

VPN 3000集中器和VPN Client 4.x for Windows之間使用RADIUS進行使用者身份驗證和記帳的IPsec配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[使用VPN 3000 Concentrator上的組](#)

[VPN 3000集中器如何使用組和使用者屬性](#)

[VPN 3000系列集中器配置](#)

[RADIUS伺服器組態](#)

[為VPN客戶端使用者分配靜態IP地址](#)

[VPN客戶端配置](#)

[新增記帳](#)

[驗證](#)

[驗證VPN集中器](#)

[驗證VPN客戶端](#)

[疑難排解](#)

[VPN Client 4.8 for Windows故障排除](#)

[相關資訊](#)

簡介

本文檔介紹如何在Cisco VPN 3000集中器和使用RADIUS進行使用者身份驗證和記帳的Cisco VPN Client 4.x for Microsoft Windows之間建立IPsec隧道。本檔案建議使用適用於Windows的Cisco安全存取控制伺服器(ACS)執行更簡單的RADIUS組態，對連線到VPN 3000集中器的使用者進行驗證。VPN 3000集中器上的組是被視為單個實體的使用者集合。與單個使用者不同，組配置可以簡化系統管理和簡化配置任務。

請參閱[PIX/ASA 7.x和Cisco VPN Client 4.x for Windows with Microsoft Windows 2003 IAS RADIUS身份驗證配置示例](#)，以在Cisco VPN Client(4.x for Windows)與使用Microsoft Windows 2003 Internet Authentication Service(IAS)RADIUS伺服器的PIX 500系列安全裝置7.x之間設定遠端訪問VPN連線。

請參閱[使用RADIUS進行使用者身份驗證](#)在Cisco IOS路由器和Cisco VPN客戶端4.x for Windows之間配置IPsec，以配置路由器與使用RADIUS進行使用者身份驗證的Cisco VPN客戶端4.x之間的連線

。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝用於Windows RADIUS的Cisco Secure ACS，並且可在其他裝置上正常運行。
- Cisco VPN 3000 Concentrator已配置並可通過HTML介面進行管理。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure ACS for Windows (版本4.0)
- 帶有映像檔案4.7.2.B的Cisco VPN 3000系列集中器
- Cisco VPN使用者端4.x

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

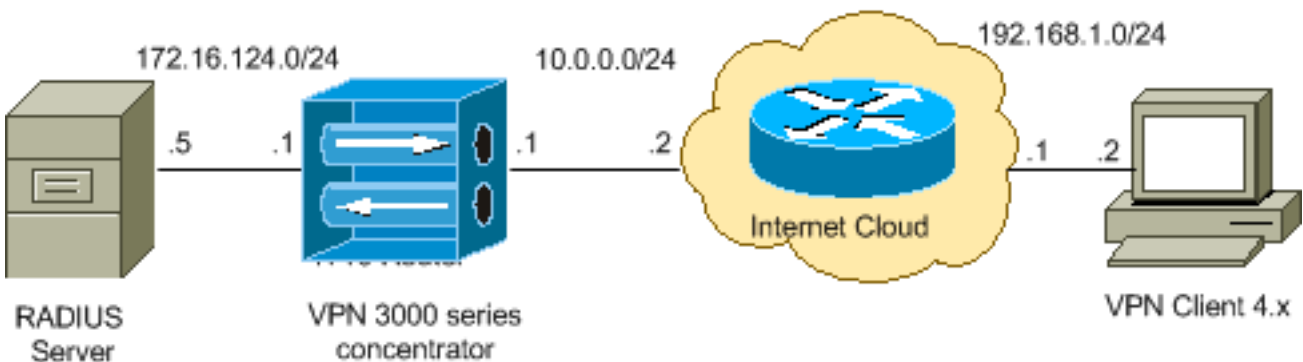
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是[RFC 1918](#)，已在實驗室環境中使用。

使用VPN 3000 Concentrator上的組

可以為Cisco Secure ACS for Windows和VPN 3000 Concentrator定義組，但它們使用組的方式有所不同。執行以下任務以簡化操作：

- 在VPN 3000 Concentrator上為建立初始通道時配置單個組。這通常稱為隧道組，用於使用預共用金鑰（組密碼）建立到VPN 3000集中器的加密網際網路金鑰交換(IKE)會話。這是應在要連線到VPN集中器的所有Cisco VPN客戶端上配置的相同組名和密碼。
- 在Cisco Secure ACS for Windows伺服器上配置使用標準RADIUS屬性和供應商特定屬性(VSA)進行策略管理的組。應與VPN 3000集中器一起使用的VSA是RADIUS(VPN 3000)屬性。
- 在適用於Windows RADIUS的Cisco Secure ACS伺服器上配置使用者，並將他們分配到同一服務器上配置的其中一個組。使用者繼承為其組定義的屬性，當使用者通過身份驗證時，Cisco Secure ACS for Windows會將這些屬性傳送到VPN集中器。

VPN 3000集中器如何使用組和使用者的屬性

VPN 3000集中器使用VPN集中器驗證隧道組和使用RADIUS驗證使用者後，必須組織已接收的屬性。無論驗證是在VPN集中器中進行還是在RADIUS中進行，VPN集中器都會按以下優先順序使用屬性：

1. **使用者屬性** — 這些屬性始終優先於任何其他屬性。
2. **Tunnel Group attributes** — 使用者通過身份驗證時未返回的任何屬性都由Tunnel Group屬性填充。
3. **基本組屬性** — 使用者或隧道組屬性中缺少的任何屬性都由VPN集中器基本組屬性填充。

