

# 使用Cisco 200/300系列託管交換機和Windows Server 2008的RADIUS配置

## 目標

遠端授權撥入使用者服務(RADIUS)提供強健的使用者驗證方式，以允許存取網路服務。因此，RADIUS伺服器提供集中式存取控制，其中伺服器管理員會決定特定區段是否使用RADIUS進行驗證。本文說明在客戶端/伺服器環境中建立RADIUS的一般步驟，在該環境中，客戶端由Cisco 200/300系列託管交換機代表，伺服器運行的是啟用RADIUS的Windows Server 2008。

## 適用裝置

- Cisco 200/300系列託管交換器

## 逐步程序

配置分為兩部分。首先必須將交換器設定為RADIUS使用者端，然後必須為RADIUS正確設定伺服器。

## 在交換機上設定RADIUS

步驟 1. 在SG200/300系列配置實用程式中，選擇Security > RADIUS。RADIUS頁面隨即開啟：

## RADIUS

### Use Default Parameters

IP Version:           Version 6   Version 4

- ☀ Retries:                       (Range: 1 - 10, Default: 3)
- ☀ Timeout for Reply:            sec. (Range: 1 - 30, Default: 3)
- ☀ Dead Time:                    min. (Range: 0 - 2000, Default: 0)
- Key String:                      (0/128 ASCII Alphanumeric Characters Used)

Apply

Cancel

### RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Retries	Dead Time	Usage Type
--------------------------	--------	----------	------------	-------------------	---------------------	---------	-----------	------------

0 results found.

Add...

Edit...

Delete

步驟 2.輸入預設RADIUS設定。

- IP版本 — 顯示支援的IP版本。
- Retries — 在此欄位中，輸入發生失敗前傳送到RADIUS伺服器的要求數量。
- 回覆超時 — 在此欄位中輸入時間（以秒為單位），交換機將等待來自RADIUS伺服器的應答，然後再次嘗試查詢。
- Dead Time — 在此欄位中，輸入交換器繞過RADIUS伺服器之前等待的時間（以分鐘為單位）。
- 金鑰字串 — 在此欄位中，輸入用於在交換機和RADIUS伺服器之間進行身份驗證和加密的預設字串。金鑰必須與RADIUS伺服器上設定的金鑰相符。

步驟 3.按一下「Apply」，使用RADIUS設定更新交換器的執行組態。



步驟 4.您需要將RADIUS伺服器新增到交換器。按一下「Add」。Add RADIUS Server頁面在新視窗中開啟：

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type: Global

\* Server IP Address/Name:

\* Priority:  (Range: 0 - 65535)

Key String:  Use Default  
 User Defined  (0/128 ASCII Alphanumeric Characters Used)

\* Timeout for Reply:  Use Default  
 User Defined  sec. (Range: 1 - 30, Default: 3)

\* Authentication Port:  (Range: 0 - 65535, Default: 1812)

\* Retries:  Use Default  
 User Defined  (Range: 1 - 10, Default: 3)

\* Dead Time:  Use Default  
 User Defined  min. (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

步驟 5. 在伺服器的欄位中輸入值。如果要使用預設值，請在所需欄位中選擇Use Default。

- 伺服器定義 — 在此欄位中，可以指定如何通過IP地址或伺服器名稱連線到伺服器。
- IP版本 — 如果伺服器將由IP地址標識，請選擇IPv4或IPv6地址。
- IPv6地址型別 — 此欄位顯示IPv6地址的全域性型別。
- 伺服器IP地址/名稱 — 在此欄位中，輸入RADIUS伺服器的IP地址或域名。
- 優先順序 — 在此欄位中輸入伺服器的優先順序。如果配置了多個伺服器，交換機將根據此優先順序值嘗試連線到每台伺服器。
- 金鑰字串 — 在此欄位中，輸入用於在交換機和RADIUS伺服器之間進行身份驗證和加密的預設字串。金鑰必須與RADIUS伺服器上設定的金鑰相符。
- 回覆超時 — 在此欄位中輸入時間（以秒為單位），交換機將等待來自RADIUS伺服器的應答，然後再次嘗試查詢。
- Authentication Port — 在此欄位中，輸入為身份驗證請求的RADIUS伺服器設定的UDP埠號。
- Retries — 在此欄位中，輸入發生失敗前傳送到RADIUS伺服器的要求數量。
- Dead Time — 在此欄位中，輸入交換器繞過RADIUS伺服器之前等待的時間（以分鐘為單位）。
- 使用型別 — 在此欄位中，輸入RADIUS伺服器的身份驗證型別。有三種選擇：

— 登入 — RADIUS伺服器會對想要管理交換器的使用者進行驗證。

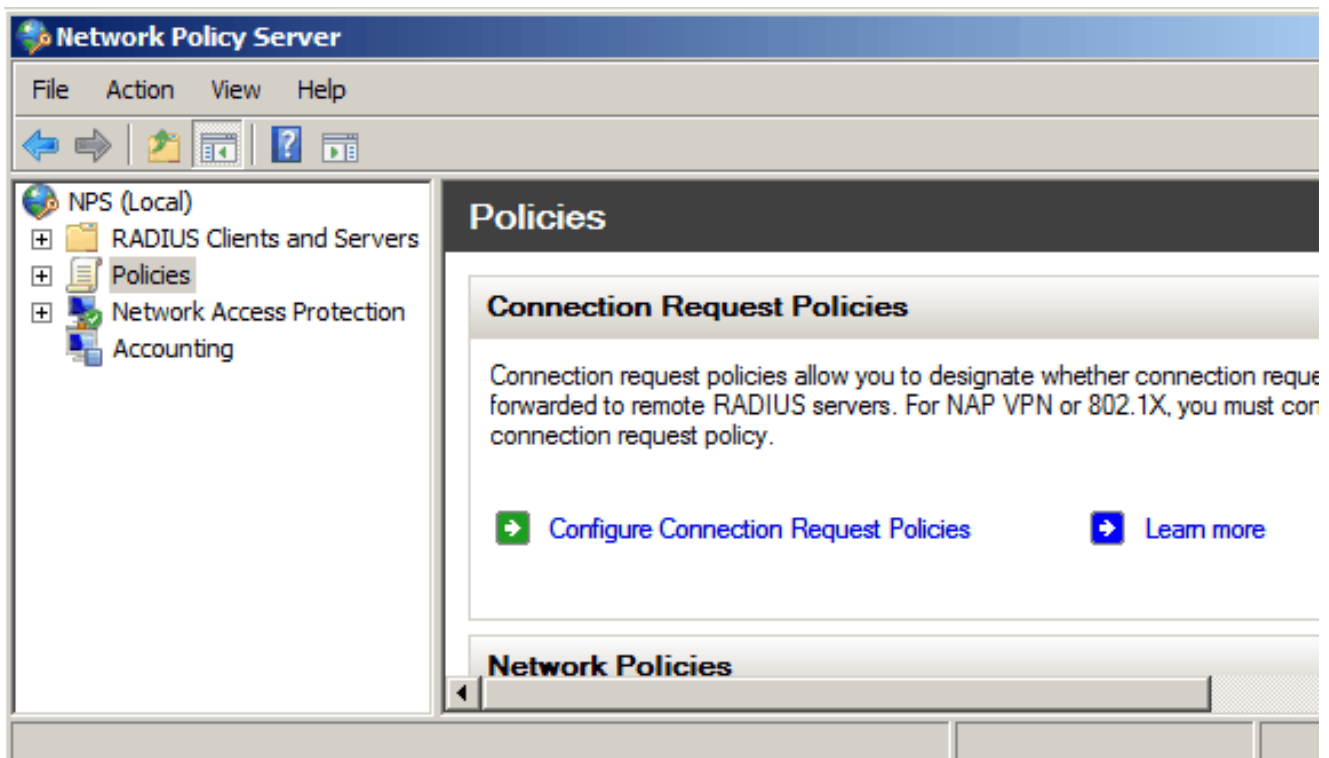
- 802.1X — RADIUS伺服器用於802.1X身份驗證。

— 全部 — RADIUS伺服器用於登入和802.1X驗證。

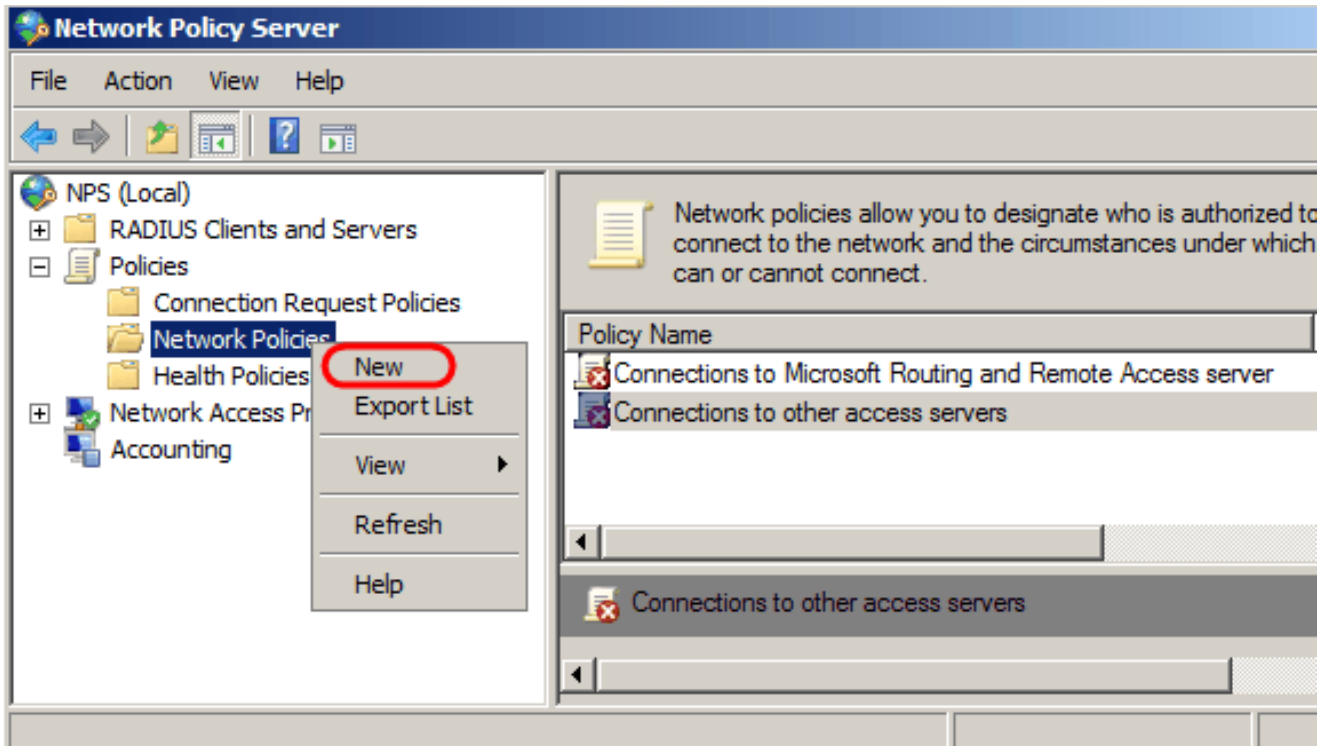
步驟 6.按一下Apply，將伺服器定義新增到交換機的運行配置中。

## 為RADIUS配置Windows Server 2008

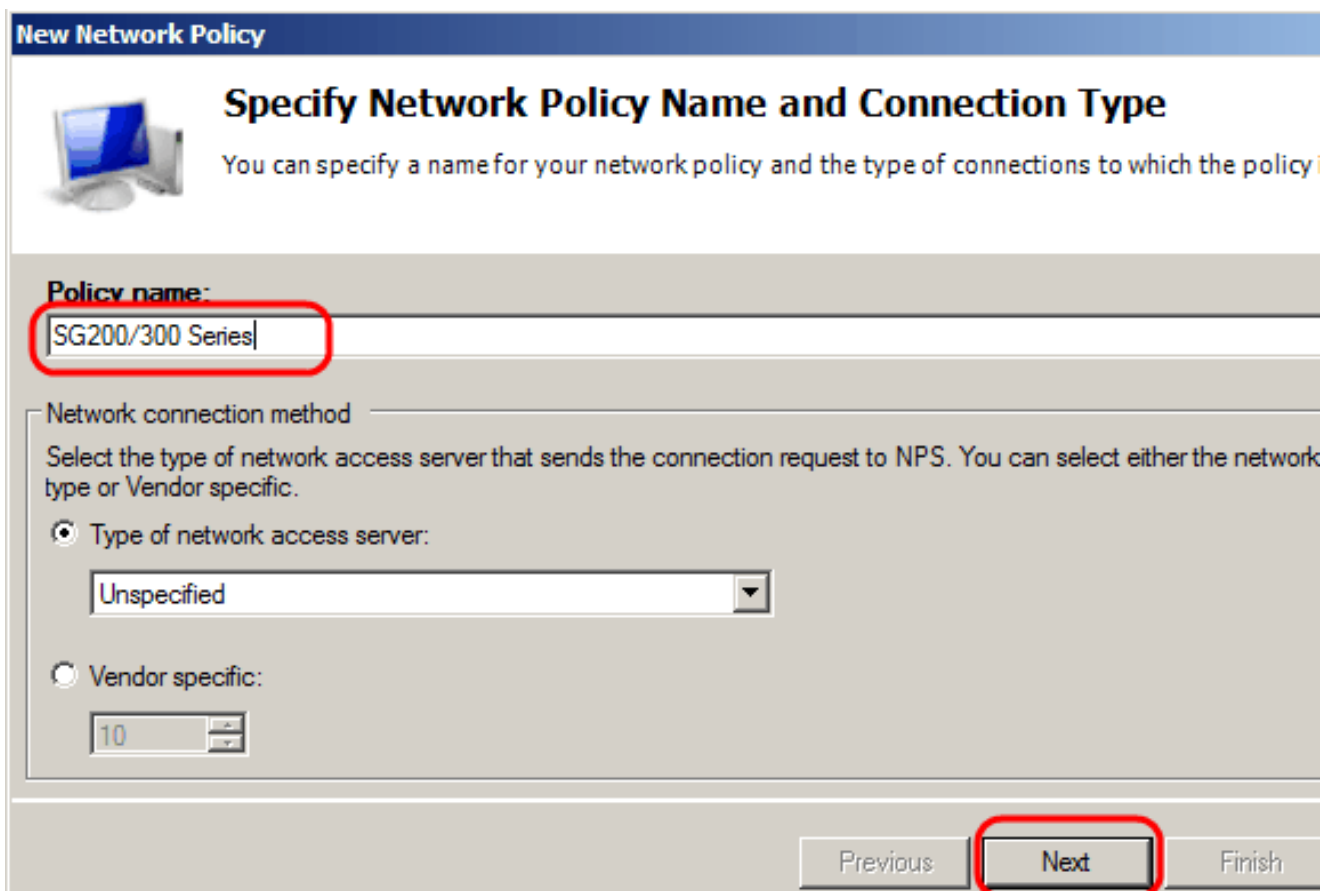
步驟 1.在Windows Server 2008電腦中，選擇開始>管理工具>網路策略伺服器。Network Policy Server視窗開啟：



步驟 2.要為網路的特定網段啟用RADIUS伺服器，您需要建立新的網路策略。要建立新的網路策略，請選擇Policies > Network Policy，然後按一下右鍵並選擇New。New Network Policy視窗開啟：



步驟 3.在Policy Name欄位中，輸入新策略的名稱。按「Next」（下一步）。



步驟 4.您需要指定此策略的條件。需要兩個條件：RADIUS伺服器要實施到哪個使用者段，以及連線到該段的方法。按一下Add以新增這些條件。

## New Network Policy



### Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection of one condition is required.

**Conditions:**

Condition	Value
-----------	-------

Condition description:

**Add...** Edit...

Previous Next Finish

步驟 5. 在「組」下有三個選項：「Windows組」、「電腦組」和「使用者組」。根據網路的設定選擇組，然後按一下新增。將根據選定的組開啟一個新視窗，按一下Add Groups。

**Select condition**

Select a condition, and then click Add.

Groups

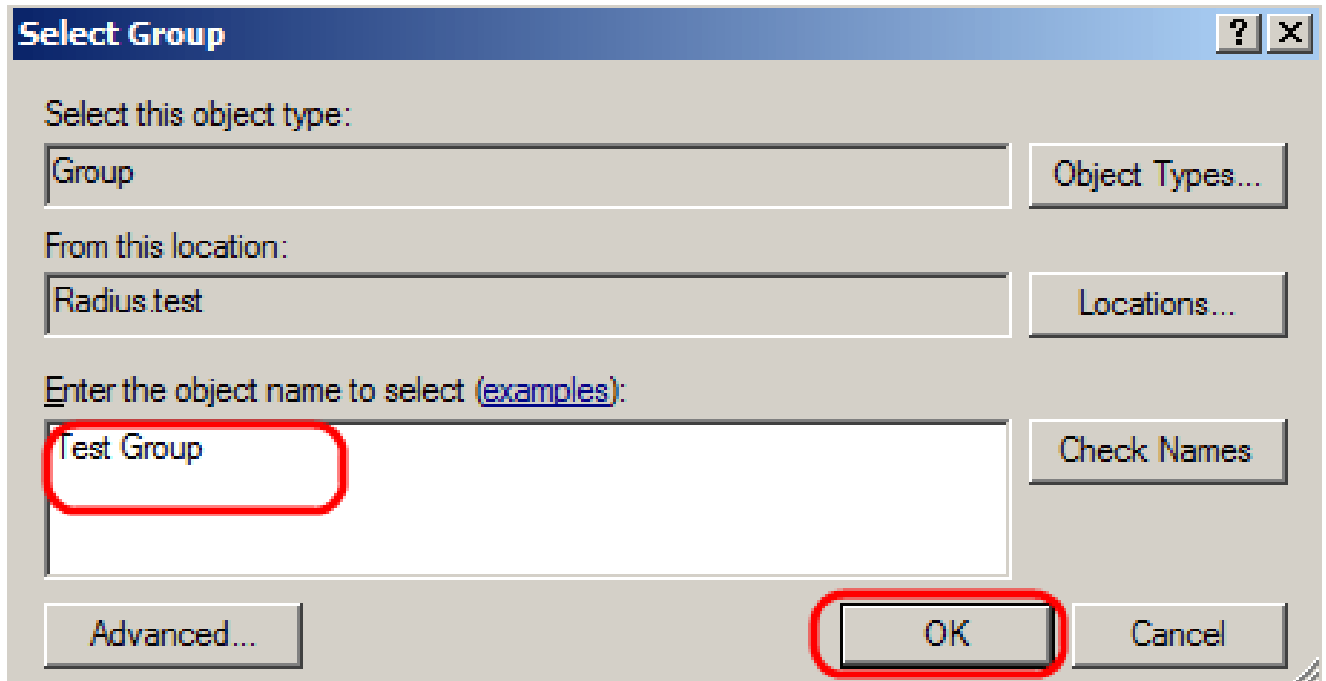
- Windows Groups**  
The Windows Groups condition specifies that the connecting user or computer must belong to one of the s
- Machine Groups**  
The Machine Groups condition specifies that the connecting computer must belong to one of the selected
- User Groups**  
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

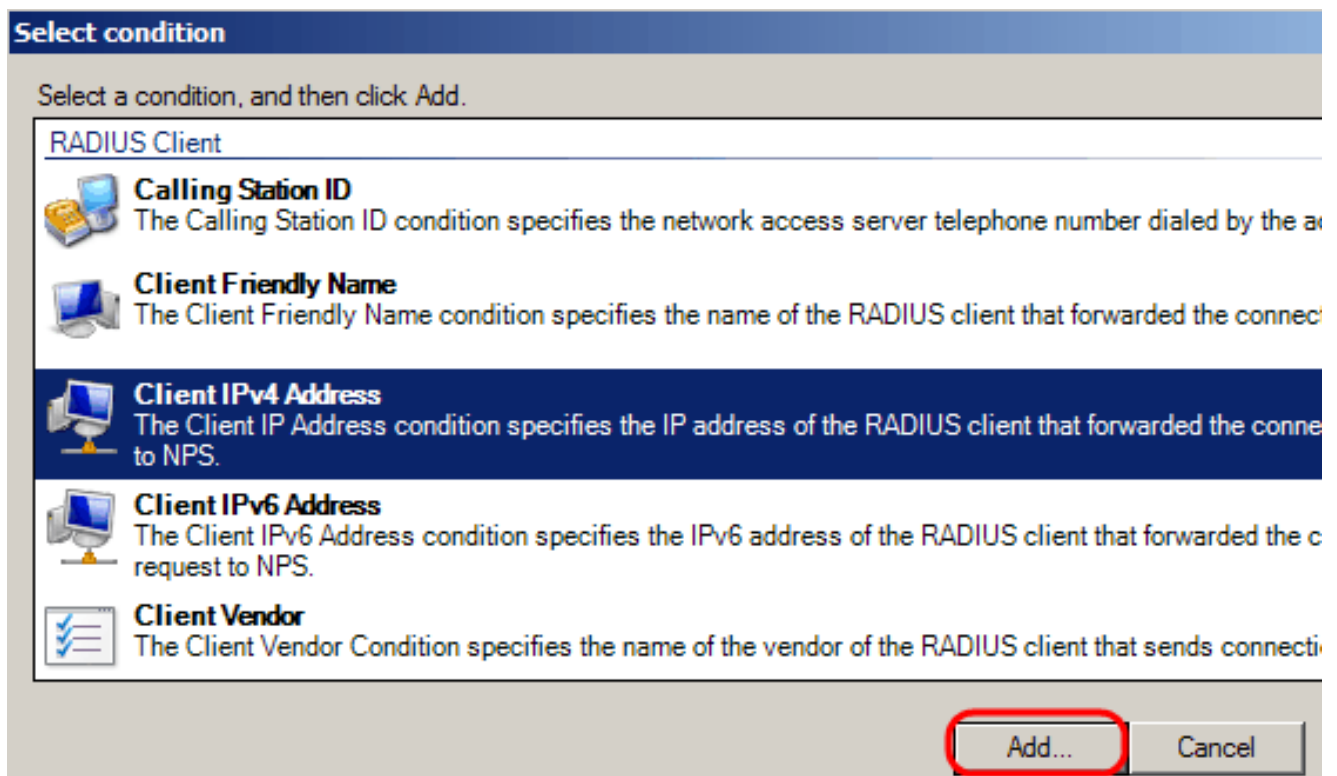
- Location Groups**  
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) locatio required to match this policy. The HCAP protocol is used for communication between NPS and some third network access servers (NASs). See your NAS documentation before using this condition.
- HCAP User Groups**

**Add...** Cancel

步驟 6. 選擇對象型別和位置，然後輸入對象的名稱。按一下「Ok」，然後「Ok」。按一下Add以新增下一個條件。



步驟 7. 在 RADIUS Client 下，選擇 IPv4 Address 作為將伺服器連線到 RADIUS 客戶端的方法，在本例中，RADIUS 客戶端將成為交換機 IP 地址。按一下「Add」。



步驟 8. 輸入相應的 IP 地址，然後按一下 Ok。顯示一個包含新增條件的清單，按一下下一步。

步驟 9. 在「指定訪問許可權」(Specify Access Permission) 頁面中，選擇授予訪問許可權 (Access Granted)。按「Next」(下一步)。

## New Network Policy



### Specify Access Permission

Configure whether you want to grant network access or deny network access if the policy.

Access granted

Grant access if client connection attempts match the conditions of this policy.

Access denied

Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)

Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous

Next

步驟 10. 在身份驗證頁面中，設定最適合您網路的身份驗證方法。按「Next」（下一步）。





## Configure Authentication Methods

Configure one or more authentication methods required for the connection request authentication, you must configure an EAP type. If you deploy NAP with 802.1X or Protected EAP in connection request policy, which overrides network policy authentication.

EAP types are negotiated between NPS and the client in the order in which they are listed.

### EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

### Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
  - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.
- Perform machine health check only

Previous

Next

步驟 11.在「配置約束」視窗中，使用預設值。按「Next」（下一步）。

步驟 12.在Configure Settings頁面的RADIUS Attributes下，按一下Vendor Specific，然後按一下Add。

注意：此頁中的其餘設定均設定為預設值。您只需處理特定於供應商的設定。

## New Network Policy



### Configure Settings

NPS applies settings to the connection request if all of the network policy conditions are matched.

#### Settings:

##### RADIUS Attributes



Standard



Vendor Specific

##### Network Access Protection



NAP Enforcement



Extended State

##### Routing and Remote Access



Multilink and Bandwidth Allocation Protocol (BAP)



IP Filters



Encryption



IP Settings

To send additional attributes to RADIUS clients, select a Vendor then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
------	--------	-------

Add...

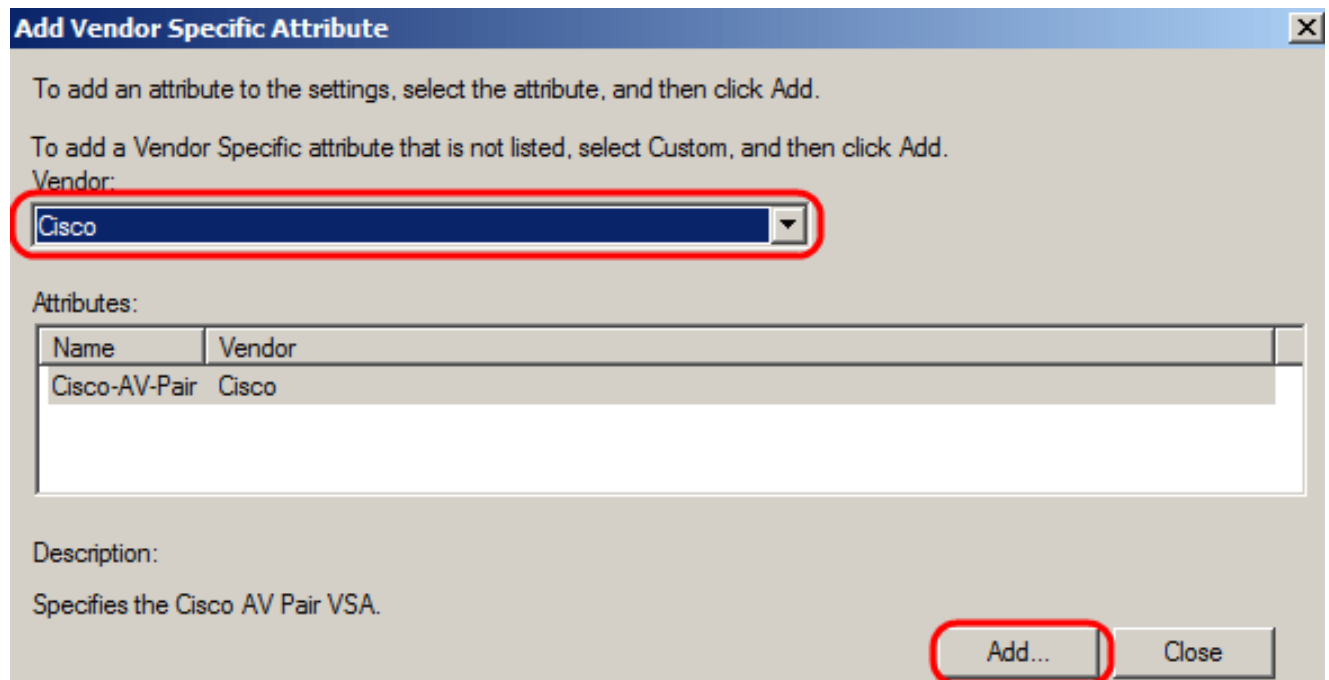
Edit...

Remove

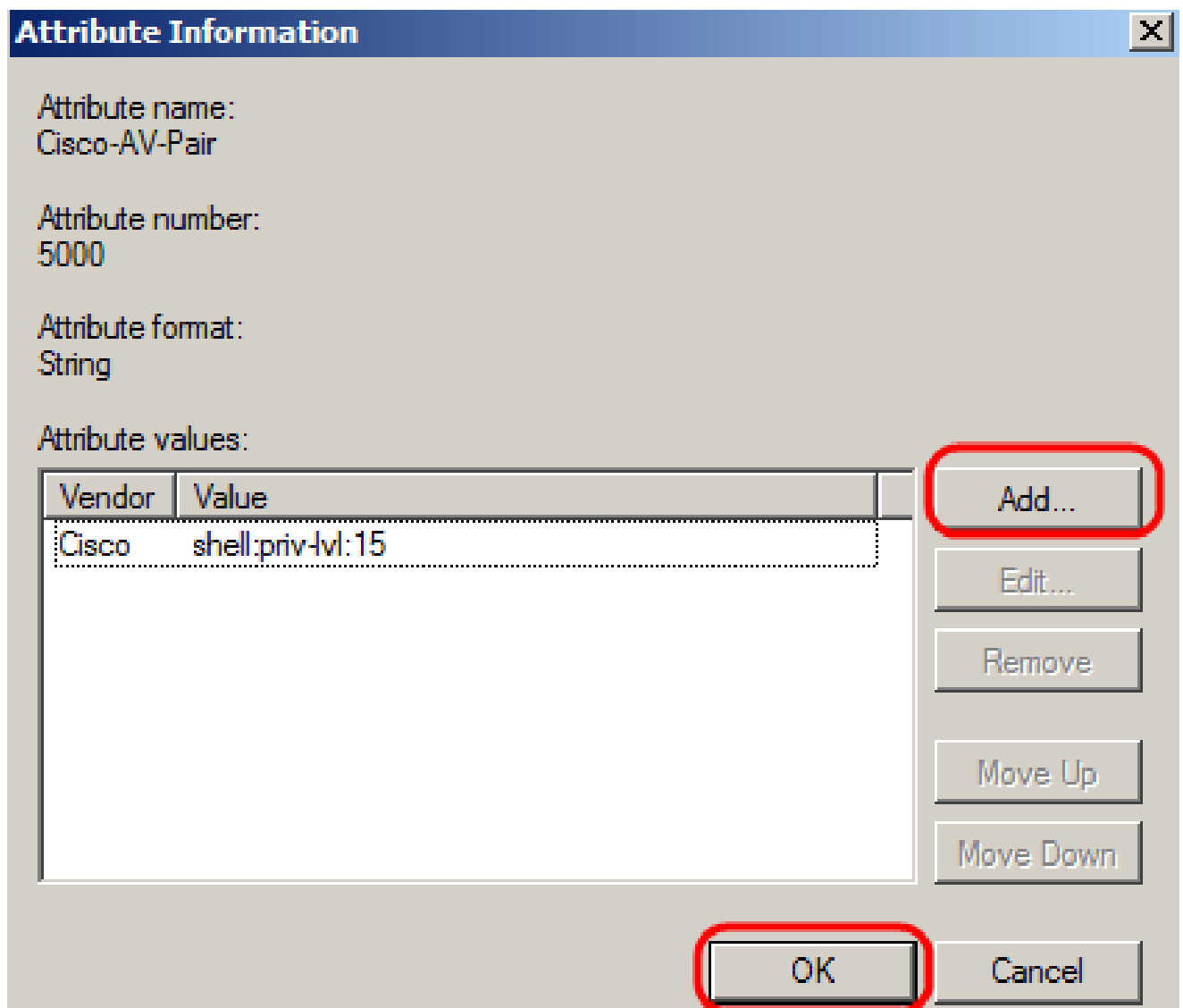
Previous

Next

在Vendor下，選擇Cisco。按一下「Add」。Attribute Information視窗開啟。



在「屬性資訊」視窗中，按一下Add，然後輸入值shell:priv-lvl:15。按一下「OK」（確定）。




注意：這是思科分配的值，用於RADIUS伺服器授予對基於Web的交換機配置實用程式的訪問許可權。

按一下Ok以關閉「Attribute Information」視窗，然後按一下Close以關閉「Add Vendor Specific Attribute」視窗。按「Next」（下一步）。

步驟 13.將顯示此策略的設定摘要，按一下完成。網路策略已建立。

**New Network Policy**



## Completing New Network Policy

You have successfully created the following network policy:

**SG200/300 Series**

**Policy conditions:**

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

**Policy settings:**

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OF
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous Next **Finish**

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。