認証を使用した VPN クライアントと通信するための VPN 3000 コンセントレータの設定

内容

概要

このドキュメントでは、証明書を使用した Cisco VPN 3000 シリーズ コンセントレータと VPN クライアントの設定方法の段階的な手順について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN 3000コンセントレータソフトウェアバージョン4.0.4Aに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

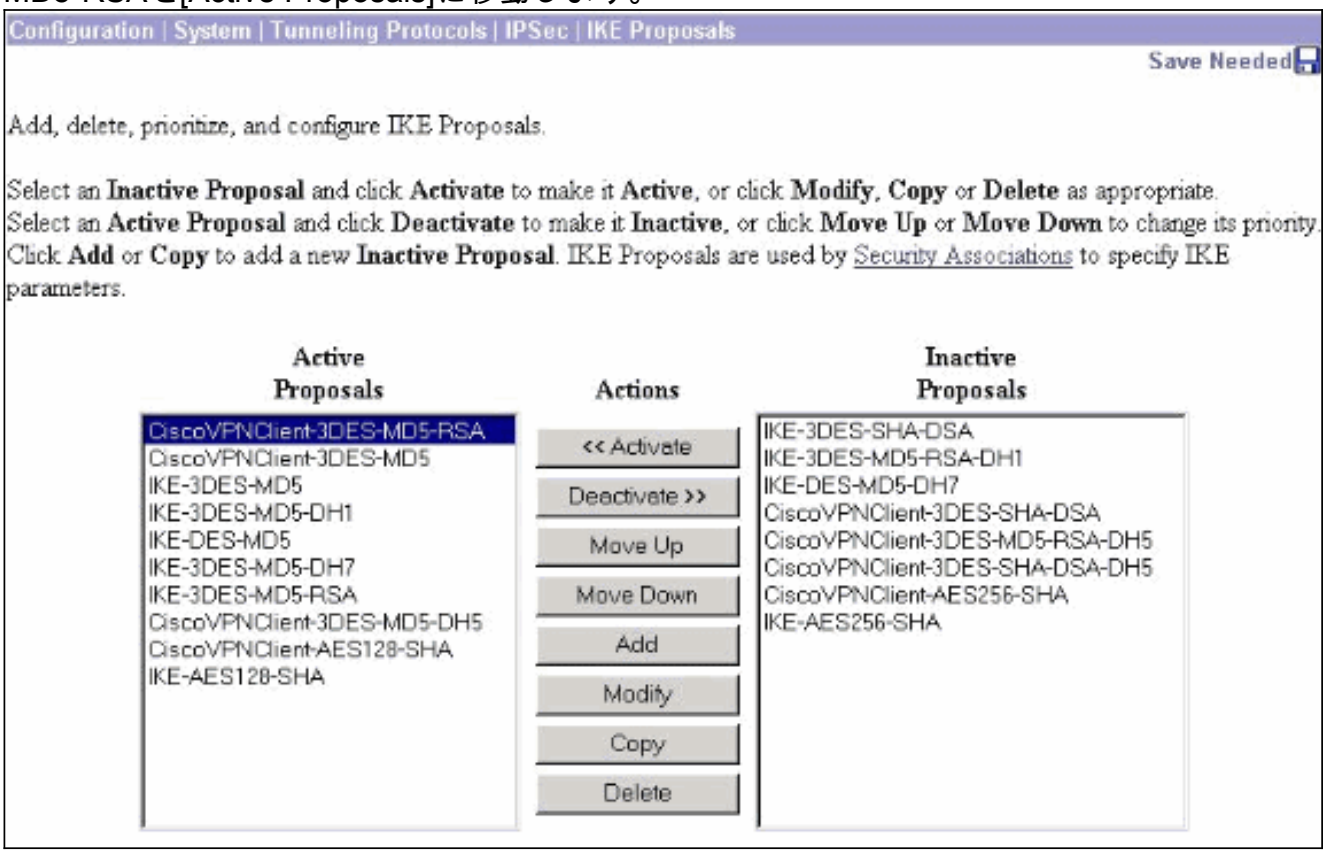
表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

