

디지털 인증서 및 SSL 인증서를 얻기 위해 Cisco VPN 3000 Concentrator 4.7.x 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN Concentrator에 디지털 인증서 설치](#)

[VPN Concentrator에 SSL 인증서 설치](#)

[VPN Concentrator에서 SSL 인증서 갱신](#)

[관련 정보](#)

소개

이 문서에는 디지털 또는 ID 인증서 및 SSL 인증서를 사용하여 인증하도록 Cisco VPN 3000 Series Concentrator를 구성하는 방법에 대한 단계별 지침이 포함되어 있습니다.

참고: VPN Concentrator에서 다른 SSL 인증서를 생성하기 전에 로드 밸런싱을 비활성화해야 인증서 생성이 차단됩니다.

PIX/ASA 7.x와 동일한 시나리오에 대한 자세한 내용은 [ASA에서 ASDM을 사용하여 Microsoft Windows CA에서 디지털 인증서를 얻는 방법](#)을 참조하십시오.

Cisco IOS® 플랫폼과 동일한 시나리오에 대한 자세한 내용은 [Cisco IOS Certificate Enrollment Using Enhanced Enrollment Commands Configuration Example](#)을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 버전 4.7을 실행하는 Cisco VPN 3000 Concentrator를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

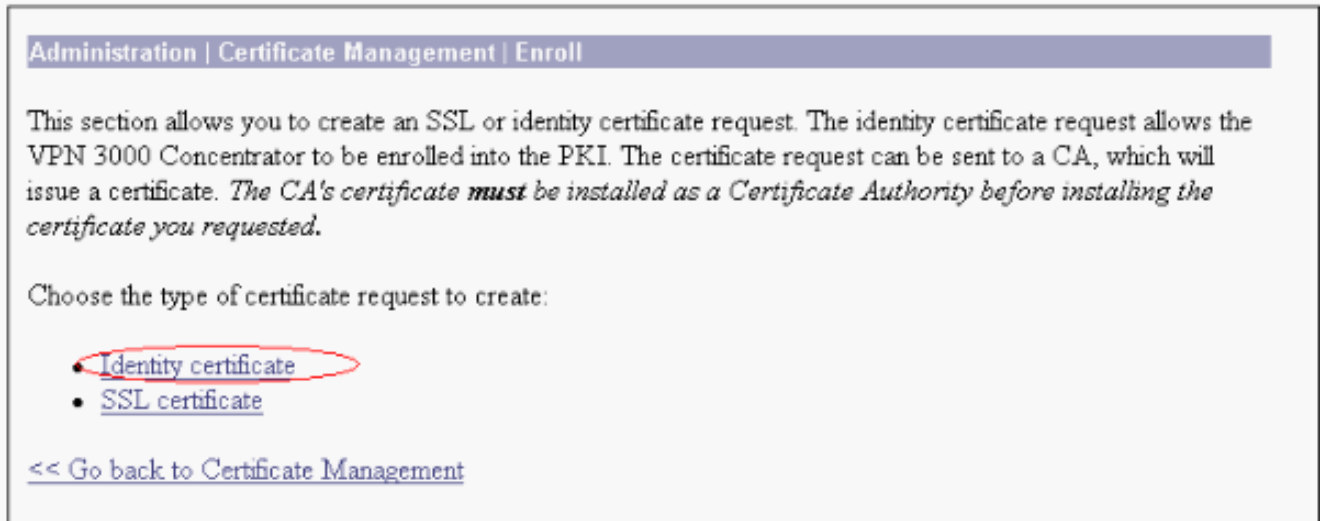
표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

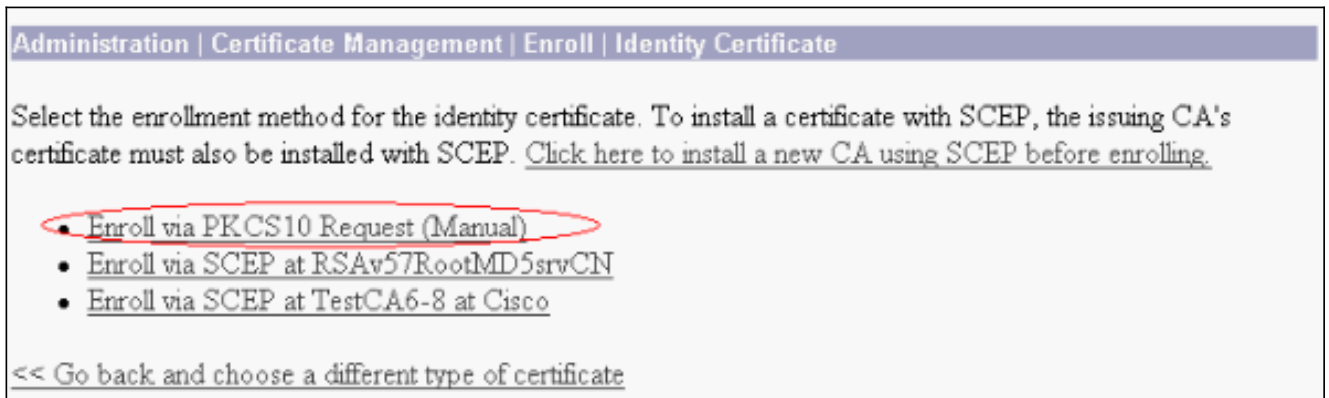
VPN Concentrator에 디지털 인증서 설치

다음 단계를 완료하십시오.

1. 디지털 또는 ID 인증서 요청을 선택하려면 **Administration(관리) > Certificate Management(인증서 관리) > Enroll(등록)**을 선택합니다



2. **Administration(관리) > Certificate Management(인증서 관리) > Enrollment(등록) > Identity Certificate(ID 인증서)**를 선택하고 **Enroll via PKCS10 Request(Manual)**를 클릭합니다



3. 요청한 필드를 입력하고 Enroll(등록)을 클릭합니다. 이 예에서는 이러한 필드를 입력합니다.
.Common Name(일반 이름) - altiga30Organizational Unit(조직 단위) - IPSECCERT(OU는 구성된 IPsec 그룹 이름과 일치해야 함)조직—Cisco SystemsLocality(지역) - RTP시/도—NorthCarolina국가—미국정규화된 도메인 이름 - (여기서는 사용되지 않음)키 크기—512참고: SSL 인증서 또는 SCEP(Simple Certificate Enrollment Protocol)를 사용하여 ID 인증서를 요청할 경우 이러한 옵션만 사용할 수 있습니다.RSA 512비트RSA 768비트RSA 1024비트RSA 2048비트DSA 512비트DSA 768비트DSA 1024비트

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.

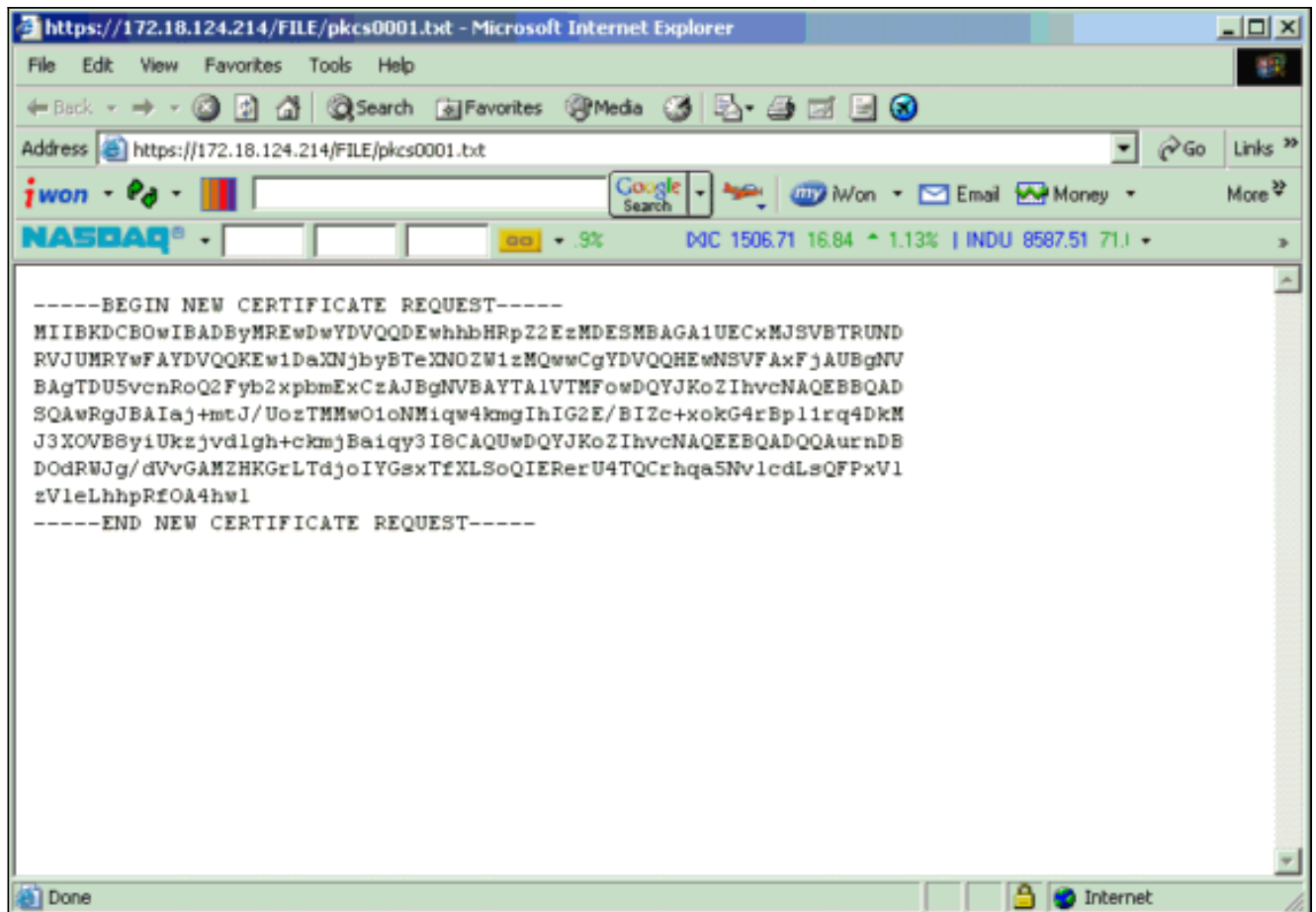
4. Enroll을 클릭하면 여러 창이 나타납니다. 첫 번째 창은 인증서를 요청했음을 확인합니다

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.

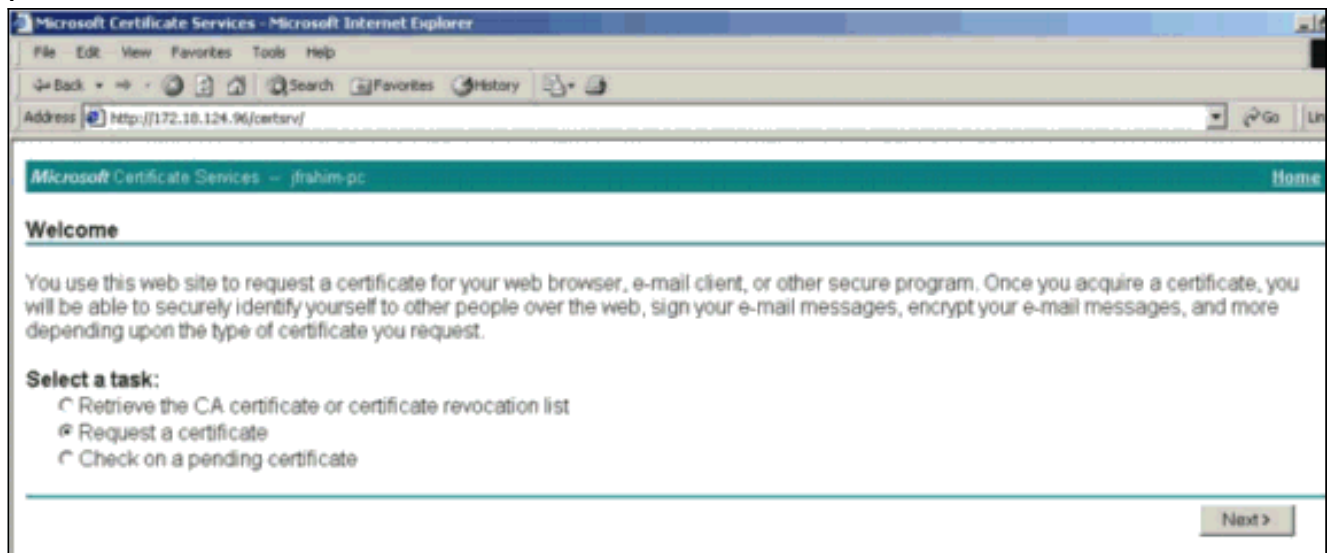
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the [File Management page](#) to delete the certificate request.

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

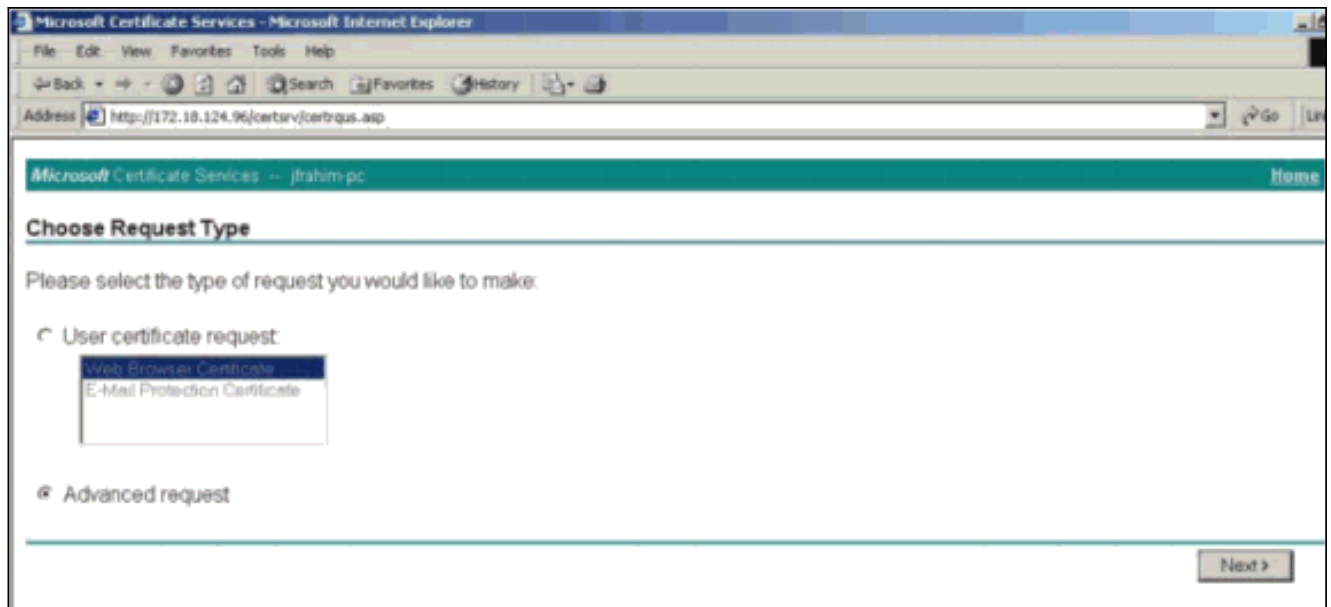
새 브라우저 창이 열리고 PKCS 요청 파일이 표시됩니다



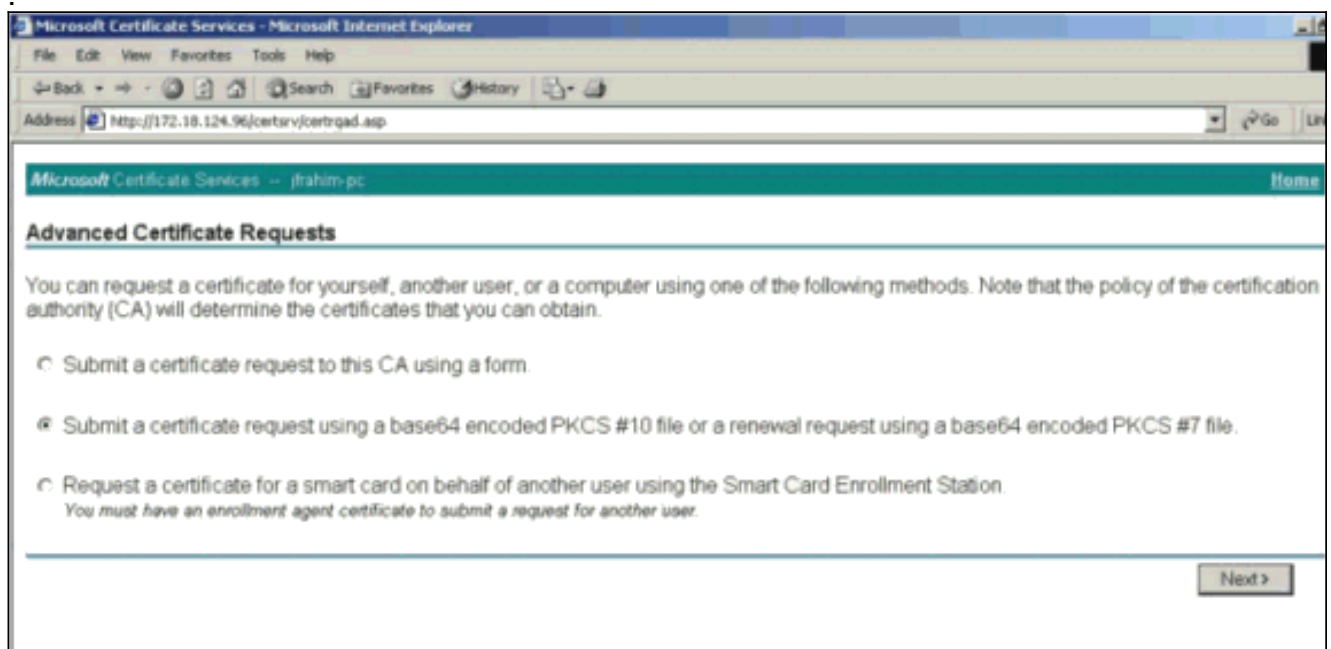
5. CA(Certification Authority) 서버에서 요청을 강조 표시하고 CA 서버에 붙여넣어 요청을 제출합니다. Next(다음)를 클릭합니다



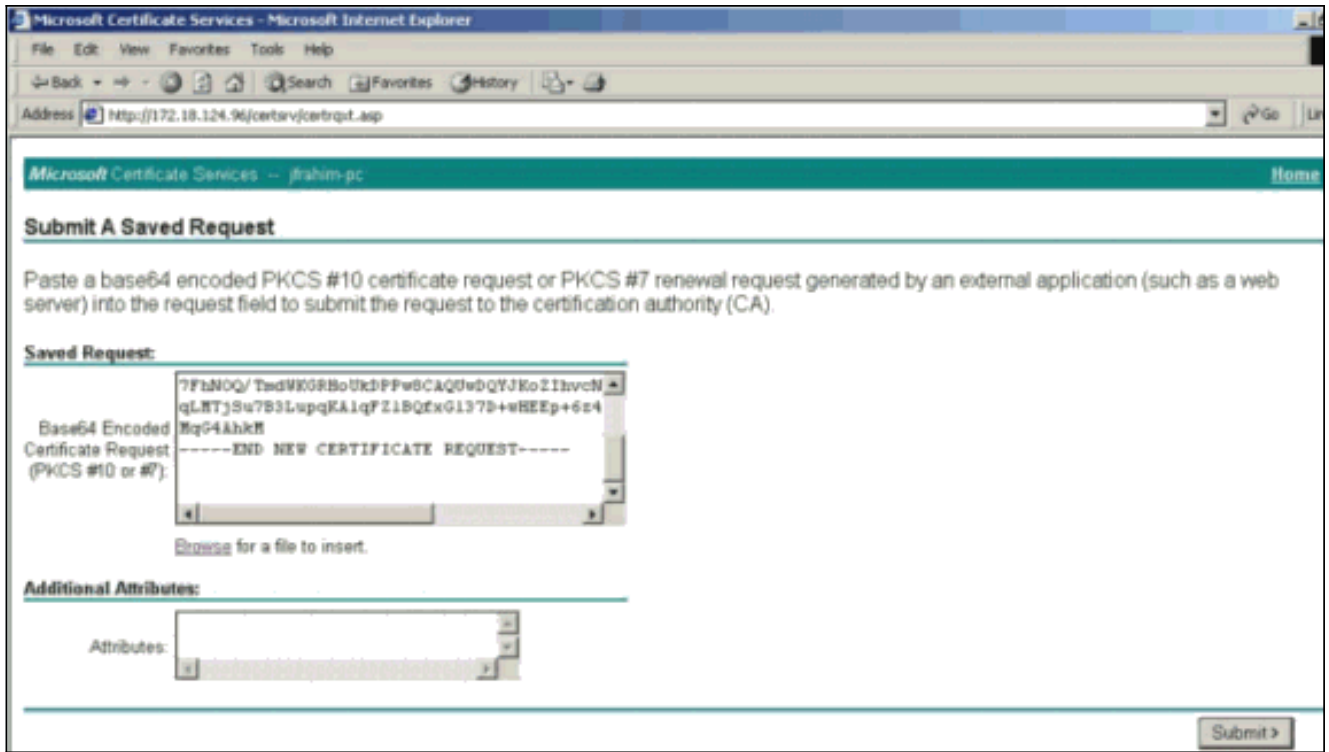
6. Advanced request(고급 요청)를 선택하고 Next(다음)를 클릭합니다



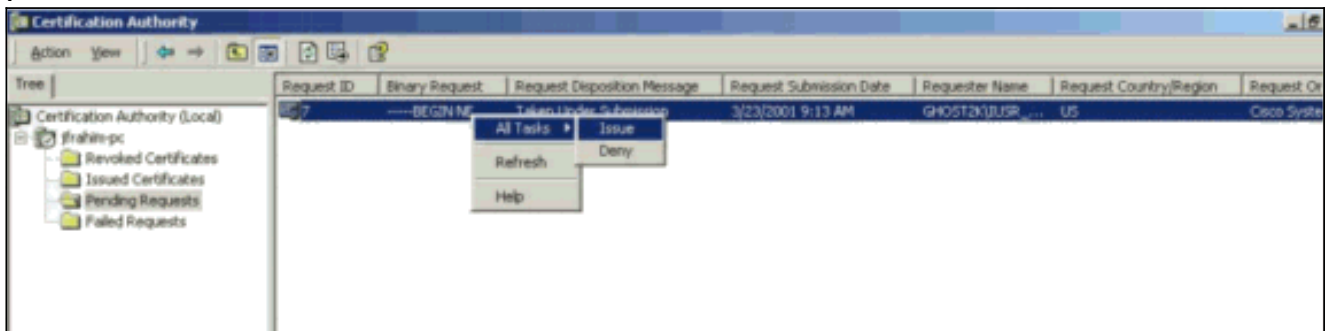
7. Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file(base64로 인코딩된 PKCS 파일을 사용하여 인증서 요청 제출)을 선택한 다음 Next(다음)를 클릭합니다



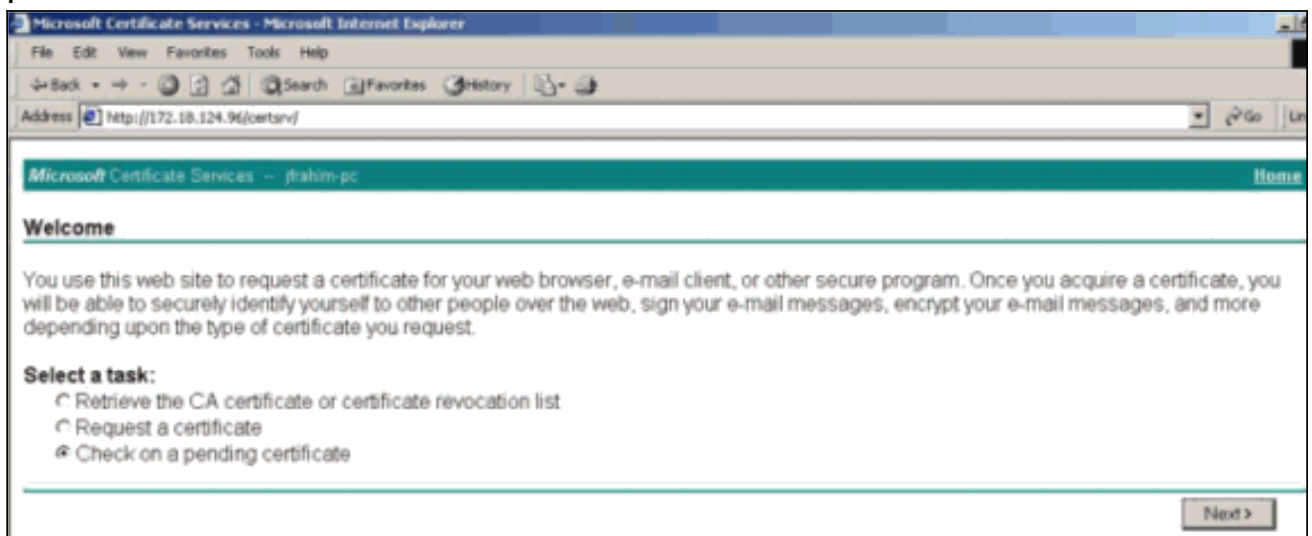
8. PKCS 파일을 잘라내어 Saved Request 섹션 아래의 텍스트 필드에 붙여넣습니다. 그런 다음 Submit(제출)을 클릭합니다



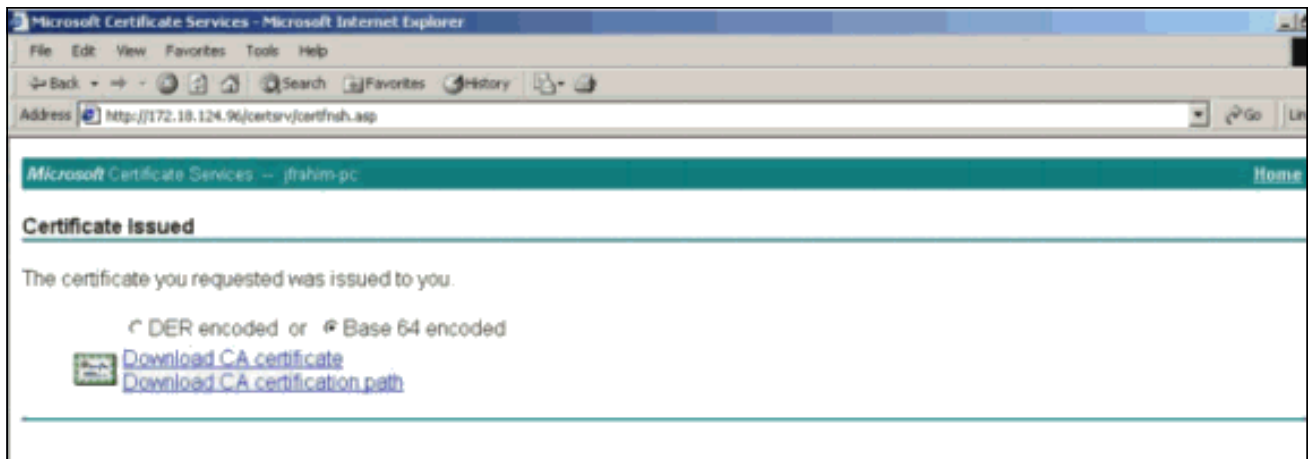
9. CA 서버에서 ID 인증서를 발급합니다



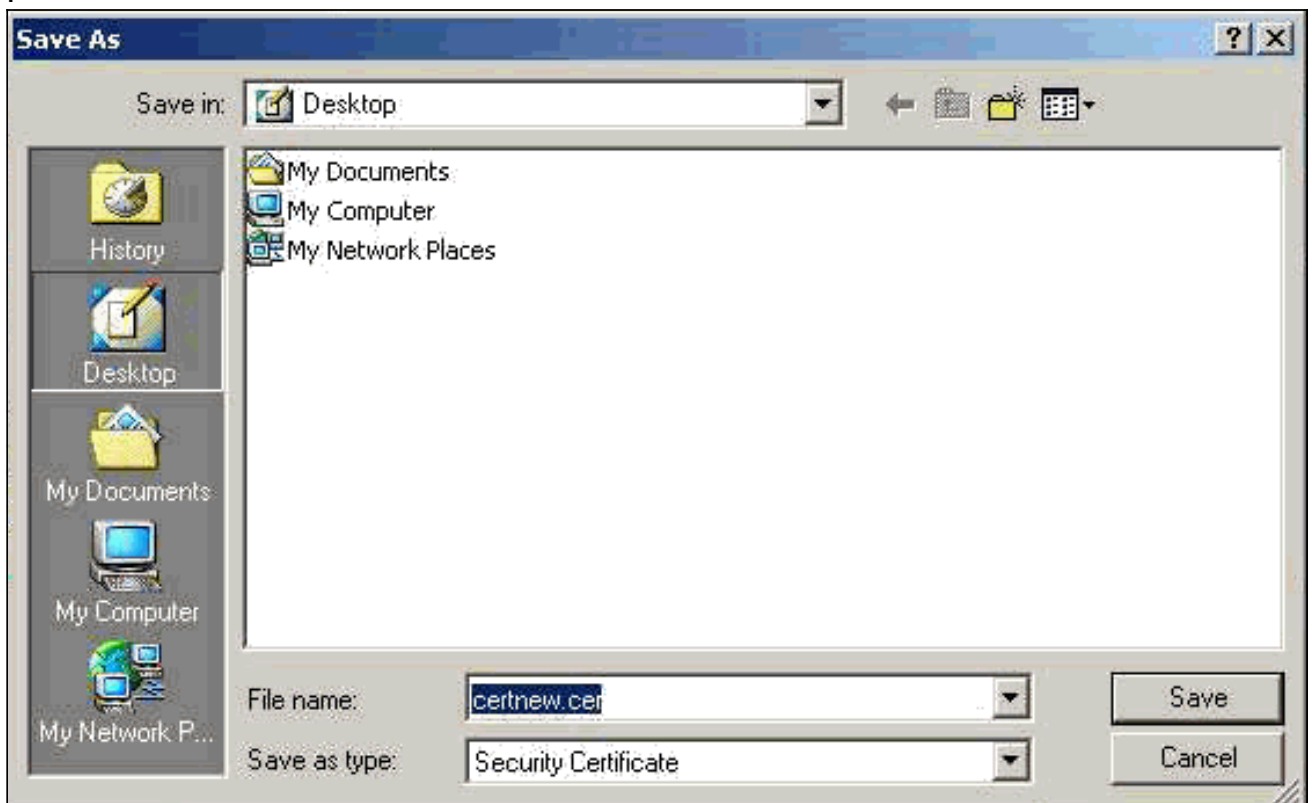
10. 루트 및 ID 인증서를 다운로드합니다. CA 서버에서 보류 중인 인증서 확인을 선택하고 다음을 클릭합니다



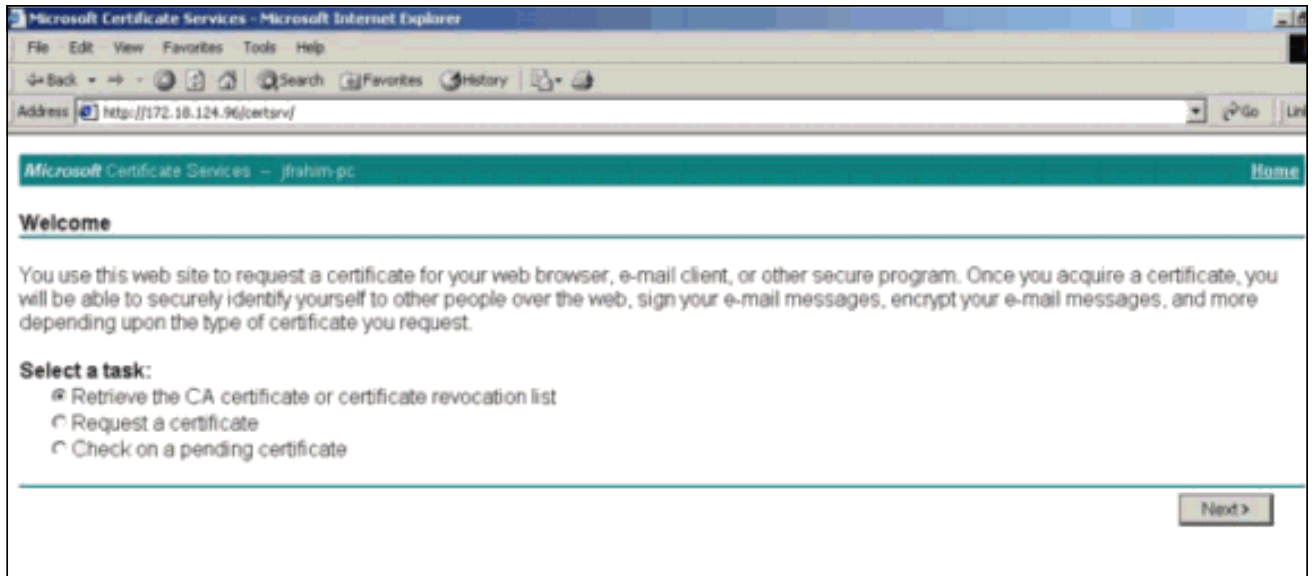
11. Base 64 encoded를 선택하고 CA 서버에서 Download CA certificate(CA 인증서 다운로드)를 클릭합니다



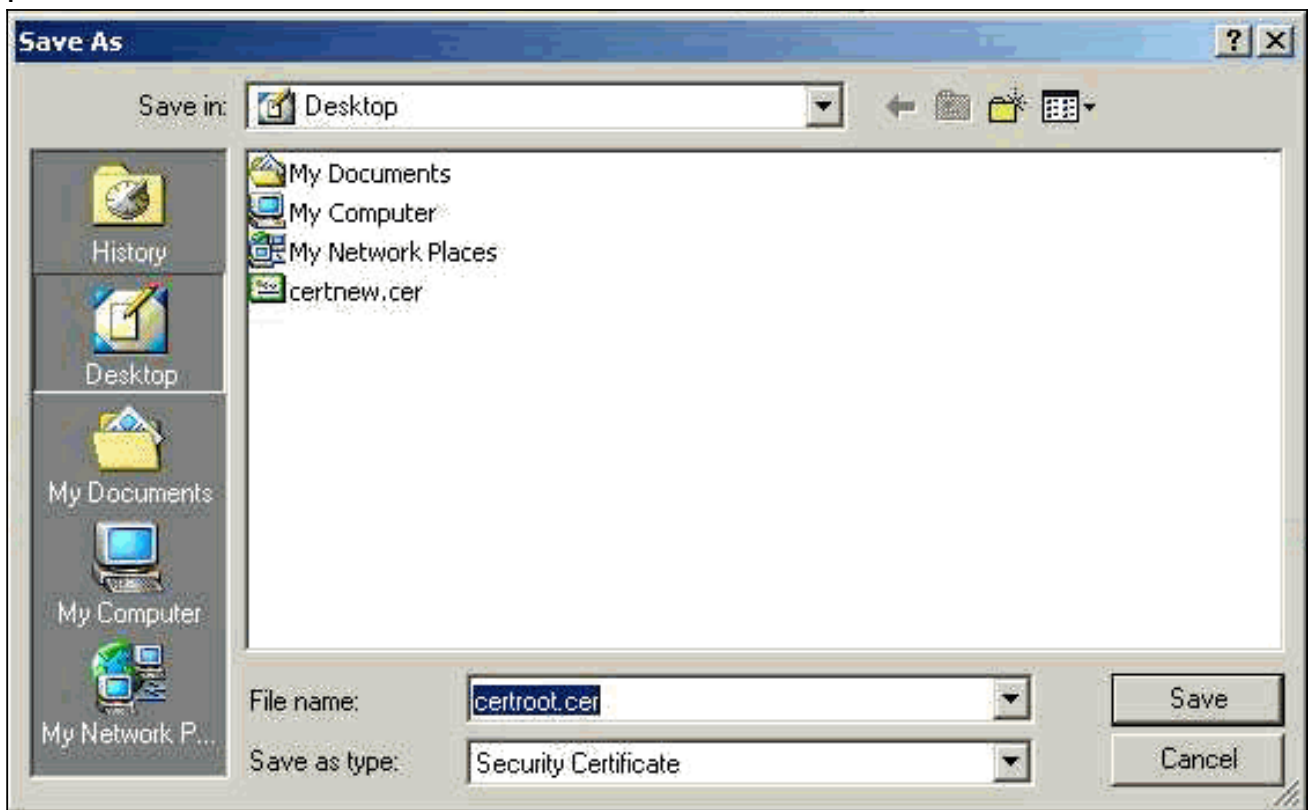
12. 로컬 드라이브에 ID 인증서를 저장합니다



13. CA 서버에서 루트 인증서를 가져오려면 **Retrieve the CA certificate or certificate revocation list**(CA 인증서 또는 인증서 폐기 목록 검색)를 선택합니다. 그런 다음 **Next(다음)**를 클릭합니다



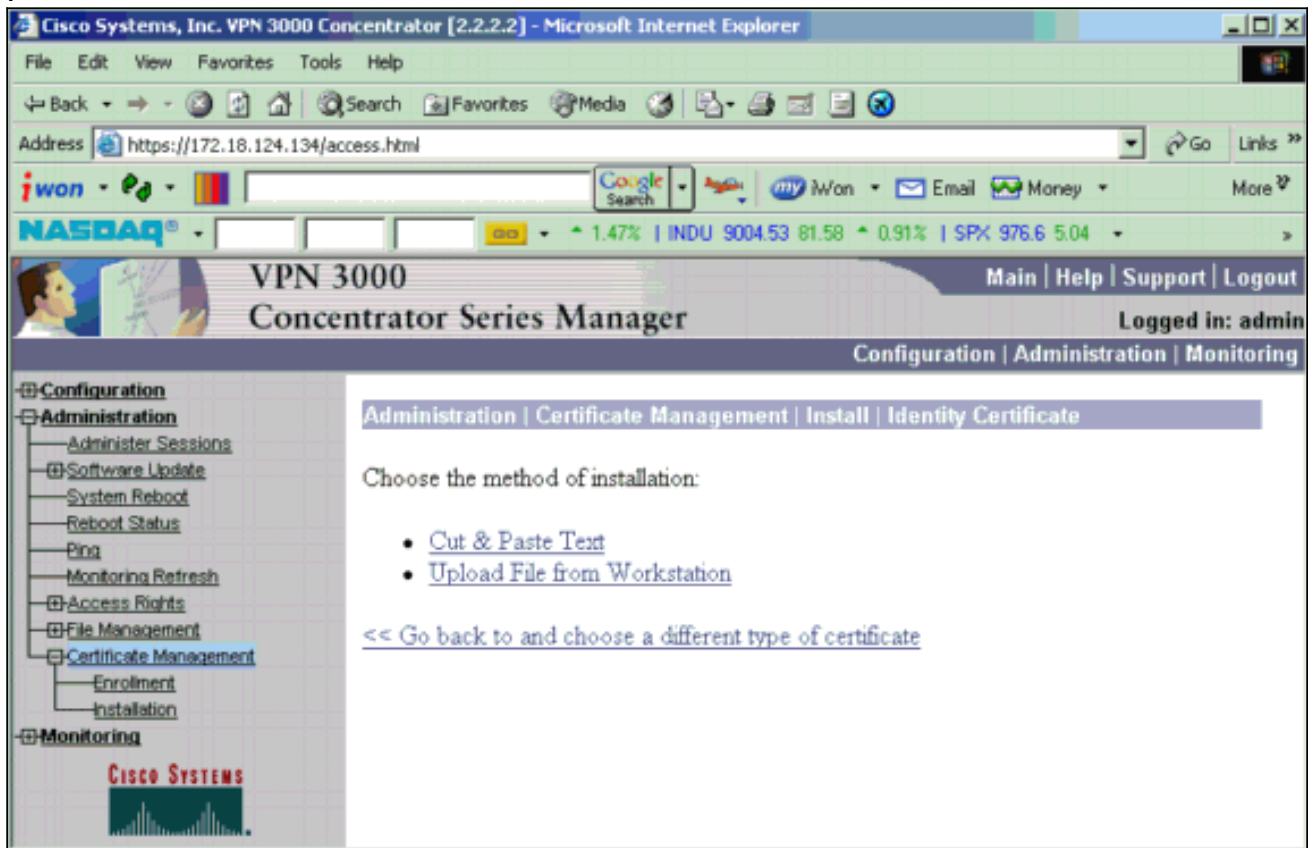
14. 로컬 드라이브에 루트 인증서를 저장합니다



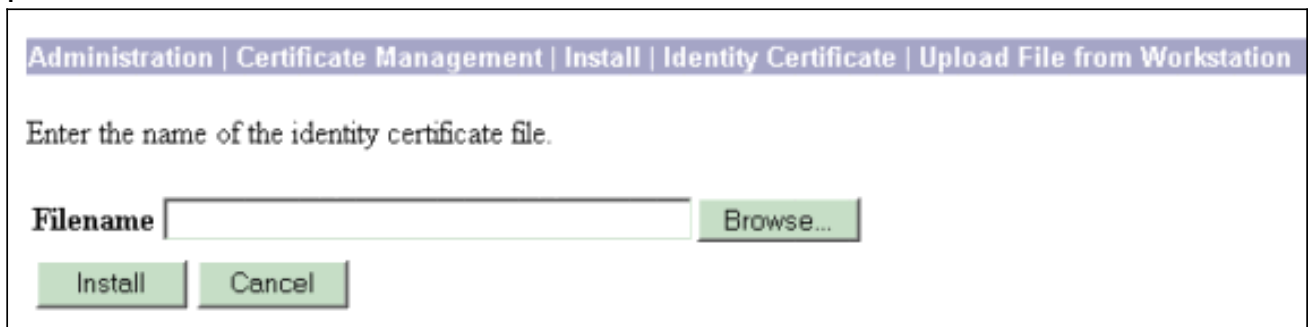
15. VPN 3000 Concentrator에 루트 및 ID 인증서를 설치합니다. 이렇게 하려면 **Administration > Certificate Manager > Installation > Install certificate objects via enrollment**를 선택합니다. Enrollment Status(등록 상태)에서 Install(설치)을 클릭합니다



16. Upload File from Workstation을 클릭합니다



17. Browse(찾아보기)를 클릭하고 로컬 드라이브에 저장한 루트 인증서 파일을 선택합니다 .Install(설치)을 선택하여 VPN Concentrator에 ID 인증서를 설치합니다. 관리 | Certificate Management(인증서 관리) 창이 확인으로 나타나고 새 ID 인증서가 Identity Certificates(ID 인증서) 테이블에 나타납니다



참고: 인증서가 실패할 경우 새 인증서를 생성하려면 다음 단계를 완료합니다
 .Administration(관리) > **Certificate Management(인증서 관리)**를 선택합니다.Actions(작업) 상자에서 Delete(삭제)를 클릭하여 SSL Certificate(SSL 인증서) 목록을 표시합니다
 .Administration(관리) > **System Reboot(시스템 재부팅)**를 선택합니다.**Save the active configuration at time reboot(재부팅 시 활성 컨피그레이션 저장)**을 선택하고 **Now(지금)**를 선택한 다음 **Apply(적용)**를 클릭합니다. 이제 다시 로드가 완료된 후 새 인증서를 생성할 수 있습니다.

VPN Concentrator에 SSL 인증서 설치

브라우저와 VPN Concentrator 간에 보안 연결을 사용하는 경우 VPN Concentrator에는 SSL 인증서가 필요합니다. 또한 VPN Concentrator 및 WebVPN을 관리하는 데 사용하는 인터페이스 및 WebVPN 터널을 종료하는 각 인터페이스에 대한 SSL 인증서가 필요합니다.

VPN 3000 Concentrator 소프트웨어를 업그레이드한 후 VPN 3000 Concentrator가 재부팅될 때 인터페이스 SSL 인증서가 없는 경우 자동으로 생성됩니다. 자체 서명 인증서는 자체 생성되므로 이 인증서는 확인 불가합니다. 어떤 인증 기관에서도 ID를 보증하지 않았습니다. 그러나 이 인증서를 사용하면 브라우저를 사용하여 VPN Concentrator에 처음 연결할 수 있습니다. 다른 자체 서명 SSL 인증서로 교체하려면 다음 단계를 완료하십시오.

1. 관리 > 인증서 관리를 선택합니다

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(생성)를 클릭하여 SSL Certificate(SSL 인증서) 테이블에 새 인증서를 표시하고 기존 인증서를 교체합니다. 이 창에서는 VPN Concentrator가 자동으로 생성하는 SSL 인증서에 대한 필드를 구성할 수 있습니다. 이러한 SSL 인증서는 인터페이스 및 로드 밸런싱을 위한 것입니다

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.

확인 가능한 SSL 인증서(즉, Certificate Authority에서 발급한 인증서)를 얻으려면 ID 인증서를 얻는 데 사용하는 것과 동일한 절차를 사용하려면 이 문서의 [VPN Concentrator](#) 섹션에 [디지털 인증서 설치](#) 섹션을 참조하십시오. 그러나 이번에는 Administration(관리) > **Certificate Management(인증서 관리)** > **Enroll(등록)** 창에서 **SSL 인증서(ID 인증서 대신)**를 클릭합니다

.참고: 관리 참조 [VPN 3000 Concentrator Reference Volume II](#)의 [인증서 관리](#) 섹션 II: 디지털 인증서 및 SSL 인증서에 대한 전체 정보를 보려면 [관리 및 모니터링 릴리스 4.7](#)을 참조하십시오.

VPN Concentrator에서 SSL 인증서 갱신

이 섹션에서는 SSL 인증서를 갱신하는 방법에 대해 설명합니다.

VPN Concentrator에서 생성한 SSL 인증서용인 경우 SSL 섹션에서 **Administration(관리) > Certificate Management(인증서 관리)**로 이동합니다. 갱신 옵션을 클릭하고 SSL 인증서를 갱신합니다.

외부 CA 서버에서 부여한 인증서에 대한 인증서인 경우 다음 단계를 완료합니다.

1. 퍼블릭 인터페이스에서 만료된 인증서를 삭제하려면 Administration(관리) > Certificate Management(인증서 관리) > Delete(SSL 인증서)를 선택합니다

Administration | Certificate Management Wednesday, 19 September 2007 00:01:34 [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 인증서 삭제를 확인하려면 **Yes**를 클릭합니다

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. 새 SSL 인증서를 생성하려면 Administration(관리) > Certificate Management(인증서 관리) > Generate(생성)를 선택합니다

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



공용 인터페이스에 대한 새 SSL 인증서가 나타납니다

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

관련 정보

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [IPSec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)