配置VPN 3000集中器以使用證書與VPN客戶端通訊

目錄

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

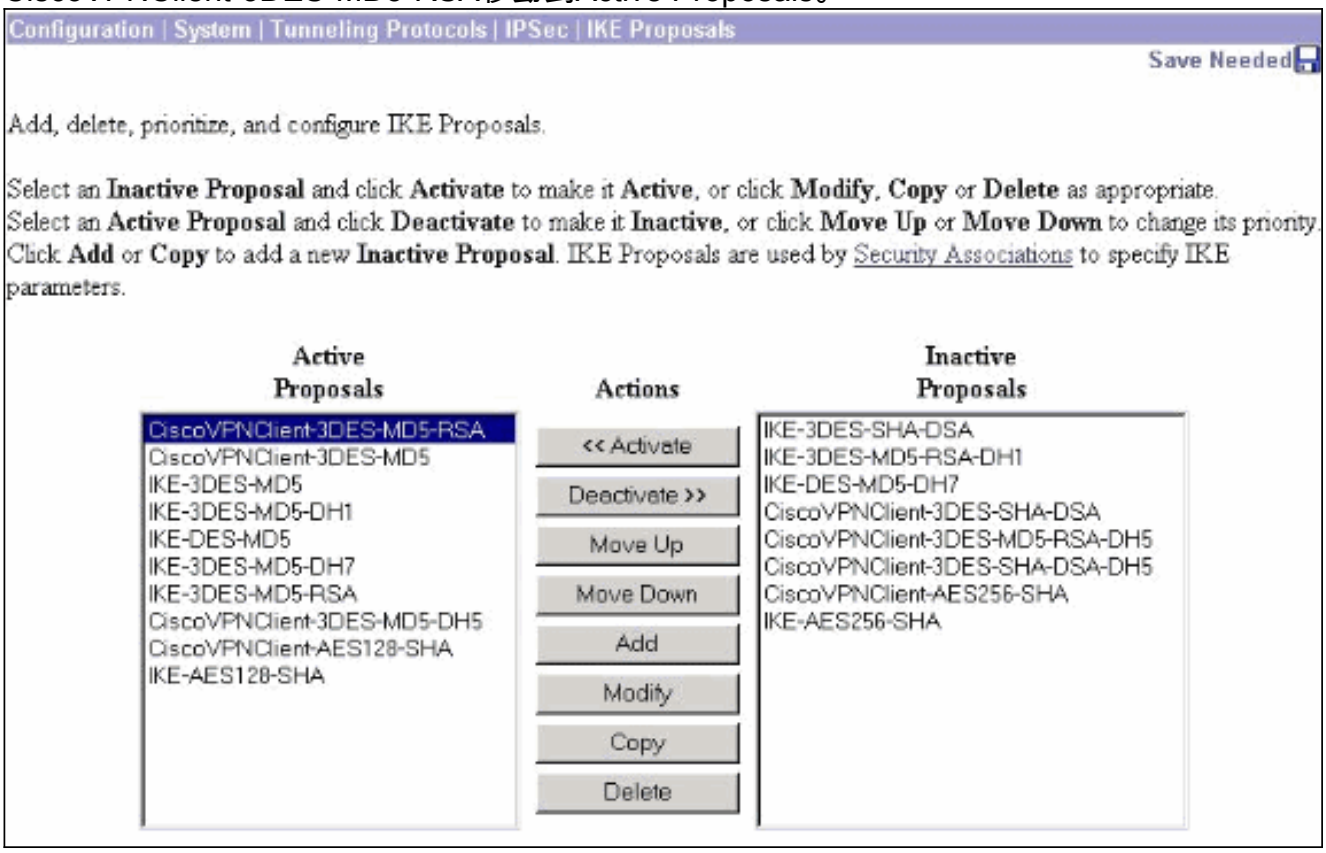
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