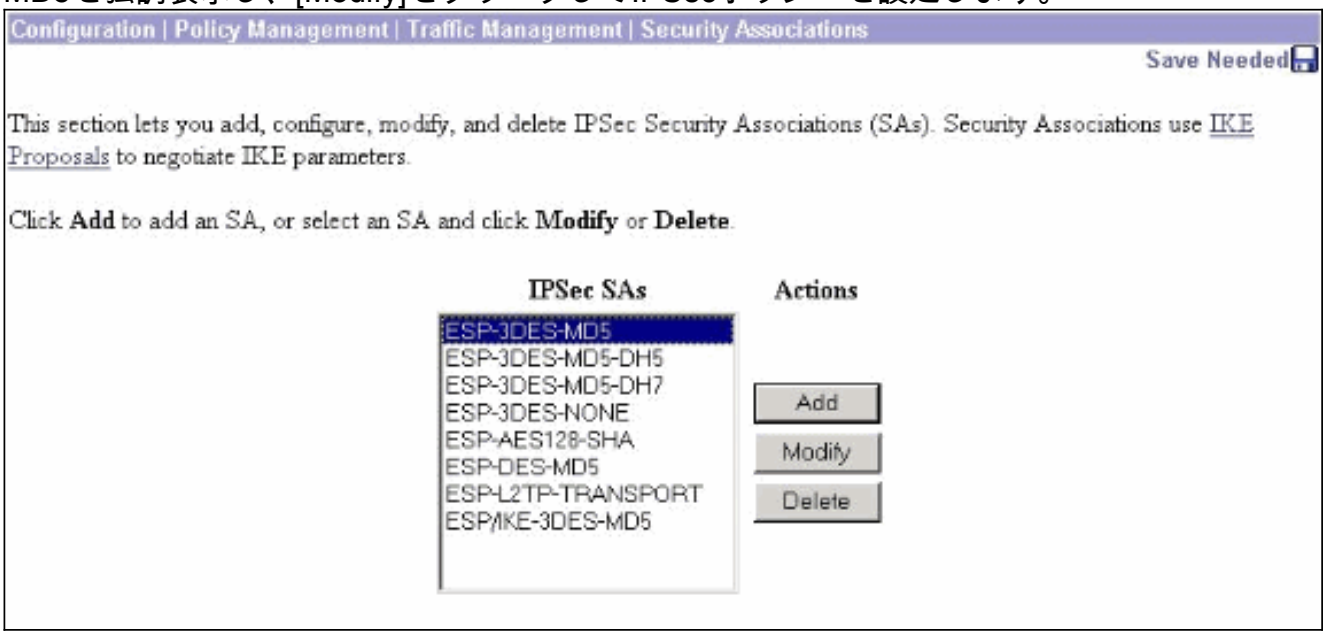
VPN クライアントのVPN 3000 Concentrator 証明

VPN ClientのVPN 3000コンセントレータ証明書を設定するには、次の手順を実行します。

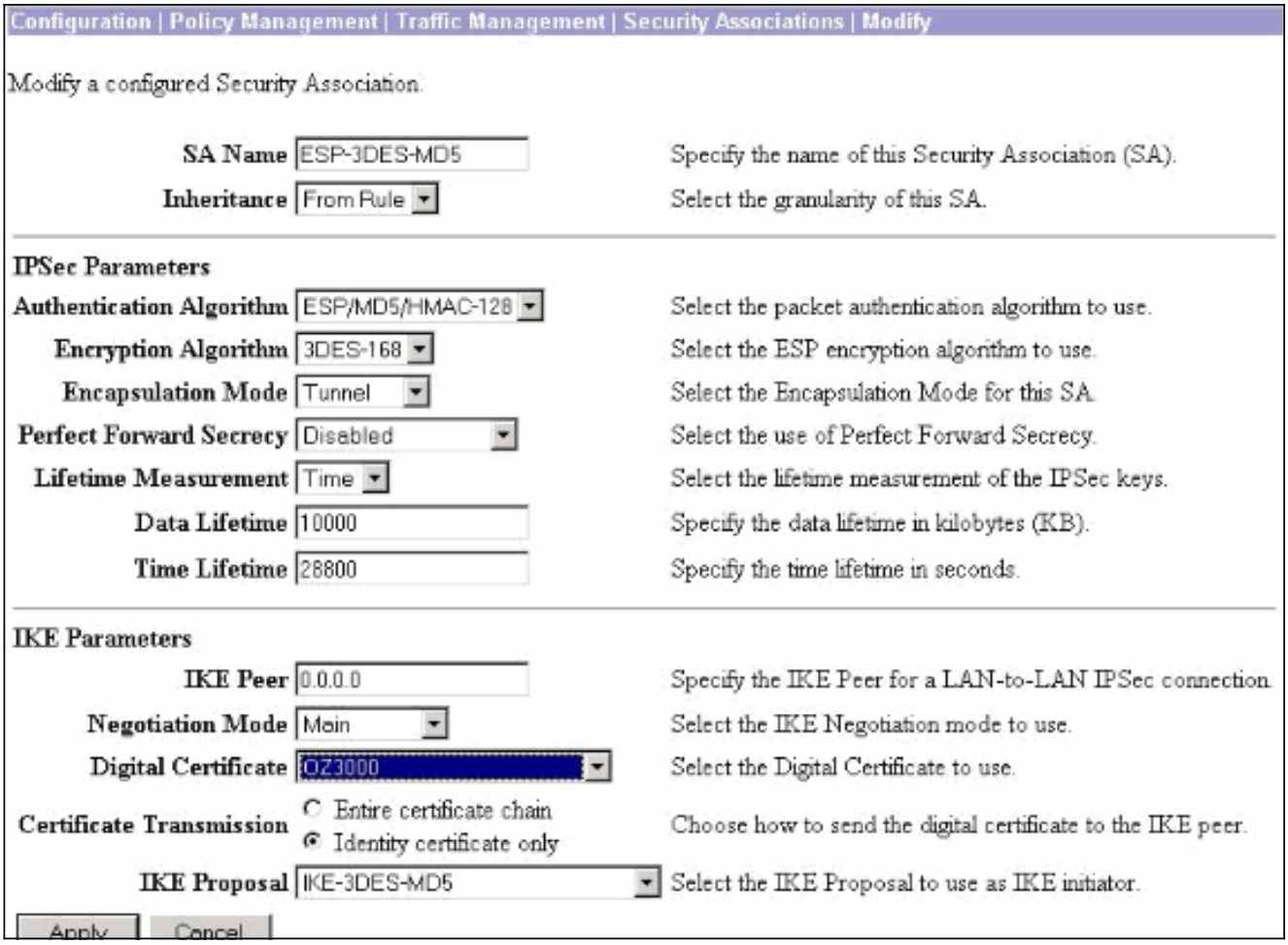
1. VPN 3000コンセントレータシリーズマネージャで証明書を使用するようにIKEポリシーを設定する必要があります。IKEポリシーを設定するには、[Configuration] > [System] > [Tunneling Protocols] > [IPsec] > [IKE Proposals] の順に選択し、CiscoVPNClient-3DES-MD5-RSAを[Active Proposals]に移動します。



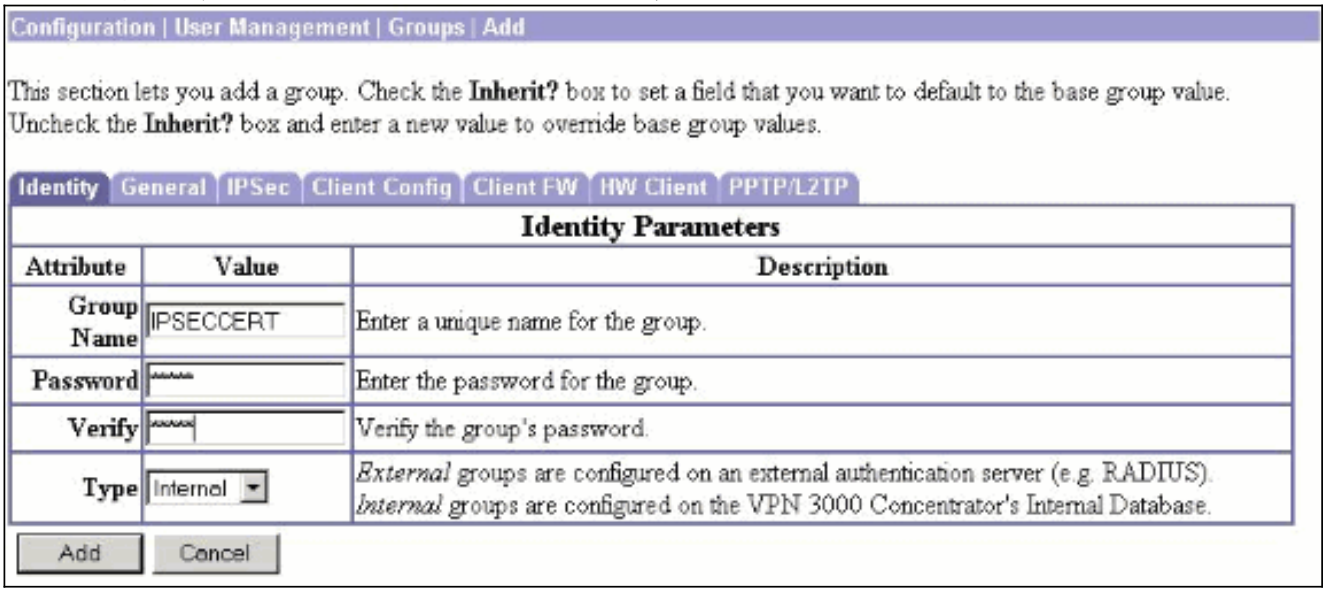
2. 証明書を使用するようにIPsecポリシーを設定する必要もあります。[Configuration] > [Policy Management] > [Traffic Management] > [Security Associations]を選択し、ESP-3DES-MD5を強調表示し、[Modify]をクリックしてIPSecポリシーを設定します。



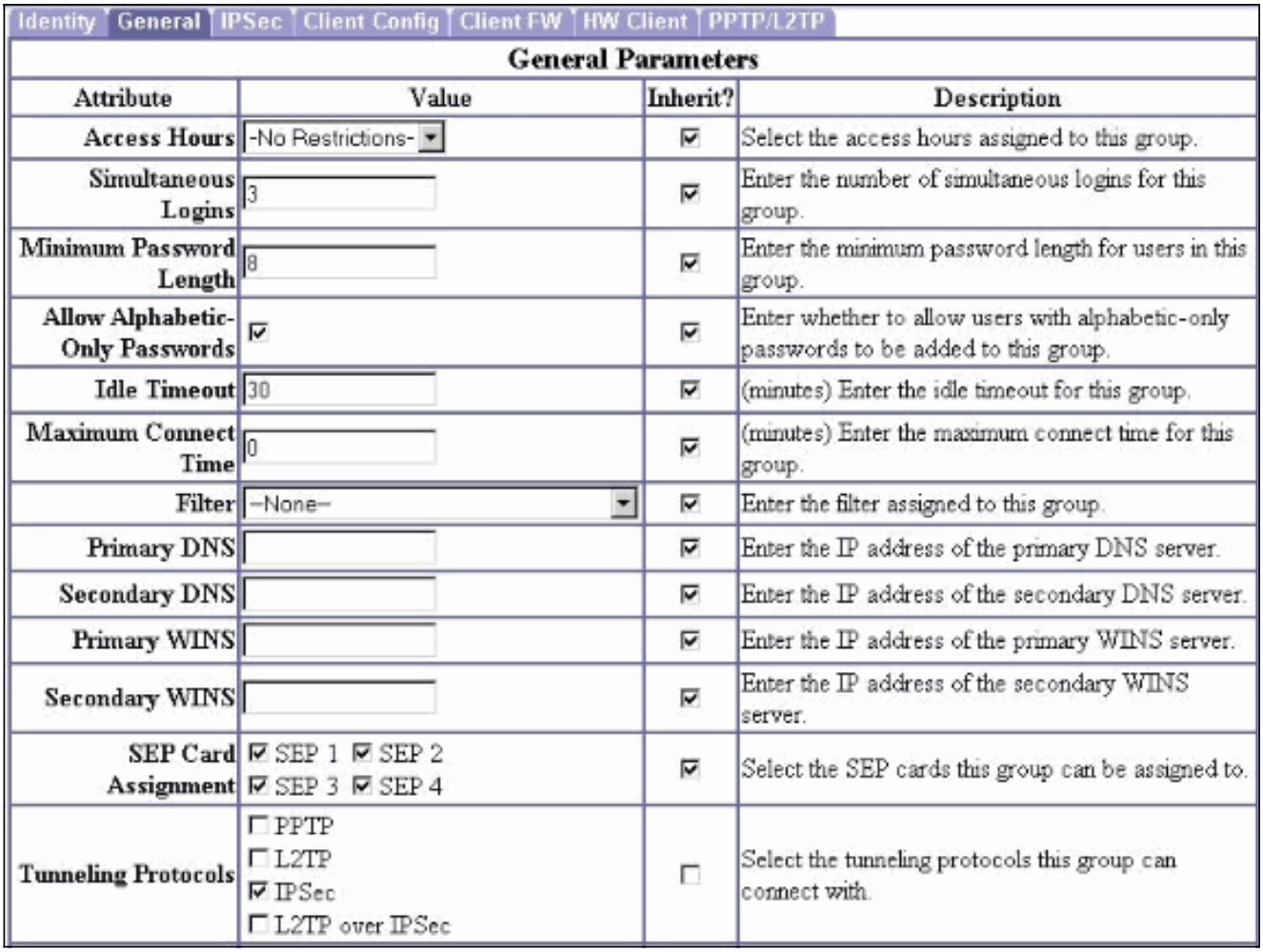
3. [Modify]ウィンドウの[Digital Certificates]で、インストールされているID証明書を選択します。[IKE Proposal]で**[CiscoVPNClient-3DES-MD5-RSA]を選択し、[Apply]をクリックします。**



4. IPsecグループを設定するには、[Configuration] > [User Management] > [Groups] > [Add] を選択し、ID証明書のOrganizational Unit(OU)に一致するIPSECCERTグループ名を追加して、パスワードを選択します。証明書を使用している場合、このパスワードは使用されません。この例では、「cisco123」がパスワードです。



5. 同じページで、[General]タブをクリックし、トンネリングプロトコルとして[IPsec]を選択していることを確認します。

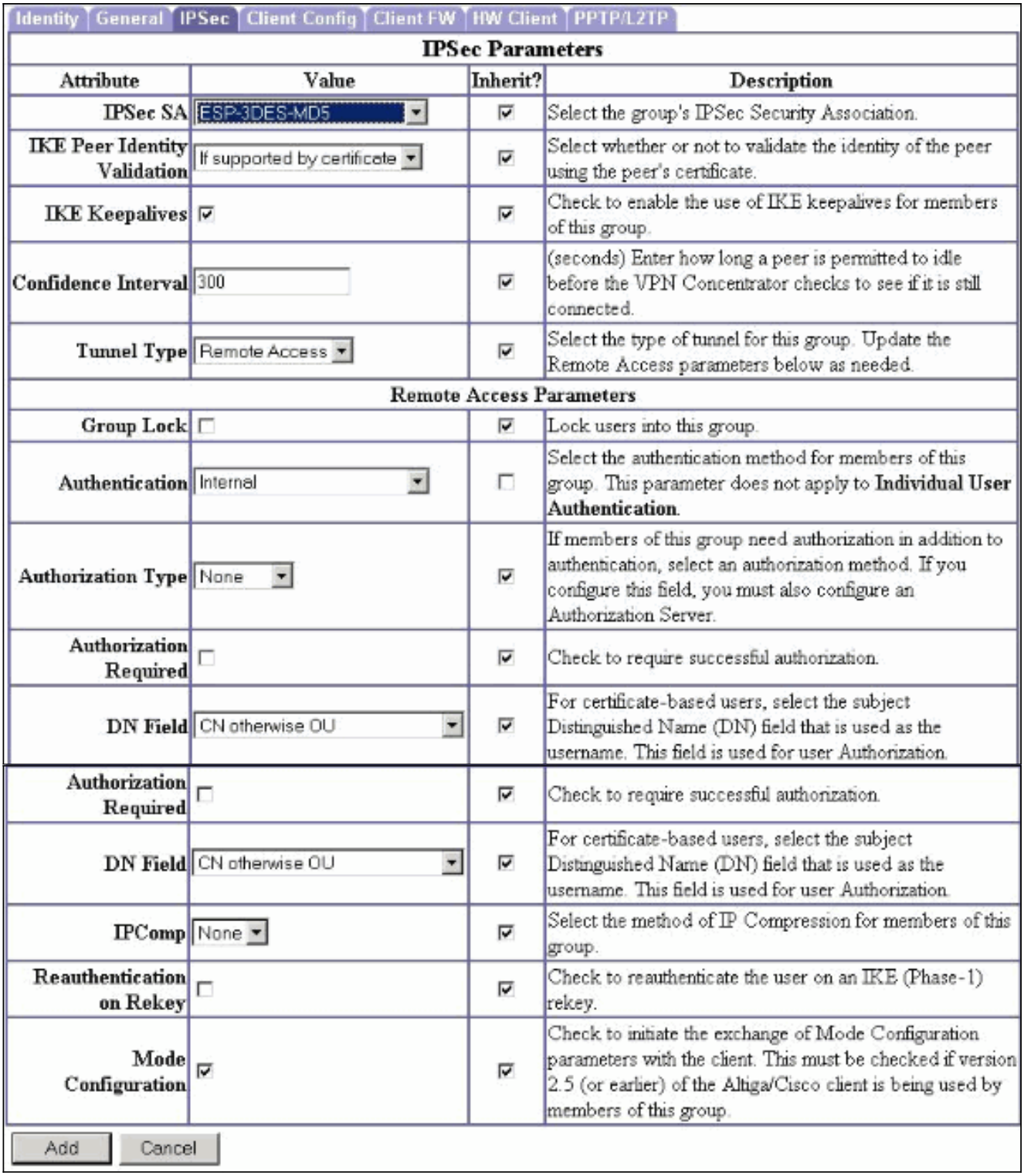


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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]タブをクリックし、[IPsec SA]で設定済みのIPsec Security Association (SA)が選択されていることを確認し、[**Apply**]をクリックします。



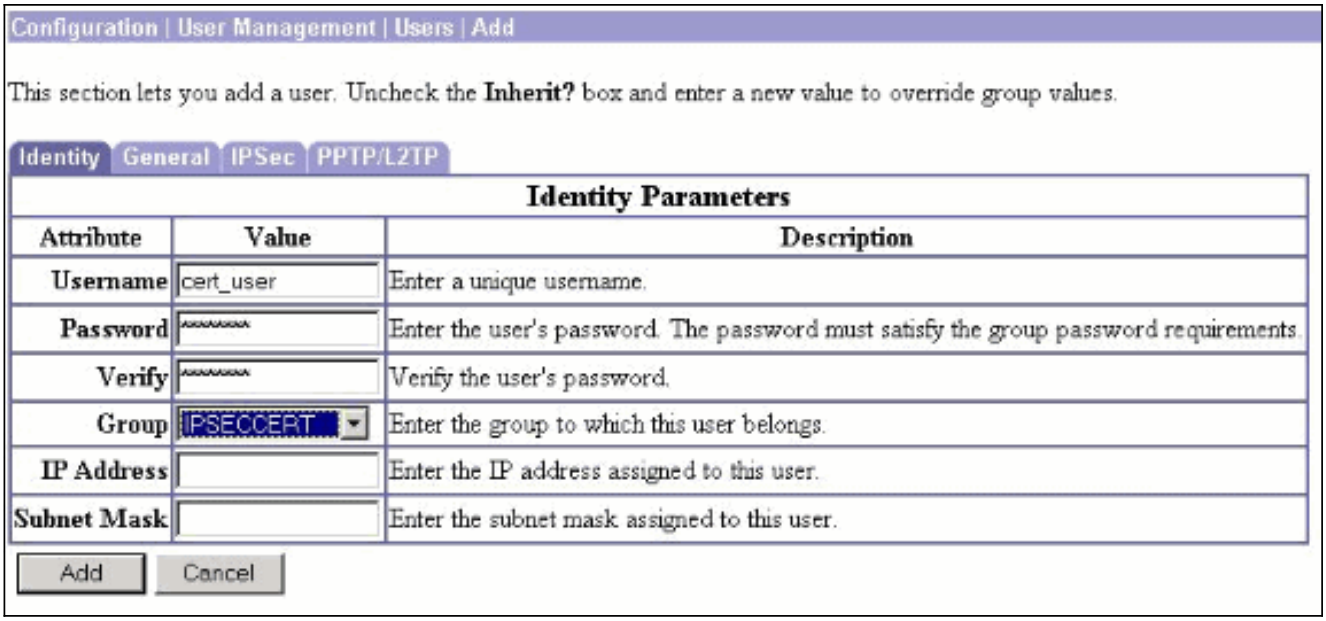
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

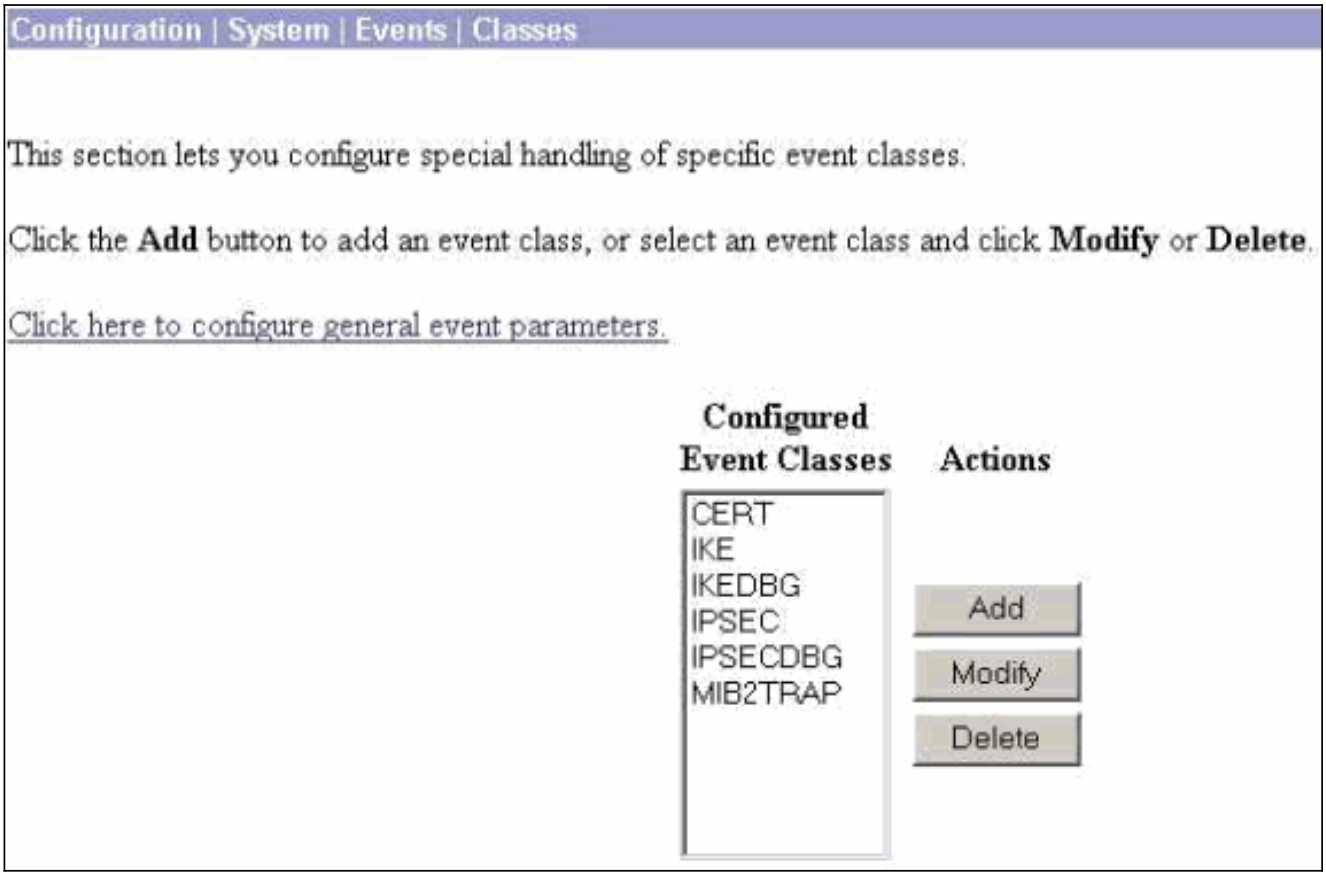
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of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

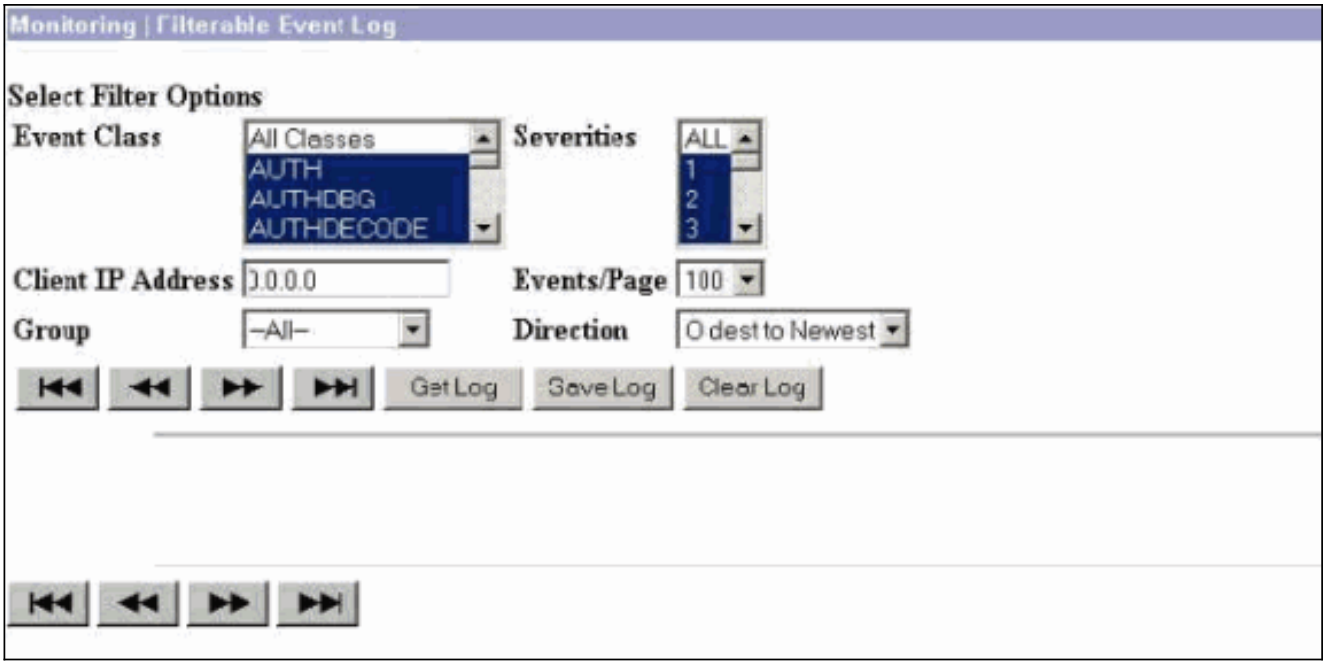
7. VPN 3000コンセントレータでIPsecグループを設定するには、[Configuration] > [**User Management**] > [**Users**] > [Add]の順に選択し、ユーザ名、パスワード、およびグループ名を指定し、[**Add**]をクリックします。この例では、次のフィールドを使用します。ユーザ名= cert_userパスワード：cisco123確認= cisco123グループ= IPSECCERT



8. VPN 3000コンセントレータでデバッグを有効にするには、**Configuration > System > Events > Classes**の順に選択し、次のクラスを追加します。CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10



9. [Monitoring] > [Filterable Event Log] を選択して、デバッグを表示します。



注：IPアドレスを変更する場合は、新しいIPアドレスを登録し、発行された証明書を後で新しいアドレスにインストールできます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

トラブルシューティングの詳細[については、『VPN 3000コンセントレータの接続に関する問題のトラブルシューティ](#)ング』を参照してください。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco VPN 3002 Hardware Client
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems