

Configurazione di IPSec da VPN Client versione 3.5 Solaris a VPN 3000 Concentrator

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Connessione a VPN Concentrator](#)

[Risoluzione dei problemi](#)

[Debug](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene spiegato come configurare VPN Client 3.5 per Solaris 2.6 in modo da connettersi a un concentratore VPN 3000.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti prerequisiti.

- In questo esempio viene utilizzata una chiave già condivisa per l'autenticazione di gruppo. Il nome utente e la password (autenticazione estesa) vengono controllati rispetto al database interno di VPN Concentrator.
- Il client VPN deve essere installato correttamente. Per ulteriori informazioni sull'installazione, fare riferimento a [Installazione del client VPN per Solaris](#).
- Deve esistere una connettività IP tra il client VPN e l'interfaccia pubblica del concentratore VPN. Le informazioni sulla subnet mask e sul gateway devono essere impostate correttamente.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Cisco VPN Client per Solaris 2.6 versione 3.5, immagine 3DES. (nome immagine: vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Cisco VPN Concentrator Tipo: 3005 Bootcode Rev: Altiga Networks/VPN Concentrator versione 2.2.int_9 Jan 19 2000 05:36:41 Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Series versione 3.1.Rel agosto 2001 13:47:37

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

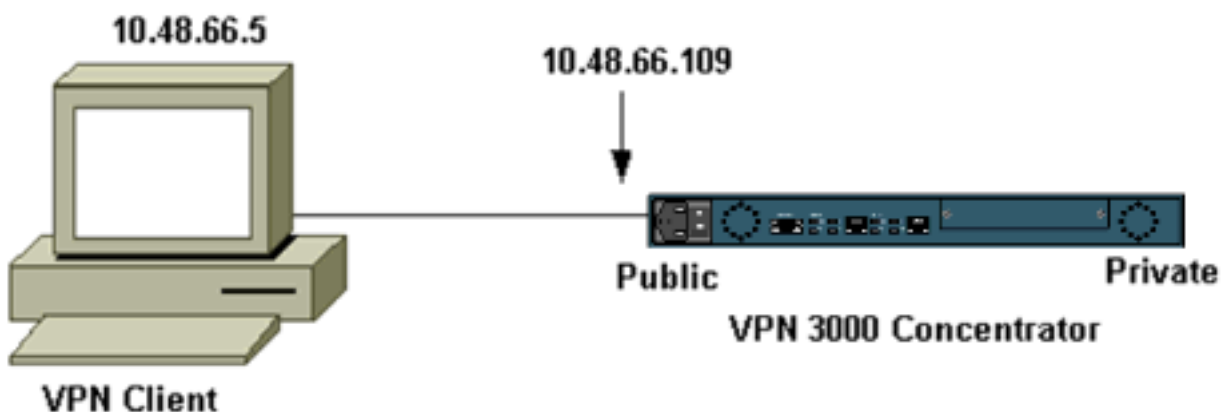
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Nota: per la connessione del client VPN 3.5 al concentratore VPN, è necessaria la versione 3.0 o successiva.

Configurazioni

Creazione di un profilo utente per la connessione

I profili utente sono memorizzati nella directory /etc/CiscoSystemsVPNClient/Profiles. Questi file di testo hanno estensione .pcf e contengono i parametri necessari per stabilire una connessione a un concentratore VPN. Potete creare un nuovo file o modificarne uno esistente. Nella directory dei profili è disponibile un profilo di esempio, sample.pcf. In questo esempio viene illustrato come utilizzare il file per creare un nuovo profilo denominato toCORPORATE.pcf.

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

È possibile utilizzare l'editor di testo preferito per modificare questo nuovo file, inCORPORATE.pcf. Prima di apportare modifiche, il file è simile al seguente.

Nota: se si desidera utilizzare IPSec over Network Address Translation (NAT), la voce EnableNat nella configurazione seguente deve essere "EnableNat=1" anziché "EnableNat=0".

```
[main]  
Description=sample user profile  
Host=10.7.44.1  
AuthType=1  
GroupName=monkeys  
EnableISPCConnect=0  
ISPCConnectType=0  
ISPCConnect=  
ISPCCommand=  
Username=chimchim  
SaveUserPassword=0  
EnableBackup=0  
BackupServer=  
EnableNat=0  
CertStore=0  
CertName=  
CertPath=  
CertSubjectName=  
CertSerialHash=00000000000000000000000000000000  
DHGroup=2  
ForceKeepAlives=0
```

Fare riferimento [a Profili utente](#) per una descrizione delle parole chiave dei profili utente.

Per configurare correttamente il profilo, è necessario conoscere almeno i valori equivalenti per le informazioni seguenti.

- Il nome host o l'indirizzo IP pubblico del concentratore VPN (10.48.66.109)
- Nome del gruppo (RemoteClient)
- La password del gruppo (cisco)
- Il nome utente (joe)

Modificare il file con le informazioni in modo che sia simile a quanto riportato di seguito.

```
[main]  
Description=Connection to the corporate  
Host=10.48.66.109  
AuthType=1  
GroupName=RemoteClient  
GroupPwd=cisco  
EnableISPCConnect=0
```

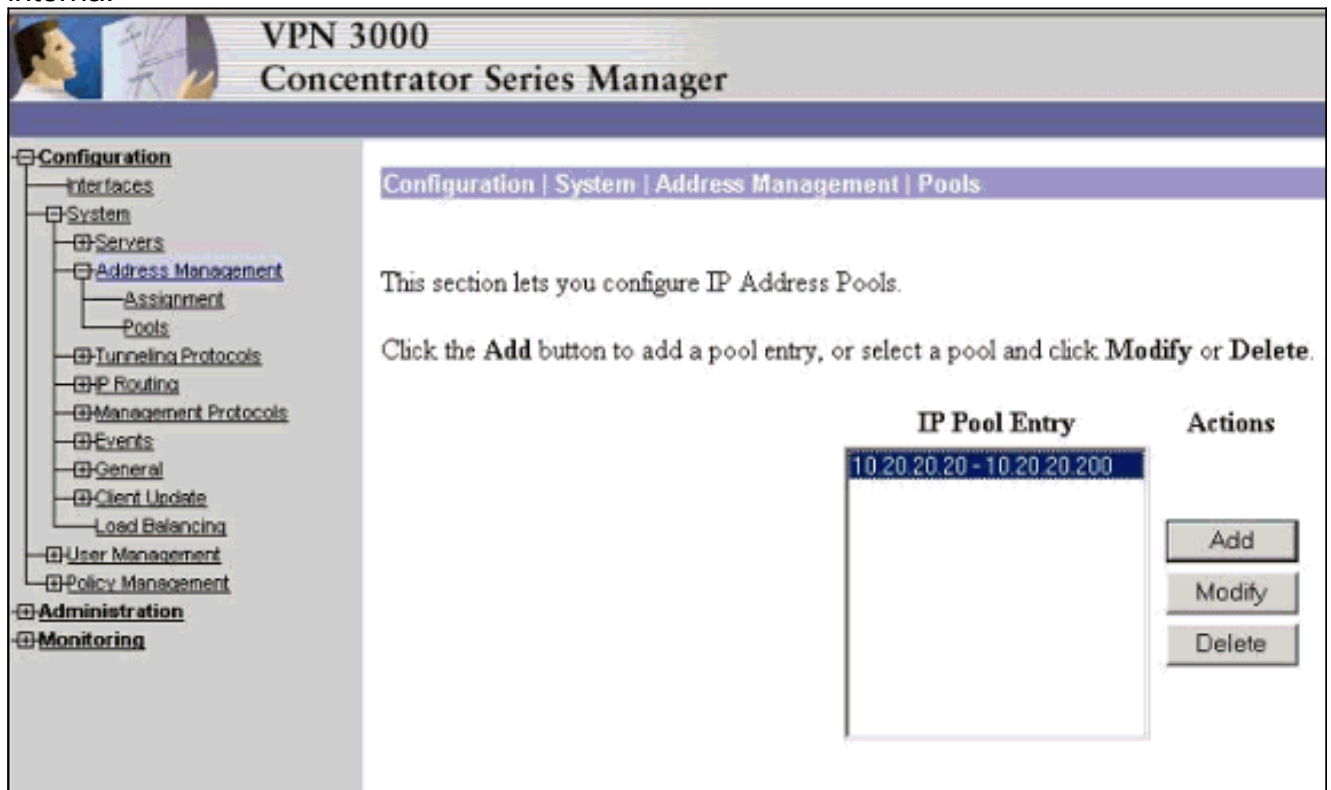
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=joe
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0

Configurazione di VPN Concentrator

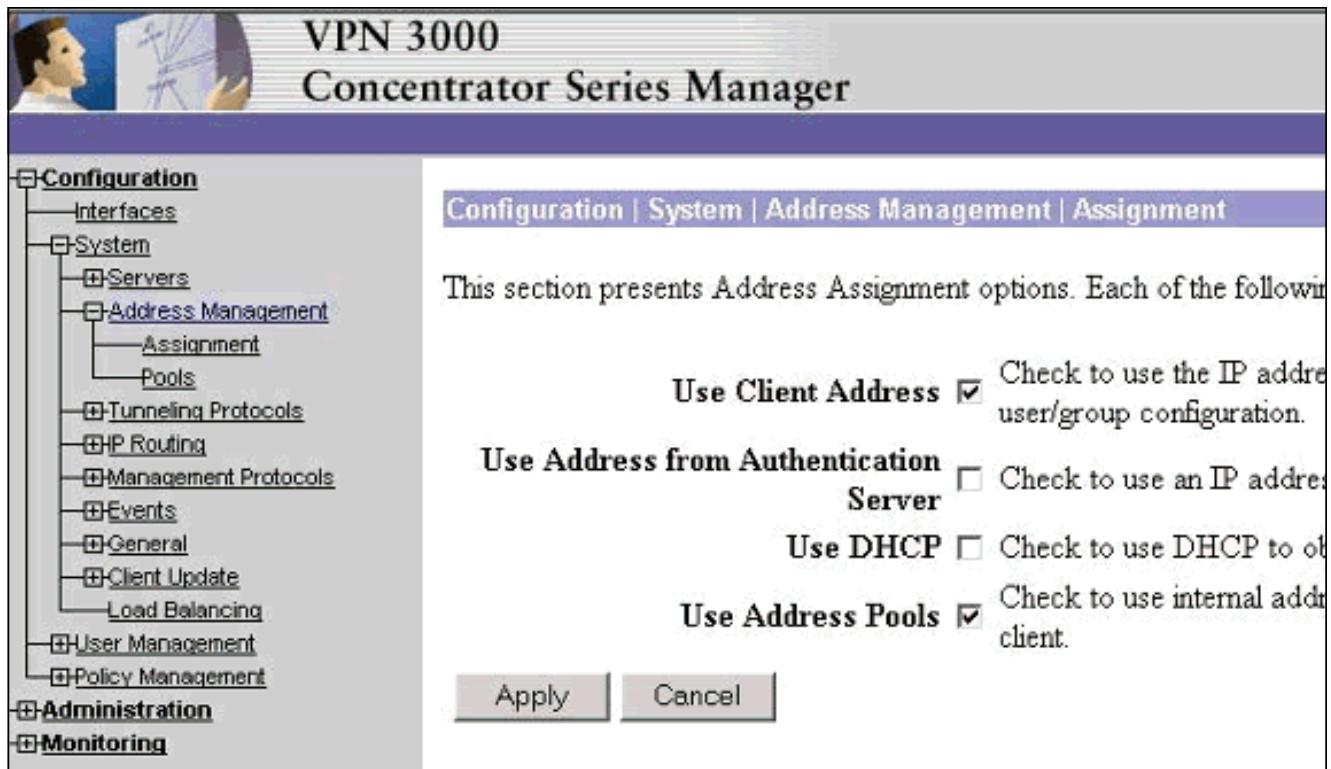
Utilizzare la procedura seguente per configurare VPN Concentrator.

Nota: a causa dei limiti di spazio, le immagini acquisite mostrano solo aree parziali o rilevanti.

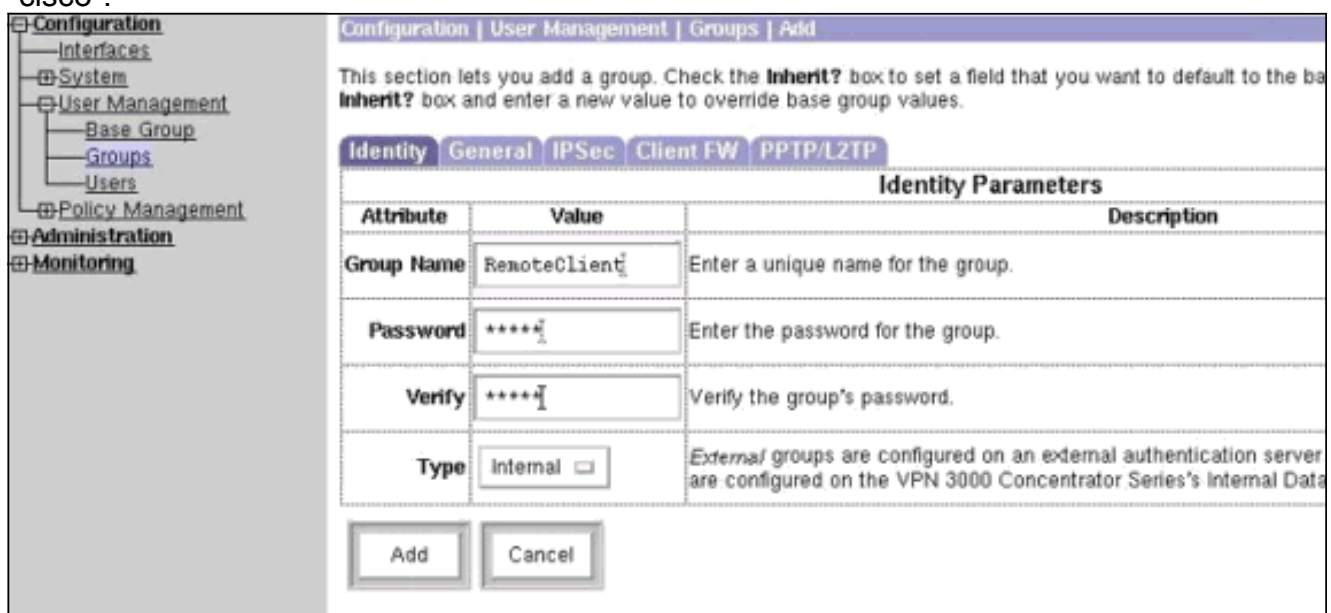
1. Assegnare il pool di indirizzi. Per assegnare un intervallo di indirizzi IP disponibili, puntare un browser all'interfaccia interna di VPN Concentrator e selezionare **Configurazione > Sistema > Gestione indirizzi > Pool**. Fare clic su **Add**. Specificare un intervallo di indirizzi IP che non sia in conflitto con altri dispositivi nella rete interna.



2. Per indicare a VPN Concentrator di utilizzare il pool, selezionare **Configurazione > Sistema > Gestione indirizzi > Assegnazione**, selezionare la casella **Usa pool di indirizzi** e quindi fare clic su **Applica**.



3. Aggiungere un gruppo e una password. Selezionare **Configurazione > Gestione utenti > Gruppi**, quindi fare clic su **Aggiungi gruppo**. Immettere le informazioni corrette e quindi fare clic su **Aggiungi** per inviare le informazioni. In questo esempio viene utilizzato un gruppo denominato "RemoteClient" con una password di "cisco".



4. Nella scheda IPSec del gruppo verificare che l'autenticazione sia impostata su **Interno**.

Configuration | User Management | Groups | Modify RemoteClient

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

Identity | General | **IPSec** | Client FW | PPTP/L2TP

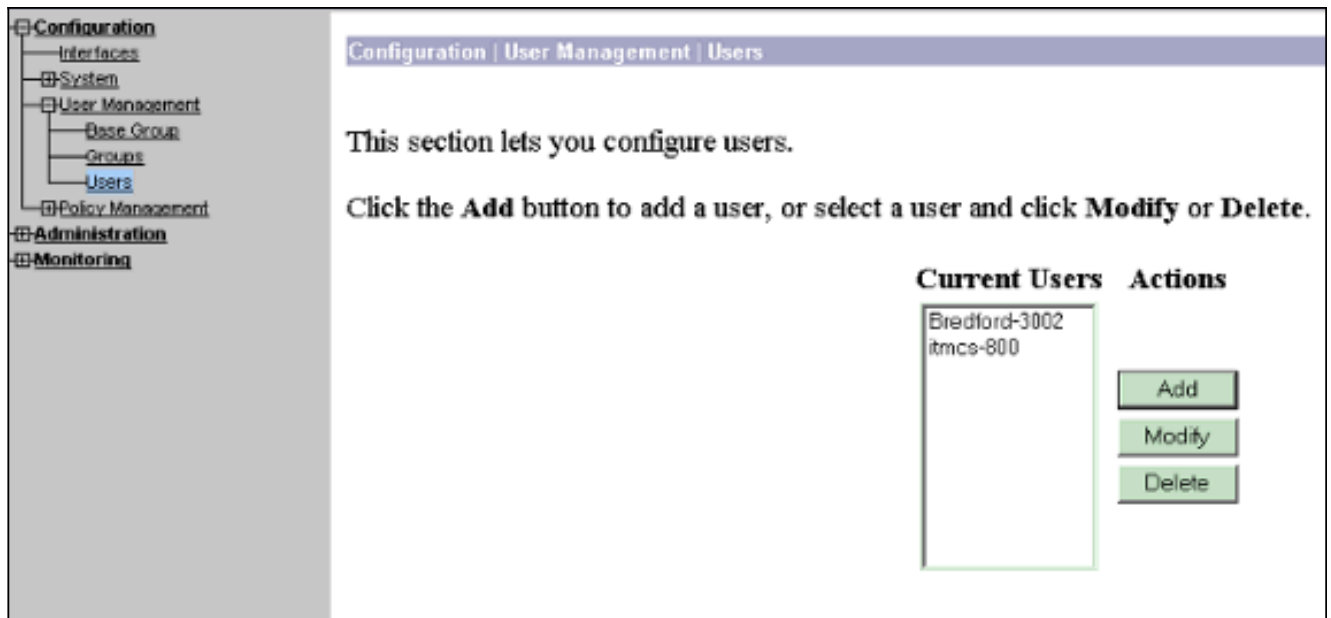
IPSec Parameters		
Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>
Remote Access Parameter		
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

5. Nella scheda Generale del gruppo verificare che **IPSec** sia selezionato come protocollo di tunneling.

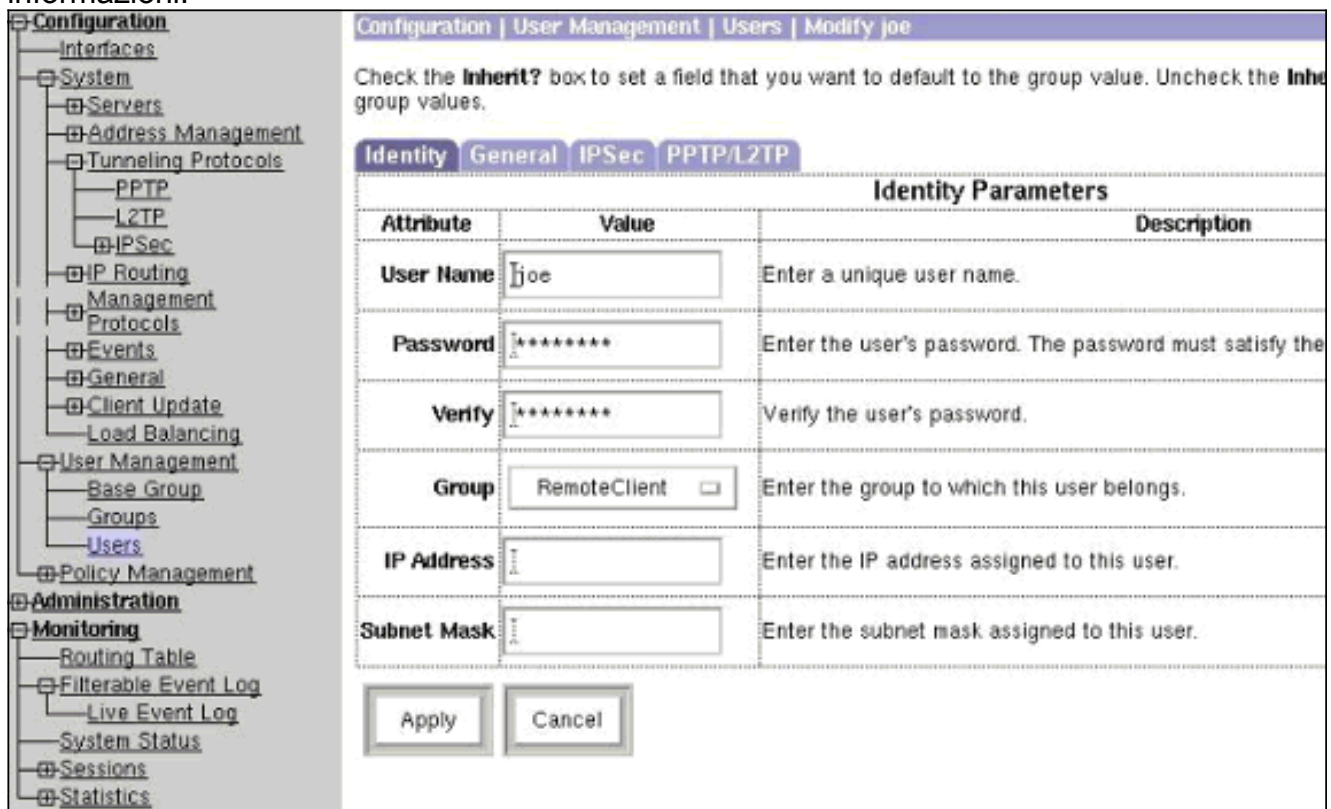
Configuration | User Management | Groups | Modify RemoteClient

General Parameters		
Attribute	Value	Inherit?
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>
Simultaneous Logins	3	<input checked="" type="checkbox"/>
Minimum Password Length	8	<input checked="" type="checkbox"/>
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Idle Timeout	30	<input checked="" type="checkbox"/>
Maximum Connect Time	0	<input checked="" type="checkbox"/>
Filter	-None-	<input checked="" type="checkbox"/>
Primary DNS		<input checked="" type="checkbox"/>
Secondary DNS		<input checked="" type="checkbox"/>
Primary WINS		<input checked="" type="checkbox"/>
Secondary WINS		<input checked="" type="checkbox"/>
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	<input type="checkbox"/>

6. Per aggiungere l'utente a VPN Concentrator, selezionare **Configurazione > Gestione utenti > Utenti**, quindi fare clic su **Aggiungi**.



7. Immettere le informazioni corrette per il gruppo, quindi fare clic su **Applica** per inviare le informazioni.



[Verifica](#)

[Connessione a VPN Concentrator](#)

Ora che il client VPN e il concentratore sono stati configurati, il nuovo profilo dovrebbe funzionare per la connessione al concentratore VPN.

```
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 >
```

[Risoluzione dei problemi](#)

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

[Debug](#)

Per abilitare i debug, usare il comando **ipseclog**. Di seguito è riportato un esempio.

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

[Debug del client durante la connessione al concentratore](#)

```
[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

[Debug sul VPN Concentrator](#)

Selezionare **Configurazione > Sistema > Eventi > Classi** per attivare il debug seguente in caso di errori di connessione degli eventi.

- **AUTH** - Gravità del log 1-13
- **IKE** - Gravità da registrare 1-6
- **IPSEC** - Gravità del registro 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	Actions
AUTH	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
IKE	
IPSEC	

Per visualizzare il registro, selezionare **Monitoraggio > Registro eventi**.

Informazioni correlate

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Cisco VPN serie 3000 Client Support Page](#)
- [Pagina di supporto per IPSec](#)
- [Supporto tecnico – Cisco Systems](#)