# Configuração do VPN 3000 Concentrator para se comunicar com o VPN Client usando certificados

## Índice



## Introdução

Este documento inclui instruções passo a passo em como configurar o Concentradores Cisco VPN série 3000 com os clientes VPN com o uso dos Certificados.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

A informação neste documento é baseada na versão de software 4.0.4A do Cisco VPN 3000 Concentrator.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

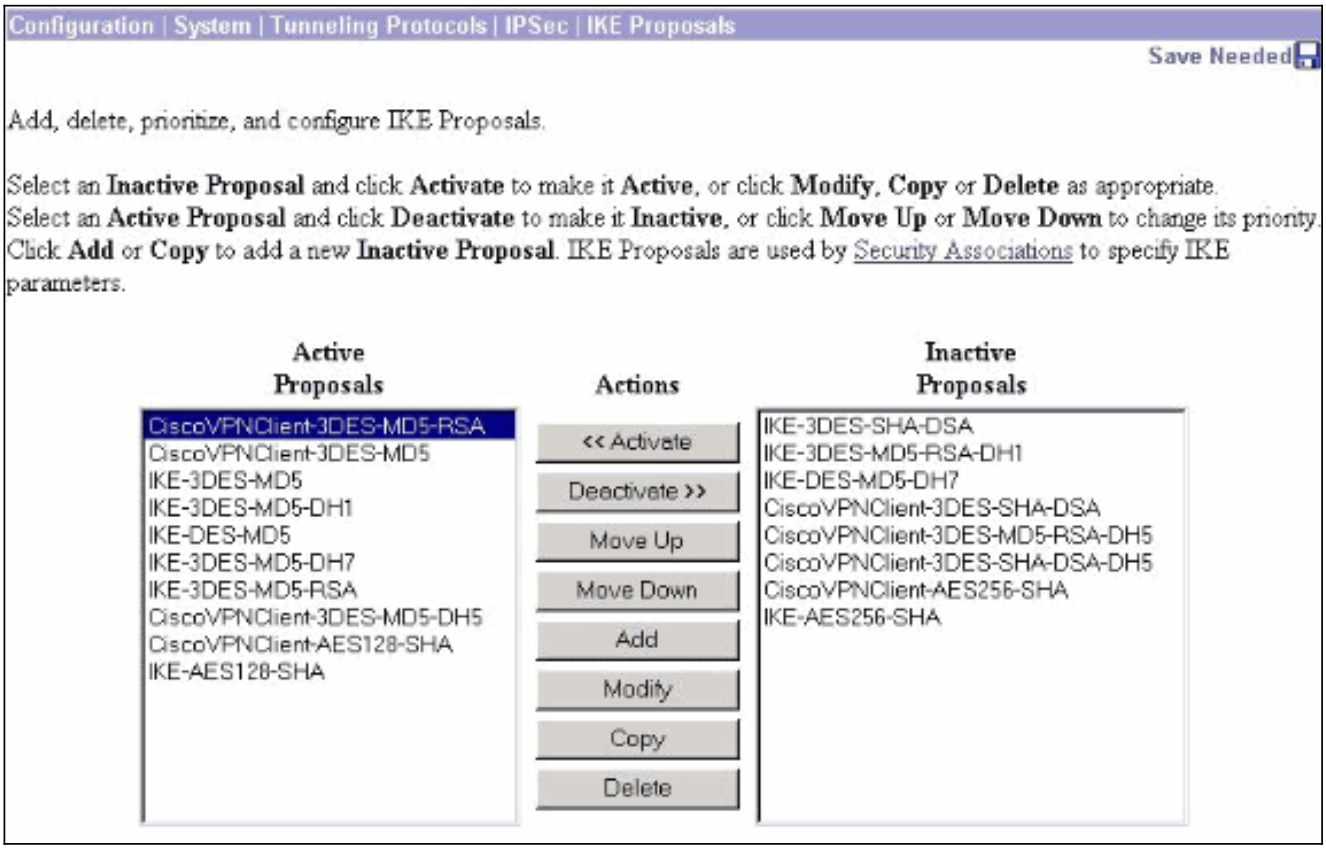
### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

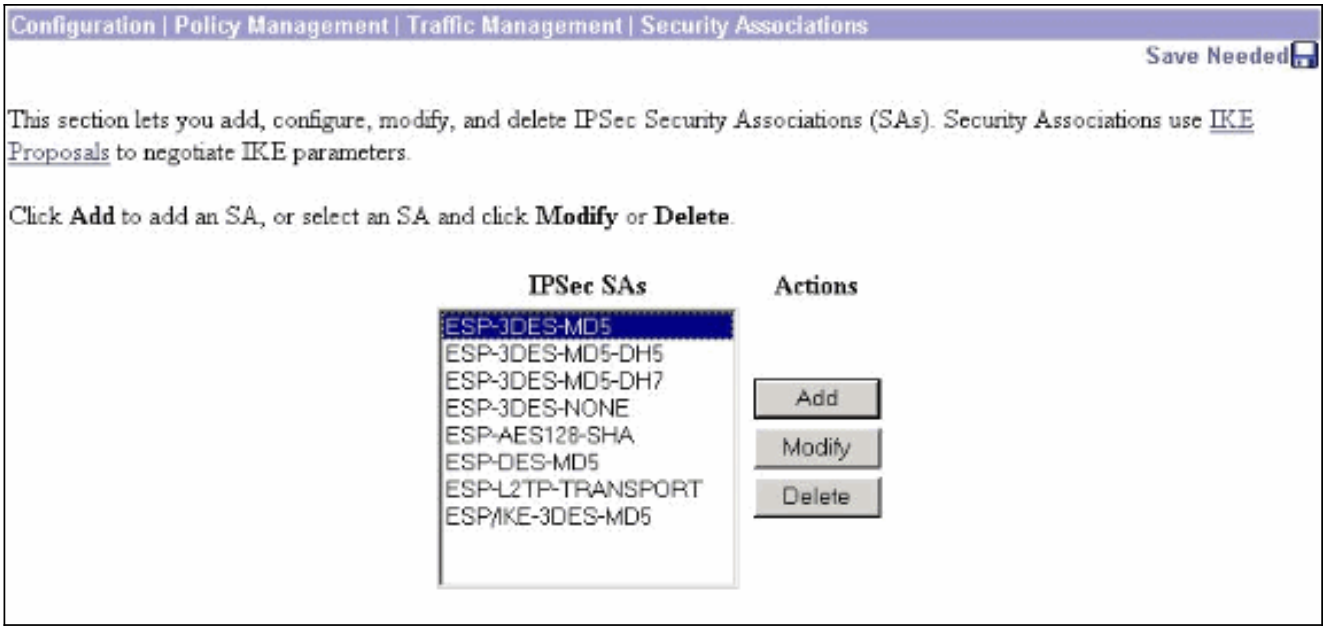
# Certificados do VPN 3000 Concentrator para clientes VPN

Termine estas etapas a fim configurar Certificados do VPN 3000 concentrator para clientes VPN.

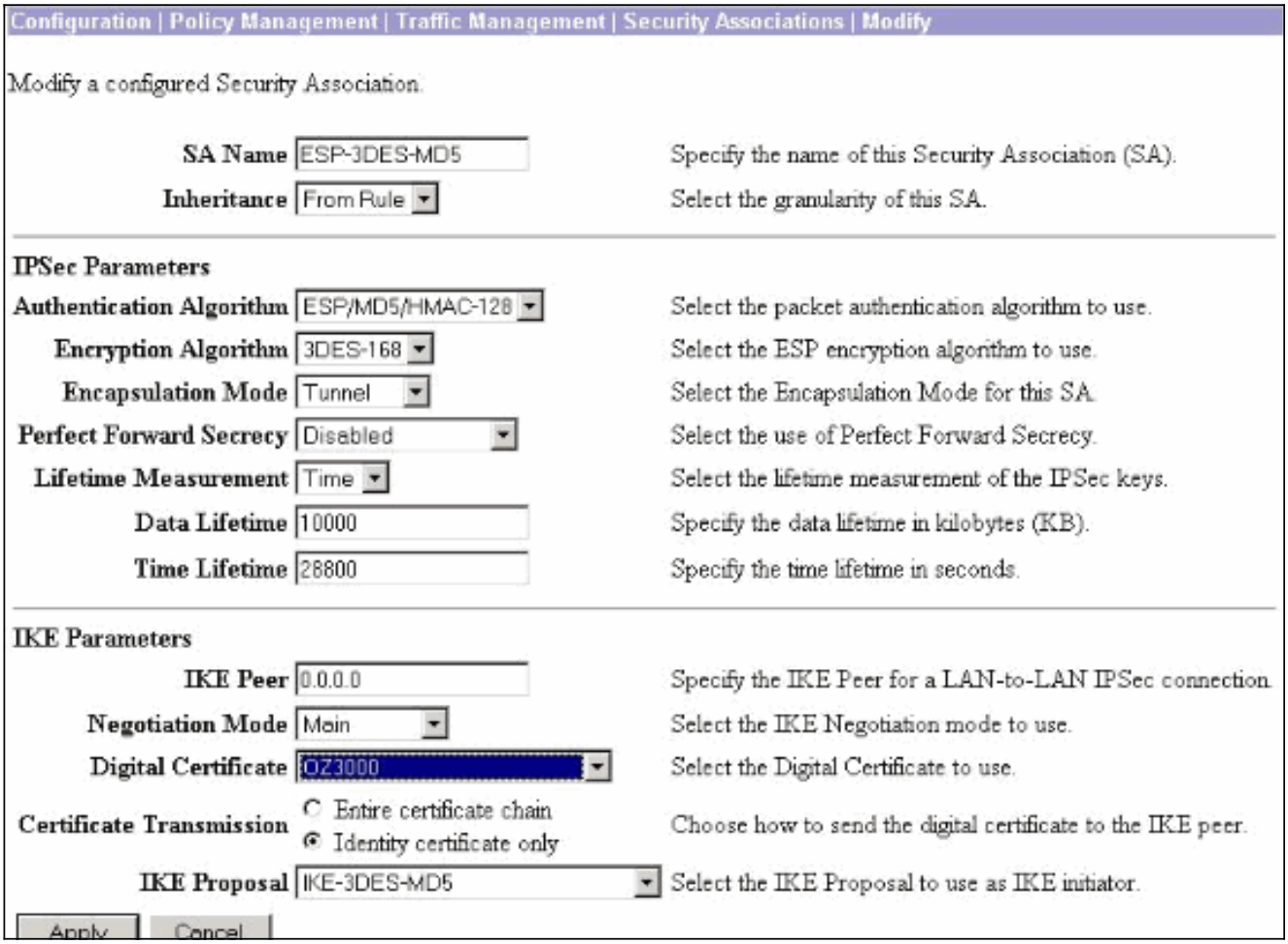
1. A política de IKE deve ser configurada para usar Certificados no gerente da VPN 3000 Concentrator Series. A fim configurar a política de IKE, o **configuração > sistema > protocolos de tunelamento > IPSEC > propostas de IKE** seleto, e o movimento **CiscoVPNClient-3DES-MD5-RSA aos** propósitos ativo.



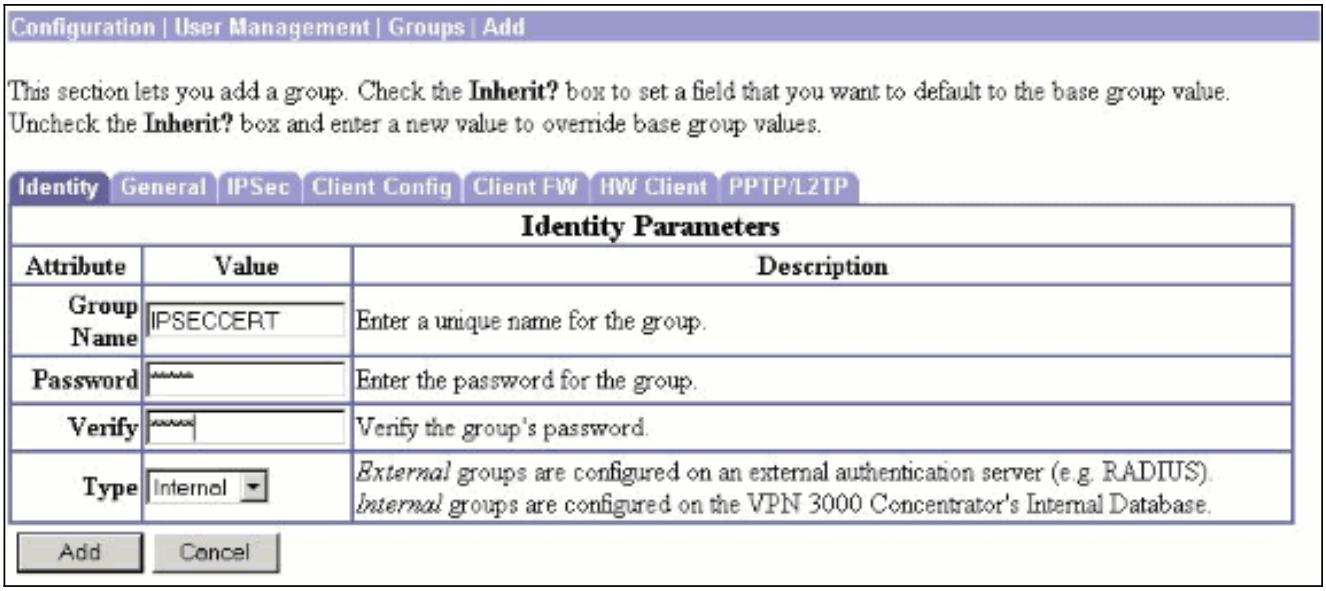

2. Você deve igualmente configurar a política de IPsec para usar Certificados. **O Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança** seleto, o destaque **ESP-3DES-MD5** e clica então **altera para configurar a política de IPsec** para configurar a política de IPsec.




3. No indicador da alteração, sob Certificados digitais, certifique-se selecionar seu certificado de identidade instalado. Sob a proposta IKE, **CiscoVPNClient-3DES-MD5-RSA** seletos e o clique **aplicam-se**.




4. A fim configurar um grupo IPSec, selecione o **configuração > gerenciamento de usuário > grupos > adicionar**, adicionam um grupo chamado **IPSECCERT** (o nome do grupo IPSECCERT combina a unidade organizacional (OU) no certificado de identidade), e selecionam uma senha.Esta senha não é usada em qualquer lugar se você usa Certificados. Neste exemplo, "cisco123" é a
senha.



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.

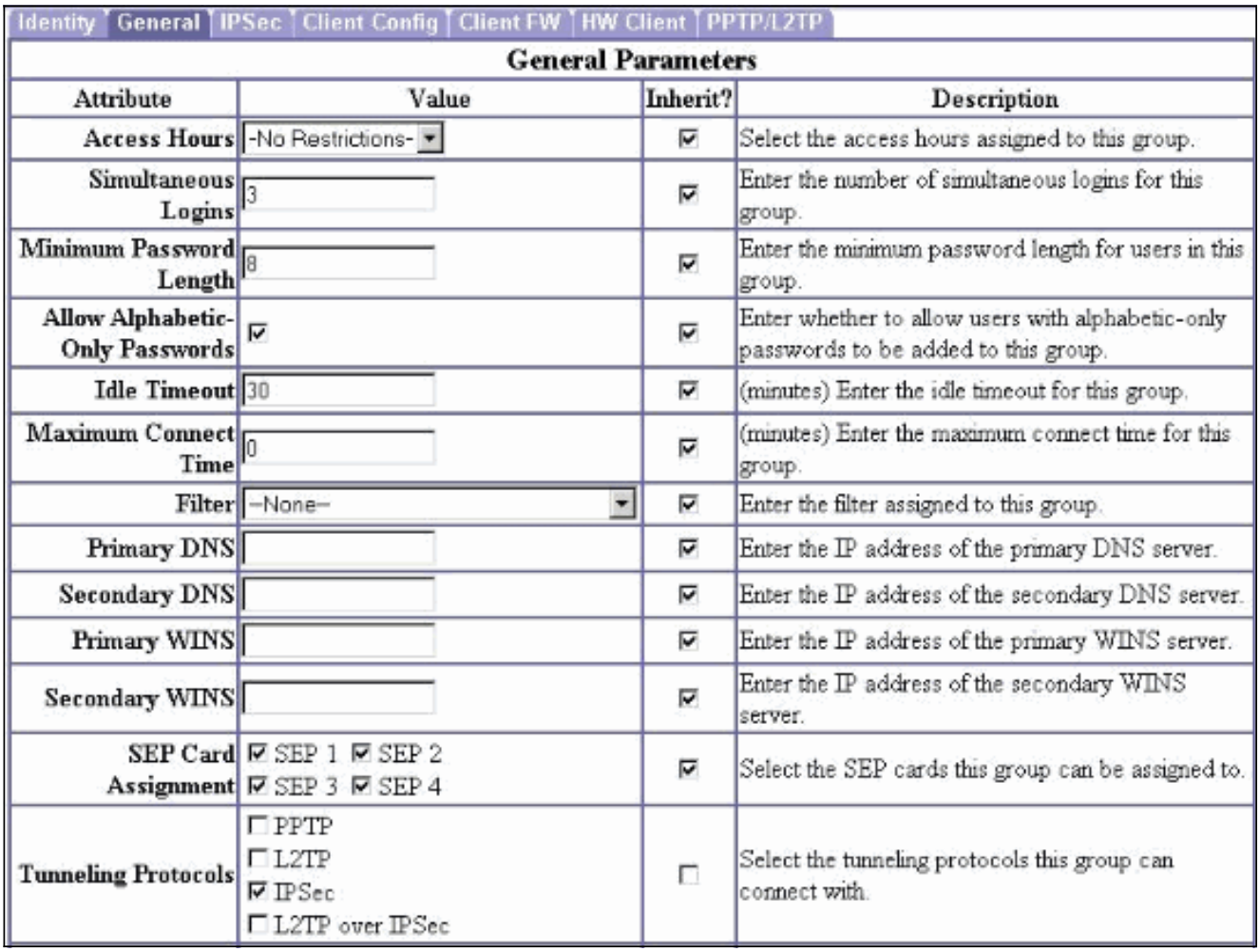
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

**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. Na mesma página, clique o tab geral e certifique-se de que você seleciona o **IPsec** como o protocolo de tunelamento.

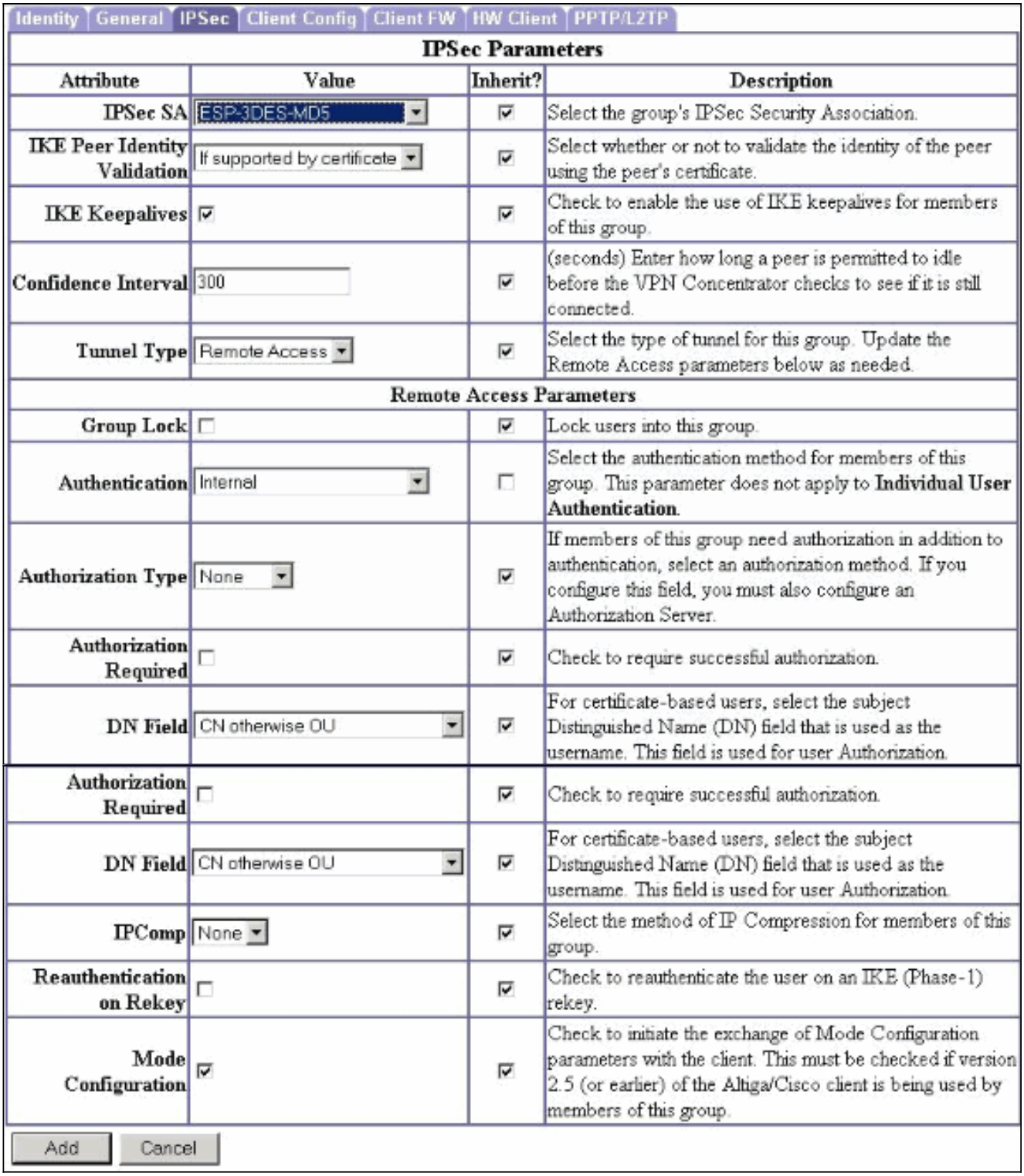


Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

**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. Clique a aba do IPsec e certifique-se de que sua associação de segurança IPSec configurada (SA) está selecionada sob IPsec SA e clique **se aplica**.



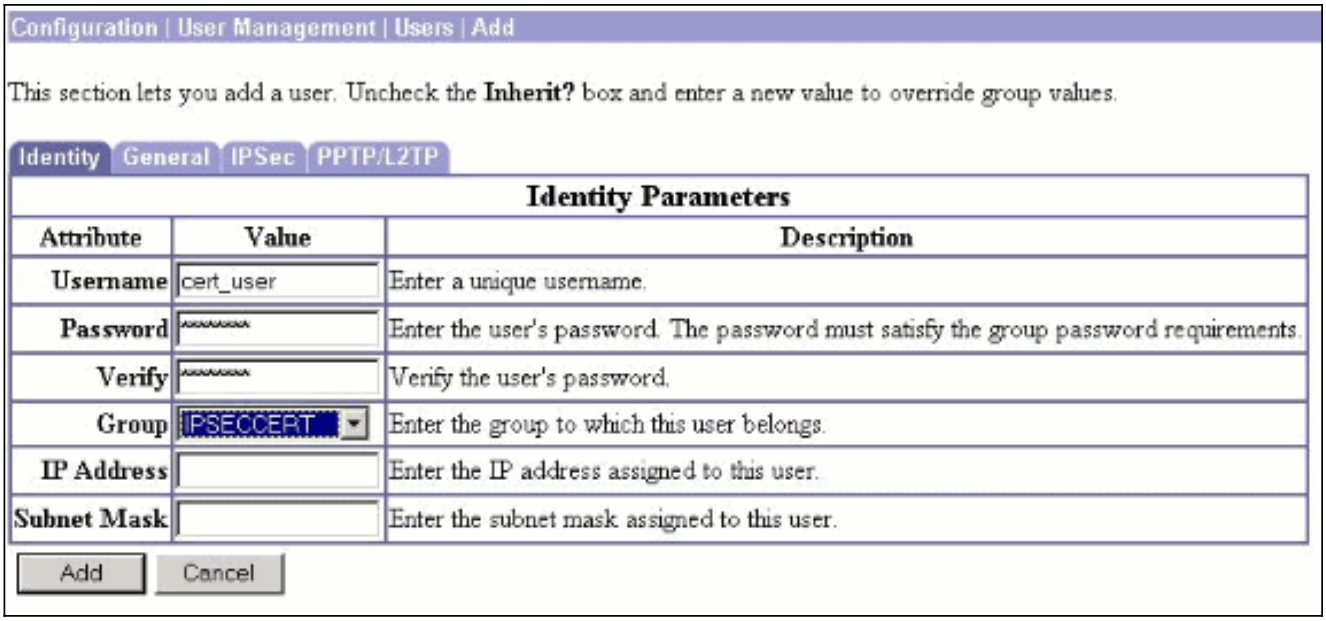
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

**IPSec Parameters**

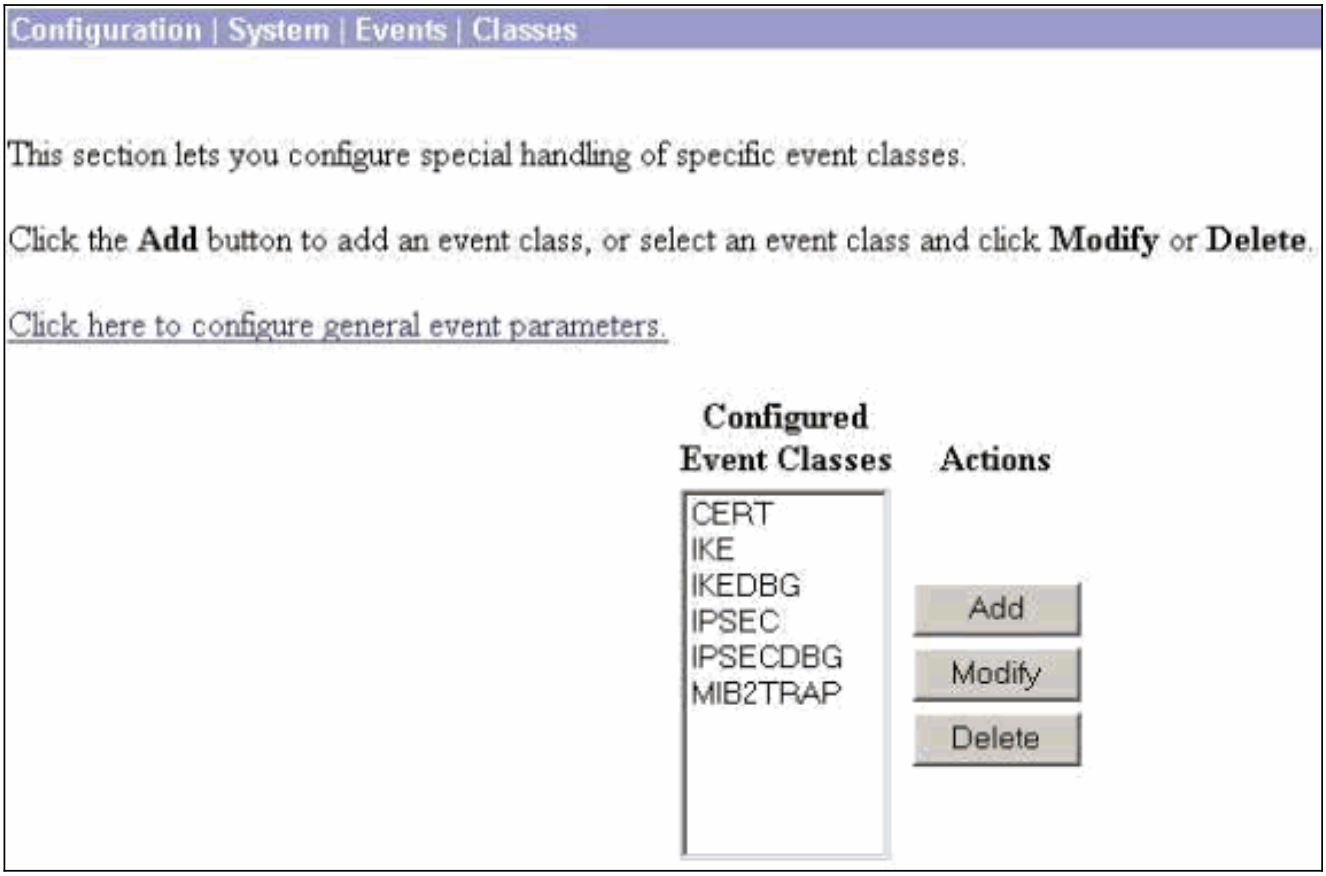
| Attribute | Value | Inherit? | Description |
|---|---|---|---|
| **IPSec SA** | ESP-3DES-MD5 | ☑ | Select the group's IPSec Security Association. |
| **IKE Peer Identity Validation** | If supported by certificate | ☑ | Select whether or not to validate the identity of the peer using the peer's certificate.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

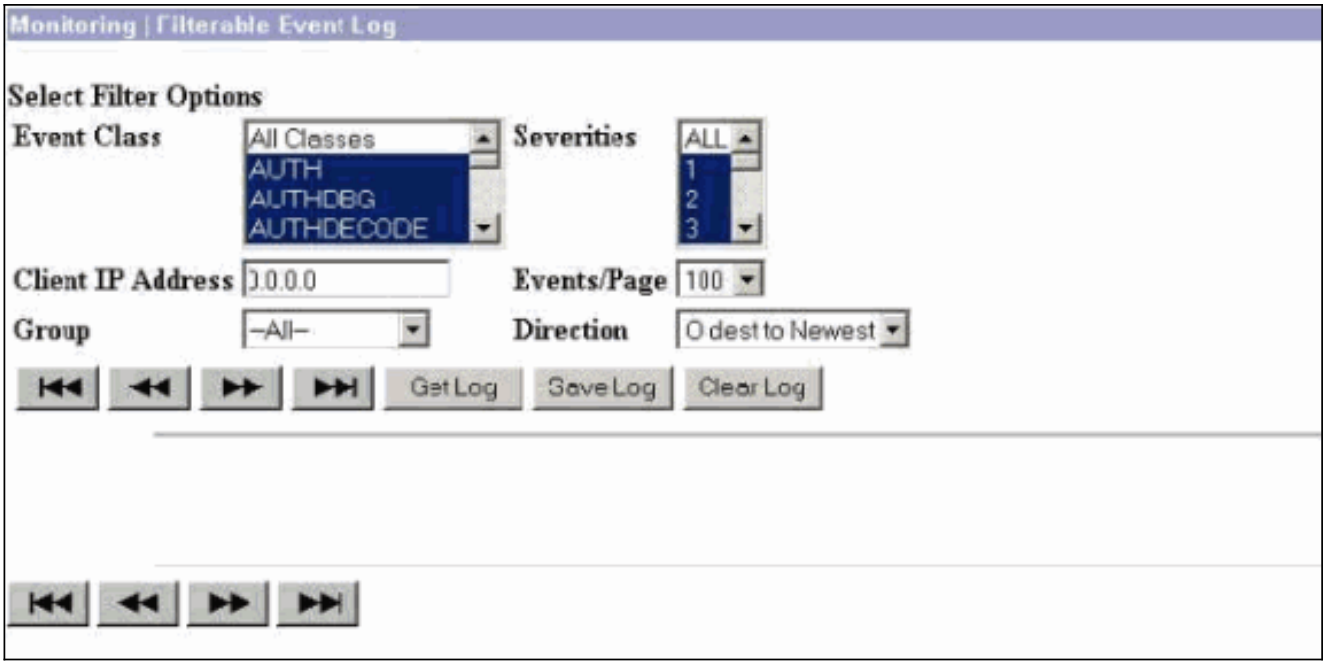
7. A fim configurar um grupo IPSec no VPN 3000 concentrator, selecione o **configuração > gerenciamento de usuário > usuários > adicionar**, especifique um nome de usuário, a senha, e o nome do grupo, e clique-os então **adicionam**.No exemplo, estes campos são usados:Nome de usuário = cert_userSenha = cisco123Verifique = cisco123Grupo = IPSECCERT




8. A fim permitir a eliminação de erros no **configuração > sistema > eventos > classes** seleto do VPN 3000 concentrator e adicionar estas classes:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-
10




9. **A monitoração** seleta > ordem **filtrável do início de uma sessão do evento** para ver debuga.




**Note**: Se você decide mudar os endereços IP de Um ou Mais Servidores Cisco ICM NT, você pode fazer um registro dos endereços IP de Um ou Mais Servidores Cisco ICM NT novos e instalar o certificado emitido mais atrasado com aqueles endereços novos.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshooting

Refira pesquisando defeitos problemas de conexão no VPN 3000 concentrator para a informação adicional de Troubleshooting.

## Informações Relacionadas

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems