

デジタル証明書および SSL 証明書を取得するための Cisco VPN 3000 コンセントレータ 4.7.x の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VPNコンセントレータへのデジタル証明書のインストール](#)

[VPNコンセントレータへのSSL証明書のインストール](#)

[VPNコンセントレータでのSSL証明書の更新](#)

[関連情報](#)

概要

このドキュメントでは、デジタルまたは ID 証明書および SSL 証明書を使用して認証するために、Cisco VPN 3000 シリーズ コンセントレータを設定する方法について手順を追って説明します。

注：VPNコンセントレータでは、別のSSL証明書を生成する前にロードバランシングを無効にする必要があります。これは、証明書の生成が妨げられるためです。

PIX/ASA 7.x での同じシナリオに関する詳細については、『[ASDM を使用して Microsoft Windows CA から ASA のデジタル証明書を取得する方法](#)』を参照してください。

Cisco IOS(R) プラットフォームを使用する場合の同様のシナリオについては、『[拡張された登録コマンドを使用した Cisco IOS の証明書登録の設定例](#)』を参照してください。

前提条件

要件

このドキュメントに特有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、バージョン4.7が稼働するCisco VPN 3000コンセントレータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

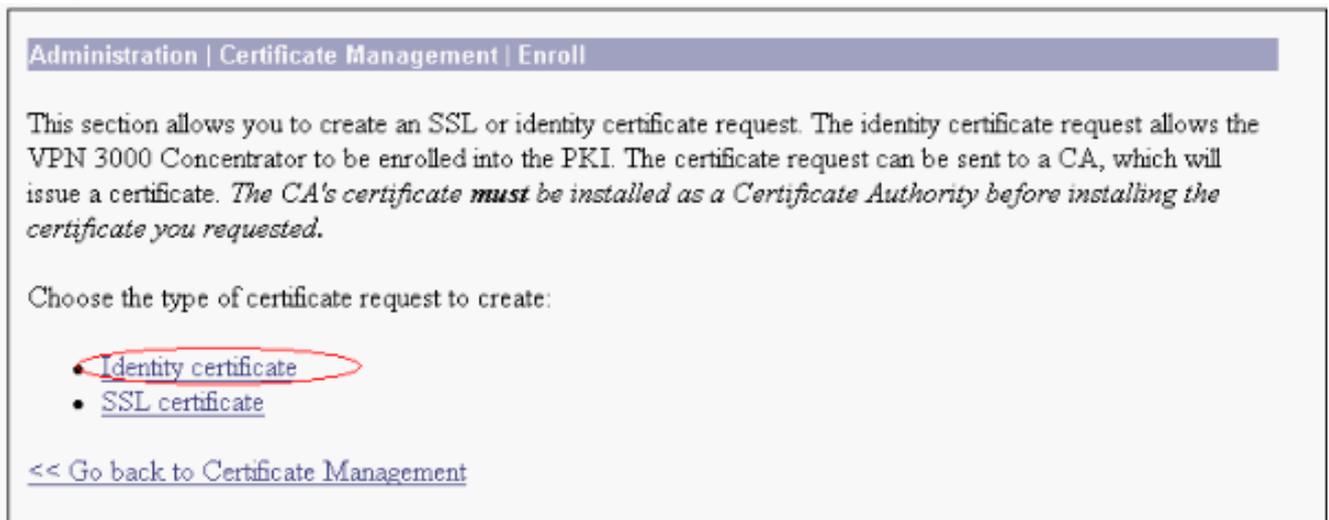
表記法

ドキュメント表記の詳細については、『[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。

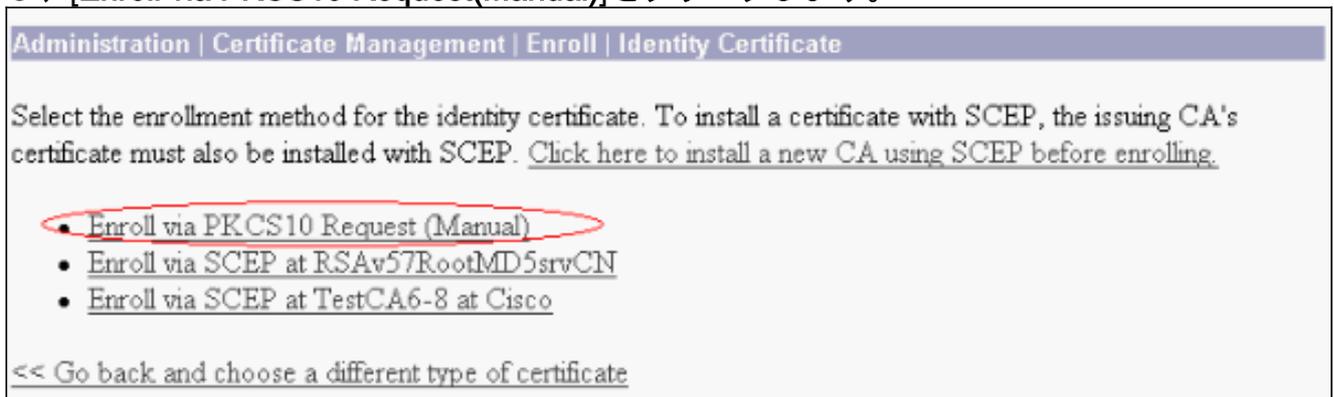
VPNコンセントレータへのデジタル証明書のインストール

次のステップを実行します。

1. [Administration] > [Certificate Management] > [Enroll]の順に選択し、デジタルまたはID証明書要求を選択します。



2. [Administration] > [Certificate Management] > [Enrollment] > [Identity Certificate]の順に選択し、[Enroll via PKCS10 Request(Manual)]をクリックします。



3. 必要なフィールドに入力し、[登録]をクリックします。この例では、これらのフィールドに入力します。共通名:altiga30組織単位:IPSECCERT (OUは設定済みのIPsecグループ名と一致する必要があります) 組織:シスコシステムズLocality:RTP州/州:NorthCarolina国:米国完全修飾ドメイン名(FQDN):(ここでは使用しません) キーサイズ:512注:Simple Certificate Enrollment Protocol(SCEP)を使用してSSL証明書またはID証明書のいずれかを要求する場合、使用できるRSAオプションは次の場合のみです。RSA 512ビットRSA 768ビットRSA 1024ビットRSA 2048ビットDSA 512ビットDSA 768ビットDSA 1024ビット

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Common Name (CN)	<input type="text" value="altiga30"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="IPSECCERT"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco Systems"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="RTP"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NorthCarolina"/>	Enter the State or Province.
Country (C)	<input type="text" value="US"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA/DSA key pair.

4. [登録]をクリックすると、いくつかのウィンドウが表示されます。最初のウィンドウで、証明書を要求したことを確認します。

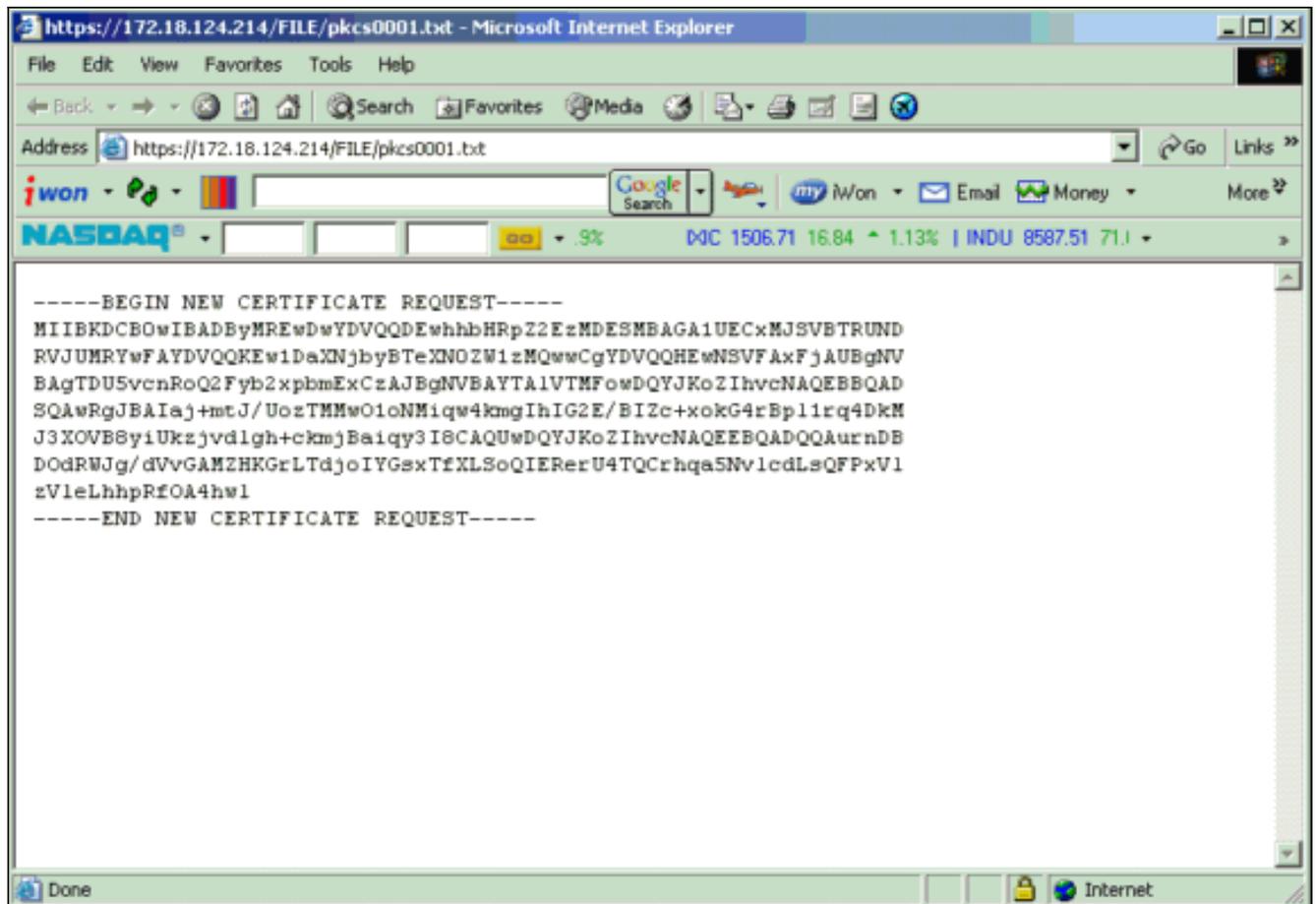
Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated. In a few seconds, a new browser window will open up with the certificate request. The request can be saved as a file, or copied then pasted into a CA's management interface.

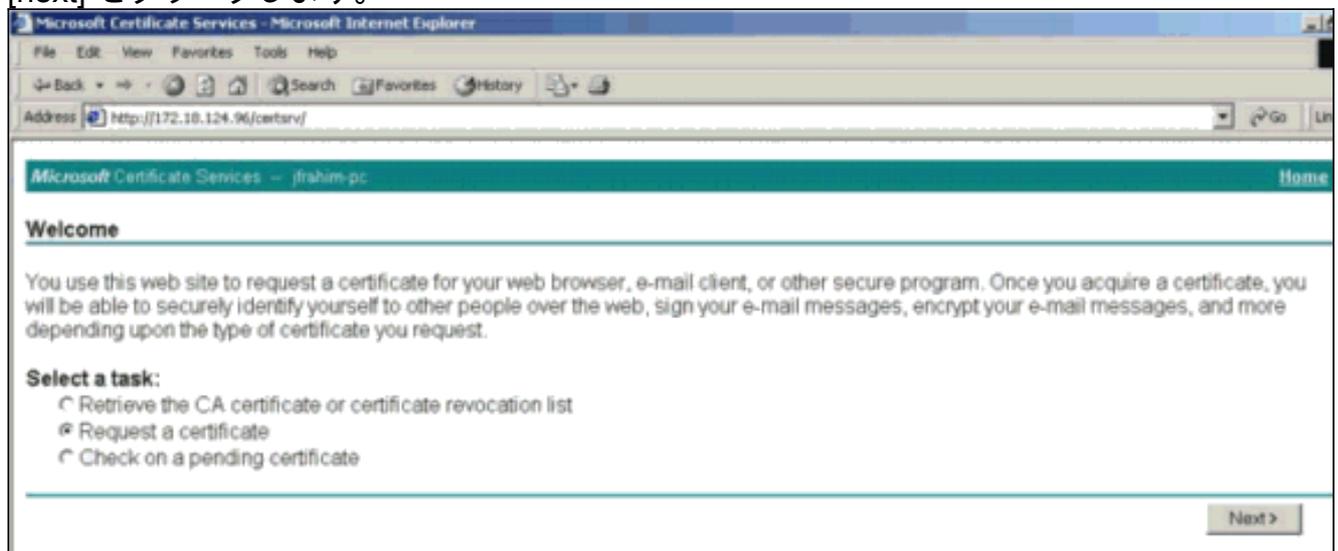
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file, go to the [File Management page](#) to delete the certificate request.

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

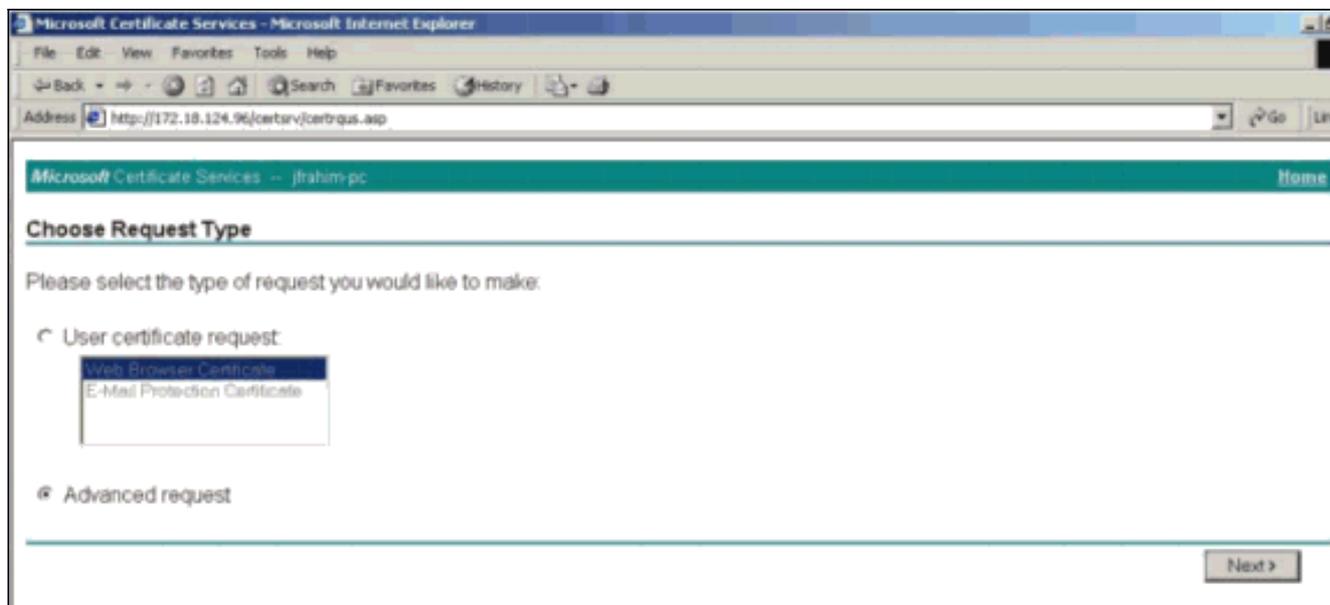
新しいブラウザウィンドウが開き、PKCS要求ファイルが表示されます。



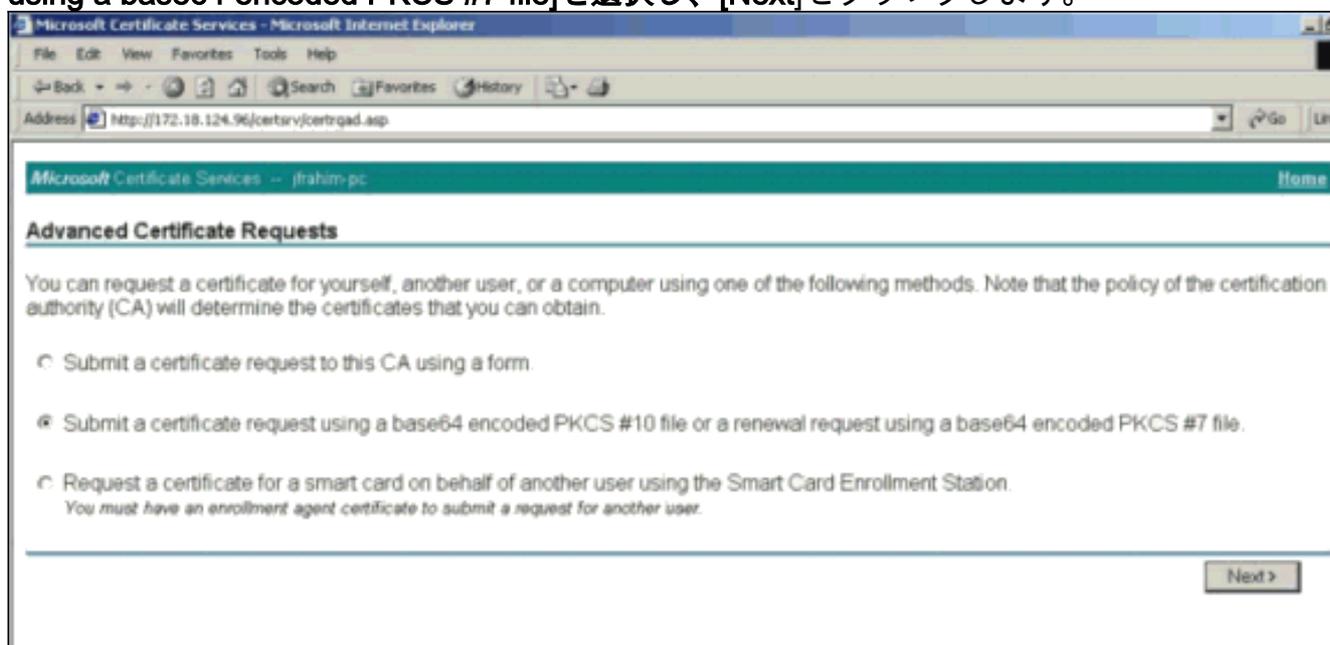
5. 証明機関(CA)サーバで、要求を強調表示し、CAサーバに貼り付けて要求を送信します。
[next] をクリックします。



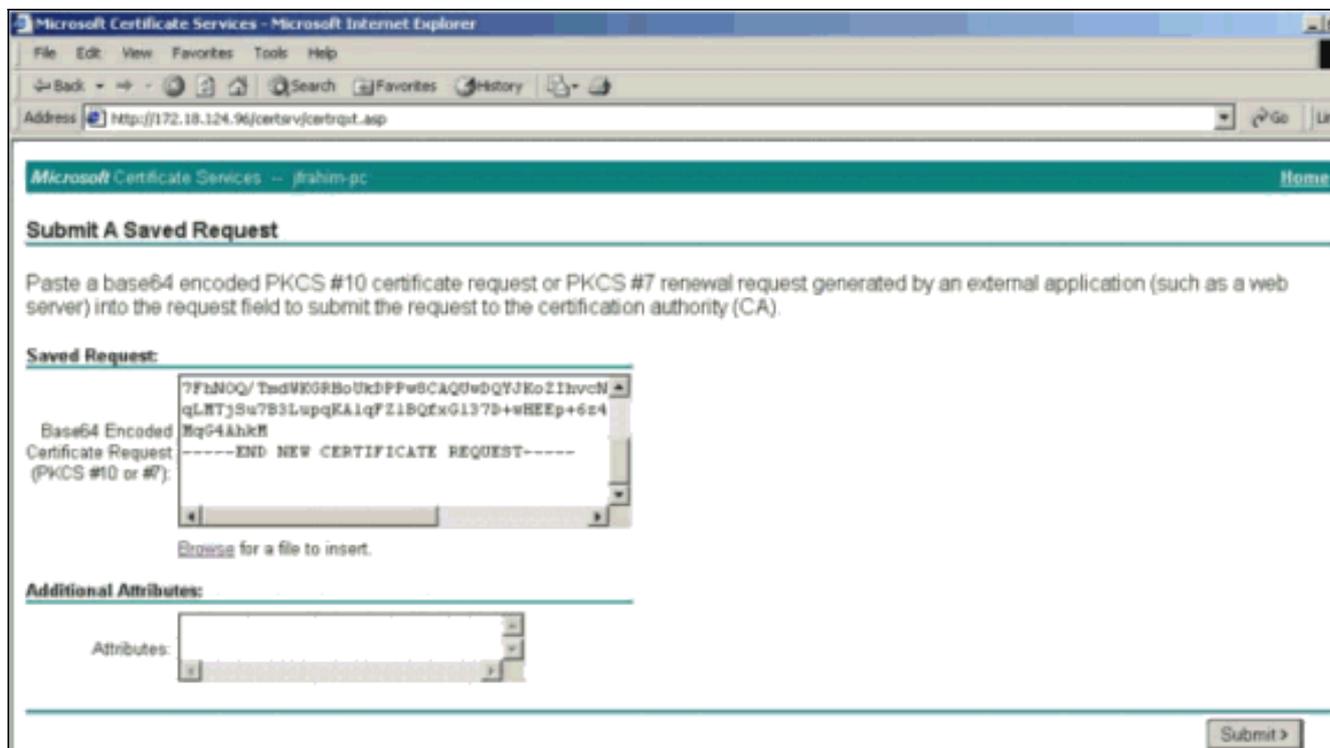
6. [Advanced request]を選択し、[Next]をクリックします。



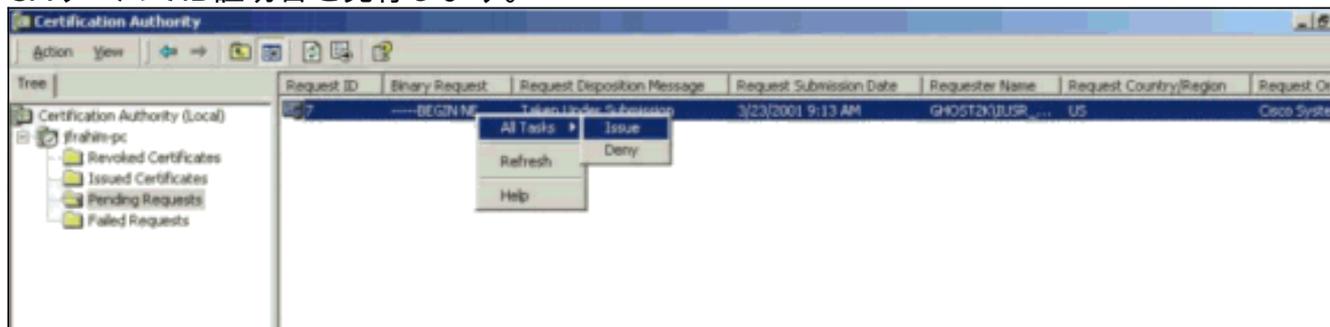
7. [Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file]を選択し、[Next]をクリックします。



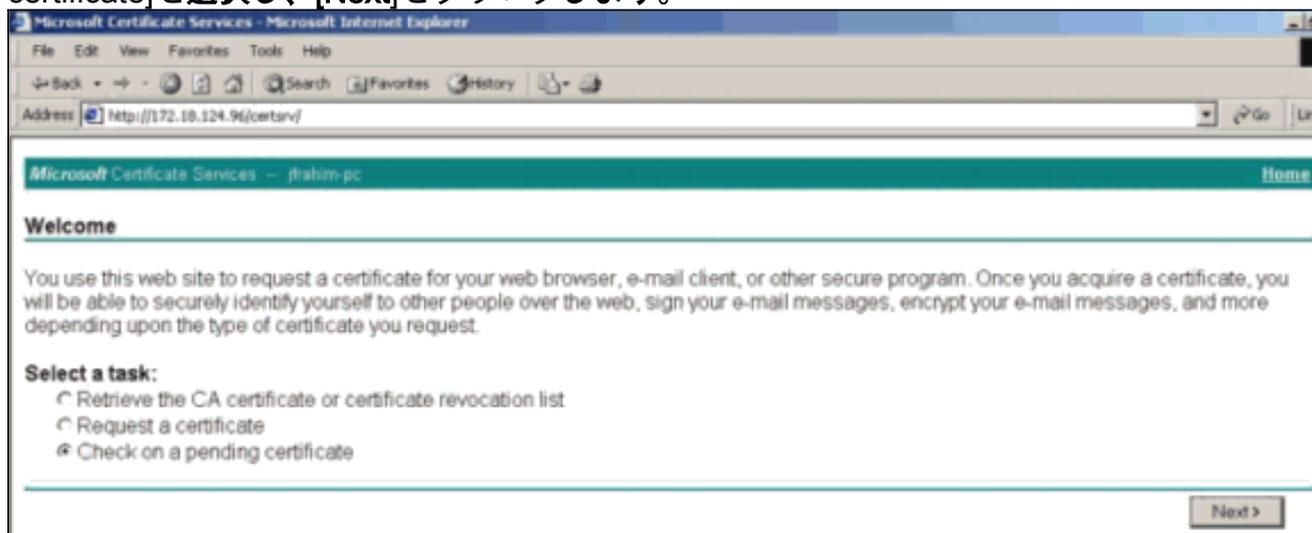
8. [Saved Request]セクションのテキストフィールドにPKCSファイルをカットアンドペーストします。次に、[Submit] をクリックします。



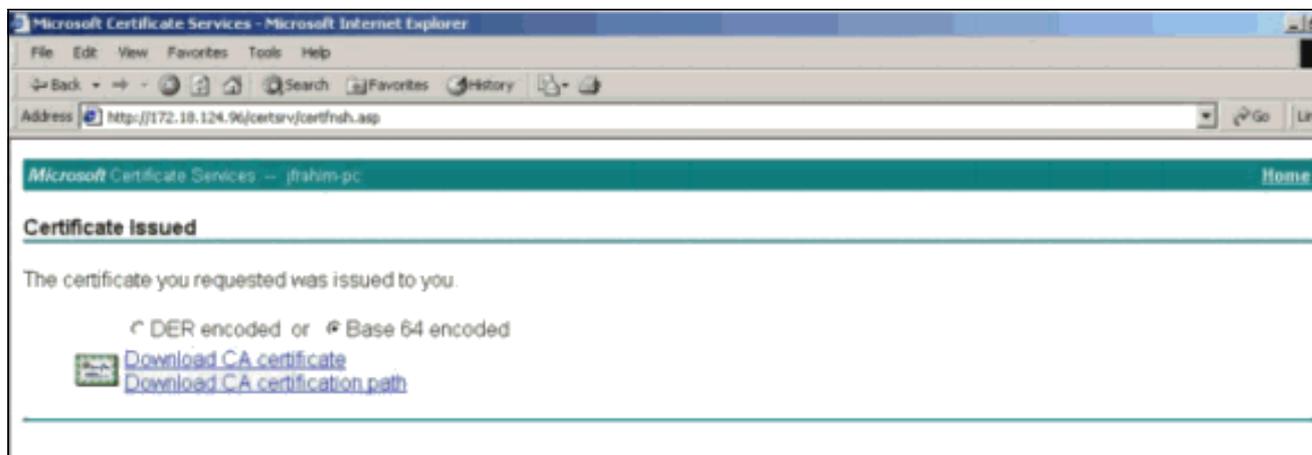
9. CAサーバでID証明書を発行します。



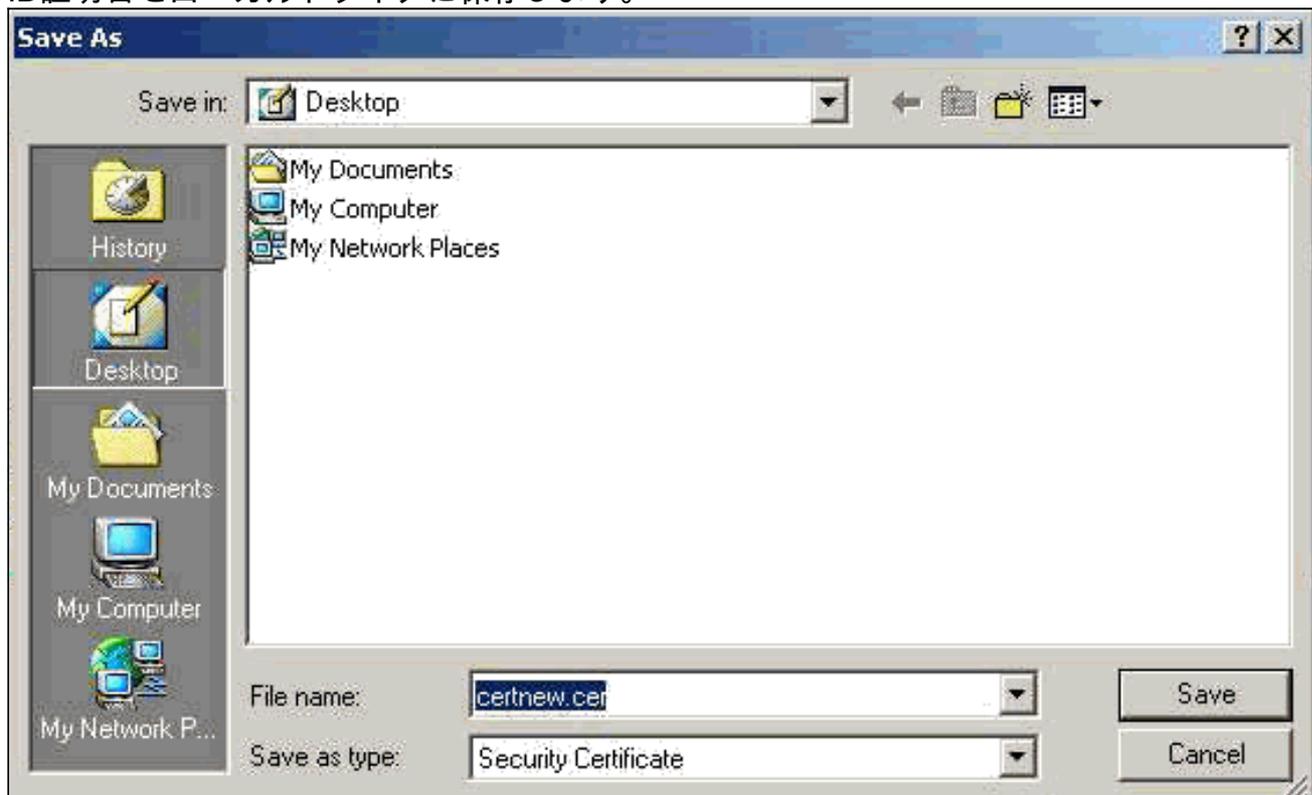
10. ルート証明書とID証明書をダウンロードします。CAサーバで、[Check on a pending certificate]を選択し、[Next]をクリックします。



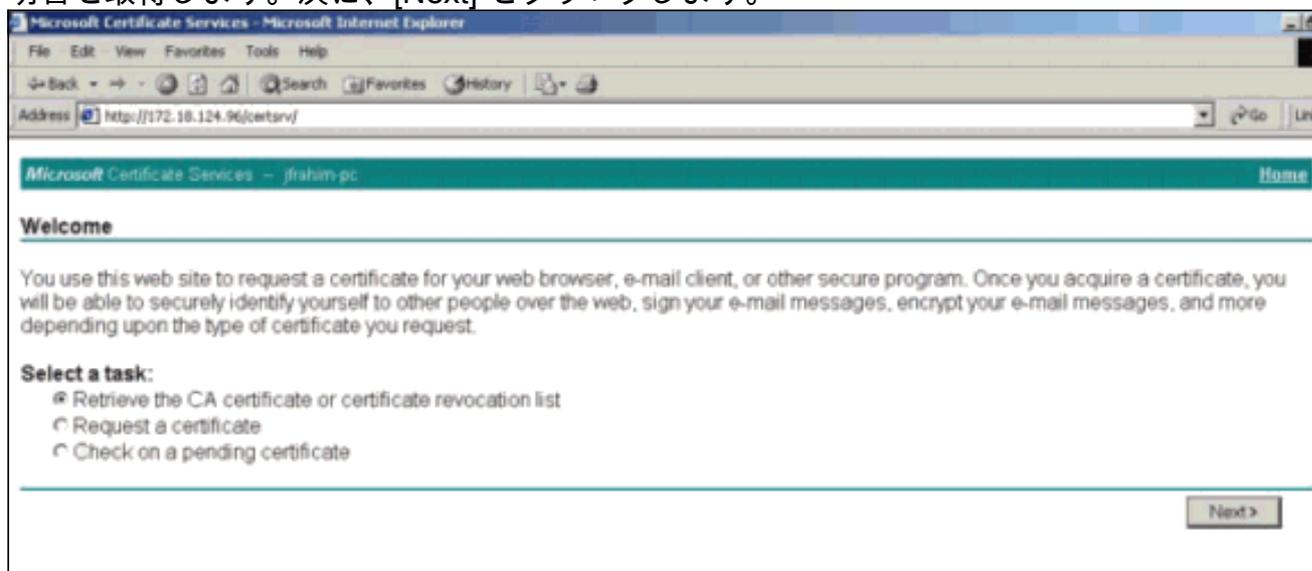
11. [Base 64 encoded]を選択し、CAサーバで[Download CA certificate]をクリックします。



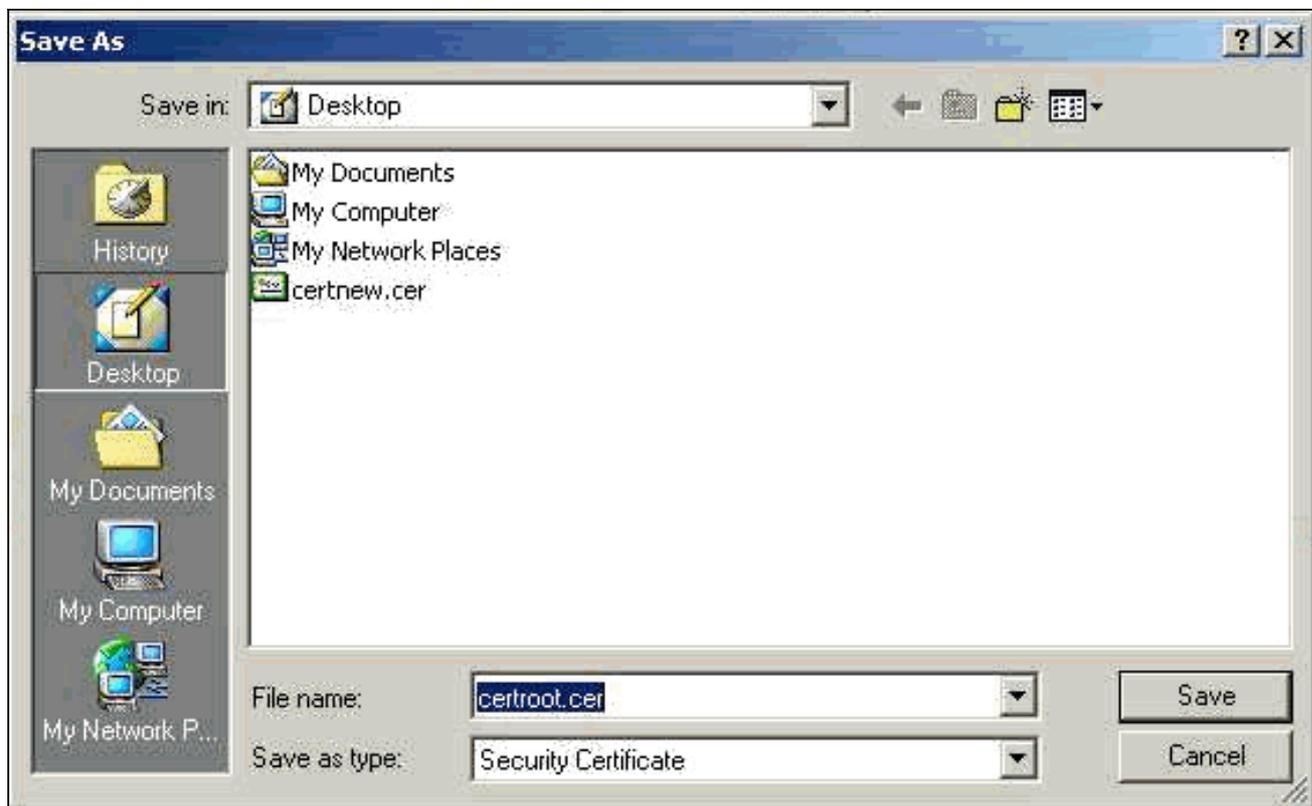
12. ID証明書をローカルドライブに保存します。



13. CAサーバで、[Retrieve the CA certificate or certificate revocation list]を選択して、ルート証明書を取得します。次に、[Next] をクリックします。



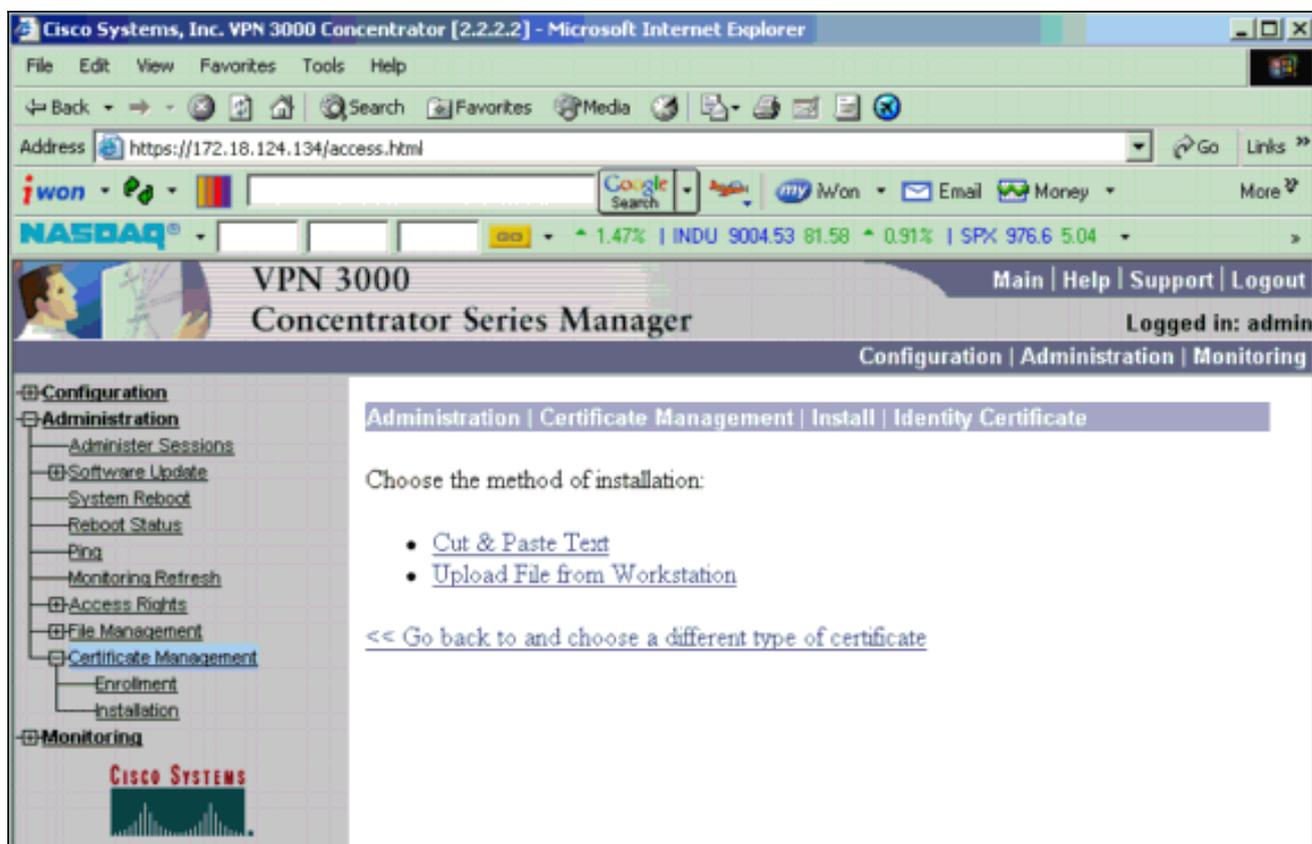
14. ローカルドライブにルート証明書を保存します。



- VPN 3000コンセントレータにルート証明書とID証明書をインストールします。これを行うには、[Administration] > [Certificate Manager] > [Installation] > [Install certificate obtain via enrollment] の順に選択します。[Enrollment Status]で、[Install]をクリックします。



- [Upload File from Workstation]をクリックします。



17. [Browse]をクリックし、ローカルドライブに保存したルート証明書ファイルを選択します。[Install] を選択して、VPNコンセントレータにID証明書をインストールします。行政 | [Certificate Management]ウィンドウが確認として表示され、新しいID証明書が[Identity Certificates]テーブルに表示されます。

注：証明書が失敗した場合に新しい証明書を生成するには、次の手順を実行します。
[Administration] > [Certificate Management]を選択します。SSL証明書リストの[Actions]ボックスで[Delete]をクリックします。[Administration] > [System Reboot]を選択します。
[Save the active configuration at time of reboot]を選択し、[Now]を選択して[Apply]をクリックします。リロードが完了すると、新しい証明書を生成できるようになりました。

VPNコンセントレータへのSSL証明書のインストール

ブラウザとVPNコンセントレータ間のセキュアな接続を使用する場合、VPNコンセントレータにはSSL証明書が必要です。また、VPNコンセントレータ、WebVPN、およびWebVPNトンネルを終端する各インターフェイスの管理に使用するインターフェイスにSSL証明書が必要です。

インターフェイスSSL証明書が存在しない場合、VPN 3000コンセントレータソフトウェアをアップグレードした後にVPN 3000コンセントレータがリブートすると自動的に生成されます。自己署名証明書は自己生成されるため、この証明書は検証できません。認証局は、そのIDを保証していません。ただし、この証明書を使用すると、ブラウザを使用してVPNコンセントレータに最初に

接続できます。別の自己署名SSL証明書に置き換える場合は、次の手順を実行します。

1. [Administration] > [Certificate Management]を選択します。

Administration | Certificate Management Monday, 05 January 2004 16:31:11
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
ms-root-sha-06-2001 at cisco	ms-root-sha-06-2001 at cisco	06/04/2022	No	View Configure Delete

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Gateway A at Cisco Systems	ms-root-sha-06-2001 at cisco	02/04/2004	View Renew Delete

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.5.6.1 at Cisco Systems, Inc.	10.5.6.1 at Cisco Systems, Inc.	02/01/2006	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	01/05/2004	Generate

2. [Generate] をクリックして、SSL証明書テーブルに新しい証明書を表示し、既存の証明書を置き換えます。このウィンドウでは、VPNコンセントレータが自動的に生成するSSL証明書のフィールドを設定できます。これらのSSL証明書は、インターフェイスおよびロードバランシング用です。

Administration | Certificate Management | Generate SSL Certificate

You are about to generate a certificate for the Public Interface . The certificate will have the following DN for both Subject and Issuer.

The certificate will be valid for 3 years from yesterday.

Common Name (CN) Enter the Common Name, usually the IP or DNS address of this interface.

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

RSA Key Size Select the key size for the generated RSA key pair.

検証可能なSSL証明書（つまり認証局が発行したもの）を取得する場合は、ID証明書の取得に使用するのと同じ手順を使用するために、このドキュメントの「[VPNコンセントレータへのデジタル証明書のインストール](#)」セクションを参照してください。ただし、今回は、[Administration] > [Certificate Management] > [Enroll]ウィンドウで、(ID証明書の代わりにSSL証明書をクリックします。注：管理を参照してください | VPN 3000 Concentrator Reference Volume IIのCertificate Managementセクション：デジタル証明書およびSSL証明書に関する完全な情報については、管理および監視リリース4.7。

[VPNコンセントレータでのSSL証明書の更新](#)

このセクションでは、SSL証明書の更新方法について説明します。

VPNコンцентрータによって生成されたSSL証明書の場合は、SSLセクションのAdministration > Certificate Managementの順に進みます。renewオプションをクリックし、SSL証明書を更新します。

外部CAサーバによって許可された証明書の場合は、次の手順を実行します。

1. SSL CertificatesでAdministration > Certificate Management > Deleteの順に選択して、期限切れの証明書をパブリックインターフェイスから削除します。

Administration | Certificate Management Wednesday, 19 September 2007 00:01:4
[Refresh](#)

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut... at Equifax	08/16/2008	View Renew Delete Export Generate Enroll Import



SSL証明書の削除を確認するには、[Yes]をクリックします。

Subject

CN=pearlygates.ocp.org
 OU=Domain Control Validated - QuickSSL Premium(R)
 OU=See www.geotrust.com/resources/cps (c)07
 OU=GT94824223
 O=pearlygates.ocp.org
 C=US

Issuer

OU=Equifax Secure Certificate Authority
 O=Equifax
 C=US

Serial Number 07E267**Signing Algorithm** SHA1WithRSA**Public Key Type** RSA (1024 bits)**Certificate Usage** Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment**MD5 Thumbprint** 2C:EC:8D:8B:FE:59:9D:F8:04:A6:B2:1B:C5:09:9A:27**SHA1 Thumbprint** 6E:9A:7C:D3:02:FE:10:1C:75:79:00:AA:6A:73:84:54:C2:DC:BE:95**Validity** 8/16/2007 at 17:26:35 to 8/16/2008 at 17:26:35**CRL Distribution Point** http://crl.geotrust.com/crls/secureca.crlAre you **sure** you want to delete this certificate?

2. [Administration] > [Certificate Management] > [Generate]を選択して、新しいSSL証明書を作成します。

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	No Certificate Installed.			Generate Enroll Import



パブリックインターフェイスの新しいSSL証明書が表示されます。

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	View Renew Delete Export Generate Enroll Import

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](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)