Konfigurieren des VPN 3000-Konzentrators für die Kommunikation mit dem VPN-Client mithilfe von Zertifikaten

Inhalt

Einführung

Dieses Dokument enthält schrittweise Anweisungen zur Konfiguration der Cisco VPN Concentrators der Serie 3000 mit VPN-Clients unter Verwendung von Zertifikaten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco VPN 3000 Concentrator Software, Version 4.0.4A.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

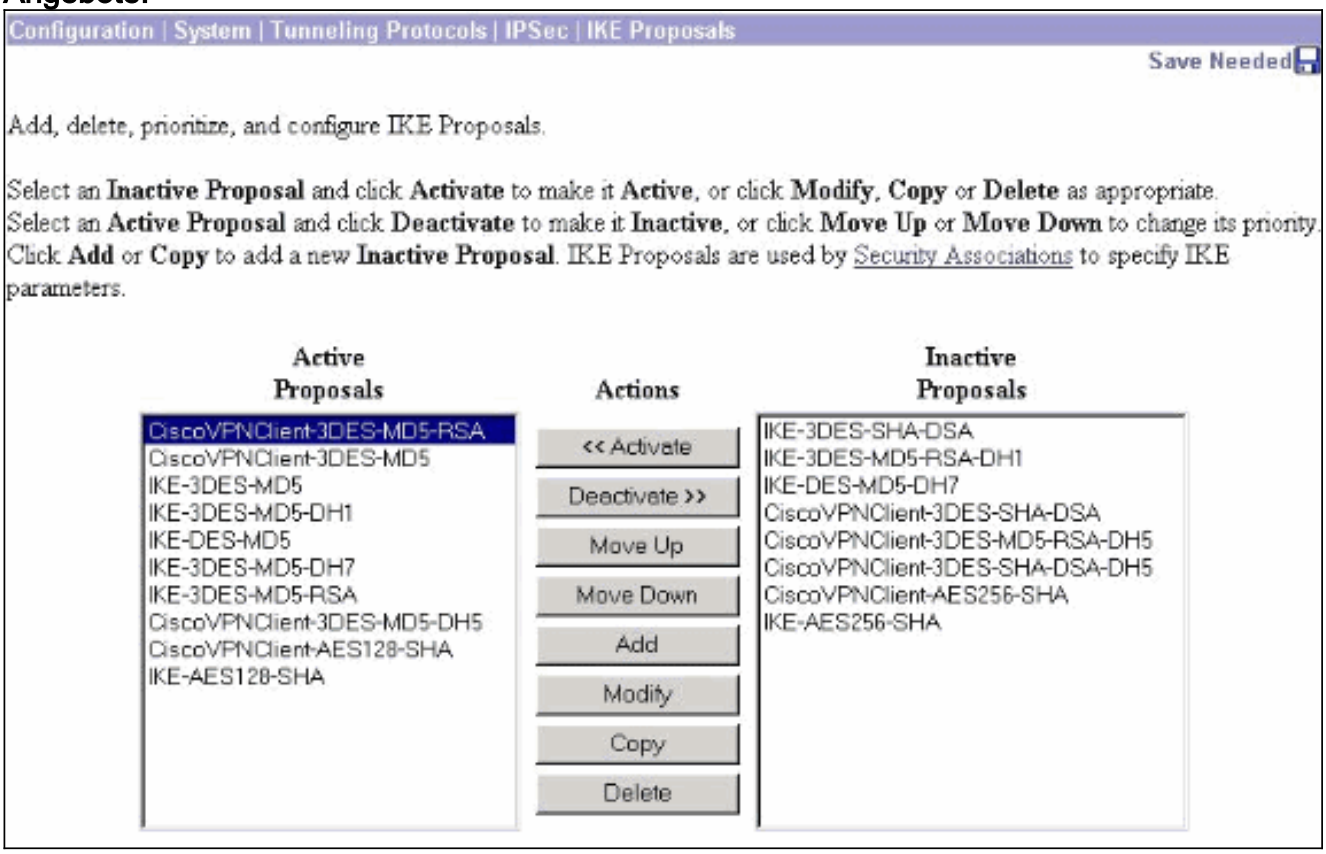
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

