Configurazione di VPN 3000 Concentrator per comunicare con il client VPN utilizzando i certificati

Sommario

Introduzione

Questo documento include istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator con client VPN con l'uso di certificati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco VPN 3000 Concentrator versione 4.0.4A.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

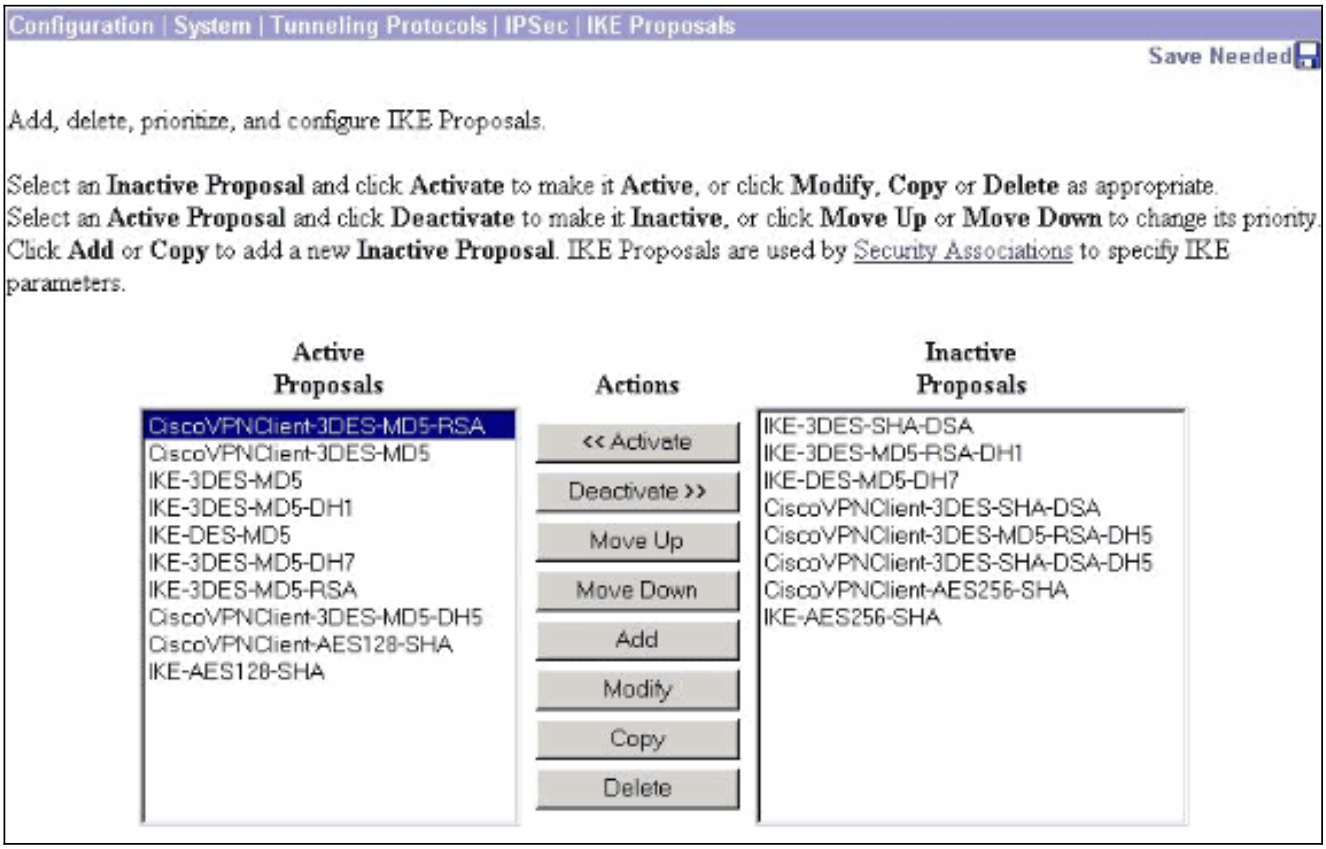
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

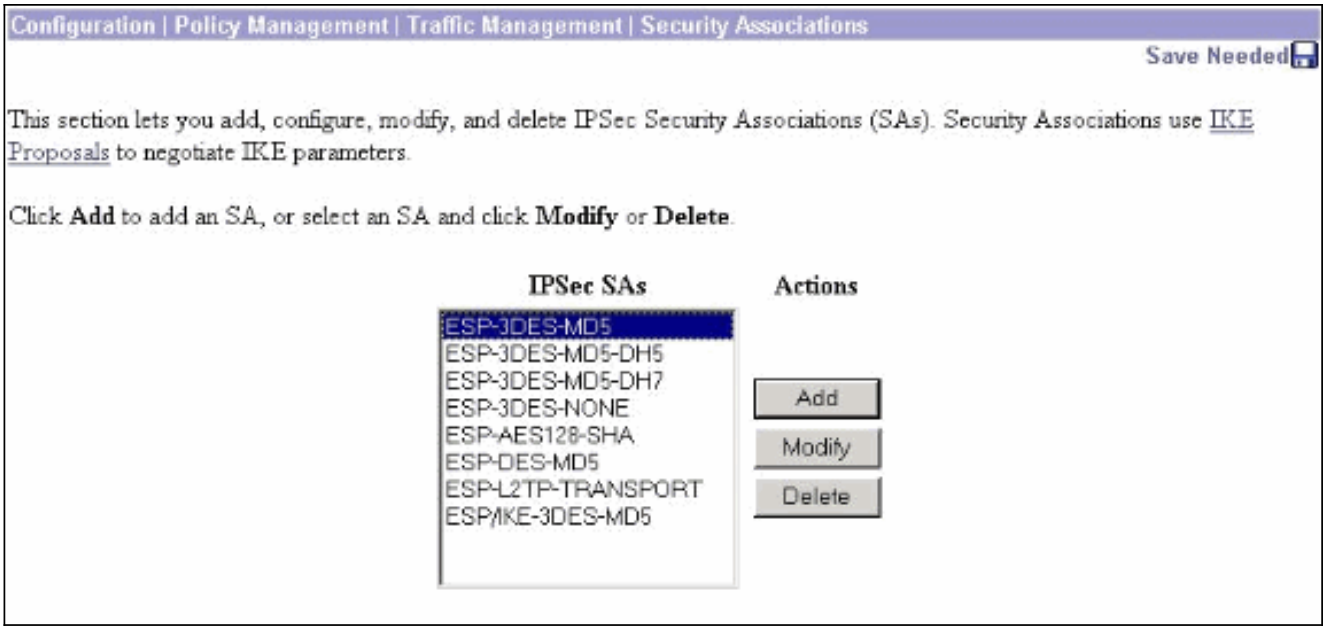
Certificati VPN 3000 Concentrator per client VPN

Completare questa procedura per configurare i certificati VPN 3000 Concentrator per i client VPN.

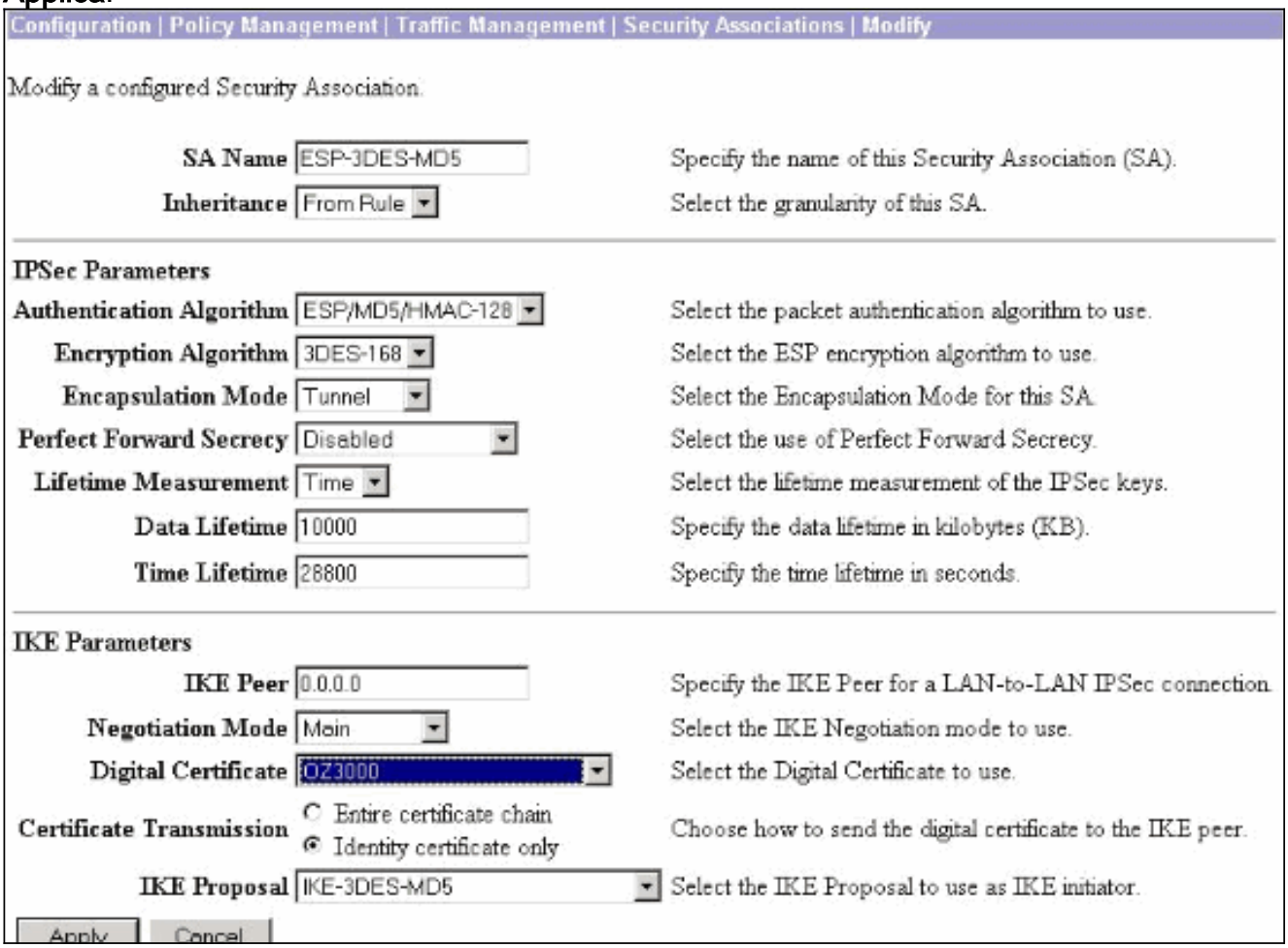
1. Ènecessario configurare il criterio IKE per l'utilizzo di certificati su VPN 3000 Concentrator Series Manager. Per configurare la policy IKE, selezionare Configurazione > Sistema > Protocolli di tunneling > **IPsec** > **Proposte IKE**, quindi spostare **CiscoVPNClient-3DES-MD5-RSA** nelle proposte
attive.



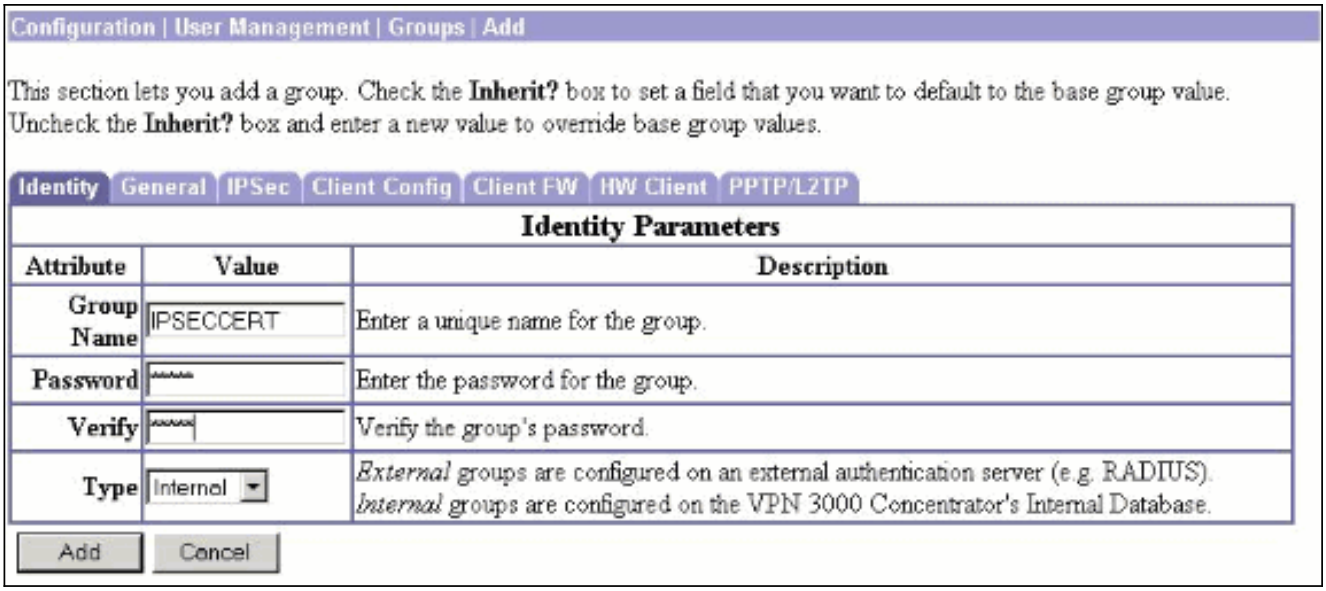
2. Èinoltre necessario configurare il criterio IPSec per l'utilizzo dei certificati. Selezionare Configurazione > Gestione criteri > Gestione traffico > **Associazioni di sicurezza**, evidenziare **ESP-3DES-MD5** e fare clic su **Modifica per configurare il criterio IPSec** per configurare il criterio
IPSec.



3. Nella finestra Modifica, in Certificati digitali, assicurarsi di selezionare il certificato di identità installato. In Proposta IKE selezionare **CiscoVPNClient-3DES-MD5-RSA** e fare clic su **Applica**.



4. Per configurare un gruppo IPSec, selezionare Configurazione > **Gestione utenti** > **Gruppi** > **Aggiungi**, aggiungere un gruppo denominato **IPSECCERT** (il nome del gruppo IPSECCERT corrisponde all'unità organizzativa nel certificato di identità) e selezionare una password.Questa password non viene utilizzata in alcun modo se si utilizzano certificati. Nell'esempio, "cisco123" è la
password.



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.

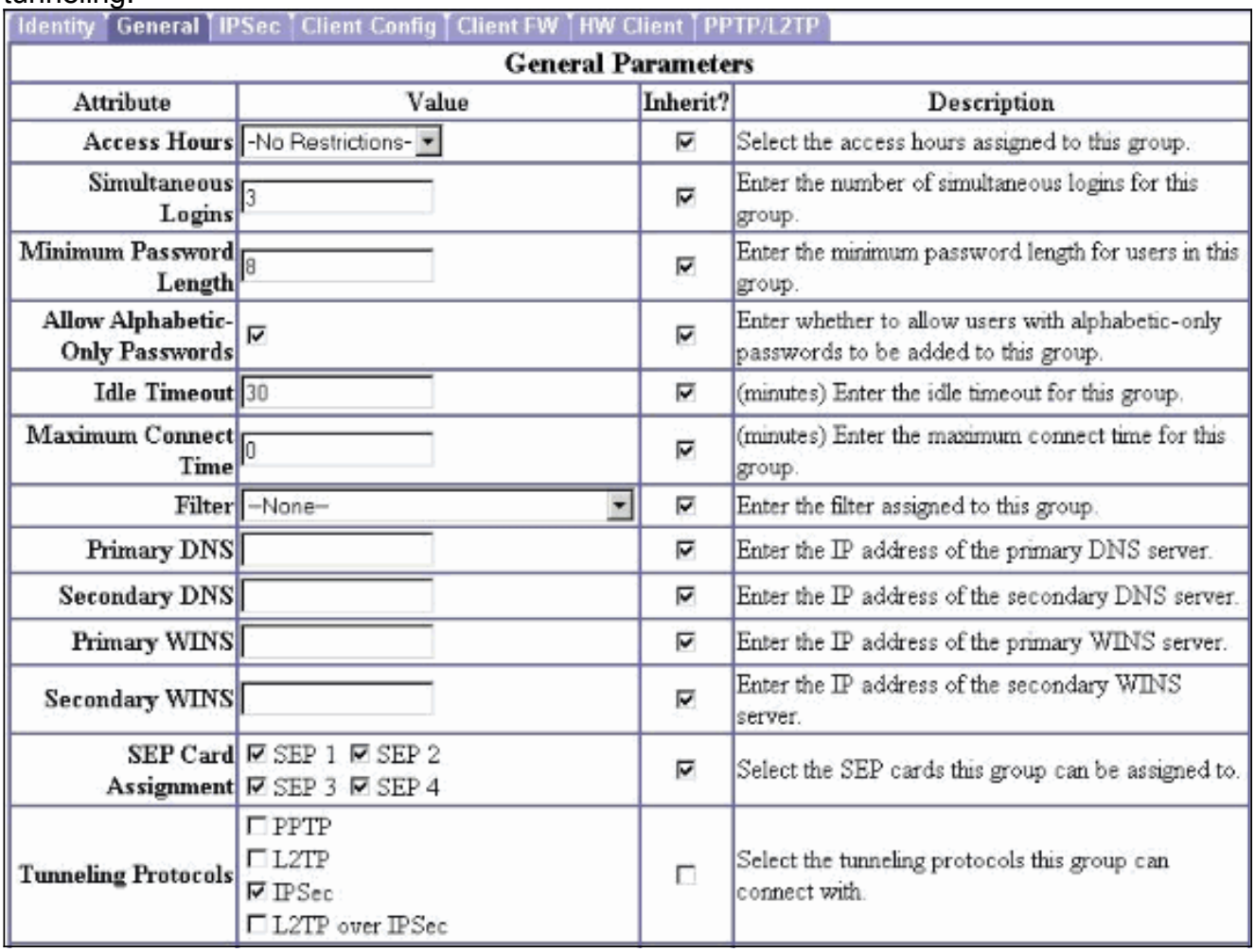
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Nella stessa pagina, fare clic sulla scheda General (Generale) e verificare di aver selezionato **IPsec** come protocollo di tunneling.



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. Fare clic sulla scheda IPSec e verificare che l'associazione di protezione (SA) IPSec configurata sia selezionata in SA IPSec e fare clic su **Applica**.

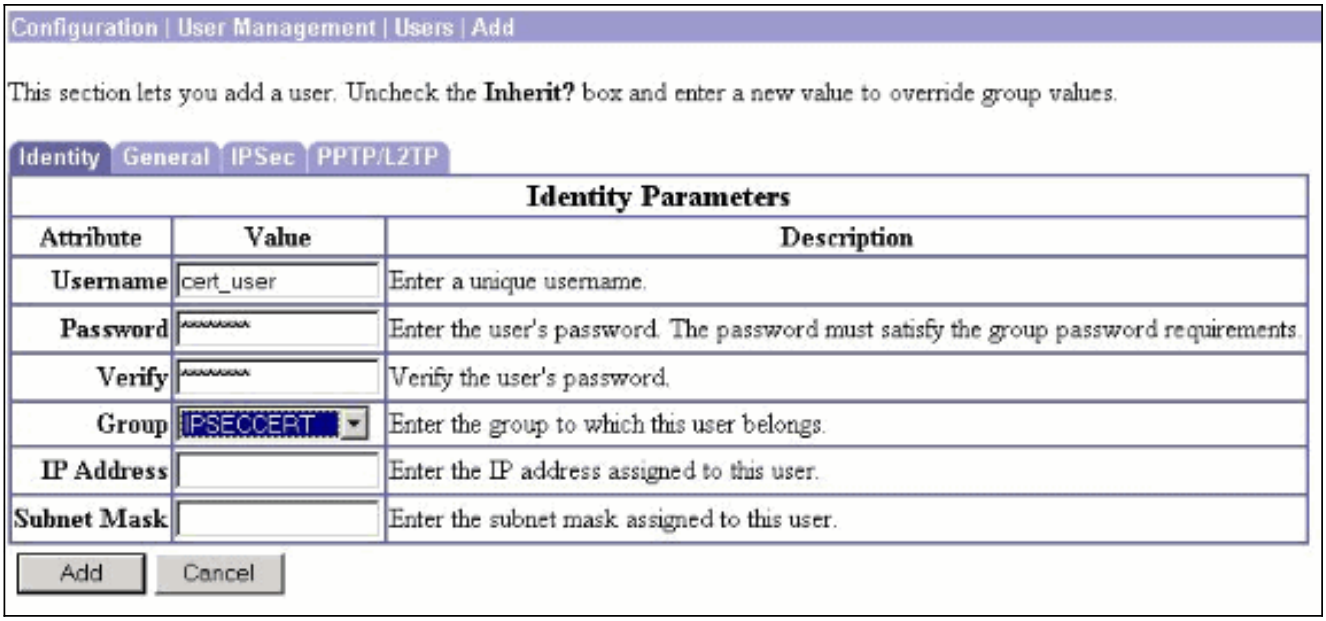
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

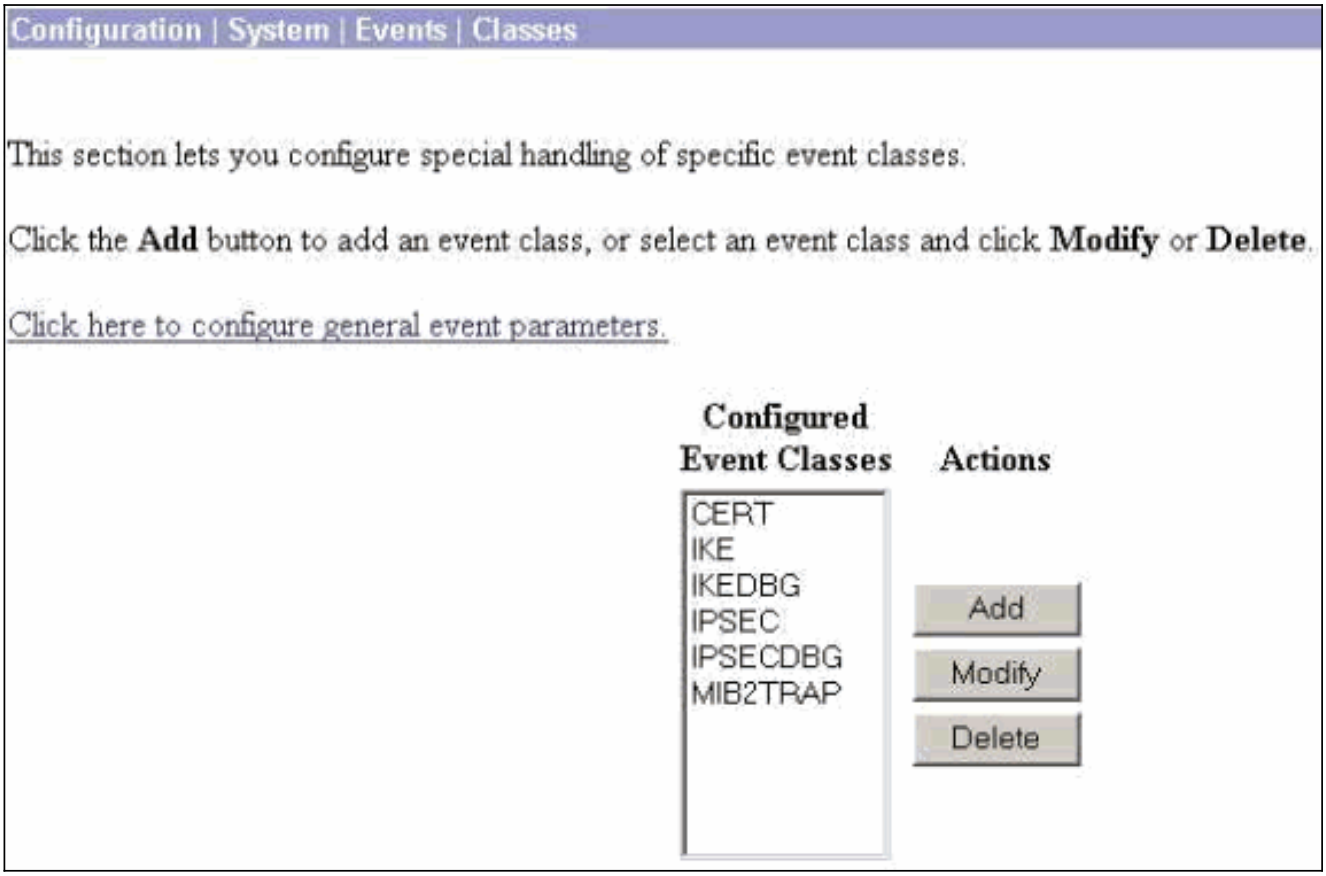
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

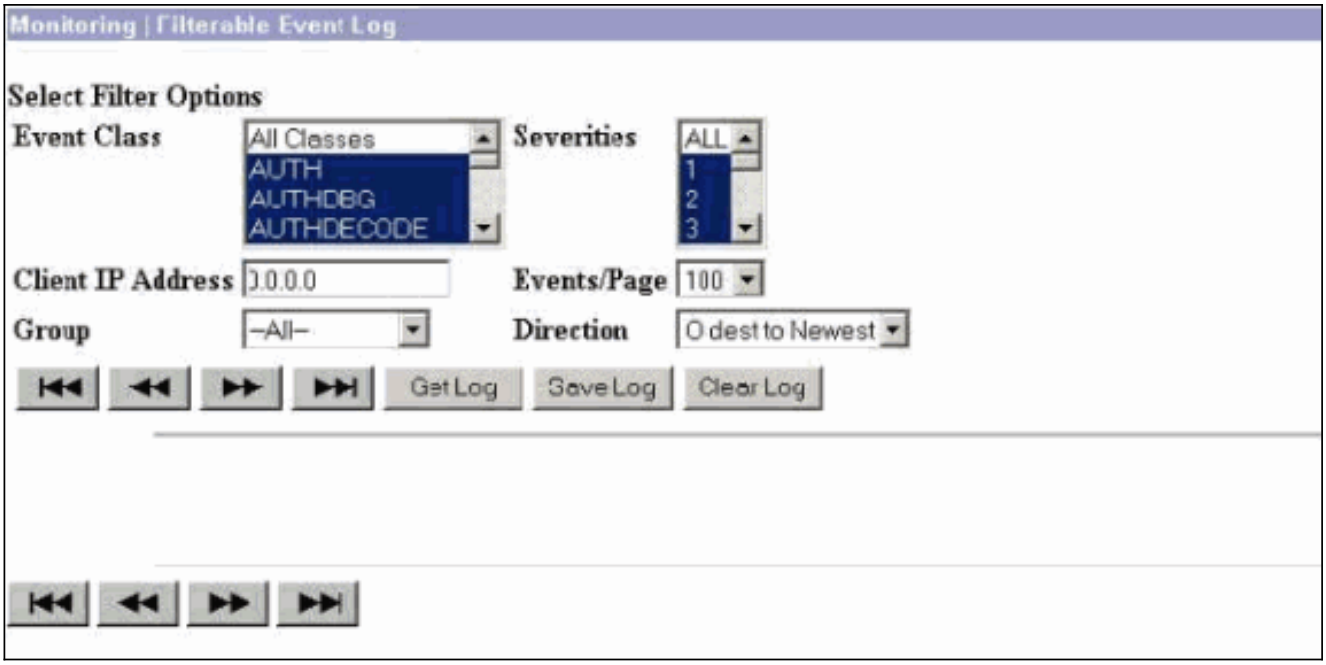
7. Per configurare un gruppo IPSec nel concentratore VPN 3000, selezionare Configurazione > **Gestione utenti > Utenti > Aggiungi**, specificare un nome utente, una password e il nome del gruppo, quindi fare clic su **Aggiungi**.Nell'esempio vengono utilizzati i campi seguenti:Nome utente = cert_userPassword = cisco123Verifica = cisco123Group = IPSECCERT



8. Per abilitare il debug su VPN 3000 Concentrator, selezionare **Configurazione > Sistema > Eventi > Classi** e aggiungere le seguenti classi:CERTIFICATO 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. Per visualizzare i debug, selezionare **Monitoraggio > Registro eventi filtrabili**.



Nota: se si decide di modificare gli indirizzi IP, è possibile effettuare la registrazione dei nuovi indirizzi IP e installare il certificato rilasciato in un secondo momento con questi nuovi indirizzi.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi, fare riferimento a Risoluzione dei problemi di connessione su VPN 3000 Concentrator.

Informazioni correlate

- Cisco VPN serie 3000 concentrator
- Client hardware Cisco VPN 3002
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems