使用Microsoft RADIUS配置Cisco VPN 3000集中器

目錄

簡介

Microsoft Internet Authentication Server(IAS)和Microsoft Commercial Internet System(MCIS 2.0)目前可用。Microsoft RADIUS伺服器很方便，因為它使用主域控制器上的Active Directory作為其使用者資料庫。不再需要維護單獨的資料庫。它還支援點對點隧道協定(PPTP)VPN連線的40位和128位加密。請參閱Microsoft清單：配置撥號的IAS和VPN訪問文檔 ，瞭解更多資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

在Windows 2000和Windows 2003上安裝並配置RADIUS伺服器

安裝RADIUS伺服器

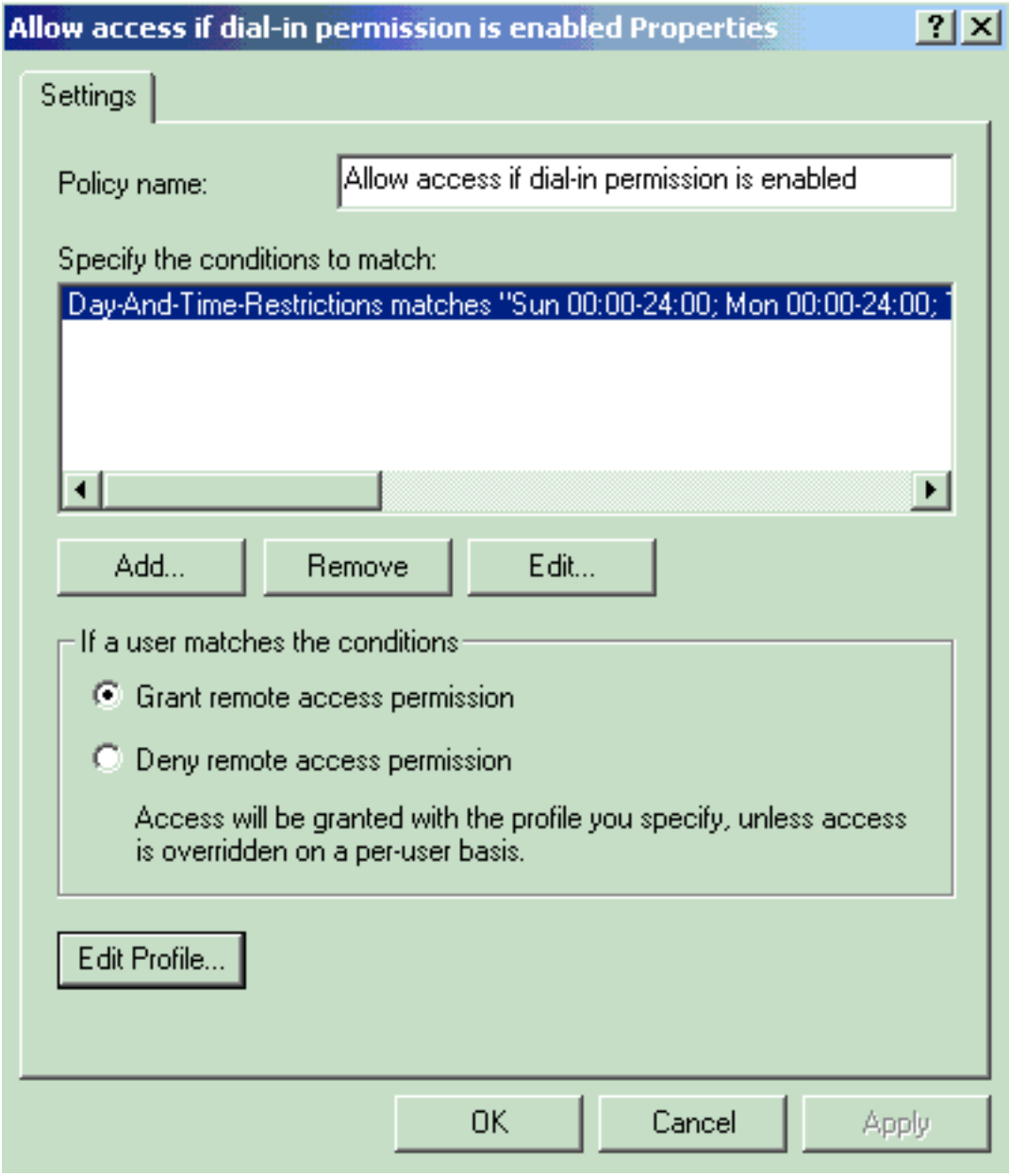
如果尚未安裝RADIUS伺服器(IAS)，請執行以下步驟，以進行安裝。如果您已安裝RADIUS伺服器，請繼續執行組態步驟。

1. 插入Windows Server光碟並啟動安裝程式。
2. 按一下**Install Add-On Components**，然後按一下**Add/Remove Windows Components**。
3. 在元件中，按一下**Networking Services**（但不選中或清除覈取方塊），然後按一下**Details**。
4. 選中**Internet Authentication Service**，然後按一下**OK**。
5. 按「**Next**」（下一步）。

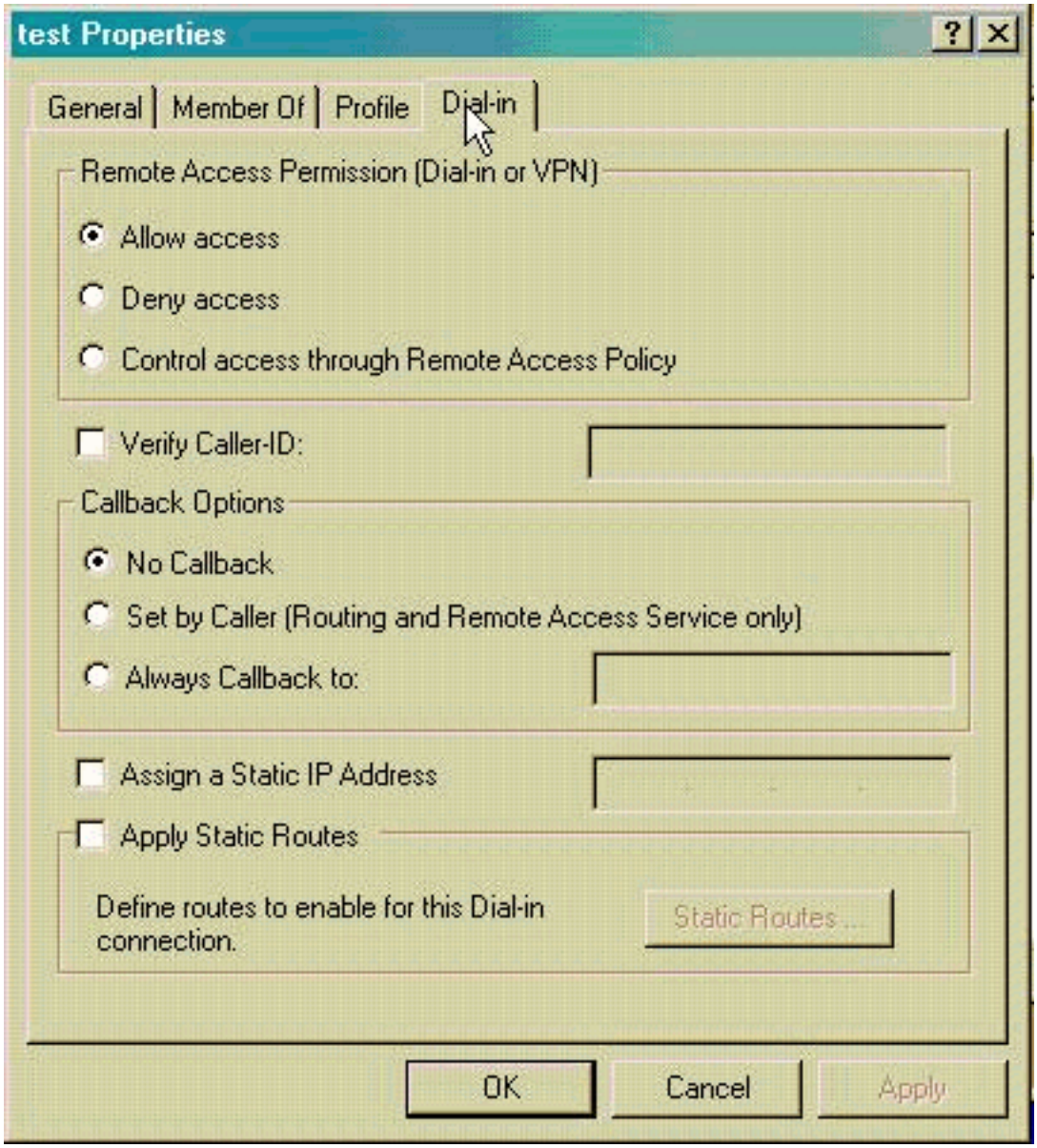
使用IAS配置Microsoft Windows 2000 Server

完成以下步驟即可設定RADIUS伺服器(IAS)和啟動服務，以便在VPN集中器上驗證使用者身分。

1. 選擇**開始>程式>管理工具> Internet身份驗證服務**。
2. 按一下右鍵**Internet Authentication Service**，然後從出現的子選單中按一下**Properties**。
3. 前往RADIUS索引標籤檢查連線埠的設定。如果您的RADIUS驗證和RADIUS記帳使用者資料包協定(UDP)埠與驗證和記帳中提供的預設值（1812和1645,1813和1646）不同，請鍵入您的埠設定。完成後按一下**OK**。**注意：**請勿更改預設埠。使用逗號將多個埠設定用於身份驗證或記帳請求，從而分隔埠。
4. 按一下右鍵**Clients**並選擇**New Client**，以將VPN集中器作為身份驗證、授權和記帳(AAA)客戶端新增到RADIUS伺服器(IAS)。**注意：**如果在兩個Cisco VPN 3000集中器之間配置了冗餘，則還必須將備份的Cisco VPN 3000集中器作為RADIUS客戶端新增到RADIUS伺服器。
5. 輸入友好名稱並選擇為**Protocol Radius**。
6. 在下一個視窗中使用IP地址或DNS名稱定義VPN集中器。
7. 從客戶端 — 供應商捲軸中選擇**Cisco**。
8. 輸入共用金鑰。**注意：**您必須記住*您使*用的確切密碼。您需要此資訊才能配置VPN集中器。
9. 按一下「**Finish**」（結束）。
10. 按兩下**Remote Access Policies**，然後按兩下顯示在視窗右側的策略。**注意：**安裝IAS後，遠端訪問策略應該已經存在。在Windows 2000中，根據使用者帳戶的撥入屬性和遠端訪問策略授予授權。遠端訪問策略是一組條件和連線設定，使網路管理員在授權連線嘗試時更具靈活性。Windows 2000路由和遠端訪問服務和Windows 2000 IAS都使用遠端訪問策略來確定是接受還是拒絕連線嘗試。在這兩種情況下，遠端訪問策略都儲存在本地。有關如何處理連線嘗試的詳細資訊，請參閱Windows 2000 IAS文檔。



11. 選擇**授予遠端訪問許可權**，然後按一下**編輯配置檔案**以配置撥入屬性。
12. 在Authentication頁籤上選擇要用於身份驗證的協定。選中**Microsoft Encrypted Authentication version 2**並取消選中所有其他身份驗證協定。**注意：**此撥入配置檔案中的設定必須與VPN 3000集中器配置和撥入客戶端中的設定匹配。在此示例中，使用不採用PPTP加密的MS-CHAPv2身份驗證。
13. 在Encryption頁籤上選中**No Encryption**。
14. 按一下「**OK**」以關閉「撥入」設定檔，然後按一下「**OK**」以關閉遠端存取原則視窗。
15. 按一下右鍵**Internet身份驗證服務**，然後按一下控制檯樹中的**啟動服務**。**注意：**您也可以使用此功能停止服務。
16. 完成這些步驟，修改使用者以允許連線。選擇**Console > Add/Remove Snap-in**。按一下**Add**並選擇**Local Users and Groups管理單元**。按一下「**Add**」。確保選擇**Local Computer**按一下「**Finish**」，然後「**OK**」。
17. 展開**Local User and Groups**，然後按一下左窗格中的**Users**資料夾。在右窗格中，按兩下要允許訪問的使用者（VPN使用者）。
18. 轉到「撥入」頁籤，然後在「遠端訪問許可權（撥入或VPN）」下選擇**Allow Access**。



19. 按一下「**Apply**」和「**OK**」以完成操作。如果需要，可以關閉Console Management視窗並儲存會話。您修改的使用者現在可以通過VPN客戶端訪問VPN集中器。請記住，IAS伺服器僅對使用者資訊進行身份驗證。VPN集中器仍然執行組身份驗證。

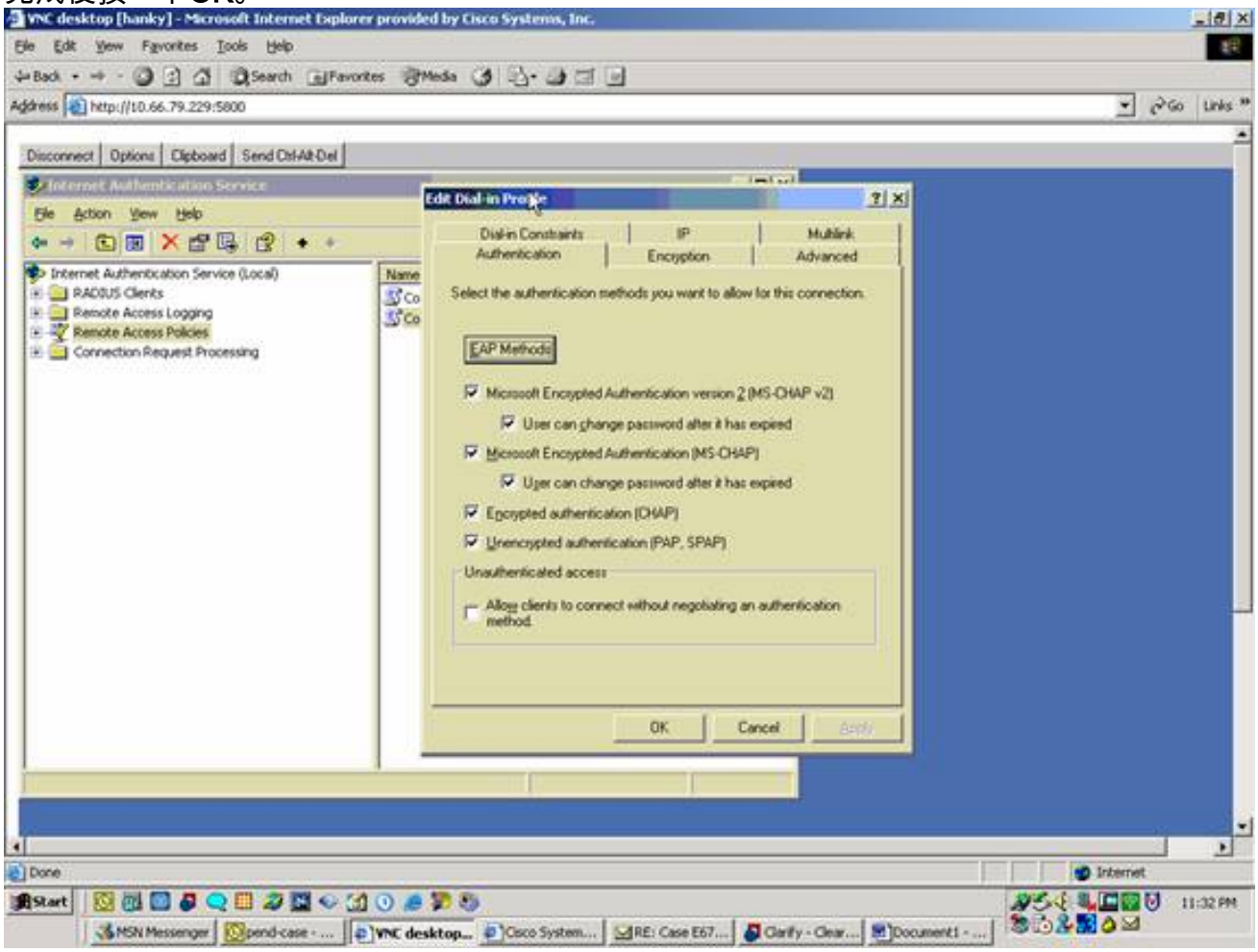
使用IAS配置Microsoft Windows 2003 Server

完成以下步驟，以便使用IAS配置Microsoft Windows 2003伺服器。

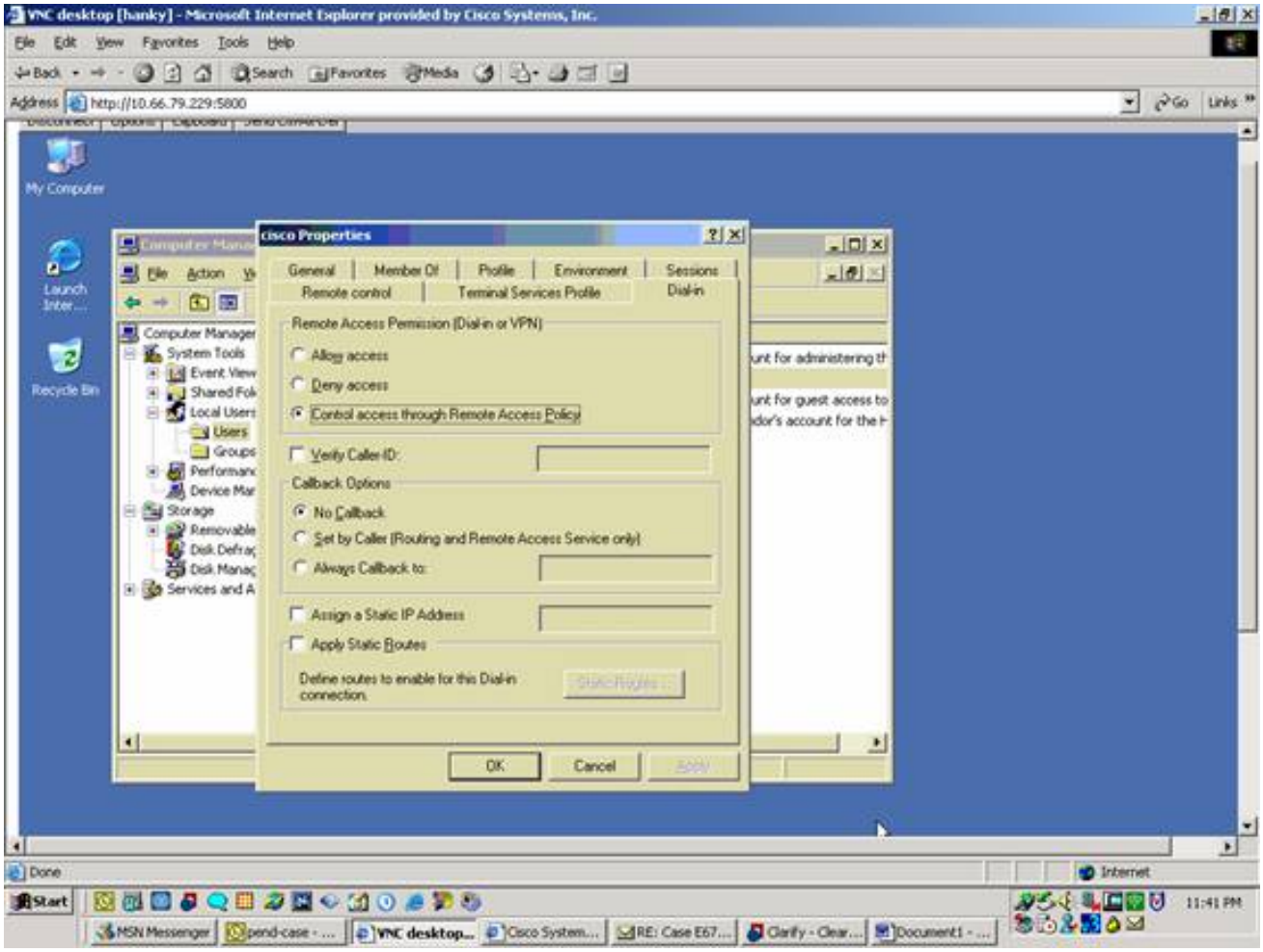
注意：這些步驟假設IAS已安裝在本地電腦上。如果不是，請通過**控制面板>新增/刪除程式**新增此項。

1. 選擇**Administrative Tools > Internet Authentication Service**，然後按一下右鍵**RADIUS Client**以新增新的RADIUS客戶端。鍵入客戶端資訊後，按一下**OK**。
2. 輸入友好名稱。
3. 在下一個視窗中使用IP地址或DNS名稱定義VPN集中器。
4. 從客戶端 — 供應商捲軸中選擇**Cisco**。
5. 輸入共用金鑰。**注意：***您必須記住您使用的確切密碼。您需要此資訊才能配置VPN集中器。*
6. 按一下「**OK**」以完成。
7. 轉到**遠端訪問策略**，按一下右鍵**連線到其他訪問伺服器**，然後選擇**屬性**。
8. 選擇**授予遠端訪問許可權**，然後按一下**編輯配置檔案**以配置撥入屬性。

9. 在Authentication頁籤上選擇要用於身份驗證的協定。選中**Microsoft Encrypted Authentication version 2**並取消選中所有其他身份驗證協定。**注意：**此撥入配置檔案中的設定必須與VPN 3000集中器配置和撥入客戶端中的設定匹配。在此示例中，使用不採用PPTP加密的MS-CHAPv2身份驗證。
10. 在Encryption頁籤上選中**No Encryption**。
11. 完成後按一下**OK**。



12. 按一下右鍵**Internet身份驗證服務**，然後按一下控制檯樹中的**啟動服務**。**注意：**您也可以使用此功能來停止服務。
13. 選擇**Administrative Tools > Computer Management > System Tools > Local Users and Groups**，按一下右鍵**Users**，然後選擇**New Users**，以便將使用者新增到本地電腦帳戶中。
14. 使用思科密碼「vpnpassword」新增使用者並檢查此配置檔案資訊。在「General（常規）」頁籤上，確保選中**Password Never Expired**選項，而不是「User Must Change Password（使用者必須更改密碼）」選項。在「撥入」頁籤上，為**允許訪問**（或保留「通過遠端訪問策略控制訪問」的預設設定）選擇選項。完成後按一下**OK**。

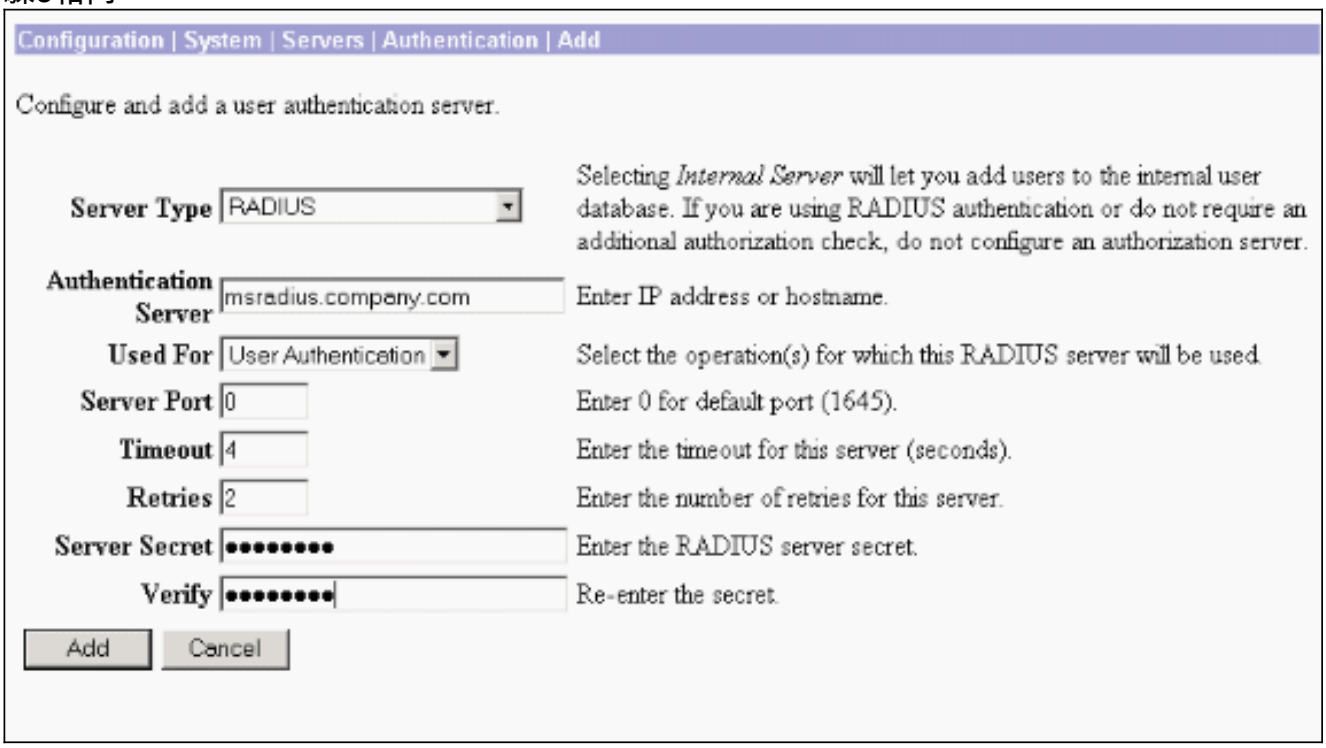


配置用於RADIUS身份驗證的Cisco VPN 3000集中器

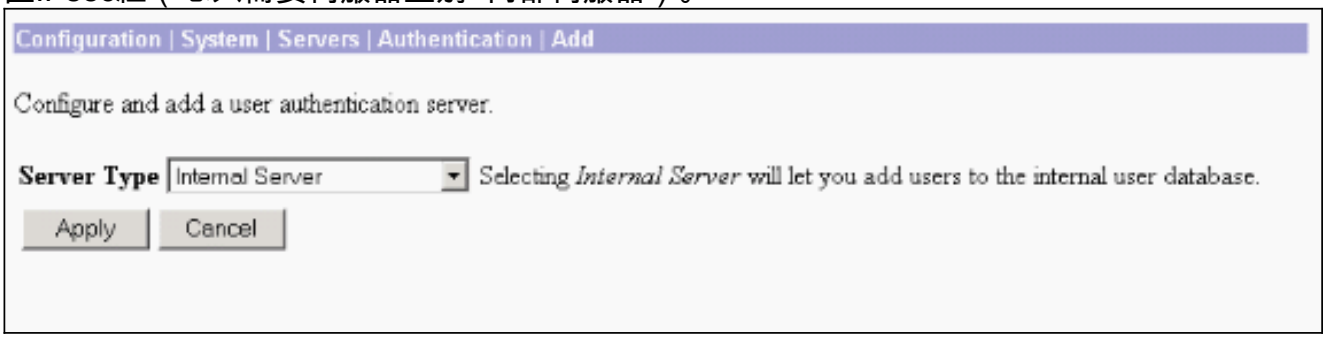
完成以下步驟，配置用於RADIUS身份驗證的Cisco VPN 3000集中器。

1. 使用Web瀏覽器連線到VPN集中器，然後從左側框架選單中選擇**Configuration > System > Servers > Authentication**。

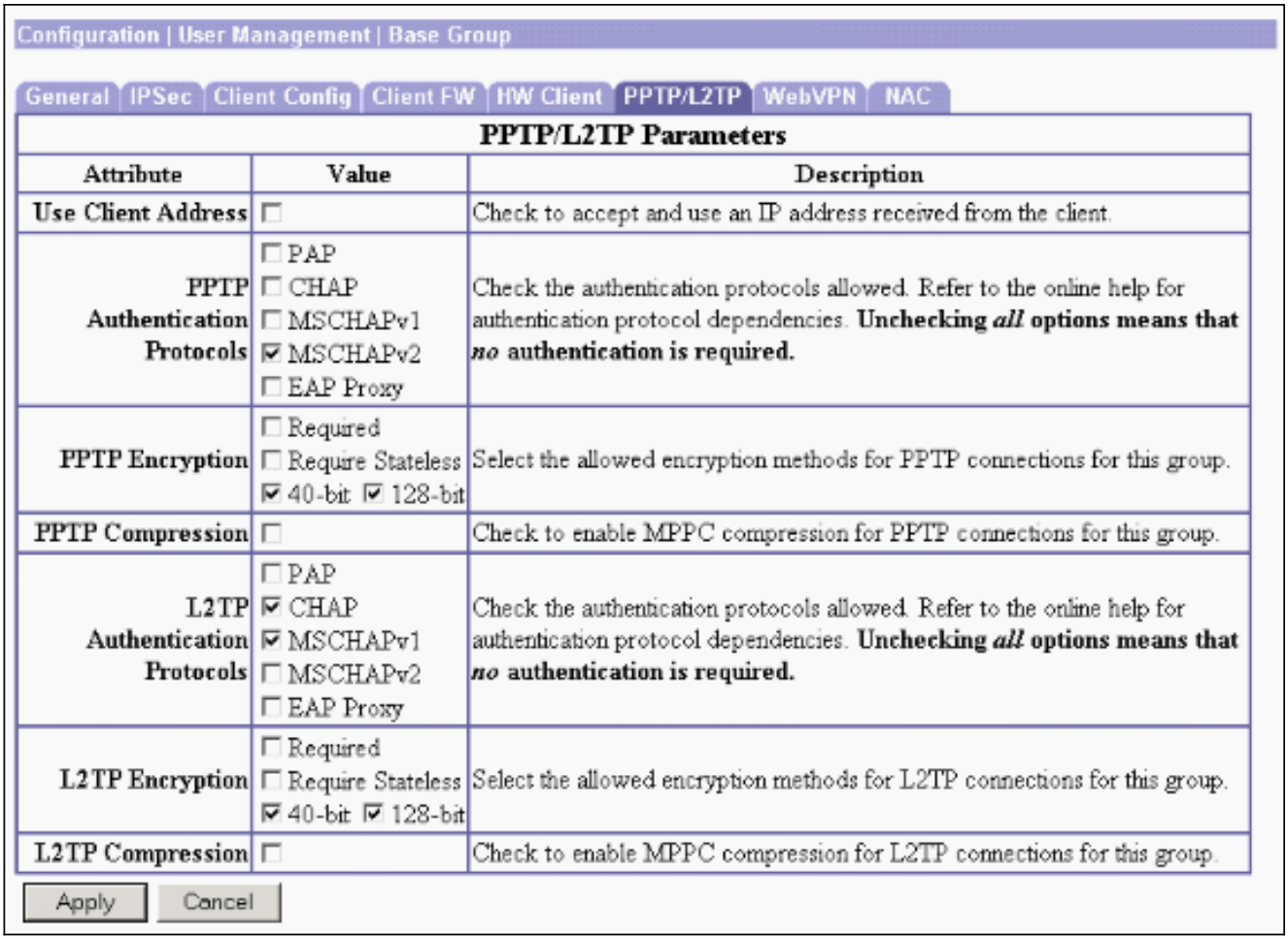
2. 按一下**Add**並配置這些設定。伺服器型別= RADIUS身份驗證伺服器= RADIUS伺服器(IAS)的IP地址或主機名伺服器埠= 0（0=預設=1645）伺服器密碼=與[配置RADIUS伺服器](#)一節中的步驟8相同



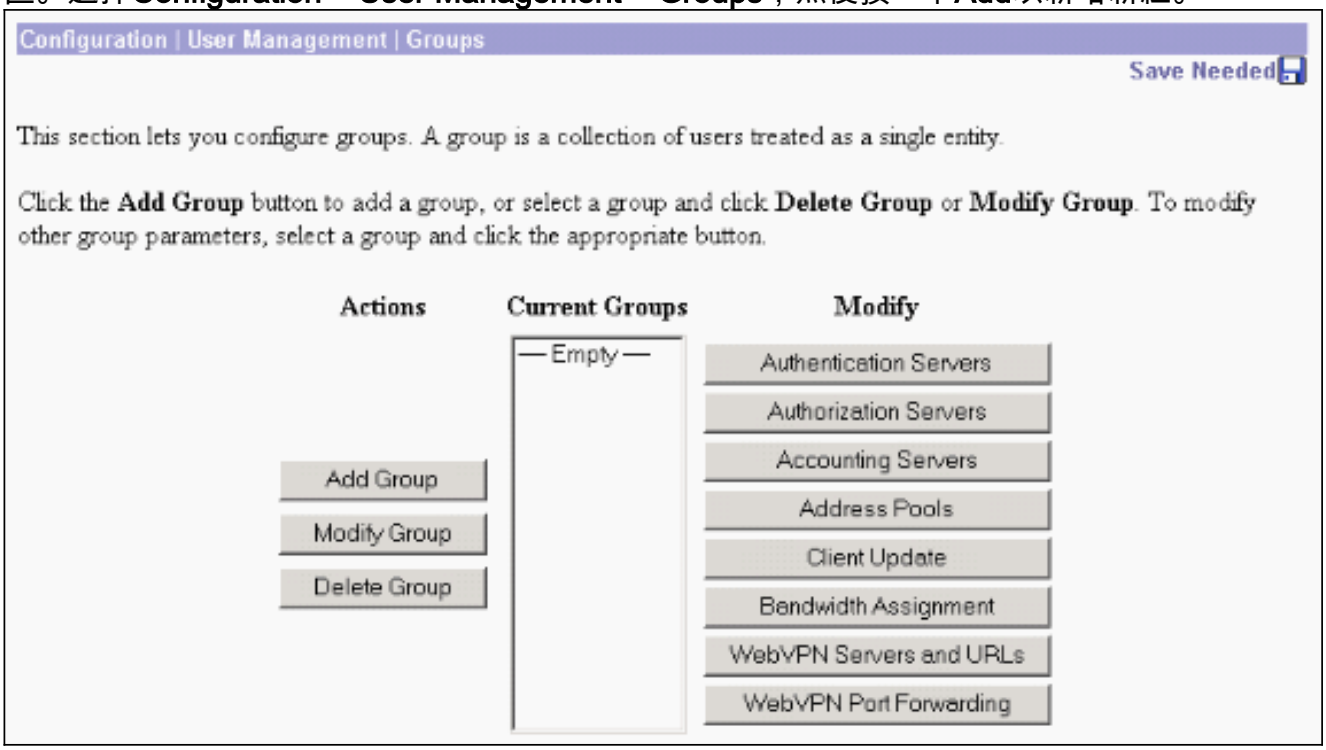
3. 按一下「**Add**」將變更新增到執行組態中。
4. 按一下**Add**，選擇**Internal Server**作為Server Type，然後按一下**Apply**。稍後需要此命令以配置IPsec組（您只需要伺服器型別=內部伺服器）。



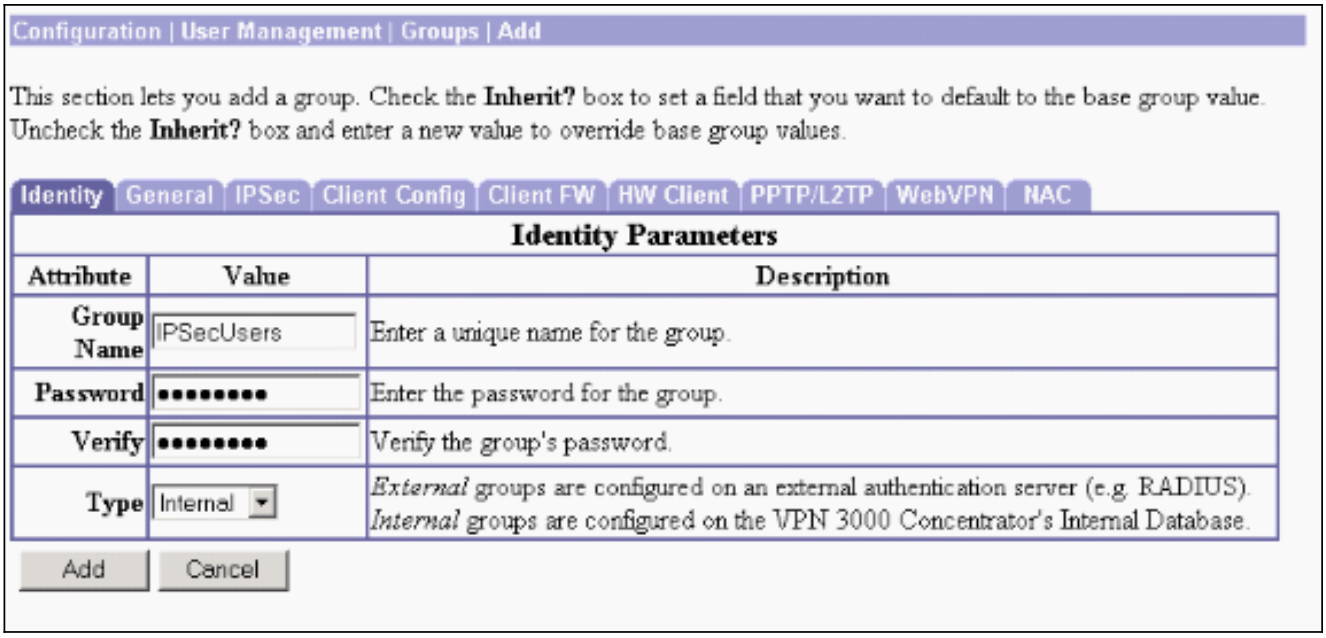
5. 為PPTP使用者或VPN客戶端使用者配置VPN集中器。**PPTP**完成這些步驟，以便為PPTP使用者配置。選擇**Configuration > User Management > Base Group**，然後按一下**PPTP/L2TP**頁籤。選擇**MSCHAPv2**，然後在PPTP Authentication Protocols部分取消選中其他身份驗證協定。



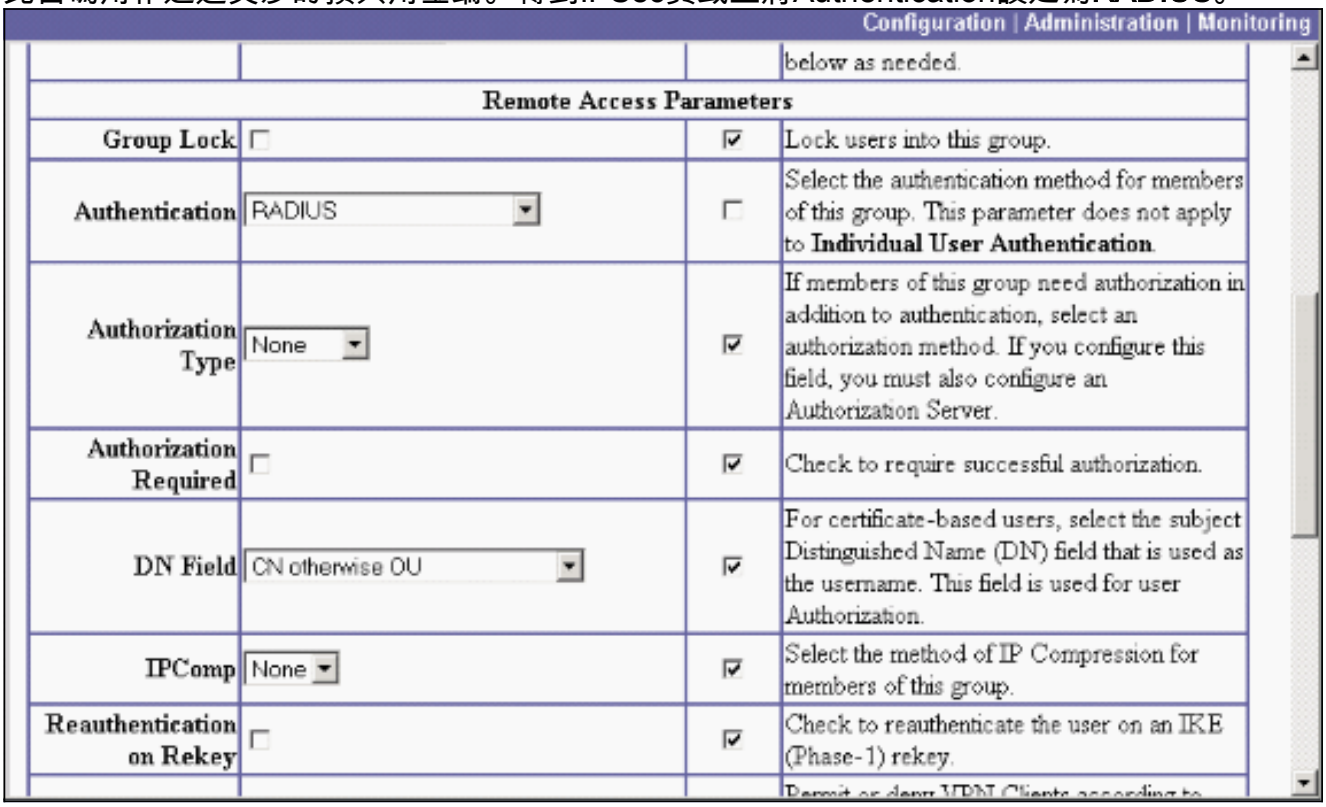
按一下頁面底部的**Apply**，將更改新增到運行配置中。現在，PPTP使用者連線時，會透過RADIUS伺服器(IAS)進行驗證。**VPN使用者端**完成以下步驟，以便為VPN客戶端使用者進行配置。選擇**Configuration > User Management > Groups**，然後按一下**Add**以新增新組。



鍵入組名（例如IPsecUsers）和密碼。



此密碼用作通道交涉的預共用金鑰。轉到IPSec頁籤並將Authentication設定為**RADIUS**。



這允許透過RADIUS驗證伺服器驗證IPsec使用者端。按一下頁面底部的**Add**，將更改新增到運行配置中。現在，當IPsec客戶端連線並使用您配置的組時，它們將由RADIUS伺服器進行身份驗證。

驗證

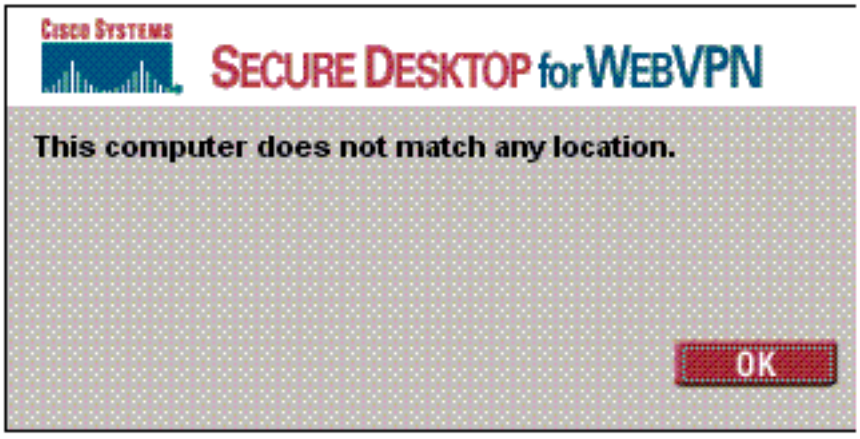
目前沒有適用於此組態的驗證程序。

疑難排解

WebVPN身份驗證失敗

以下各節提供了可用於對配置進行故障排除的資訊。

- **問題**:WebVPN使用者無法對RADIUS伺服器進行身份驗證，但可以通過VPN集中器的本地資料庫成功進行身份驗證。它們會收到錯誤，例如「登入失敗」和此消息。



原因:當使用除集中器內部資料庫之外的任何資料庫時，通常會發生此類問題。WebVPN使用者首次連線到集中器時必須使用預設身份驗證方法時點選基本組。此方法通常設定為集中器的內部資料庫，而不是已配置的RADIUS或其他伺服器。**解決方案**：WebVPN使用者進行身份驗證時，集中器會檢查在**Configuration > System > Servers > Authentication**中定義的伺服器清單，並使用頂部的清單。確保將您希望WebVPN使用者進行身份驗證的伺服器移至此清單頂部。例如，如果RADIUS應是驗證方法，則需要將RADIUS伺服器移動到清單頂端，以將驗證推送到它。**注意：**僅因為WebVPN使用者最初點選了基本組，並不意味著他們只限於基本組。可以在集中器上配置其他WebVPN組，並且使用者可以由填充屬性25(**OU=groupname)的RADIUS伺服器分*配給***。如需詳細說明，請參閱使用RADIUS伺服器將使用者鎖定到VPN 3000集中器群組。

針對Active Directory的使用者身份驗證失敗

在Active Directory伺服器中，在失敗使用者的使用者屬性的「帳戶」頁籤上，可以看到以下覈取方塊：

[x]不需要預先驗證

如果取消選中此覈取方塊，**請選中**，並嘗試再次與此使用者進行身份驗證。

相關資訊

- Cisco VPN 3000系列集中器
- Cisco VPN 3002硬體使用者端
- IPSec 協商/IKE 通訊協定
- RADIUS（遠端驗證撥入使用者服務）支援頁面
- 遠端驗證撥入使用者服務(RADIUS)
- 技術支援與文件 - Cisco Systems