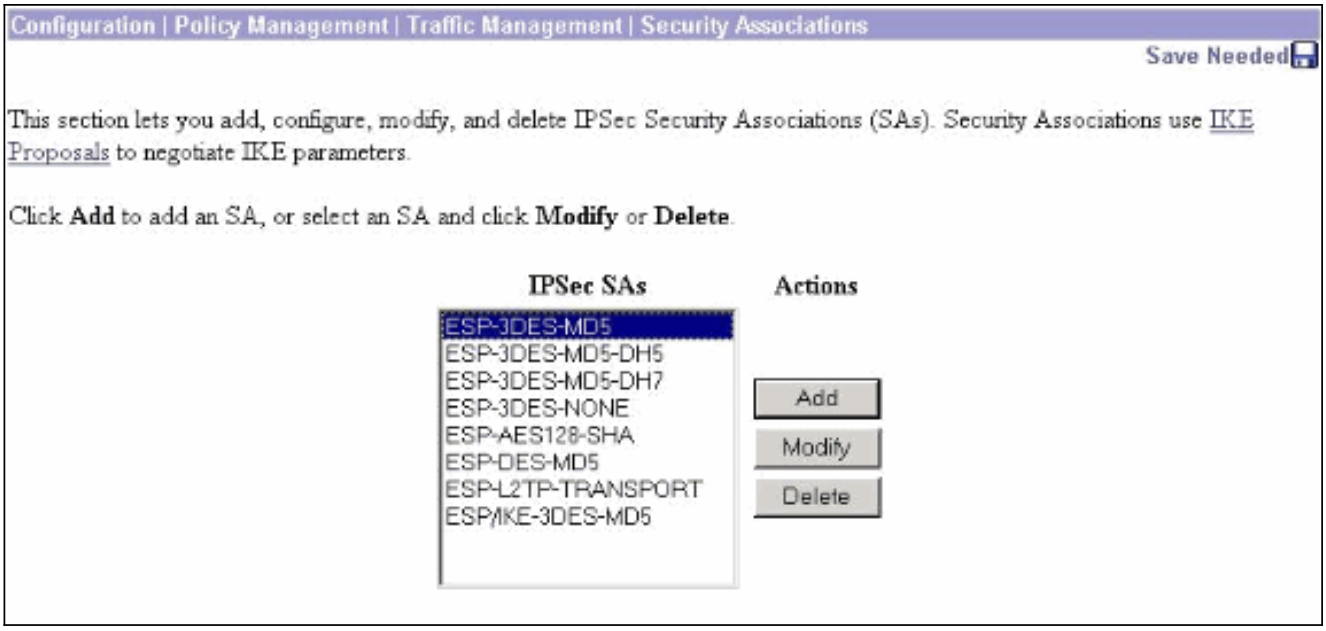
VPN 3000 Concentrator-Zertifikate für VPN-Clients

Führen Sie diese Schritte aus, um VPN 300 Concentrator-Zertifikate für VPN-Clients zu konfigurieren.

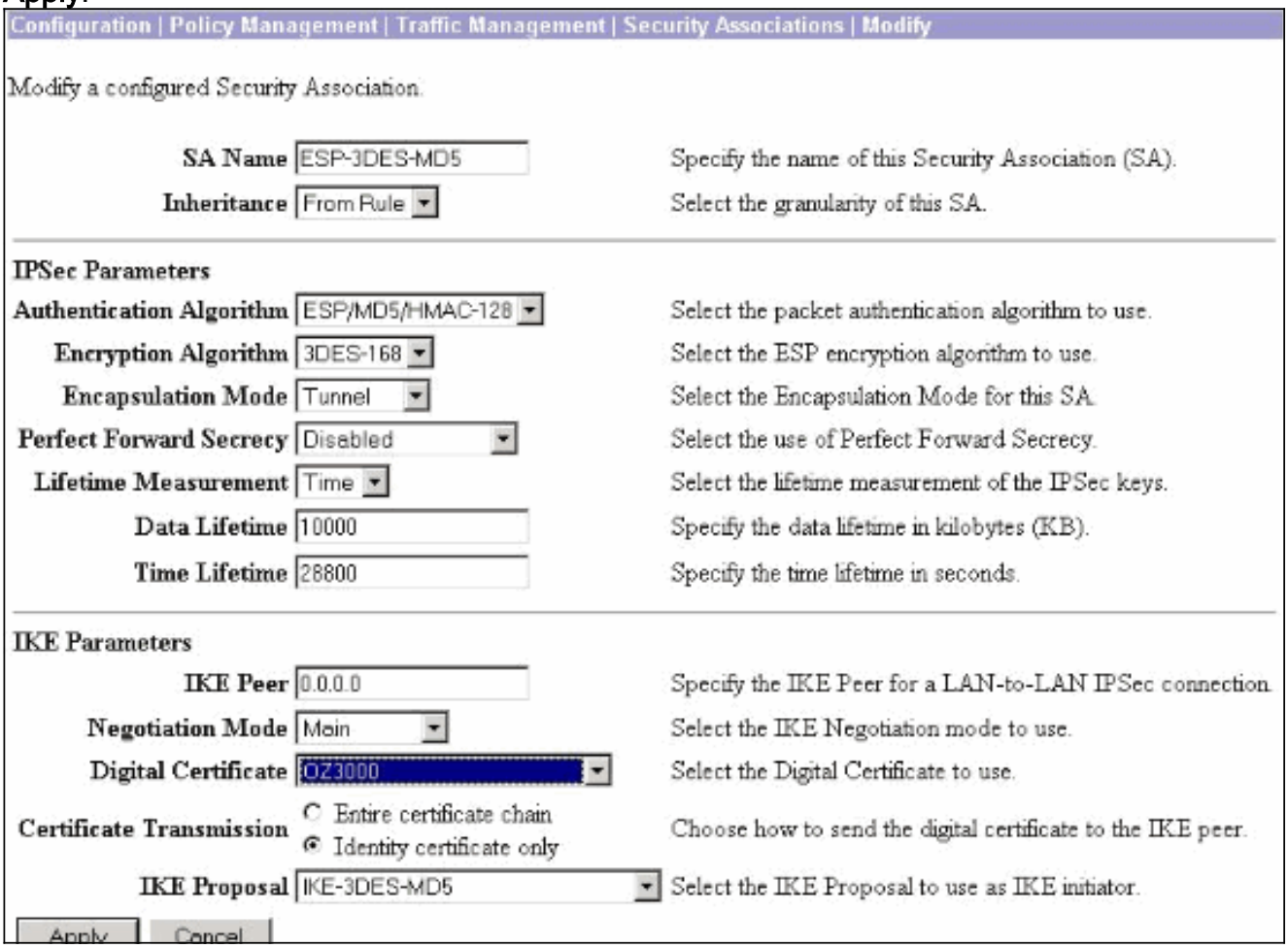
1. Die IKE-Richtlinie muss für die Verwendung von Zertifikaten im Manager der VPN 3000 Concentrator-Serie konfiguriert werden. Um die IKE-Richtlinie zu konfigurieren, wählen Sie **Configuration > System > Tunneling Protocols > IPsec > IKE Proposal aus, und verschieben Sie CiscoVPNClient-3DES-MD5-RSA in die aktiven Angebote.**



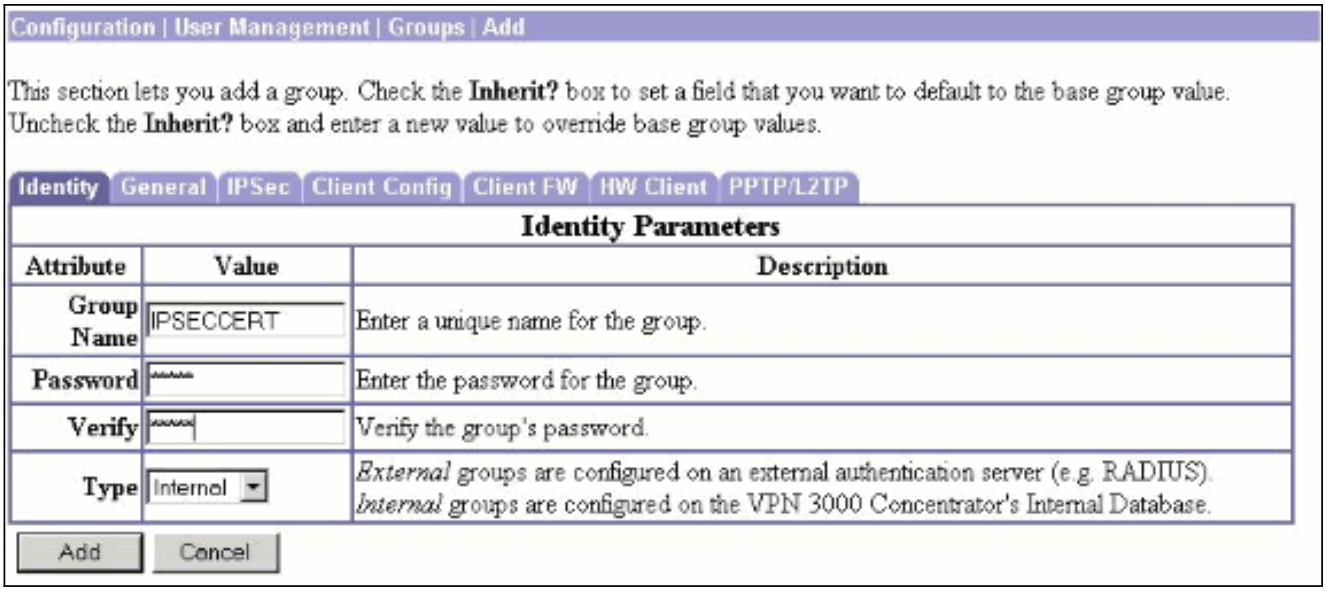
2. Sie müssen auch die IPsec-Richtlinie so konfigurieren, dass Zertifikate verwendet werden. Wählen Sie **Configuration > Policy Management > Traffic Management > Security Associations (Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Sicherheitszuordnungen) aus**, markieren Sie **ESP-3DES-MD5, und klicken Sie dann auf Modify, um die IPsec-Richtlinie für die Konfiguration der IPsec-Richtlinie zu konfigurieren.**



3. Wählen Sie im Fenster Ändern unter Digitale Zertifikate das installierte Identitätszertifikat aus. Wählen Sie unter IKE-Angebot die Option **CiscoVPNClient-3DES-MD5-RSA aus,** und klicken Sie auf **Apply**.



4. Um eine IPsec-Gruppe zu konfigurieren, wählen Sie **Configuration > User Management > Groups > Add** aus, fügen Sie die Gruppe **IPSECCERT hinzu (der IPSECCERT-Gruppenname stimmt mit der Organisationseinheit (OU) im Identitätszertifikat überein), und wählen Sie ein Kennwort aus.**Dieses Kennwort wird nirgends verwendet, wenn Sie Zertifikate verwenden. In diesem Beispiel ist "cisco123" das Kennwort.



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.

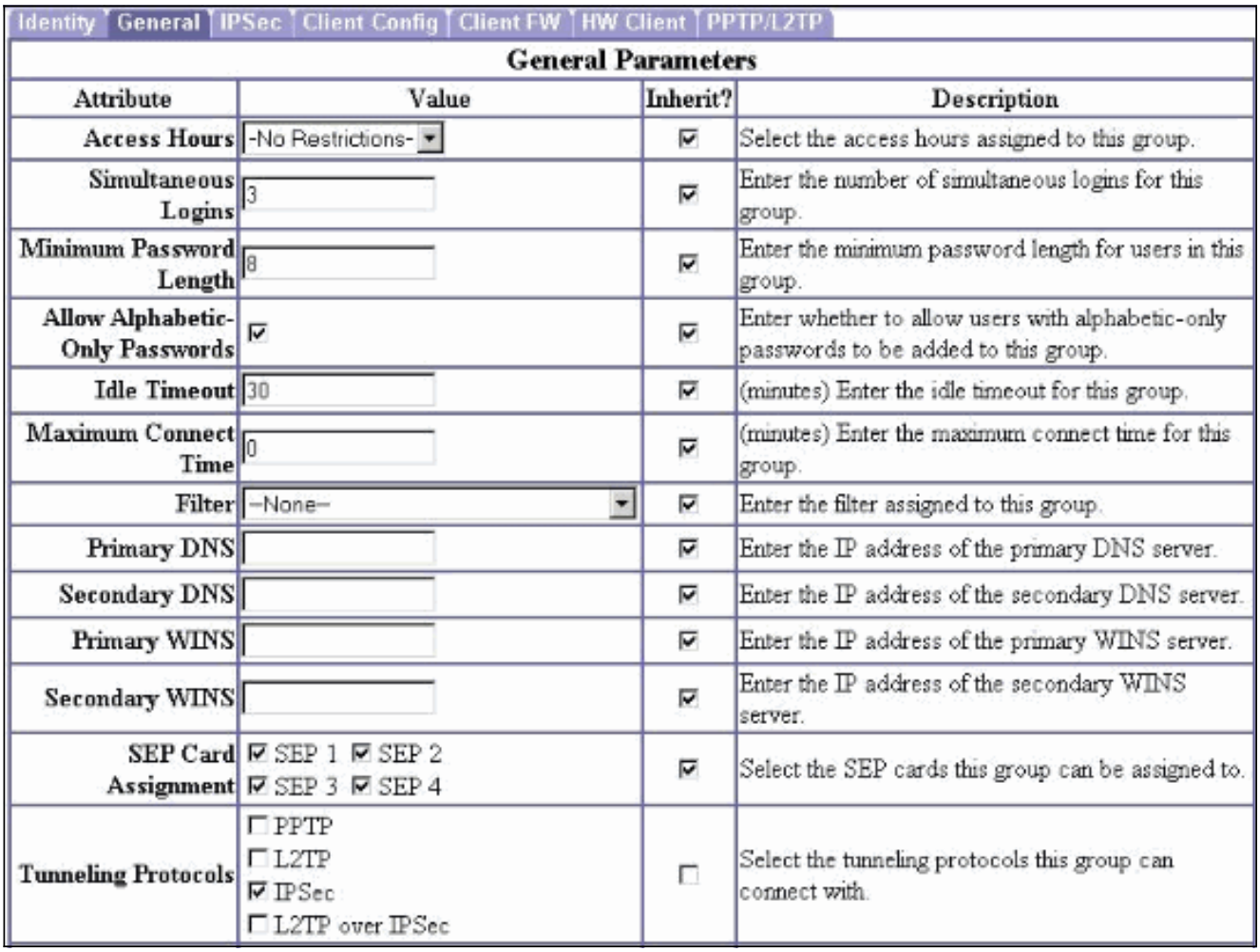
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Klicken Sie auf derselben Seite auf die Registerkarte Allgemein, und wählen Sie **IPsec** als Tunneling Protocol
aus.

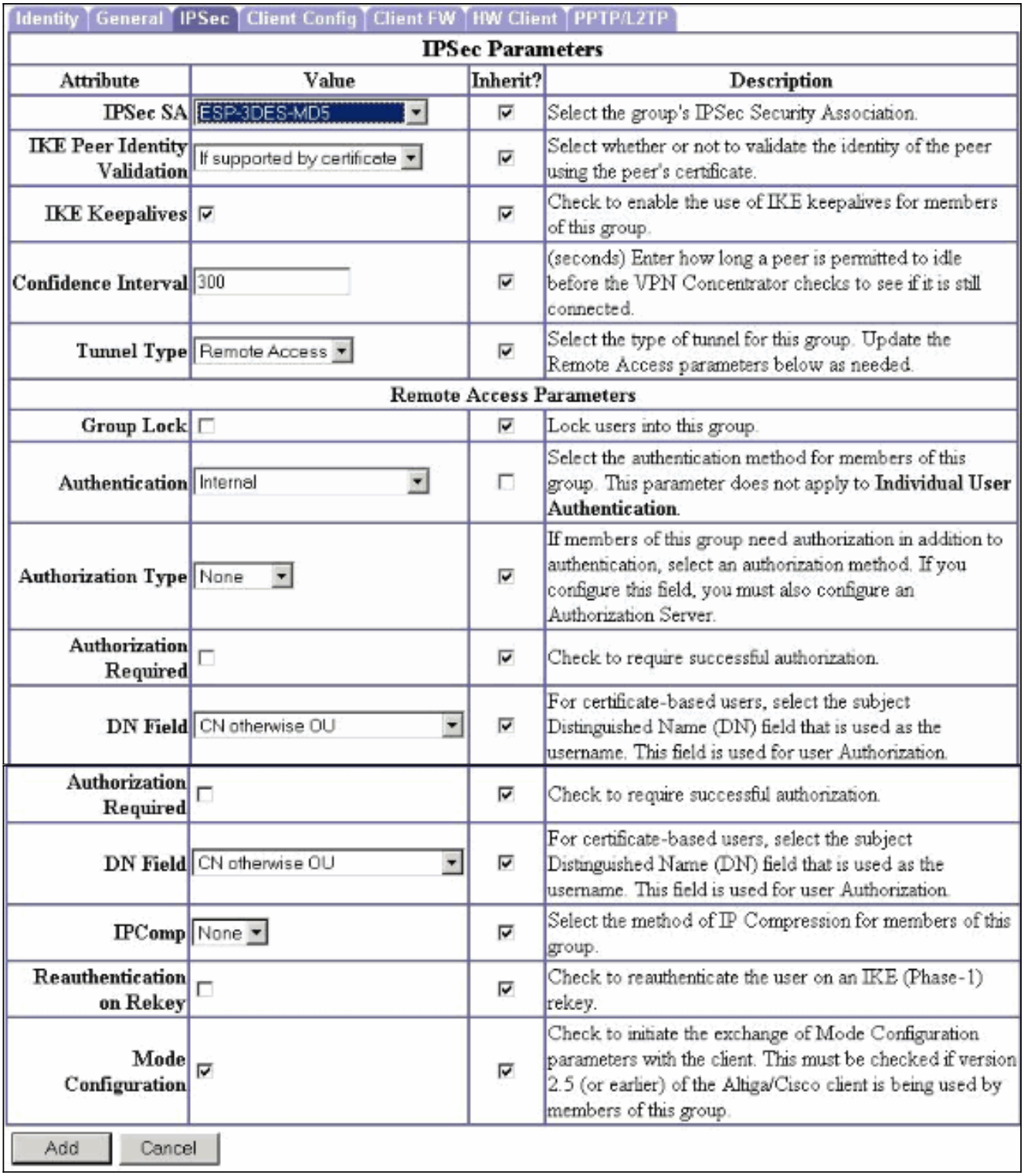


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Klicken Sie auf die Registerkarte IPsec (IPsec), und stellen Sie sicher, dass Ihre konfigurierte IPsec Security Association (SA) unter IPsec SA (IPsec-SA) ausgewählt ist, und klicken Sie auf **Apply**
(Übernehmen).



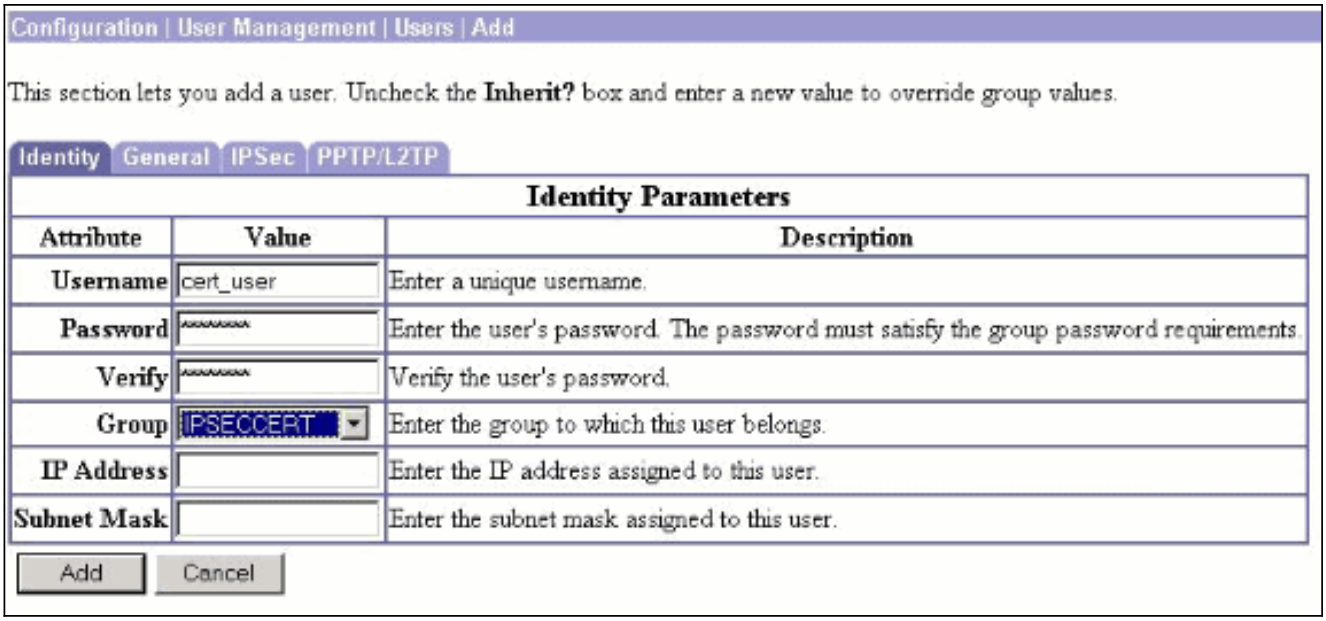
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

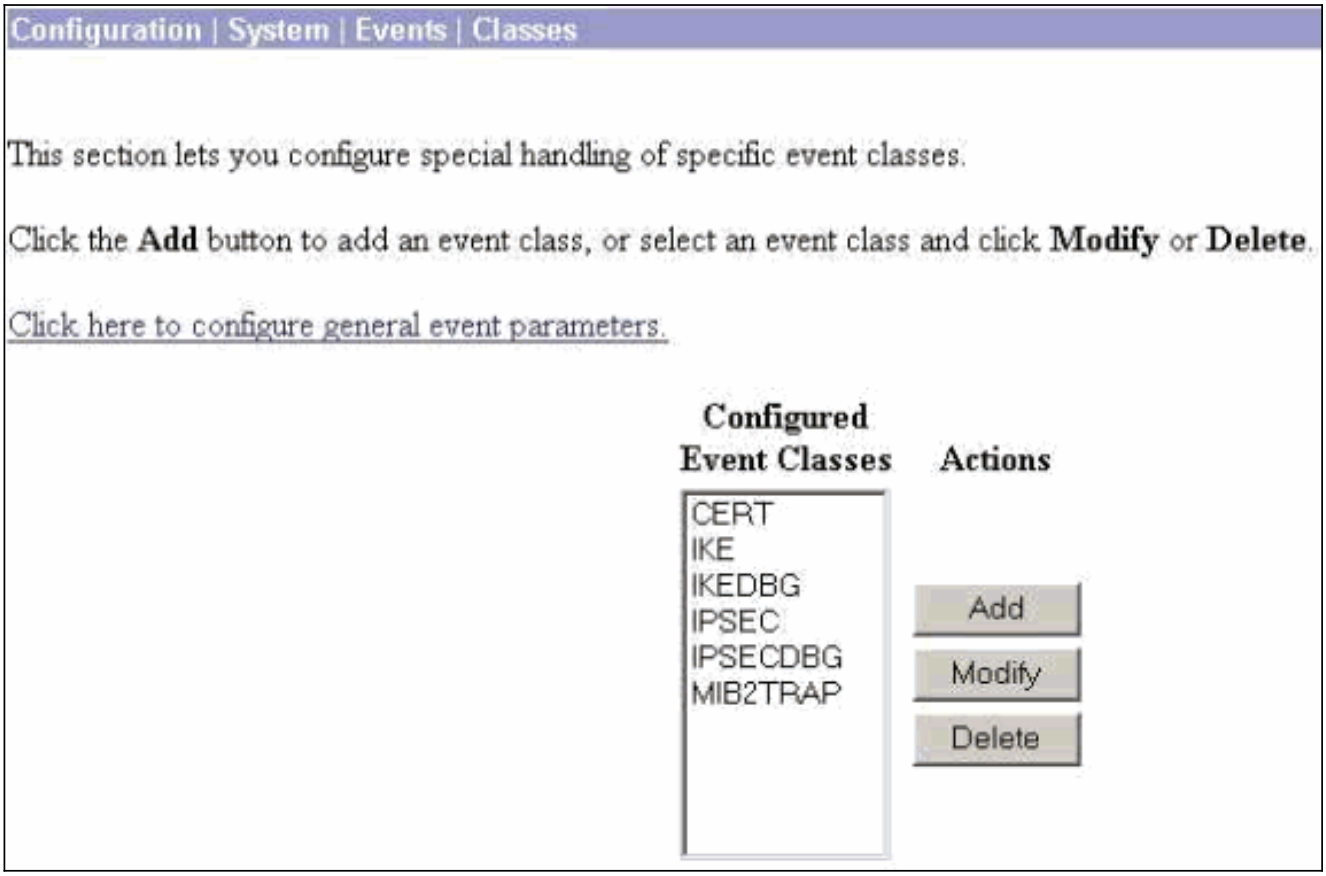
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

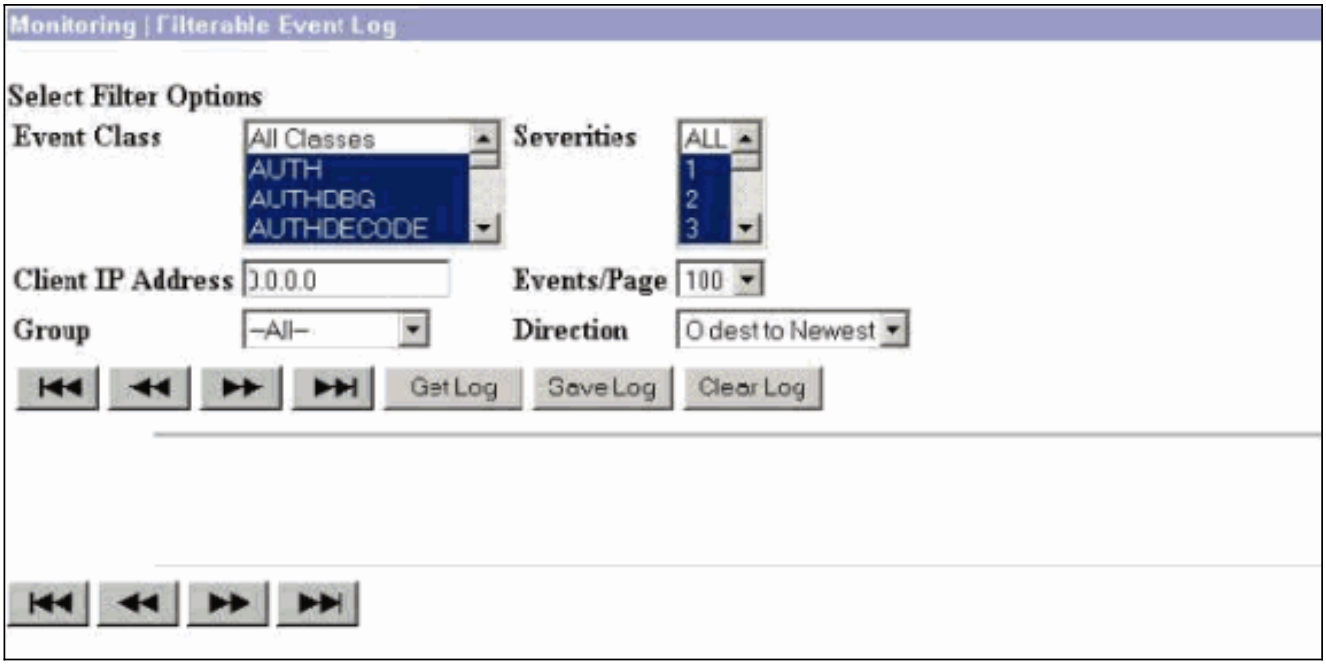
7. Um eine IPsec-Gruppe im VPN 3000-Konzentrator zu konfigurieren, wählen Sie **Konfiguration > Benutzerverwaltung > Benutzer > Hinzufügen**, geben Sie einen Benutzernamen, ein Kennwort und den Gruppennamen an, und klicken Sie dann auf **Hinzufügen.**Im Beispiel werden folgende Felder verwendet:Benutzername = cert_userKennwort = cisco123Verifizieren = cisco123Gruppe = IPSECCERT



8. Um das Debuggen auf dem VPN 3000 Concentrator zu aktivieren, wählen Sie **Configuration > System > Events > Classes aus**, und fügen Sie folgende Klassen hinzu:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. Wählen Sie **Monitoring > Filterable Event Log** (**Überwachung > Filterbares Ereignisprotokoll**, um die Debuggen
anzuzeigen.



Hinweis: Wenn Sie die IP-Adressen ändern möchten, können Sie die neuen IP-Adressen registrieren und das ausgestellte Zertifikat später mit diesen neuen Adressen installieren.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Weitere Informationen zur Fehlerbehebung finden Sie unter Beheben von Verbindungsproblemen im VPN 3000 Concentrator.

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 3000
- Cisco VPN 3002 Hardware-Clients
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems