Cisco IOS ルータに Cisco VPN 3000 コンセントレータを CA サーバとして設定し、登録する方法

目次

はじめに

このドキュメントでは、Cisco IOS® ルータを Certificate Authority（CA; 認証局）サーバとして設定する方法について説明しています。 さらに、IPSec 認証のためのルートおよび ID 証明書を得るために Cisco IOS ルータに Cisco VPN 3000 コンセントレータを登録する方法を説明します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.3(4)T3 を実行する Cisco 2600 シリーズ ルータ
- Cisco VPN 3030 コンセントレータ バージョン 4.1.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

証明書サーバの RSA キー ペアの生成およびエクスポート

第一歩は Cisco IOS CA サーバが使用する RSA キーペアを作成することです。 ルータ（R1）で、ここに見られるように RSA キーを生成して下さい:

```
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: 証明書サーバで使用するキー ペア（*key-label*）に、同じ名前を使用する必要があります（後述の **crypto pki server cs-label** コマンドを使用します）。

生成したキー ペアのエクスポート

キーはそれから Non-volatile RAM （NVRAM）か TFTP に必要があります（設定に基づいて）エクスポートされる。 この例では、NVRAM を使用します。 実装に基づいて、可能性としては証明書情報を保存するのに別途の TFTPサーバを使用したいと思うかもしれません。

```
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)#
```

TFTPサーバを使用する場合、ここに見られるように生成されてキーペアを再インポートできます :

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

注: 証明書サーバからキーをエクスポートできないようにする場合は、エクスポートできないキーペアとしてキーをエクスポートした後、そのキーを証明書サーバにインポートして戻します。 従って、キーは再度はずすことができません。

生成済キー ペアの検証

show crypto key mypubkey rsa コマンドを呼び出すことによって作成されたキーペアを確認できます:

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

```
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
```

ルータでの HTTP サーバの有効化

Cisco IOS CA サーバは、Simple Certificate Enrollment Protocol（SCEP）を使用して実行される登録だけをサポートしています。 さらに、これを可能にするには、ルータで組み込み Cisco IOS HTTP サーバが稼働している必要があります。 それをイネーブルにするために、**ip http server コマンドを**使用して下さい:

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

ルータでの CA サーバのイネーブル化および設定

次の手順に従います。

1. 非常に重要なのは、証明書サーバでは手作業で生成したキー ペアに同じ名前を使用する必要があるということです。 次のように、ラベルは生成済キー ペアのラベルに一致しています。
   ```
   R1(config)#crypto pki server cisco1
   ```
   証明書サーバをイネーブルにした後、事前設定のデフォルト値を使用するか、CLI から証明書サーバの機能用に値を指定できます。
2. **database url** コマンドは、CA サーバのすべてのデータベース エントリを書き出す場所を指定します。このコマンドを指定しない場合、すべてのデータベース エントリはフラッシュに書き込まれます。
   ```
   R1(cs-server)#database url nvram:
   ```
   注: TFTP サーバを使用する場合は、URL を **tftp://<ip_address>/directory** にする必要があります。
3. データベース レベルを次のように設定します。
   ```
   R1(cs-server)#database level minimum
   ```
   どのようなデータが証明書登録データベースで保存されるかこのコマンド 制御。**最小値**—十分な情報は競合なしで新しい証明書を発行するためにだけ続けるように保存されます; デフォルト値。**names** : minimum レベルで得られる情報のほか、各証明書のシリアル番号および主体者名。**complete** : minimum レベルおよび names レベルで得られる情報のほか、発行済みの各証明書がデータベースに書き込まれます。**注: complete** キーワードを指定すると、大量の情報が生成されます。 それが発行される場合、またデータを**データベース url コマンド**によって保存するため外部 TFTPサーバを規定 する必要があります。
4. 指定された DN 文字列に CA 発行者名を設定します。 この例では、cisco1.cisco.com の CN（Common Name）、RTP の L（局所性）、および米国の C（国）は使用されます:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```
5. CA 証明書または証明書のライフタイムを日単位で指定します。有効な値の範囲は *1 ~ 1825 日*です。 デフォルト CA 認証ライフタイムは **3 年**であり、デフォルト証明書ライフタイムは **1 年**です。 最大証明書ライフタイムは *1 か月* CA 認証のライフタイムよりより少しです。 次に、例を示します。
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. 証明書サーバで使用する CRL のライフタイムを時間単位で定義します。 最大ライフタイム値は **336 時間**（2 週）です。 デフォルト値は **168 時間**（1 週）です。
   ```
   R1(cs-server)#lifetime crl 24
   ```
7. 認証サーバによって発行される証明書で使用されるべき Certificate Revocation List Distribution Point（CDP）を定義して下さい。 URL は HTTP URL である必要があります。 たとえば、サーバの IP アドレスは 172.18.108.26 です。
   ```
   R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
   ```

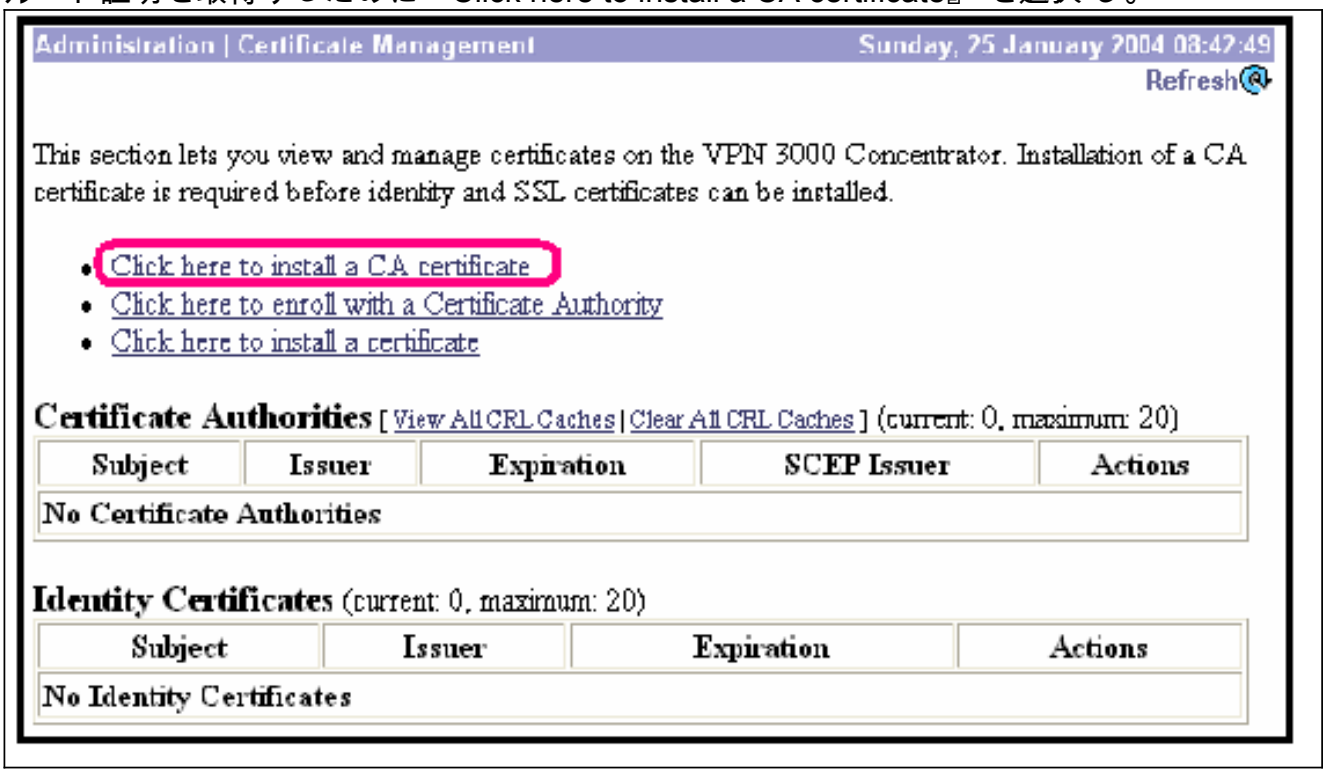
8. **no shutdown コマンドの**発行によって CA サーバをイネーブルに設定して下さい。
```
R1(cs-server)#no shutdown
```

注: 証明書サーバの設定完了後だけ、このコマンドを発行します。

Cisco VPN 3000 コンセントレータを設定し、登録して下さい

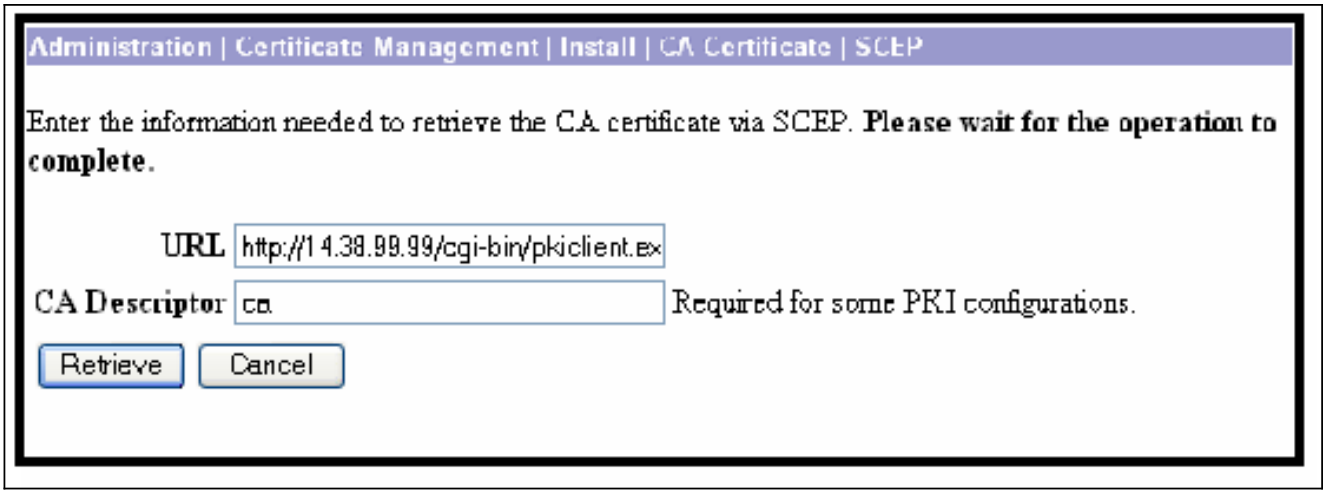
次の手順に従います。

1. Administration > Certificate Management の順に選択 することは Cisco IOS CA サーバからルート証明を取得するために『Click here to install a CA certificate』 を選択 し。

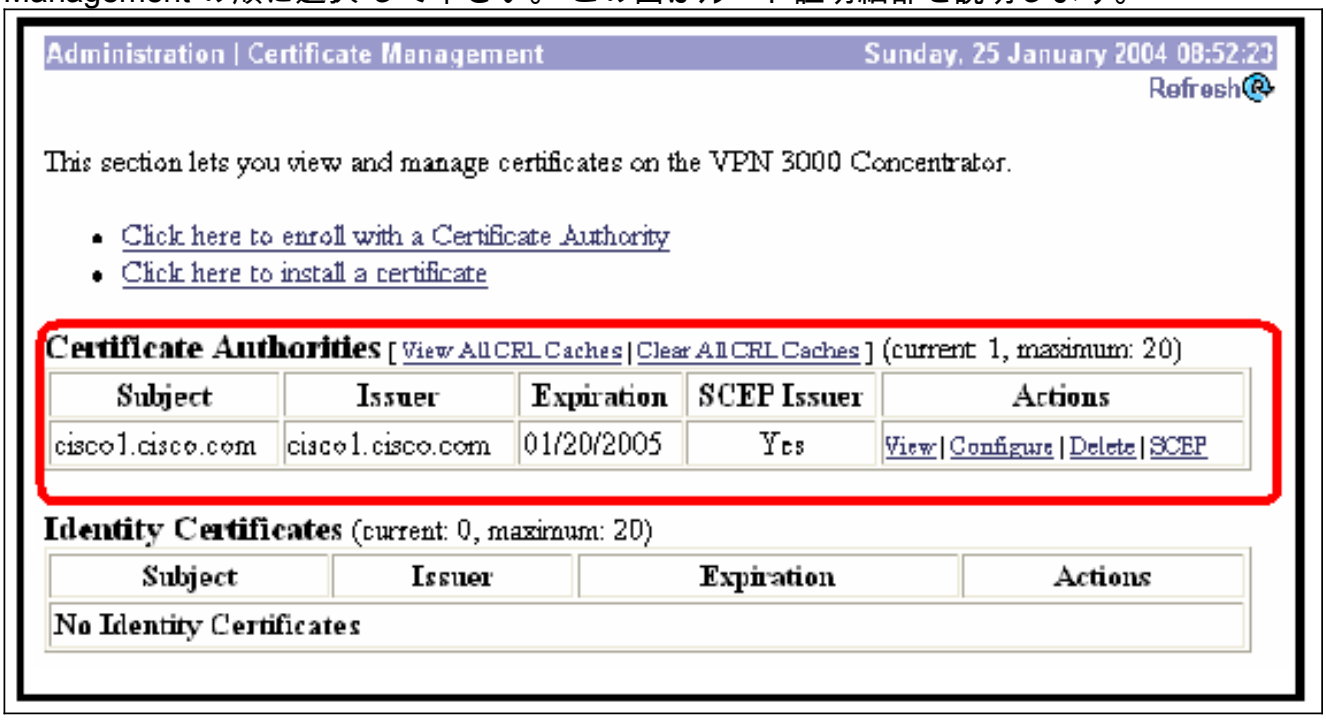


2. インストールの方式として **SCEP を**選択して下さい。

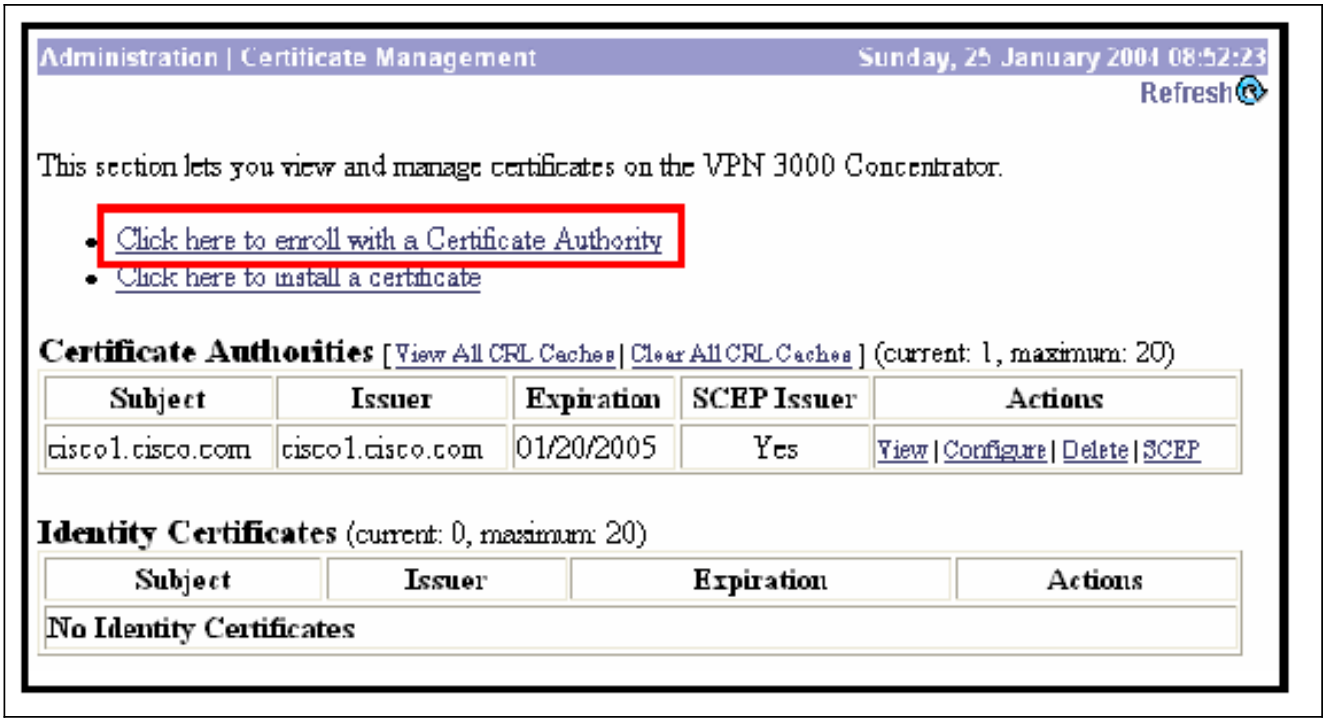
3. Cisco IOS CA サーバの URL を、CA 記述子入力し、『Retrieve』 をクリック して下さい。
注: この例の正しい URL は http://14.38.99.99/cgi-bin/pkiclient.exe （ /cgi-bin/pkiclient.exe のフル パスを含んで下さい ）です。



ルート証明がインストールされていたことを確認するために Administration > Certificate Management の順に選択 して下さい。 この図はルート証明細部を説明します。

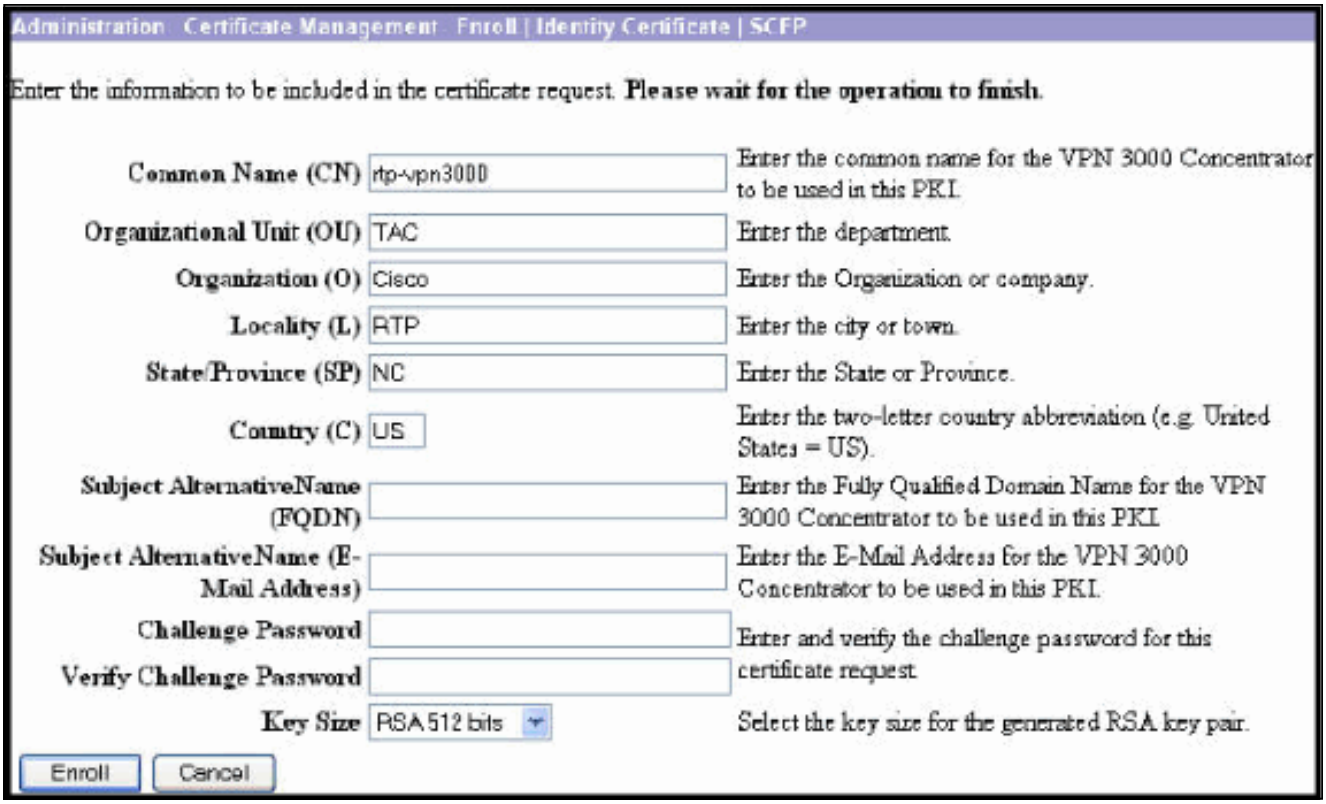


4. Cisco IOS CA サーバからの ID 証明書を得るために『Click here to enroll with a Certificate Authority』 を選択 して下さい。

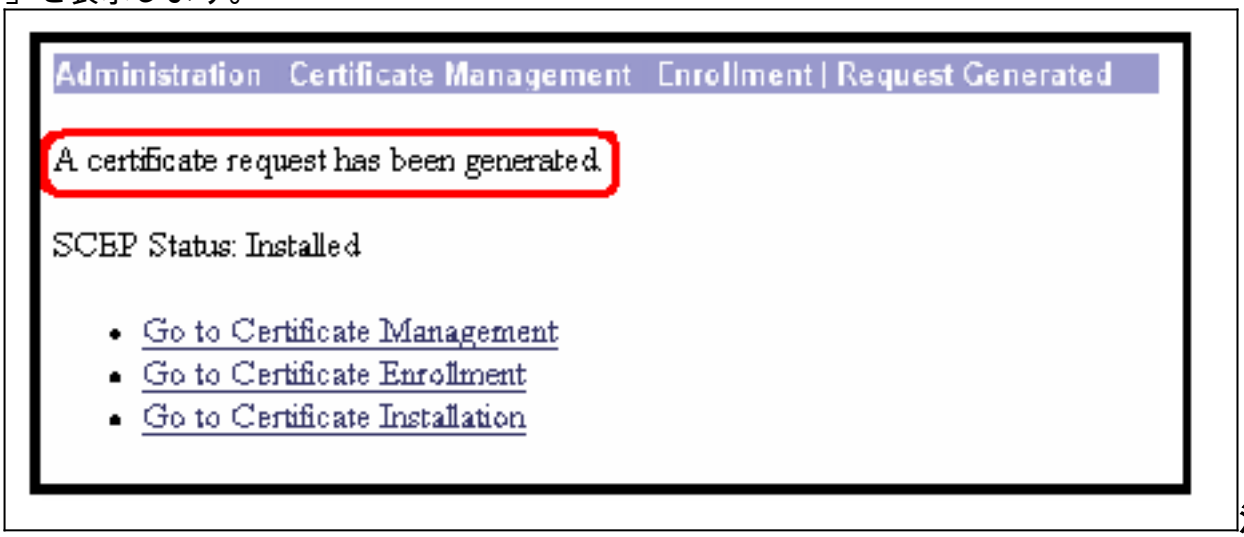


5. **cisco1.cisco.com で SCEP によって**『Enroll』 を選択 して下さい（cisco1.cisco.com は Cisco IOS CA サーバの CN です）。

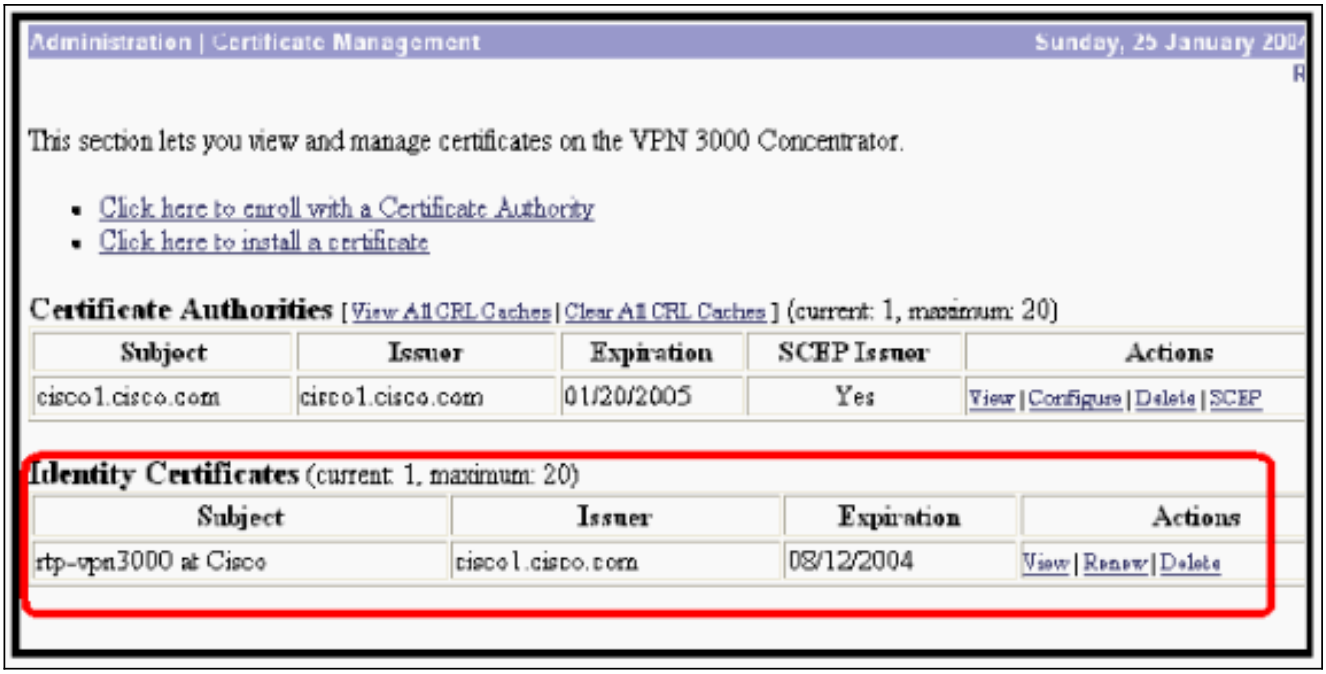
6. 証明書要求の内に含まれているべきすべての情報の入力によって登録形式を記入して下さい。形式の完了の後で、CA サーバに登録要求を始めるために『Enroll』 をクリック して下さい。



『Enroll』 をクリック した後、VPN 3000 コンセントレータは「証明書要求生成されました」を表示します。



注: Cisco IOS CA サーバは自動的に**自動** Cisco IOS CA サーバ サブコマンド**許可**の証明書を許可するために設定することができます。 このコマンドはこの例のために使用されます。 ID 証明書の細部を参照するために、Administration > Certificate Management の順に選択 して下さい。 表示される証明書はこれに類似したです。



確認

確認情報については確認を生成されたキーペア セクション参照して下さい。

トラブルシューティング

トラブルシューティング情報に関しては、VPN 3000 コンセントレータの接続に関する問題のトラブルシューティングか、または IP Security Troubleshooting - Understanding and Using debug Commands を参照して下さい。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems