# 配置VPN client 3.x获得数字证书

## 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>规则</u> 配置 VPN 客户端 <u>验证</u> <u>故障排除</u> 相关信息

# <u>简介</u>

本文档演示如何配置Cisco VPN Client 3.x以获取数字证书。

# <u>先决条件</u>

## <u>要求</u>

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于运行Cisco VPN Client 3.x的PC。

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。

### <u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则。</u>

## <u> 配置 VPN 客户端</u>

要配置 VPN 客户端,请完成以下步骤。

1. 选择Start > Programs > Cisco Systems Inc. VPN client > Certificate Manager以启动VPN Client Certificate Manager。

1	2				Accessories	•	
	Ø				Startup	•	
Red	:ycle Bin	į.		e	Internet Explorer		
				Ľ;	Outlook Express		
- 8				C	Microsoft Outlook		
	and the				Boson Software	•	
		N			PGP	+	
		New Orrice Document			Microsoft Excel		
		Open Office Documer	it 🛛	W	Microsoft Word		
					Internet Apps	÷	
	3	Windows Update		8	MSN Messenger Service		
	-		- 7		Windows Media Player		
	924	Programs			Microsoft TechNet	•	
	-	Documents	-,	3	Microsoft FrontPage		
		Documentes			Fix-It Utilities 3.0	•	
		Settings	۲		Administrative Tools	÷	
/er	6				Jasc Software	•	
er	2	Search			Tools	•	
0	2	Help			VMware	•	
ğ					Windows Media	÷	
2	No.	Run			HyperTerminal Private Edition	•	
MS		<b>A</b>			WS_FTP Pro	•	
P	Sin .	Log Off administrator		MS AF8	Cisco TFTP Server	E	💈 Certificate Manager 👘
Vin		Shut Down		3	Microsoft PowerPoint	6	Help Location: G:\Pro
>	47		L same		MusicMatch	1 6	Jug Viewer
	Start	🖸 🤤 🖸 🚫	DI		Napster	+	🧧 Uninstall VPN Client
				G	Cisco Systems Inc. VPN Client	28	VPN Dialer

2. 选择"个人证书"选项卡,然后单击**"新建**"。

ate requests that a CA h	NAMES AND A DESCRIPTION OF
	as yet to approve.
rtificates Enrollment Re	equests
5008	
	ertificates Enrollment Re

:IPsec无法完成对用户进行VPN连接身份验证的计算机证书。

 当VPN客户端提示您输入密码时,请指定密码以保护证书。任何需要访问证书私钥的操作都需 要指定的密码才能继续。

Certificate Password P	rotection
CISCO SYSTEMS	Password protecting your certificate provides an additional level of security. This password is optional. By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue. Note - File based enrollments require the password certificate is imported.
选择File,在Enrollment团 Enrollment - Network of Cisco Systems	Back Next > Cancel Help 页面上使用PKCS #10格式请求证书。然后,单击下一步。 or File : The enrolment wizard allows you to request a personal identity certificate from a Certificate Authority (CA). Network based enrollment allows you to connect directly
	To a LA over a network connection. File based enrollment will produce a certificate request file which you need to submit to your administrator. Please select the method you wish to proceed with: Enrollment type: Network File
	( <u>B</u> ack <u>N</u> ext > Cancel Help

5. 单击Browse,然后为证书请求文件指定文件名。对于文件类型,选择PEM Encoded Request File(\*.req)**,然后单**击"Save"。

Save As			? ×
Save in: 🚺	Desktop		* 💷 *
My Docum My Compu My Networ cases jazib ypn	ents in client2.req ter in client5.req rk Places		
File name:	client5.req		Save
Save as type:	PEM Encoded Request File	• (*.req)	Cancel

6. 在VPN Client Enrollment页面上单击Next。

Construction of the	To create an enrollment request file, please select the type of file you wish to generate.
CISCO SYSTEMS	Contact your network administrator if you are not sure which encoded file type is required.
	When you select a file extension in the Browse dialog the associated file type will be selected on this page.
	<u>F</u> ile name: *
	C:\My Documents\client5.req
	File type:
	Base 64 encoded (.req)
	O Binary encoded (.p1U)
	* Required Field
	* Required Fiel
	< Back Next > Cancel Help

7. 填写登记表上的字段。此示例显示字段:公用名=用户1部门= IPSECCERT(这应与VPN 3000集中器上的组织单位(OU)和组名称匹配。)公司=思科系统州=北卡罗来纳州国家/地区=美 国电邮= User1@email.comIP地址=(可选;用于指定证书请求的IP地址)域= cisco.com完成后 单击"下一步"。

	Enter your certificate e provided below.	enrollment information in the fields
CISCO SYSTEMS	Common Name (cn):*	User1
Illu	Department (ou):	IPSECCERT
	C <u>o</u> mpany (o):	Cisco Systems
	<u>S</u> tate (st):	NorthCarolina
-0	Co <u>u</u> ntry (c):	US
	<u>E</u> mail (e):	User1@email.com
	IP Address:	
- Contraction	Do <u>m</u> ain:	cisco.com
		* Required Fi

Enrollment - Summary		×
CISCO SYSTEMS	This is a summary of the information you have provided this certificate enrollment request. Select Finish to proceed with the enrollment or Back to make modifications.	for
	Enrollment: File - client5.req Certificate Store: Cisco Common Name: User1 Department: IPSECCERT Company: Cisco Systems State: NorthCarolina Country: US Email: User1@email.com IP Address: Domain: cisco.com	
	Back Finish Cancel Help	

9. 选择Enrollment Requests选项卡以检查VPN客户端证书管理器上的请求。

isco systems the client certilit	ate Manager
rsonal certificates identify you to peop signed by a certificate authority.	ole and hosts you communicate with ar
sertificate authority (CA) is an organiza	ation that issues certificates
rollment requests are certificate reque	ets that a CA has yet to approve
comment requests are certificate reque	sis india CA has yei to approve.
ersonal Certificates   CA Certificates	Enrollment Requests
Certificate	Store
User5	Request
	<u>Options</u> •

- 10. 同时启动证书颁发机构(CA)服务器和VPN客户端接口以提交请求。
- 11. 选择Request a certificate(请求证书),然后单击CA服务器上的Next(下一步)。

Back	
Agdecc 101 Into //192169250/cetuw/	■ 3 <sup>2</sup> Eo   Links *
Microsoft Certificate Services — verificaence	Hama
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure progr will be able to securely identify yourself to other people over the web, sign your e-mail messages, enco depending upon the type of certificate you request.	ram. Once you acquire a certificate, you rypt your e-mail messages, and more
Select a task: C Retrieve the CA certificate or certificate revocation list R Request a certificate C Check on a pending certificate	
	Next3
] Does	😨 listenat
为请 <b>求类</b> 型选择"高级请求",然后单 <b>击"下一步</b> "。	
Biccosoft Centricato Services - Historial Informat Explorer Ele Edit View Favartes Iools Help	
Sack torvivid Stop Hetesh Home Search Favorites History Mail Fint Address @ http://192.168.2.50/cetorv/cetropus.asp	•
MUCHOSOM CADIFICIAL SEMICES - WILLASSENAR	
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request:	
Web Browser Certificate E-Mail Protection Certificate	

- B

Links

Internet

13. 在"Advanced Certificate Requests"下,选择"Submit a certificate request using a base64 encoded PKCS #10 file"或"renewal request using a base64 encoded PKCS #7 file",然后单 击Next。

8] Done

Microsoft Certificate Services - Microsoft Internet Explorer	2 8 X
Elle Edit View Fgronkes Iools Help	19
Hande Frankrid Stop Refeets Home Search Fevorities History Mail Print	
Address 🕘 http://192.168.2.50/cettorv/cetropad.exp	▼ ∂Go   Links *
Microsoft Certificate Services – win2kservor	Elome -
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the prauthority (CA) will determine the certificates that you can obtain.	olicy of the certification
O 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 egent certificate to submit a request for another user.</li> </ul>	
	Next >
8) Done	2 Internet

# 14. 突出显示VPN Client请求文件,并将其粘贴到Saved Request下的CA服务器。然后请点击**提** 交。

For For Terr	Fgwantes Iools Help	
🕹 🖕 🤿 Back Freverd	Stop Refeet Home Search Fevorites History Mail Print	
ddiese 💽 Mip://193	2.168.2.50/cetrm/cetrpt.arp	▼ (∂Go )I
170000000000000000000000000000000000000		
AICPOSON CERTICS	ze Sentes → wrzksenar	ti sin
ubmit A Save	d Request	
aste a base64 erver) into the r	i encoded PKCS #10 centricate request or PKCS #7 renewal request generated by an external application (such a request field to submit the request to the certification authority (CA).	is a web
0110171110 0101	equeer new reactions are requeer to an existence on dealering (en).	
aved Request		
	BEGIN NEW CERTIFICATE REQUEST	
Base64 Encoded	HIBGJCBXQIBADBINKAWDGTDVQQDFACBYXL022AO BOGwDOYDVOQKFAZbbHRy22ExETAPBoNVBAcTCGZy	
ertificate Request	YTELMARGA1UEBhMCdXMwXDANBgRqnk109wOBAQEF	
(PKCS #10 or #7):	n+ftsc6JkDkIGSI6wGOgyuBwSO6YS7Ds57Yu59em Hi3teve/keOkkAkAFMADGCSeGSTD3D0FEBAUAA0FA =	
	A STATE OF	
	Browse for a file to insert.	
ditional Attribu	doe:	
Attributes:		
	x x	
		Submit >
	-	

15. 在CA服务器上,为VPN客户端请求颁发身份证书。

Certification Authority Action View ↓ ← → €					
Tree	Request ID Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/
Certification Authority (Local) frahm-pc Revoked Certificates Ssued Certificates Pending Requests Failed Requests	EGN NG	Al Tasks I Inder Submission Al Tasks I Issue Refresh Help	3/23/2001 9:13 AM	GHOST2KJUSR	US

16. 将根证书和身份证书下载到VPN客户端。在CA服务器上,选择**Check on a pending** certificate,然后单击Next。

Microsoft Certificate Services - jfrahim-pc
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:
C Retrieve the CA certificate or certificate revocation list
C Request a certificate
Check on a pending certificate
Next >

### 17. 选择Base 64 encoded。然后单击在CA服务器上下载CA证书。

unergent certificate gettiefen - Tunnur he				Hon
Certificate Issued				
C DER encoded or C B Download CA certificate Download CA certification	ued to you. Far Download Saving Centrew C Save As Estimated Download Transfer tr P Close I My Do My Do	Save in: Save in: My Douller My Computer My Network I Computer My Network I Computer Noton	As Places	212
		File name	client cet.cer.	<ul> <li>Save</li> </ul>

18. 从Retrieve the CA Certificate or Certificate Revocation List页面选择要下载的文件,以获取 CA服务器上的根证书。然后,单击**下一步**。

Microsoft Certific	cate Senices - jfrahim-pc				<u></u>				Home
Retrieve The	CA Certificate Or Certification path to allow	ficate Rev	ocation List	ertificates issi	ued from this	certification	authority	1.	
It is not necess because the C. Choose file to	ary to manually install th A certification path will I download:	Suma		.6		icate from	n this ce	rtificatio	on authority,
CA Certificate	Current [irehim-pc(2)] Previous [irehim-pc(1)] Previous [irehim-pc] C DER encoded or Download CA certifica Download CA certifica Download latest certifica	certnew.cer Estimated to Download to Transfer sals	Save As Save in: Ristory Desktop My Documents	My Documents My Computer My Network Pl Cares jazb Vpn client_cert.cer	S. laces		+ (1)		1×
			My Network P	File name: Save as type:	client_root_cert Security Certific	cer	_	•	Save Cancel

19. 选择**Certificate Manager > CA Certificate > Import on the VPN Client**,然后选择根CA文件 以安装根证书和身份证书。

	Open		? X
ization that issues certificates.	Look in: M Desktop	-	* 68+
uests that a CA has yet to approve.		The Property of the Property o	
	My Documents Elient_cert.cer		
S Enrollment Requests	My Computer Enclient_root_cert.cer		
Store	ases		
1.0000	jazib		
Import Certificate - Source 🦳 👘	D vpn		
The certifi imported fu			1
CISCO SYSTEMS importing i	File name: client_root_cert.cer		Open
below.	Files of type: X 509 DEB Files (* der * cer)		Cancel
Certifica	(These spectrum is a spectrum	12 7	/
C Micro	osoft certificate:		
	<u>×</u>		
Prile:			
	Browse		
Import pass	word		
K Back	Next> Cancel Help		

20. 选择**Certificate Manager > Personal Certificates > Import**,然后选择身份证书文件。

Import Certificate - Sou	irce	×
Cisco Systems Intellingual III.	The certificate source ident imported from. Additionally, importing is protected by a p below. Certificate source: Microsoft certificate: File:	tifies where the certificate is if the certifcate you are password, please enter it
Open	Import password:	Cancel Help
Look in: Desktop		
My Documents My Computer My Network Places acases jazib ypn	client_cert.cer	
File name: client_cr	ert.cer	Open
Files of type: X.509 D	EB Files (* der * cer)	Cancel

21. 确保身份证书显示在"个人证书"选项卡下。

Cisco Systems VPN Clier	nt Certificate Manager	
Personal certificates identify y are signed by a certificate aut	you to people and hosts you communication the temperature of temperatu	ate with and
A certificate authority (CA) is a	an organization that issues certificates.	
Enrollment requests are certifi	icate requests that a CA has yet to app	rove.
(5)		
Personal Certificates   CA C	Certificates Enrollment Requests	
Certificate	Store	
User5	Cisco	
Stores: <all></all>	▼ <u>N</u> ew	otions 👻

22. 确保根证书出现在CA Certificates选项卡下。

signed by a certificate a	uthority.
ertificate authority (UA) is colliment requests are port	an organization that issues certificates.
ionment requests are cert	incare requests that a CA has yet to applove.
ersonal Certificates	Certificates Enrollment Requests
Certificate	Store
jfrahim-pc	CA

## <u>验证</u>

当前没有可用于此配置的验证过程。

# <u>故障排除</u>

当您尝试向Microsoft CA服务器注册时,它可能会生成此错误消息。

Initiating online request Generating key pair Generating self-signed Certificate Initiating online request Received a response from the CA Your certificate request was denied 如果收到此错误消息,请参阅Microsoft CA日志了解详细信息,或参阅这些资源了解详细信息。

- Windows找不到处理请求的证书颁发机构
- XCCC:当您请求安全会议的证书时,会出现"Your Certificate Request was Denied"错误消息

# 相关信息

- IPsec 协商/IKE 协议
- <u>技术支持和文档 Cisco Systems</u>