Configurando o Cisco VPN 3000 Concentrator 4.7.x para obter um certificado digital e um certificado SSL

Contents

Introduction

Este documento inclui instruções passo a passo sobre como configurar os Cisco VPN 3000 Series Concentrators para autenticar com o uso de certificados digitais ou de identidade e certificados SSL.

Observação: no VPN Concentrator, o balanceamento de carga deve ser desabilitado antes de gerar outro certificado SSL, pois isso impede a geração do certificado.

Consulte Como obter um certificado digital de uma CA do Microsoft Windows usando o ASDM em um ASA para saber mais sobre o mesmo cenário com o PIX/ASA 7.x.

Consulte Exemplo de Configuração de Inscrição de Certificado do Cisco IOS Usando Comandos de Inscrição Avançados para saber mais sobre o mesmo cenário com as Plataformas Cisco IOS®.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN 3000 Concentrator que executa a versão 4.7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

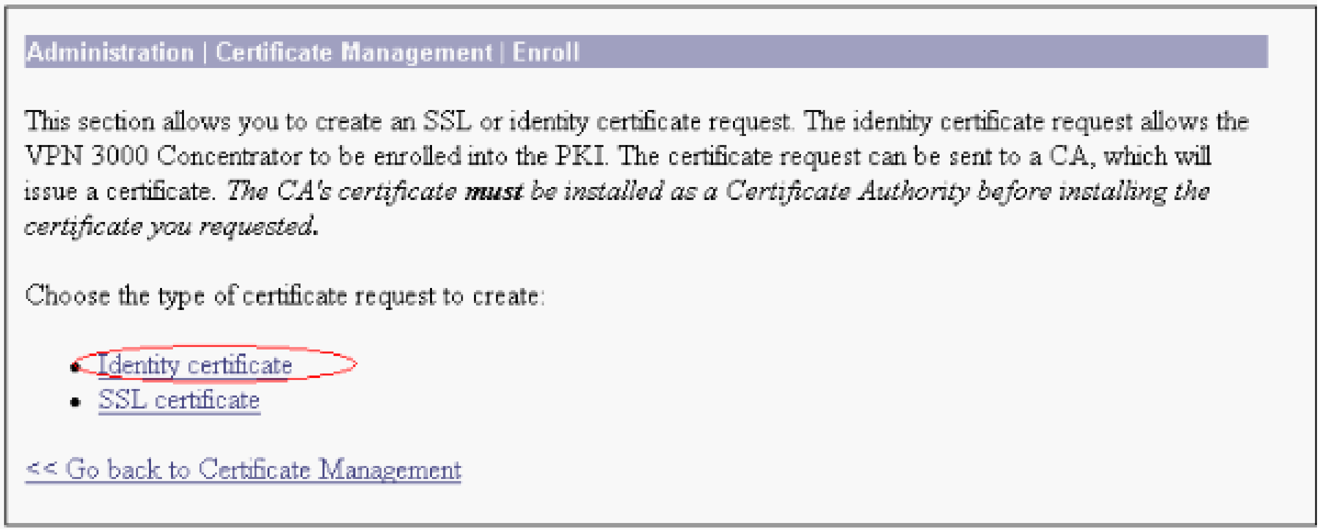
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Instalar certificados digitais no VPN Concentrator

Conclua estes passos:

1. Escolha **Administration > Certificate Management > Enroll** para selecionar a solicitação de certificado digital ou de identidade.



Administration | Certificate Management | Enroll

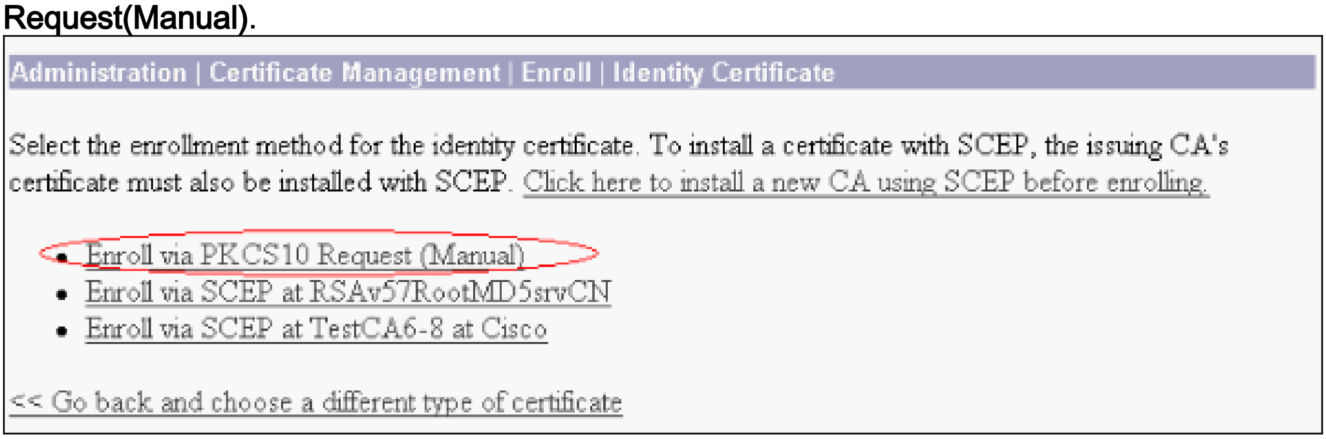
This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested.*

Choose the type of certificate request to create:

- Identity certificate
- SSL certificate

<< Go back to Certificate Management

2. Escolha **Administration > Certificate Management > Enrollment > Identity Certificate** e clique em **Enroll via PKCS10 Request(Manual)**.



Administration | Certificate Management | Enroll | Identity Certificate

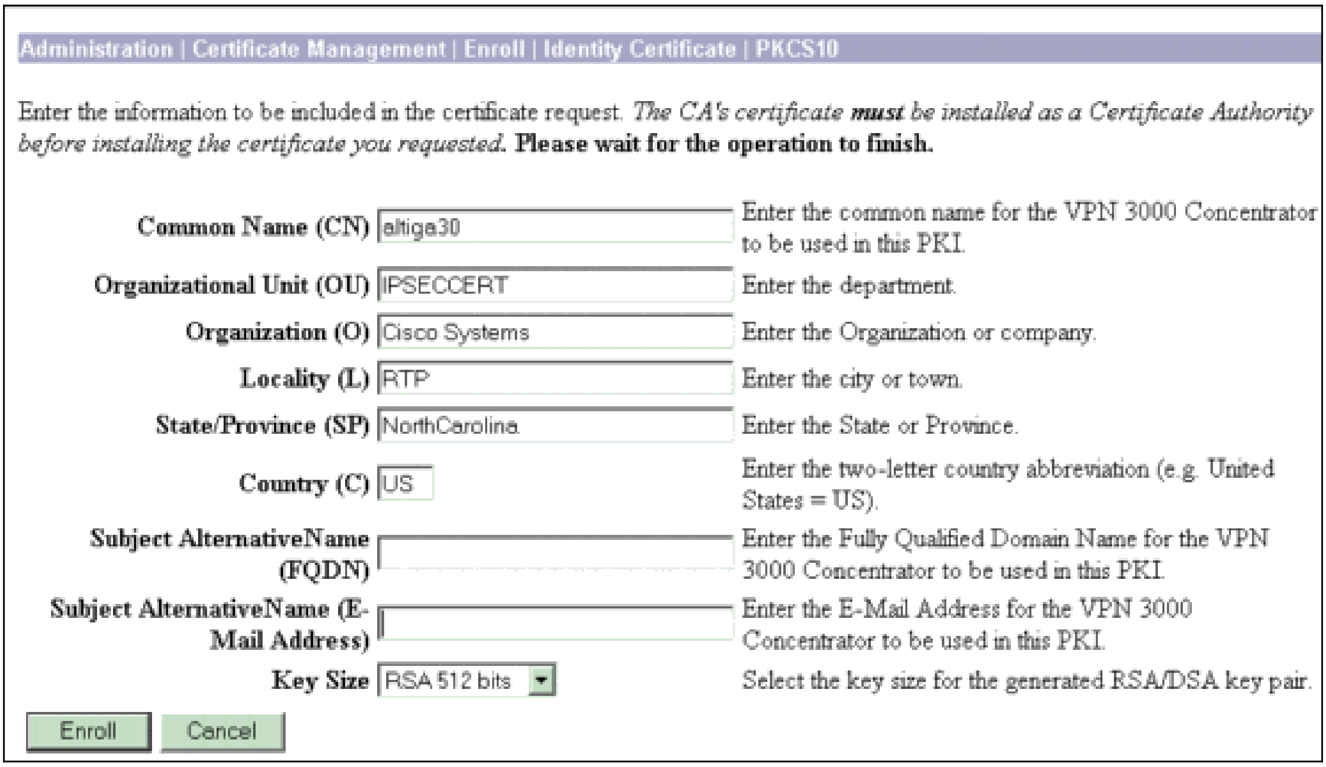
Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. Click here to install a new CA using SCEP before enrolling.

- Enroll via PKCS10 Request (Manual)
- Enroll via SCEP at RSAv57RootMD5srvCN
- Enroll via SCEP at TestCA6-8 at Cisco

<< Go back and choose a different type of certificate

3. Preencha os campos solicitados e clique em **Inscrever**.Esses campos são preenchidos neste exemplo.**Nome comum** — altiga30**Unidade organizacional**—IPSECCERT (a OU deve corresponder ao nome de grupo IPsec configurado)**Organização** — Cisco Systems**Localidade** — RTP**Estado/Província** — Carolina do Norte**País** — EUA**Nome de domínio totalmente qualificado** —(não usado aqui)**Tamanho da chave** — 512**Observação:** se você solicitar um certificado SSL ou um certificado de identidade usando o Simple Certificate

Enrollment Protocol (SCEP), essas são as únicas opções RSA disponíveis.RSA 512 bitsRSA 768 bitsRSA 1024 bitsRSA 2048 bitsDSA 512 bitsDSA 768 bitsDSA 1024 bits

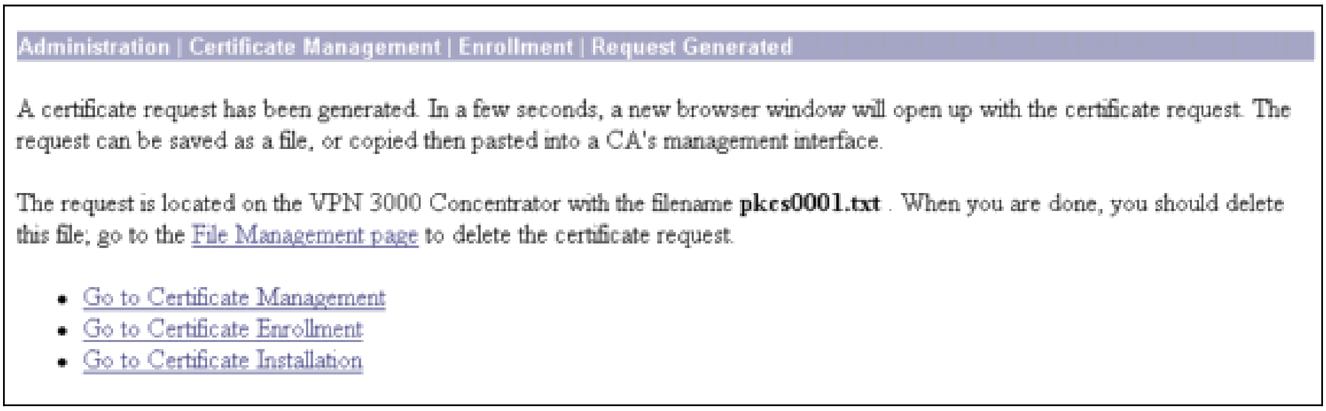


Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

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

4. Depois de clicar em **Inscrever-se**, várias janelas serão exibidas. A primeira janela confirma que você solicitou um certificado.



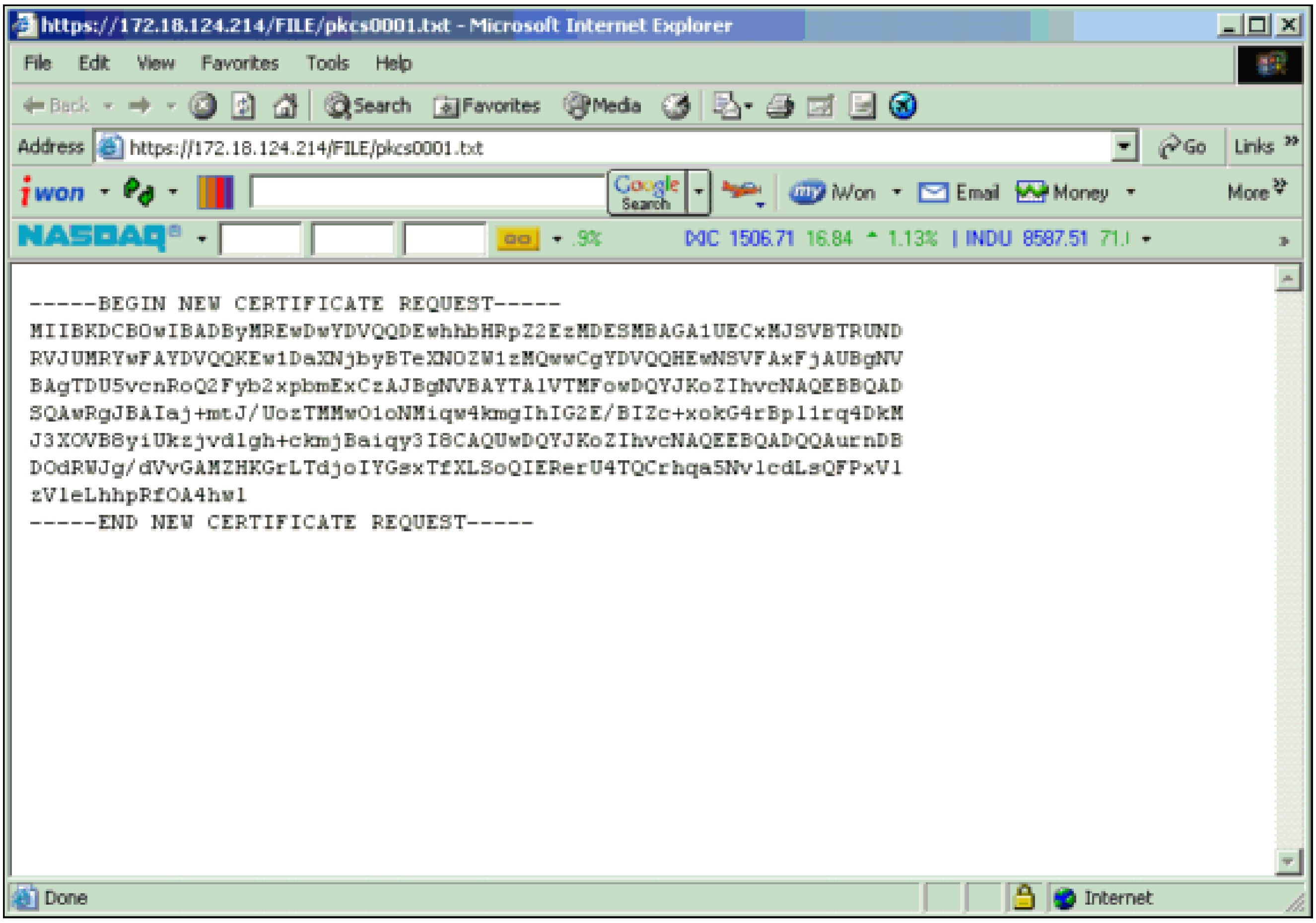
Administration | Certificate Management | Enrollment | Request Generated

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.

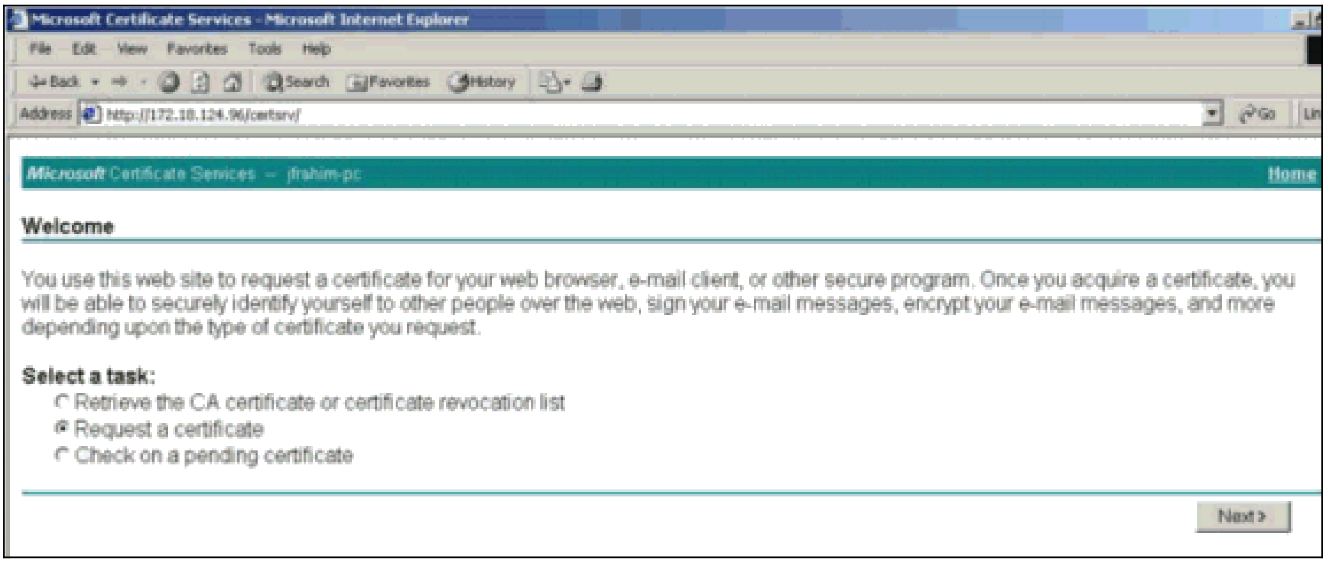
- Go to Certificate Management
- Go to Certificate Enrollment
- Go to Certificate Installation

Uma nova janela do navegador também é aberta e exibe seu arquivo de solicitação PKCS.


https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.18.124.214/FILE/pkcs0001.txt
Go Links
Done
Internet

