

配置 VPN 3000 集中器，使之通过证书与 VPN 客户端通信

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[VPN 3000 集中器对 VPN 客户端的证书](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文包括关于如何的逐步指导配置有VPN客户端的Cisco VPN 3000系列集中器有使用的证书。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据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

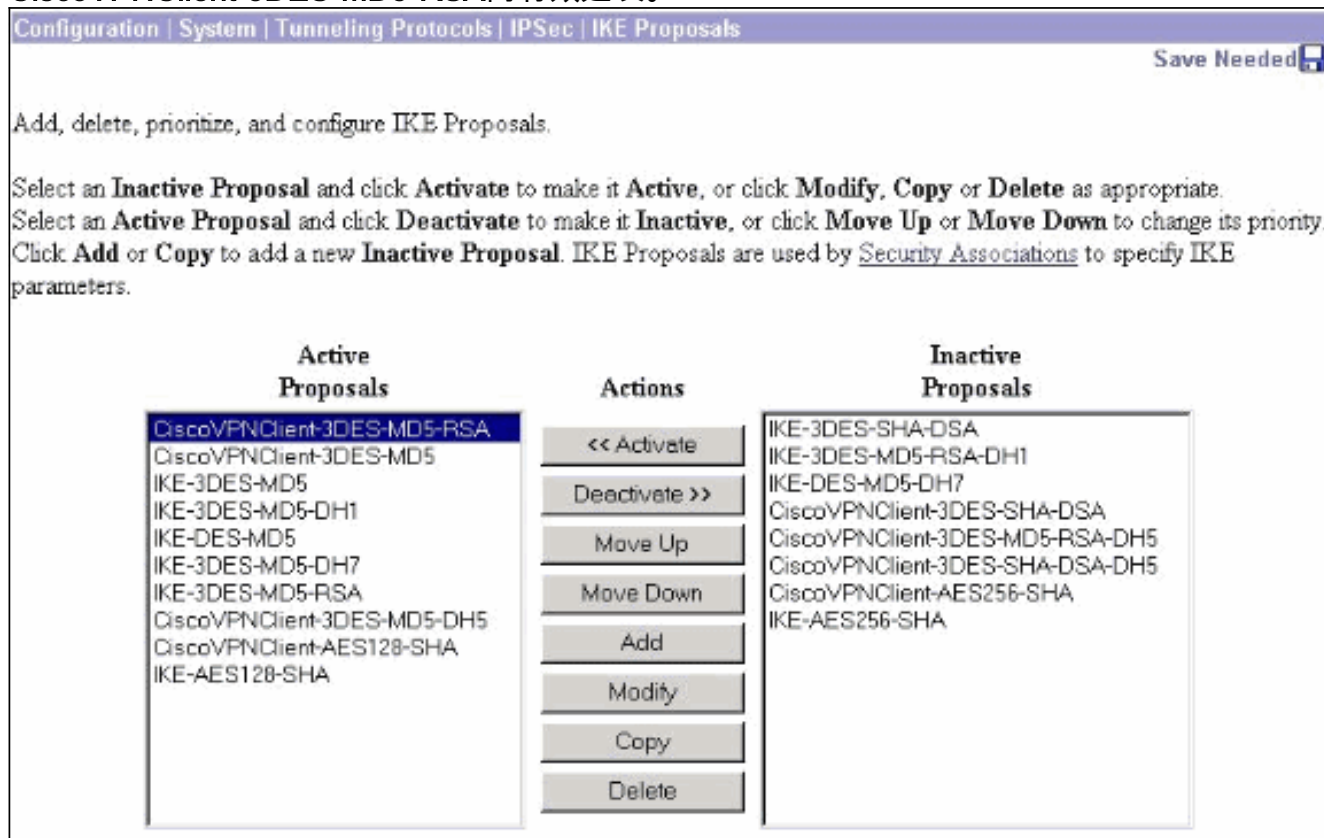
有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

VPN 3000 集中器对 VPN 客户端的证书

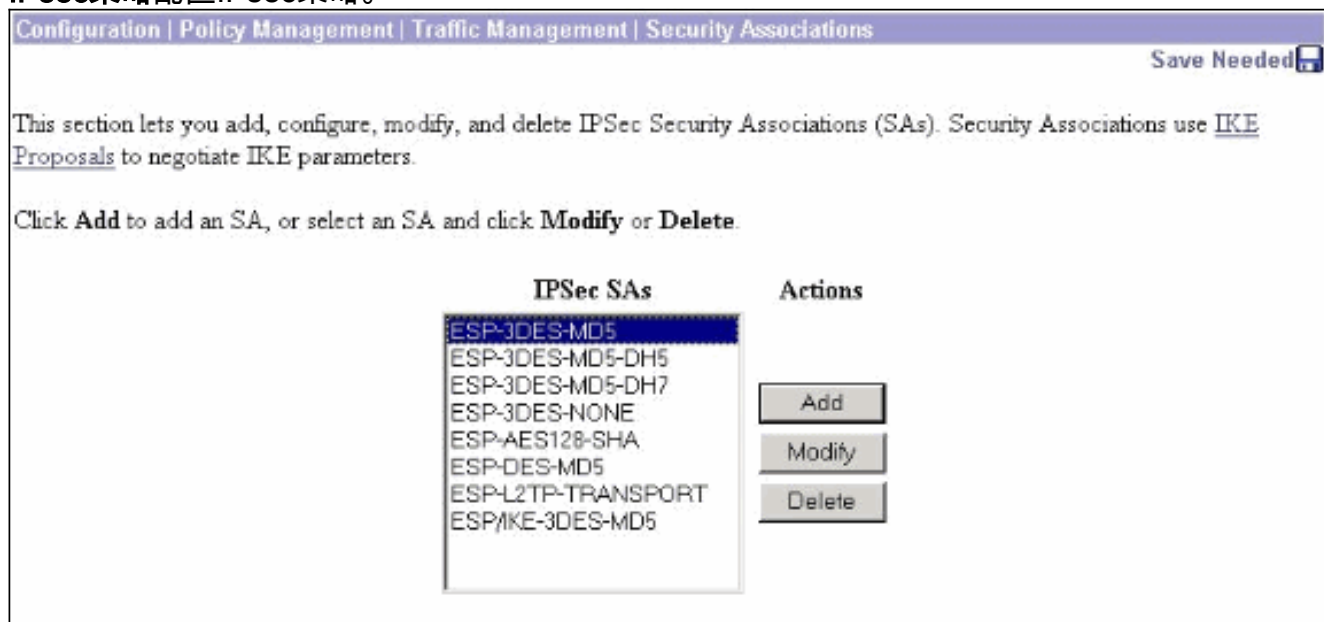
完成这些步骤为了配置VPN客户端的VPN 3000集中器证书。

1. 必须配置IKE策略使用在VPN 3000集中器系列管理器的证书。为了配置IKE策略，请选择

Configuration > System > Tunneling Protocols > IPsec > IKE Proposals , 并且移动 CiscoVPNClient-3DES-MD5-RSA向有效建议。



2. 您必须也配置IPsec策略使用证书。选择Configuration > Policy Management > Traffic Management > Security Associations , 突出显示ESP-3DES-MD5和然后单击修改配置IPsec策略配置IPsec策略。



3. 在Modify窗口 , 在数字证书下 , 请确保选择您的已安装身份证书。在IKE建议下 , 请选择 CiscoVPNClient-3DES-MD5-RSA并且单击应用。

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

IKE Proposal Select the IKE Proposal to use as IKE initiator.

4. 为了配置IPSec组，请选择**Configuration > User Management > Groups > Add**，添加组呼叫IPSECCERT (IPSECCERT组名匹配在身份证书的组织单位(OU))，并且选择密码。此密码任何地方，如果使用证书，没有使用。在本例中，"cisco123"是密码。

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	<input type="text" value="IPSECCERT"/>	Enter a unique name for the group.
Password	<input type="password"/>	Enter the password for the group.
Verify	<input type="password"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

5. 在同一个页，请点击常规选项卡并且确保您选择IPsec作为隧道协议。

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP			
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.

6. 点击IPsec选项并且确保您的已配置的IPsec安全关联(SA)选择在SA IPsec下并且单击应用。

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP			
IPsec Parameters			
Attribute	Value	Inherit?	Description
IPsec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPsec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	<input checked="" type="checkbox"/>	(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	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Aliga/Cisco client is being used by members of this group.

Add Cancel

7. 为了配置VPN 3000集中器的一个IPSec组，请选择**Configuration > User Management > Users > Add**，指定用户名、密码和组名和然后单击**添加**。在示例中，使用这些字段：用户名= cert_user 口令 = cisco123 验证= cisco123Group= IPSECCERT

Configuration | User Management | Users | Add

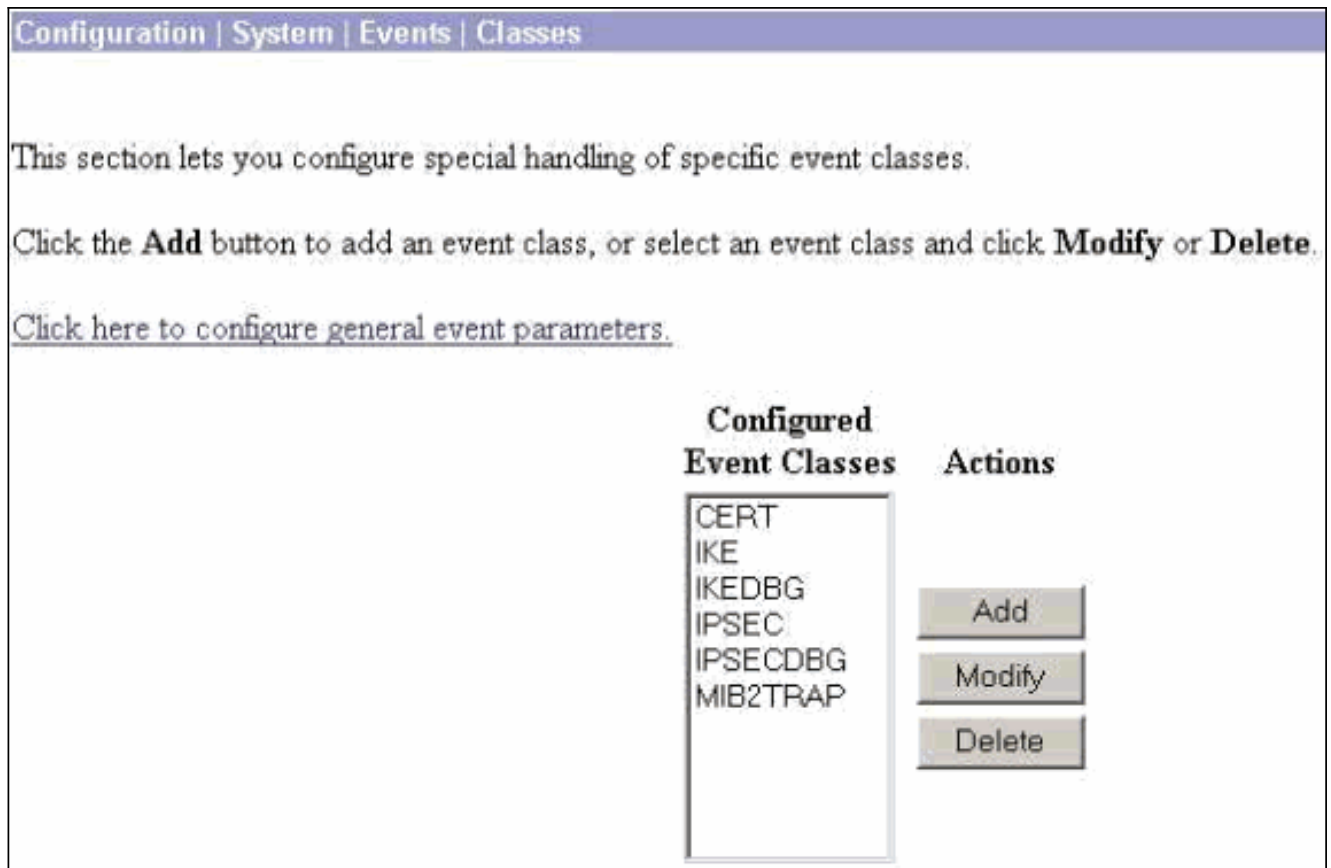
This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPSec PPTP/L2TP

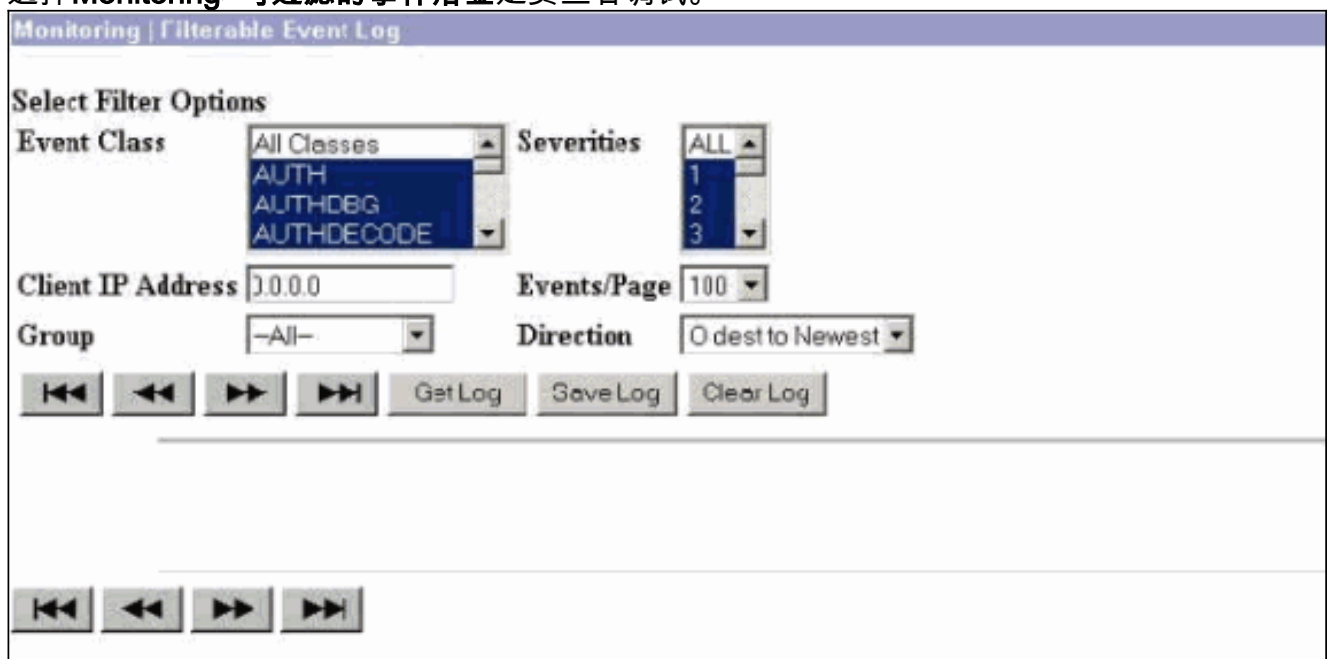
Identity Parameters		
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.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

Add Cancel

8. 为了启用在VPN 3000集中器的调试请选择**Configuration > System > Events > Classes**并且添加这些类：CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECCDBG 1-10



9. 选择Monitoring>可过滤的事件洛金定货查看调试。



注意：如果决定更改IP地址，您能做登记新的IP地址和安装已签发证书后与那些新建的地址。

验证

当前没有可用于此配置的验证过程。

故障排除

参考[在VPN 3000集中器的故障排除连接问题](#)对更进一步的故障排除信息。

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](#)