

# Configurazione di Cisco VPN 3000 Concentrator 4.7.x per ottenere un certificato digitale e un certificato SSL

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Installare i certificati digitali sul concentratore VPN](#)

[Installare i certificati SSL sul concentratore VPN](#)

[Rinnova certificati SSL sul concentratore VPN](#)

[Informazioni correlate](#)

## Introduzione

Questo documento include istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator per l'autenticazione con l'utilizzo di certificati digitali o di identità e certificati SSL.

**Nota:** in Concentrator VPN, è necessario disabilitare il bilanciamento del carico prima di generare un altro certificato SSL, in quanto ciò impedisce la generazione del certificato.

Per ulteriori informazioni sullo stesso scenario con PIX/ASA 7.x, consultare il documento sulla [procedura per ottenere un certificato digitale da una CA di Microsoft Windows usando ASDM su un'ASA](#).

Per ulteriori informazioni sullo stesso scenario delle piattaforme Cisco IOS®, fare riferimento all'[esempio di configurazione della registrazione di certificati Cisco IOS con i comandi di registrazione avanzata](#).

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Per questo documento, è stato usato Cisco VPN 3000 Concentrator versione 4.7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

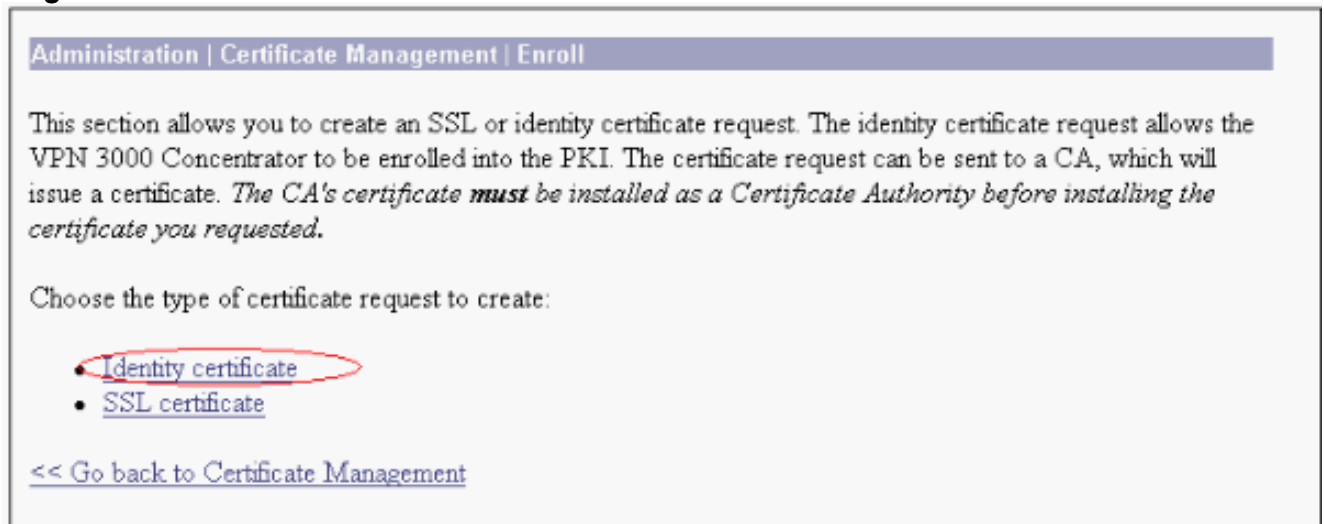
## [Convenzioni](#)

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

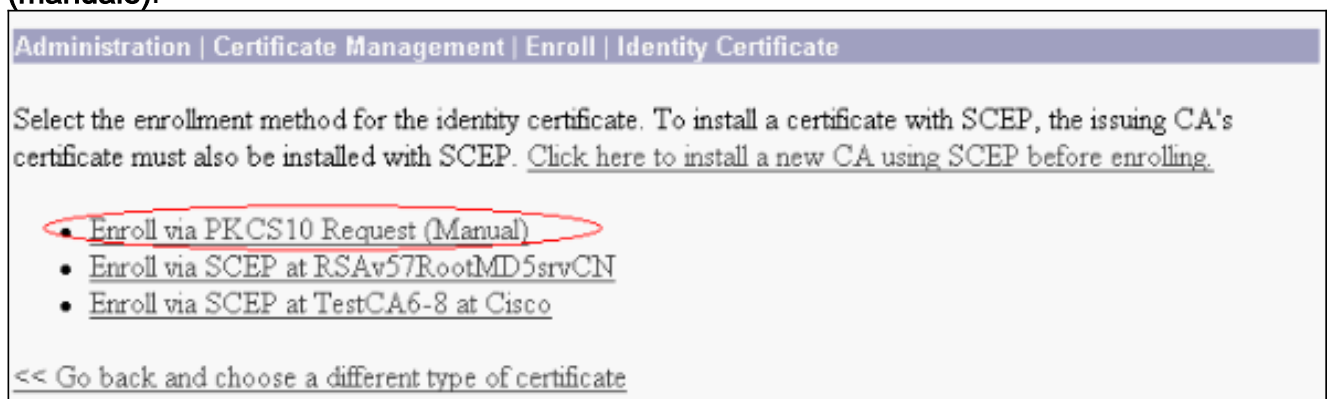
## [Installare i certificati digitali sul concentratore VPN](#)

Attenersi alla seguente procedura:

1. Per selezionare la richiesta di certificato digitale o di identità, scegliere **Amministrazione > Gestione certificati > Registra**.



2. Scegliere **Amministrazione > Gestione certificati > Registrazione > Certificato di identità e fare clic su Registra tramite richiesta PKCS10 (manuale)**.



3. Compilare i campi richiesti e quindi fare clic su **Registra**. Questi campi vengono compilati in questo esempio. **Nome comune:** altiga30 **Unità organizzativa** - IPSECCERT (l'unità organizzativa deve corrispondere al nome di gruppo IPsec configurato) **Organizzazione**—Cisco Systems **Località:** RTP **Stato/Provincia**—Carolina del Nord **Paese**—US **Nome di dominio completo** - (non utilizzato qui) **Dimensione chiave**—512 **Nota:** se si richiede un certificato SSL o un certificato di identità utilizzando il

protocollo SCEP (Simple Certificate Enrollment Protocol), queste sono le uniche opzioni RSA disponibili. RSA 512 bit RSA 768 bit RSA 1024 bit RSA 2048 bit DSA 512 bit DSA 768 bit DSA 1024 bit

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. Dopo aver fatto clic su **Registra**, vengono visualizzate diverse finestre. La prima finestra conferma che è stato richiesto un certificato.

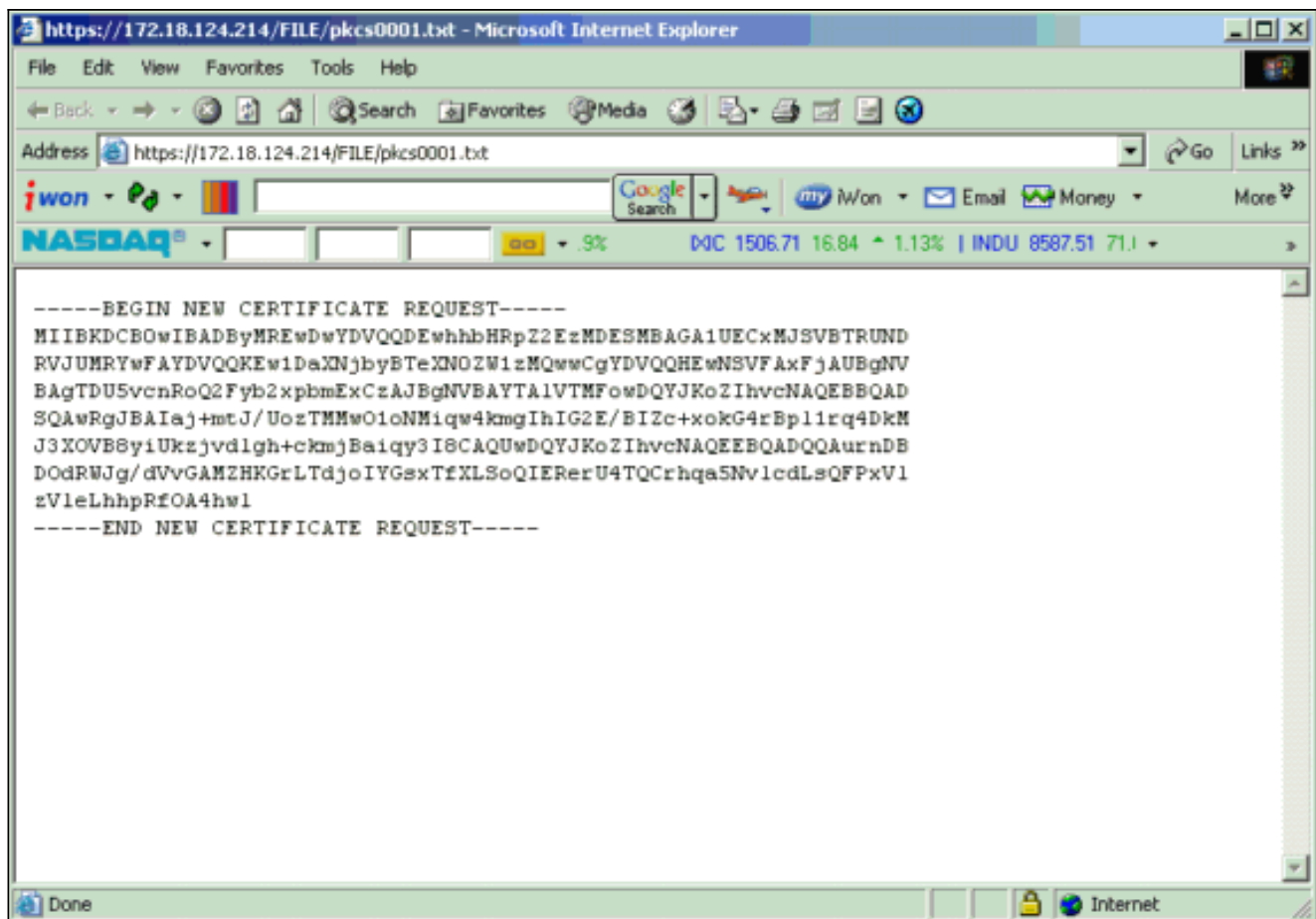
Administration | Certificate Management | Enrollment | Request Generated

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.

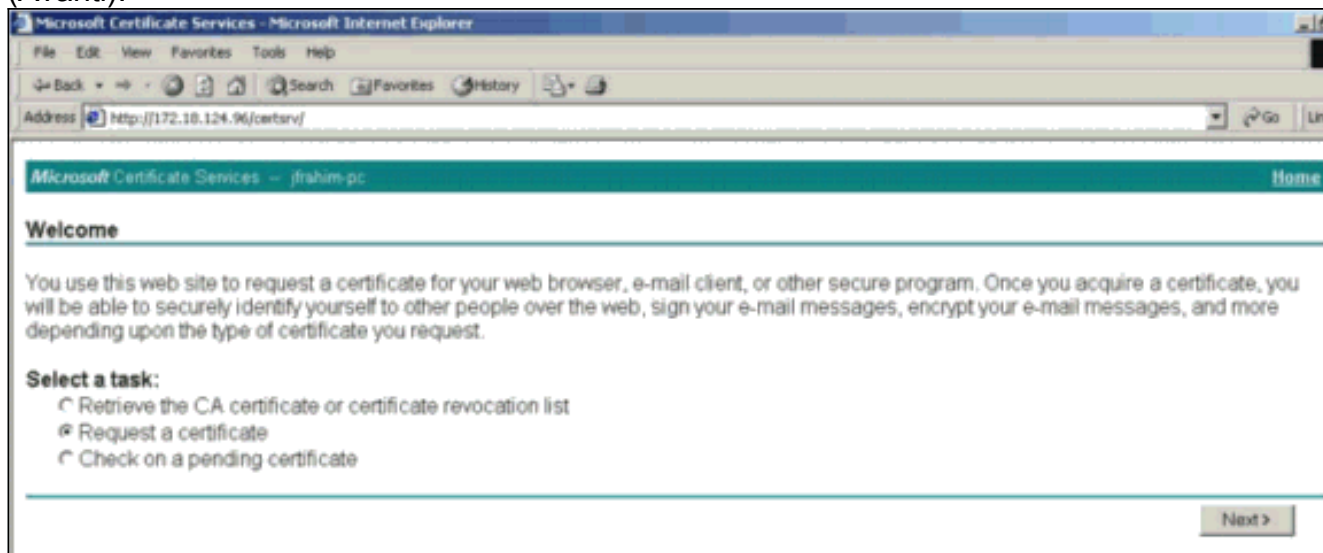
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the [File Management page](#) to delete the certificate request.

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

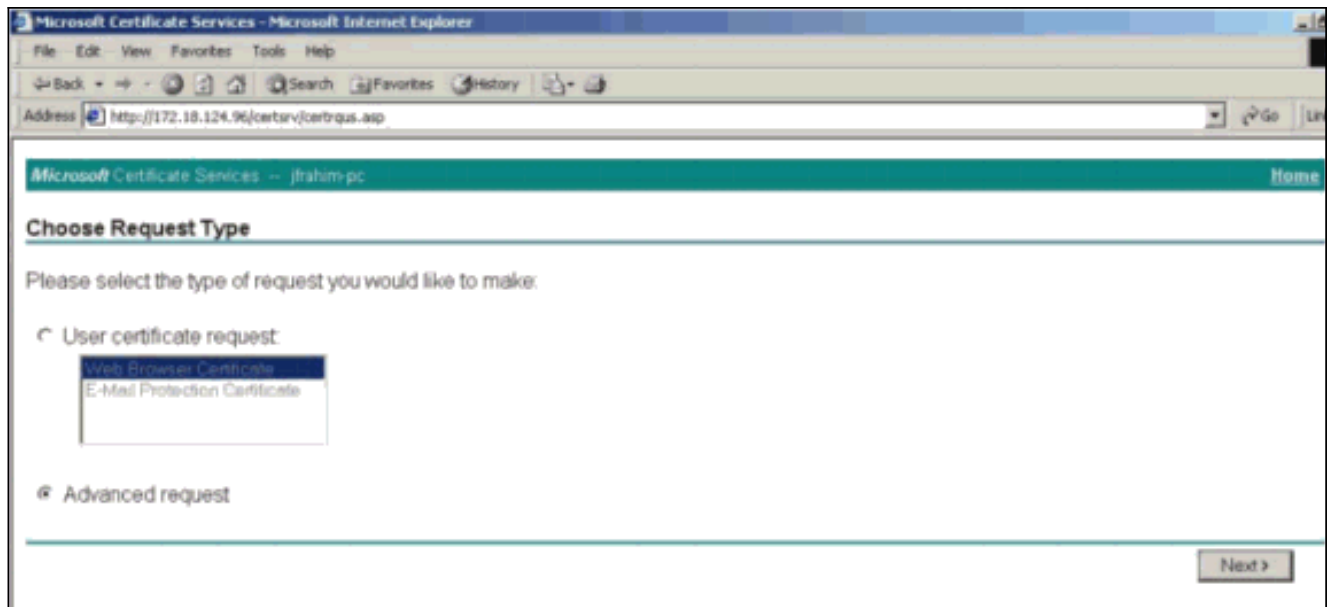
Viene inoltre visualizzata una nuova finestra del browser in cui è visualizzato il file di richiesta PKCS.



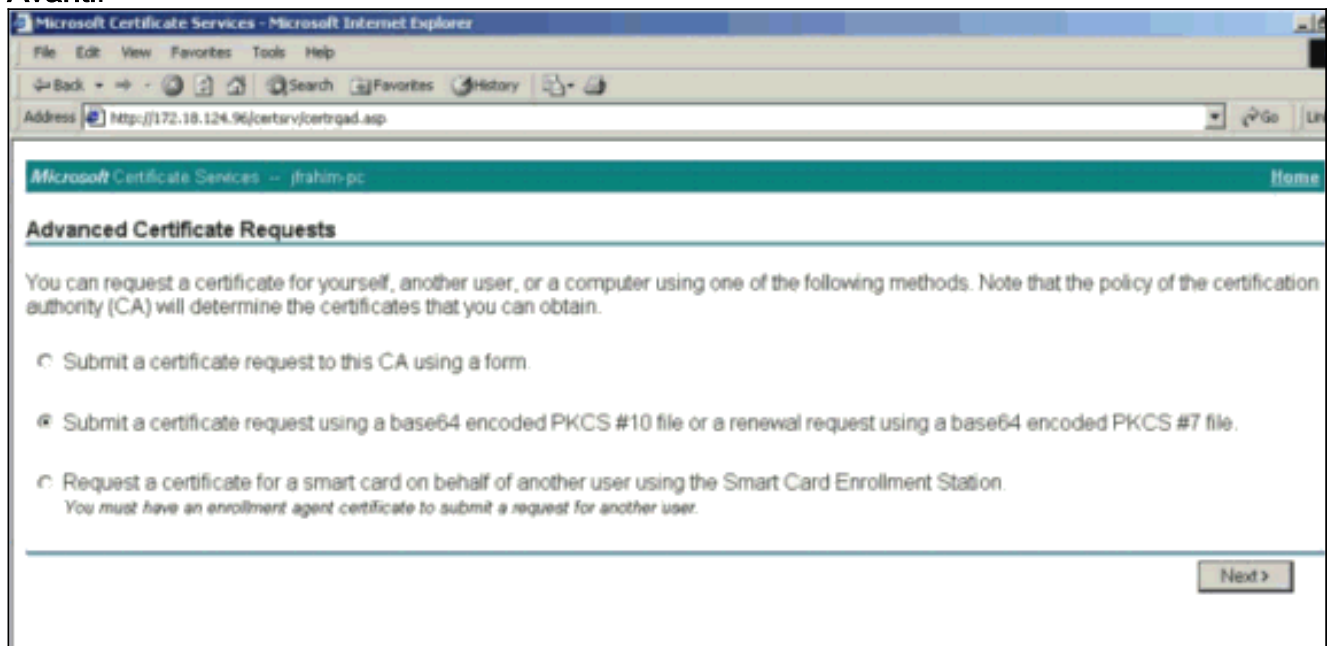
5. Sul server Autorità di certificazione (CA), evidenziare la richiesta e incollarla nel server CA per inviare la richiesta. Fare clic su **Next** (Avanti).



