De VPN 3000 Concentrator configureren om met de VPN-client te communiceren met behulp van certificaten

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[VPN 3000 Concentrator-certificaten voor VPN-clients](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document bevat stap-voor-stap instructies over de manier waarop u Cisco VPN 3000 Series Concentrators met VPN-clients kunt configureren met gebruik van certificaten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN 3000 Concentrator softwareversie 4.0.4A.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

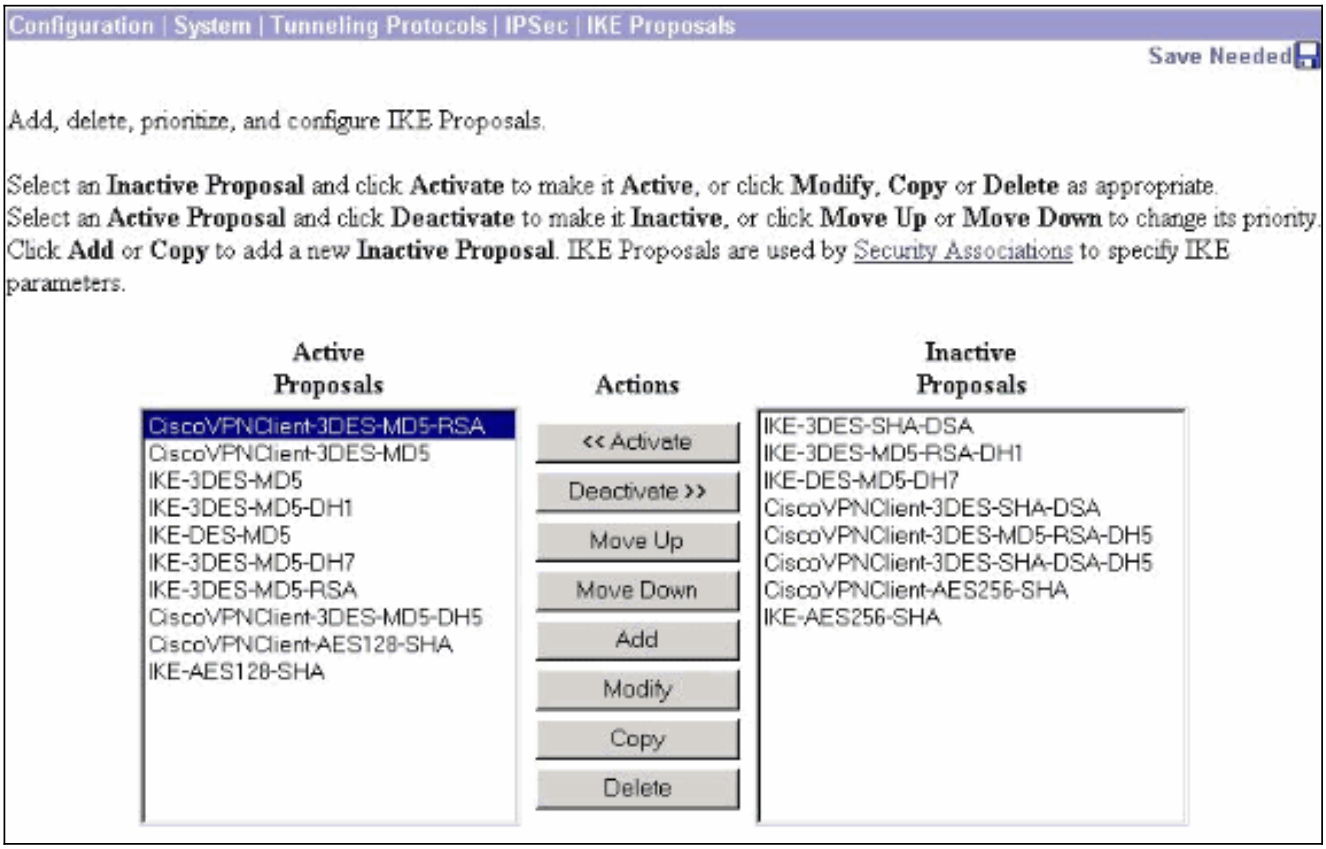
Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

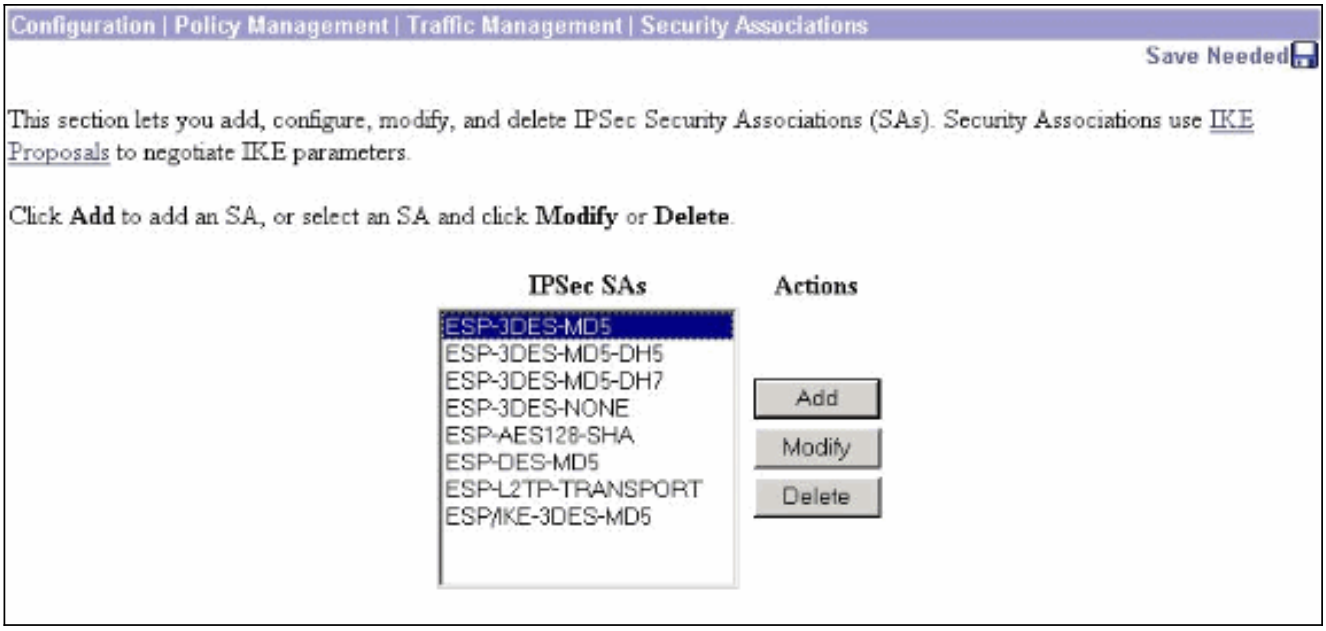
VPN 3000 Concentrator-certificaten voor VPN-clients

Voltooi deze stappen om VPN 3000 Concentrator-certificaten voor VPN-clients te configureren.

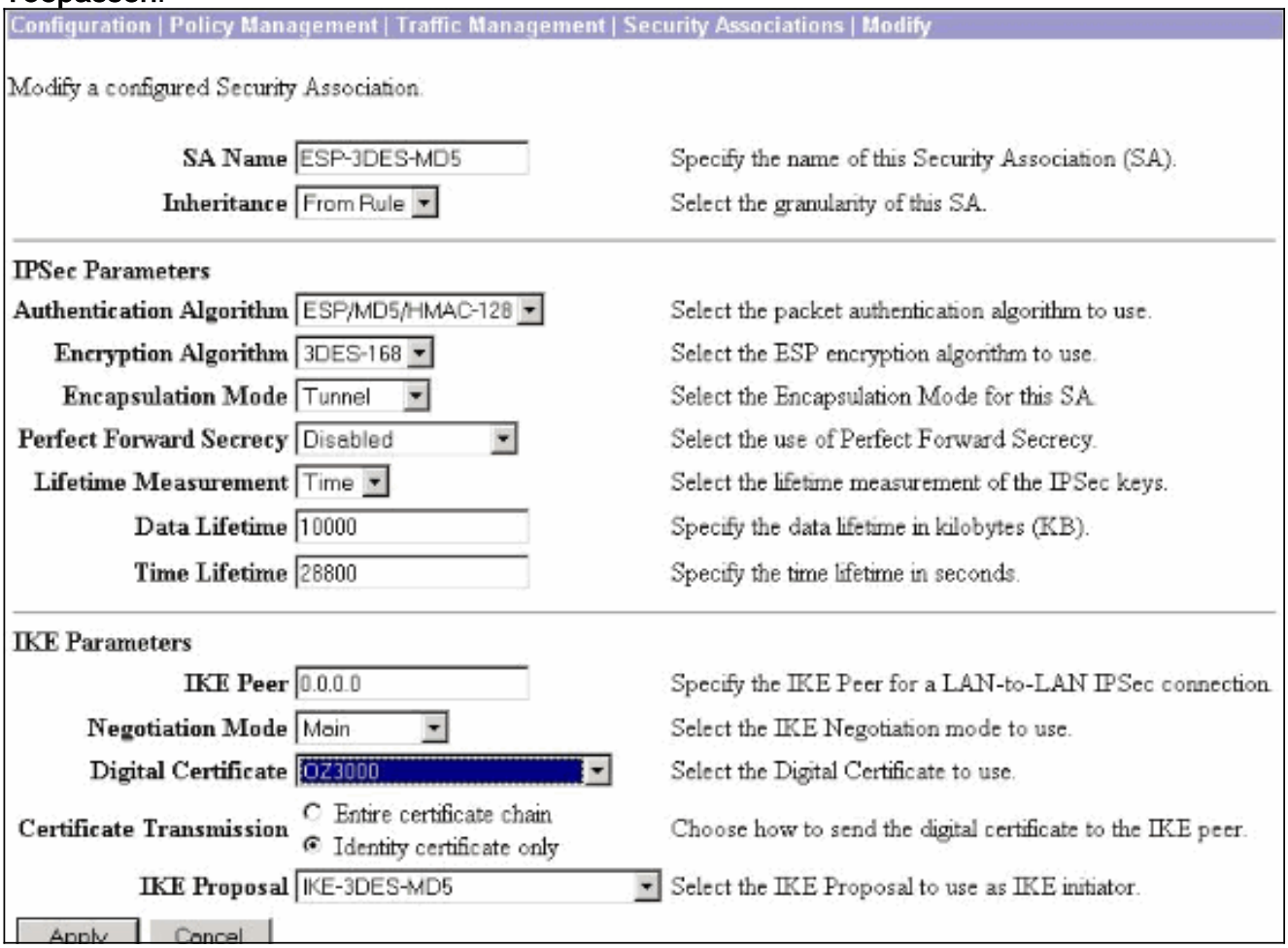
1. Het IKE-beleid moet worden geconfigureerd om certificaten te gebruiken in VPN 3000 Concentrator Series Manager. Om het IKE-beleid te configureren selecteert u **Configuration > System > Tunneling Protocols > IPsec > IKE-voorstellen en zet Cisco VPN-client-3DES-MD5-RSA in op de actieve voorstellen.**



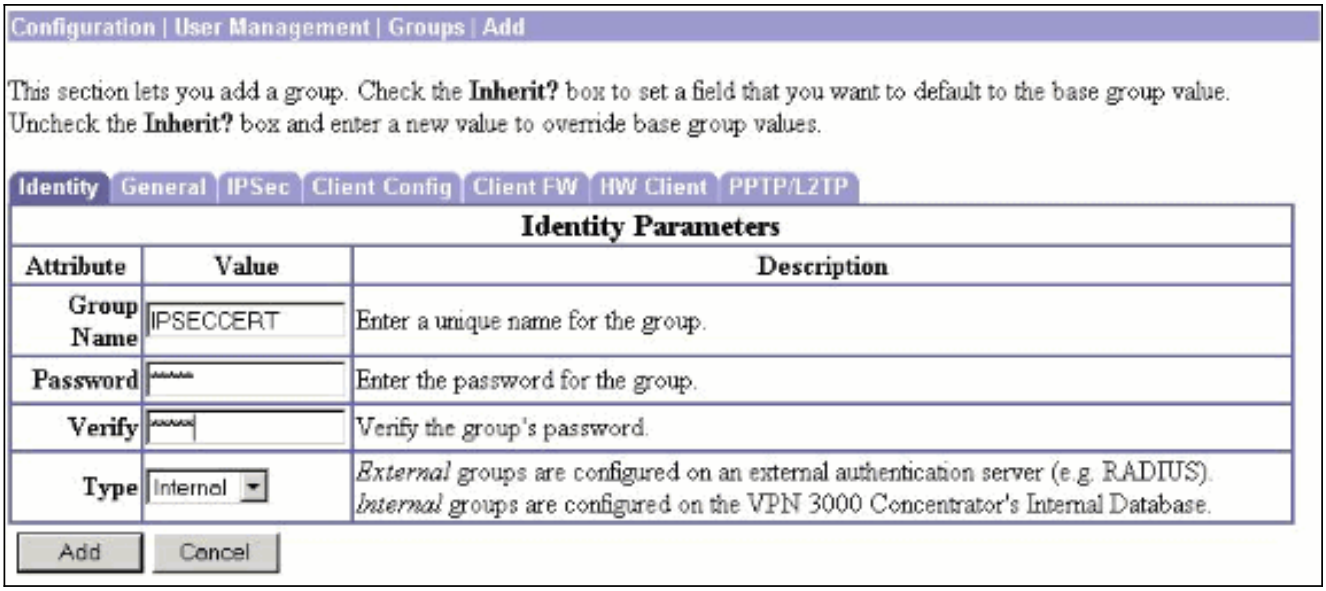
2. U moet ook het IPsec-beleid configureren om certificaten te gebruiken. Selecteer **Configuration > Policy Management > Traffic Management > Security Associations**, toets **ESP-3DES-MD5 en klik vervolgens op Wijzigen om het IPsec-beleid te configureren om het IPsec-beleid te configureren.**



3. Zorg er in het venster Wijzigen onder Digitale Certificaten voor dat u het geïnstalleerde identiteitsbewijs selecteert. Selecteer onder IKE Proposal **Cisco VPN,client-3DES-MD5-RSA** en klik op **Toepassen**.



4. Om een IPsec-groep te configureren selecteert u **Configuration > User Management > Group > Add**, voegt u een groep **IPSECCERT (de IPSECCERT-groepsnaam komt overeen met de Organisatorische eenheid (OU) in het identiteitsbewijs) en selecteert u een wachtwoord.**Dit wachtwoord wordt nergens gebruikt als u certificaten gebruikt. In dit voorbeeld is "cisco123" het
wachtwoord.



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.

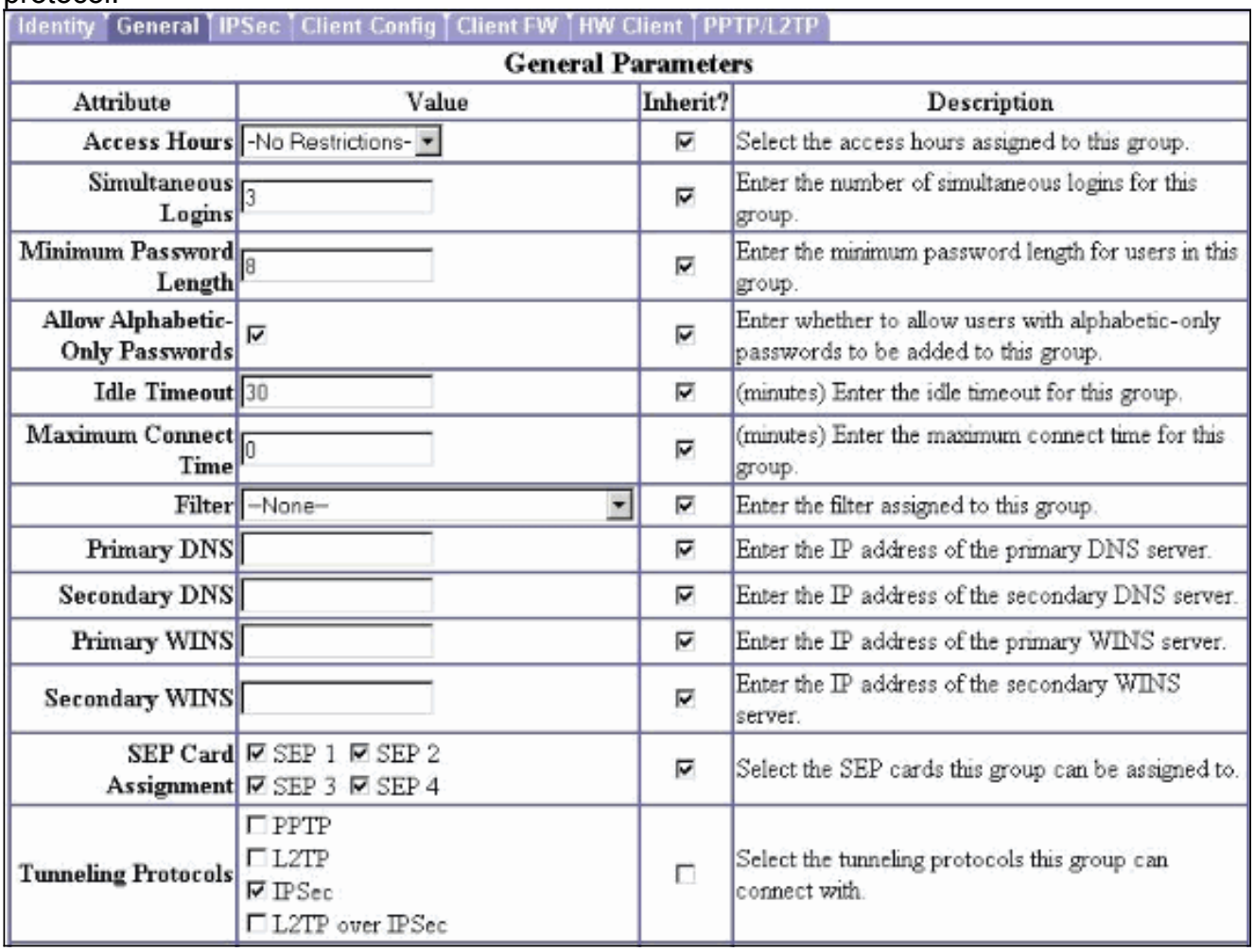
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	IPSECCERT	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

Add | Cancel

5. Klik op het tabblad Algemeen en zorg ervoor dat u **IPsec** selecteert als het tunneling-protocol.

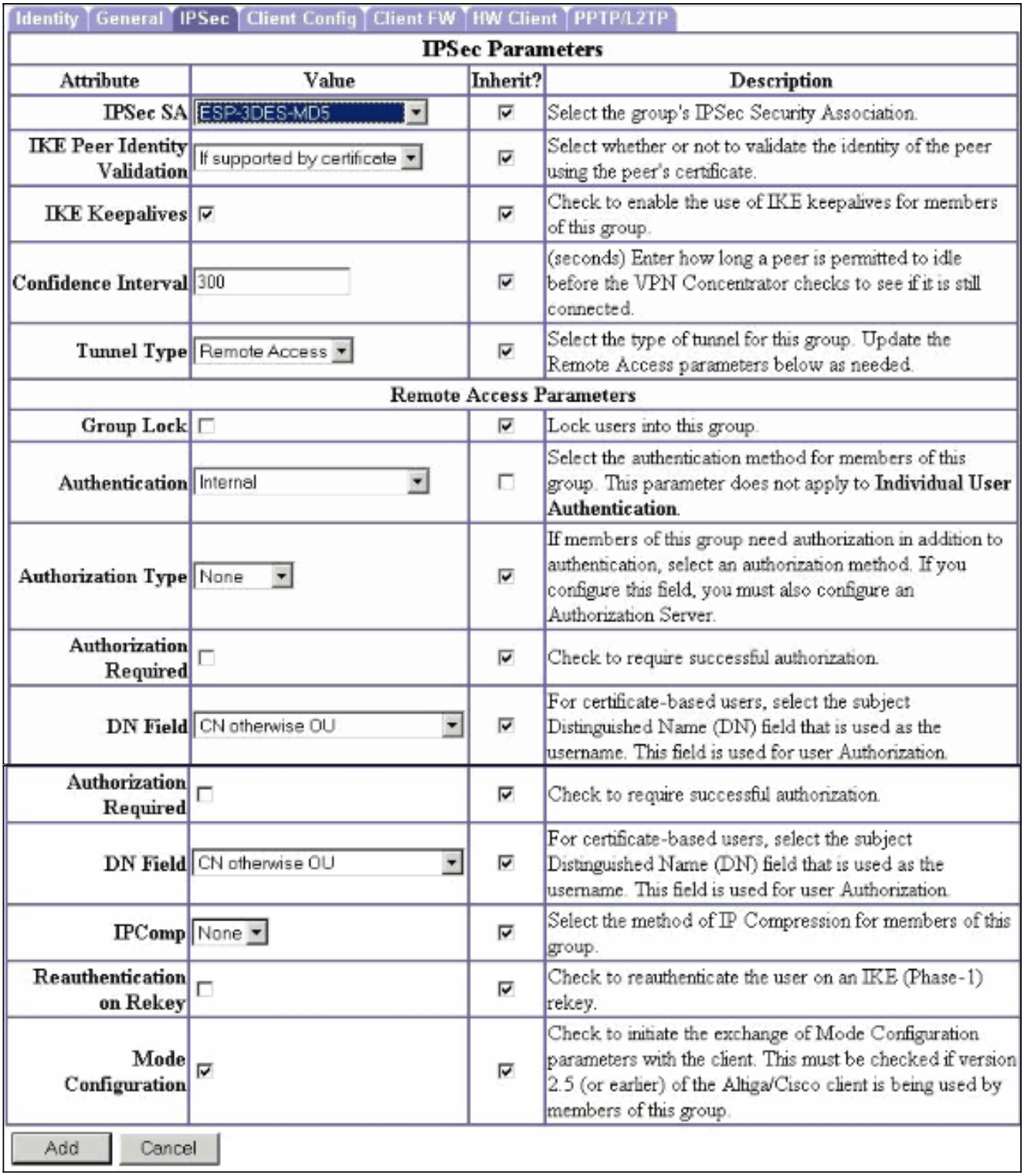


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Klik op het tabblad IPsec en zorg ervoor dat uw geconfigureerde IPsec Security Association (SA) is geselecteerd onder IPsec SA en klik op **Toepassen**.



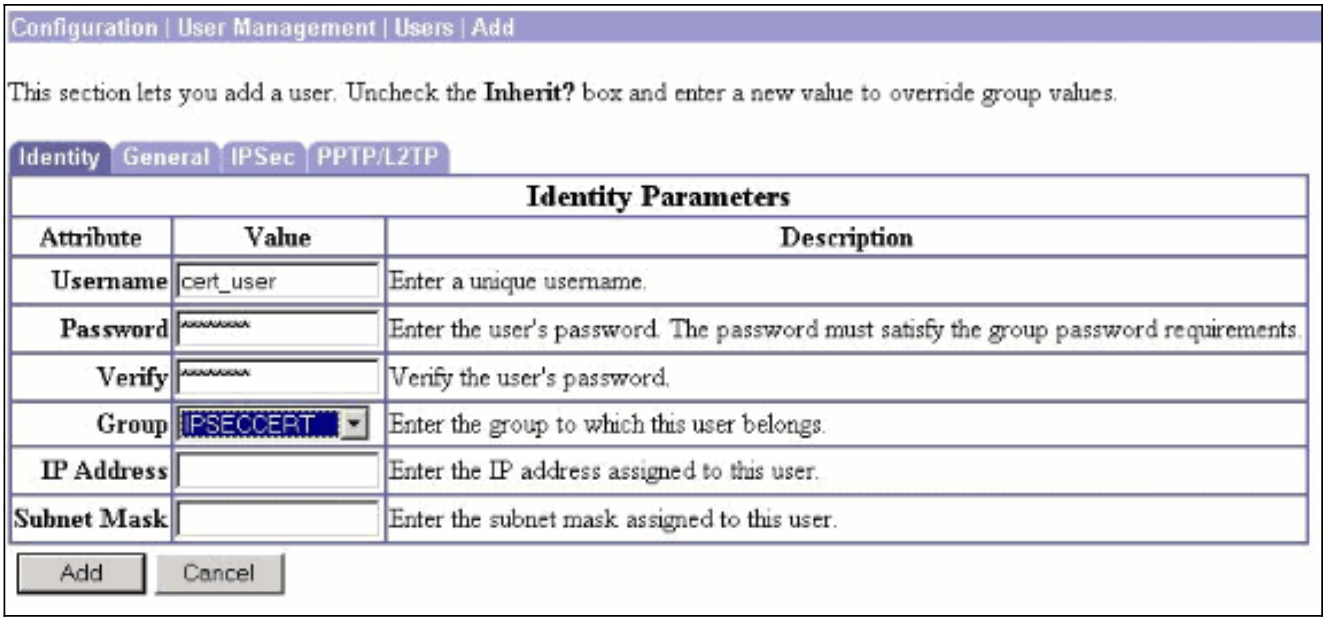
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

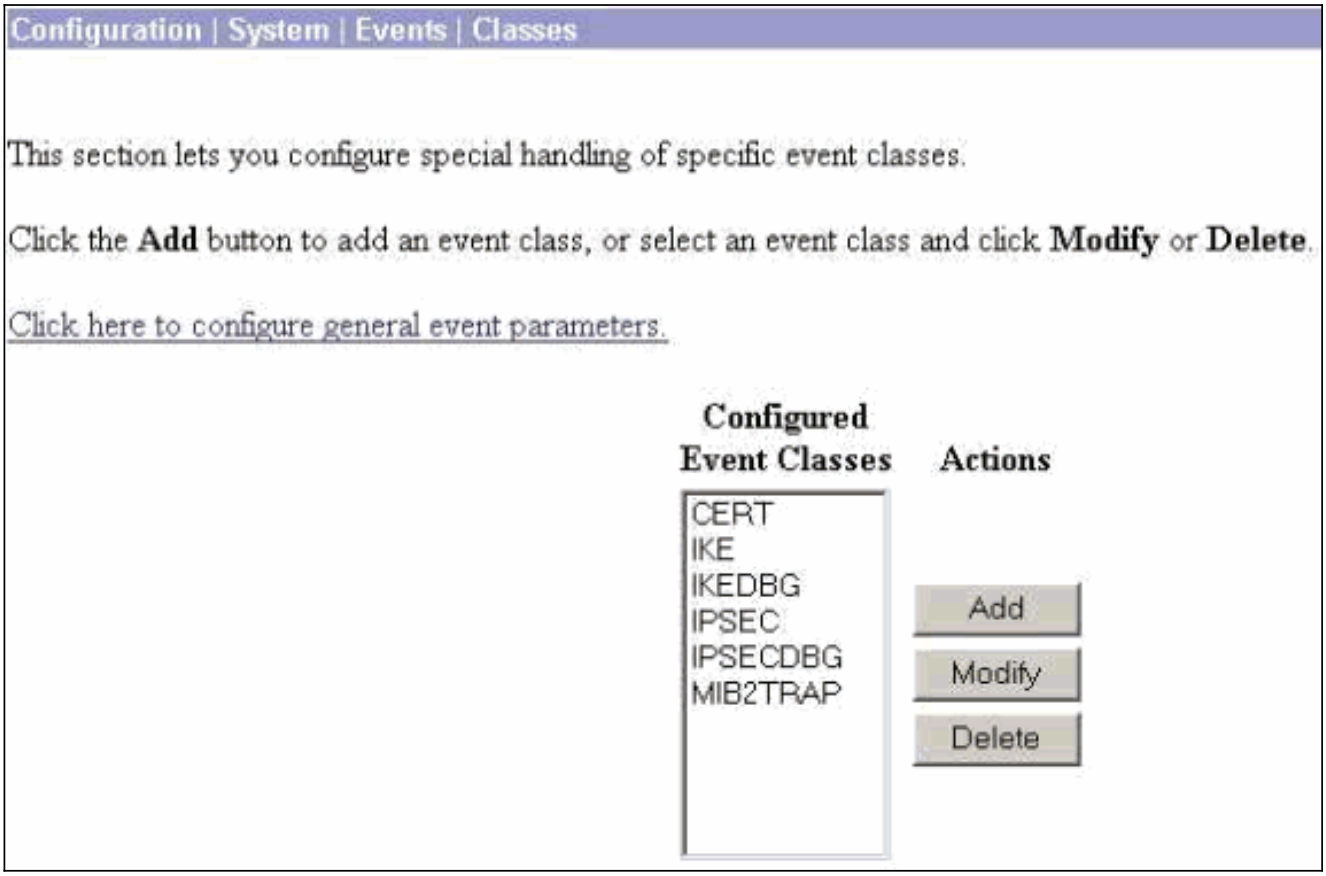
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of 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

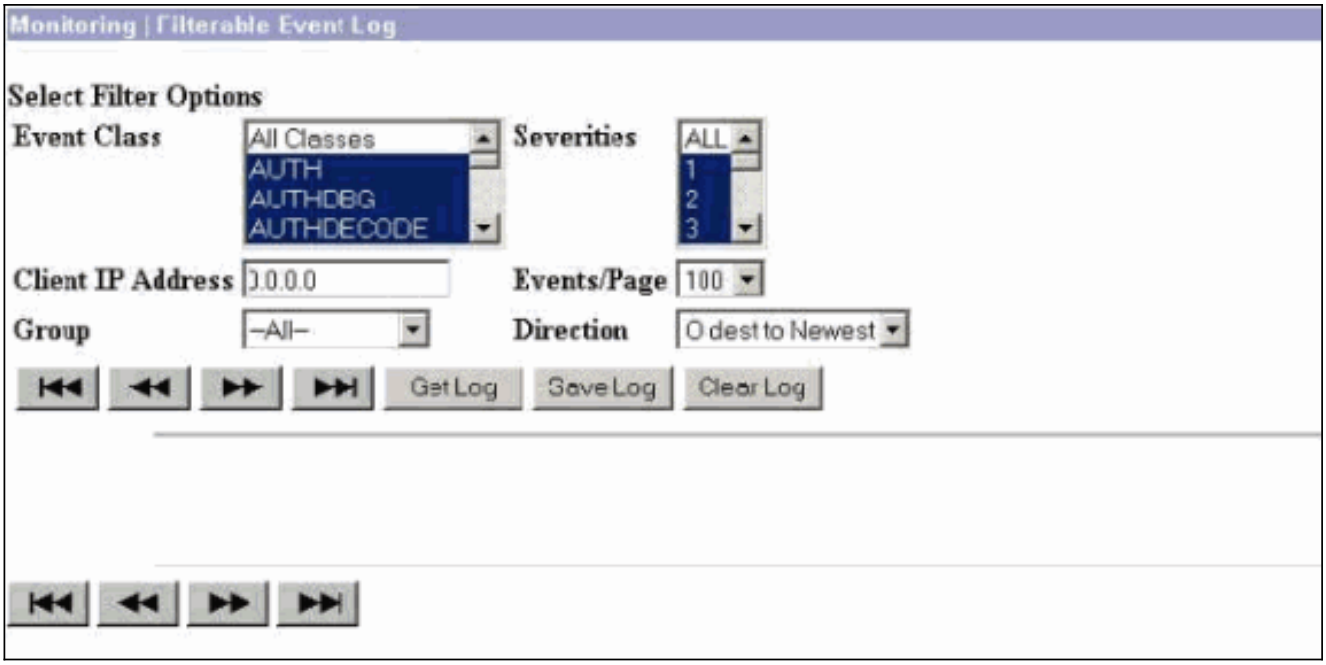
7. Om een IPsec-groep te configureren in het VPN 3000-**centrator**, selecteert u **Configuration > User Management > Gebruikers > Add**, specificeert u een gebruikersnaam, wachtwoord en de naam van de groep en vervolgens klikt u op **Add.**In het voorbeeld worden deze velden gebruikt:Gebruikersnaam = cert_userWachtwoord = cisco123Controleer = cisco123Groep = IPSECCERT



8. Zo selecteert u het foutoptreden op de VPN 3000 Concentrator **Configuration > System > Events > Classes** en voegt u deze klassen toe:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. Selecteer **Monitoring > Filterable Event Log** om de beelden te bekijken.



N.B.: Als u de IP-adressen wilt wijzigen, kunt u de nieuwe IP-adressen inschrijven en het afgegeven certificaat later met deze nieuwe adressen installeren.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Raadpleeg verbindingsproblemen met probleemoplossing in de VPN 3000-concentratie voor meer informatie over probleemoplossing.

Gerelateerde informatie

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 hardwareclients
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems