Konfigurieren des Cisco VPN 300 Concentrator 4.7.x zum Abrufen eines digitalen Zertifikats und eines SSL-Zertifikats

Inhalt

Einführung

Dieses Dokument enthält schrittweise Anweisungen zur Konfiguration der Cisco VPN Concentrators der Serie 3000 für die Authentifizierung mithilfe von digitalen Zertifikaten oder Identitätszertifikaten und SSL-Zertifikaten.

Hinweis: Im VPN-Concentrator muss der Lastenausgleich deaktiviert werden, bevor Sie ein weiteres SSL-Zertifikat generieren, da dies die Zertifikatgenerierung verhindert.

Weitere Informationen zum Szenario mit PIX/ASA 7.x finden Sie unter So erhalten Sie ein digitales Zertifikat von einer Microsoft Windows CA mithilfe von ASDM auf einer ASA.

Weitere Informationen zum Szenario mit Cisco IOS®-Plattformen finden Sie im Konfigurationsbeispiel für die Cisco IOS-Zertifikatsregistrierung unter Verwendung erweiterter Anmeldebefehle.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco VPN 3000 Concentrator, auf dem Version 4.7 ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

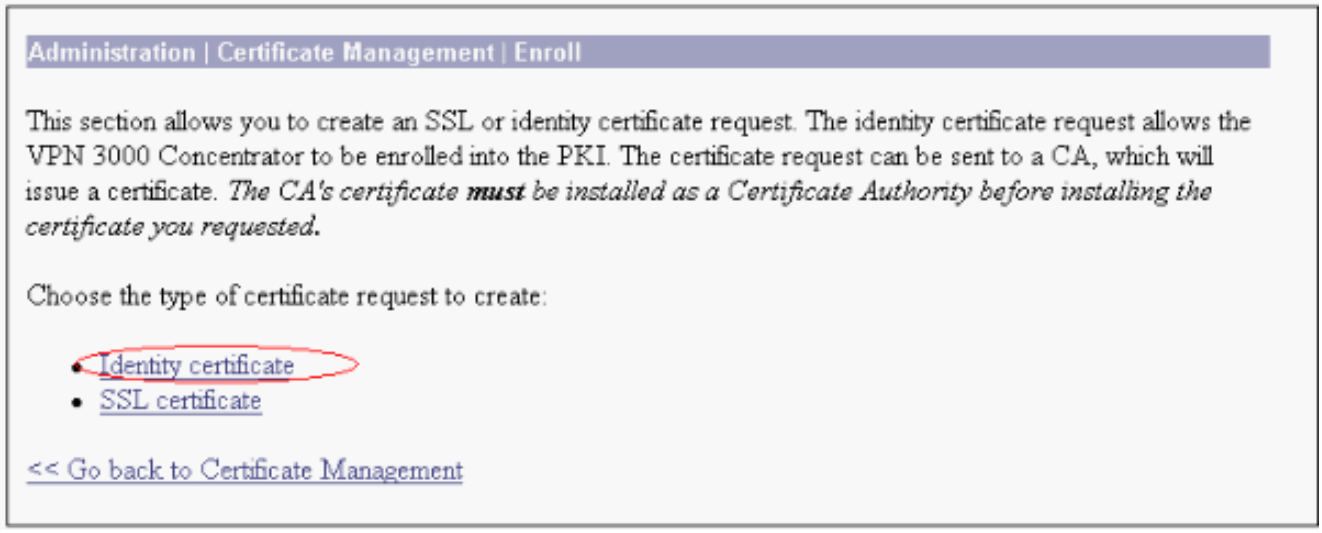
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

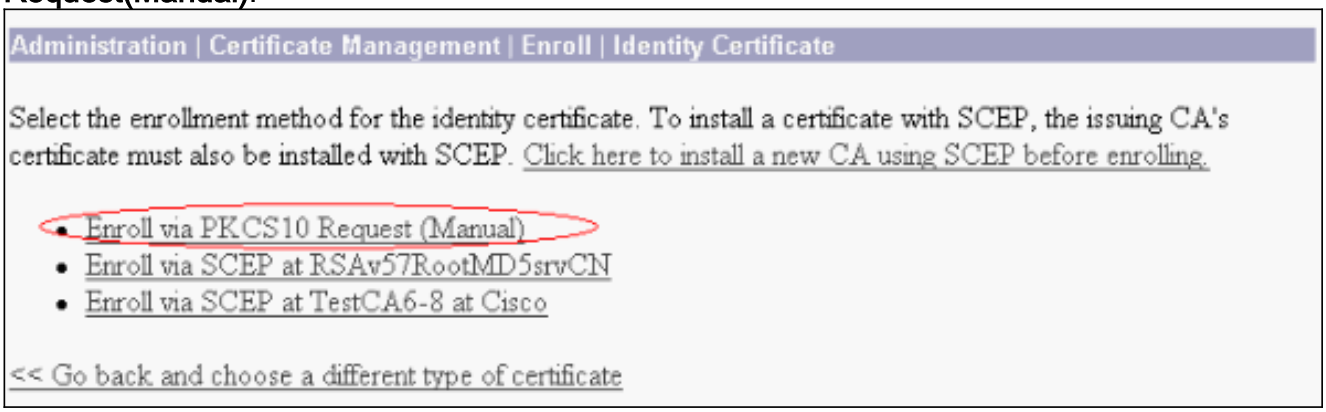
Installieren digitaler Zertifikate im VPN-Konzentrator

Gehen Sie wie folgt vor:

1. Wählen Sie **Administration > Certificate Management > Enroll (Verwaltung > Zertifikatsverwaltung > Anmeldung) aus,** um die Anforderung eines digitalen Zertifikats oder eines Identitätszertifikats auszuwählen.

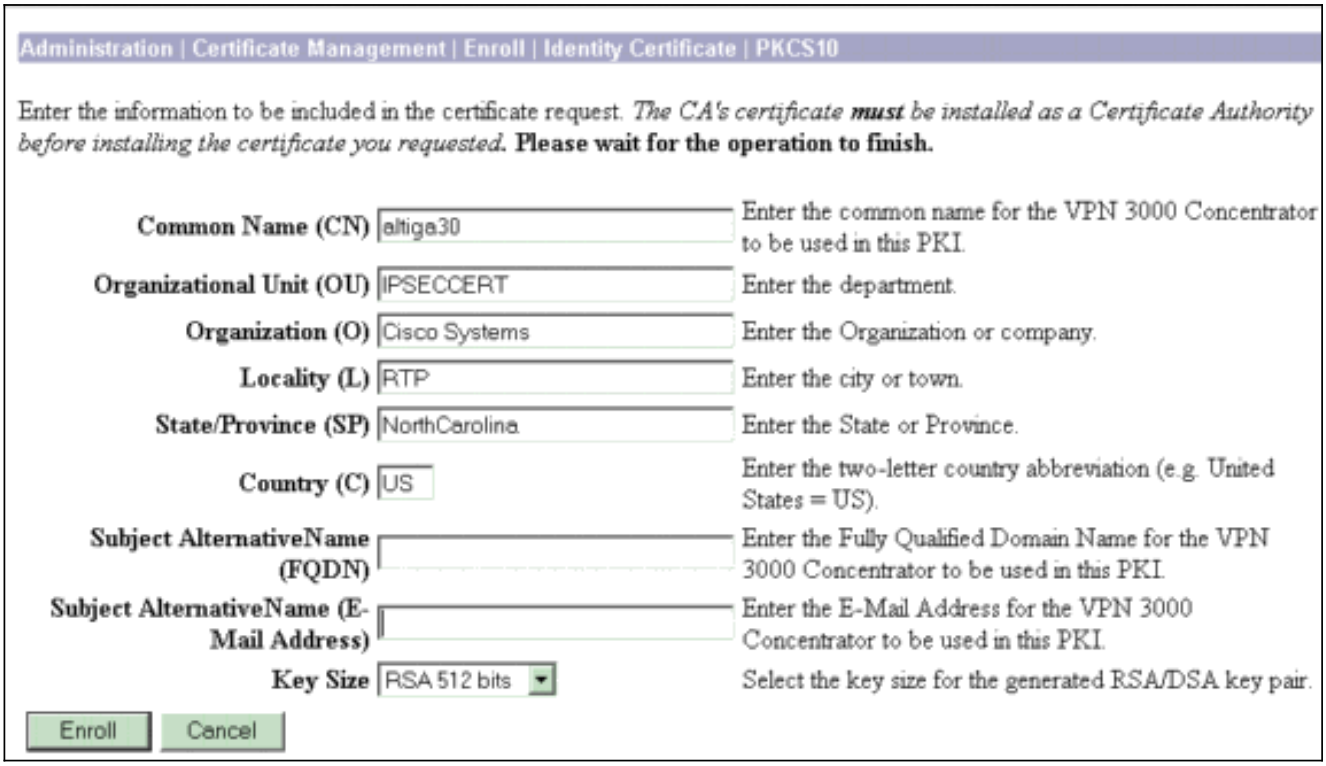


2. Wählen Sie **Administration > Certificate Management > Enrollment > Identity Certificate aus,** und klicken Sie auf **Registrieren über PKCS10 Request(Manual)**.

