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

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Installieren digitaler Zertifikate im VPN-Konzentrator Installieren von SSL-Zertifikaten im VPN Concentrator Verlängern Sie SSL-Zertifikate für den VPN Concentrator. Zugehörige Informationen

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 <u>zum</u> Szenario mit PIX/ASA 7.x<u>finden Sie</u> unter<u>So erhalten Sie ein digitales</u> 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

<u>Anforderungen</u>

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 <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Installieren digitaler Zertifikate im VPN-Konzentrator

Gehen Sie wie folgt vor:

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

auszuwählen.

Administration Certificate Management Enroll	
This section allows you to create an SSL or identity certificat VPN 3000 Concentrator to be enrolled into the PKI. The ce issue a certificate. The CA's certificate must be installed a certificate you requested.	e request. The identity certificate request allows the ertificate request can be sent to a CA, which will s a Certificate Authority before installing the
Choose the type of certificate request to create:	
Identity certificate SSL certificate	
<< Go back to Certificate Management	

 Wählen Sie Administration > Certificate Management > Enrollment > Identity Certificate aus, und klicken Sie auf Registrieren über PKCS10 Reguest(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. <u>Click here to install a new CA using SCEP before enrolling</u>.

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

 Füllen Sie die erforderlichen Felder aus, und klicken Sie dann auf Registrieren. Diese Felder sind in diesem Beispiel ausgefüllt. Common Name - Altiga30Organisationseinheit -IPSECCERT (die Organisationseinheit muss mit dem konfigurierten IPsec-Gruppennamen übereinstimmen)Organisation - Cisco SystemsLokalität - RTPBundesland -NorthCarolinaLand - USAVollqualifizierter 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				
Administration Certificate Management Enroll Identity Cer	tificate 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)	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.			
Enroll Cancel				

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

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 <u>File Management page</u> to delete the certificate request.
<u>Go to Certificate Management</u> <u>Go to Certificate Enrollment</u> Go to Certificate Installation

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

https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	驟
← Back - → - ② 🔄 🚮 ② Search ③ Favorites ③ Media 🕥 🖓 - 🎒 🗹 🖃 🕄	
Address 🗃 https://172.18.124.214/FILE/pkcs0001.txt	Links »
iwon - 🗞 - 📕 🖸 🔀 Search - 🚧 🏧 Won - 🖂 Email 🐼 Money - 🕅	4ore ¥
NASCAQ®	>
	^
MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRp22EzMDESMBAGA1UECxMJSVBTRUND RVJUMRYwFAYDVQQKEw1DaXNjbyBTeXNO2W1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDUSvcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQVJKoZIhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwO1oNMiqw4kmgIhIG2E/BIZc+xokG4rBp11rq4DkM J3XOVB8yiUkzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB DOGRWJg/dVvGAM2HKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqaSNv1cdLsQFPxV1 zVleLhhpRf0A4hw1 END NEW CERTIFICATE REQUEST	K
🕘 Done	11.

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

Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit. View Favorites Tools Help		
Gesch + + · G G G GSearch GFevorites GHistory	5- @	
Address 1 http://172.10.124.96/certsrv/		260 U
Microsoft Certificate Services - jfrahim-pc		Home
Welcome		
You use this web site to request a certificate for your web b will be able to securely identify yourself to other people over depending upon the type of certificate you request.	prowser, e-mail client, or other secure program. Once you acquire a certificat or the web, sign your e-mail messages, encrypt your e-mail messages, and m	ie, you tore
Select a task: C Retrieve the CA certificate or certificate revocation lis Request a certificate Check on a pending certificate	st	
	Ne	ot >.

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

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
4-Back + + - () () () () Search () Favorites () History () + ()	
Address Address http://172.18.124.96/certsrv/certrqus.asp	• (*Go) Lin
Microsoft Certificate Services Jitahim-pc	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request:	
Web Browser Certificate E-Meil Protection Certificate	
@ Advanced request	
	Next >

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.			
Microsoft Certificate Services - Microsoft Internet Explorer			-15
File Edit View Pavorites Tools Help			
4-Back + → - (2) (2) (2) Search (2) Favorites (3) History (2) - (2)			
Address 🖉 http://172.18.124.96/certsry/certrgad.asp	• •	₽G0]][#
Microsoft Certificate Senices Ifrahim-pc		He	ontre
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 authority (CA) will determine the certificates that you can obtain.	e certi	ificat	tion
C 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.		
C 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.			
	Nex	d>	I

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

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
+Back + + · ③ ③ ④ ④ @Search @Favorites @History □ - @	
Address Mtp://172.18.124.96/certsrvjcertrqst_asp	ເ∂ີ ເວັ] U
Microsoft Certificate Services - jfrahim-pc	Home
Submit A Saved Request	
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated t server) into the request field to submit the request to the certification authority (CA).	by an external application (such as a web
Saved Request:	
7FbNOQ/TmdWK0RBoUkDPPwBCAQUwDQYJKo21hvcN QLNTjSu7B3LupqKA1qF21BQfxG137D+wHEEp+6s4 Base64 Encoded MqG4AhkH Certificate Request (PKCS #10 or #7):	
Browse for a file to insert.	
Additional Attributes:	
	Submit >

9. Stellen Sie das Identitätszertifikat auf dem CA-Server

aus.							
Certification Authority			and a second second				_ 15
Action Yew 🗇 🔿 💽		3					
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)	10)7	DEGIN M	Takan Under Gubotistop All fasks II Issue Refresh Deny Help	3/23/2001 9:13 AM	GHOSTƏQUUR	30	Cisco Syste

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

vveiter.			
Microsoft Certificate Services - Microsoft Internet Explorer			-10
File Edit View Favorites Tools Help			
4+8ack - → - ◎ ② △ ②Search @Favortes ③ristory 2-3			
Address Phtp://172.10.124.96/certanv/		260	Ju
Microsoft Certificate Services /hahim-pc		Ho	me
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 ce will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, depending upon the type of certificate you request.	ntifica , and r	te, yoi nore	u
Select a task:			
C Retrieve the CA certificate or certificate revocation list			
Request a certificate			
Check on a pending certificate			
	N	< http://www.com	I

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. Save As					? X
Save in:	Desktop		•	← 🛍 👉 📰•	
History History Desktop My Documents My Computer	My Document My Computer My Network F	s: laces			
	File name:	certnew.cer		. •	Save
My Network P	Save as type:	Security Certificate			Cancel

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

Microsoft Certificate Services - Microsoft Internet Explorer	
Fée Edit - View Favorites Tools Help	
4-back - → - () () () () () Search () Favorites () History () - ()	
Address 1/172.18.124.96/certsrv/	▼ (² %)
Microsoft Certificate Services – jfrahim-pc	Hom
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure will be able to securely identify yourself to other people over the web, sign your e-mail messages depending upon the type of certificate you request.	program. Once you acquire a certificate, you s, encrypt your e-mail messages, and more
Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate C Check on a pending certificate	
- energia ponega concerta	News
	Prept >

14. Speichern Sie das Stammzertifikat auf Ihrem lokalen



Save As						<u>?</u> ×
Save in:	Desktop		•	* 📾 🔿	:::: · •	
History History Desktop My Documents My Computer	My Document: My Computer My Network P Certnew.cer	aces				
	File name:	certroot.cer				Save
My Network P	Save as type:	Security Certificate		X		Cancel

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.

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

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

Eisco Systems, Inc. VPN 3000 Cor	ncentrator [2.2.2.2] - Microsoft Internet Explorer	
File Edit View Favorites Tools	Help	
⇔Back • → • 🙆 🗿 🚮 🥘	Search 🗟 Favorites 🎯 Media 🎯 🗟 - 🎒 🖼	
Address 🙆 https://172.18.124.134/ao	cess.html	▼ 🖓 Go Links »
iwon - 🛯 - 📕	Cougle - 🦗 🍏	won 🔹 🖂 Email 🔛 Money 🔹 🛛 More 🎙
NASDAQ® -	. * 1.47% INDU 9004.53 81	.58 * 0.91% SPX 976.6 5.04 · »
VPN 3	000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Administration Administration Administration Administration Administration Software Update System Reboot Reboot Status Ping Montoring Retresh Brick Certificate Management Enrolment Installation Cisco Systems Cisco Systems	Administration Certificate Management I Choose the method of installation: • <u>Cut & Paste Text</u> • <u>Upload File from Workstation</u> << Go back to and choose a different type of	stall Identity Certificate

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.

Administration Certificate Management Install Id	entity Certificate Upload File from Workstation .
Enter the name of the identity certificate file.	
Filename	Browse
Install Cancel	

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.										
Administ	ration Certificate	e Managerr	nent				Mon	ıday, O	5 Januar <mark>y 200</mark> 4	16:31:1
									R	etresh (
This sectio • <u>Clic</u> • <u>Clic</u> Certifica	n lets you view and <u>& here to enroll with</u> <u>& here to install a ce</u> te Authorities [V	manage certi <u>a Certificate</u> r <u>tificate</u> 'iew All CRL (ficates on the VPN 1 Authority Caches Clear All CRI	3000 Concen	utrator. urrent: 1. max	inuur	: 20)			
	Subject		Issuer		Expirat	tion	SCEP Issuer		Actions	
ms-root-si	ha-06-2001 at cisco	ms-	root-sha-0é-2001 at	cisco	06/04/202	2	No	View	Configure Delete	
Identity	Certificates (cum Subject	ent: 1, maxima	un: 20)	Issuer			Expiration		Actions	
Gateway /	A at Cisco Systems		ms-root-sha-Dó-	2001 at cisco)		02/04/2004	View R	enew Delete	
SSL Cer	tificates Subject	ŧ	Issuer	1	Expiration			Action	2	
Private	10.5.6.1 at Cisco Sy	stems, Inc.	10.5.6.1 at Cisco Sy	stems, Inc.	02/01/2006	View	Renew Delete E:	mort 6	enerate Enroll Im	port
SSH Ho:	st Key									
	Key Size	ł	Сеу Туре		Date 6	iener	rated		Actions	
1024 bits		RSA		01/05/2004				Go	nozato	

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

Administration Certificate Management Generate SSL Co	ertificate
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.
Generate Cancel	

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

Zertifizierungsstelle ausgestelltes Zertifikat), lesen Sie den Abschnitt <u>Install Digital</u> <u>Certificates on the VPN Concentrator (Digitale Zertifikate installieren</u>) 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 <u>VPN 300</u> <u>Concentrator-Referenzvolumens II: Administration and Monitoring Release 4.7</u> 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

loschen.	
Administration Certificate Management	Wednesday, 19 September 2007 00:01:
	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			

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 Impor
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut at Equifax	08/16/2008	View Renew Delete) Export Generate Enroll Import

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

Subject

N=pearlygates.ocp.org	
U=Domain Control Validated - QuickSSL Premium(R)	
U=See www.geotrust.com/resources/cps (c)07	
)U=GT94824223	
)=pearlygates.ocp.org	
U=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
c	RL Distribution Point http://crl.geotrust.com/crls/secureca.crl

Are you sure you want to delete this certificate?

Yes	No

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

generieren.	
Administration Certificate Management	Wednesday, 19 September 2007 00:05:
	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	No Certificate Installed.		(Generate) Enroll Import
Public	No Certificate Installed.		(Generate) Enroll Import

angezeigt.

Administration | Certificate Management

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 <u>Renew</u> <u>Delete</u> <u>Export</u> <u>Generate</u> <u>Enroll</u> <u>Import</u>

Zugehörige Informationen

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