VPN 3000系列集中器配置

完成本節中的步驟，以便為IPsec連線所需的引數配置Cisco VPN 3000集中器，並為VPN使用者配置AAA客戶端，以通過RADIUS伺服器進行身份驗證。

在本實驗設定中，首先通過控制檯埠訪問VPN集中器，然後新增最小配置，如以下輸出所示：

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
```

```

----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>

```

VPN集中器顯示在Quick Configuration (快速配置) 中，這些專案已配置。

- 時間/日期
- Configuration > Interfaces(public=10.0.0.1/24, private=172.16.124.1/24)中的介面/掩碼
- Configuration > System > IP routing > Default_Gateway(10.0.0.2)中的預設網關

此時，可從內部網路通過HTML訪問VPN集中器。

注意：如果從外部管理VPN集中器，則還要執行以下步驟：

1. 選擇Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1.Private (預設)。
2. 選擇Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation以新增外部管理器的IP地址。

僅當您從外部管理VPN集中器時，才需要執行這些步驟。

完成這兩個步驟後，可通過GUI使用Web瀏覽器並連線到剛配置的介面的IP來完成其餘配置。在此示例及此刻，可從內部網路通過HTML訪問VPN集中器：

1. 選擇Configuration > Interfaces，以便在啟動GUI後重新檢查介面。

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. 完成以下步驟，將適用於Windows RADIUS的Cisco Secure ACS伺服器新增到VPN 3000集中器配置中。選擇Configuration > System > Servers > Authentication，然後從左側選單中按一下Add。

Configure and add a user authentication server.

<p>Server Type <input type="text" value="RADIUS"/></p> <p>Authentication Server <input type="text" value="172.16.124.5"/></p> <p>Used For <input type="text" value="User Authentication"/></p> <p>Server Port <input type="text" value="0"/></p> <p>Timeout <input type="text" value="4"/></p> <p>Retries <input type="text" value="2"/></p> <p>Server Secret <input type="text" value="j0A0ic0ic0ic0A"/></p> <p>Verify <input type="text" value="j0A0ic0ic0ic0A"/></p> <p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	<p>Selecting <i>Internal Server</i> will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at</p> <p>Enter IP address or hostname.</p> <p>Select the operation(s) for which this RADIUS se</p> <p>Enter 0 for default port (1645).</p> <p>Enter the timeout for this server (seconds).</p> <p>Enter the number of retries for this server.</p> <p>Enter the RADIUS server secret.</p> <p>Re-enter the secret.</p>
---	---

選擇伺服器型別RADIUS，並為適用於Windows RADIUS伺服器的Cisco Secure ACS新增這些引數。將所有其它引數保留為其預設狀態。**Authentication Server** — 輸入適用於Windows RADIUS伺服器的Cisco Secure ACS的IP地址。**Server Secret** — 輸入RADIUS伺服器金鑰。此金鑰必須與在Cisco Secure ACS for Windows配置中配置VPN 3000集中器時使用的金鑰相同。**Verify** — 重新輸入密碼進行驗證。這會將身份驗證伺服器新增到VPN 3000集中器的全域性配置中。除已明確定義身份驗證伺服器外，此伺服器由所有組使用。如果沒有為組配置身份驗證伺服器，它將恢復為全域性身份驗證伺服器。

- 完成以下步驟，以便在VPN 3000集中器上配置隧道組。從左側選單中選擇**Configuration > User Management > Groups**，然後按一下Add。在「配置」頁籤中更改或新增這些引數。在更改以下所有引數之前，請勿按一下「應用」：**注意**：這些引數是遠端訪問VPN連線所需的最低引數。這些引數還假設VPN 3000集中器上的基本組中的預設設定未更改。**身份**

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

組名稱(Group Name) — 鍵入組名稱。例如IPsecUsers。**Password** — 輸入組的密碼。這是IKE會話的預共用金鑰。**Verify** — 重新輸入密碼進行驗證。**型別(Type)** — 將此值保留為預設值：內部。

IPsec

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

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.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to perform keepalive checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Updates are needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for members of this group. This method only applies to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

Tunnel Type — 選擇Remote-Access。**Authentication** - RADIUS。這告知VPN集中器使用什麼方法來驗證使用者。**Mode Config** — 檢查模式配置。按一下「Apply」。

- 完成以下步驟，以便在VPN 3000集中器上配置多個身份驗證伺服器。定義組後，突出顯示該組，然後按一下Modify列下的**Authentication Servers**。可以為每個組定義單獨的身份驗證伺服器，即使這些伺服器在全域性伺服器中不存在。

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	ipsecgroup (Internally Configured)	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

選擇伺服器型別RADIUS，然後為您的Cisco Secure ACS for Windows RADIUS伺服器新增這些引數。將所有其它引數保留為其預設狀態。**Authentication Server** — 輸入適用於Windows RADIUS伺服器的Cisco Secure ACS的IP地址。**Server Secret** — 輸入RADIUS伺服器金鑰。此金鑰必須與在Cisco Secure ACS for Windows配置中配置VPN 3000集中器時使用的金鑰相

同。Verify — 重新輸入密碼進行驗證。

5. 選擇 Configuration > System > Address Management > Assignment，然後選中 Use Address from Authentication Server，以便在客戶端通過身份驗證後，從RADIUS伺服器中建立的IP池將IP地址分配給VPN客戶端。

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client.

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply Cancel

RADIUS伺服器組態

本文檔的這一部分介紹將Cisco Secure ACS配置為VPN客戶端使用者身份驗證的RADIUS伺服器所需的過程，由Cisco VPN 3000系列集中器 — AAA客戶端轉發。

按兩下ACS Admin圖示，以在運行Cisco Secure ACS for Windows RADIUS伺服器的PC上啟動管理會話。如果需要，請使用正確的使用者名稱和密碼登入。

1. 完成以下步驟，將VPN 3000集中器新增到Cisco Secure ACS for Windows伺服器配置中。選擇Network Configuration，然後按一下Add Entry以將AAA客戶端新增到RADIUS伺服器。

The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main area is titled 'Select' and contains a table of AAA Clients. The table has three columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. There are two entries in the table. Below the table are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

為VPN 3000集中器新增以下引數

:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Submit

Submit + Apply

Cancel

AAA Client Hostname — 輸入VPN 3000集中器的主機名（用於DNS解析）。**AAA Client IP Address** — 輸入VPN 3000集中器的IP地址。**Key** — 輸入RADIUS伺服器金鑰。此金鑰必須與在VPN集中器上新增身份驗證伺服器時配置的金鑰相同。**Authenticate Using** — 選擇**RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**。這允許VPN 3000 VSA顯示在Group configuration視窗中。按一下「**Submit**」。選擇**Interface Configuration**，按一下**RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**，然後選中**Group [26] Vendor-Specific**。

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

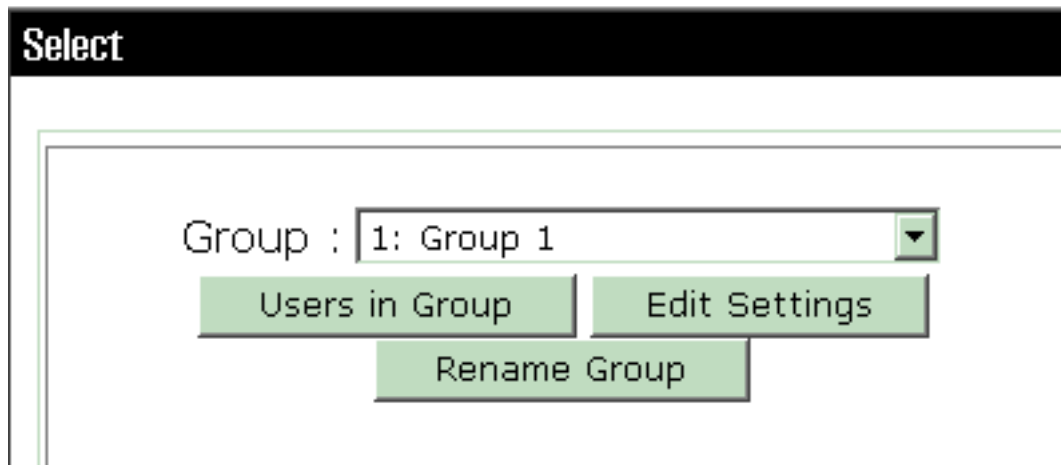
Submit

Cancel

註：「RADIUS屬性26」是指所有供應商特定的屬性。例如，選擇**Interface Configuration > RADIUS(Cisco VPN 3000)**，然後看到所有可用的屬性都以026開頭。這顯示所有這些供應商特定的屬性都屬於IETF RADIUS 26標準。預設情況下，這些屬性不會顯示在使用者或組設定中。要在組設定中顯示，請在網路配置中建立使用RADIUS進行身份驗證的AAA客戶端（本例中為VPN 3000集中器）。然後，從介面配置檢查需要顯示在User Setup（使用者設定）、Group Setup（組設定）或兩者中的屬性。如需可用屬性及其用法的詳細資訊，請參閱[RADIUS屬性](#)。按一下「**Submit**」。

2. 完成這些步驟，將組新增到Cisco Secure ACS for Windows配置中。選擇**Group Setup**，然後選擇其中一個模板組，例如Group 1，然後按一下**Rename Group**。

Group Setup




將名稱更改為適合您組織的名稱。例如ipsecgroup。由於使用者被新增到這些組中，因此使組名反映該組的實際用途。如果所有使用者都加入同一個組，則可以將其稱為VPN使用者組。按一下**Edit Settings**以編輯新重新命名組中的引數。

Group Setup


Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed
 Dialup client specifies callback number
 Use Windows Database callback settings (where possible)

按一下

Cisco VPN 3000 RADIUS並配置這些建議的屬性。這允許分配給此組的使用者繼承Cisco VPN 3000 RADIUS屬性，這允許您在Cisco Secure ACS for Windows中集中所有使用者的策略。

Group Setup

Jump To

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

注意：在技

術上，只要隧道組是在[VPN 3000系列集中器配置步驟3](#)中設定的，並且VPN集中器中的基本組不會從原始預設設定更改，則不需要配置VPN 3000 RADIUS屬性。**建議的VPN 3000屬性：**
Primary-DNS — 輸入主DNS伺服器的IP地址。**Secondary-DNS** — 輸入輔助DNS伺服器的IP地址。**Primary-WINS** — 輸入主WINS伺服器的IP地址。**Secondary-WINS** — 輸入輔助WINS伺服器的IP地址。**Tunneling-Protocols** — 選擇IPsec。這僅允許IPsec客戶端連線。不允許PPTP或L2TP。**IPsec-Sec-Association** — 輸入ESP-3DES-MD5。這可確保所有IPsec客戶端都以可用的最高加密進行連線。**IPsec-Allow-Password-Store** — 選擇Disallow，這樣不允許使用者在VPN客戶端中儲存其密碼。**IPsec-Banner** — 輸入連線時向使用者顯示的歡迎消息標語。例如，「歡迎使用MyCompany員工VPN接入！」**IPsec-Default Domain** — 輸入您公司的域名。例如，「mycompany.com」。不需要此屬性集。但是，如果您不確定VPN 3000集中器的基本組屬性是否已更改，Cisco建議您配置以下屬性：**Simultaneous-Logins** — 輸入允許使用者使用相同使用者名稱同時登入的次數。建議值為1或2。**SEP-Card-Assignment** — 選擇Any-SEP。**IPsec-Mode-Config** — 選擇ON。**IPsec over UDP** — 選擇OFF，除非您希望此組中的使用者使用IPsec over UDP協定進行連線。如果選擇ON，則VPN客戶端仍然能夠本地禁用IPsec over UDP並正常連線。**IPsec over UDP埠** — 選擇範圍從4001到49151的UDP埠號。

僅當IPsec over UDP為ON時才使用此選項。下一組屬性要求先在VPN集中器上設定一些設定，然後才能使用。僅建議高級使用者執行此操作。**Access-Hours** — 這要求您在VPN 3000集中器上的**Configuration > Policy Management**下設定一系列訪問時數。而是使用適用於Windows的Cisco Secure ACS中可用的訪問小時數來管理此屬性。**IPsec-Split-Tunnel-List** — 這要求您在VPN集中器上的**Configuration > Policy Management > Traffic Management**下設定**網路清單**。這是傳送到使用者端的網路清單，告知使用者端只對清單中的網路加密資料。在Group setup中選擇**IP assignment**，然後選中**Assigned from AAA server Pool**，以便在VPN客戶端使用者通過身份驗證後為其分配IP地址。

Group Setup

Jump To IP Address Assignment

IP Assignment

- No IP address assignment
- Assigned by dialup client
- Assigned from AAA Client pool
- Assigned from AAA server pool

Available Pools

Selected Pools

pool1

->

<-


Up Down

選擇System

configuration > IP pools以便為VPN客戶端使用者建立IP池，然後按一下Submit。

System Configuration

Edit


New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

Submit

Cancel

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

選擇Submit >

Restart以儲存配置並啟用新組。重複這些步驟以新增更多組。

3. 在Cisco Secure ACS for Windows上配置使用者。選擇User Setup，輸入使用者名稱，然後按

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

一下Add/Edit。

用者設定部分下配置以下引數


:

在使

User Setup


User: ipsecuser1 (New User)

Account Disabled


Supplementary User Info 

Real Name

Description

User Setup 

Password Authentication:



CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password


Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:



Password Authentication — 選擇ACS Internal Database。Cisco Secure PAP - Password — 輸入使用者的密碼。Cisco Secure PAP — 確認密碼 — 重新輸入新使用者的密碼。使用者分配到的組 — 選擇在上一步中建立的組的名稱。按一下「Submit」以儲存和啟用使用者設定。重複這些步驟以新增其他使用者。

[為VPN客戶端使用者分配靜態IP地址](#)

請完成以下步驟：

1. 建立新的VPN組IPSECGRP。
2. 建立想要接收靜態IP的使用者，然後選擇IPSECGRP。選擇Assign static IP address，使用在Client IP Address Assignment下分配的靜態IP地址。

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm
Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

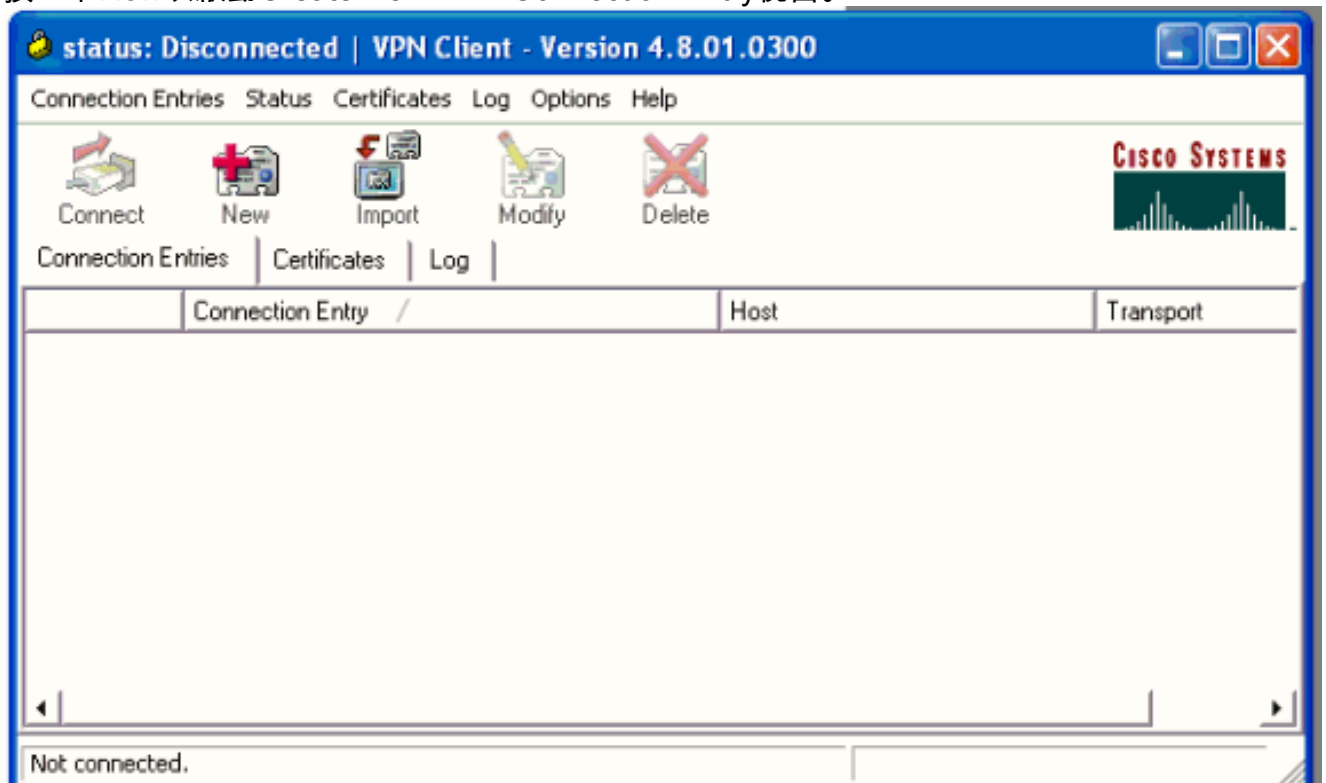
Submit

Delete

Cancel

本節介紹VPN客戶端配置。

1. 選擇**Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 按一下**New**以啟動Create New VPN Connection Entry視窗。



3. 出現提示時，為您的條目指定名稱。如果需要，也可以輸入說明。在Host列中指定VPN 3000 Concentrator公共介面IP地址，然後選擇**Group Authentication**。然後提供組名稱和密碼。按一下**Save**以完成新的VPN連線條目。

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [Dropdown]

Send CA Certificate Chain

Erase User Password | Save | Cancel

注意：請確

保將VPN客戶端配置為使用在Cisco VPN 3000系列集中器中配置的相同組名和密碼。

新增記帳

驗證運作後，您可以新增計量。

1. 在VPN 3000上，選擇**Configuration > System > Servers > Accounting Servers**，然後新增**Cisco Secure ACS for Windows**伺服器。
2. 選擇**Configuration > User Management > Groups**，突出顯示一個組並按一下**Modify Acct**時，可以將各個記帳伺服器新增到每個組。**伺服器**。然後輸入記帳伺服器的IP地址及伺服器金鑰。

Configure and add a RADIUS user accounting server.

Accounting Server	<input type="text" value="172.16.124.5"/>	Enter IP address or hostname.
Server Port	<input type="text" value="1646"/>	Enter the server UDP port number.
Timeout	<input type="text" value="1"/>	Enter the timeout for this server (se
Retries	<input type="text" value="3"/>	Enter the number of retries for this
Server Secret	<input type="password" value="*****"/>	Enter the RADIUS server secret.
Verify	<input type="password" value="*****"/>	Re-enter the server secret.

在Cisco Secure ACS for Windows中，記賬記錄如下輸出所示

Select

RADIUS Accounting active.csv

Regular Expression: Start Date & Time: End Date & Time: Rows per Page:

Filtering is not applied.

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets
10/27/2006	18:38:20	ipseuser1	ipsegroup	192.168.1.2	Start	E8700001	..	Framed	PPP
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off

驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

驗證VPN集中器

在VPN 3000 Concentrator端，選擇Administration > Administering Sessions以驗證遠端VPN通道的建立。

Remote Access Sessions

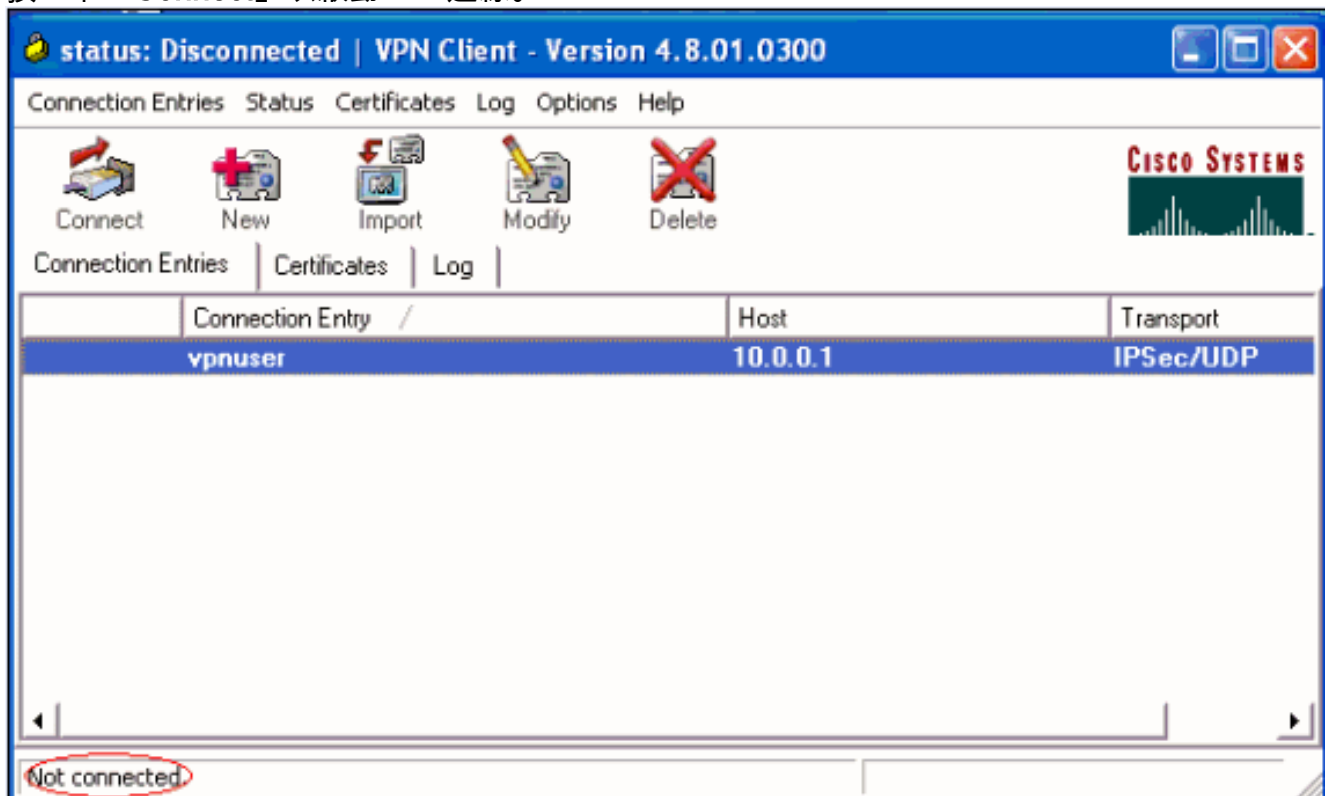
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

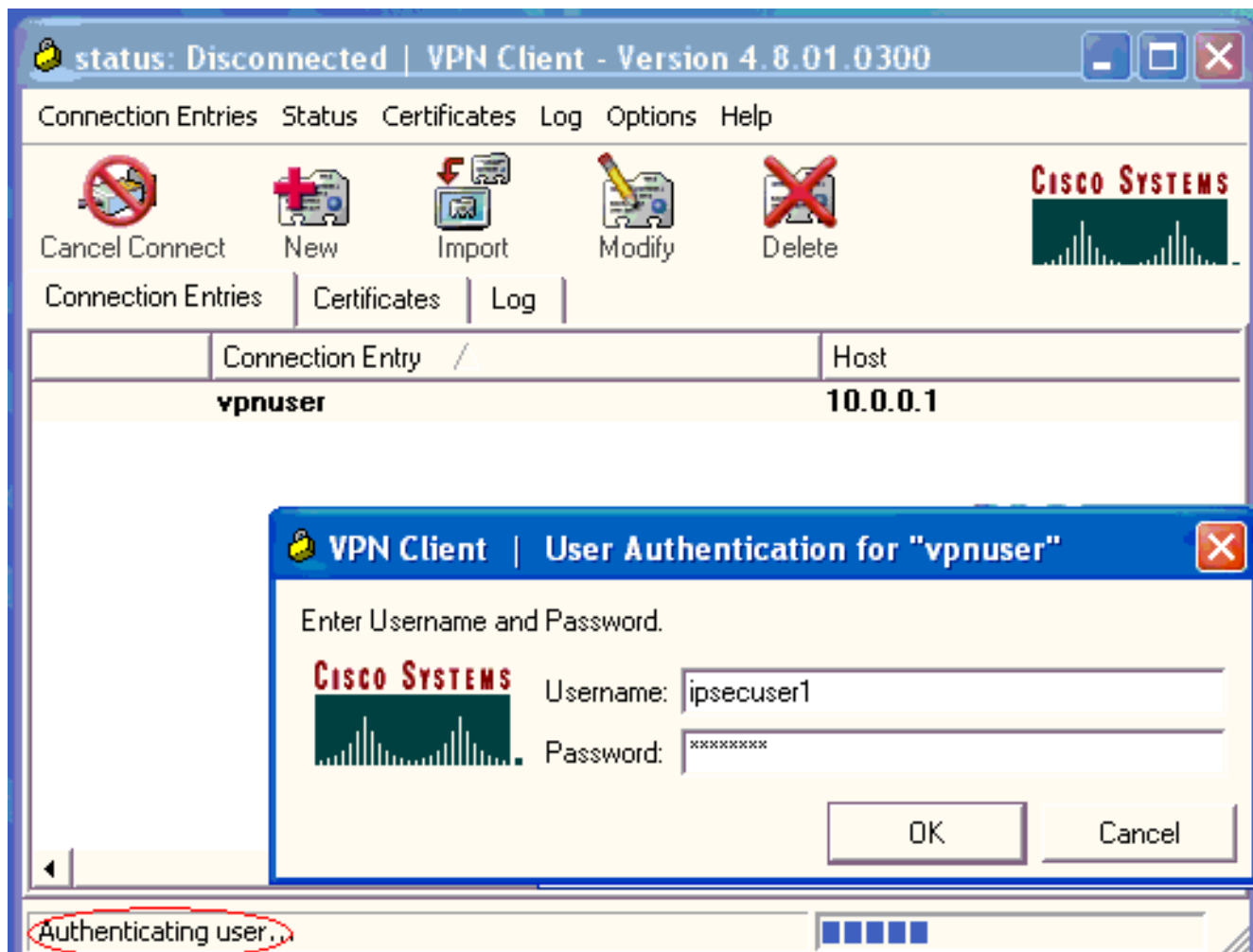
驗證VPN客戶端

完成以下步驟以驗證VPN客戶端。

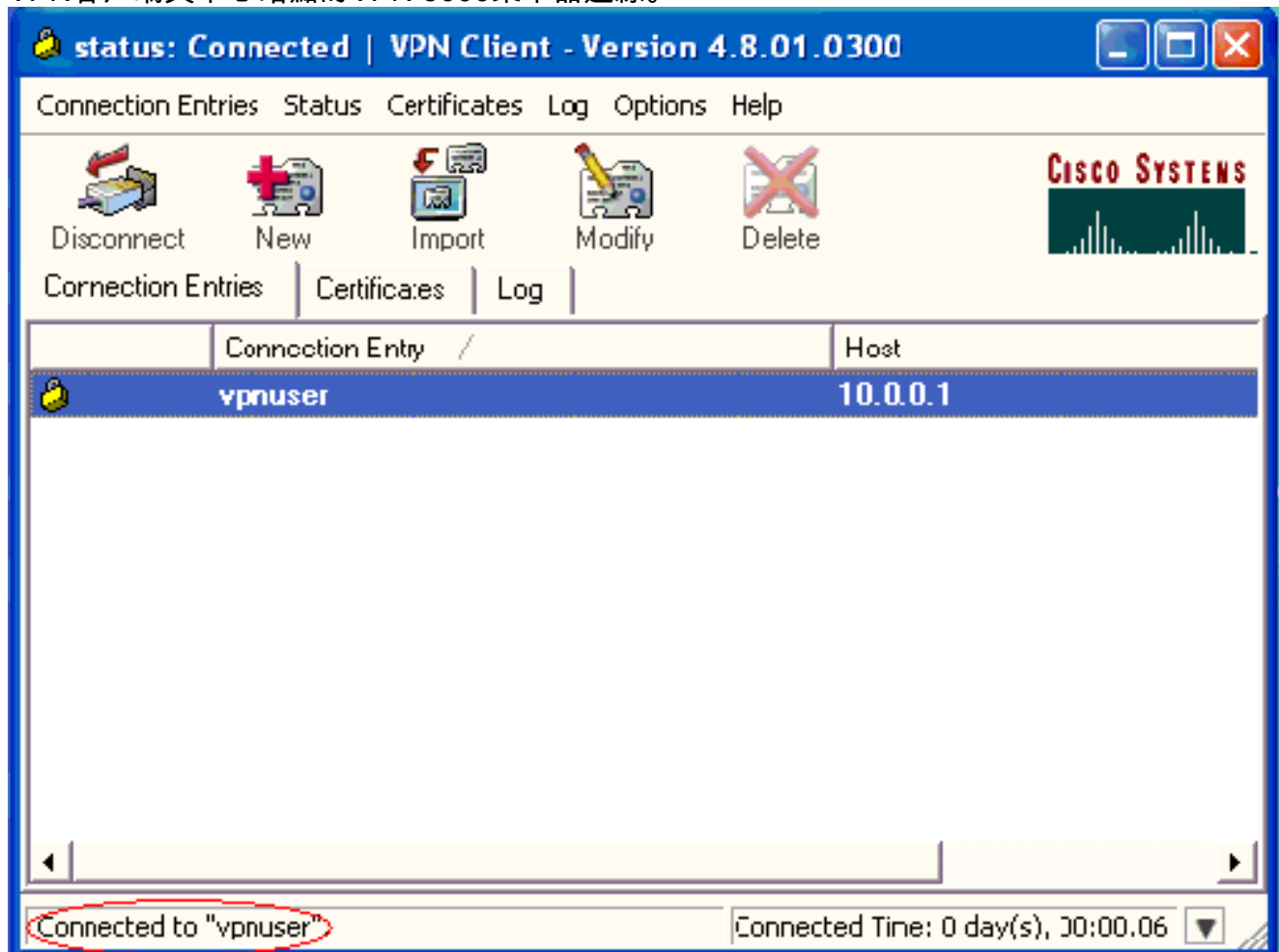
1. 按一下「Connect」以啟動VPN連線。



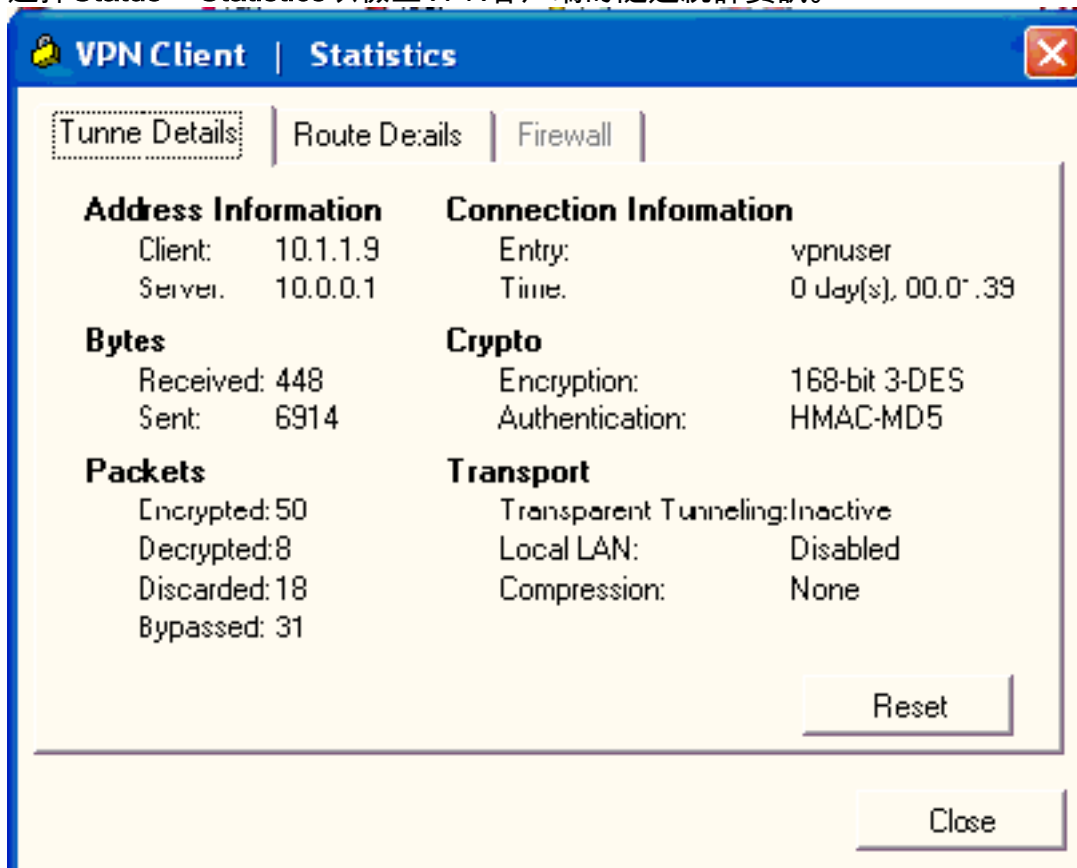
2. 出現此視窗以進行使用者身份驗證。輸入有效的使用者名稱和密碼以建立VPN連線。



3. VPN客戶端與中心站點的VPN 3000集中器連線。



4. 選擇 **Status > Statistics** 以檢查VPN客戶端的隧道統計資訊。



疑難排解

完成以下步驟即可對組態進行疑難排解。

1. 選擇 **Configuration > System > Servers > Authentication**，然後完成以下步驟，以測試RADIUS伺服器 and VPN 3000集中器之間的連線。選擇伺服器，然後按一下**測試**。

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or

Authentication Servers	Actions
<div style="border: 1px solid gray; background-color: #e6f2ff; padding: 2px;">172.16.124.5 (Radius/User Authentication)</div> Internal (Internal)	<div style="border: 1px solid gray; width: 100%; height: 20px; margin-bottom: 2px; background-color: #e6f2ff; text-align: center;">Add</div> <div style="border: 1px solid gray; width: 100%; height: 20px; margin-bottom: 2px; background-color: #e6f2ff; text-align: center;">Modify</div> <div style="border: 1px solid gray; width: 100%; height: 20px; margin-bottom: 2px; background-color: #e6f2ff; text-align: center;">Delete</div> <div style="border: 1px solid gray; width: 100%; height: 20px; margin-bottom: 2px; background-color: #e6f2ff; text-align: center;">Move Up</div> <div style="border: 1px solid gray; width: 100%; height: 20px; margin-bottom: 2px; background-color: #e6f2ff; text-align: center;">Move Down</div> <div style="border: 1px solid gray; width: 100%; height: 20px; background-color: #e6f2ff; text-align: center;">Test</div>

輸入RADIUS使用者名稱和密碼，然後按一下OK。

Enter a username and password with which to test. **Please wait for the operation**

Username

Password

Success

Authentication Successful

身份驗證成功。

2. 如果失敗，則可能是配置問題或IP連線問題。檢查ACS伺服器上的失敗嘗試日誌中是否存在與失敗相關的消息。如果此日誌中未顯示消息，則可能存在IP連線問題。RADIUS要求無法到達RADIUS伺服器。驗證應用到適當VPN 3000集中器介面的過濾器允許RADIUS(1645)資料包傳入和傳出。如果測試身份驗證成功，但登入VPN 3000集中器仍失敗，請通過控制檯埠檢查可過濾事件日誌。如果連線不起作用，則可以在選擇**Configuration > System > Events > Classes > Modify(Severity to Log=1-9, Severity to Console=1-3)**時，將AUTH、IKE和IPsec事

件類新增到VPN集中器。AUTHDBG、AUTHDECODE、IKEDBG、IKEDECODE、IPSECDBG和IPSECDECODE也可用，但可提供過多的資訊。如果有關從RADIUS伺服器向下傳遞的屬性的詳細資訊，則AUTHDECODE、IKEDECODE和IPSECDECODE在Log=1-13級別的Severity級別提供此資訊。

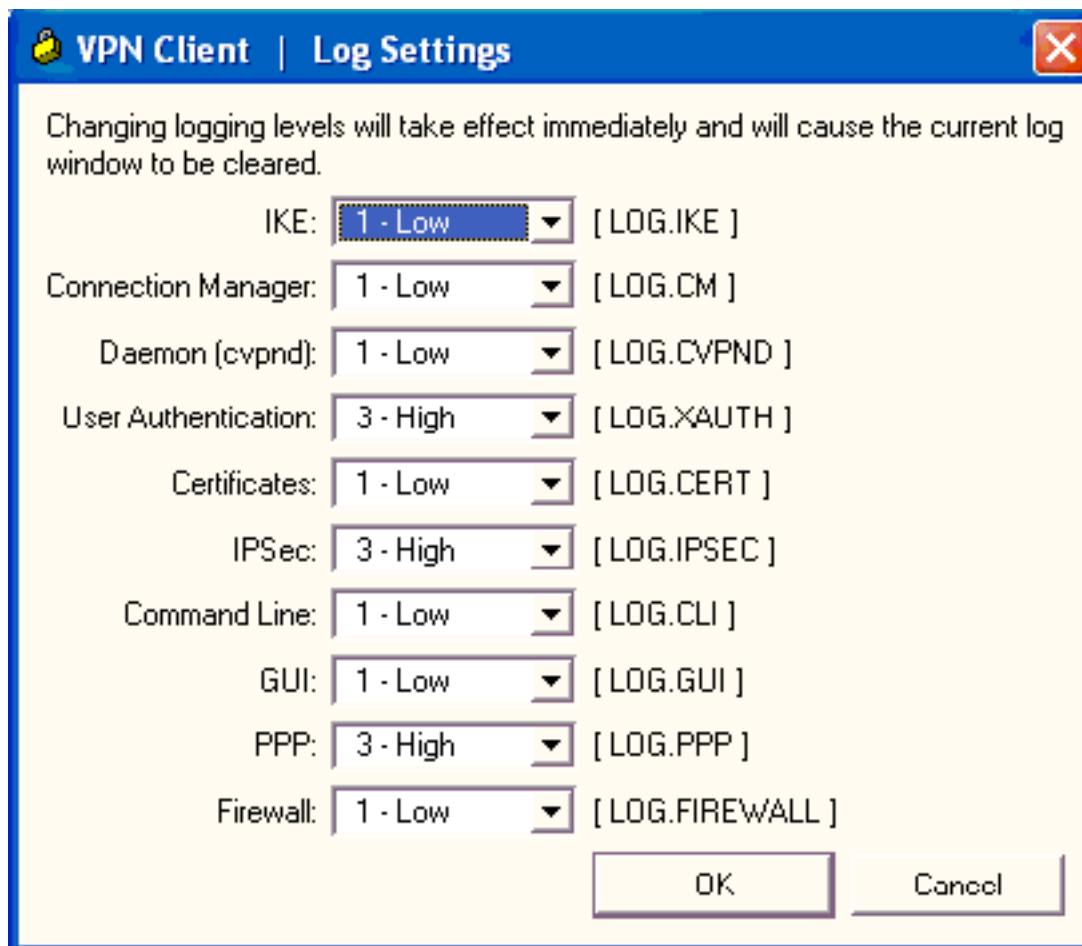
3. 從Monitoring > Event Log中檢索事件日誌。



[VPN Client 4.8 for Windows故障排除](#)

完成以下步驟以對VPN Client 4.8 for Windows進行故障排除。

1. 選擇Log > Log settings以啟用VPN客戶端中的日誌級別。



2. 選擇Log > Log Window以檢視VPN客戶端中的日誌條目。

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

相關資訊

- [Cisco VPN 3000系列集中器支援頁面](#)
- [Cisco VPN使用者端支援頁面](#)
- [IPSec 協商/IKE 通訊協定](#)
- [Cisco Secure ACS for Windows支援頁](#)
- [在RADIUS伺服器上設定動態過濾器](#)
- [技術支援與文件 - Cisco Systems](#)