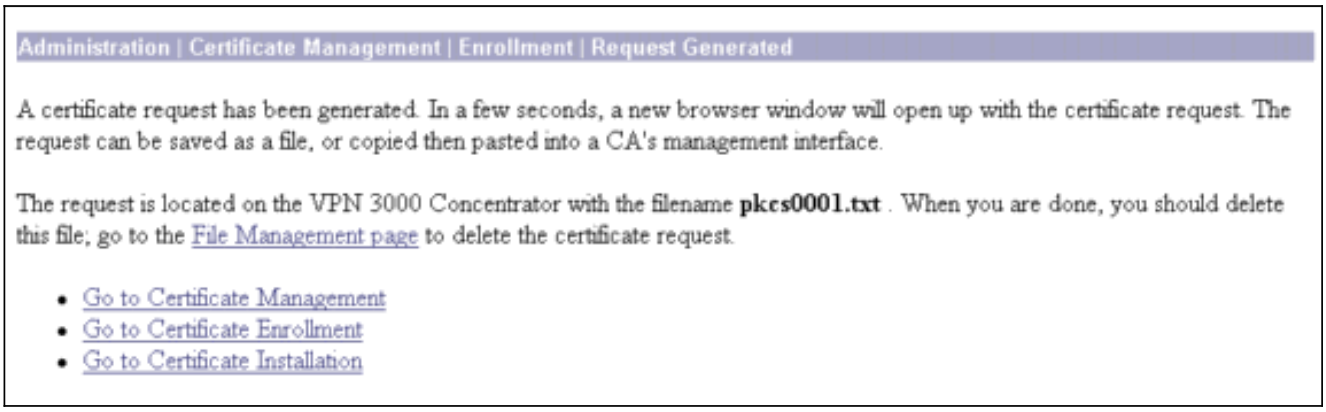


3. Füllen Sie die erforderlichen Felder aus, und klicken Sie dann auf **Registrieren**.Diese Felder sind in diesem Beispiel ausgefüllt.**Common Name** - Altiga30**Organisationseinheit** - IPSECCERT (die Organisationseinheit muss mit dem konfigurierten IPsec-Gruppennamen übereinstimmen)**Organisation** - Cisco Systems**Lokalität** - RTP**Bundesland** - NorthCarolina**Land** - USA**Vollqualifizierter Domänenname** - (hier nicht

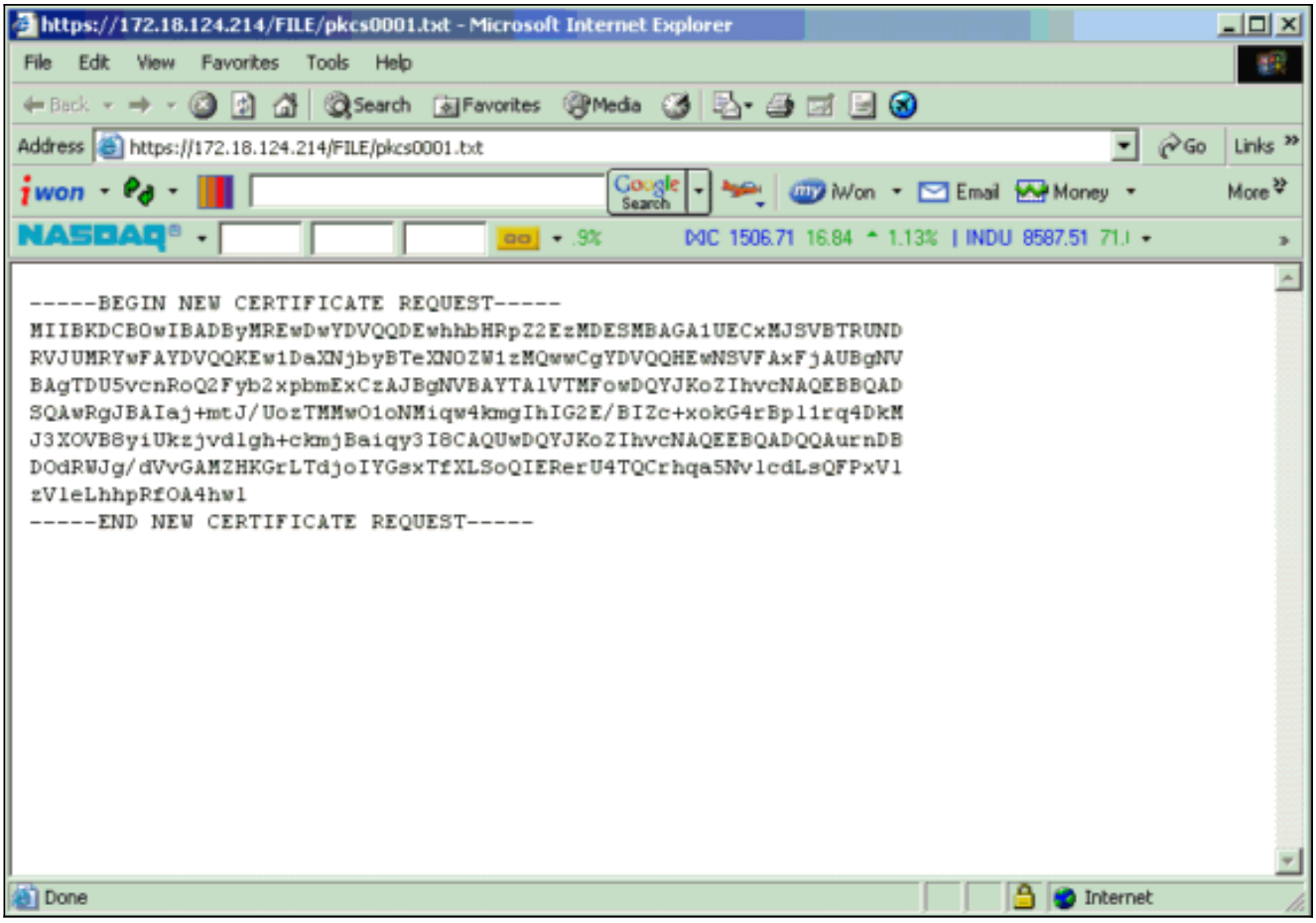
verwendet)**Schlüsselgröße** - 512**Hinweis:** Wenn Sie über Simple Certificate Enrollment Protocol (SCEP) ein SSL-Zertifikat oder ein Identitätszertifikat anfordern, sind dies die einzigen verfügbaren RSA-Optionen.RSA 512 BitRSA 768 BitRSA 1024 BitRSA 2048 BitDSA 512 BitDSA 768 BitDSA 1024
Bit



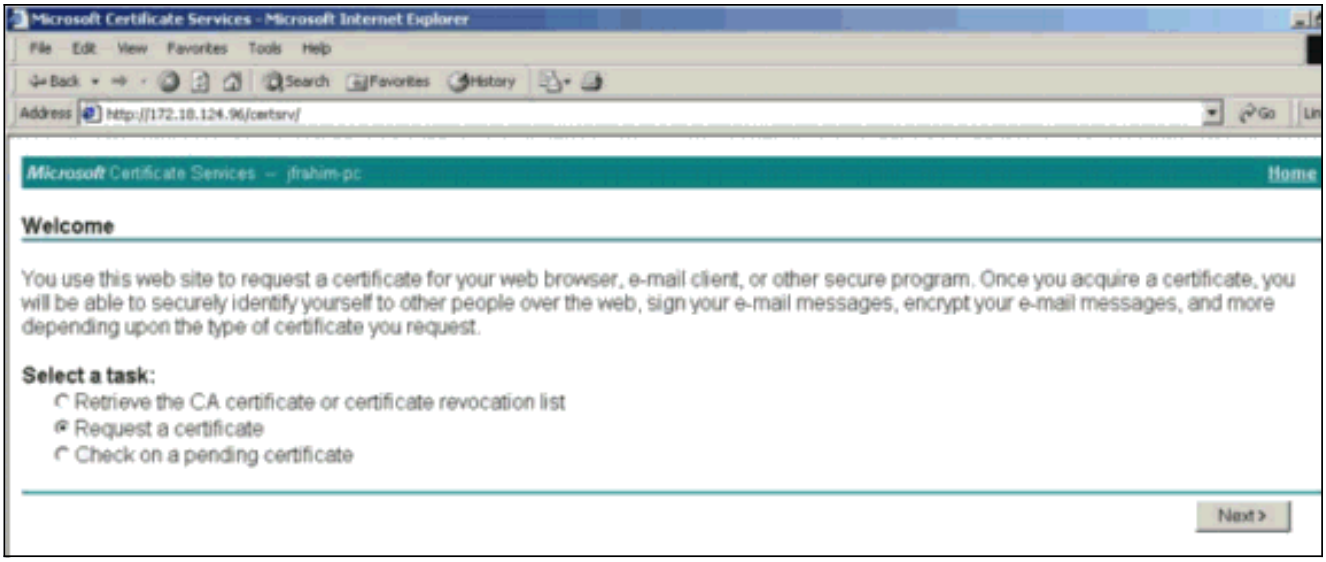
4. Nachdem Sie auf **Registrieren** geklickt haben, werden mehrere Fenster angezeigt. Im ersten Fenster wird bestätigt, dass Sie ein Zertifikat angefordert haben.



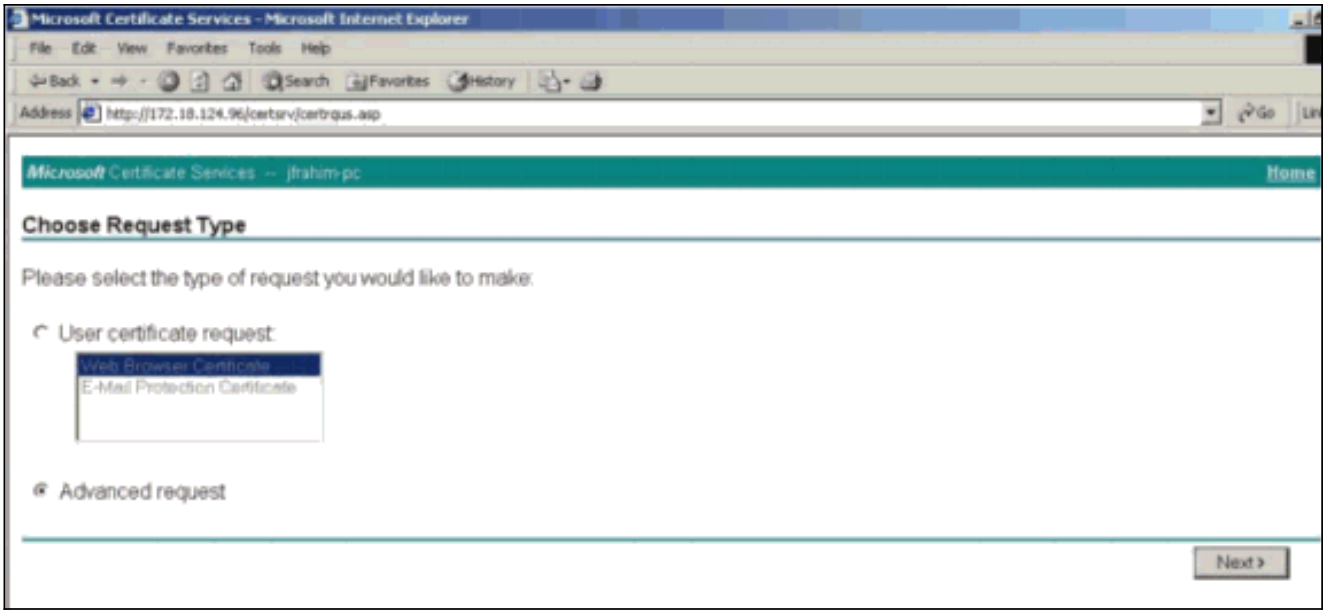
Ein neues Browserfenster wird ebenfalls geöffnet und zeigt die PKCS-Anforderungsdatei an.



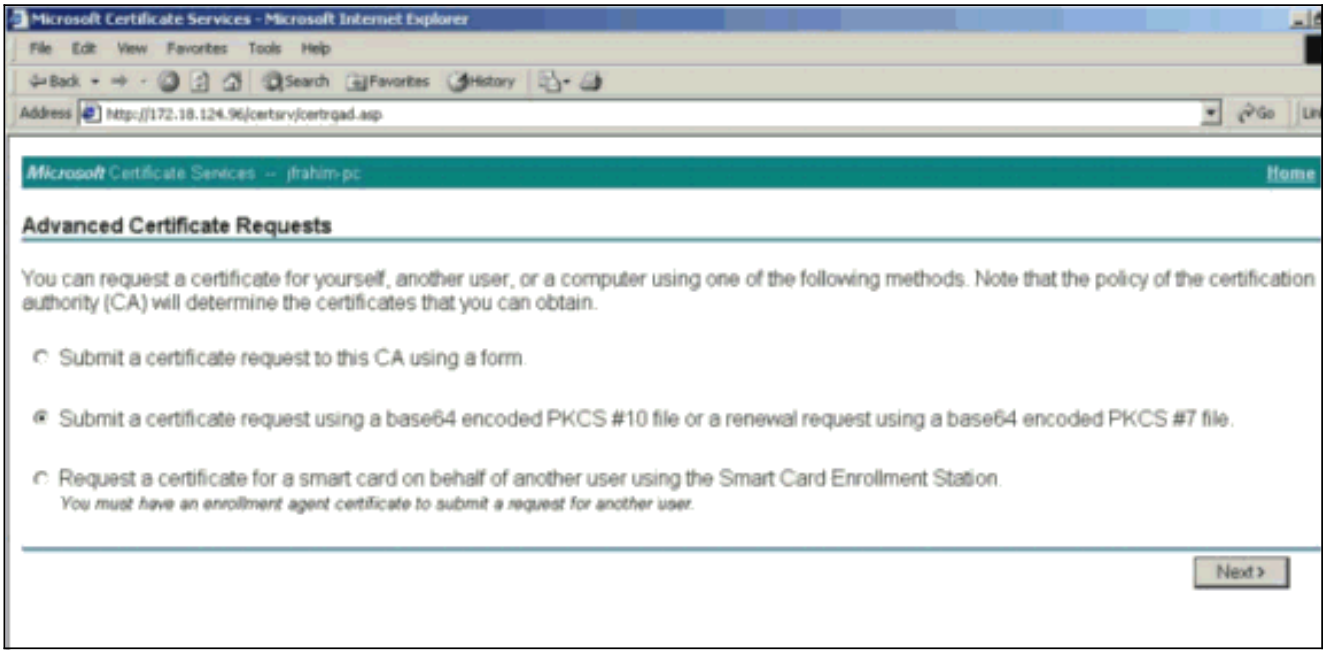
5. Markieren Sie auf Ihrem Zertifizierungsstellen-Server die Anforderung, und fügen Sie sie in Ihren CA-Server ein, um Ihre Anfrage zu senden. Klicken Sie auf **Weiter**.



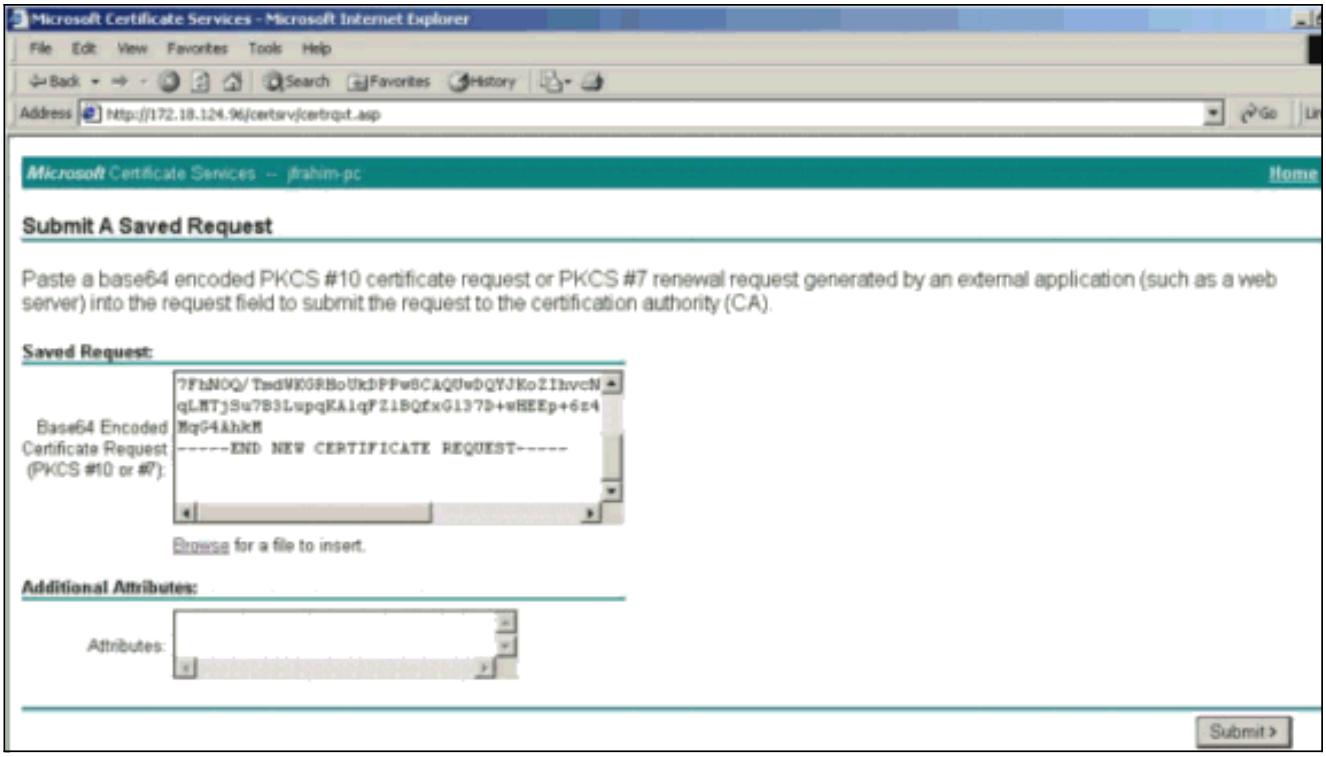
6. Wählen Sie **Erweiterte Anforderung** aus, und klicken Sie auf **Weiter**.



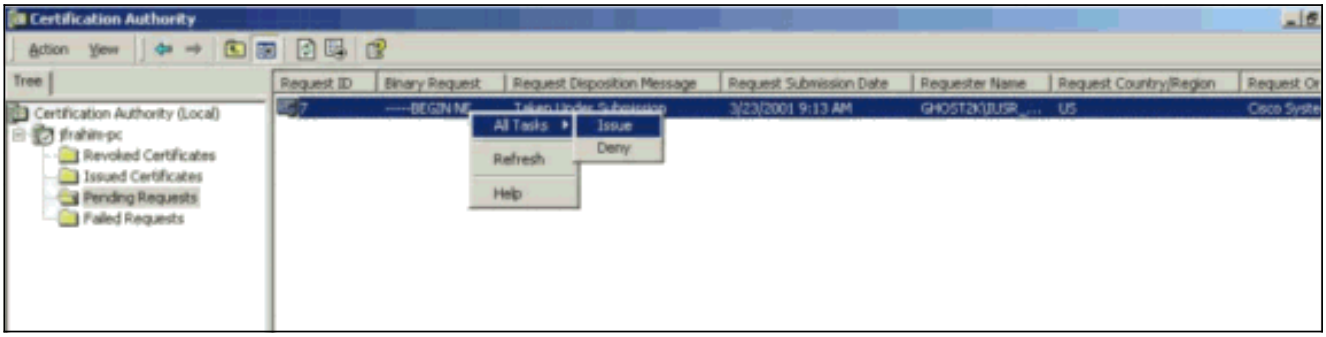
7. Wählen Sie **eine Zertifikatsanforderung mit einer Base64-kodierten PKCS #10-Datei oder eine Verlängerungsanfrage mit einer Base64-kodierten PKCS #7-Datei einreichen aus**, und klicken Sie dann auf **Weiter**.



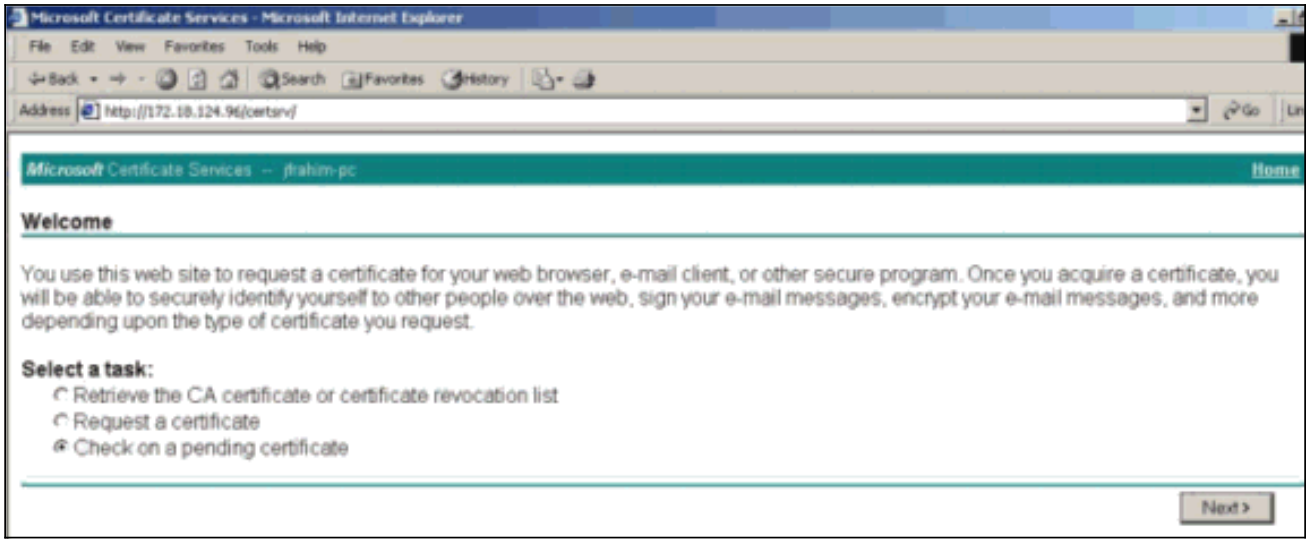
8. Schneiden Sie Ihre PKCS-Datei aus, und fügen Sie sie im Abschnitt "Gespeicherte Anforderung" in das Textfeld ein. Klicken Sie anschließend auf **Senden**.



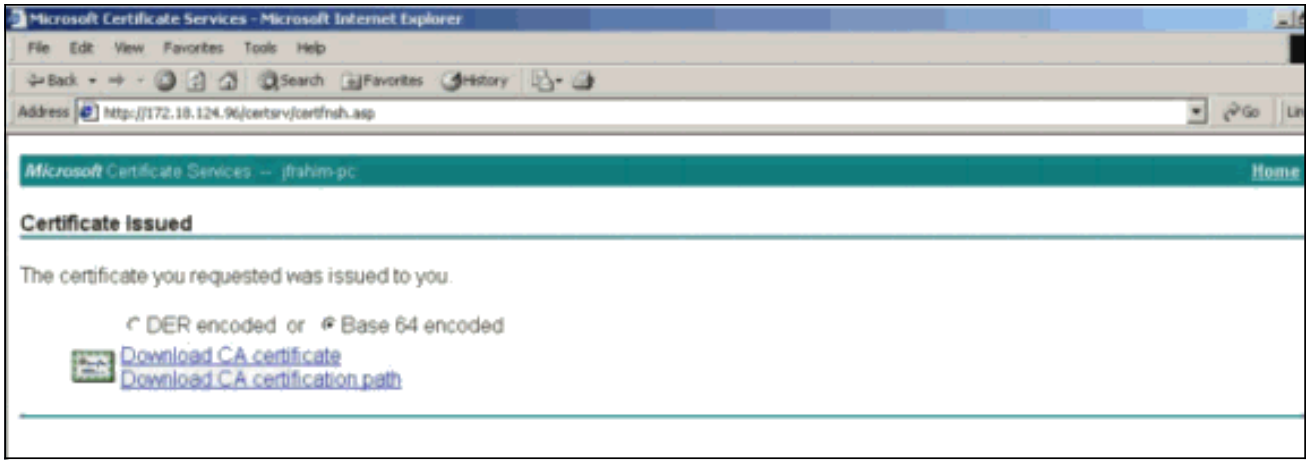
9. Stellen Sie das Identitätszertifikat auf dem CA-Server aus.



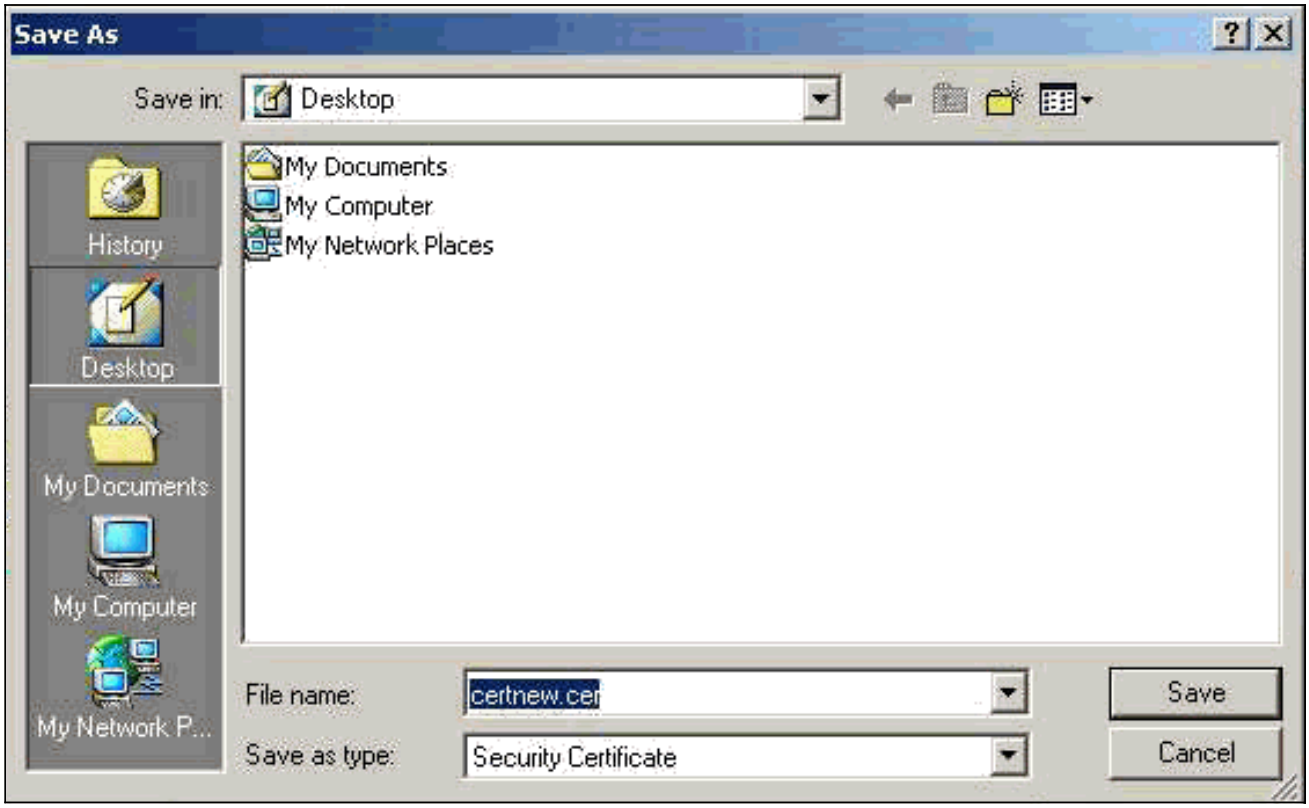
10. Laden Sie den Stamm und die Identitätszertifikate herunter. Wählen Sie auf Ihrem CA-Server **auf ein ausstehendes Zertifikat prüfen aus**, und klicken Sie auf **Weiter**.



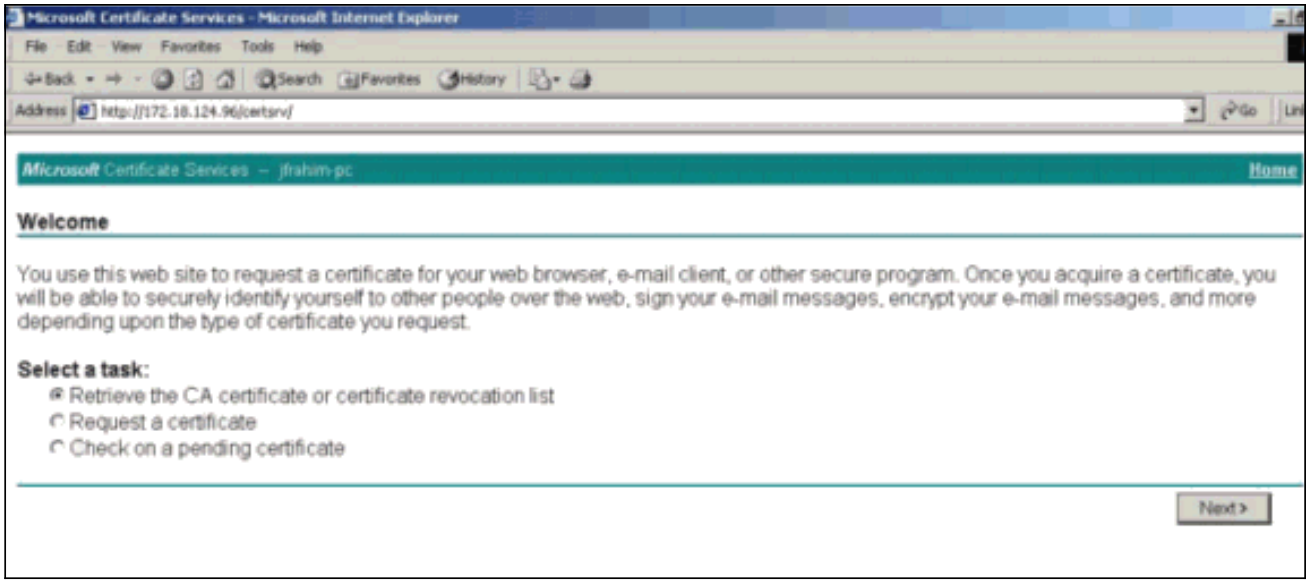
11. Wählen Sie **Base 64-verschlüsselt aus**, und klicken Sie auf **CA-Zertifikat** auf dem CA-Server **herunterladen**.



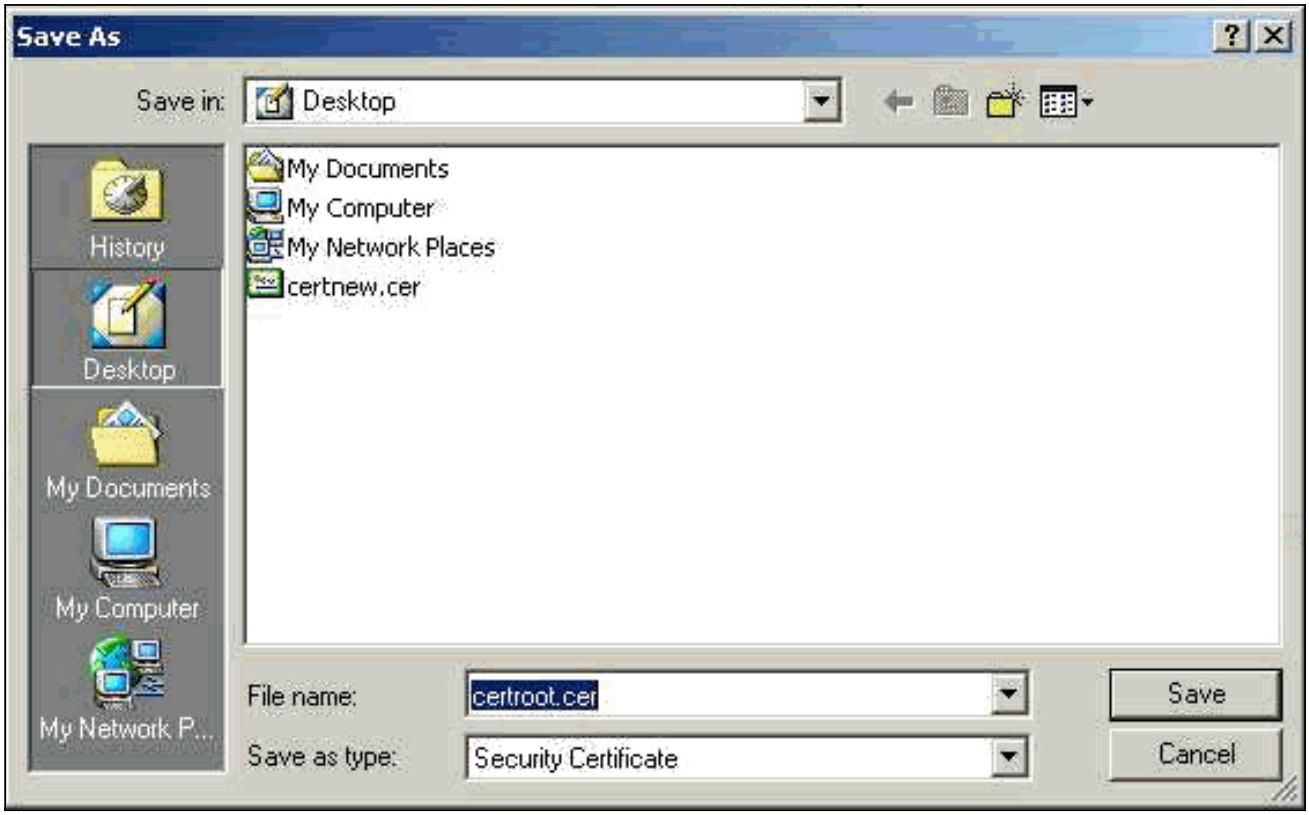
12. Speichern Sie das Identitätszertifikat auf Ihrem lokalen Laufwerk.



13. Wählen Sie auf dem CA-Server **Zertifikat oder Zertifikatswiderrufliste abrufen aus**, um das Stammzertifikat abzurufen. Klicken Sie anschließend auf **Weiter**.

