# 配置Cisco VPN 3000集中器4.7.x获得数字证书和 SSL证书

## 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>在VPN集中器上安装数字证书</u> <u>在VPN集中器上安装SSL证书</u> <u>在VPN集中器上更新SSL证书</u> <u>相关信息</u>

# <u>简介</u>

本文档包括有关如何配置Cisco VPN 3000系列集中器以使用数字或身份证书和SSL证书进行身份验 证的分步说明。

**注意:**在VPN集中器中,必须先禁用负载均衡,然后才能生成其他SSL证书,因为这会阻止证书生成。

请参阅<u>如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书,以便了解有关</u> PIX/ASA 7.x 中的相同方案的详细信息。

要了解有关Cisco IOS®平台的相同方案的详细信息,请参阅使用增强型注册命令的Cisco IOS证书 注册配置示例。

# <u>先决条件</u>

### <u>要求</u>

本文档没有任何特定的要求。

### <u>使用的组件</u>

本文档中的信息基于运行版本4.7的Cisco VPN 3000集中器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。 有关文档约定的更多信息,请参考 Cisco 技术提示约定。

# 在VPN集中器上安装数字证书

请完成以下步骤:

1. 选择管理>证书管理>注册以选择数字或身份证书请求。

Administration   Certificate Management   Enroll	
This section allows you to create an SSL or identity certificate request. The identity certificate request a VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, whi issue a certificate. The CA's certificate must be installed as a Certificate Authority before installing certificate you requested.	allows the ch will <i>2g the</i>
Choose the type of certificate request to create:	
Identity certificate     SSL certificate	
<< Go back to Certificate Management	

2. 选择Administration > Certificate Management > Enrollment > Identity Certificate, 然后单击 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. <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

 填写请求的字段,然后单击"Enroll"。本例中填写了这些字段。公用名— altiga30组织单位— IPSECCERT(OU应与已配置的IPsec组名匹配)组织- Cisco Systems位置— RTP州/省— 北 卡罗来纳国家— 美国完全限定域名— (此处未使用)密钥大小— 512注:如果使用简单证 书注册协议(SCEP)请求SSL证书或身份证书,则这些是唯一可用的RSA选项。RSA 512位 RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024位

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)	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. 单击"注册"后,将出现多个窗口。第一个窗口确认您已请求证书。

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.

- Go to Certificate Management
- · Go to Certificate Enrollment

Г

Go to Certificate Installation

系统还会打开一个新的浏览器窗口并显示您的PKCS请求文件。

https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	- 192
← Back - → - 🙆 🛐 🚮 🔞 Search 🝙 Favorites 🖓 Media 🧭 🔂 - 🚑 🖬 📄 🔞	
Address 🗃 https://172.18.124.214/FILE/pkcs0001.txt	Links »
iwon - 🗞 - 🔢 🖸 Coogle - 🦗 🎯 Won - 🖸 Email 🗠 Money -	More <sup>⊉</sup>
NASDAQ®	>
DEATH NEW ADDREDATE DEANDAR	^
<pre>MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRpZ2EzMDESMBAGA1UECxMJSVBTRUND RVJUHRYwFAYDVQQKEw1DaXNjbyBTeXNOZW1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDU5vcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQYJKoZIhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwO1oNMiqw4kmgIhIG2E/BIZc+xokG4rBpl1rq4DkM J3XOVB8y1UkzjvdIgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB DOdRWJg/dVvGAM2HKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqa5Nv1cdLsQFPxV1 zV1eLhhpRfOA4hw1 END NEW CERTIFICATE REQUEST</pre>	
Done	

## 5. 在您的证书颁发机构(CA)服务器上,突出显示该请求并将其粘贴到您的CA服务器中以提交您 的请求。单击 Next。

Microsoft Certificate Services - Microsoft Internet Explorer			
File Edit View Pavorites Tools Help			
4-Back			
Address 1 http://172.18.124.96/certsrv/	•	0	60
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 program. Once you acquire a will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail message depending upon the type of certificate you request.	certific s, and	ate. I mo	re re
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate			
	9	Next	>.

6. 选择"高**级请求"**,然后单**击"下一**步"。

Microsoft Certificate Services - Microsoft Internet Explorer	_ii
File Edit View Favorites Tools Help	
4-Back + + - ◎ ③ ④ ④ Search ⊕Favorites @History ◎ + @	
Address Abhtp://172.18.124.96/certsrv/certrqus.asp	
Microsoft Certificate Services jfrahim-pc	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request.	
Web Browser Centionte E-Mail Protection Certificate	
Advanced request	
	Next >

7. 选择Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file,然后单击Next。

Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit View Fevorites Tools Help		
4-Back + → - (2) (2) (2) Search (2) Favorites (3) History (2) - (2)		
Address Abhrp://172.18.124.96/certsry/certrqad.asp	•	(PGo Lin
Microsoft Certificate Sentces (frahim-pc		Home
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 authority (CA) will determine the certificates that you can obtain.	the cer	tification
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.	
<ul> <li>Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.</li> <li>You must have an enrollment agent certificate to submit a request for another user.</li> </ul>		
	Ne	< be

8. 将PKCS文件剪切并粘贴到Saved Request部分下的文本字段中。然后请点击**提交**。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
+Back - + - 3 3 3 3 Search ElFavorites Statory 2- 3	
Address Athp://172.18.124.96/certsrv/certrq.t.asp	💌 (🖓 Go 🗍 U
Microsoft Certificate Services itrahim-pc	Hom
Submit A Saved Request	
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request server) into the request field to submit the request to the certification authority (CA).	generated by an external application (such as a web
Saved Request: Provide Request: Provide Request: (PKCS #10 or #?): Recent for a file to insert.	
Additional Attributes:	
	Submit>

9. 在CA服务器上颁发身份证书。

Action View da -> (5) (2)						
J Burner There is a real oral of	5 69 18					
Tree Reg	quest ID Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)	7 BEGIN M	Takan Under Gribototop Al Tarks I Issue Refresh Deny Help	3/23/2001 9:13 AM	GHOSTENUUSR	05	Caco Syste

10. 下载根证书和身份证书。在您的CA服务器上,选择**Check on a pending certificate(检查挂起 的证**书),然后单**击Next(下一步**)。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
4+8ack • → · ② ② ③ ③ ③Search @Favorites @History ◎- ④	
Address 1 http://172.10.124.96/certsrv/	00 °S 💌
Microsoft Certificate Services ifrahim-pc	Hor
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or will be able to securely identify yourself to other people over the web, sign your e-m depending upon the type of certificate you request.	other secure program. Once you acquire a certificate, you nail messages, encrypt your e-mail messages, and more
Select a task:	
C Retrieve the CA certificate or certificate revocation list	
C Request a certificate	
Check on a pending certificate	
	Nand >

11. 选择Base 64 encoded,然后单击Download CA certificate on the CA server。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
+Back + + + () () () () Search ) Favorites () History () + ()	
Address D http://172.18.124.96/certsrv/certfrub.asp	• (≷©  u
Microsoft Certificate Services, 4 jitahim-pc	Home
Certificate issued	
The certificate you requested was issued to you.	
C DER encoded or re Base 64 encoded	
provide a contract of the second seco	
Download CA certification path	

Save As					? ×
Save in:	🚮 Desktop		• +	1	
History	My Documents Wy Computer My Network Pla	ačes			
Desktop					
My Documents					
My Computer					
Mu Matured P	File name:	certnew.cer			Save
My IXEWOIK F	Save as type:	Security Certificate		·	Cancel

13. 在CA服务器上,选择**Retrieve the CA certificate or certificate revocation list(检索CA证书或** 证书撤销列表)以获取根证书。然后,单击下一步。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit - View Favorites Tools Help	
4-back - → - () () () () Search () Favorites () History () - ()	
Address D http://172.18.124.96/certsrv/	<ul> <li></li></ul>
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 pr will be able to securely identify yourself to other people over the web, sign your e-mail messages, e depending upon the type of certificate you request.	rogram. Once you acquire a certificate, you encrypt your e-mail messages, and more
Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate	
	tient >

Save As						?×
Save in:	Desktop		•	+	<del>d</del>	
History History Desktop My Documents My Computer	My Document: My Computer My Network P Certnew,cer	s laces				
	File name:	certroot.cer			•	Save
My Network P	Save as type:	Security Certificate				Cancel

15. 在VPN 3000集中器上安装根证书和身份证书。为此,请选择Administration > Certificate Manager > Installation > Install certificate avaried via enrollment。在"Enrollment Status"下 ,单击Install。

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. 单击"**从工作站上传文件**"。



17. 单击**Browse**并选择您保存到本地驱动器的根证书文件。选择**Install**以在VPN集中器上安装身 份证书。管理 | Certificate Management窗口显示为确认,您的新身份证书显示在Identity Certificates表中。

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

**注意:如**果证书失败,请完成以下步骤以生成新证书。选择 Administration > Certificate Management。在SSL证书列表的"操作"(Actions)框中单击**删除**。选择**管理**>系**统重新启动**。 选择Save the active configuration at time of reboot,选择Now,然后单击Apply。重新加载 完成后,您现在可以生成新证书。

# 在VPN集中器上安装SSL证书

如果在浏览器和VPN集中器之间使用安全连接,则VPN集中器需要SSL证书。您还需要在用于管理 VPN集中器和WebVPN的接口上以及用于终止WebVPN隧道的每个接口上的SSL证书。

升级VPN 3000集中器软件后,当VPN 3000集中器重新启动时,接口SSL证书(如果不存在)将自动生成。由于自签名证书是自生成的,因此此证书不可验证。没有证书颁发机构保证其身份。但是 ,此证书允许您使用浏览器与VPN集中器进行初始联系。如果要将其替换为另一个自签名SSL证书 ,请完成以下步骤:

1. 选择管理>证书管理。

Idministration   Certificate Management Monday, 05 January 2004 16:31:1										
									Retresh	
This section <u>Clic</u> <u>Clic</u>	n lets you view and : k here to enroll with k here to install a cer	manage cert a Certificate tificate	ficates on the VPN 1 Authority	3000 Concer	atrator.		- 10			
certateat	Subject	EW ALCAL	lssuer	<u>r oacues</u> 1 (e	Expirat	ion.	SCEP Issuer	1	Actions	
ms-root-sh	na-06-2001 at cisco	ms-	root-sha-06-2001 at	cisco	06/04/202	2	No Vi		w Configure Delete	
(dentity (	Certificates (curre Subject	nt: 1, maxim	um: 20)	Issuer			Expiration		Actions	
Gateway A	at Cisco Systems		ms-root-sha-Dó-	oct-sha-D6-2001 at cisco 02/04/2			02/04/2004	4/2004 View   Renew   Delete		
SSL Cert	ificates									
Interface	Subject		Issuer		Expiration			Acti	ions	
Private	10.5.6.1 at Cisco Sys	stems, Inc.	10.5.6.1 at Cisco Sy	stems, Inc.	02/01/2006	View	<u>Renew</u>   <u>Delete</u>   <u>E</u>	xport	Generate Enroll   Import	
SSH Host Key										
	Key Size	1	Кеу Туре	Date Generated				Actions		
100411	024 bita RSA			01/05/2004 Generate				-		

# 2. 单击Generate以在SSL Certificate表中显示新证书并替换现有证书。此窗口允许您为VPN集中器自动生成的SSL证书配置字段。这些SSL证书用于接口和负载均衡。

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					

如果要获取可验证的SSL证书(即由证书颁发机构颁发的证书),请参阅本文档的<u>在VPN集中</u> 器上安装数字证书</u>部分,以便使用用于获取身份证书的相同过程。但是,此时,在 Administration > Certificate Management > **Enroll窗口**中,单击**SSL证**书(而不是Identity Certificate)。注意:请参阅管理 / VPN 3000集中器参考卷<u>II的证书管理部分:管理和监控版</u> <u>本4.7</u>,了解有关数字证书和SSL证书的完整信息。

# 在VPN集中器上更新SSL证书

本节介绍如何续约SSL证书:

如果这是VPN集中器生成的SSL证书,请转至SSL部分的Administration > Certificate Management。单击renew选项,然后该选项将更新SSL证书。

如果这是外部CA服务器授予的证书,请完成以下步骤:

### 1. 在SSL Certificates下选择Administration > Certificate Management >Delete,以便从公共接口 删除过期的证书。

Administration | Certificate Managemer

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

### 单击Yes以确认删除SSL证书。

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
re you :	ure you want to delete this certificate?

No

Yes

2. 选择Administration > Certificate Management > Generate以生成新的SSL证书。

#### Refresh(

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- · Click here to enroll with a Certificate Authority
- <u>Click here to install a certificate</u>

#### 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	<u>View   Renew   Delete   Export   Generate   Enroll   Import</u>
Public	No Certificate Installed.	Generate) Enroll   Import		
				$\widehat{\Omega}$

### 系统将显示公共接口的新SSL证书。

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

# 相关信息

- Cisco VPN 3000 系列集中器支持页
- IPsec 协商/IKE 协议
- <u>技术支持和文档 Cisco Systems</u>