配置 VPN 3000 集中器，使之通过证书与 VPN 客户端通信

目录

简介

本文档包括有关如何使用证书配置带VPN客户端的Cisco VPN 3000系列集中器的分步说明。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco VPN 3000集中器软件版本4.0.4A。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

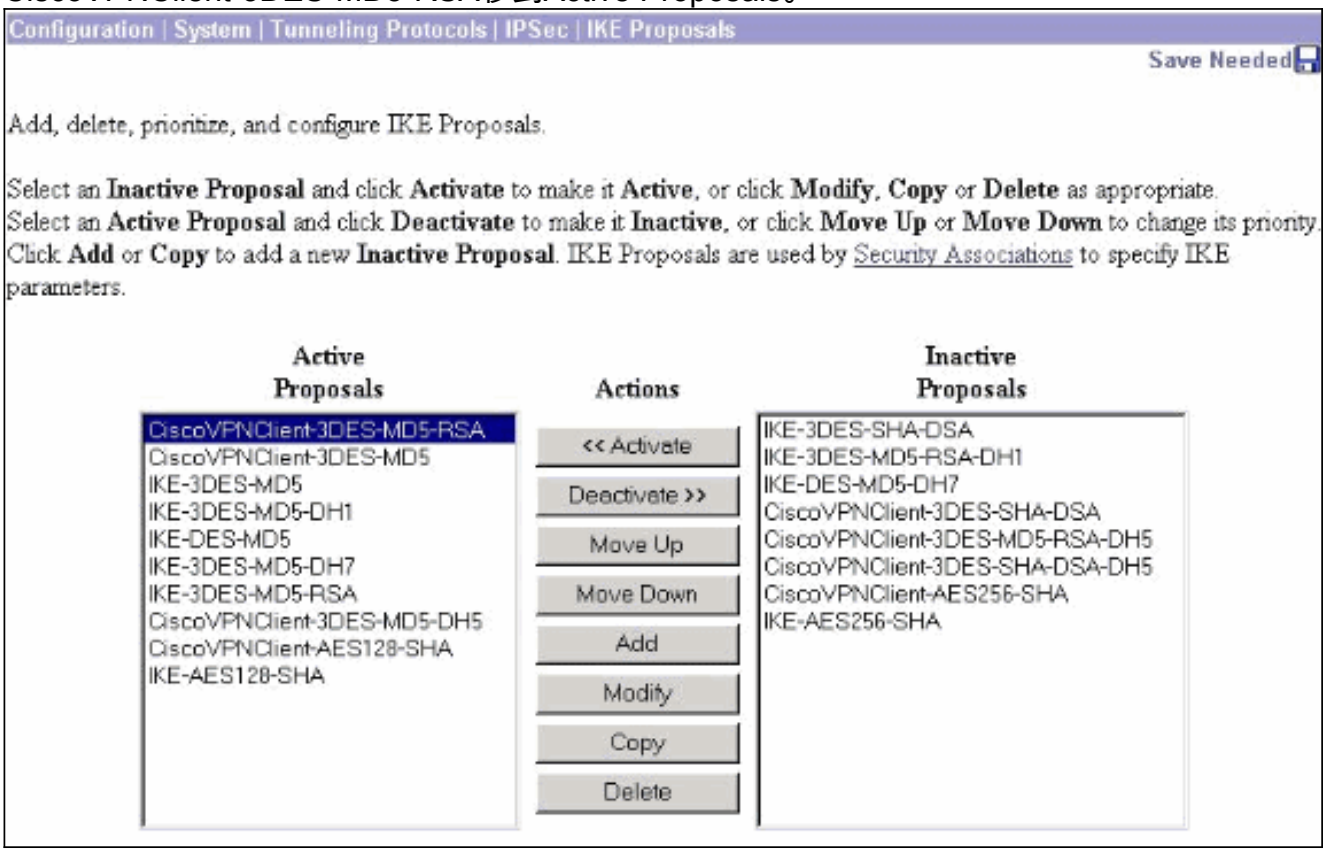
有关文档约定的更多信息，请参考 Cisco 技术提示约定。

VPN 3000 集中器对 VPN 客户端的证书

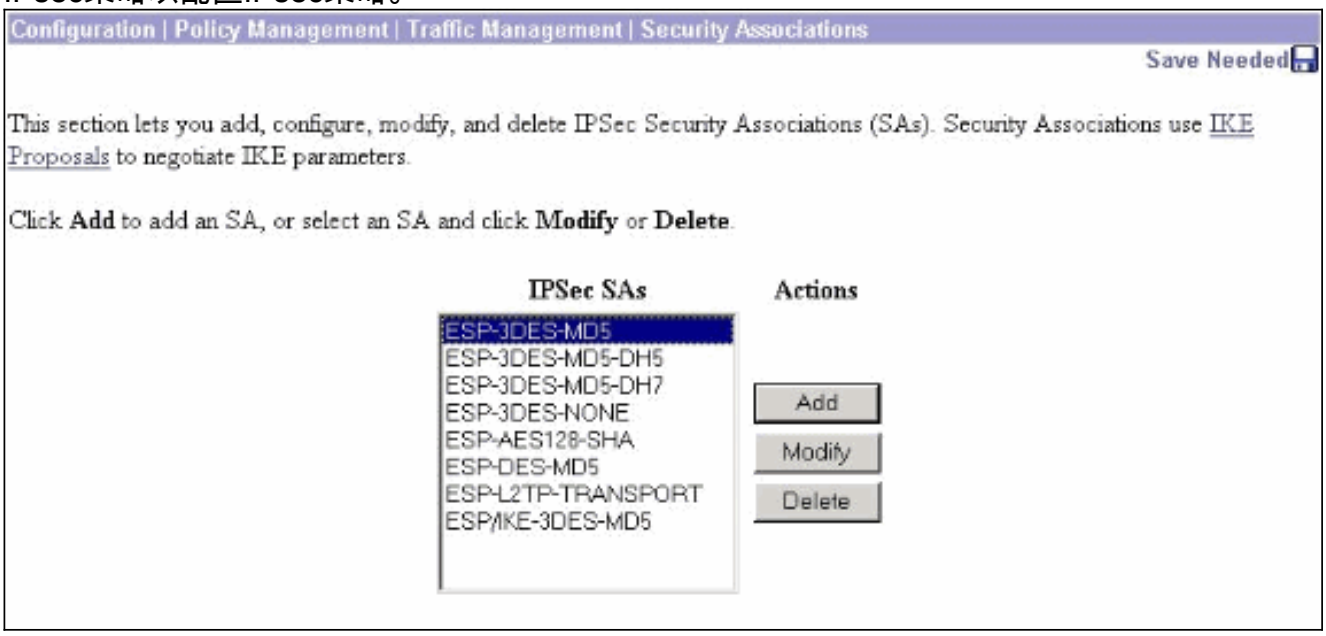
要为VPN客户端配置VPN 3000集中器证书，请完成以下步骤。

1. 必须将IKE策略配置为在VPN 3000集中器系列管理器上使用证书。要配置IKE策略，请选择

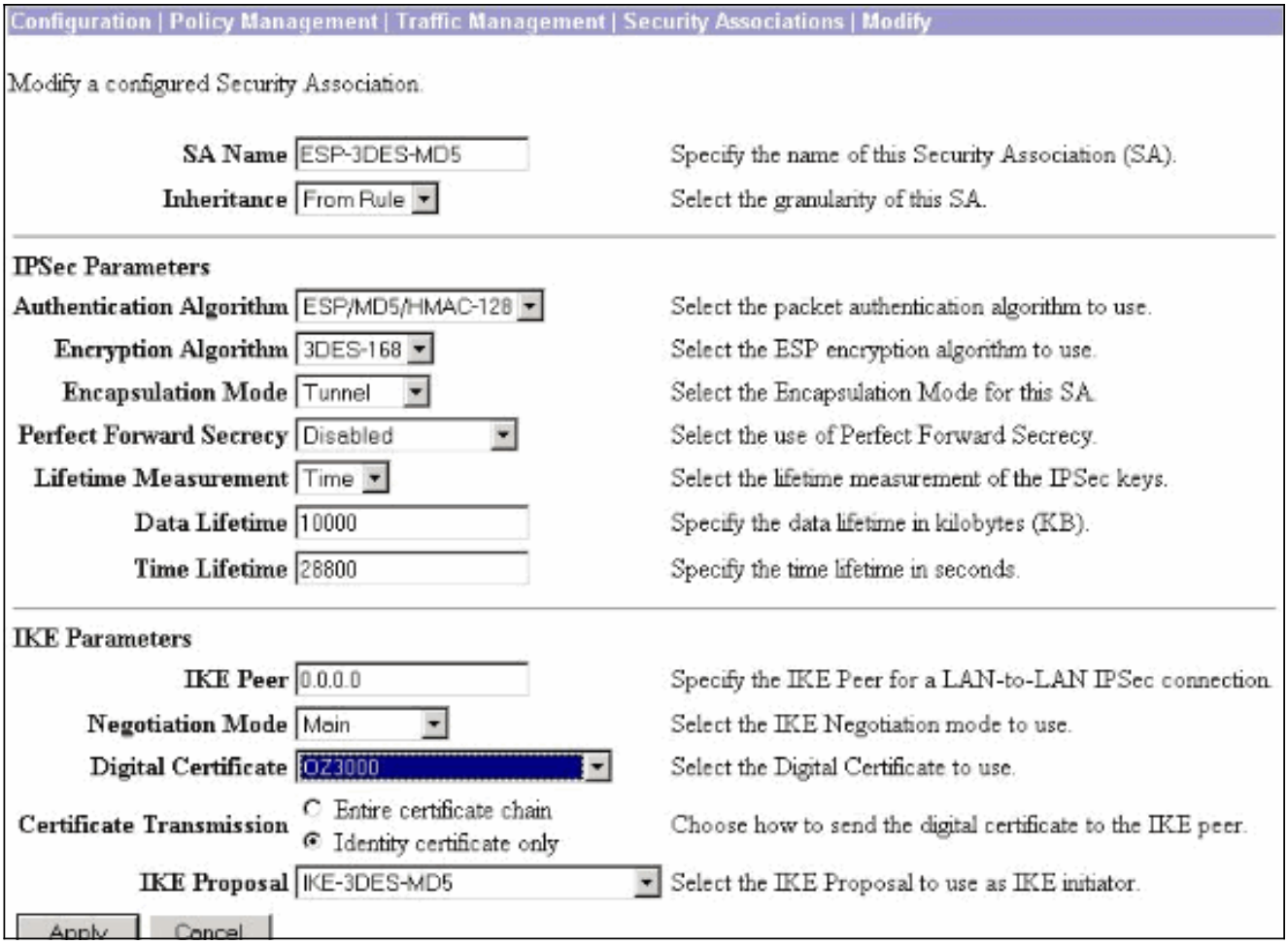
Configuration > System > Tunneling Protocols > IPsec > IKE Proposals ，并将CiscoVPNClient-3DES-MD5-RSA移到Active Proposals。



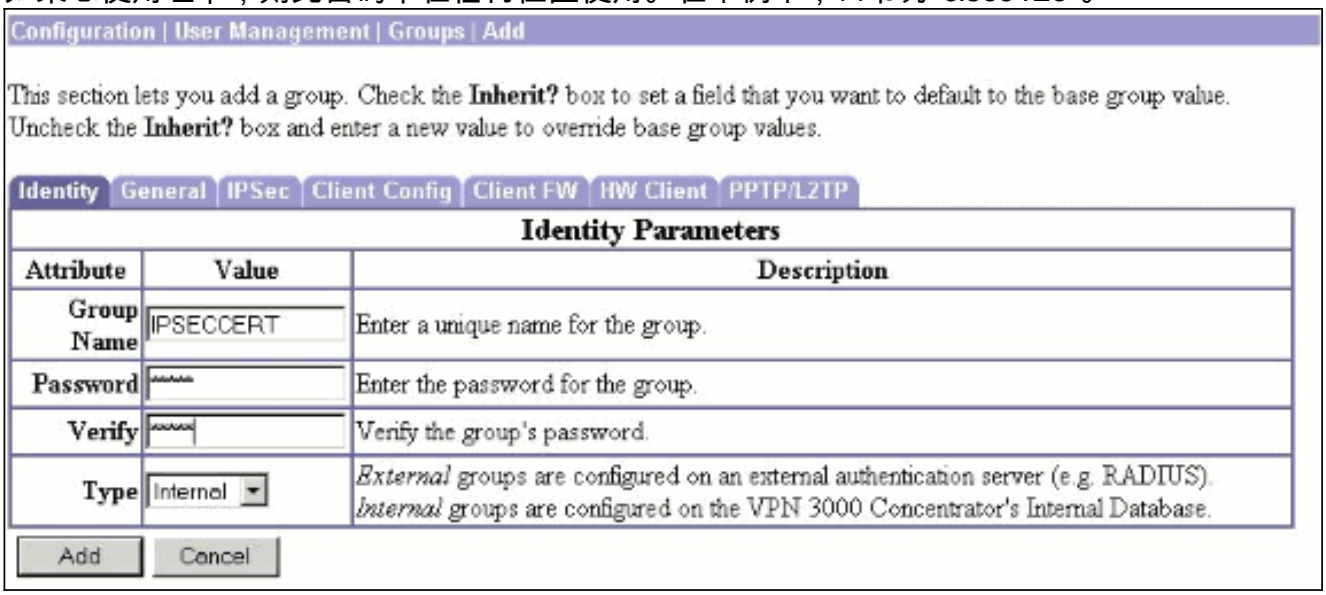
2. 您还必须配置IPsec策略以使用证书。选择Configuration > Policy Management > Traffic Management > Security Associations，突出显示ESP-3DES-MD5，然后点击Modify以配置IPsec策略以配置IPsec策略。



3. 在Modify窗口的Digital Certificates下，确保选择已安装的身份证书。在IKE Proposal下，选择**CiscoVPNClient-3DES-MD5-RSA，然后**单击Apply。



4. 要配置IPsec组，请选择Configuration > **User Management** > Groups > Add ，添加名为 **IPSECCERT** (IPSECCERT组名称与身份证书中的组织单位(OU)匹配)的组，然后选择密码。如果您使用证书，则此密码不在任何位置使用。在本例中，口令为“cisco123”。



5. 在同一页中，单击General选项卡，并确保选择IPsec作为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. 单击IPsec选项卡，确保在IPsec SA下选中已配置的IPsec安全关联(SA)，然后单击**应用**。

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组，请选择Configuration > **User Management** > Users > Add ，指定用户名、密码和组名，然后单击**Add**。在示例中，使用以下字段：用户名= cert_user口令 = cisco123验证= cisco123组= IPSECCERT

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

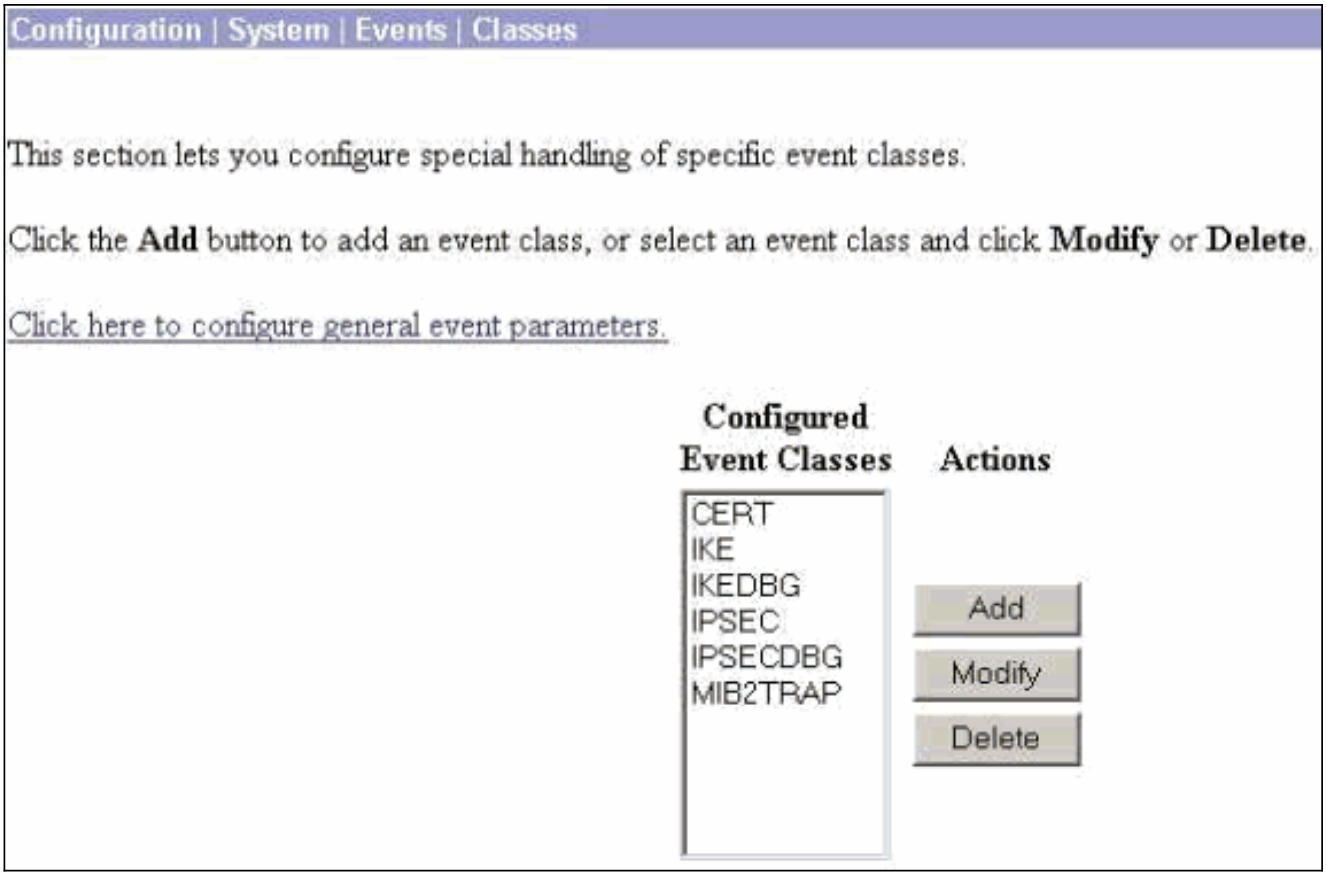
Identity | General | IPSec | PPTP/L2TP

Identity Parameters

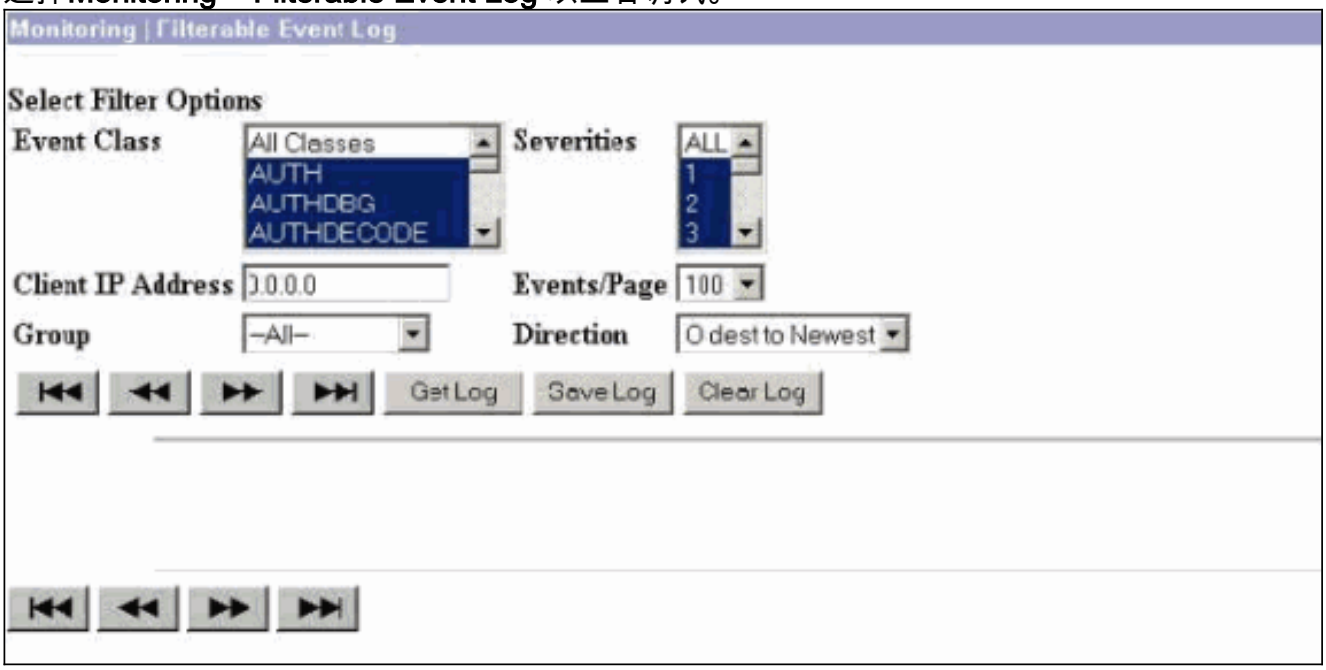
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	********	Enter the user's password. The password must satisfy the group password requirements.
Verify	********	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

8. 要在VPN 3000集中器上启用调试，请选择**Configuration > System > Events > Classes**，然后添加以下类：CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10



9. 选择Monitoring > Filterable Event Log 以查看调试。



注意：如果您决定更改IP地址，则可以注册新IP地址，然后使用这些新地址安装已颁发的证书。

验证

当前没有可用于此配置的验证过程。

故障排除

有关详细故障排除信息，请参阅VPN 3000集中器上的连接问题故障排除。

相关信息

- Cisco VPN 3000 系列集中器
- Cisco VPN 3002 硬件客户端
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems