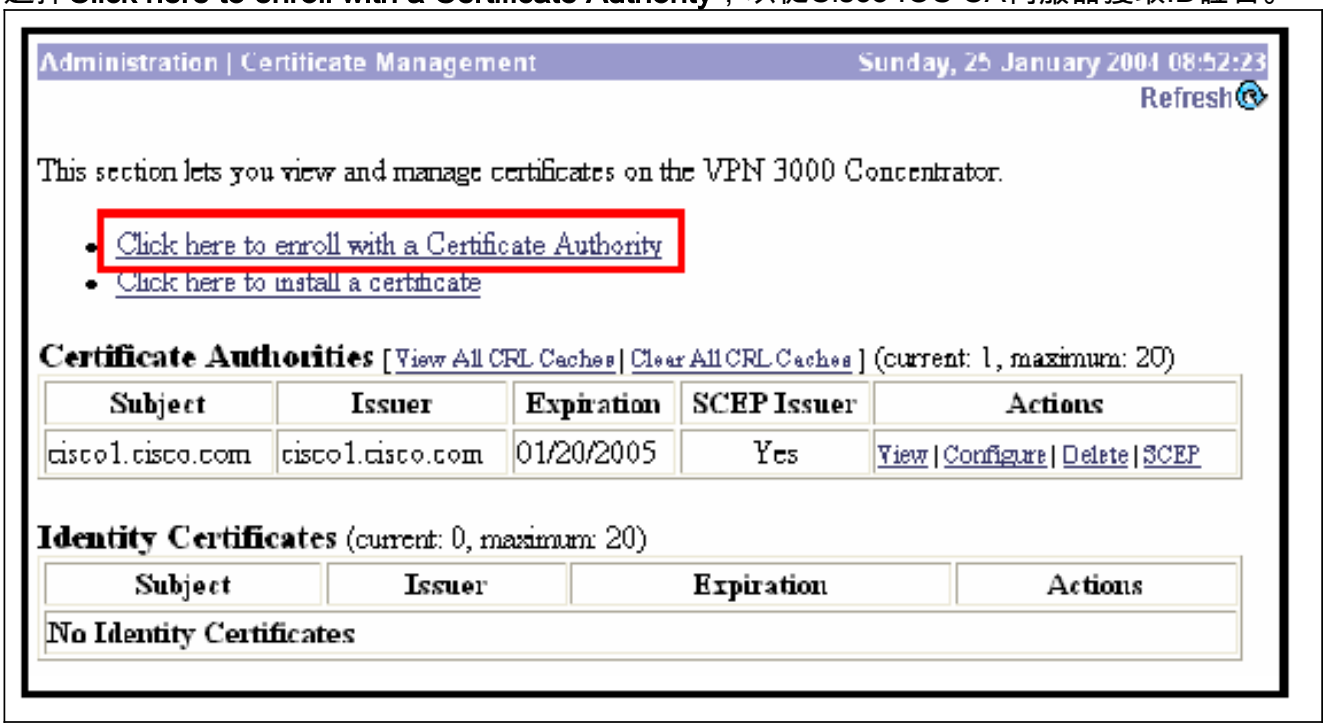
3. 輸入Cisco IOS CA伺服器的URL（CA描述符），然後按一下**Retrieve**。**注意：**本示例中的正確URL是http://14.38.99.99/cgi-bin/pkiclient.exe(必須包括/cgi-bin/pkiclient.exe的完整路徑)。



選擇**Administration > Certificate Management**以驗證是否已安裝根證書。下圖說明了根證書的詳細資訊。



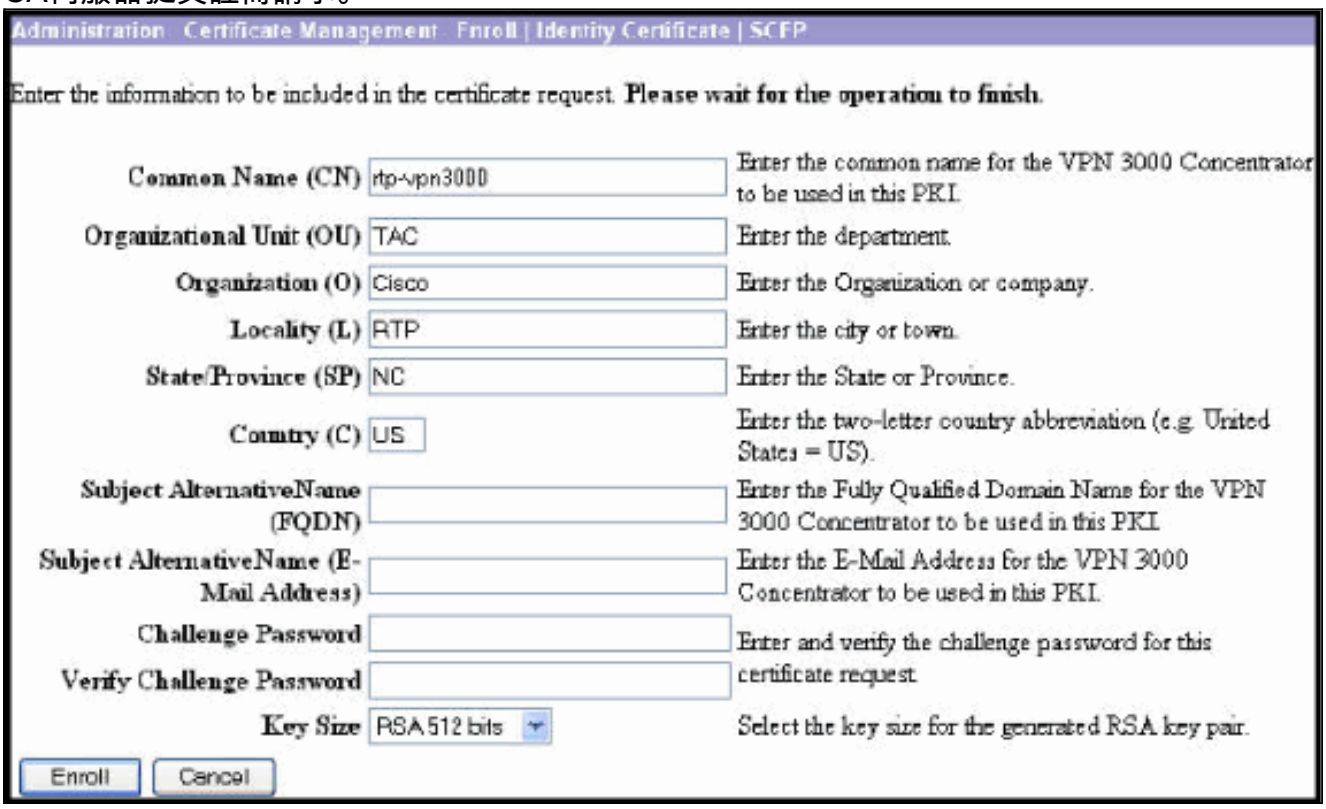
4. 選擇**Click here to enroll with a Certificate Authority**，以從Cisco IOS CA伺服器獲取ID證書。



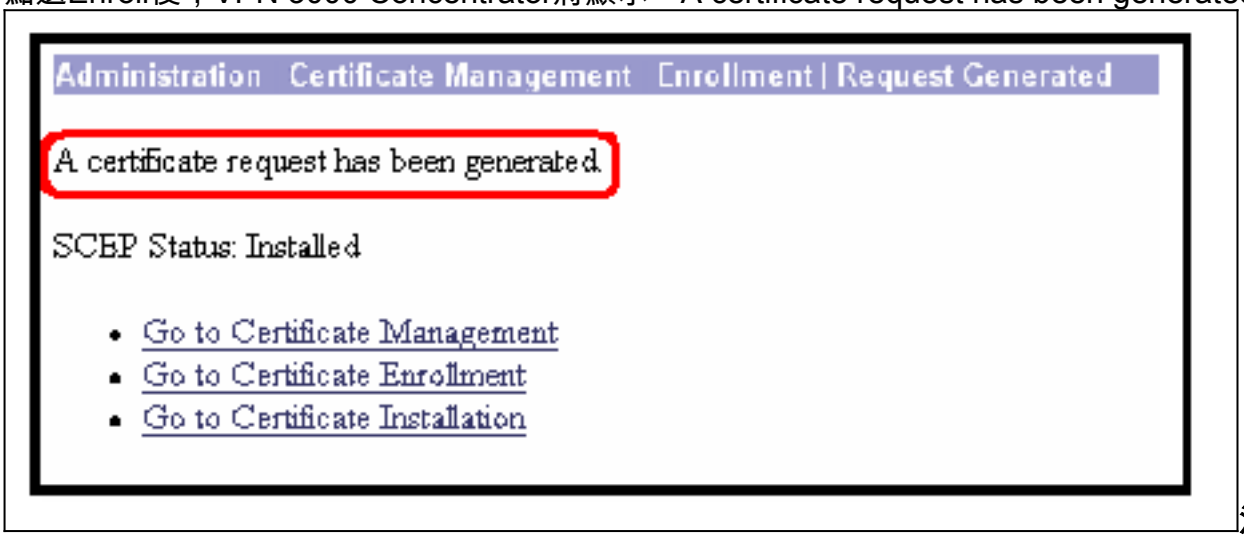
5. 選擇**Enroll via SCEP at cisco1.cisco.com**(cisco1.cisco.com是Cisco IOS CA伺服器的CN)。

6. 輸入要在證書請求中包括的所有資訊，以完成登錄檔格。填寫此表單後，按一下**Enroll**開始向

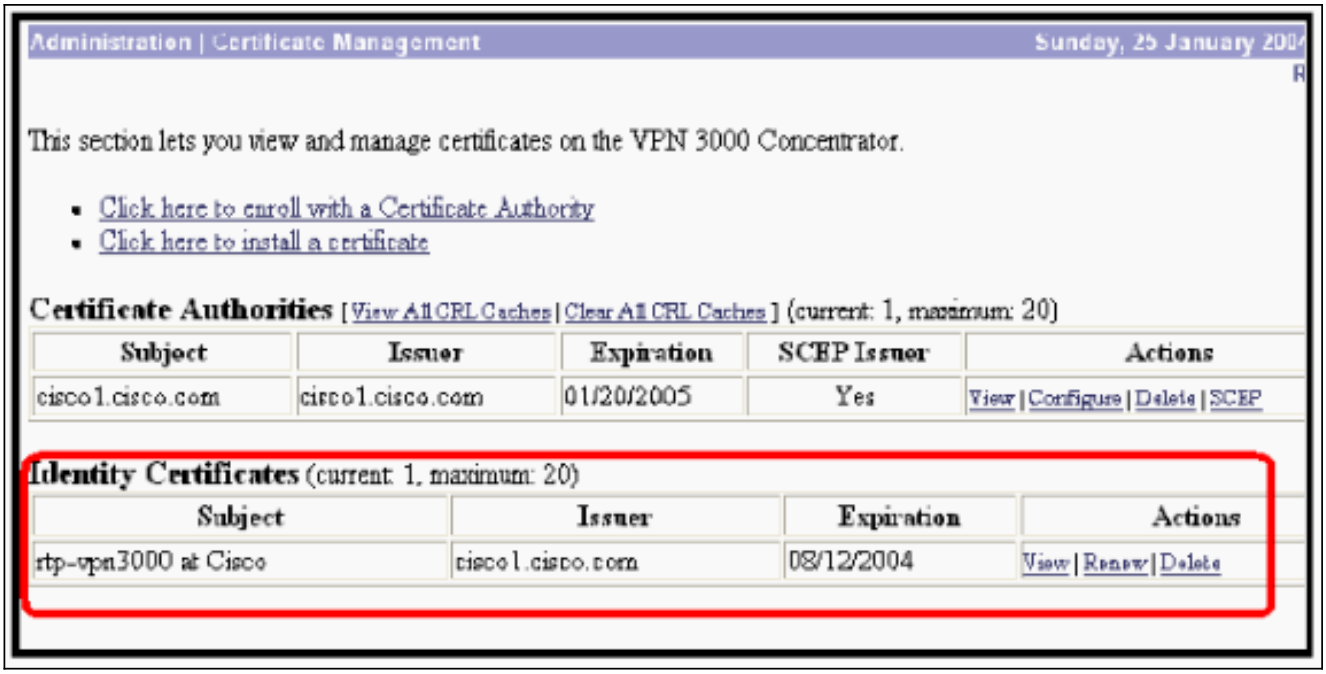
CA伺服器提交註冊請求。



點選Enroll後，VPN 3000 Concentrator將顯示「A certificate request has been generated」。



注意：可以將Cisco IOS CA伺服器配置為使用Cisco IOS CA Server子命令**grant automatic自動授予證書**。此命令用於此示例。要檢視ID證書的詳細資訊，請選擇**管理 > 證書管理**。顯示的證書與此類似。



驗證

有關驗證資訊，請參閱驗證生成的金鑰對部分。

疑難排解

如需疑難排解資訊，請參閱疑難排解VPN 3000集中器上的連線問題或IP安全性疑難排解 — 瞭解和使用debug命令。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN 3000系列使用者端支援頁面
- IPSec支援頁面
- 技術支援 - Cisco Systems