適用於VPN使用者端的VPN 3000集中器憑證

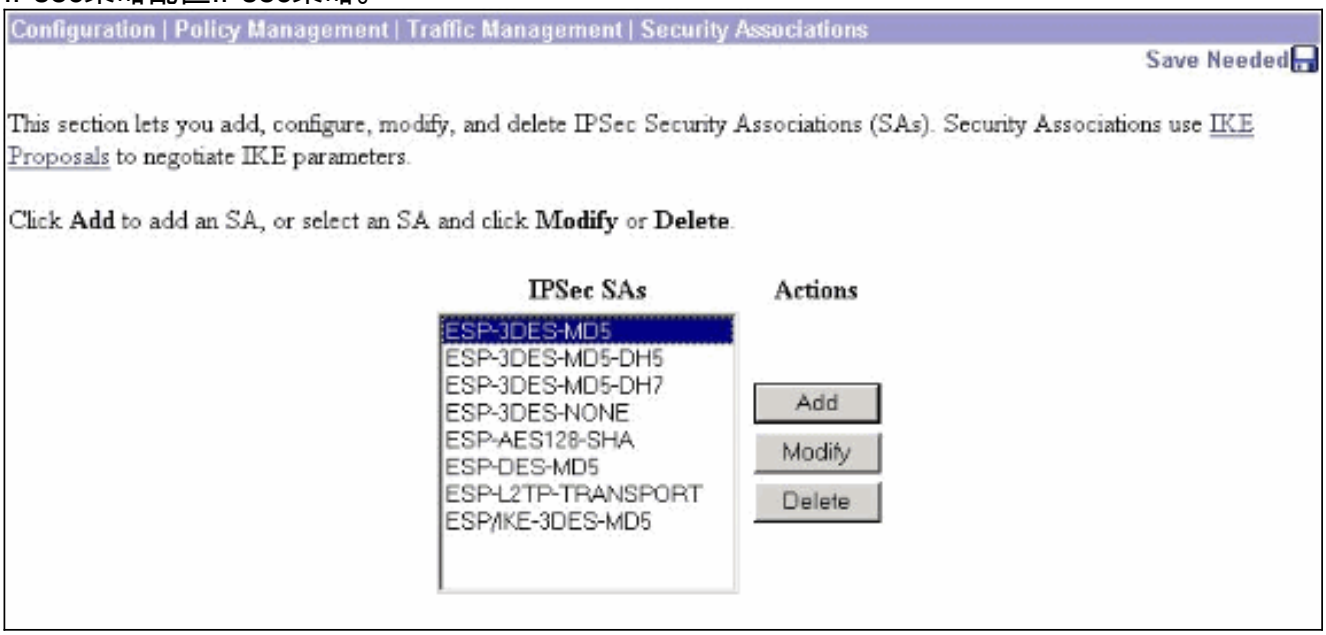
完成以下步驟，以便為VPN客戶端配置VPN 3000集中器證書。

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

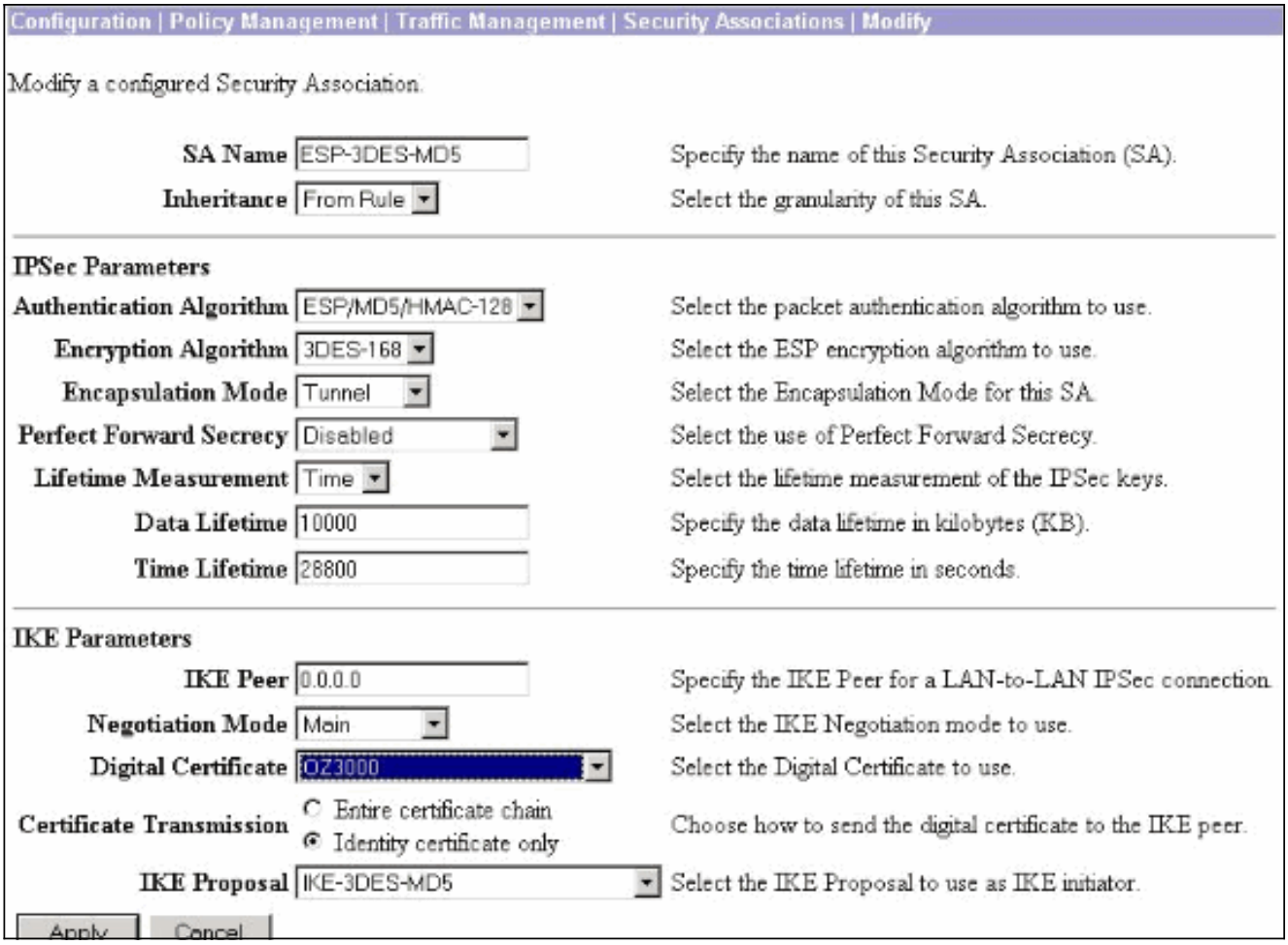
，請選擇Configuration > System > Tunneling Protocols > **IPsec** > IKE Proposals，然後將CiscoVPNClient-3DES-MD5-RSA移動到Active Proposals。



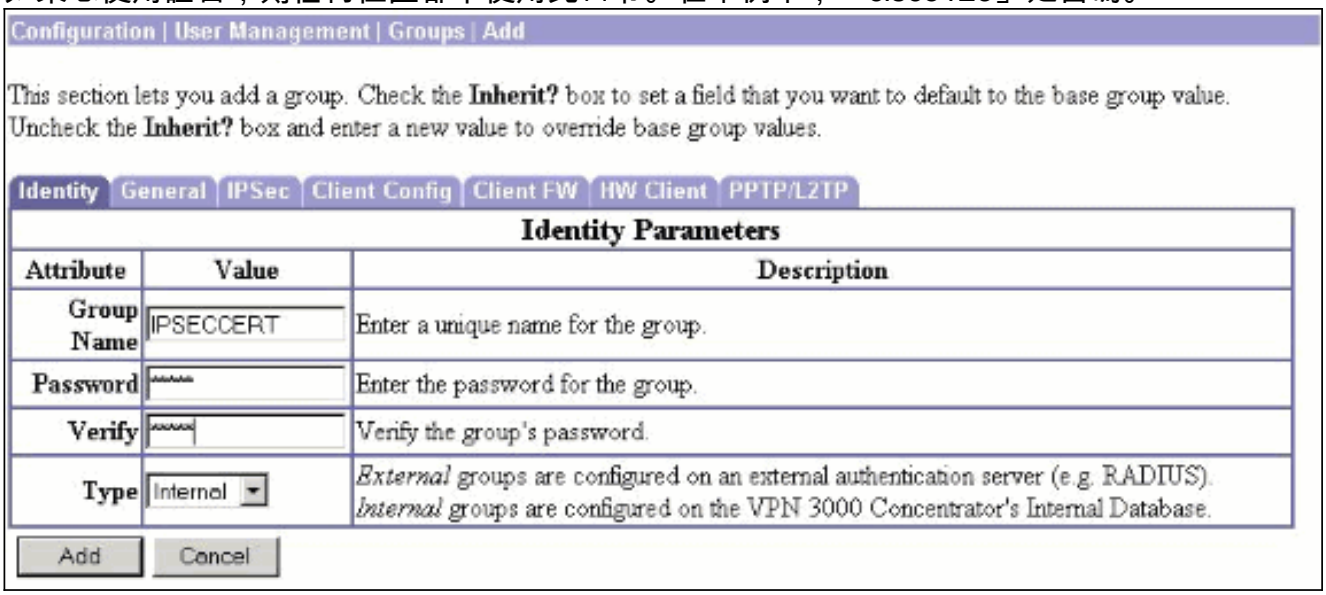
2. 還必須配置IPsec策略以使用證書。選擇Configuration > Policy Management > Traffic Management > **Security Associations**，突出顯示**ESP-3DES-MD5**，然後按一下Modify配置IPsec策略配置IPsec策略。



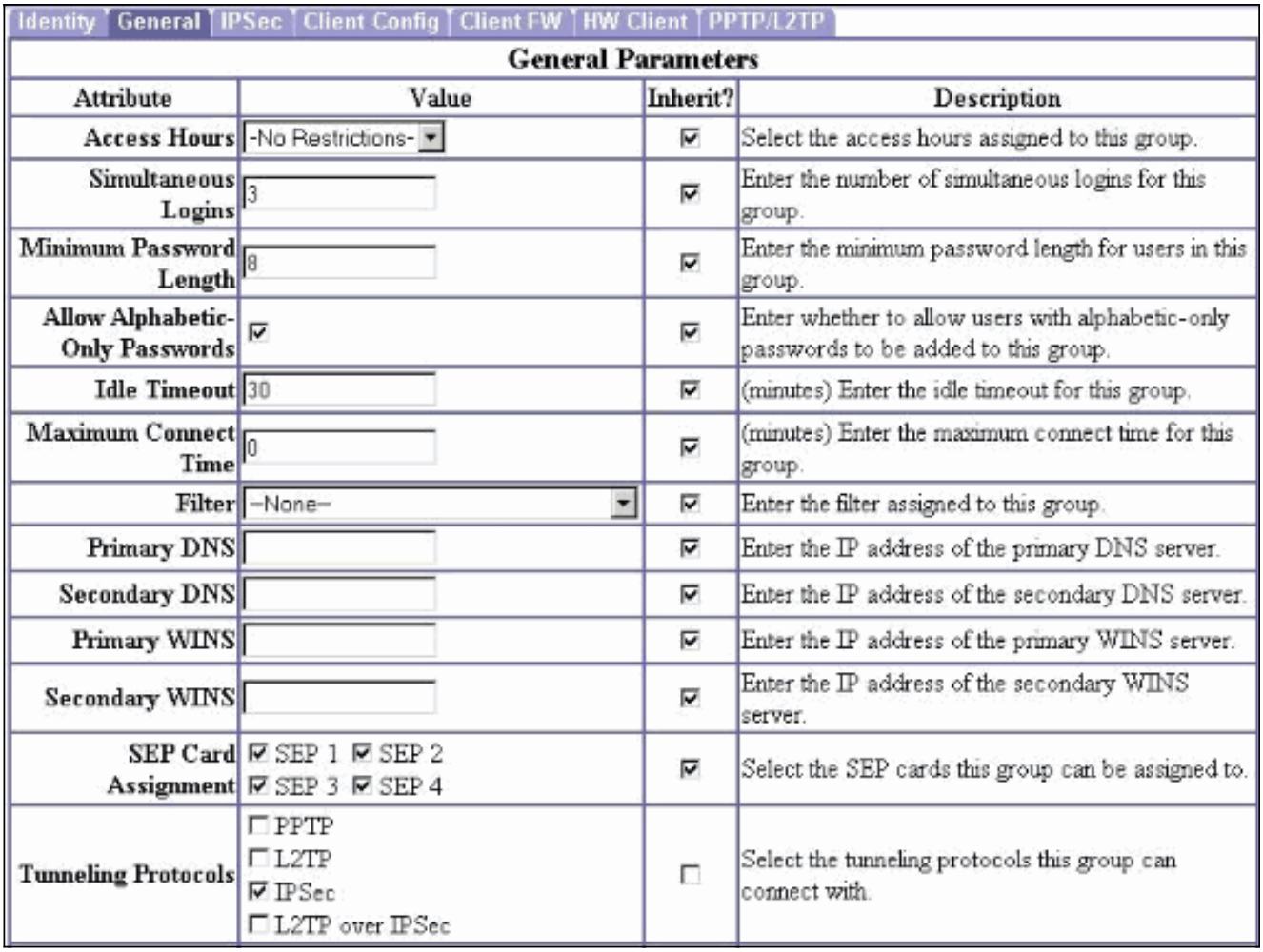
3. 在「修改」視窗的「數位證書」下，確保選擇已安裝的身份證書。在IKE建議下，選擇**CiscoVPNClient-3DES-MD5-RSA**，然後按一下**Apply**。



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。



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

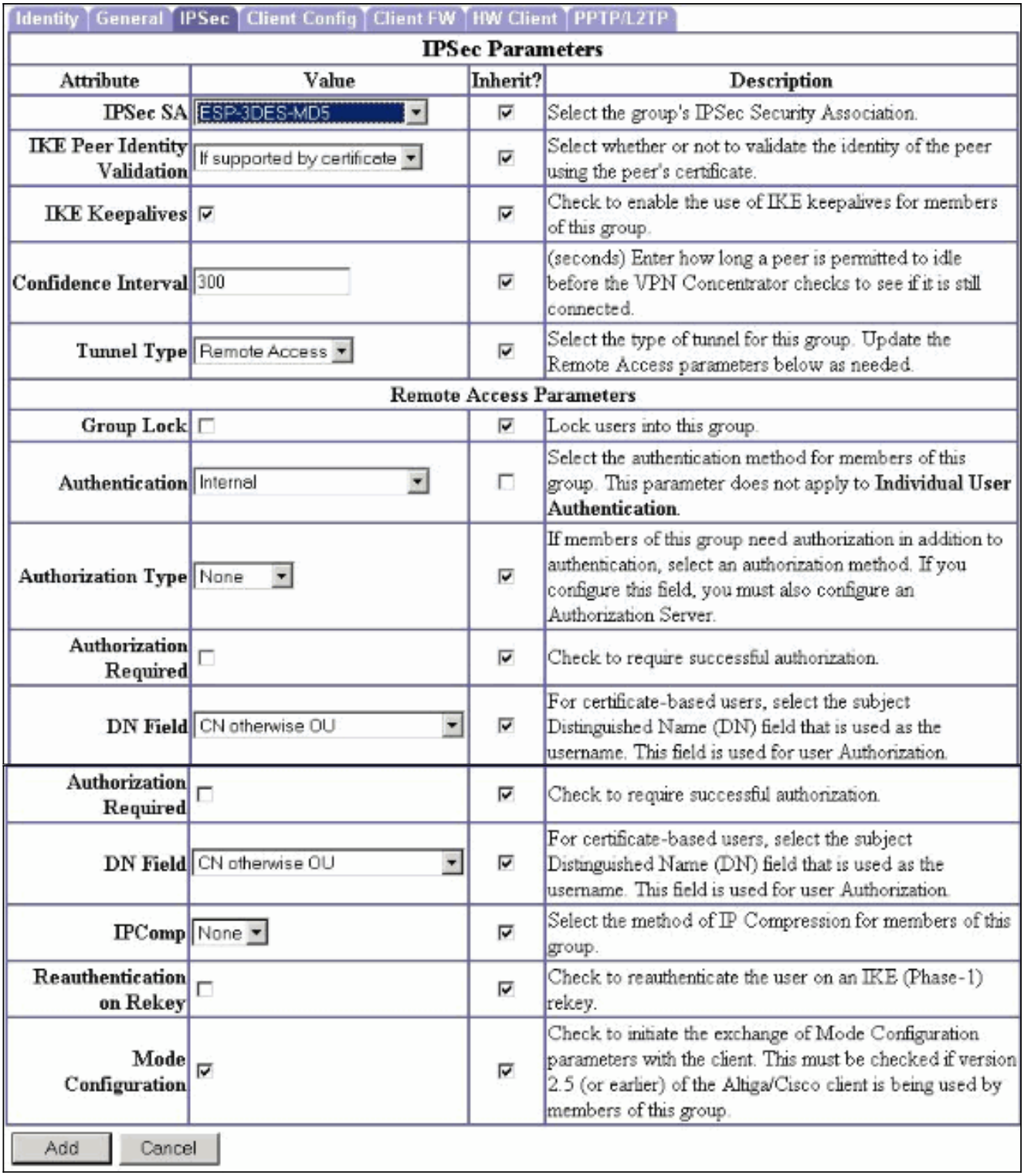


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

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



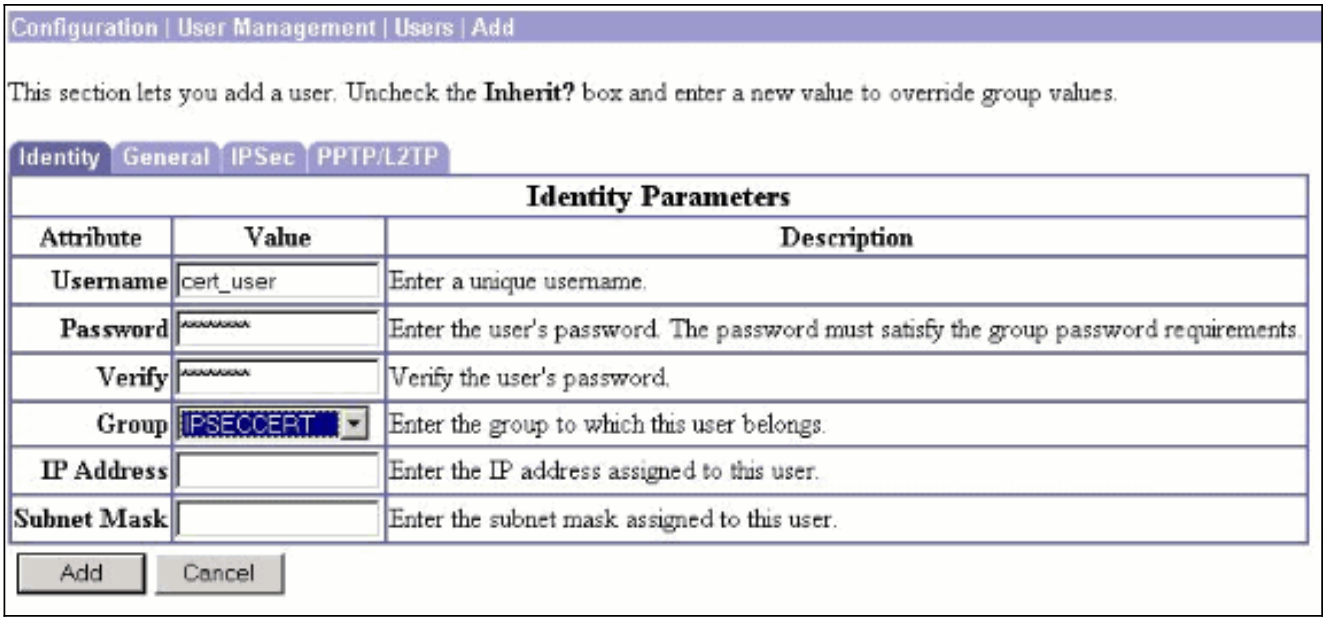
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

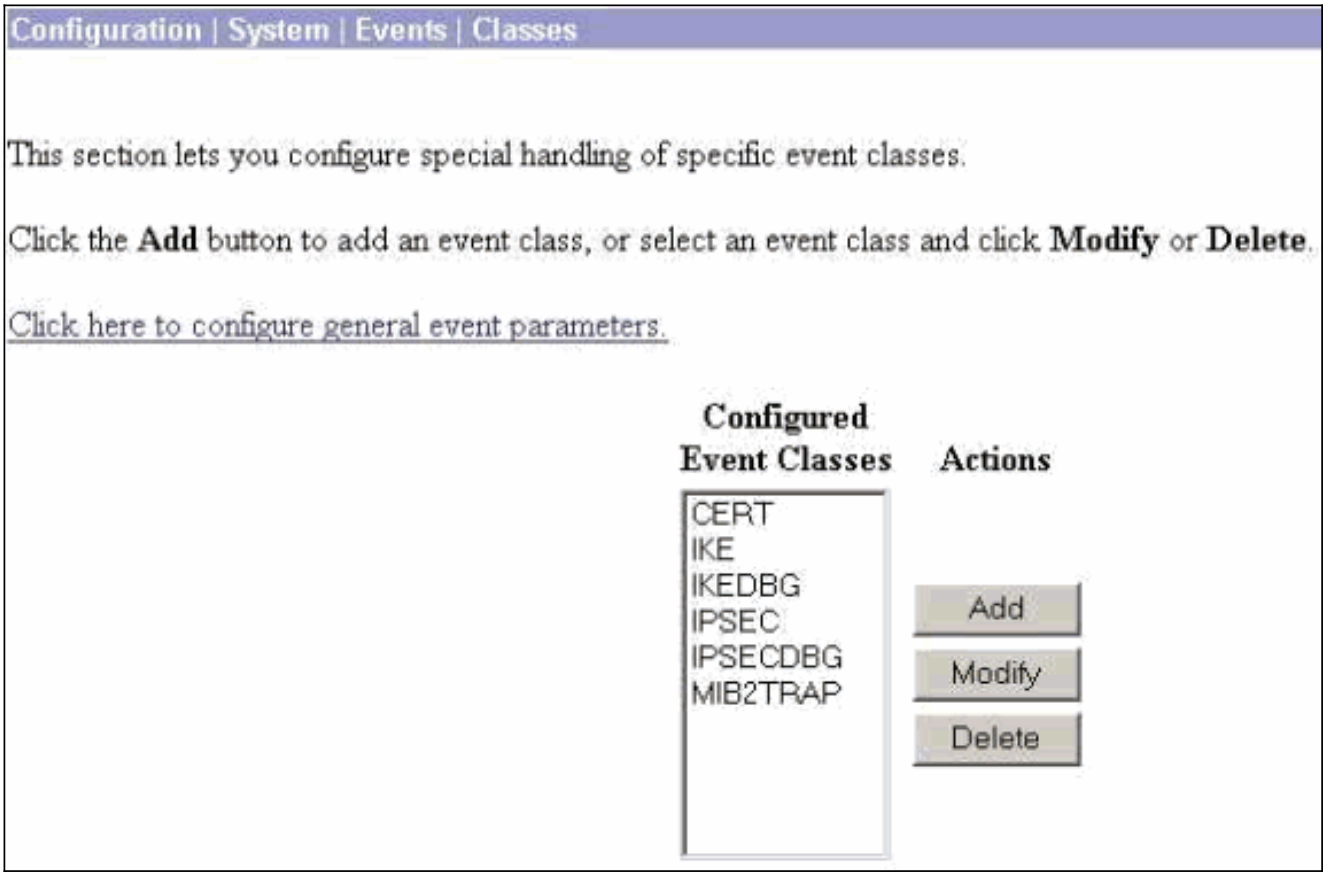
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	☑	(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	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal	☐	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	☑	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	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	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	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	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	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	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.

Add | Cancel

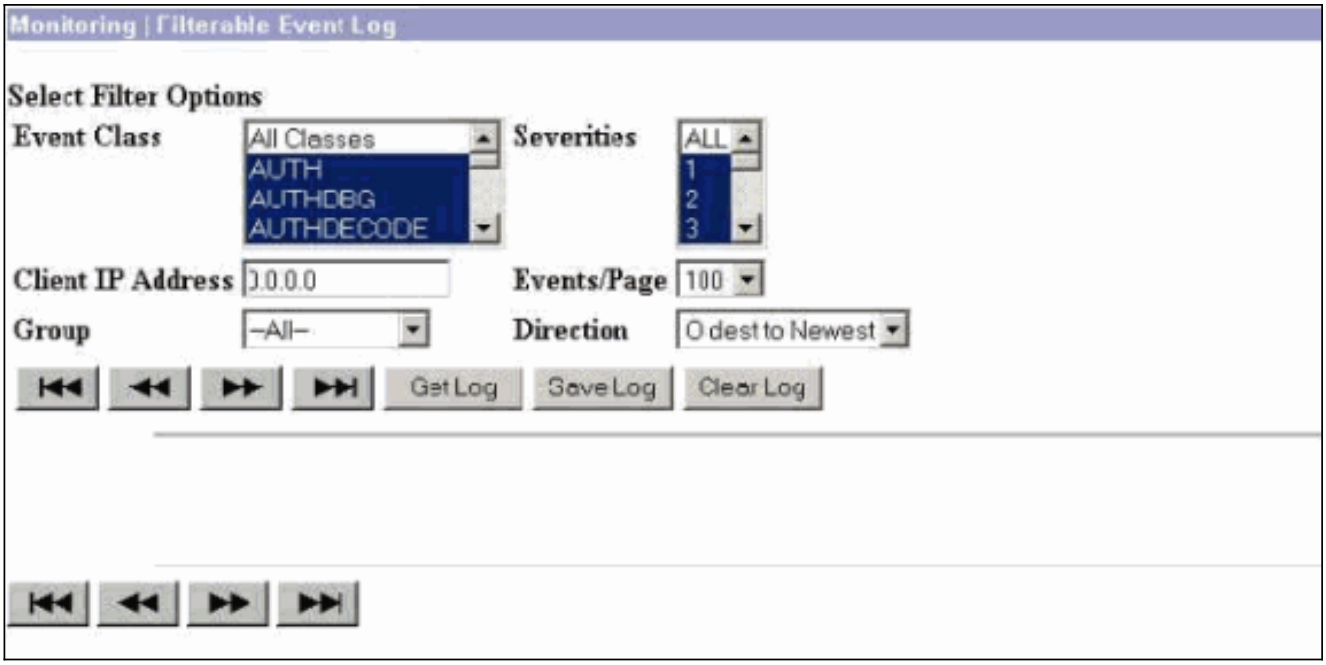
7. 要在VPN 3000集中器上配置IPsec組，請選擇Configuration > **User Management > Users > Add**，指定使用者名稱、密碼和組名，然後按一下**Add**。在示例中，使用以下欄位：使用者名稱= cert_user密碼= cisco123驗證= cisco123組= IPSECCERT



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



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