## Configuration du concentrateur Cisco VPN 3000 version 4.7.x pour obtenir un certificat numérique et un certificat SSL

### Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Installer des certificats numériques sur le concentrateur VPN Installer des certificats SSL sur le concentrateur VPN Renouveler les certificats SSL sur le concentrateur VPN Informations connexes

## **Introduction**

Ce document inclut des instructions détaillées sur la façon de configurer les concentrateurs de la gamme Cisco VPN 3000 pour s'authentifier à l'aide de certificats numériques ou d'identité et de certificats SSL.

**Remarque :** Dans le concentrateur VPN, l'équilibrage de charge doit être désactivé avant de générer un autre certificat SSL, car cela empêche la génération du certificat.

Référez-vous à <u>Comment obtenir un certificat numérique d'une autorité de certification Microsoft</u> <u>Windows utilisant ASDM sur un ASA</u> afin d'en savoir plus sur le même scénario avec PIX/ASA 7.x.

Référez-vous à <u>Exemple de configuration de l'inscription des certificats Cisco IOS à l'aide des</u> <u>commandes d'inscription avancées</u> afin d'en savoir plus sur le même scénario avec les platesformes Cisco IOS®.

## **Conditions préalables**

#### **Conditions requises**

Aucune spécification déterminée n'est requise pour ce document.

#### **Components Used**

Les informations de ce document sont basées sur le concentrateur Cisco VPN 3000 qui exécute la version 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**

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

## Installer des certificats numériques sur le concentrateur VPN

Procédez comme suit :

 Choisissez Administration > Certificate Management > Enroll afin de sélectionner la demande de certificat numérique ou d'identité.

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

 Choisissez Administration > Certificate Management > Enrollment > Identity Certificate et cliquez sur 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

 Remplissez les champs demandés, puis cliquez sur S'inscrire.Ces champs sont remplis dans cet exemple.Nom commun : altiga30Unité organisationnelle - IPSECCERT (l'unité d'organisation doit correspondre au nom de groupe IPsec configuré)Organisation - Cisco SystemsLocalité : RTPÉtat/Province—Caroline du NordPays—États-UnisNom de domaine complet - (non utilisé ici)Taille de clé—512Remarque : Si vous demandez un certificat SSL ou un certificat d'identité à l'aide du protocole SCEP (Simple Certificate Enrollment Protocol),

# ce sont les seules options RSA disponibles.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.				
Enroll Cancel					

# 4. Après avoir cliqué sur **S'inscrire**, plusieurs fenêtres s'affichent. La première fenêtre confirme que vous avez demandé un

#### certificat.

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
- · Go to Certificate Installation

Une nouvelle fenêtre de navigateur s'ouvre également et affiche votre fichier de demande PKCS.

🚰 https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	- <b>1</b> 10
← Back - → - ② 🔄 🐴 ② Search 💿 Favorites ③ Media 🍏 🖏 - 🎒 🖼 🗟	
Address 🙆 https://172.18.124.214/FILE/pkcs0001.txt 💌 200	Links »
👔 won - 🚱 - 🎆 🔽 🖸 🖓 Money -	More∛
NASDAQ®	>
	^
MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRp22EzMDESMBAGA1UECxMJSVBTRUND RVJUMRYwFAYDVQQKEw1DaXNjbyBTeXNOZW1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDUSvcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQYJKoZIhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwO1ONMiqw4kmgIhIG2E/BIZc+xokG4rBp11rq4DkM J3XOVB8yiUkzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB DOdRWJg/dVvGAMZHKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqa5NvlcdLsQFPxV1 zVleLhhpRf0A4hw1 END NEW CERTIFICATE REQUEST	4
🚵 Done 🕒 😫 🔮 Internet	11.

5. Sur votre serveur d'autorité de certification, mettez en surbrillance la demande et collez-la dans votre serveur d'autorité de certification afin d'envoyer votre demande. Cliquez sur **Next** (Suivant).

Microsoft Certificate Services - Microsoft Internet Explorer	1
File Edit. New Favorites Tools Help	
4-Back + + - O 3 1 O Search Frevertes Oriestary	
Address D http://172.10.124.96/centsrv/	- (260 Lin
Microsoft Certificate Services - ifrahim-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 cert will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, a depending upon the type of certificate you request.	ificate, you and more
Select a task:	
C Retrieve the CA certificate or certificate revocation list	
Check on a pending certificate	
	Next >

6. Sélectionnez **Demande avancée** et cliquez sur **Suivant**.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edk View Favorites Tools Help	
4+Back + + - () 2 2 2 () ()Search () Favorites ()History () + ()	
Address 🛃 http://172.18.124.96/certsrv/certrqus.asp	· (PGo Lin
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 Browsex Centrone E-Meil Protection Certificate	
@ Advanced request	
	Next >

7. Sélectionnez Soumettre une demande de certificat à l'aide d'un fichier PKCS #10 codé en base64 ou d'une demande de renouvellement à l'aide d'un fichier PKCS #7 codé en base64, puis cliquez sur

Suivant.	
Microsoft Certificate Services - Microsoft Internet Explorer	_1(
File Edit View Favorites Tools Help	
4+Back + → - ② 2 3 ③ Search ④ Favorites ③History 03 + 3	
Address Dttp://172.18.124.96/certsry/certrgad.asp	
Microsoft Certificate Sentces Iffahim-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 authority (CA) will determine the certificates that you can obtain.	of the certification
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 PKC	S #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>	
	Next>

 Coupez et collez votre fichier PKCS dans le champ de texte sous la section Requête enregistrée. Cliquez ensuite sur Soumettre.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
+Back + + - () () () () () Search () Favorites () (Hetory ) () + ()	
Address Mtp://172.18.124.96/certsrvjcertrqst_asp	• ອີເລ ] ⊔
Microsoft Certificate Services jfrahim-pc	Nome and the second
Submit A Saved Request	
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated server) into the request field to submit the request to the certification authority (CA).	by an external application (such as a web
Saved Request:	
PFbNOQ/TmdWEGRBoUkdPFw8CAQUubQYJKo21hvcN+ qLHTjSu7B3LupqKAlqFZiBQfxG137D+wHEEp+6z4 MqG4AhkH Certificate Request (PKCS #10 or #7): +	
Bipliste for a file to insert.	
Additional Attributes:	
	Submit >

9. Émettez le certificat d'identité sur le serveur

AC.							
Certification Authority			the second second				_ 6
Action Yew		ß					
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)		BEGIN NE	Takan Index Substation Al Taoks Index Substation Refresh Help	3/23/2001 9:13 AM	GHOSTEMUSR	. 05	Ceco Syste

10. Téléchargez la racine et les certificats d'identité. Sur votre serveur AC, sélectionnez Vérifier un certificat en attente, puis cliquez sur

Suivant.			
Microsoft Certificate Services - Microsoft Internet Explorer		-	ł
File Edit View Favorites Tools Help			
4+8ak + → - ◎ ② ③ ③ ③ Search @Favorites @History ◎ - ④			
Address At http://172.18.124.96/certarv/	- 0	Go L	*
Microsoft Centricate Services Inshim-pc		Hom	ł
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 cert will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, a depending upon the type of certificate you request.	tificate and mo	, you ire	
Select a task:			
C Retrieve the CA certificate or certificate revocation list			
Request a certificate			
Check on a pending certificate			
	Next	5	

11. Sélectionnez Codé Base 64, puis cliquez sur Télécharger le certificat d'Autorité de certification sur le serveur d'Autorité de certification.



12. Enregistrez le certificat d'identité sur votre lecteur

ve As					<u>?</u> ×
Save in:	🛃 Desktop		•	+ 🛍 💣 💷+	
<u>3</u>	A Document	S;			
History	📴 My Network P	laces			
Desktop					
My Computer					
tu Mahurak P	File name:	certnew.cer			Save
IV NEWVOIK P	Save as type:	Security Certificate		•	Cancel

13. Sur le serveur d'autorité de certification, sélectionnez **Récupérer le certificat d'autorité de** certification ou la liste de révocation de certificat afin d'obtenir le certificat racine. Cliquez ensuite

Next.

Microsoft Certificate Services - Microsoft Internet Explorer	
Fée Edit - View Favorites Tools Help	
4-back - → - () () () () () Search () Favorites () History () - ()	
Address 1/172.18.124.96/certsrv/	▼ ( <sup>2</sup> %)
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. Enregistrez le certificat racine sur votre lecteur



15. Installez les certificats racine et d'identité sur le concentrateur VPN 3000. Pour ce faire, sélectionnez Administration > Certificate Manager > Installation > Install certificate obtenu par inscription. Sous État de l'inscription, cliquez sur Installer.

Select a enrollment request to	install.						
Inrollment Status							
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altiga30 at Cisco Systems	N/A	05/22/2003	D	Initial	Manual	In Progress	View Install Delete

16. Cliquez sur Télécharger le fichier à partir de la station de

travail.



17. Cliquez sur **Parcourir** et sélectionnez le fichier de certificat racine que vous avez enregistré sur votre lecteur local.Sélectionnez **Installer** pour installer le certificat d'identité sur le concentrateur VPN. L'administration | La fenêtre Gestion des certificats apparaît sous forme de confirmation et votre nouveau certificat d'identité apparaît dans le tableau Certificats d'identité.

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

**Remarque :** Complétez ces étapes pour générer un nouveau certificat en cas d'échec du certificat.Sélectionnez Administration > Gestion des certificats.Cliquez sur Supprimer dans la zone Actions de la liste des certificats SSL.Sélectionnez Administration > Redémarrage du système.Sélectionnez Enregistrer la configuration active au moment du redémarrage, choisissez Maintenant, puis cliquez sur Appliquer. Vous pouvez désormais générer un nouveau certificat une fois le rechargement terminé.

## Installer des certificats SSL sur le concentrateur VPN

Si vous utilisez une connexion sécurisée entre votre navigateur et le concentrateur VPN, le concentrateur VPN nécessite un certificat SSL. Vous avez également besoin d'un certificat SSL sur l'interface que vous utilisez pour gérer le concentrateur VPN et pour WebVPN, et pour chaque interface qui termine les tunnels WebVPN.

Les certificats SSL d'interface, s'ils n'existent pas, sont générés automatiquement lorsque le concentrateur VPN 3000 redémarre après la mise à niveau du logiciel du concentrateur VPN 3000. Comme un certificat auto-signé est auto-généré, ce certificat n'est pas vérifiable. Aucune autorité de certification n'a garanti son identité. Mais ce certificat vous permet d'établir un premier contact avec le concentrateur VPN à l'aide du navigateur. Si vous souhaitez le remplacer par un autre certificat SSL autosigné, procédez comme suit :

#### 1. Choisissez Administration > Certificate

Manage	ement.									
Administ	ration   Certificate	e Managem	ient				Mor	ıday, C	05 January 2004	16:31:1
									R	etresh (
This sectio • <u>Clic</u> • <u>Clic</u> Certifica	n lets you view and <u>&amp; here to enroll with</u> <u>&amp; here to install a ce</u> <b>te Authorities</b> [ V	manage certi <u>a Certificate</u> n <u>tificate</u> View All CRL (	ficates on the VPN 1 <u>Authority</u> Caches   Clear All CRI	3000 Concent	rretor. rrent: 1. maxi	inuun	: 20)			
	Subject		Issuer		Expirat	ion	SCEP Issuer		Actions	
ms-root-si	ha-06-2001 at cisco	ms-i	root-sha-06-2001 at	ot-sha-06-2001 at cisco 06/04/2022		2	No Vi		Configure   Delete	
Identity	Certificates (cum Subject	ent: 1, maxinw	un: 20)	Issuer			Expiration		Actions	
Gateway /	A at Cisco Systems		ms-root-sha-D6-	2001 at cisco			02/04/2004	View   I	Renew   Delete	
SSL Cer	tificates		T		Employed			4 - 12		
Interface	Subject	t	Issuer		Expiration	Actions				
Private	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							port		
SSH Hos	st Key									
	Key Size	B	беу Туре		Date Generated			Actions		
1024 bits		RSA		01/05/2004				Ga	Gonorato	

2. Cliquez sur Generate afin d'afficher le nouveau certificat dans la table de certificats SSL et de remplacer le certificat existant.Cette fenêtre vous permet de configurer des champs pour les certificats SSL que le concentrateur VPN génère automatiquement. Ces certificats SSL sont destinés aux interfaces et à l'équilibrage de

cnarge.		
Administration   Certificate	Management   Generate SSL Cer	tificate
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 fo	or 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		

Si vous voulez obtenir un certificat SSL vérifiable (c'est-à-dire un certificat délivré par une autorité de certification), consultez la section <u>Installer des certificats numériques sur le</u> <u>concentrateur VPN</u> de ce document afin d'utiliser la même procédure que celle que vous

utilisez pour obtenir des certificats d'identité. Mais cette fois, dans la fenêtre Administration > Certificate Management > Enroll, cliquez sur SSL certificate (au lieu de Identity Certificate).Remarque : reportez-vous à la section Administration / Section Gestion des certificats du Concentrateur VPN 3000 Référence Volume II : Administration et surveillance version 4.7 pour obtenir des informations complètes sur les certificats numériques et les certificats SSL.

## Renouveler les certificats SSL sur le concentrateur VPN

Cette section décrit comment renouveler les certificats SSL :

S'il s'agit du certificat SSL généré par le concentrateur VPN, accédez à Administration > Certificate Management dans la section SSL. Cliquez sur l'option de renouvellement, qui renouvelle le certificat SSL.

S'il s'agit d'un certificat délivré par un serveur AC externe, procédez comme suit :

Certification

1. Choisissez Administration > Certificate Management >Delete sous SSL Certificates afin de supprimer les certificats expirés de l'interface

Administration   Certificate Managemer	nt	We	dnesday, 19	9 September 2007 00:01
				Refresh
This section lets you view and manage	certificates on the VPN 3000 Concentrator.			
<u>Click here to enroll with a Certif</u> <u>Click here to install a certificate</u> Certificate Authorities [View All CR	ficate Authority L Caches   Clear All CRL Caches ] (current: 1, m	naximum: 6)		
Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte	Thawte Test CA Root at Thawte	12/31/2020	No	View   Configure   Delete

Identity Certificates (current: 0, maximum: 2)

publique.

Certification

	Subject	Issuer	Expiratio	n Actions
No Identi	ty Certificates			
SSL Cert	ificates			
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   Imp
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut at Equifax	08/16/2008	View   Renew   Delete) Export   Generate   Enroll   Imp

Cliquez sur **Oui** afin de confirmer la suppression du certificat SSL.

#### 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
CF	L Distribution Point http://crl.geotrust.com/crls/secureca.crl

Are you sure you want to delete this certificate?



2. Choisissez Administration > Certificate Management > Generate afin de générer le nouveau certificat

#### SSL.

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

#### apparaît.

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   Renew   Delete   Export   Generate   Enroll   Import

## Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- <u>Négociation IPSec/Protocoles IKE</u>
- Support et documentation techniques Cisco Systems