인증서를 사용하여 VPN 클라이언트와 통신하도록 VPN 3000 Concentrator 구성

목차

소개

이 문서에는 인증서를 사용하여 VPN 클라이언트를 사용하여 Cisco VPN 3000 Series Concentrator를 구성하는 방법에 대한 단계별 지침이 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator 소프트웨어 버전 4.0.4A를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

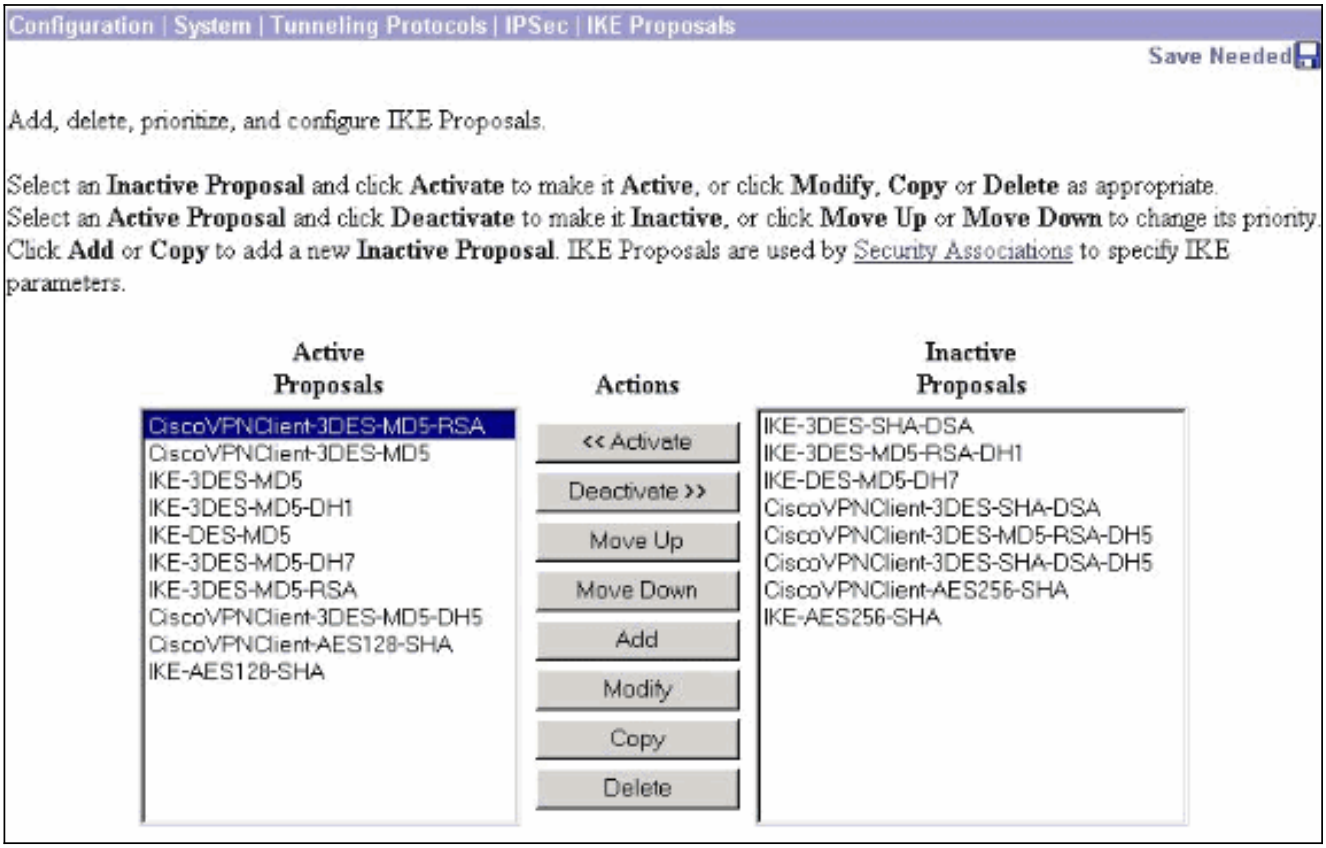
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

VPN 클라이언트용 VPN 3000 Concentrator 인증서

VPN 클라이언트에 대한 VPN 3000 Concentrator 인증서를 구성하려면 다음 단계를 완료하십시오.

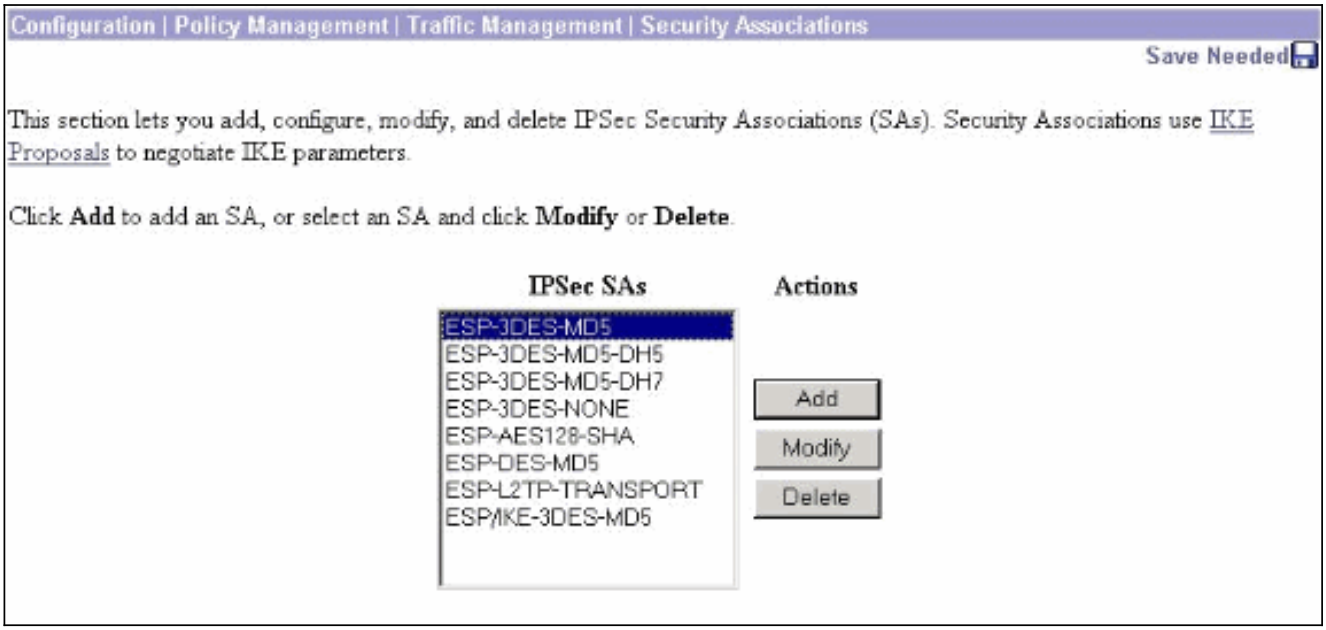
1. VPN 3000 Concentrator Series Manager에서 인증서를 사용하도록 IKE 정책을 구성해야 합니다. IKE 정책을 구성하려면 **Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPsec >** IKE Proposals(**IKE 제안)를** 선택하고 **CiscoVPNClient-3DES-MD5-RSA를 Active Proposals로 이동합니다**

.



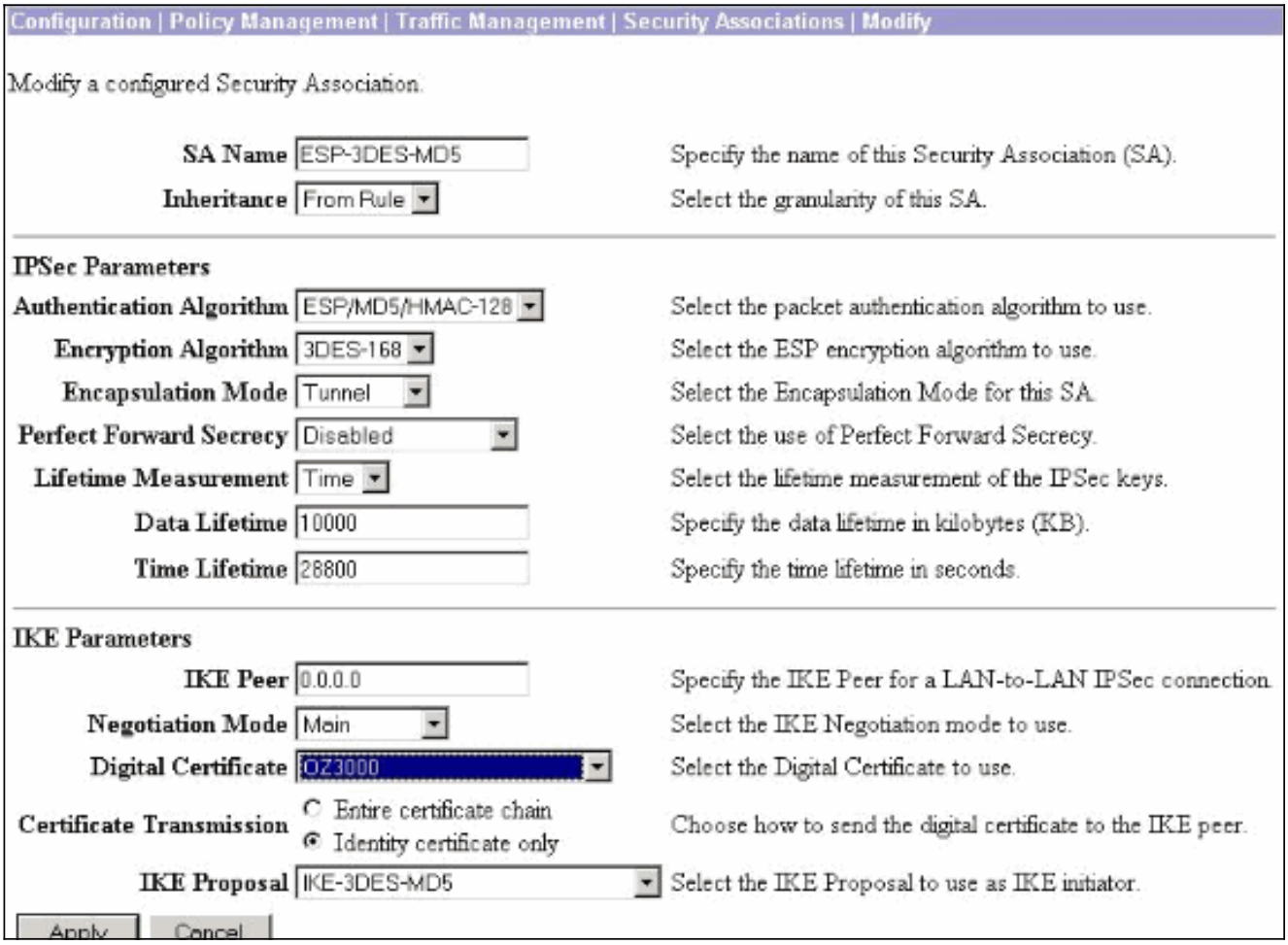
2. 또한 인증서를 사용하도록 IPsec 정책을 구성해야 합니다. Configuration(**구성**) > **Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결)를** 선택하고 **ESP-3DES-MD5를 선택한 다음 Modify(수정)를 클릭하여 IPsec 정책을 구성하여 IPsec 정책을 구성합니다**

.



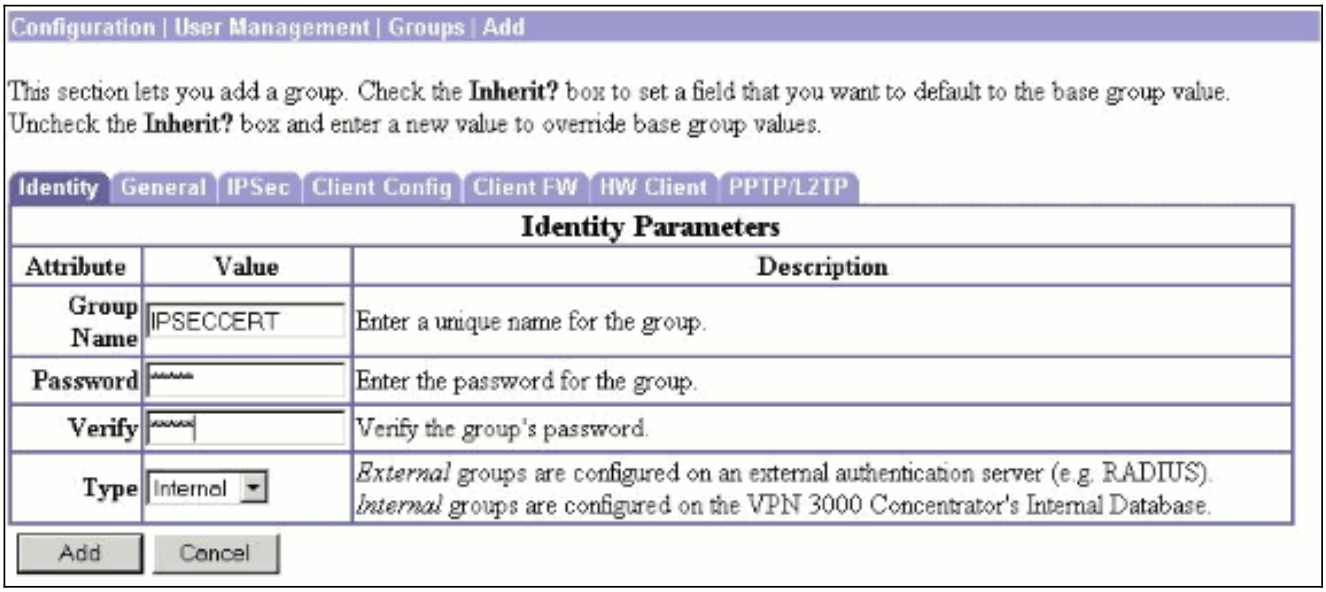
3. Modify(수정) 창의 Digital Certificates(디지털 인증서)에서 설치된 ID 인증서를 선택해야 합니다. IKE Proposal(IKE 제안)에서 **CiscoVPNClient-3DES-MD5-RSA를 선택하고 Apply(적용)를 클릭합니다**

.



4. IPsec 그룹을 구성하려면 **Configuration > User Management > Groups > Add**를 선택하고 IPSECCERT라는 그룹**을 추가합니다(IPSECCERT 그룹 이름이 ID 인증서의 OU(조직 단위)와 일치). 암호를 선택합니다.**인증서를 사용하는 경우 이 비밀번호는 사용되지 않습니다. 이 예에서 "cisco123"은 비밀번호입니다

.



5. 같은 페이지에서 General(일반) 탭을 클릭하고 IPsec을 Tunneling Protocol(터널링 프로토콜)으로 **선택해야** 합니다

.

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. IPsec 탭을 클릭하고 IPsec SA 아래에서 구성된 IPsec SA(Security Association)가 선택되었는지 확인하고 Apply(적용)를 **클릭합니다**

.

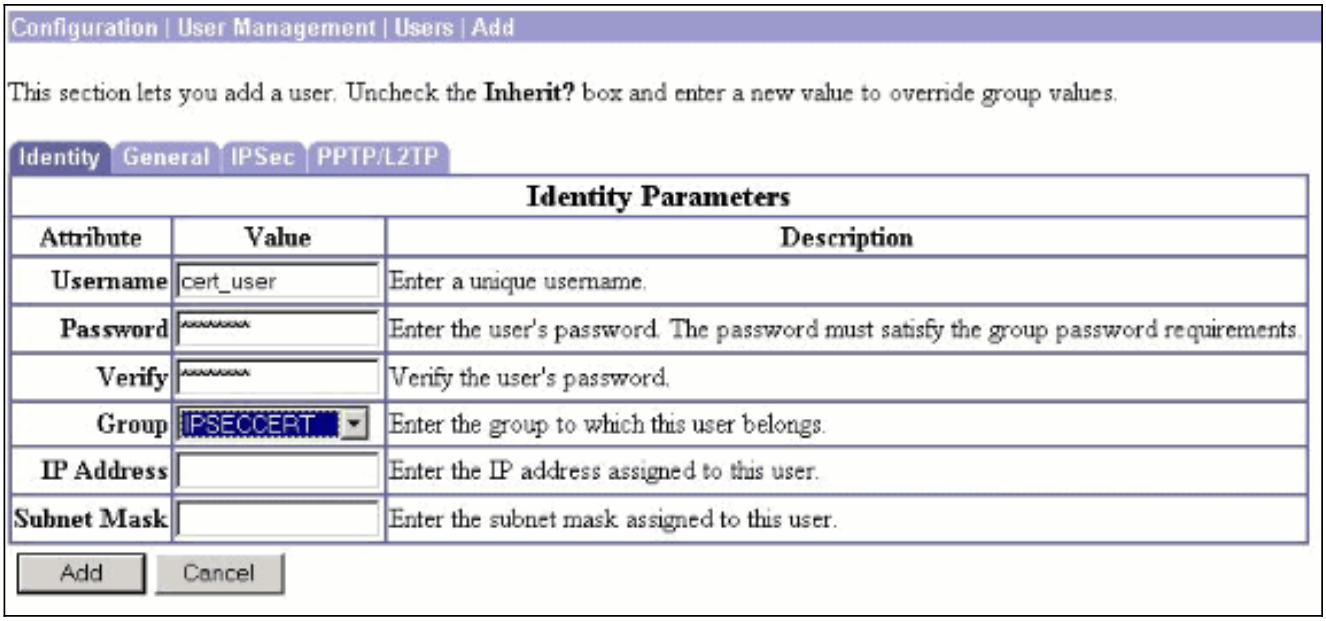
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

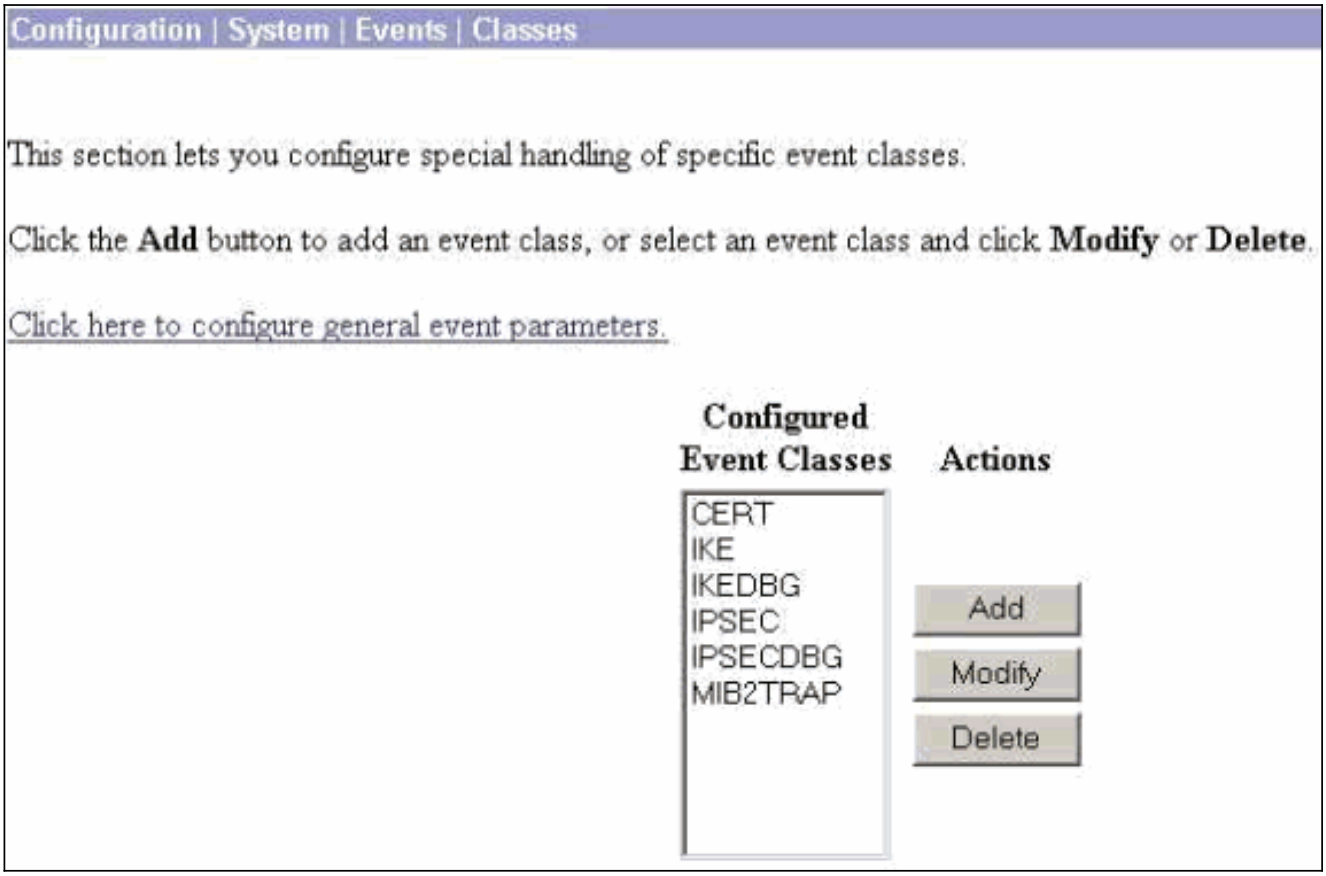
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

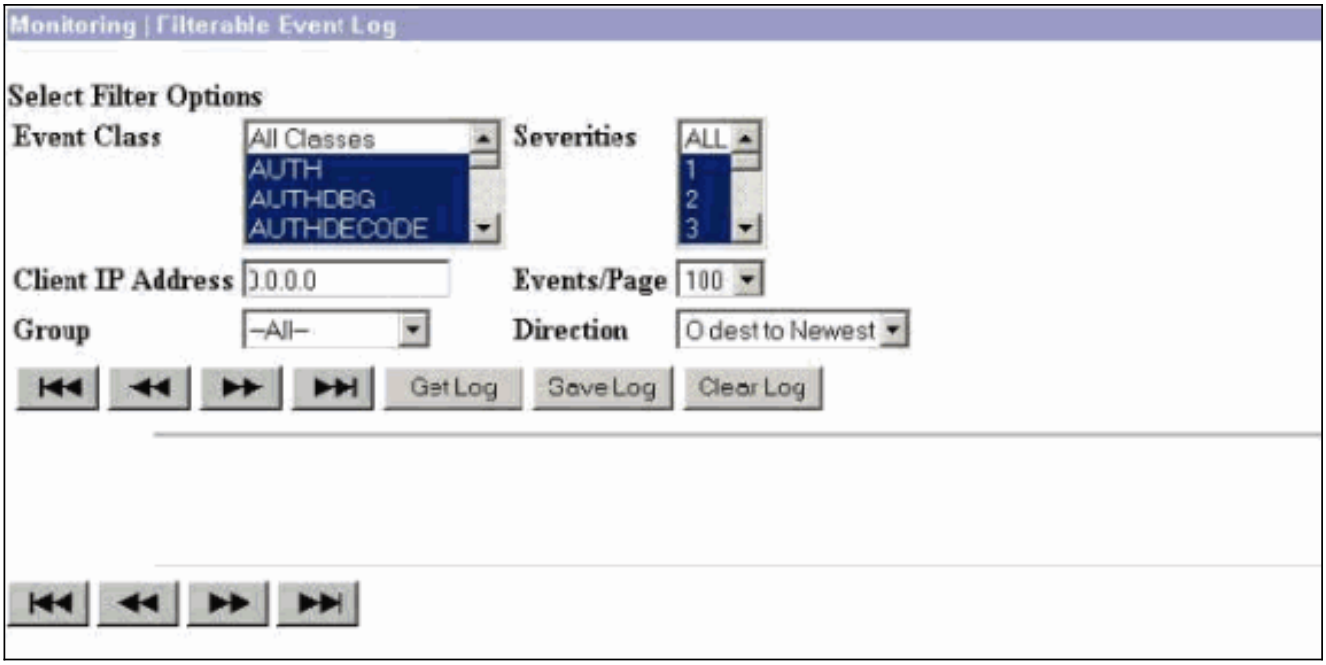
7. VPN 3000 Concentrator에서 IPsec 그룹을 구성하려면 **Configuration > User Management > Users > Add**를 선택하고 사용자 이름, 암호 및 그룹 이름을 지정한 다음 Add를 **클릭합니다.**이 예에서는 다음 필드가 사용됩니다.사용자 이름 = cert_user비밀번호 = cisco123확인 = cisco123그룹 = IPSECCERT



8. VPN 3000 Concentrator에서 디버깅을 활성화하려면 **Configuration > System > Events > Classes**를 선택하고 다음 클래스를 추가합니다.CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. 디버그를 **보려면 > Filterable Event Log**를 선택합니다
.



참고: IP 주소를 변경하려는 경우 새 IP 주소를 등록하고 발급된 인증서를 나중에 새 주소로 설치할 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

자세한 문제 해결 정보는 VPN 3000 Concentrator의 연결 문제 해결을 참조하십시오.

관련 정보

- Cisco VPN 3000 Series Concentrator
- Cisco VPN 3002 하드웨어 클라이언트
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems