配置IPSec（從VPN客戶端版本3.5 Solaris到VPN 3000集中器）

目錄

簡介

本文檔說明如何配置用於Solaris 2.6的VPN客戶端3.5以連線到VPN 3000集中器。

必要條件

需求

嘗試此配置之前，請確保滿足以下先決條件。

- 此示例使用預共用金鑰進行組身份驗證。根據VPN集中器的內部資料庫檢查使用者名稱和密碼（擴展身份驗證）。
- 必須正確安裝VPN客戶端。有關安裝的詳細資訊，請參閱安裝Solaris的VPN客戶端。
- VPN客戶端和VPN集中器的公共介面之間必須存在IP連線。必須正確設定子網掩碼和網關資訊。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco VPN Client for Solaris 2.6 3.5版，3DES映像。(映像名稱：vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)

- Cisco VPN集中器型別：3005 Bootcode版本：Altiga Networks/VPN集中器版本2.2.int_9 2000年1月19日05:36:41軟體版本：Cisco Systems， Inc./VPN 3000 Concentrator Series Version 3.1.Rel 2001年8月06日13:47:37

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

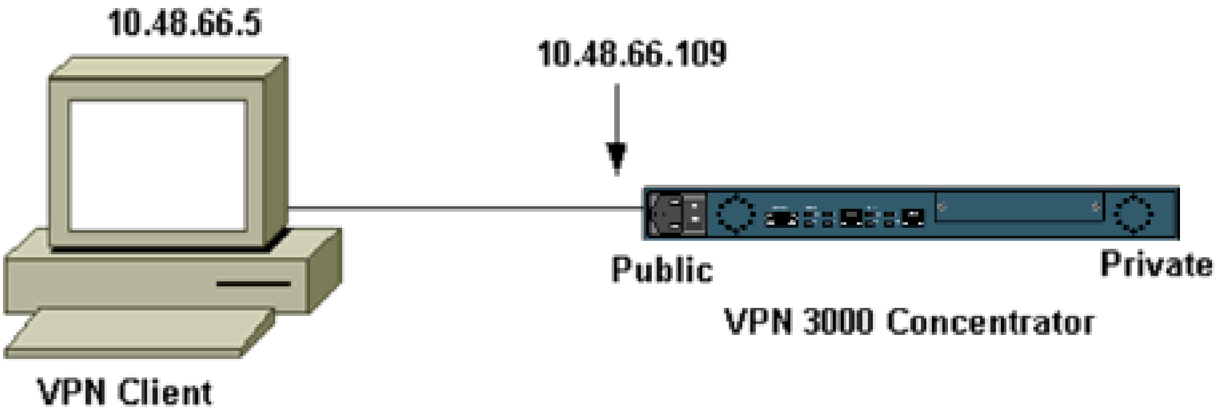
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本文檔使用下圖所示的網路設定。



注意：要將VPN客戶端3.5連線到VPN集中器，需要在集中器上安裝3.0版或更高版本。

組態

為連線建立使用者配置檔案

使用者配置檔案儲存在/etc/CiscoSystemsVPNClient/Profiles目錄中。這些文本檔案具有.pcf副檔名，並包含建立與VPN集中器的連線所需的引數。您可以建立新檔案或編輯現有檔案。您應在配置檔案目錄中查詢示例配置檔案sample.pcf。在此示例中，使用該檔案建立一個名為toCORPORATE.pcf的新配置檔案。

```
[cholera]: ~ > cd /etc/CiscoSystemsVPNClient/Profiles/
[cholera]: /etc/CiscoSystemsVPNClient/Profiles > cp sample.pcf toCORPORATE.pcf
```

您可以使用喜愛的文本編輯器編輯此新檔案toCORPORATE.pcf。進行任何修改之前，檔案如下所示。

注意：如果要使用網路地址轉換(NAT)的IPSec，則以下配置中的EnableNat條目必須表示「EnableNat=1」而不是「EnableNat=0」。

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=chimchim
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

有關使用者配置檔案關鍵字的說明，請參閱使用者配置檔案。

要成功配置您的配置檔案，至少需要瞭解以下資訊的等效值。

- VPN集中器的主機名或公共IP地址(10.48.66.109)
- 組名稱(RemoteClient)
- 組密碼(cisco)
- 使用者名稱(joe)

使用您的資訊編輯檔案，使其類似於以下內容。

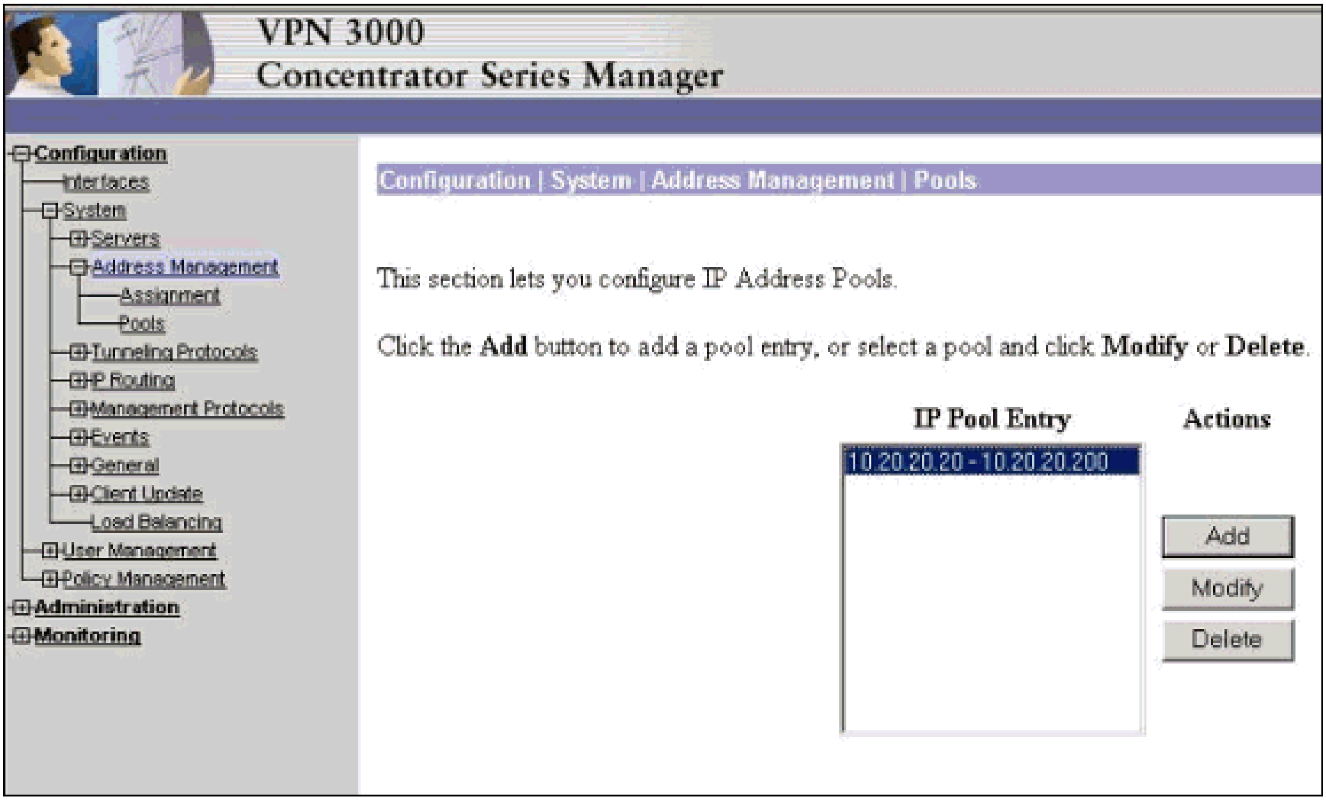
```
[main]
Description=Connection to the corporate
Host=10.48.66.109
AuthType=1
GroupName=RemoteClient
GroupPwd=cisco
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=joe
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

配置VPN集中器

使用以下步驟配置VPN集中器。

注意：由於空間限制，螢幕截圖僅顯示部分或相關區域。

1. 分配地址池。要分配可用的IP地址範圍，請將瀏覽器指向VPN集中器的內部介面，然後選擇**Configuration > System > Address Management > Pools**。按一下「**Add**」。指定與內部網路上的任何其他裝置不衝突的IP地址範圍。

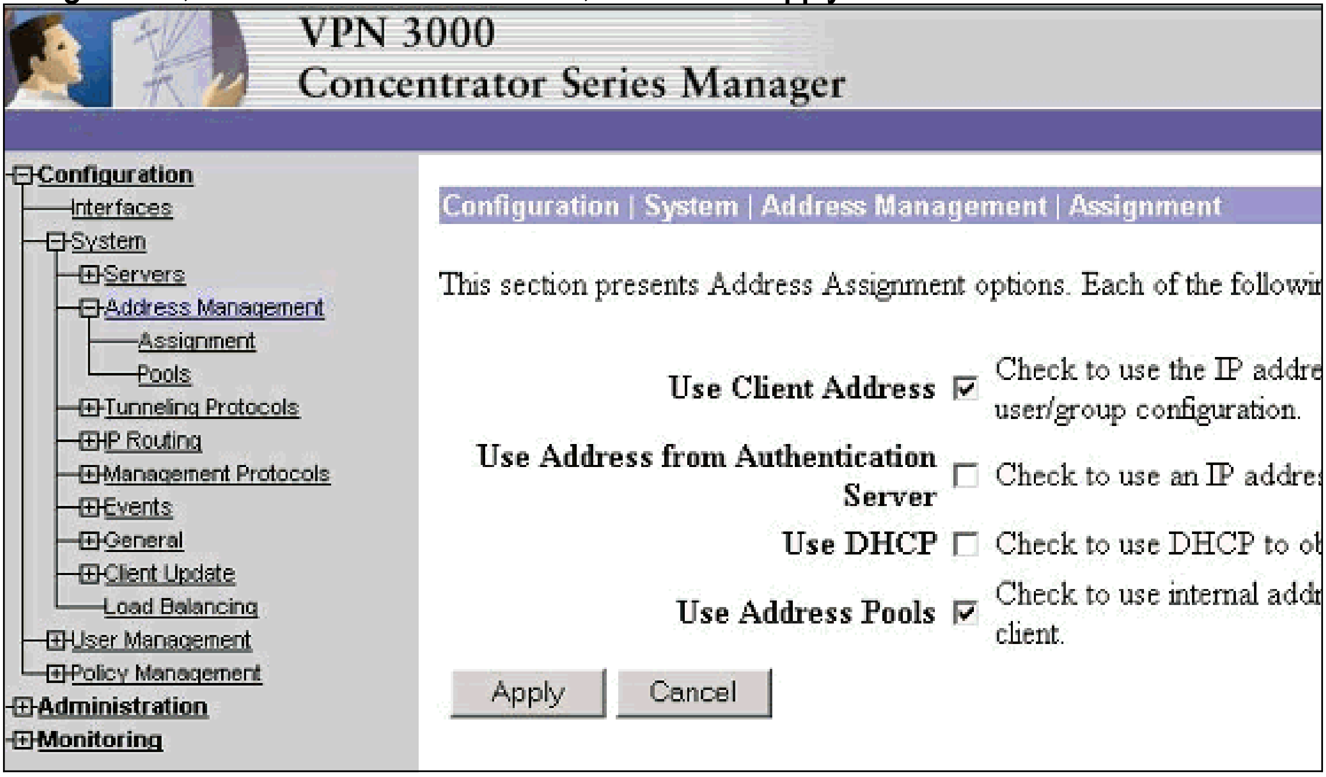


This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a pool and click **Modify** or **Delete**.

IP Pool Entry	Actions
10.20.20.20 - 10.20.20.200	

2. 要指示VPN集中器使用池，請選擇**Configuration > System > Address Management > Assignment**，選中**Use Address Pools**框，然後按一下**Apply**。

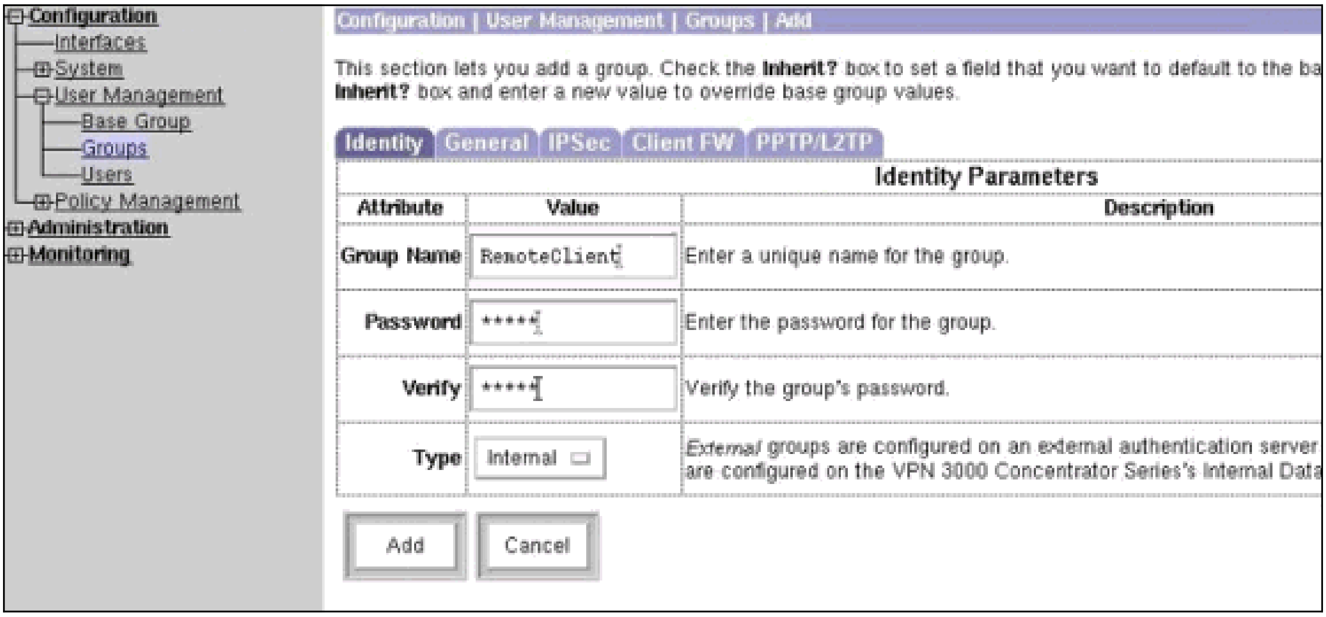


This section presents Address Assignment options. Each of the followi

Use Client Address	☑	Check to use the IP addre user/group configuration.
Use Address from Authentication Server	□	Check to use an IP addres
Use DHCP	□	Check to use DHCP to ol
Use Address Pools	☑	Check to use internal addr client.

3. 新增組和密碼。選擇**Configuration > User Management > Groups**，然後按一下**Add Group**。輸入正確的資訊，然後按一下**Add**提交資訊。此示例使用名為「RemoteClient」且口令為「

cisco」的組。



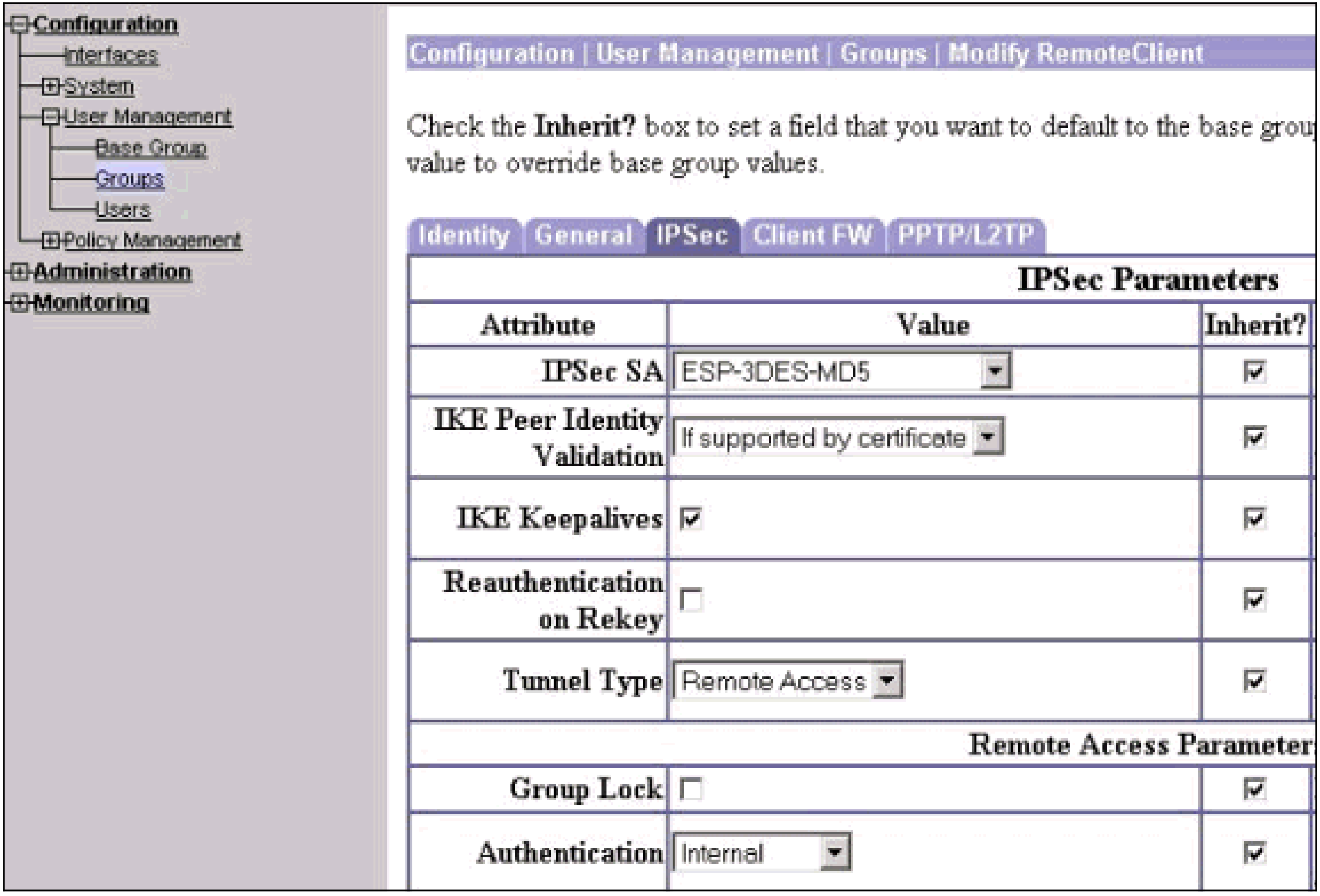
Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the ba
Inherit? box and enter a new value to override base group values.

Identity Parameters

Attribute	Value	Description
Group Name	RemoteClient	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 are configured on the VPN 3000 Concentrator Series's Internal Data

4. 在組的IPSec頁籤上，驗證身份驗證設定為**Internal**。



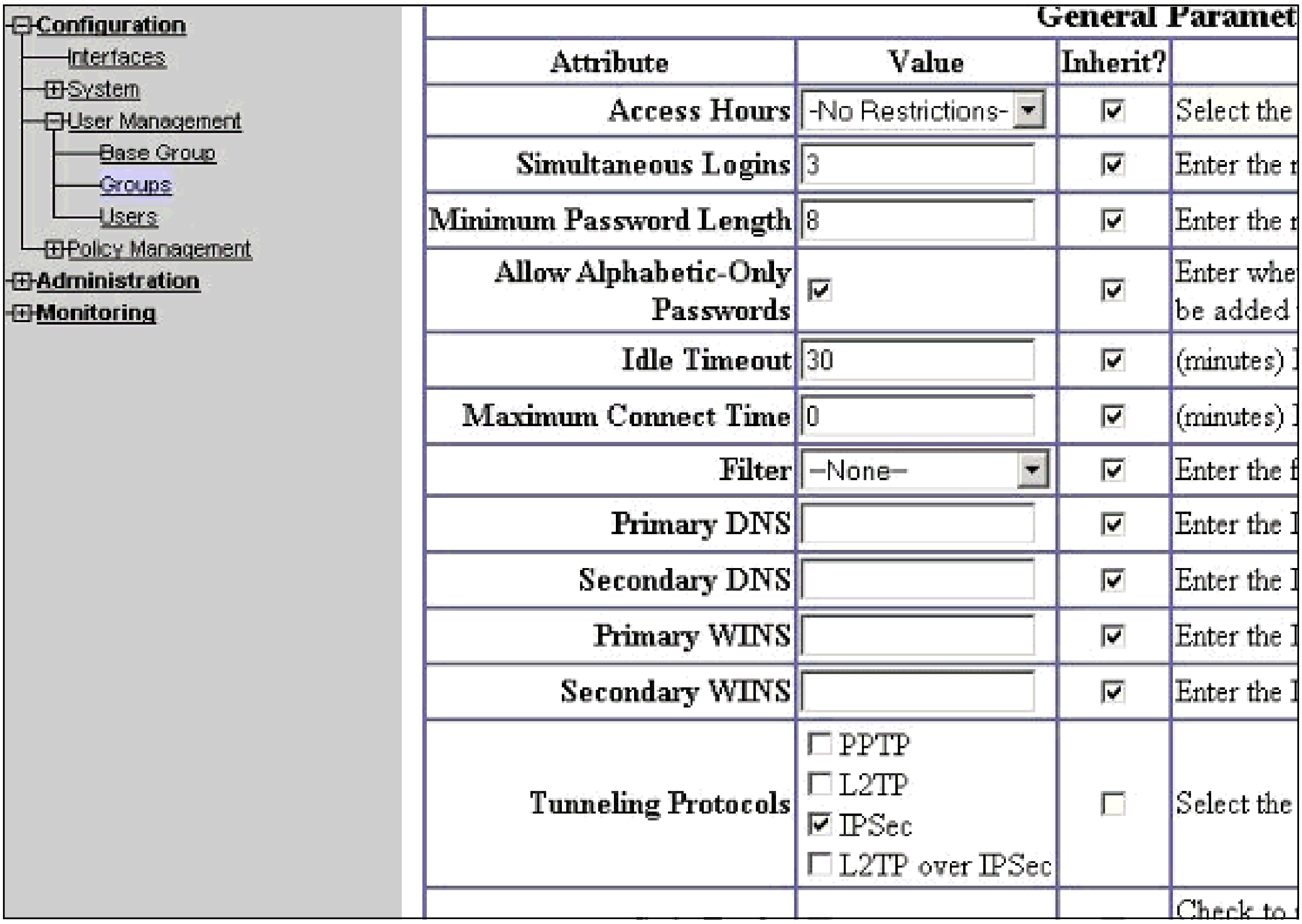
Configuration | User Management | Groups | Modify RemoteClient

Check the **Inherit?** box to set a field that you want to default to the base grou
value to override base group values.

IPSec Parameters

Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	☑
IKE Peer Identity Validation	If supported by certificate	☑
IKE Keepalives	☑	☑
Reauthentication on Rekey	□	☑
Tunnel Type	Remote Access	☑
Remote Access Parameter		
Group Lock	□	☑
Authentication	Internal	☑

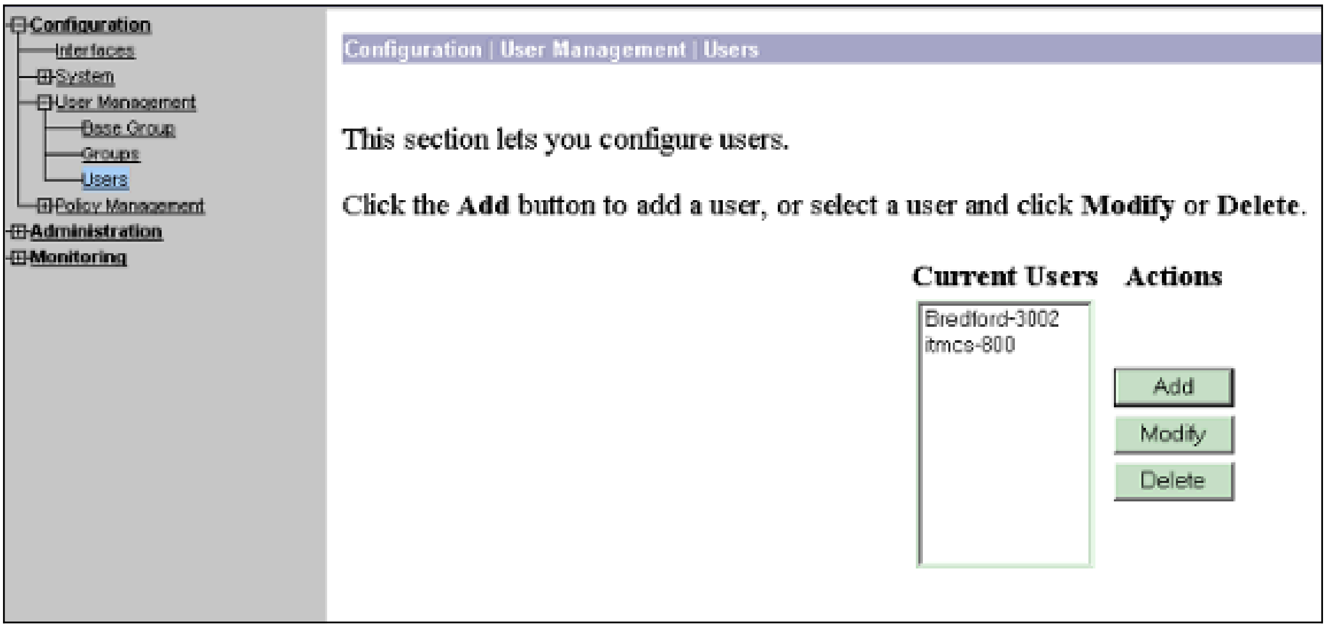
5. 在組的General頁籤上，驗證是否已選擇**IPSec**作為隧道協定。



General Paramet

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	☑	Select the
Simultaneous Logins	3	☑	Enter the n
Minimum Password Length	8	☑	Enter the n
Allow Alphabetic-Only Passwords	☑	☑	Enter whe be added
Idle Timeout	30	☑	(minutes)
Maximum Connect Time	0	☑	(minutes)
Filter	--None--	☑	Enter the f
Primary DNS		☑	Enter the I
Secondary DNS		☑	Enter the I
Primary WINS		☑	Enter the I
Secondary WINS		☑	Enter the I
Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec	□	Select the
			Check to

6. 要將使用者新增到VPN集中器，請選擇**Configuration > User Management > Users**，然後按一下**Add**。



Configuration | User Management | Users

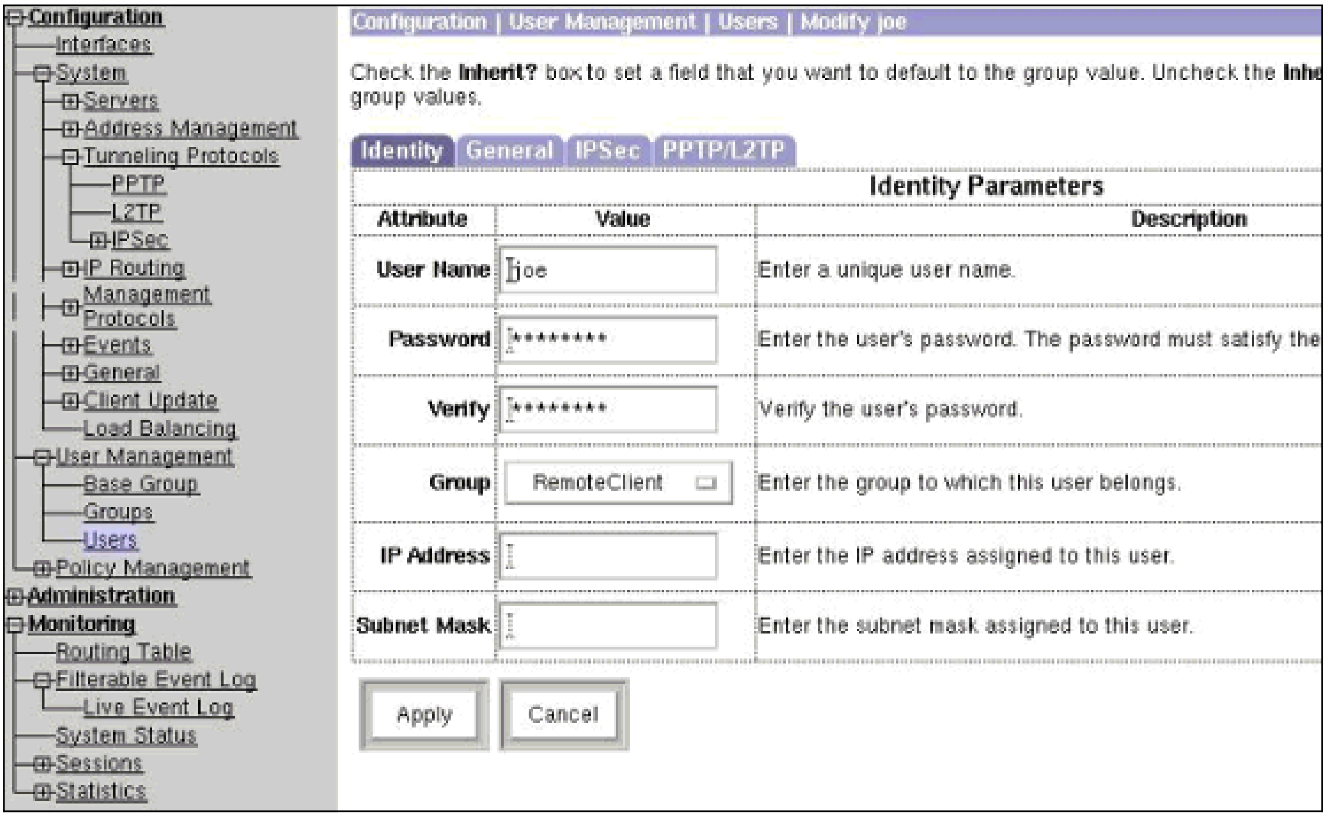
This section lets you configure users.

Click the **Add** button to add a user, or select a user and click **Modify** or **Delete**.

Current Users
Bredford-3002
itmcs-800

Actions

7. 輸入組的正確資訊，然後按一下**Apply**提交資訊。



Configuration | User Management | Users | Modify joe

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inhe**
group values.

Identity Parameters

Attribute	Value	Description
User Name	joe	Enter a unique user name.
Password	********	Enter the user's password. The password must satisfy the
Verify	********	Verify the user's password.
Group	RemoteClient	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.

驗證

連線到VPN集中器

現在配置了VPN客戶端和集中器，新的配置檔案應能連線到VPN集中器。

```
91 [cholera]: /etc/CiscoSystemsVPNClient > vpnclient connect toCORPORATE
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

Initializing the IPSec link.
Contacting the security gateway at 10.48.66.109
Authenticating user.
User Authentication for toCORPORATE...

Enter Username and Password.

Username [Joe]:
Password []:
Contacting the security gateway at 10.48.66.109
Your link is secure.
IPSec tunnel information.
Client address: 10.20.20.20
Server address: 10.48.66.109
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive.
Local LAN Access is disabled.

^Z
```

```
Suspended

[cholera]: /etc/CiscoSystemsVPNClient > bg
[1]    vpnclient connect toCORPORATE &
(The process is made to run as background process)

[cholera]: /etc/CiscoSystemsVPNClient > vpnclient disconnect

Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

Your IPSec link has been disconnected.
Disconnecting the IPSEC link.
[cholera]: /etc/CiscoSystemsVPNClient >
[1]    Exit -56                      vpnclient connect toCORPORATE

[cholera]: /etc/CiscoSystemsVPNClient >
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

調試

要啟用調試，請使用**ipseclog**命令。示例如下。

```
[cholera]: /etc/CiscoSystemsVPNClient > ipseclog /tmp/clientlog
```

連線到集中器時在客戶端上調試

```
[cholera]: /etc/CiscoSystemsVPNClient > cat /tmp/clientlog

1      17:08:49.821  01/25/2002  Sev=Info/4     CLI/0x43900002
Started vpnclient:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

2      17:08:49.855  01/25/2002  Sev=Info/4     CVPND/0x4340000F
Started cvpnd:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

3      17:08:49.857  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0xb0f0d0c0

4      17:08:49.857  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0xb0f0d0c0

5      17:08:49.858  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x637377d3
```

```
6      17:08:49.858  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x637377d3

7      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x9d4d2b9d

8      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x9d4d2b9d

9      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x5facd5bf

10     17:08:49.860  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x5facd5bf

11     17:08:49.860  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

12     17:08:49.861  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

13     17:08:49.861  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

14     17:08:49.862  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

15     17:08:49.863  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

16     17:08:49.863  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

17     17:08:50.873  01/25/2002  Sev=Info/4     CM/0x43100002
Begin connection process

18     17:08:50.883  01/25/2002  Sev=Info/4     CM/0x43100004
Establish secure connection using Ethernet

19     17:08:50.883  01/25/2002  Sev=Info/4     CM/0x43100026
Attempt connection with server "10.48.66.109"

20     17:08:50.883  01/25/2002  Sev=Info/6     IKE/0x4300003B
Attempting to establish a connection with 10.48.66.109.

21     17:08:51.099  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
10.48.66.109

22     17:08:51.099  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

23     17:08:51.100  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

24     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

25     17:08:51.400  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID,
VID) from 10.48.66.109

26     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100
```

```
27     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000001
Peer is a Cisco-Unity compliant peer

28     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 09002689DFD6B712

29     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

30     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000001
Peer supports DPD

31     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500301

32     17:08:51.505  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 10.48.66.109

33     17:08:51.510  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

34     17:08:51.511  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

35     17:08:51.511  01/25/2002  Sev=Info/4     CM/0x43100015
Launch xAuth application

36     17:08:56.333  01/25/2002  Sev=Info/4     CM/0x43100017
xAuth application returned

37     17:08:56.334  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

38     17:08:56.636  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

39     17:08:56.637  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

40     17:08:56.637  01/25/2002  Sev=Info/4     CM/0x4310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

41     17:08:56.639  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

42     17:08:56.639  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

43     17:08:56.645  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

44     17:08:56.646  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

45     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x43000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
value = 10.20.20.20

46     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: ,
value = 0x00000000
```

```
47     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: ,
value = 0x00000000

48     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Series
Version 3.1.Rel built by vmurphy on Aug 06 2001 13:47:37

49     17:08:56.648  01/25/2002  Sev=Info/4     CM/0x43100019
Mode Config data received

50     17:08:56.651  01/25/2002  Sev=Info/5     IKE/0x43000055
Received a key request from Driver for IP address 10.48.66.109,
GW IP = 10.48.66.109

51     17:08:56.652  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

52     17:08:56.653  01/25/2002  Sev=Info/5     IKE/0x43000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 10.48.66.109

53     17:08:56.653  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

54     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

55     17:08:56.663  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME)
from 10.48.66.109

56     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 86400 seconds

57     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x43000046
This SA has already been alive for 6 seconds, setting expiry
to 86394 seconds from now

58     17:08:56.666  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

59     17:08:56.666  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

60     17:08:56.667  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 28800 seconds

61     17:08:56.667  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

62     17:08:56.667  01/25/2002  Sev=Info/5     IKE/0x43000058
Loading IPsec SA (Message ID = 0x4CEF4B32 OUTBOUND SPI =
0x5EAD41F5 INBOUND SPI = 0xE66C759A)

63     17:08:56.668  01/25/2002  Sev=Info/5     IKE/0x43000025
Loaded OUTBOUND ESP SPI: 0x5EAD41F5

64     17:08:56.669  01/25/2002  Sev=Info/5     IKE/0x43000026
Loaded INBOUND ESP SPI: 0xE66C759A

65     17:08:56.669  01/25/2002  Sev=Info/4     CM/0x4310001A
```

```
One secure connection established

66     17:08:56.674  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

67     17:08:56.675  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

68     17:08:56.675  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 28800 seconds

69     17:08:56.675  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

70     17:08:56.675  01/25/2002  Sev=Info/5     IKE/0x43000058
Loading IPsec SA (Message ID = 0x88E9321A OUTBOUND SPI =
0x333B4239 INBOUND SPI = 0x6B040746)

71     17:08:56.677  01/25/2002  Sev=Info/5     IKE/0x43000025
Loaded OUTBOUND ESP SPI: 0x333B4239

72     17:08:56.677  01/25/2002  Sev=Info/5     IKE/0x43000026
Loaded INBOUND ESP SPI: 0x6B040746

73     17:08:56.678  01/25/2002  Sev=Info/4     CM/0x43100022
Additional Phase 2 SA established.

74     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

75     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

76     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x5ead41f5 into key list

77     17:08:57.753  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

78     17:08:57.753  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0xe66c759a into key list

79     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

80     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x333b4239 into key list

81     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

82     17:08:57.755  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x6b040746 into key list

83     17:09:13.752  01/25/2002  Sev=Info/6     IKE/0x4300003D
Sending DPD request to 10.48.66.109, seq# = 2948297981

84     17:09:13.752  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 10.48.66.109

85     17:09:13.758  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109
```

```
86     17:09:13.758  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)
from 10.48.66.109

87     17:09:13.759  01/25/2002  Sev=Info/5     IKE/0x4300003F
Received DPD ACK from 10.48.66.109, seq# received = 2948297981,
seq# expected = 2948297981
```

debug on the client when disconnecting

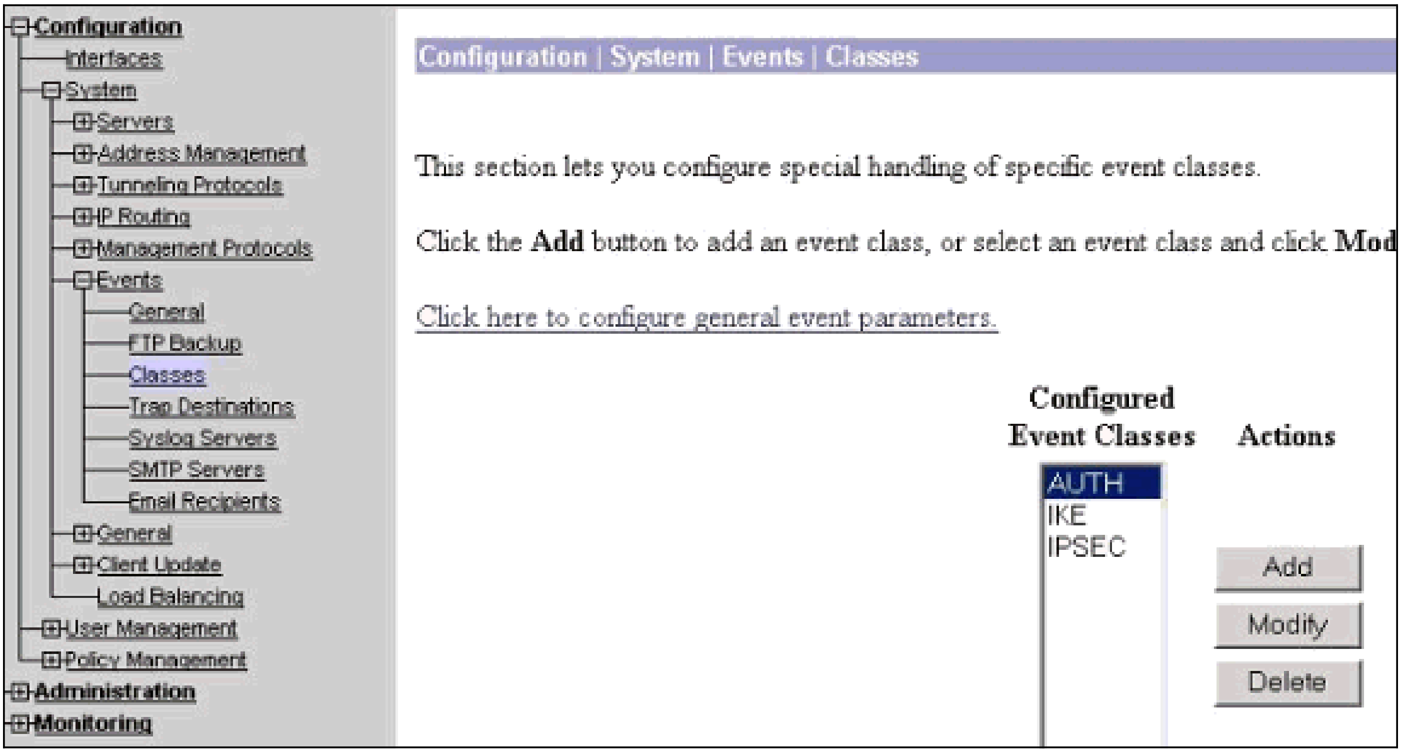
```
88     17:09:16.366  01/25/2002  Sev=Info/4     CLI/0x43900002
Started vpnclient:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

89     17:09:16.367  01/25/2002  Sev=Info/4     CM/0x4310000A
Secure connections terminated

90     17:09:16.367  01/25/2002  Sev=Info/5     IKE/0x43000018
Deleting IPsec SA: (OUTBOUND SPI = 333B4239 INBOUND SPI = 6B040746)

91     17:09:16.368  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

92     17:09:16.369  01/25/2002  Sev=Info/5     IKE/0x43000018
Deleting IPsec SA: (OUTBOUND SPI = 5EAD41F5 INBOUND SPI = E66C759A)

93     17:09:16.369  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

94     17:09:16.370  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

95     17:09:16.371  01/25/2002  Sev=Info/4     CM/0x43100013
Phase 1 SA deleted cause by DEL_REASON_RESET_SADB.
0 Phase 1 SA currently in the system

96     17:09:16.371  01/25/2002  Sev=Info/5     CM/0x43100029
Initializing CVPNDrv

97     17:09:16.371  01/25/2002  Sev=Info/6     CM/0x43100035
Tunnel to headend device 10.48.66.109 disconnected:
duration: 0 days 0:0:20

98     17:09:16.375  01/25/2002  Sev=Info/5     CM/0x43100029
Initializing CVPNDrv

99     17:09:16.377  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

100    17:09:16.377  01/25/2002  Sev=Warning/2  IKE/0x83000061
Attempted incoming connection from 10.48.66.109. Inbound
connections are not allowed.

101    17:09:17.372  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x6b040746

102    17:09:17.372  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x333b4239
```

```
103    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0xe66c759a

104    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x5ead41f5

105    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

106    17:09:17.374  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

107    17:09:17.374  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

108    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

109    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

110    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

111    17:09:17.376  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys
```

VPN集中器上的調試

選擇Configuration > System > Events > Classes，以在發生事件連線失敗時開啟以下調試。

- AUTH — 記錄嚴重性1-13
- IKE — 日誌嚴重性1-6
- IPSEC — 日誌的嚴重性1-6



Configuration | System | Events | Classes

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Mod**

Click here to configure general event parameters.

Configured Event Classes: AUTH, IKE, IPSEC

您可以通過選擇Monitoring > Event Log來檢視日誌。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN 3000系列使用者端支援頁面
- IPSec支援頁面
- 技術支援 - Cisco Systems