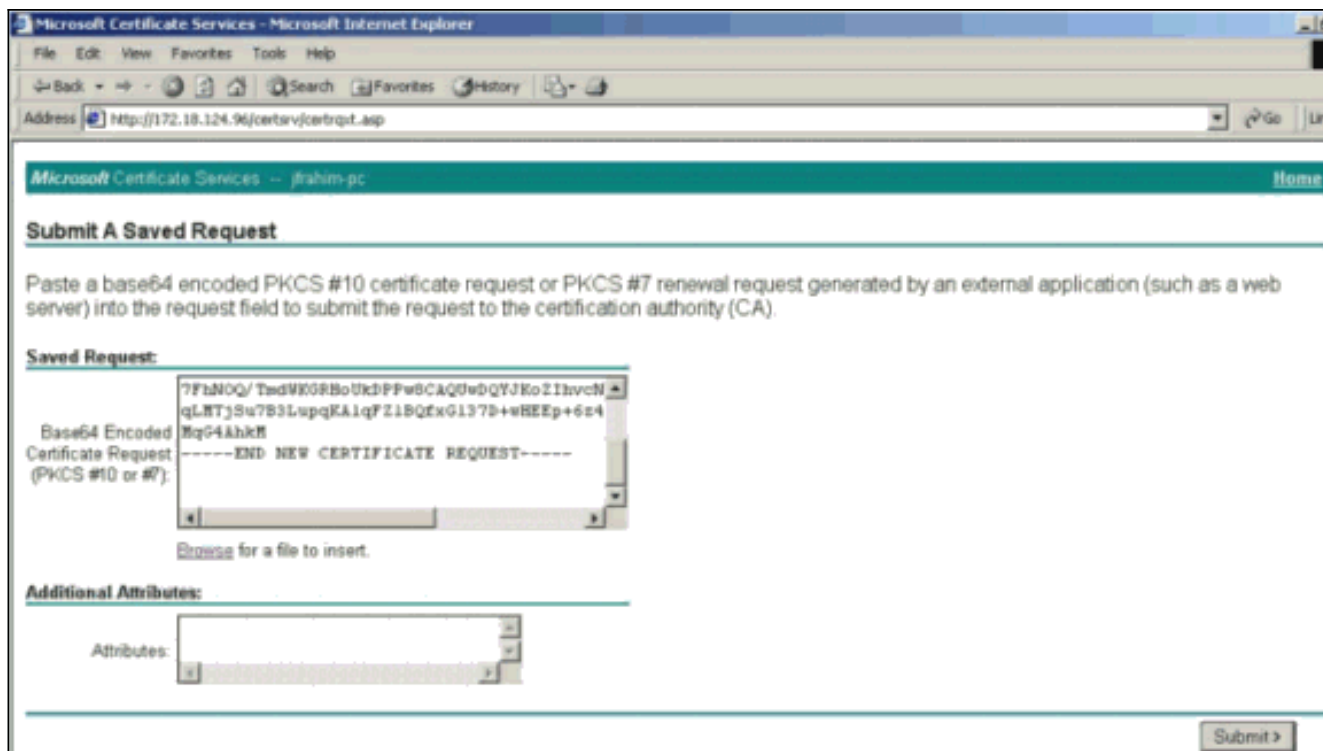
6. Selezionare **Richiesta avanzata** e fare clic su **Avanti**.



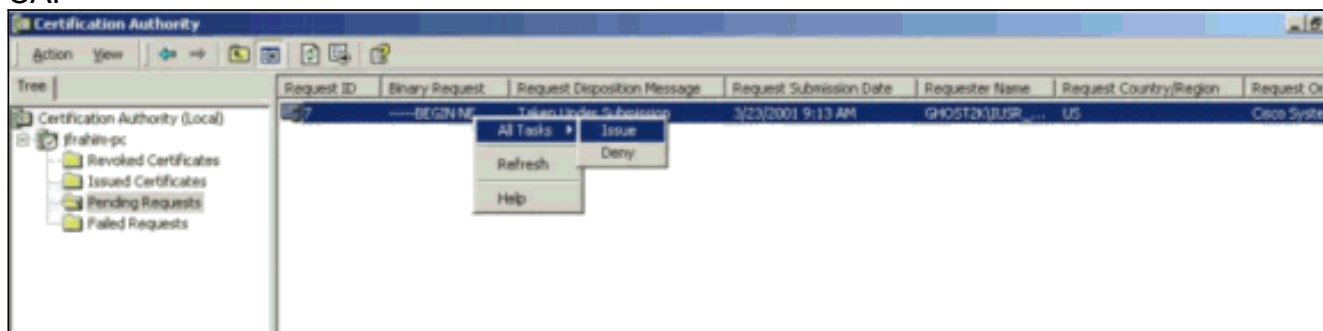
7. Selezionare **Invia una richiesta di certificato utilizzando un file PKCS #10 con codifica Base64** o una richiesta di rinnovo utilizzando un file PKCS #7 con codifica Base64, quindi fare clic su **Avanti**.



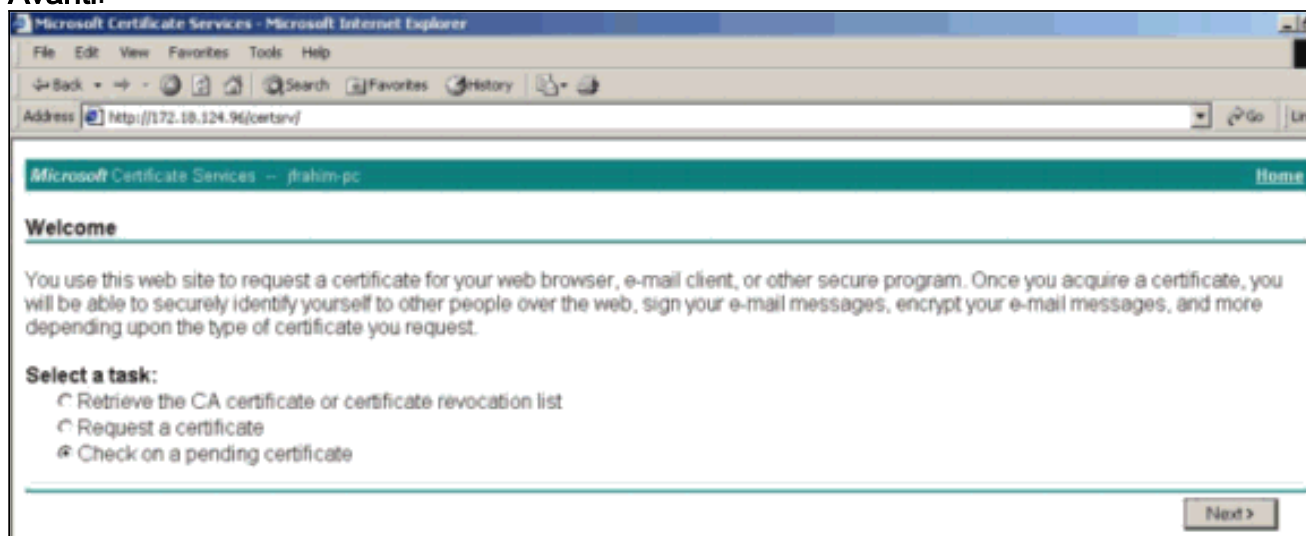
8. Tagliare e incollare il file PKCS nel campo di testo sotto la sezione **Richiesta salvata**. Quindi fare clic su **Invia**.



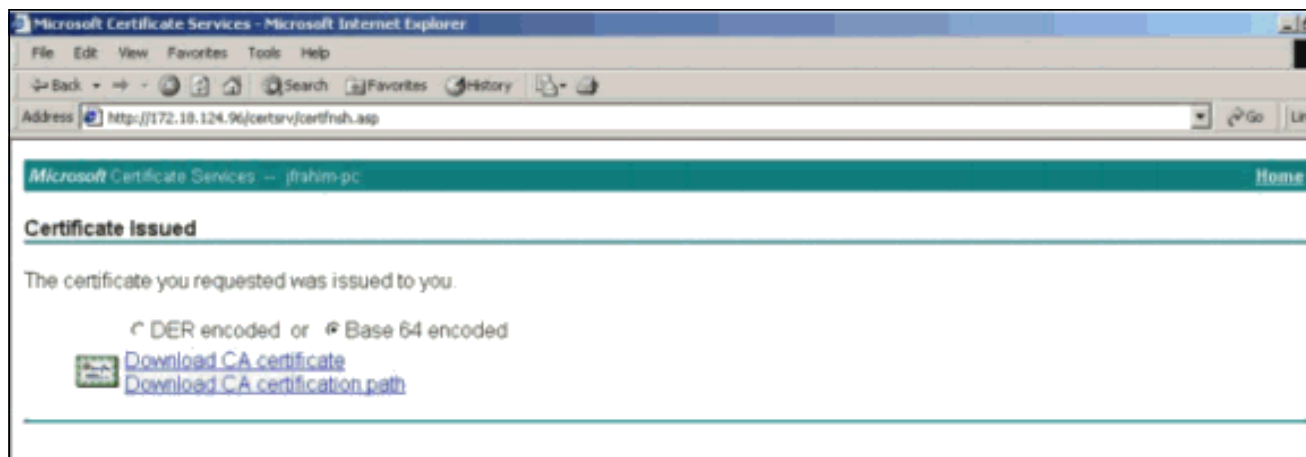
9. Rilasciare il certificato di identità sul server CA.



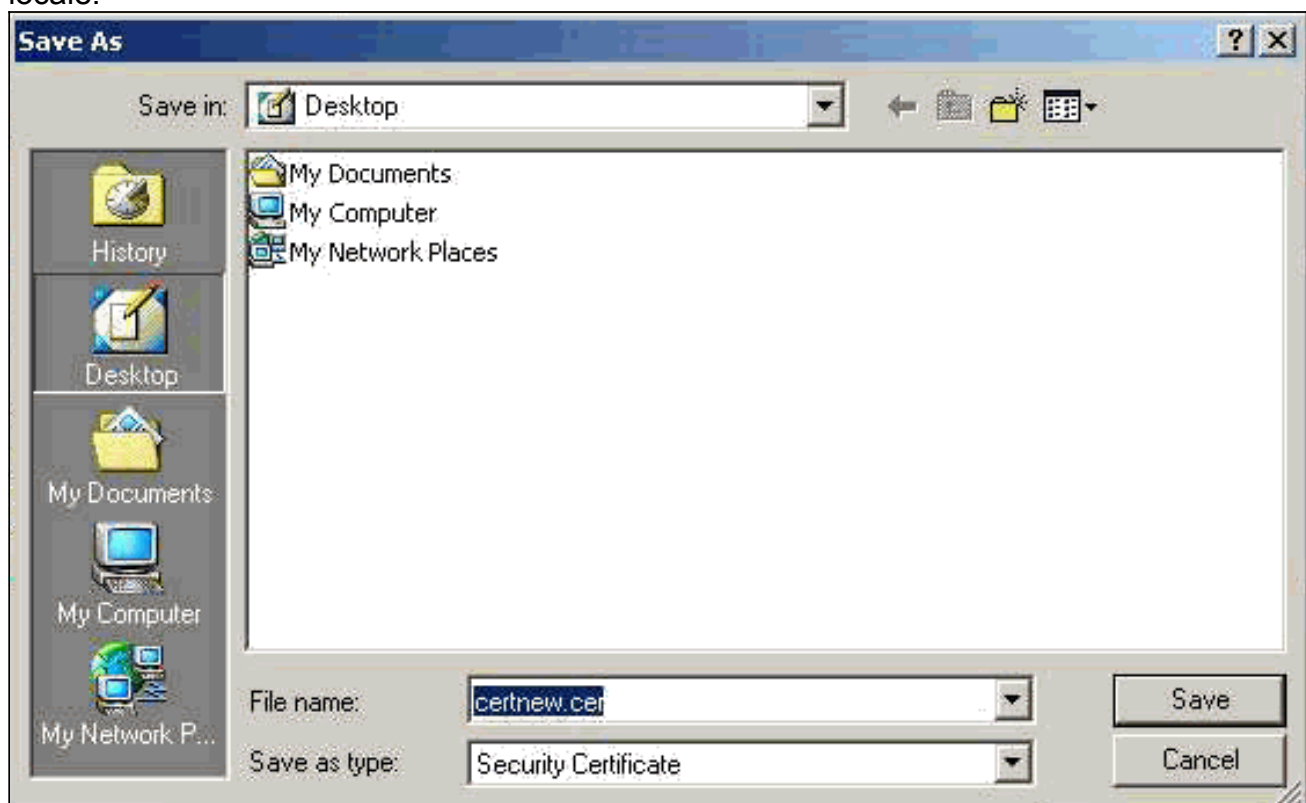
10. Scaricare la radice e i certificati di identità. Sul server CA selezionare **Verifica un certificato in sospeso** e fare clic su **Avanti**.



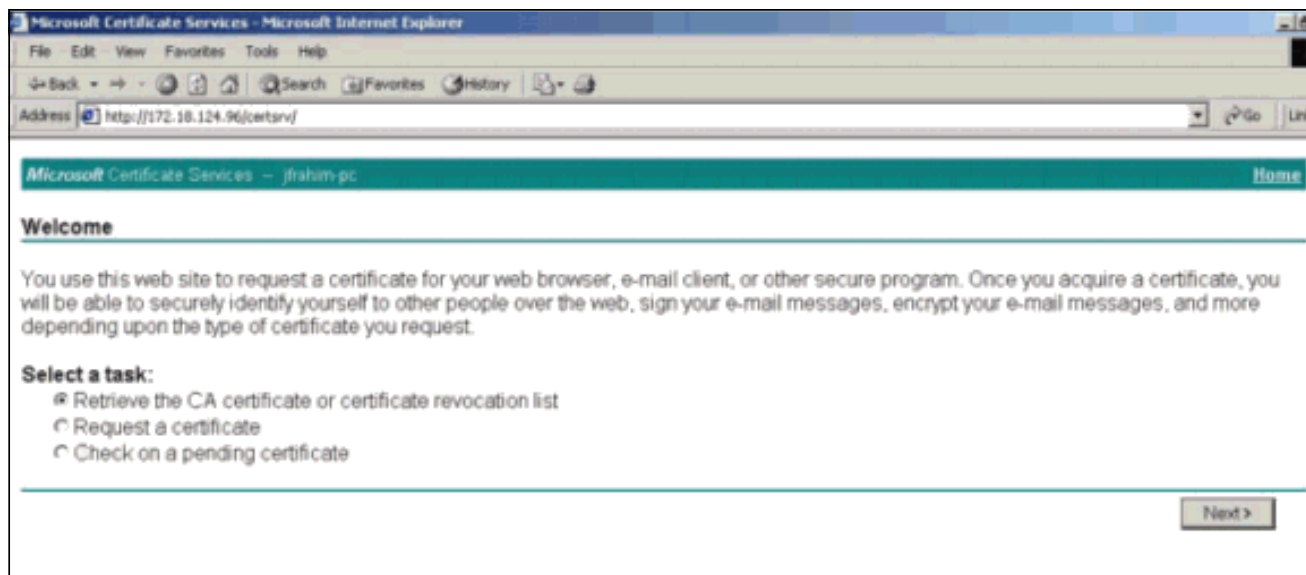
11. Selezionare **Codificato Base 64** e fare clic su **Scarica certificato CA** sul server CA.



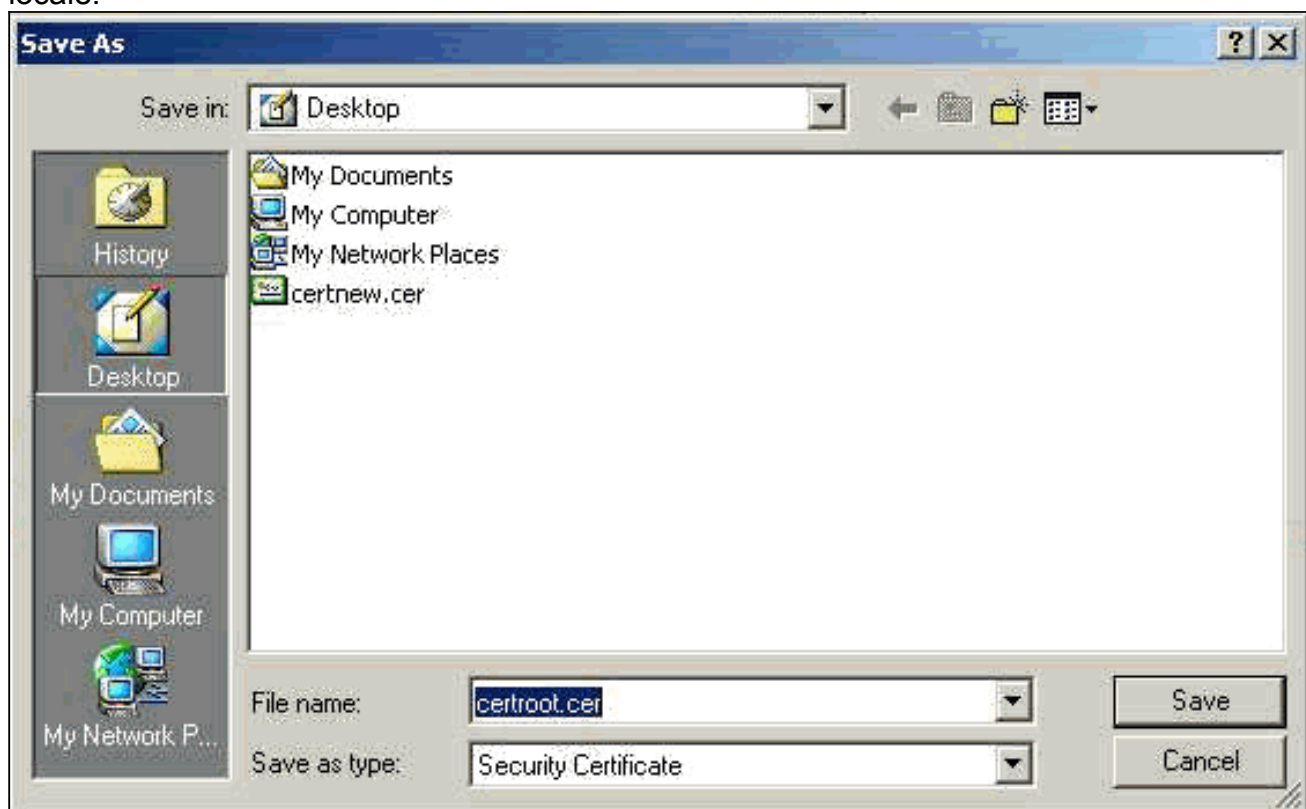
12. Salvare il certificato di identità nell'unità locale.



13. Sul server CA selezionare **Recupera il certificato CA** o **l'elenco di revoche di certificati** per ottenere il certificato radice. Quindi fare clic su **Avanti**.



14. Salvare il certificato radice nell'unità locale.



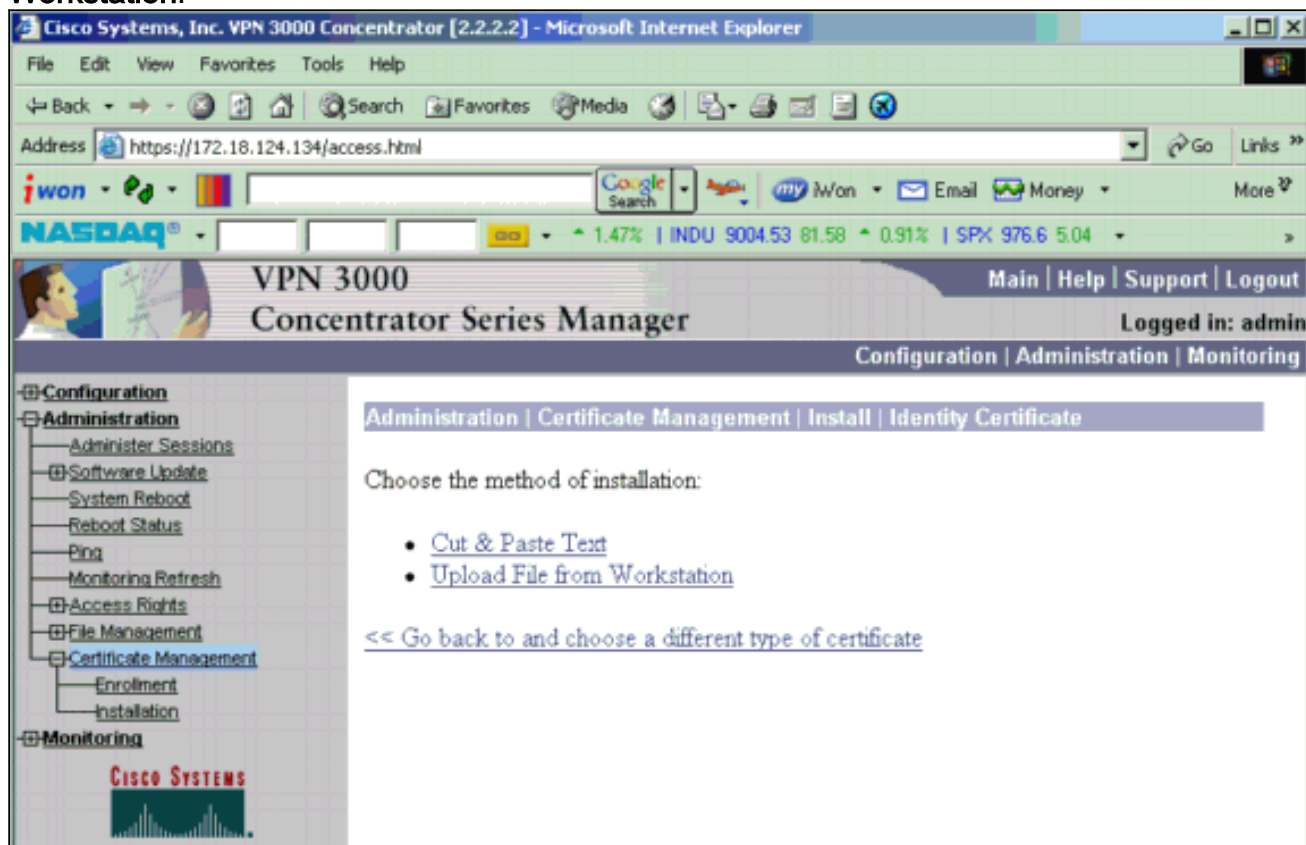
15. Installare i certificati radice e di identità nel concentratore VPN 3000. A tale scopo, selezionare **Amministrazione > Gestione certificati > Installazione > Installa il certificato ottenuto mediante la registrazione**. In Stato registrazione fare clic su **Installa**.



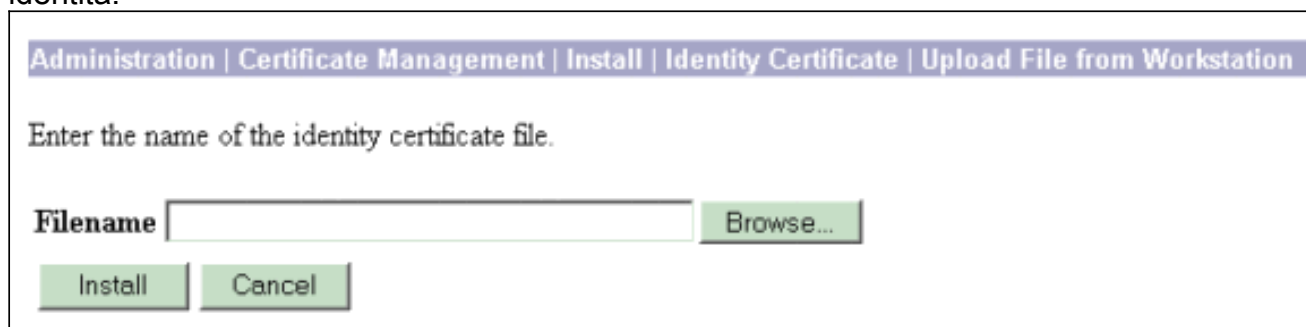
16. Fare clic su **Upload File from**



## Workstation.



17. Fare clic su **Sfogliare** e selezionare il file del certificato radice salvato nell'unità locale. Selezionare **Installa** per installare il certificato di identità nel concentratore VPN. Amministrazione | La finestra Gestione certificati viene visualizzata come conferma e il nuovo certificato di identità viene visualizzato nella tabella Certificati di identità.



**Nota:** completare la procedura seguente per generare un nuovo certificato in caso di errore del certificato. Selezionare **Amministrazione > Gestione certificati**. Fare clic su **Elimina** nella casella Azioni relativa all'elenco dei certificati SSL. Selezionare **Amministrazione > Riavvio del sistema**. Selezionare **Save the active configuration at time of reboot**, scegliere **Now** (Salva la configurazione attiva al momento del riavvio), quindi fare clic su **Apply (Applica)**. È ora possibile generare un nuovo certificato al termine del ricaricamento.

## [Installare i certificati SSL sul concentratore VPN](#)

Se si utilizza una connessione protetta tra il browser e VPN Concentrator, VPN Concentrator richiede un certificato SSL. È inoltre necessario un certificato SSL sull'interfaccia utilizzata per gestire il concentratore VPN e per WebVPN, nonché per ogni interfaccia che termina i tunnel WebVPN.

I certificati SSL dell'interfaccia, se inesistenti, vengono generati automaticamente quando VPN 3000 Concentrator viene riavviato dopo l'aggiornamento del software VPN 3000 Concentrator. Poiché un certificato autofirmato è generato automaticamente, non è verificabile. Nessuna autorità di certificazione ha garantito la propria identità. Tuttavia, questo certificato consente di stabilire un contatto iniziale con il concentratore VPN utilizzando il browser. Se si desidera sostituirlo con un altro certificato SSL autofirmato, eseguire la procedura seguente:

1. Scegliere **Amministrazione > Gestione certificati**.

The screenshot shows the 'Administration | Certificate Management' page. It includes a navigation bar with the date 'Monday, 05 January 2004 16:31:1' and a 'Refresh' button. The main content area contains several sections:

- Certificate Authorities**: A table with columns for Subject, Issuer, Expiration, SCEP Issuer, and Actions. One entry is shown: 'ms-root-sha-06-2001 at cisco'.
- Identity Certificates**: A table with columns for Subject, Issuer, Expiration, and Actions. One entry is shown: 'Gateway A at Cisco Systems'.
- SSL Certificates**: A table with columns for Interface, Subject, Issuer, Expiration, and Actions. One entry is shown for the 'Private' interface. The 'Generate' button in the Actions column is circled in red.
- SSH Host Key**: A table with columns for Key Size, Key Type, Date Generated, and Actions. One entry is shown: '1024 bits' RSA key generated on '01/05/2004'.

2. Per visualizzare il nuovo certificato nella tabella Certificato SSL e sostituire quello esistente, fare clic su **Genera**. Questa finestra consente di configurare i campi per i certificati SSL generati automaticamente da Concentrator VPN. Questi certificati SSL sono destinati alle interfacce e al bilanciamento del carico.

The screenshot shows the 'Administration | Certificate Management | Generate SSL Certificate' window. It contains the following information and fields:

- Text: 'You are about to generate a certificate for the Public Interface. The certificate will have the following DN for both Subject and Issuer.'
- Text: 'The certificate will be valid for 3 years from yesterday.'
- Form fields for DN configuration:
  - Common Name (CN): 10.86.194.175
  - Organizational Unit (OU): VPN 3000 Concentrator
  - Organization (O): Cisco Systems, Inc.
  - Locality (L): Franklin
  - State/Province (SP): Massachusetts
  - Country (C): US
  - RSA Key Size: 1024-bits (dropdown menu)
- Buttons: 'Generate' and 'Cancel'.

Se si desidera ottenere un certificato SSL verificabile, ovvero un certificato rilasciato da un'Autorità di certificazione, vedere la sezione [Installazione dei certificati digitali sul concentratore VPN](#) in questo documento per utilizzare la stessa procedura utilizzata per

ottenere i certificati di identità. In questo caso, nella finestra **Amministrazione > Gestione certificati > Registrazione** fare clic su **Certificato SSL** (anziché su Certificato di identità). **Nota:** consultare la sezione *Amministrazione / Sezione Certificate Management* di [VPN 3000 Concentrator Reference Volume II: Administration and Monitoring Release 4.7](#) per informazioni complete sui certificati digitali e i certificati SSL.

## Rinnova certificati SSL sul concentratore VPN

In questa sezione viene descritto come rinnovare i certificati SSL:

Se si tratta del certificato SSL generato dal concentratore VPN, passare alla sezione **Amministrazione > Gestione certificati** su SSL. Fare clic sull'opzione **renew** per rinnovare il certificato SSL.

Se si tratta di un certificato concesso da un server CA esterno, attenersi alla seguente procedura:

1. Per eliminare i certificati scaduti dall'interfaccia pubblica, scegliere **Amministrazione > Gestione certificati > Elimina** in *Certificati SSL*.

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	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>

**Identity Certificates** (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
<b>No Identity Certificates</b>			

**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	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut... at Equifax	08/16/2008	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>



Fare clic su **Sì** per confermare l'eliminazione del certificato SSL.

**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.crl

Are you **sure** you want to delete this certificate?

2. Per generare il nuovo certificato SSL, scegliere **Amministrazione > Gestione certificati > Genera**.

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	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>

**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	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>
Public	No Certificate Installed.			<a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>



Verrà visualizzato il nuovo certificato SSL per l'interfaccia pubblica.

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	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>

**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	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">Generate</a>   <a href="#">Enroll</a>   <a href="#">Import</a>

## [Informazioni correlate](#)

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Negoziazione IPSec/protocolli IKE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)