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRpZ2EzMDESMBAGA1UECxMJSVBTRUND
RVJUMRYwFAYDVQQKEw1DaXNjbyBTeXNOZW1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV
BAgTDU5vcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQYJKoZIhvcNAQEBBQAD
SQAwRgJBAIaj+mtJ/UozTMMwO1oNMiqw4kmgIhIG2E/BIZc+xokG4rBp11rq4DkM
J3XOVB8yiUkzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB
DOdRWJg/dVvGAMZHKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqa5NvlcdLsQFPxVl
zVleLhhpRfOA4hwl
-----END NEW CERTIFICATE REQUEST-----
```

5. No servidor da Autoridade de Certificação (AC), realce a solicitação e cole-a no servidor da AC para enviar sua solicitação. Clique em Next.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.96/certsrv/
Go
Microsoft Certificate Services -- jfrahim-pc
Home

Welcome

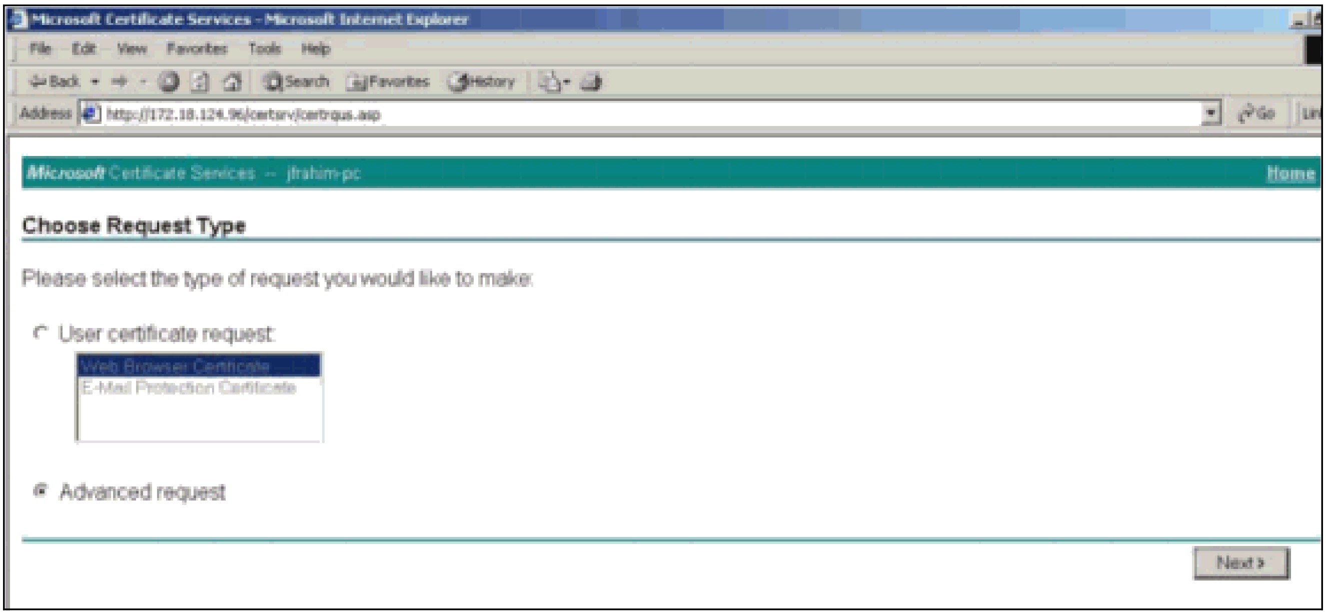
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Next >

6. Selecione **Solicitação avançada** e clique em **Avançar**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Home
Next >

http://172.18.124.96/certsrv/certrqus.asp

Microsoft Certificate Services -- jfrahim-pc

Choose Request Type

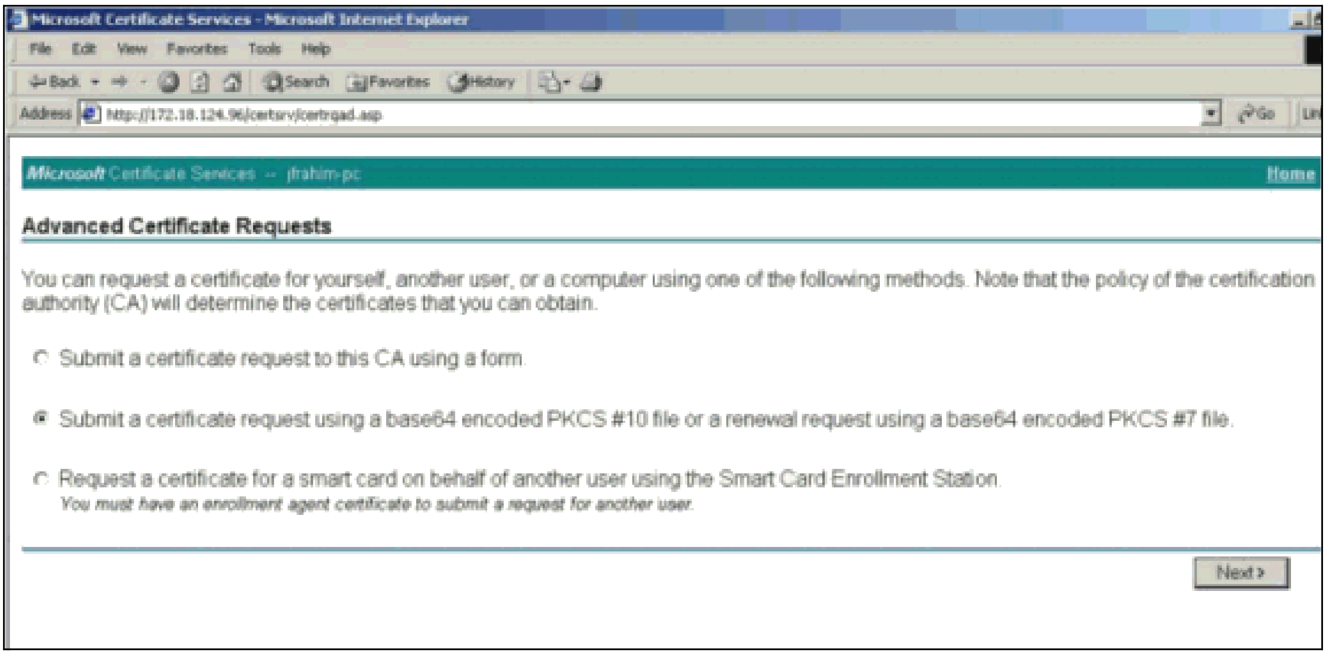
Please select the type of request you would like to make:

○ User certificate request:

Web Browser Certificate
E-Mail Protection Certificate

● Advanced request

7. Selecione **Submit a certificate request using a base64 encoded PKCS #10 file or a renew request using a base64 encoded PKCS #7 file** e clique em **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Home
Next >

http://172.18.124.96/certsrv/certrqad.asp

Microsoft Certificate Services -- jfrahim-pc

Advanced Certificate Requests

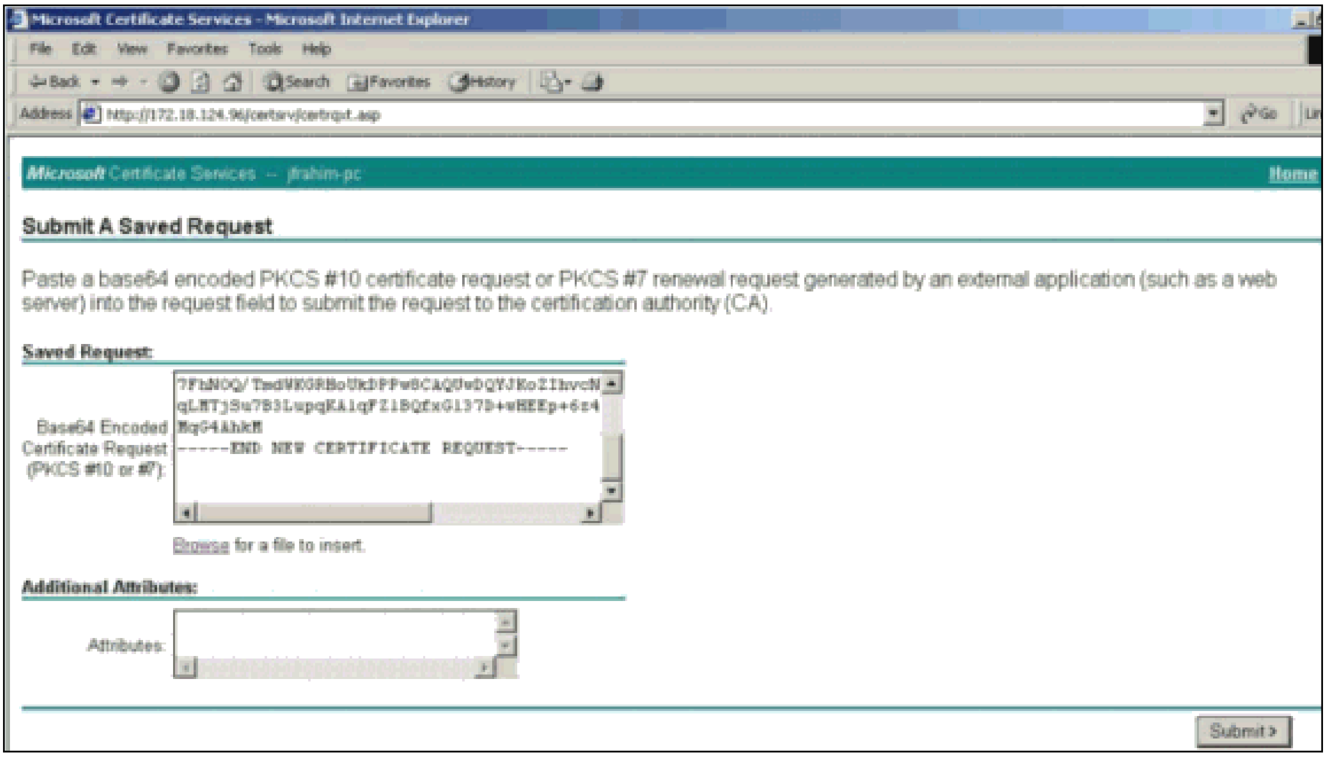
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

8. Corte e cole seu arquivo PKCS no campo de texto na seção Solicitação salva. Em seguida, clique em **Enviar**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.96/certsrv/certrqxt.asp
Go
Microsoft Certificate Services -- jfrahim-pc
Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

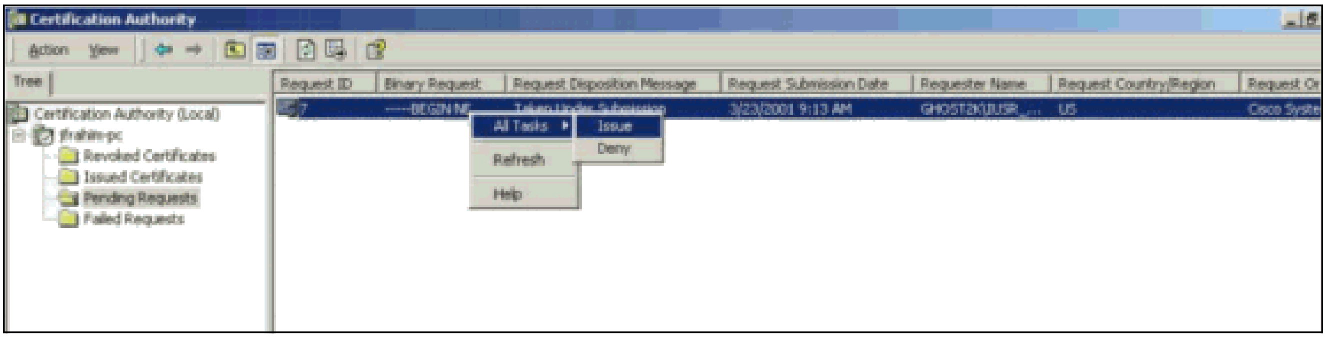
```
7FbNOQ/TmdWKGRBoUkDPPw8CAQUwDQYJKoZIhvcN
qLRTjSu7B3LupqKAlqFZiBQfxG137D+wHEEp+6z4
Mq64AhkM
-----END NEW CERTIFICATE REQUEST-----
```

Browse for a file to insert.

Additional Attributes:

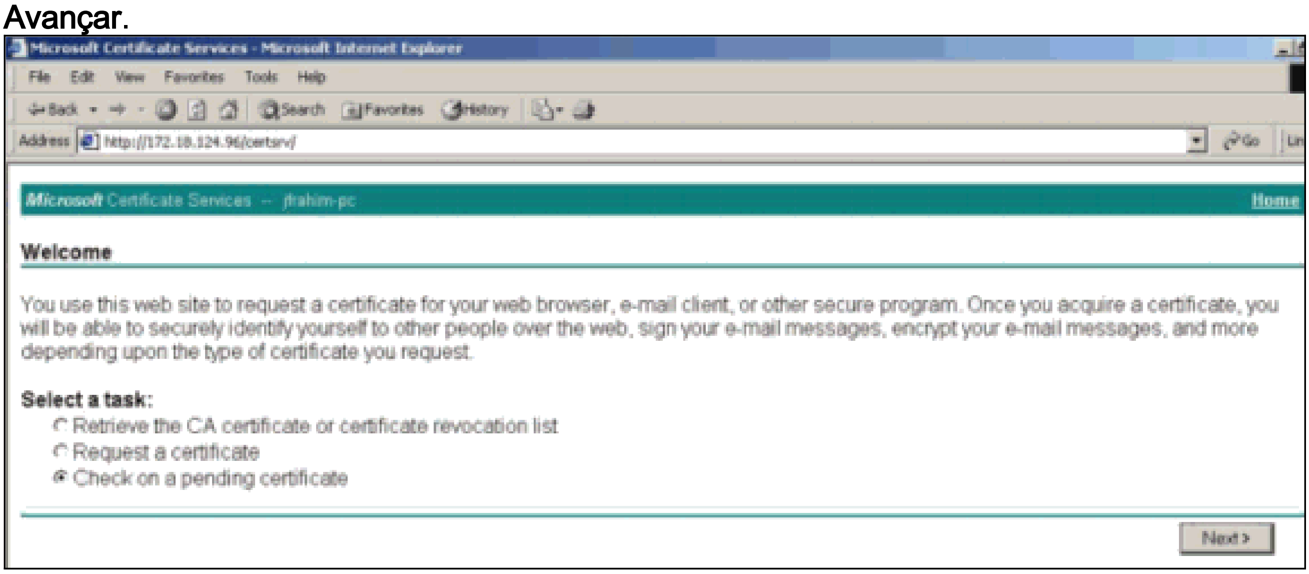
Attributes:

9. Emita o certificado de identidade no servidor CA.



Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
7	-----BEGIN NE	Taken Under Submission	3/23/2001 9:13 AM	GHOST2K\IUSR_...	US	Cisco Syste

10. Faça o download da raiz e dos certificados de identidade. No servidor CA, selecione **Verificar um certificado pendente** e clique em **Avançar**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.96/certsrv/
Go
Microsoft Certificate Services -- jfrahim-pc
Home

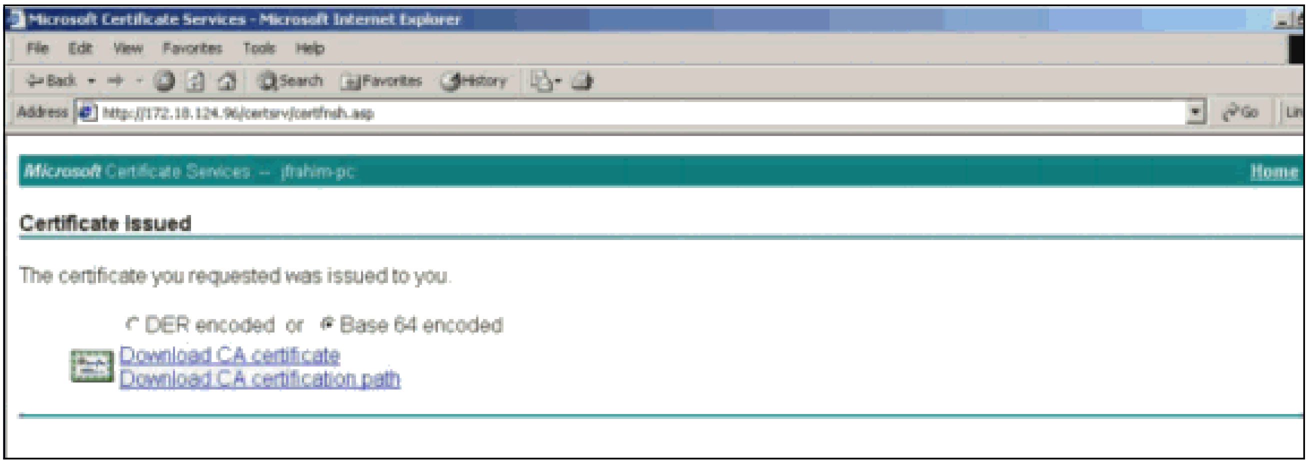
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
○ Request a certificate
● Check on a pending certificate

11. Selecione **Base 64 codificada** e clique em **Download de certificado CA** no servidor CA.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Home

http://172.18.124.96/certsrv/certfnsh.asp

Microsoft Certificate Services -- jfrahim-pc

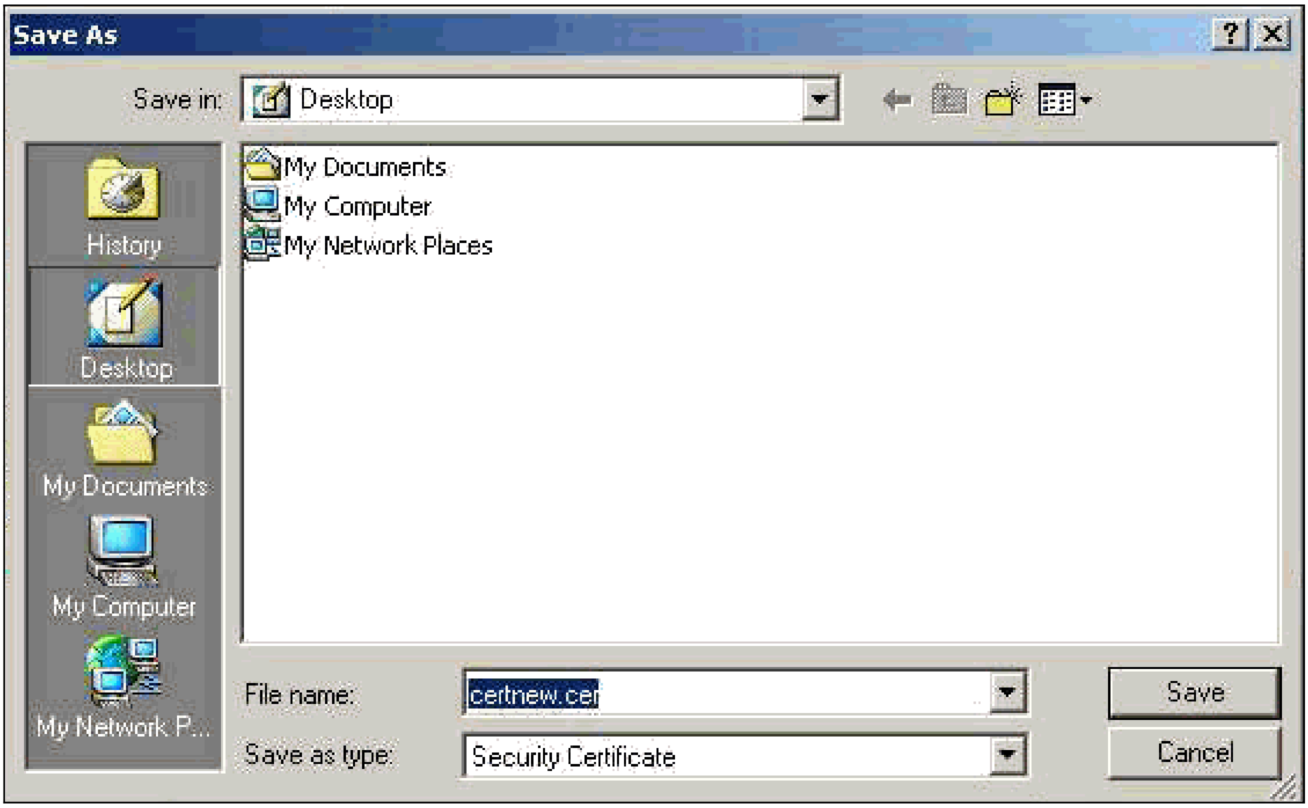
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download CA certificate
Download CA certification path

12. Salve o certificado de identidade na unidade local.



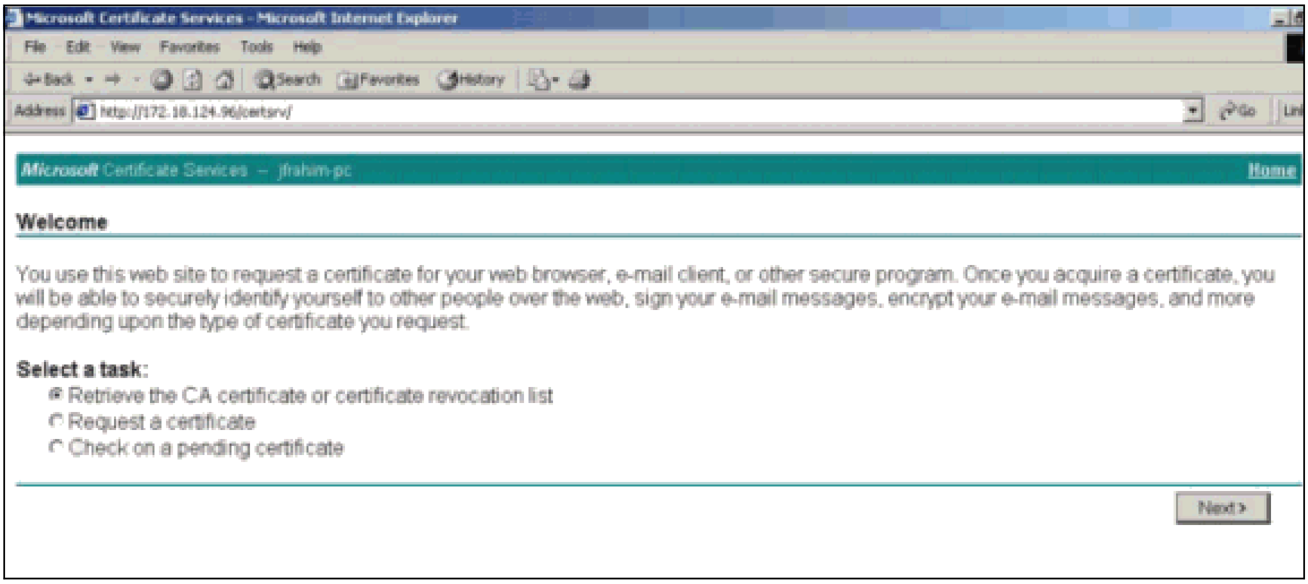
Save in: Desktop

My Documents
My Computer
My Network Places

File name: certnew.cer

Save as type: Security Certificate

13. No servidor CA, selecione **Recuperar o certificado CA ou a lista de revogação de certificado** para obter o certificado raiz. Em seguida, clique em Avançar.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.96/certsrv/
Go
Microsoft Certificate Services -- jfrahim-pc
Home

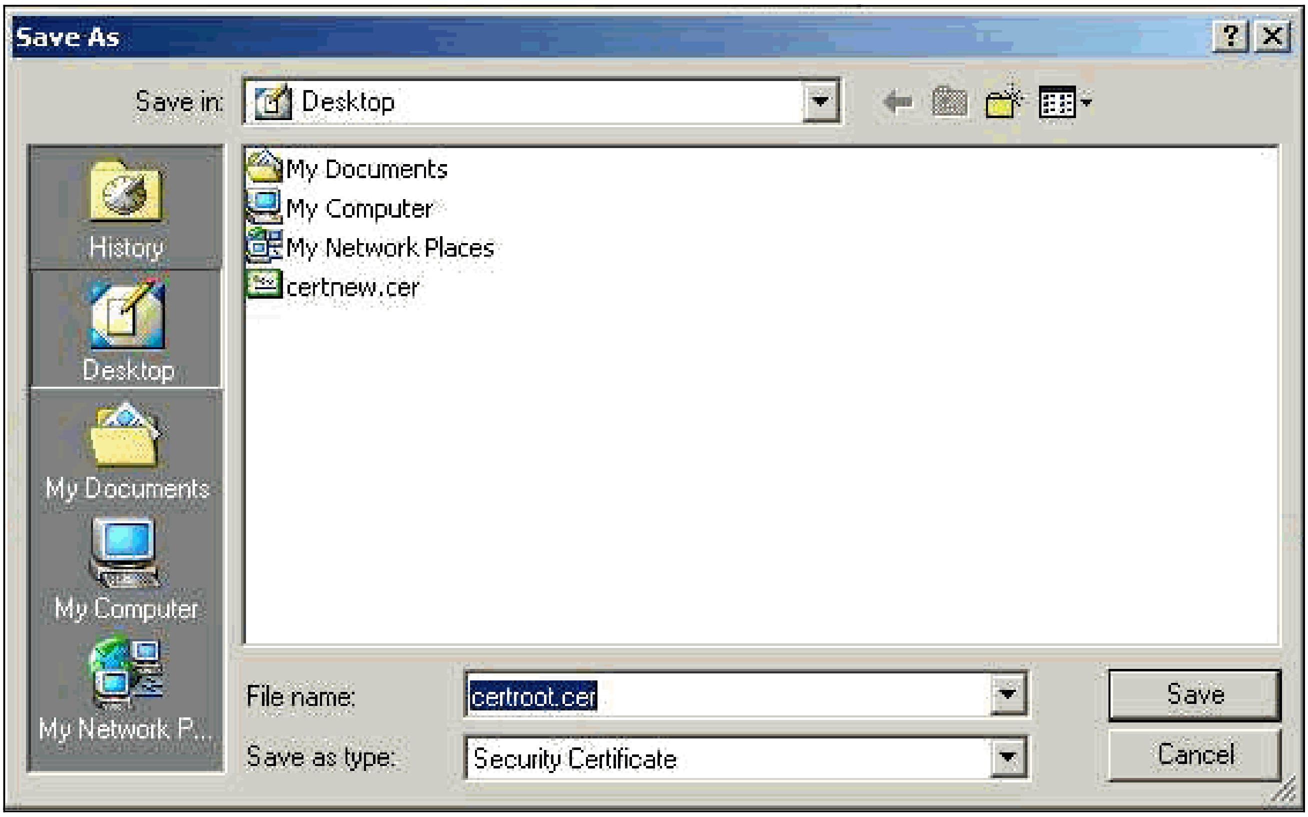
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- ● Retrieve the CA certificate or certificate revocation list
- ○ Request a certificate
- ○ Check on a pending certificate

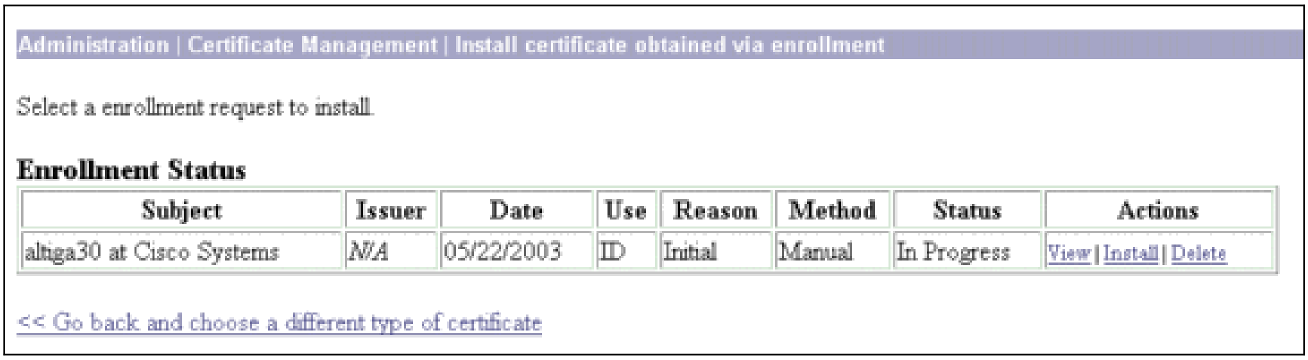
14. Salve o certificado raiz na unidade local.



File name: certroot.cer

Save as type: Security Certificate

15. Instale os certificados raiz e de identidade no VPN 3000 Concentrator. Para fazer isso, selecione **Administration** > **Certificate Manager** > **Installation** > **Install certificate obtido por meio da inscrição**. Em Status da inscrição, clique em **Instalar**.



Administration | Certificate Management | Install certificate obtained via enrollment

Select a enrollment request to install.

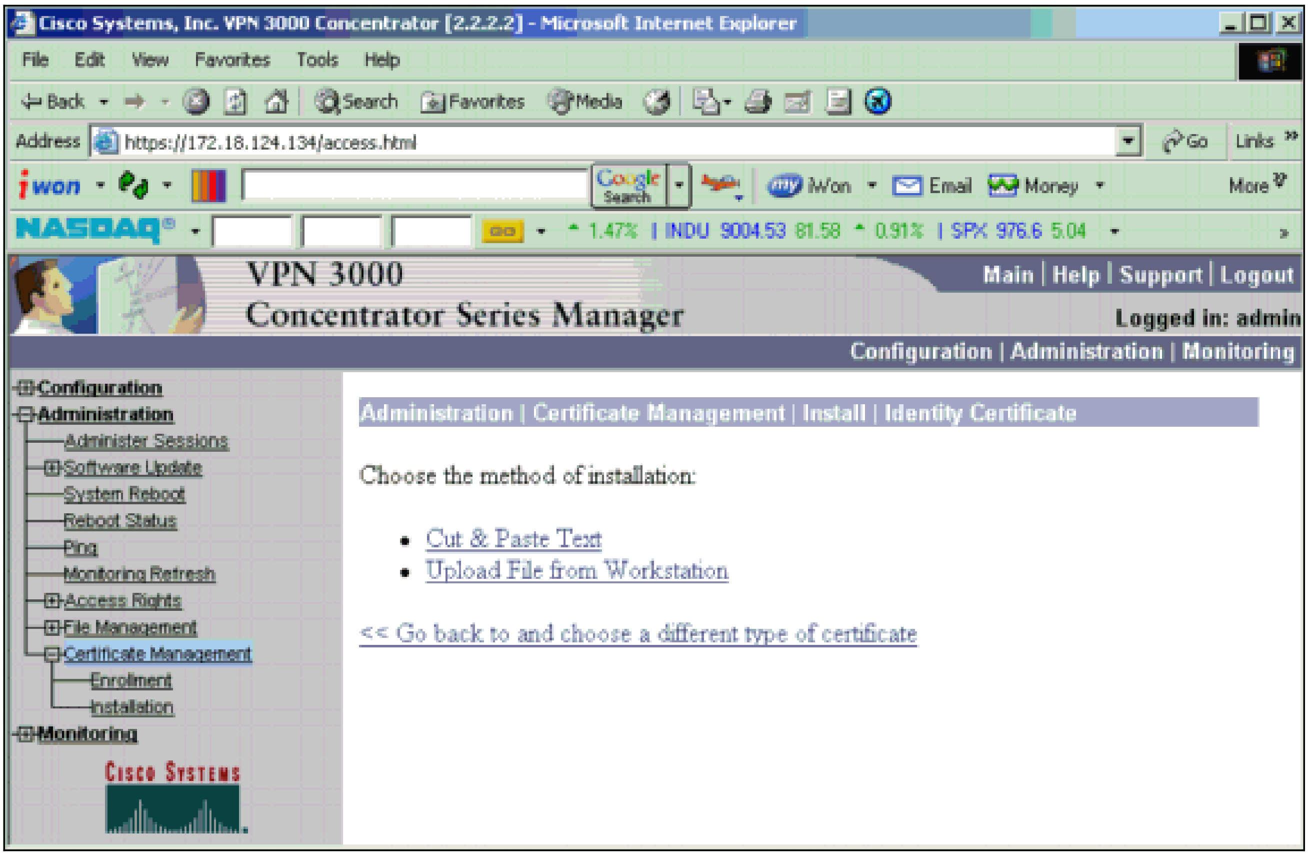
Enrollment Status

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altiga30 at Cisco Systems	N/A	05/22/2003	ID	Initial	Manual	In Progress	View | Install | Delete

<< Go back and choose a different type of certificate

16. Clique em **Carregar arquivo da estação de**

trabalho.


Cisco Systems, Inc. VPN 3000 Concentrator [2.2.2.2] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.18.124.134/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Cisco Systems

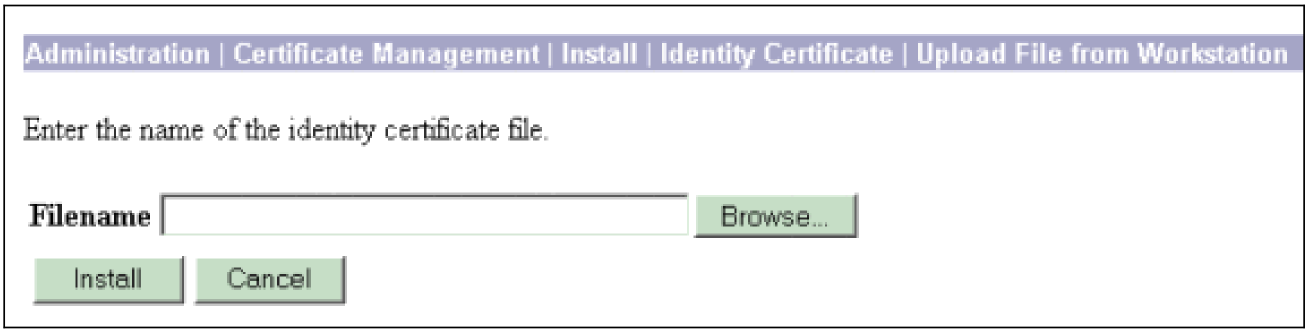
Administration | Certificate Management | Install | Identity Certificate

Choose the method of installation:

- Cut & Paste Text
- Upload File from Workstation

<< Go back to and choose a different type of certificate

17. Clique em **Procurar** e selecione o arquivo de certificado raiz que você salvou na unidade local.Selecione **Instalar** para instalar o certificado de identidade no VPN Concentrator. A Administração | A janela Gerenciamento de certificados é exibida como uma confirmação e seu novo certificado de identidade é exibido na tabela Certificados de identidade.



Administration | Certificate Management | Install | Identity Certificate | Upload File from Workstation

Enter the name of the identity certificate file.

Filename

Nota: Conclua estes passos para gerar um novo certificado se o certificado falhar.Selecione **Administration** > **Certificate Management**.Clique em **Excluir** na caixa Ações da listagem Certificado SSL.Selecione **Administration** > **System Reboot**.Selecione **Salvar a configuração ativa no momento da reinicialização**, escolha **Agora** e clique em **Aplicar**. Agora você pode gerar um novo certificado após a conclusão do recarregamento.

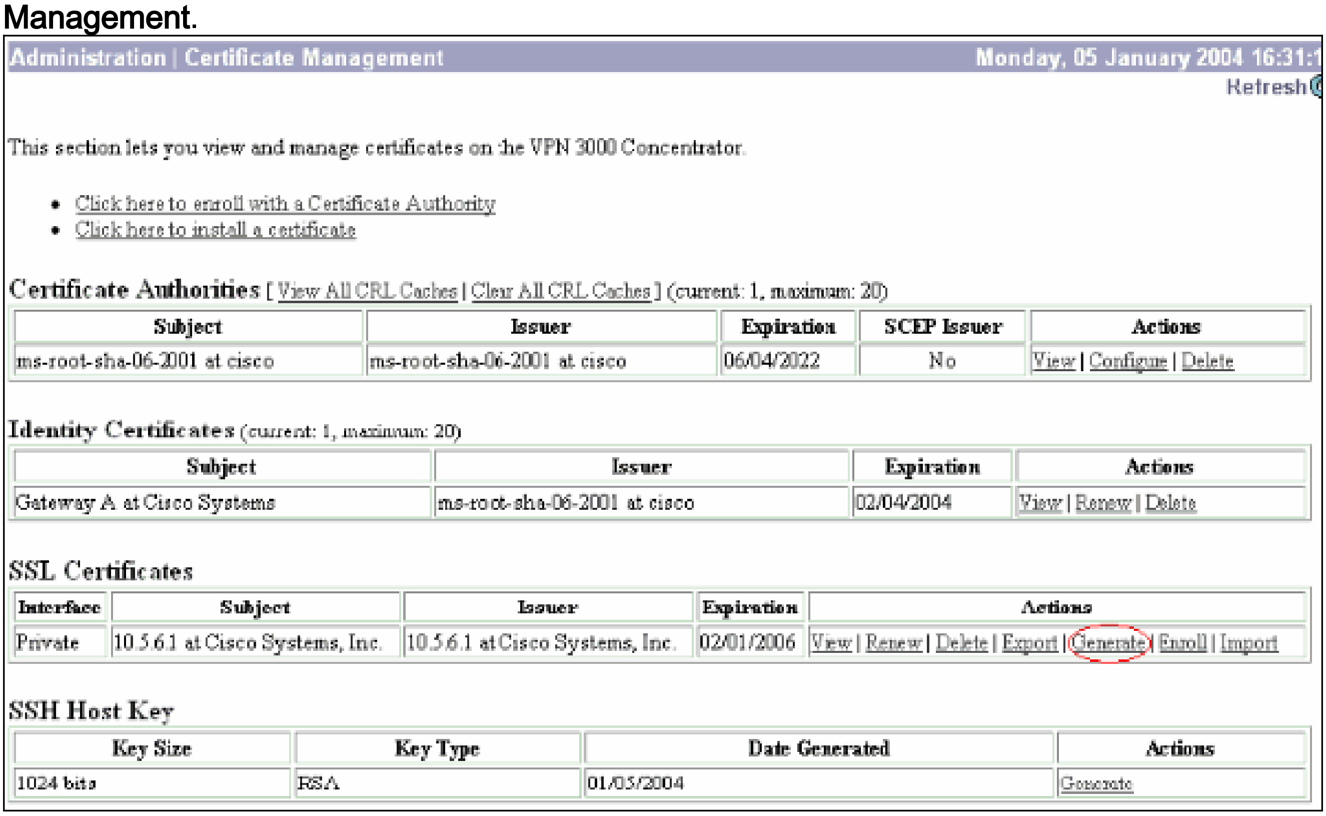
Instalar certificados SSL no VPN Concentrator

Se você usar uma conexão segura entre seu navegador e o VPN Concentrator, o VPN Concentrator exigirá um certificado SSL. Você também precisa de um certificado SSL na interface que usa para gerenciar o VPN Concentrator e para WebVPN, e para cada interface que termina os túneis WebVPN.

Os certificados SSL da interface, se não existirem, são gerados automaticamente quando o VPN

3000 Concentrator é reinicializado após a atualização do software VPN 3000 Concentrator. Como um certificado autoassinado é gerado automaticamente, esse certificado não é verificável. Nenhuma autoridade de certificação garantiu sua identidade. Mas esse certificado permite que você faça contato inicial com o VPN Concentrator usando o navegador. Para substituí-lo por outro certificado SSL autoassinado, faça o seguinte:

1. Escolha **Administration > Certificate Management**.



Administration | Certificate Management

Monday, 05 January 2004 16:31:1

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

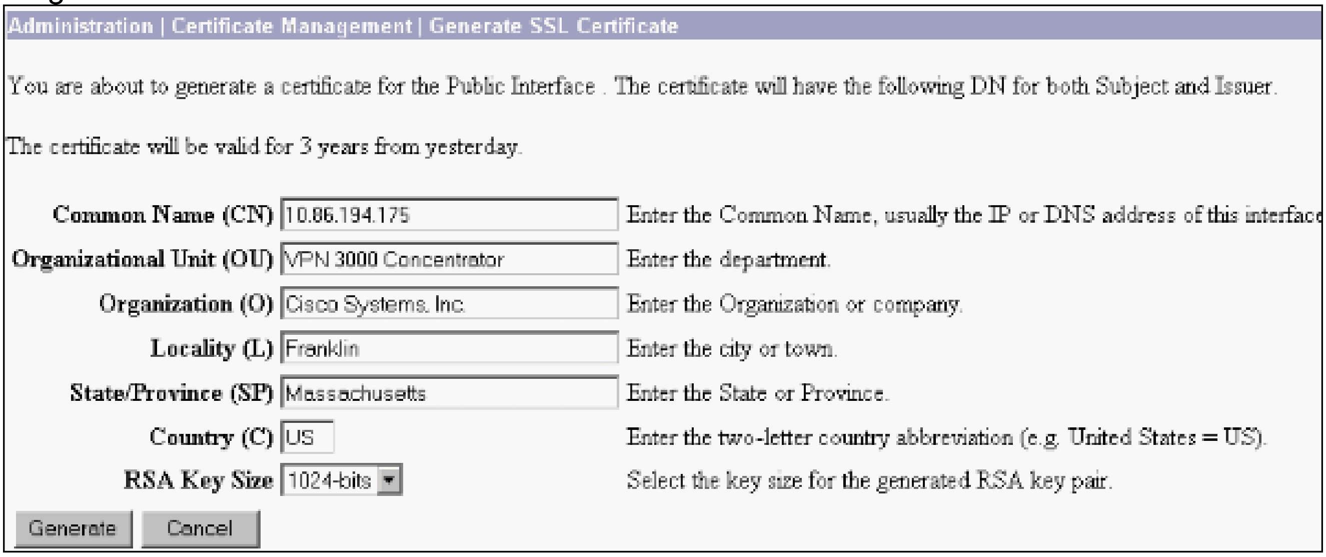
SSL Certificates

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. Clique em **Gerar** para exibir o novo certificado na tabela Certificado SSL e substituir o certificado existente.Essa janela permite configurar campos para certificados SSL que o VPN Concentrator gera automaticamente. Esses certificados SSL são para interfaces e para balanceamento de carga.



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)	10.86.194.175	Enter the Common Name, usually the IP or DNS address of this interface
Organizational Unit (OU)	VPN 3000 Concentrator	Enter the department.
Organization (O)	Cisco Systems, Inc	Enter the Organization or company.
Locality (L)	Franklin	Enter the city or town.
State/Province (SP)	Massachusetts	Enter the State or Province.
Country (C)	US	Enter the two-letter country abbreviation (e.g. United States = US).
RSA Key Size	1024-bits	Select the key size for the generated RSA key pair.

Se quiser obter um certificado SSL verificável (isto é, um certificado emitido por uma autoridade de certificação), consulte a seção Instalar certificados digitais no VPN Concentrator deste documento para usar o mesmo procedimento usado para obter certificados de identidade. Mas desta vez, na janela **Administração > Gerenciamento de**

Certificados > Inscrever, clique em **Certificado SSL** (em vez de Certificado de Identidade).**Observação:** consulte a *Administração |* Seção *de gerenciamento de certificado* do VPN 3000 Concentrator Reference Volume II: Administration and Monitoring Release 4.7 para obter informações completas sobre certificados digitais e SSL.

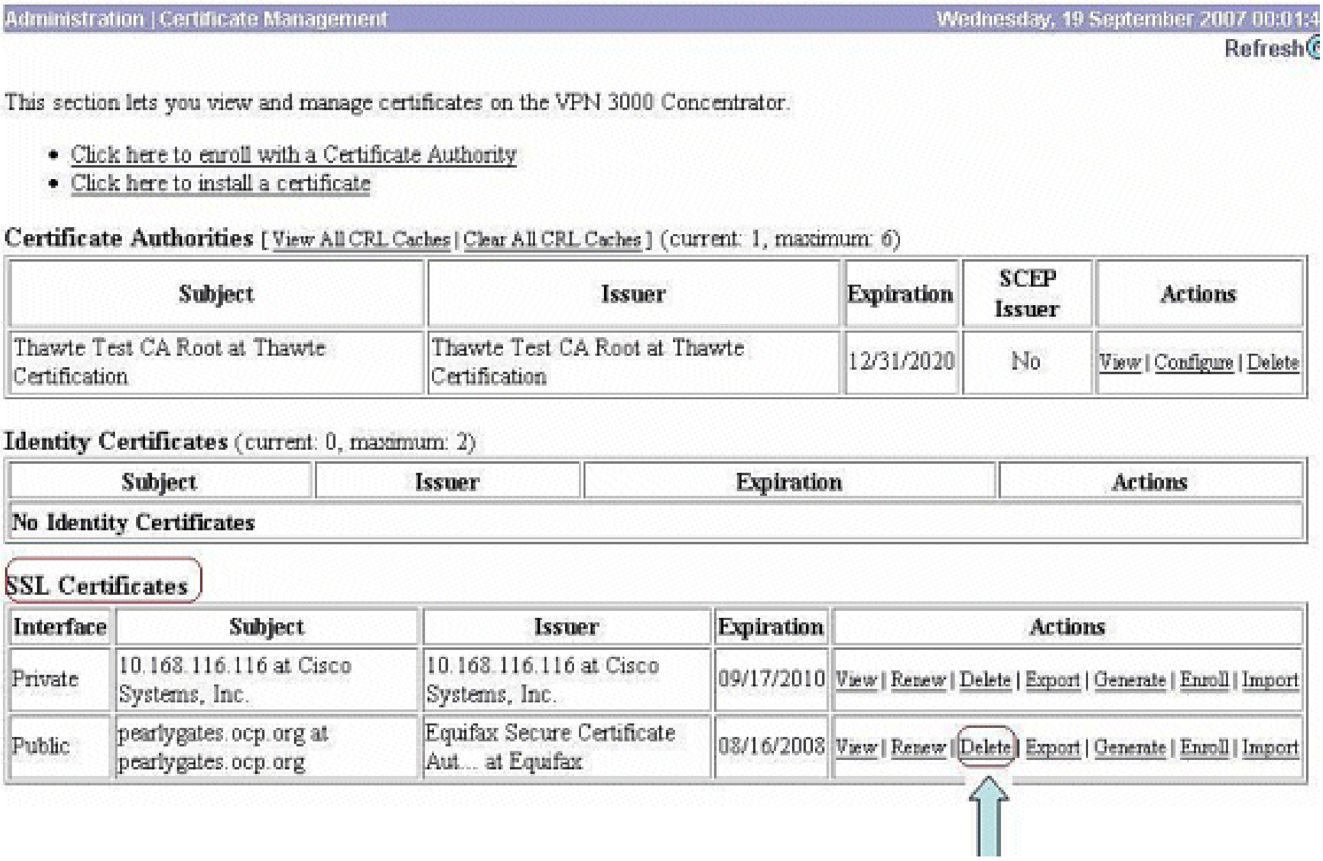
Renovar certificados SSL no VPN Concentrator

Esta seção descreve como renovar os certificados SSL:

Se for para o certificado SSL gerado pelo VPN Concentrator, vá para **Administration > Certificate Management** na seção SSL. Clique na opção **renovar** e ela renovará o certificado SSL.

Se for para um certificado concedido por um servidor de CA externo, faça o seguinte:

1. Escolha **Administração > Gerenciamento de Certificados >Excluir** em *Certificados SSL* para excluir os certificados expirados da interface pública.



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

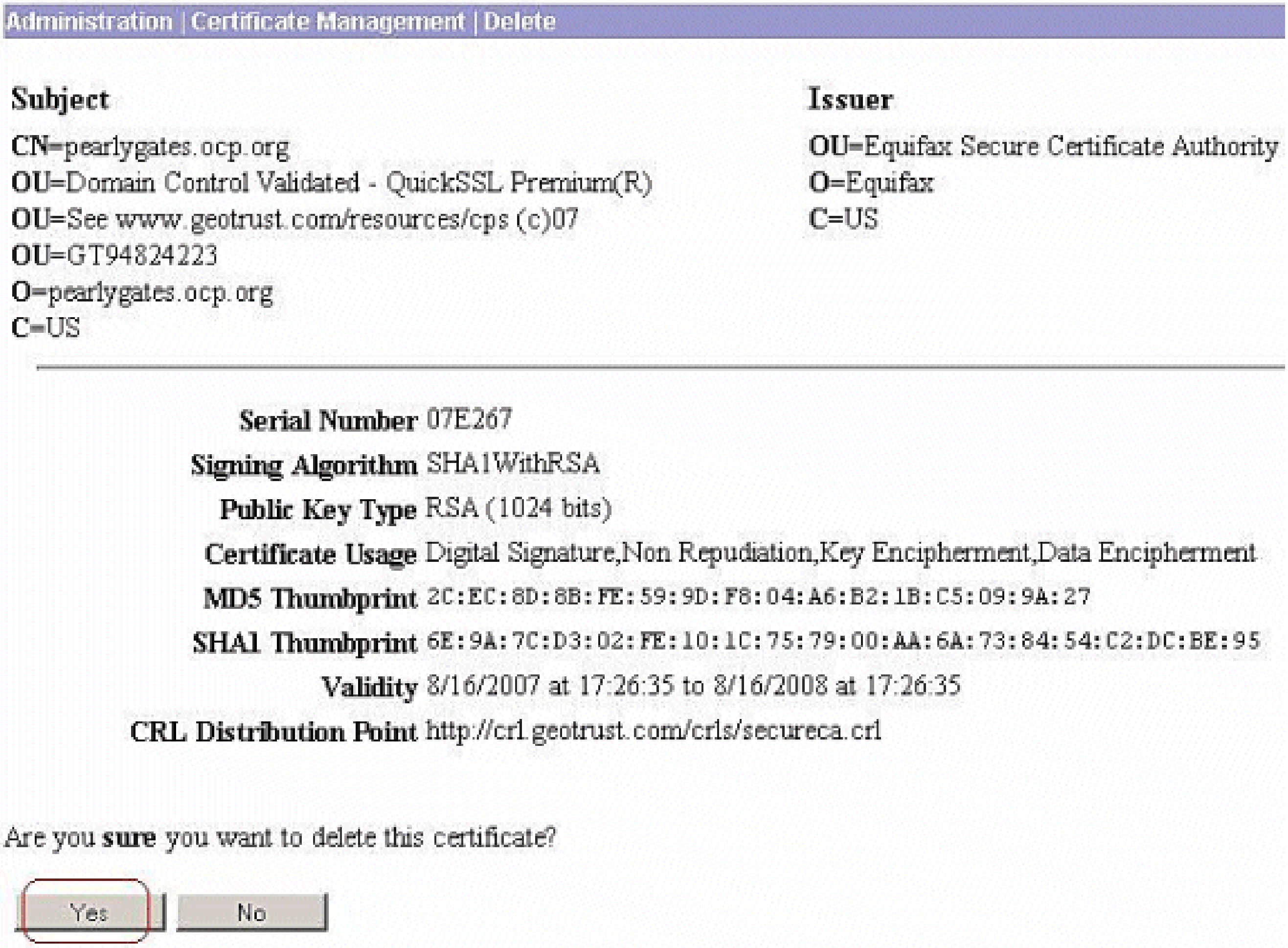
Identity Certificates (current: 0, maximum: 2)

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

Clique em **Sim** para confirmar a exclusão do certificado SSL.



Administration | Certificate Management | Delete

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

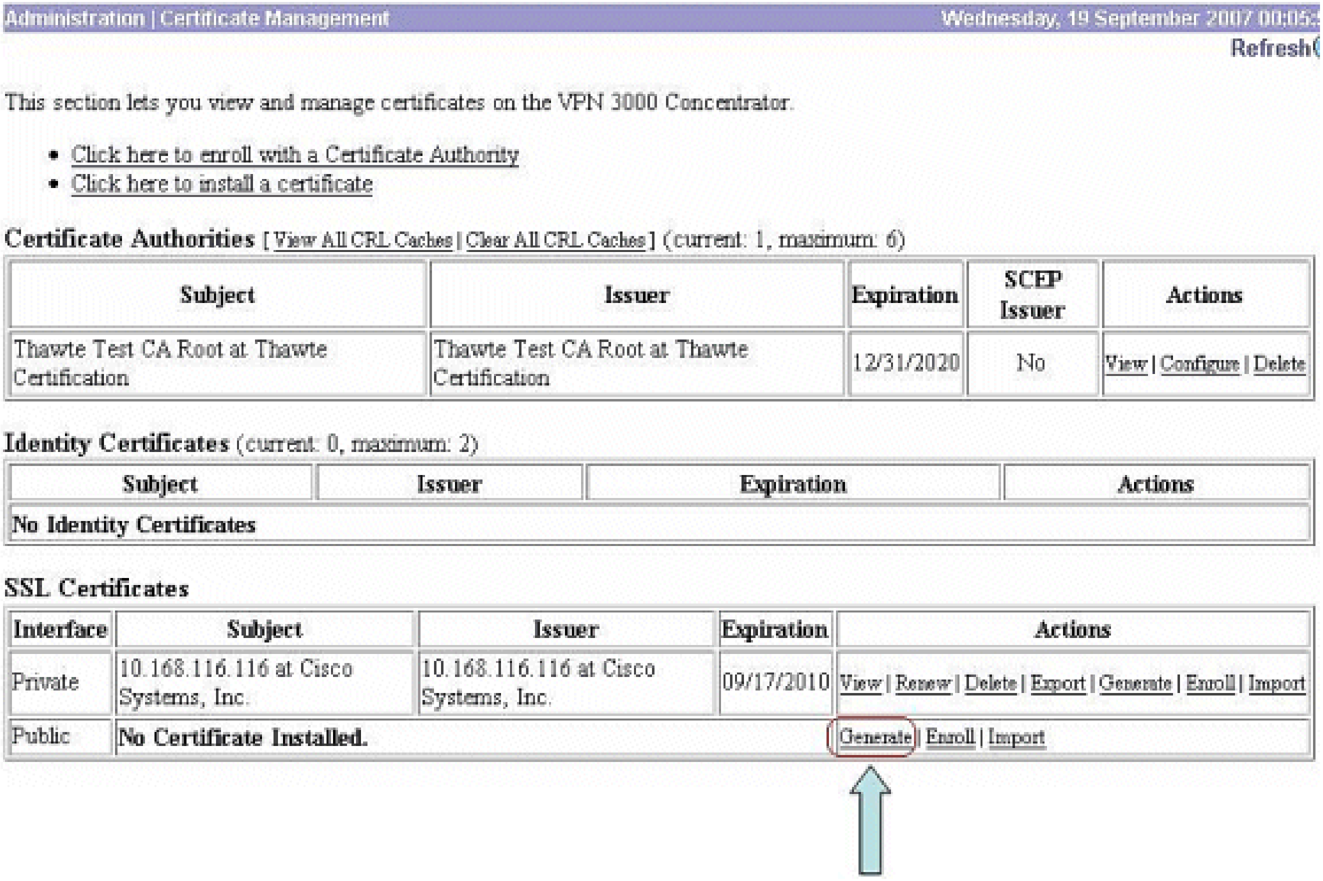
Issuer

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. Escolha **Administration > Certificate Management > Generate** para gerar o novo certificado SSL.



Administration | Certificate Management Wednesday, 19 September 2007 00:05:

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

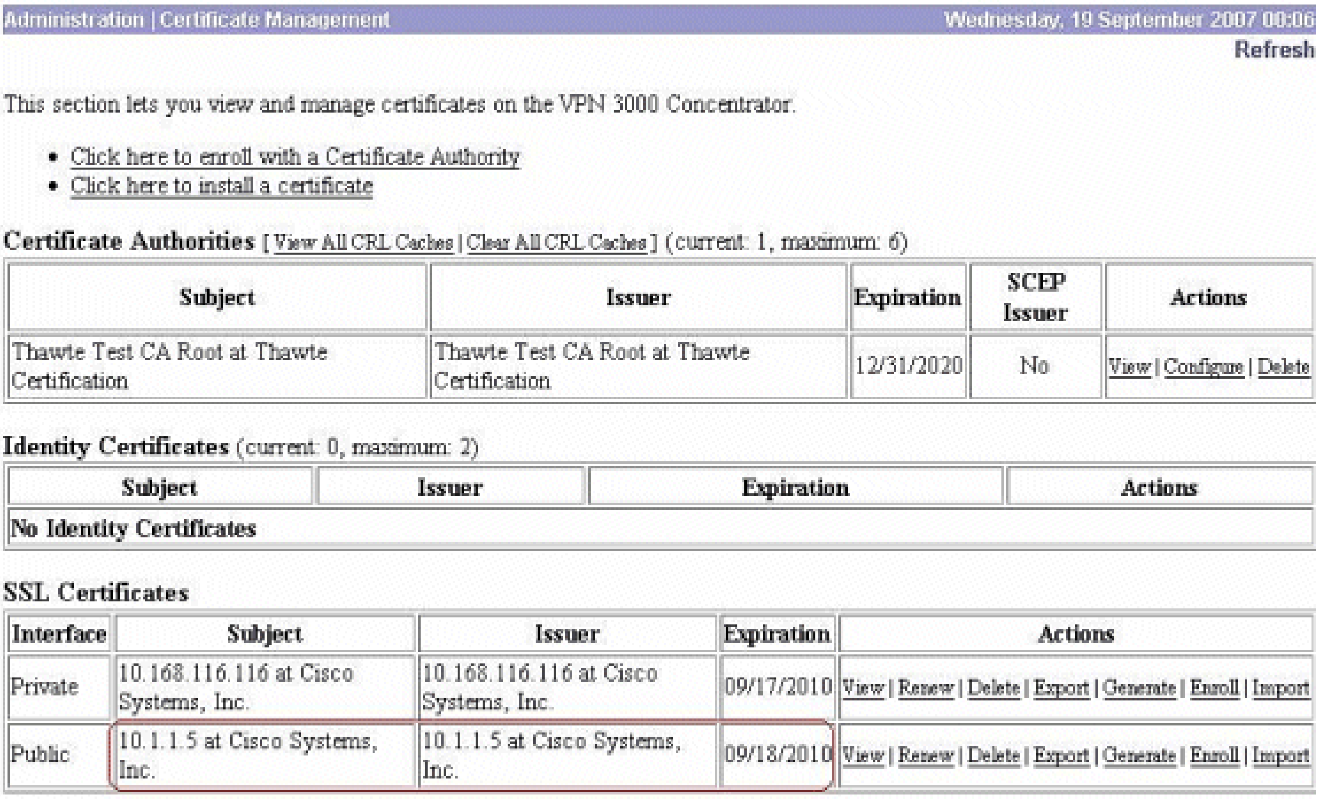
Identity Certificates (current: 0, maximum: 2)

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

O novo certificado SSL para a interface pública é exibido.



Administration | Certificate Management Wednesday, 19 September 2007 08:06

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

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems