

配置VPN 3000集中器以使用證書與VPN客戶端通訊

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[適用於VPN使用者端的VPN 3000集中器憑證](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔包含有關如何使用證書配置帶VPN客戶端的Cisco VPN 3000系列集中器的分步說明。

[必要條件](#)

[需求](#)

本文件沒有特定需求。

[採用元件](#)

本文檔中的資訊基於Cisco VPN 3000集中器軟體版本4.0.4A。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

[慣例](#)

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

[適用於VPN使用者端的VPN 3000集中器憑證](#)

完成以下步驟，以便為VPN客戶端配置VPN 3000集中器證書。

1. 必須將IKE策略配置為使用VPN 3000 Concentrator Series Manager上的證書。要配置IKE策略

，請選擇 Configuration > System > Tunneling Protocols > IPsec > IKE Proposals，然後將 CiscoVPNClient-3DES-MD5-RSA 移動到 Active Proposals。

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority. Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
<ul style="list-style-type: none">CiscoVPNClient-3DES-MD5-RSACiscoVPNClient-3DES-MD5IKE-3DES-MD5IKE-3DES-MD5-DH1IKE-DES-MD5IKE-3DES-MD5-DH7IKE-3DES-MD5-RSACiscoVPNClient-3DES-MD5-DH5CiscoVPNClient-AES128-SHAIKE-AES128-SHA	<ul style="list-style-type: none"><< ActivateDeactivate >>Move UpMove DownAddModifyCopyDelete	<ul style="list-style-type: none">IKE-3DES-SHA-DSAIKE-3DES-MD5-RSA-DH1IKE-DES-MD5-DH7CiscoVPNClient-3DES-SHA-DSACiscoVPNClient-3DES-MD5-RSA-DH5CiscoVPNClient-3DES-SHA-DSA-DH5CiscoVPNClient-AES256-SHAIKE-AES256-SHA

2. 還必須配置 IPsec 策略以使用證書。選擇 Configuration > Policy Management > Traffic Management > Security Associations，突出顯示 ESP-3DES-MD5，然後按一下 Modify 配置 IPsec 策略配置 IPsec 策略。

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPsec SAs	Actions
<ul style="list-style-type: none">ESP-3DES-MD5ESP-3DES-MD5-DH5ESP-3DES-MD5-DH7ESP-3DES-NONEESP-AES128-SHAESP-DES-MD5ESP-L2TP-TRANSPORTESP/IKE-3DES-MD5	<ul style="list-style-type: none">AddModifyDelete

3. 在「修改」視窗的「數位證書」下，確保選擇已安裝的身份證書。在 IKE 建議下，選擇 CiscoVPNClient-3DES-MD5-RSA，然後按一下 Apply。

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

IKE Proposal Select the IKE Proposal to use as IKE initiator.

4. 要配置IPsec組，請選擇Configuration > User Management > Groups > Add，新增名為IPSECCERT(IPSECCERT組名稱與身份證書中的組織單位(OU)匹配)的組，然後選擇密碼。如果您使用證書，則任何位置都不使用此口令。在本例中，「cisco123」是密碼。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | **IPSec** | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	<input type="text" value="IPSECCERT"/>	Enter a unique name for the group.
Password	<input type="password"/>	Enter the password for the group.
Verify	<input type="password"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

5. 在同一頁上，按一下General頁籤，並確保選擇IPsec作為隧道協定。

Identity				General	IPSec	Client Config	Client FW	HW Client	PPTP/L2TP
General Parameters									
Attribute	Value		Inherit?	Description					
Access Hours	-No Restrictions-		<input checked="" type="checkbox"/>	Select the access hours assigned to this group.					
Simultaneous Logins	3		<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.					
Minimum Password Length	8		<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.					
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.					
Idle Timeout	30		<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.					
Maximum Connect Time	0		<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.					
Filter	-None-		<input checked="" type="checkbox"/>	Enter the filter assigned to this group.					
Primary DNS			<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.					
Secondary DNS			<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.					
Primary WINS			<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.					
Secondary WINS			<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.					
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4		<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.					
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec		<input type="checkbox"/>	Select the tunneling protocols this group can connect with.					

6. 按一下IPsec頁籤，並確保已配置的IPsec安全關聯(SA)在IPsec SA下處於選中狀態，然後按一下Apply。

Identity				General				IPSec				Client Config				Client FW				HW Client				PPTP/L2TP			
IPSec Parameters																											
Attribute	Value								Inherit?	Description																	
IPSec SA	ESP-3DES-MD5								<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.																	
IKE Peer Identity Validation	If supported by certificate								<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.																	
IKE Keepalives	<input checked="" type="checkbox"/>								<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.																	
Confidence Interval	300								<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.																	
Tunnel Type	Remote Access								<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.																	
Remote Access Parameters																											
Group Lock	<input type="checkbox"/>								<input checked="" type="checkbox"/>	Lock users into this group.																	
Authentication	Internal								<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .																	
Authorization Type	None								<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.																	
Authorization Required	<input type="checkbox"/>								<input checked="" type="checkbox"/>	Check to require successful authorization.																	
DN Field	CN otherwise OU								<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.																	
Authorization Required	<input type="checkbox"/>								<input checked="" type="checkbox"/>	Check to require successful authorization.																	
DN Field	CN otherwise OU								<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.																	
IPComp	None								<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.																	
Reauthentication on Rekey	<input type="checkbox"/>								<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.																	
Mode Configuration	<input checked="" type="checkbox"/>								<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.																	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>																											

7. 要在VPN 3000集中器上配置IPsec組，請選擇Configuration > User Management > Users > Add，指定使用者名稱、密碼和組名，然後按一下Add。在示例中，使用以下欄位：使用者名稱= cert_user密碼= cisco123驗證= cisco123組= IPSECCERT

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

8. 要在VPN 3000集中器上啟用調試，請選擇Configuration > System > Events > Classes並新增以下類：CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10

Configuration | System | Events | Classes

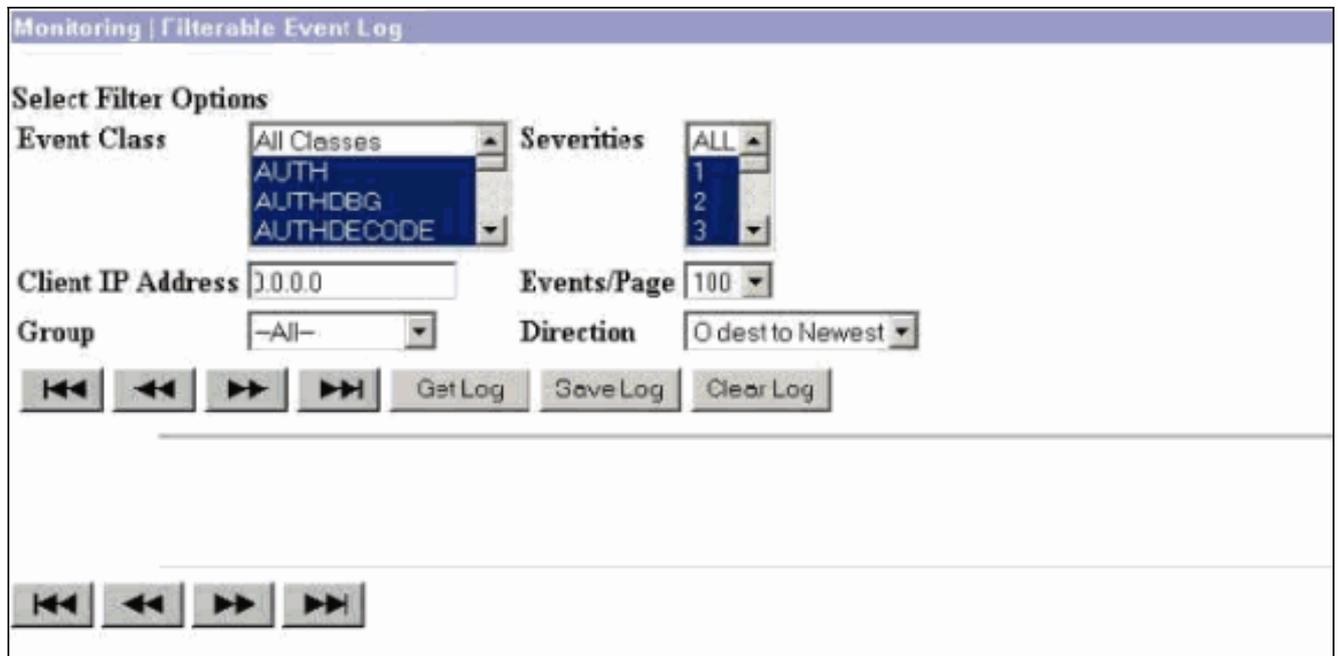
This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

Configured Event Classes	Actions
CERT IKE IKEDBG IPSEC IPSECDBG MIB2TRAP	Add Modify Delete

9. 選擇Monitoring > Filterable Event Log以檢視調試。



注意：如果您決定更改IP地址，您可以註冊新的IP地址，並在以後使用這些新地址安裝已頒發的證書。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

有關進一步的故障排除資訊，請參閱[排除VPN 3000集中器上的連線問題](#)。

相關資訊

- [Cisco VPN 3000系列集中器](#)
- [Cisco VPN 3002硬體使用者端](#)
- [IPSec 協商/IKE 通訊協定](#)
- [技術支援與文件 - Cisco Systems](#)