デジタル証明書を取得するための VPN Client 3.x の設定

内容

<u>概要 前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>VPN クライアントの設定</u> <u>確認</u> <u>トラブルシュート</u> <u>関連情報</u>

概要

このドキュメントでは、デジタル証明書を取得するように Cisco VPN Client 3.x を設定する方法 について説明します。

<u>前提条件</u>

<u>要件</u>

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN Client 3.xが稼働するPCに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法』を参照してください。</u>

VPN クライアントの設定

VPN Clientを設定するには、次の手順を実行します。

1. [Start] > [Programs] > [Cisco Systems Inc. VPN client] > [Certificate Manager] の順に選択して、VPN Client Certificate Managerを起動します。



2. [Personal Certificates]タブを選択し、[New]をクリックします。

Personal certificates identify are signed by a certificate au	you to people and hosts you communicate athority.	with and
A certificate authority (CA) is	an organization that issues certificates.	
Enrollment requests are certi	ficate requests that a CA has yet to approv	/e.
Personal Certificates CA (Certificates Enrollment Requests	40
Certificate	Store	
Stores: ZAIN	Nou Ref	
Stores. TANK		2115
in the second		

*続*のユーザを認証するマシン証明書は、IPsecでは実行できません。

3. VPN Clientからパスワードの入力を求められたら、証明書を保護するためのパスワードを指 定します。証明書の秘密キーへのアクセスを必要とする操作を続行するには、指定されたパ スワードが必要です。

Certificate Password Pr	otection	×
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.	2
	Note - File based enrollments require the password used here to be re-entered when the approved certificate is imported. Password: Confirmation Password:	
	Back Next > Cancel Help	

4. [Enrollment] ページで[File]を選択し、PKCS #10形式を使用して証明書を要求します。次に 、[Next] をクリックします。

rollment - Network o	The enrollment wizard allows you to request a personal	×
	identity certificate from a Certificate Authority (CA).	
CISCO SYSTEMS	Network based enrollment allows you to connect directly	Ų
aullin aullin -	to a CA 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:	1
	C Network	
		0
(***		
<	: <u>Back N</u> ext> Cancel Help	

5. [Browse]をクリックし、証明書要求ファイルのファイル名を指定します。ファイルの種類として、[PEM Encoded Request File (*.req)]を選択し、[保存]をクリックします。

ave As		?)
Save in: [Desktop	📸 🎹 -
My Docum My Compu My Netwo cases	ents e client2.req iter <mark>e client5.req</mark> rk Places	
🛄 jazib 🔁 vpn		
	client5 reg	 Caue
Flie name:	Telleritoried	Jave

6. [VPN Client Enrollment]ページで[Next]をクリックします。



 7. 登録フォームのフィールドに入力します。次の例は、フィールドを示しています。共通名= User1部門= IPSECCERT(これは、VPN 3000コンセントレータの組織単位(OU)とグループ 名と一致する必要があります)。会社=シスコ州=ノースカロライナ国=米国電子メール= User1@email.comIPアドレス=(オプション;証明書要求のIPアドレスを指定するために使用 される)ドメイン= cisco.com完了したら、[Next] をクリックします。

October Oversetter	provided below.	enroliment information in the fields
CISCO SYSTEMS	Common Name (cn):*	User1
illinillin	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
SO A	IP Address:	
	Do <u>m</u> ain:	cisco.com
		* Required Field

8. <u>[完了]をク**リック**して、登録を続行します。</u>

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

9. [Enrollment Requests]タブを選択して、VPN Client Certificate Managerの要求を確認します

ersonal certificates ide	entify you to peop	le and hosts you communicate	e with
e signed by a certifica	ate authority.		
certificate authority (C	CA) is an organiza	ition that issues certificates.	
nrollment requests are	certificate reque	sts that a CA has yet to approv	ve.
Personal Certificates	CA Certificates	Enroliment Requests	
Certificate		Store	
User5		Request	
		Optic	ons ◄
		<u>Optia</u>	ons 🖣

- 10. 認証局(CA)サーバとVPN Clientインターフェイスを同時に起動して、要求を送信します。
- 11. [Request a certificate]を選択し、CAサーバで[Next]をクリックします。

Historell Celificale Services - Missealt Internet Explana	
Ein Edi Yew Faroten Jack Heb	5 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Arr	
(gdscs 42) Mp //182 168 2 50/centrol	→ 1 ² Eo Units
Microsoft Cartificata Services verziesarver	Barna
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. (will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt y depending upon the type of certificate you request.	Once you acquire a certificate, you our e-mail messages, and more
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate C Checker or certificate	
C Check on a periong berolicate	
	Nunt >
1 Passa	

12. <u>要求の**種類に対**して[Advanced request]を選択し、[Next]をクリックします。</u>

Microsoft Cectificale Services - Microsoft Internet Explorer	_ 6 2
Elle Edit View Favorites Iools Help	
Sack Fronted Stop Reflect Home Search Fevories History Mail Print	
Address 🕘 http://192.168.2.50/centurv/centrquis.esp	▼ PGo Links
Microsoft Certificate Sentces win2ksener	tiene
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request:	
Mets Environment Centrificate	
© Artvanced request	
< romanaa aagaala	
	Next>
B) Droe	a leterest

13. [Advanced Certificate Requests]で、[Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file]を選択し、 [Next]をクリックします。

Microsoft Certificate Services - Microsoft Internet Explorer	_ 8 ×
Elle Edit View Favorites Iools Help	
→ → ② ☑ ③ ③ ③ ③ ③ Back Finound Stop Retech Home Search Favorites History Mail Print	
Address @ http://192.168.2.50/cettorv/cetrgad.asp	💌 🔗 Go 🔋 Linka 🏁
Microsoft Certificate Services - win2kserver	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note authority (CA) will determine the certificates that you can obtain.	e that the policy of the certification
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.	
	Next >
8) Done	💌 💼 Internet

14. VPN Client要求ファイルを強調表示し、[Saved Request]の下のCAサーバに貼り付けます。

火に、 [SUDMII] をクリックします。 到Microsoft Carlificate Services - Microsoft Internet Explorer		- 8 -
Elle Edit View Favorites Iools Help		
tree → O D An O D A D A D A D A D A D A D A D A D A D		
Address 🕘 http://192.168.2.50/cetturv/cettrpd.asp		5 Links
Microsoft Cartificate Senires - worksenor		lone
		No.
Submit A Saved Request		
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external a server) into the request field to submit the request to the certification authority (CA).	epplication (such as a web	>
Saved Request:		
Base64 Encoded Certificate Request (PKCS #10 or #7): Base64 Encoded Base64		
Additional Attributes:		
Attributes:		
	Submit >	
		-
	nesete your post and an	2

15. CAサーバで、VPN Client要求のID証明書を発行します。

Action View					
Tree	Request ID Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/
Certification Authority (Local)	EGIN NF	Al Tasks > Issue Refresh Help	3,23/2001 9:13 AM	GHOST2K/JUSR	US

16. ルート証明書とID証明書をVPN Clientにダウンロードします。CAサーバで、[Check on a pending certificate]を選択し、[Next]をクリックします。

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. [Base 64 encoded] を選択します。次に、CAサーバで**[Download CA certificate]を**クリックします。

Microsoff Certificate Services - jfrahim-pc					Home
Certificate Issued The certificate you requested was issue C DER encoded or C Ba Download CA certificate Download CA certification	ed to you. Fde Download Saving cetherer of Estimated Download Transfer rr I Close 1 I Clos	Desktop My Documents My Computer My Network Place cases isab isab	15	◆ 個 🗗 🗊・	2 ×
	My Network P	File name:	client_cert.cer Security Certificate		Save Cancel

18. [Retrieve the CA Certificate or Certificate Revocation List]ページからダウンロードするファ イルを選択し、CAサーバのルート証明書を取得します。次に、[Next] をクリックします。

Microsoft Certific	cate Senices - jfrahim-pc					<u>.</u>					Home
Retrieve The	CA Certificate Or Certif	ficate Revo	cation List								
Install this CA of It is not necess because the C.	certification path to allow ary to manually install th A certification path will t	your compi	iter to trust c	ertificates issu	ued from	this certific	ation : e from	autho n this	cer	tificatio	on authority,
Choose file to CA Certificate:	Ourrent (frehim-pc(2)) Previous (frehim-pc(2))	Saving certnew.cer	ave As				-	-	an a		<u>?[x</u>
	C DER encoded or Download CA certifica Download Iatest certifica	Estimated tr Download tr Transfer sats I Close th	Save in: Windowy Decktop My Documents Documents	My Decuments My Computer My Network Ple cases jaab Vpn client_cert_cer	aces			+	(i)) (
			My Network P	File name: Save as type:	client_roo Security 0	L_cert.cer Certificate				•	Save Cancel

19. [Certificate Manager] > [CA Certificate] > [Import on the VPN Client] を選択し、ルートCAフ ァイルを選択して、ルート証明書とID証明書をインストールします。

	Open		? X
ization that issues certificates.	Look in: M Desktop	+ + = =	* 60+
uests that a CA has yet to approve.			
s Enrollment Requests	My Documents Client_cert.cer My Computer My Network Places		
Store	iazib vpn		
The certifi imported fr	File name:	r	Open
below.		L	open
Certifica	Files of type: X.509 DER Files (".der;".cer)	<u> </u>	Cancel
C Mich	rosoft certificate:		
Import pas	sword:		
	Next > Cancel Help		

20. [Certificate Manager] > [Personal Certificates] > [Import] を選択し、ID証明書ファイルを選 択します。

Import Certificate - Sou	rce X
CISCO SYSTEMS	The certificate source identifies where the certificate is imported from. Additionally, if the certificate you are importing is protected by a password, please enter it below. Certificate source: Microsoft certificate: File: Browse Import password:
Open Look in: Desktop	Back Next > Cancel Help ? ×
My Documents My Computer My Network Places Cases jazib ypn File name:	Client_cert.cer
Files of type: X.509 D	ER Files (*.der;*.cer)

21. ID証明書が[Personal Certificates]タブに表示されていることを確認します。

e signed by a certificate a certificate authority (CA) is	authority. s an organization that issues certificates.
rollment requests are cer	tificate requests that a CA has yet to approve.
ersonal Certificates 🛛 🖂	Certificates Enrollment Requests
Certificate	Store
User5	Cisco

22. ルート証明書が[CA Certificates]タブに表示されていることを確認します。

e signed by a certificate a	uthority.
rollment requests are cert	ificate requests that a CA has yet to approve.
'ersonal Certificates LA	Certificates Enrollment Requests
Certificate	Store
	CA.
jfrahim-pc	

<u>確認</u>

現在、この設定に使用できる確認手順はありません。

<u>トラブルシュート</u>

Microsoft CAサーバに登録しようとすると、次のエラーメッセージが生成される可能性があります。

Initiating online request Generating key pair Generating self-signed Certificate Initiating online request Received a response from the CA Your certificate request was denied このエラーメッセージが表示された場合は、Microsoft CAのログで詳細を確認するか、これらの リソースで詳細を確認してください。

- <u>要求を処理する認証局が見つかりません</u>
- <u>XCCC:セキュアな会議の証明書を要求すると、「Your Certificate Request was Denied」エラ</u> <u>ーメッセージが表示される</u>

<u>関連情報</u>

- IPSec ネゴシエーション/IKE プロトコル
- <u>テクニカル サポートとドキュメント Cisco Systems</u>