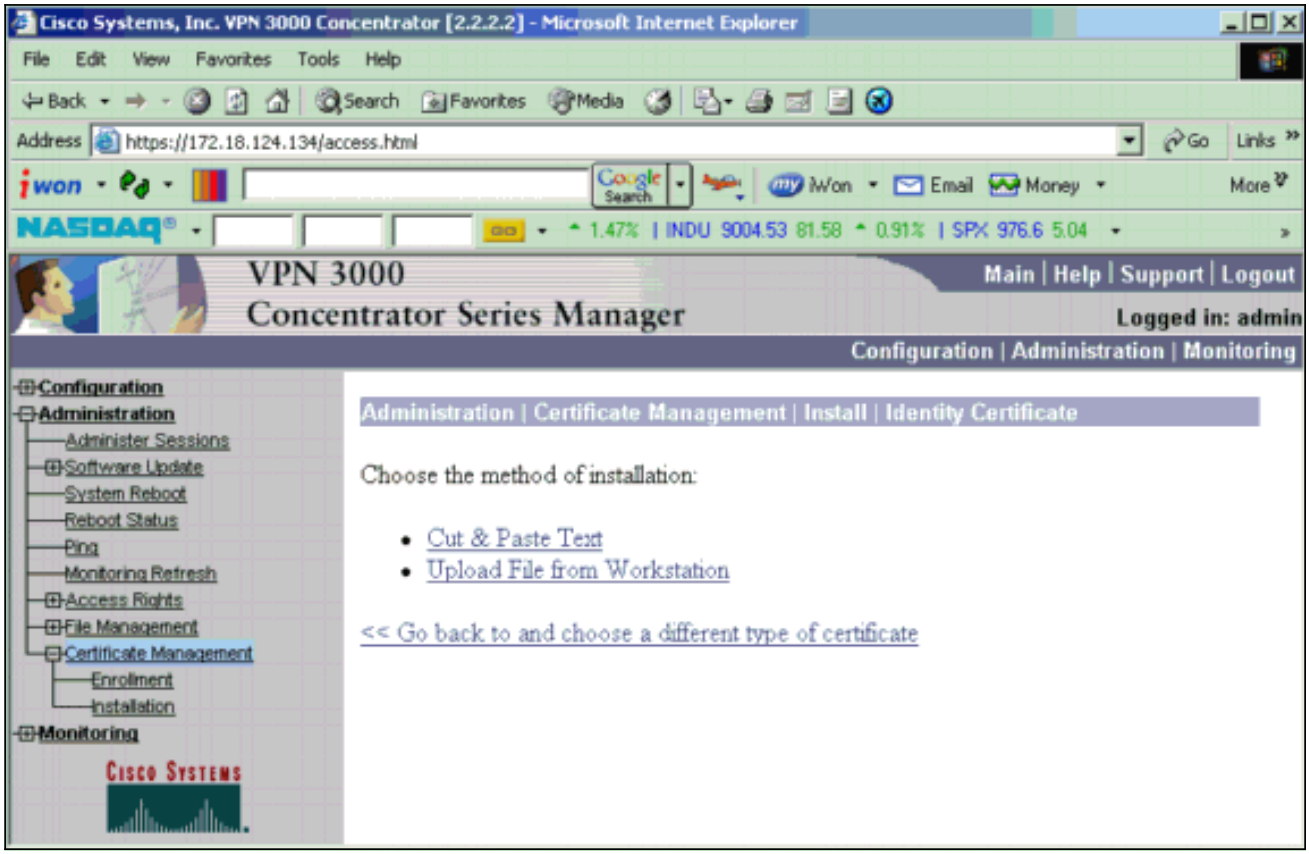


14. Speichern Sie das Stammzertifikat auf Ihrem lokalen Laufwerk.

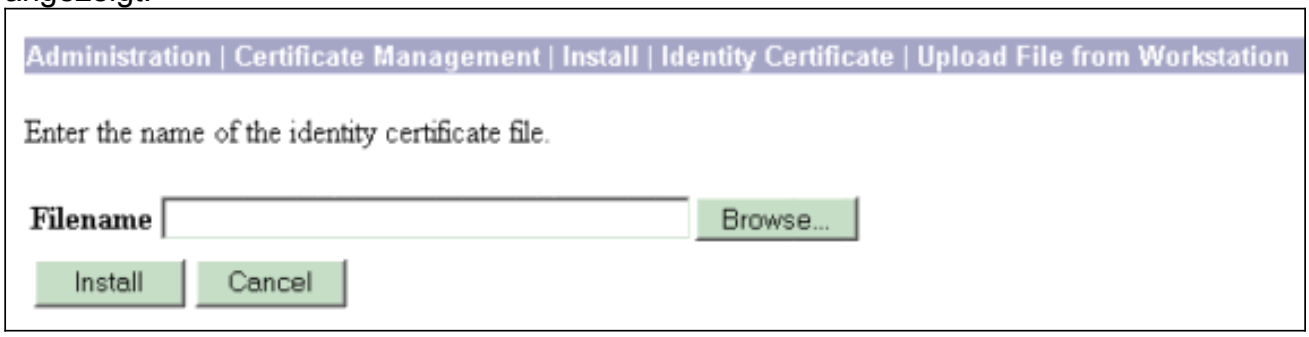


15. Installieren Sie die Root- und Identitätszertifikate im VPN 3000 Concentrator. Wählen Sie dazu **Administration > Certificate Manager > Installation > Install certificate created by enrollment (Verwaltung > Zertifikatsmanager > Installation > Installationszertifikat) aus**. Klicken Sie unter "Registrierungsstatus" auf **Installieren**.

16. Klicken Sie auf **Datei von Workstation hochladen**.



17. Klicken Sie auf **Durchsuchen** und wählen Sie die Stammzertifikatdatei aus, die Sie auf dem lokalen Laufwerk gespeichert haben.Wählen Sie **Install** aus, um das Identitätszertifikat auf dem VPN Concentrator zu installieren. Die Verwaltung | Das Fenster Certificate Management (Zertifikatsverwaltung) wird als Bestätigung angezeigt, und Ihr neues Identitätszertifikat wird in der Tabelle Identity Certificates (Identitätszertifikate) angezeigt.



Hinweis: Gehen Sie wie folgt vor, um ein neues Zertifikat zu generieren, wenn das Zertifikat fehlschlägt.Wählen Sie **Administration > Certificate Management aus**.Klicken Sie in der Liste SSL-Zertifikat im Feld Aktionen auf **Löschen**.Wählen Sie **Administration > System Reboot aus**.Wählen Sie **die aktive Konfiguration zum Zeitpunkt des Neustarts speichern aus**, wählen Sie **Jetzt** aus, und klicken Sie auf **Übernehmen**. Nach dem erneuten Laden können Sie jetzt ein neues Zertifikat generieren.

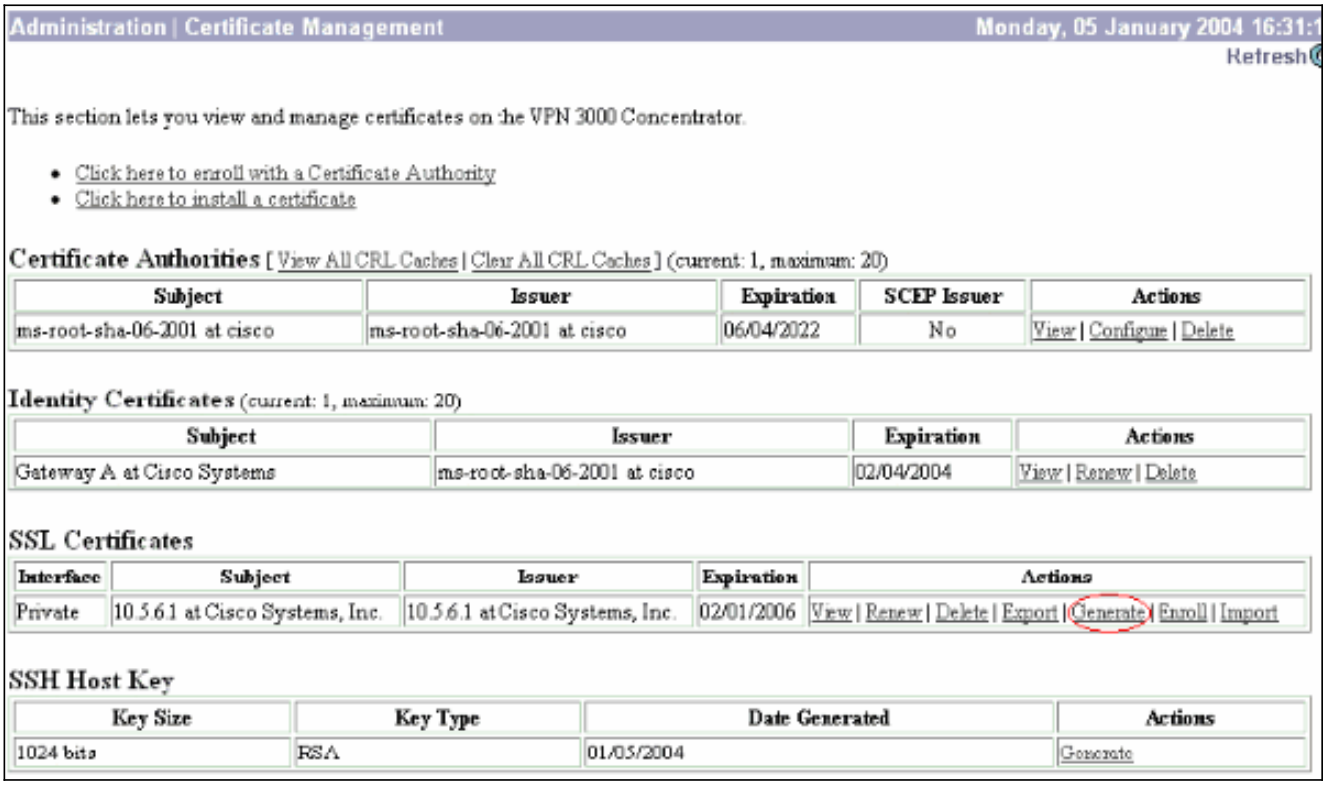
Installieren von SSL-Zertifikaten im VPN Concentrator

Wenn Sie eine sichere Verbindung zwischen Ihrem Browser und dem VPN Concentrator verwenden, benötigt der VPN Concentrator ein SSL-Zertifikat. Sie benötigen außerdem ein SSL-Zertifikat für die Schnittstelle, die Sie zum Verwalten des VPN Concentrator und für WebVPN

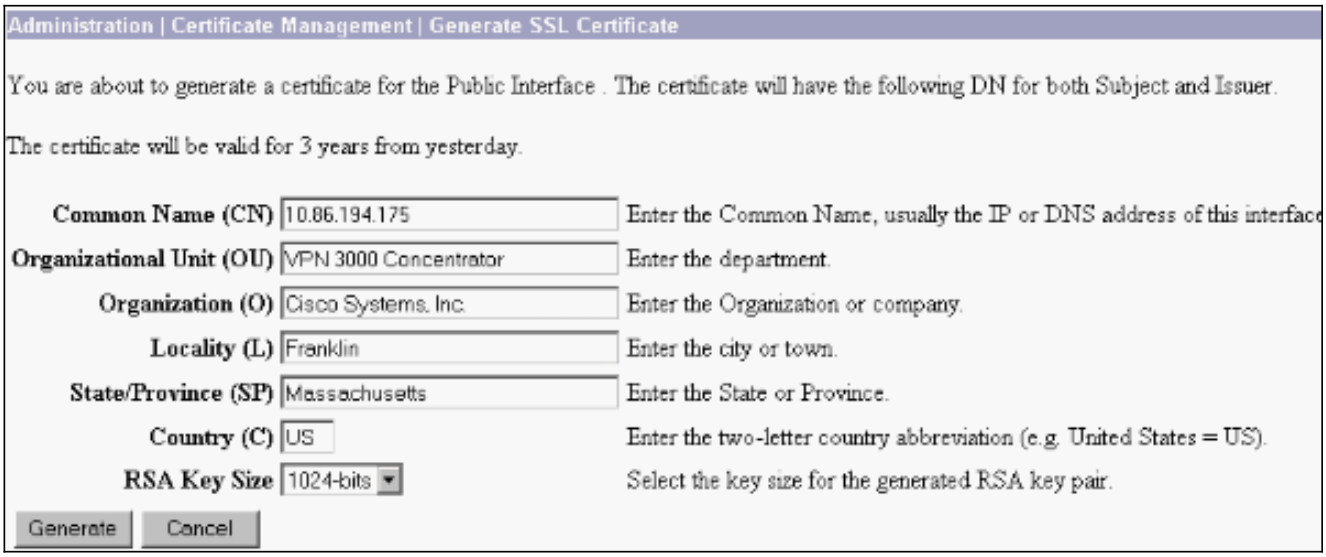
verwenden, sowie für jede Schnittstelle, die WebVPN-Tunnel terminiert.

Die SSL-Schnittstellenzertifikate (sofern nicht vorhanden) werden automatisch generiert, wenn der VPN 3000 Concentrator nach dem Aktualisieren der VPN 3000 Concentrator-Software neu startet. Da ein selbstsigniertes Zertifikat selbst erstellt wird, ist dieses Zertifikat nicht verifizierbar. Keine Zertifizierungsstelle hat ihre Identität garantiert. Mit diesem Zertifikat können Sie jedoch zunächst über den Browser mit dem VPN Concentrator Kontakt aufnehmen. Wenn Sie es durch ein anderes selbst signiertes SSL-Zertifikat ersetzen möchten, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Administration > Certificate Management aus**.



2. Klicken Sie auf **Generate (Generieren)**, um das neue Zertifikat in der Tabelle für das SSL-Zertifikat anzuzeigen und das vorhandene zu ersetzen.In diesem Fenster können Sie Felder für SSL-Zertifikate konfigurieren, die vom VPN Concentrator automatisch generiert werden. Diese SSL-Zertifikate sind für Schnittstellen und für den Lastenausgleich bestimmt.



Wenn Sie ein verifizierbares SSL-Zertifikat erwerben möchten (d. h. ein von einer

Zertifizierungsstelle ausgestelltes Zertifikat), lesen Sie den Abschnitt Install Digital Certificates on the VPN Concentrator (Digitale Zertifikate installieren) dieses Dokuments, um das gleiche Verfahren zum Abrufen von Identitätszertifikaten zu verwenden. Klicken Sie dieses Mal jedoch im Fenster **Administration > Certificate Management > Enroll** (**Verwaltung > Zertifikatsverwaltung > Anmeldung**) auf **SSL-Zertifikat** (anstelle von Identity Certificate).**Hinweis:** Siehe *Administration | Certificate Management*-Abschnitt des VPN 300 Concentrator-Referenzvolumens II: Administration and Monitoring Release 4.7 für vollständige Informationen über digitale Zertifikate und SSL-Zertifikate.

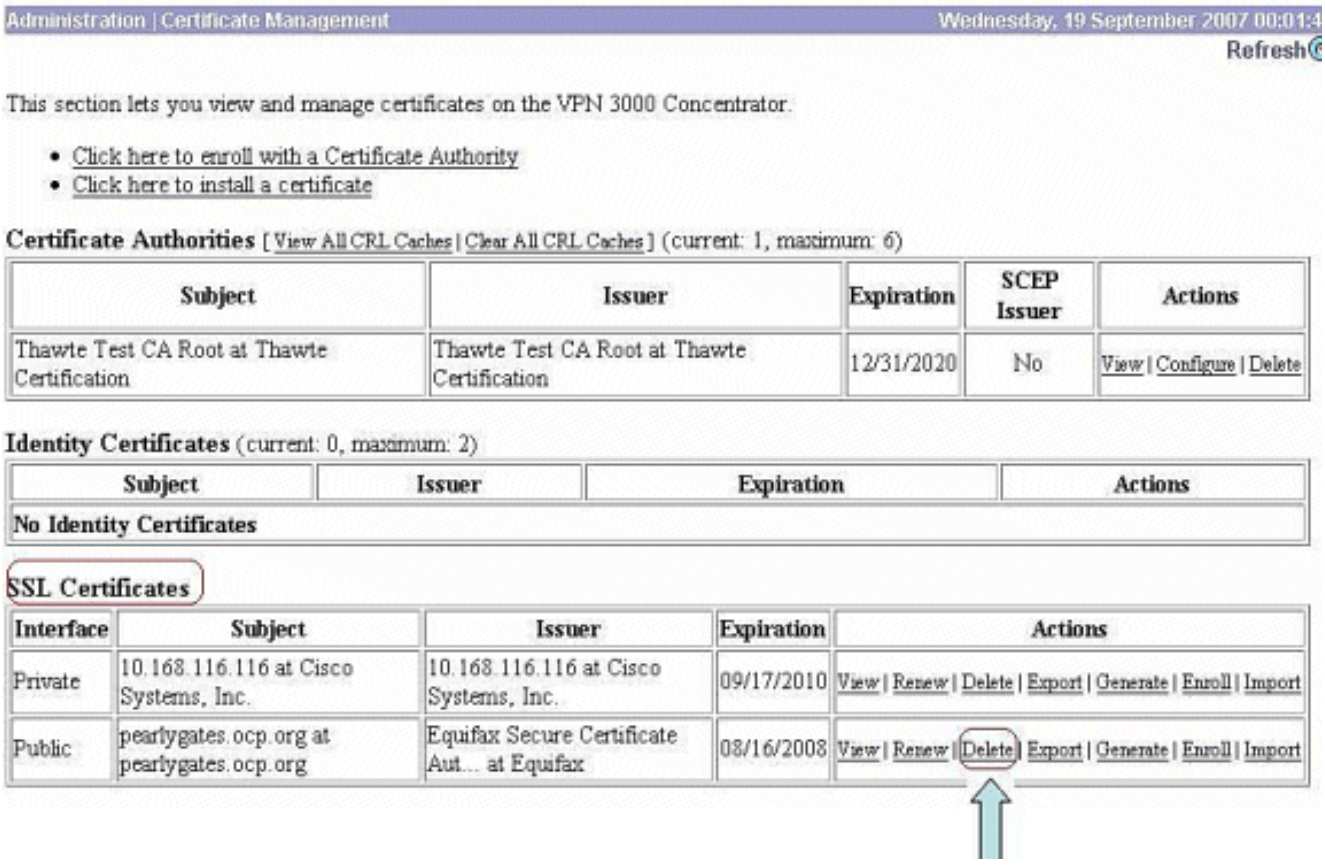
Verlängern Sie SSL-Zertifikate für den VPN Concentrator.

In diesem Abschnitt wird beschrieben, wie Sie die SSL-Zertifikate erneuern:

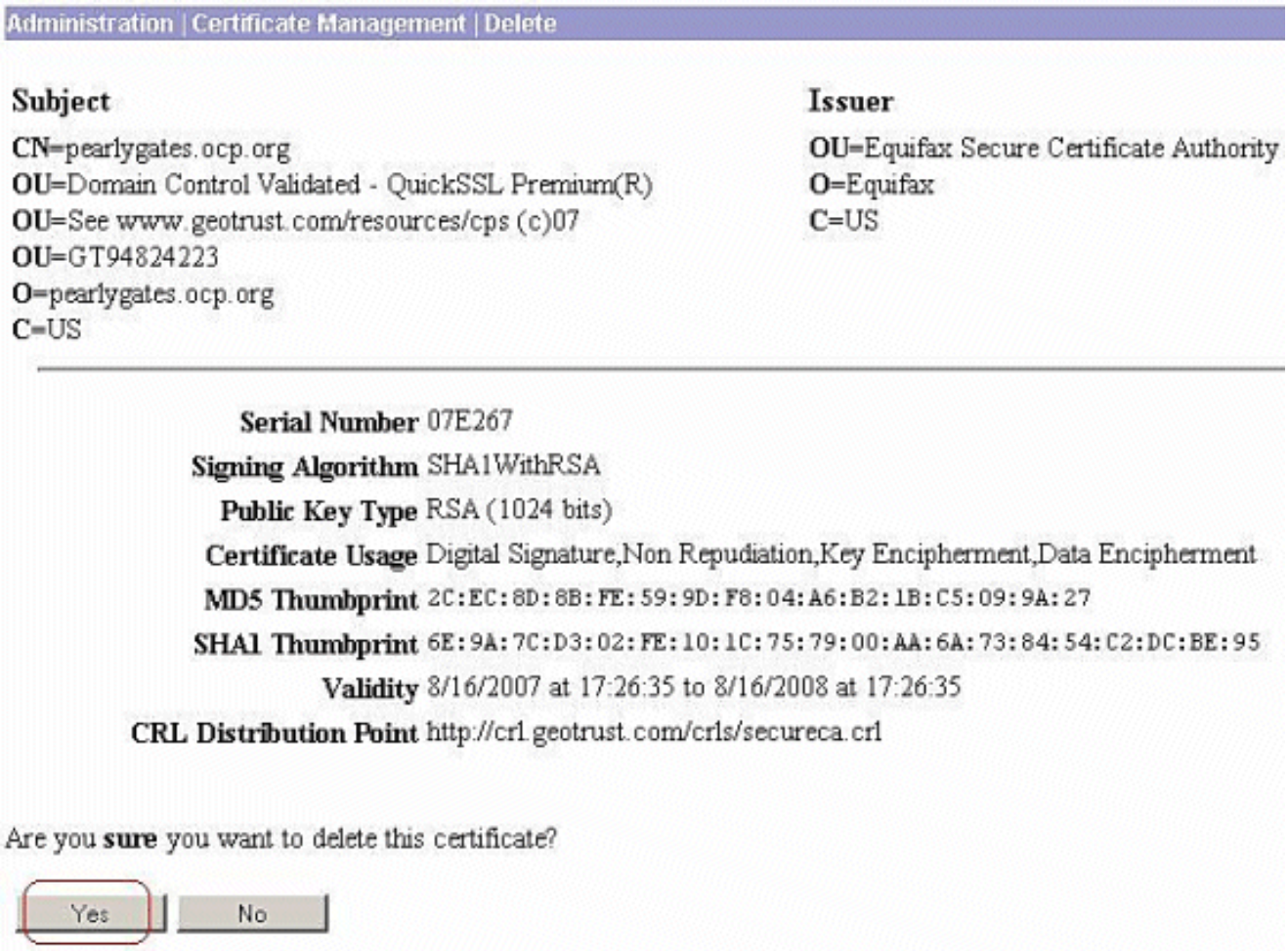
Wenn es sich um das SSL-Zertifikat handelt, das vom VPN Concentrator generiert wurde, gehen Sie im Abschnitt "SSL" zu **Administration > Certificate Management**. Klicken Sie auf die **Verlängerungsoption**, die das SSL-Zertifikat erneuert.

Wenn es sich um ein Zertifikat handelt, das von einem externen CA-Server erteilt wurde, gehen Sie wie folgt vor:

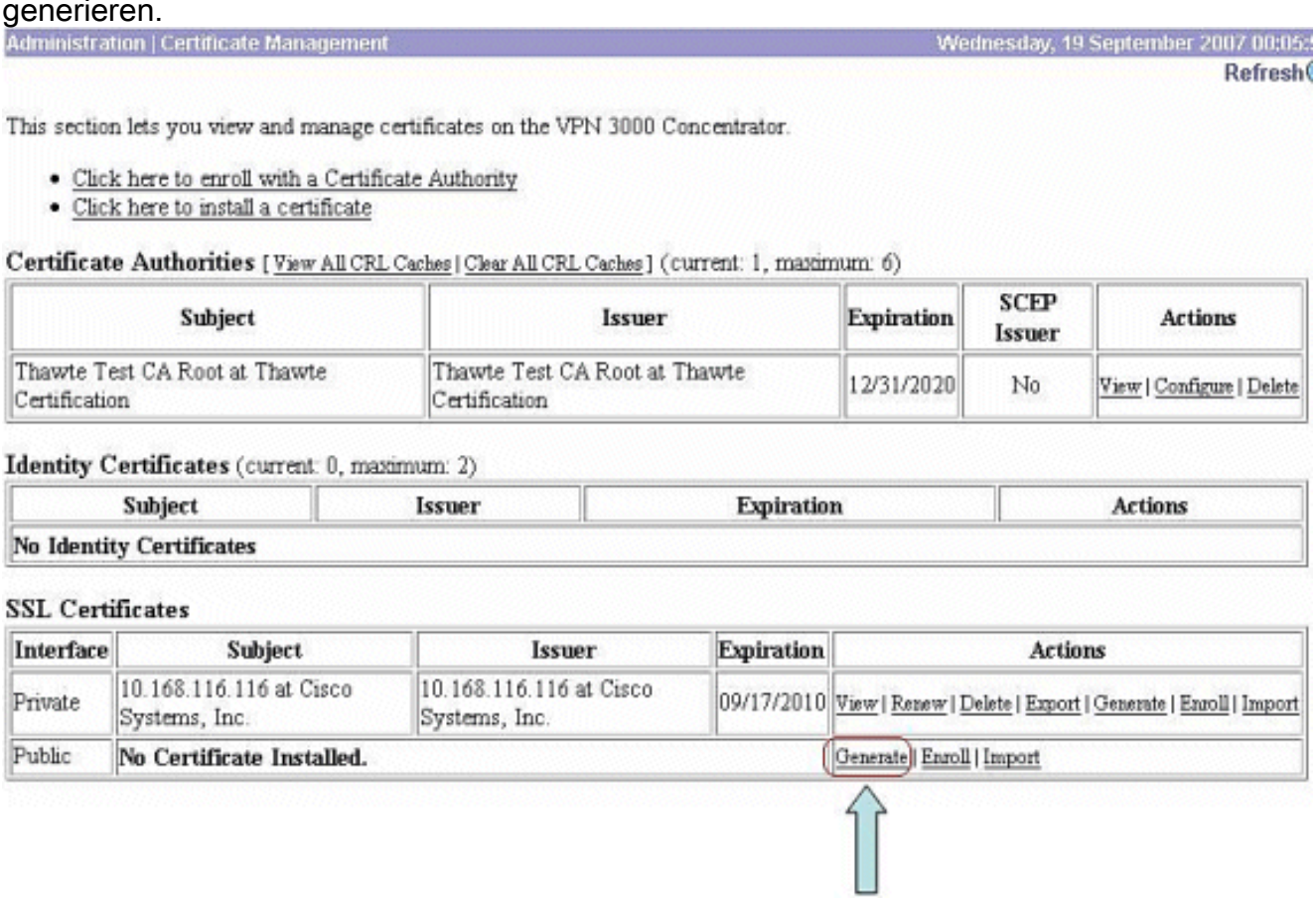
1. Wählen Sie **Administration > Certificate Management >Delete** unter *SSL Certificates aus*, um die abgelaufenen Zertifikate aus der öffentlichen Oberfläche zu löschen.



Klicken Sie auf **Ja**, um die Löschung des SSL-Zertifikats zu bestätigen.

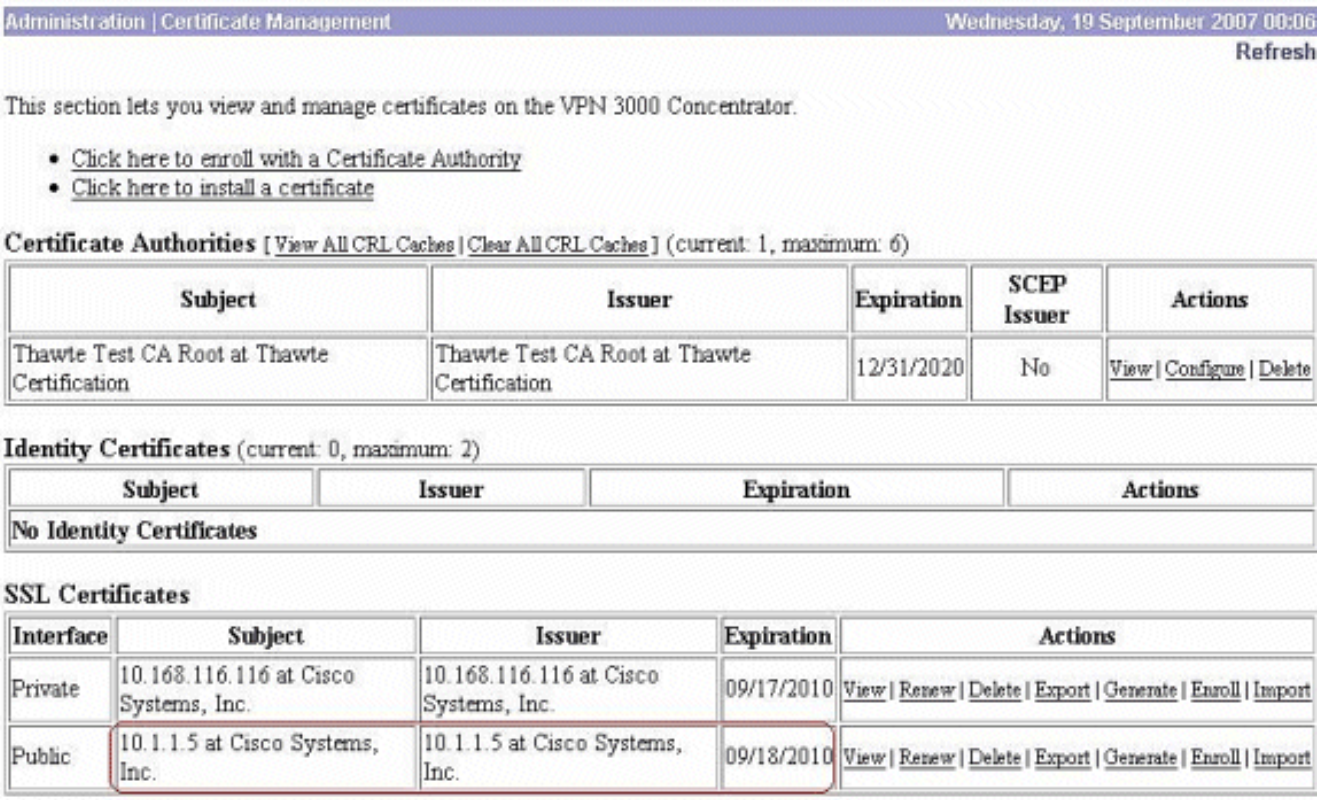


2. Wählen Sie **Administration > Certificate Management > Generate (Verwaltung > Zertifikatsverwaltung > Generieren)**, um das neue SSL-Zertifikat zu generieren.



Das neue SSL-Zertifikat für die öffentliche Schnittstelle wird

angezeigt.



Administration | Certificate Management — Wednesday, 19 September 2007 00:06

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	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

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems