

在CSPM中配置Cisco Secure IDS感測器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[組態](#)

[定義CSPM主機所在的網路](#)

[新增CSPM主機](#)

[新增感測器裝置](#)

[配置感測器](#)

[相關資訊](#)

簡介

本文說明在Cisco Secure Policy Manager(CSPM)上配置Cisco Secure Intrusion Detection System(IDS)感測器的過程。本檔案假設您已經在電腦上安裝CSPM 2.3.1版。版本「1」允許在Cisco Catalyst®6000交換機中管理IDS裝置(裝置感測器、Cisco IOS®路由器或IDS刀片)。本文檔還假設IDS郵局引數已正確定義。其中包括HOSTID、ORGID、HOSTNAME和ORGNAME。請注意，要使CSPM主機與感測器通訊，ORGID和ORGNAME必須與感測器上定義的相匹配。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據CSPM 2.3.1及更新版本。

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。

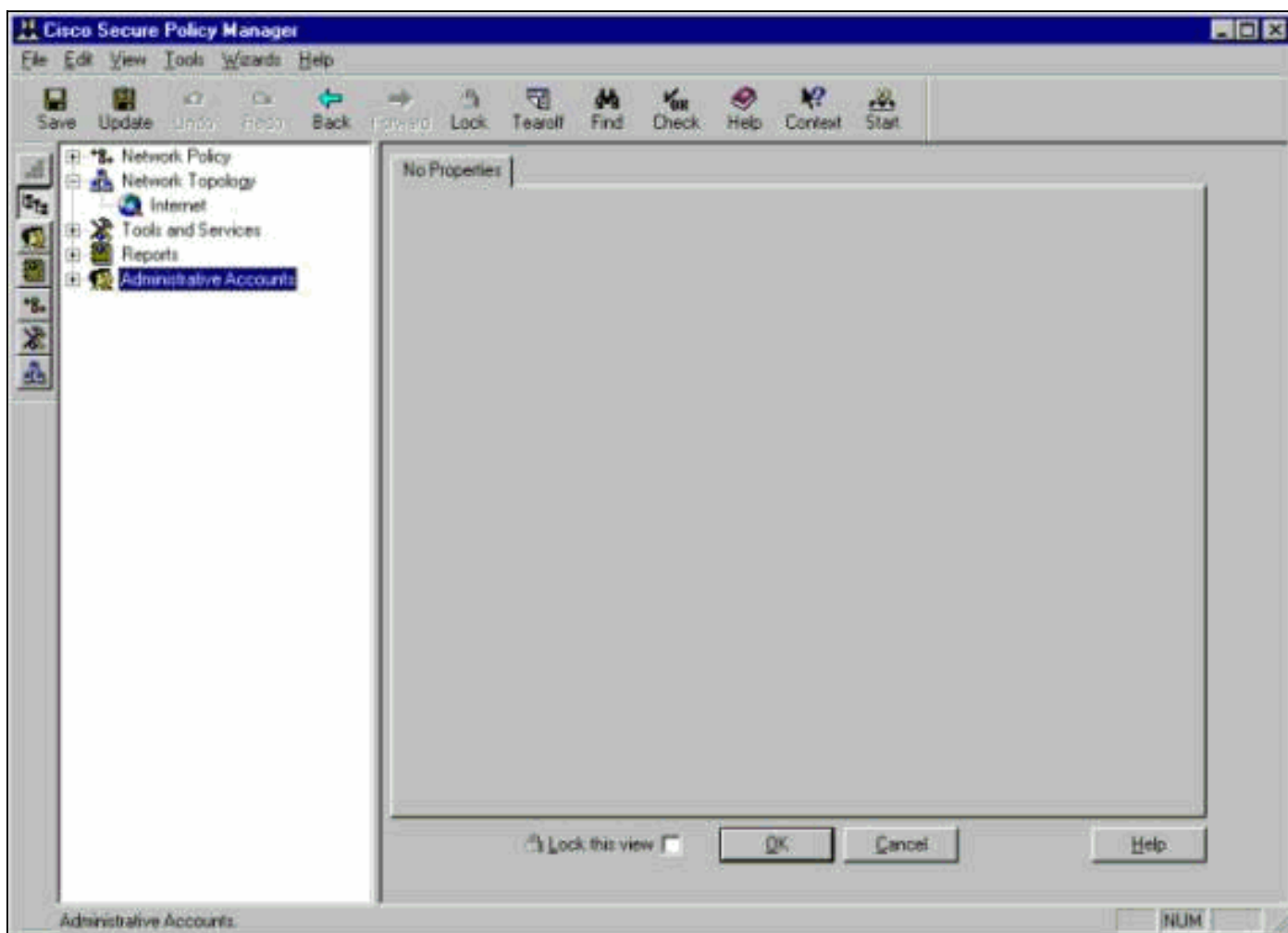
慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

組態

以下各節說明了在CSPM中配置IDS感測器的過程。

啟動CSPM並登入。此時將顯示一個空白模板（初始啟動），允許您定義網路。



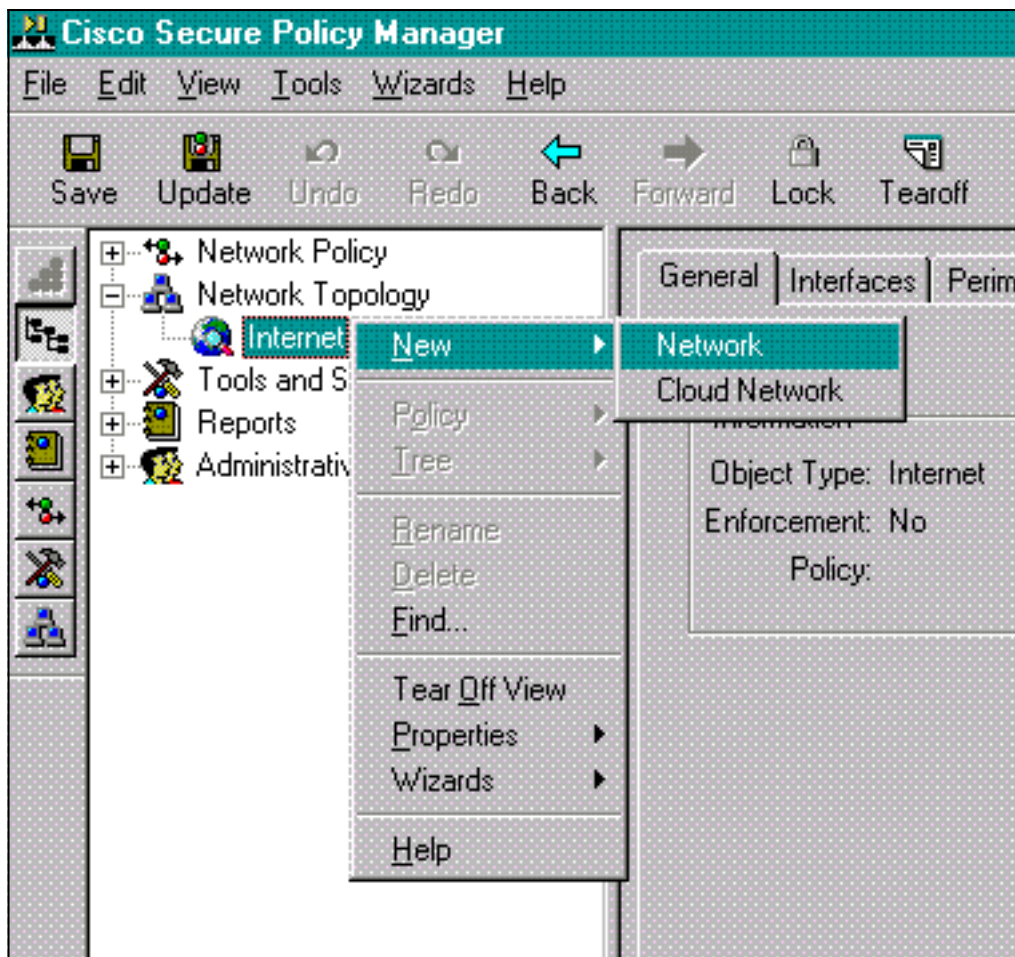
在IDS的CSPM拓撲中，這三個定義是必需的。

1. 定義感測器控制介面所在的網路和CSPM主機所在的網路。如果它們位於同一子網中，則只需定義一個網路。首先定義此網路。
2. 在其網路中定義CSPM主機。如果沒有CSPM主機定義，則無法管理感測器。
3. 在其網路中定義感測器。

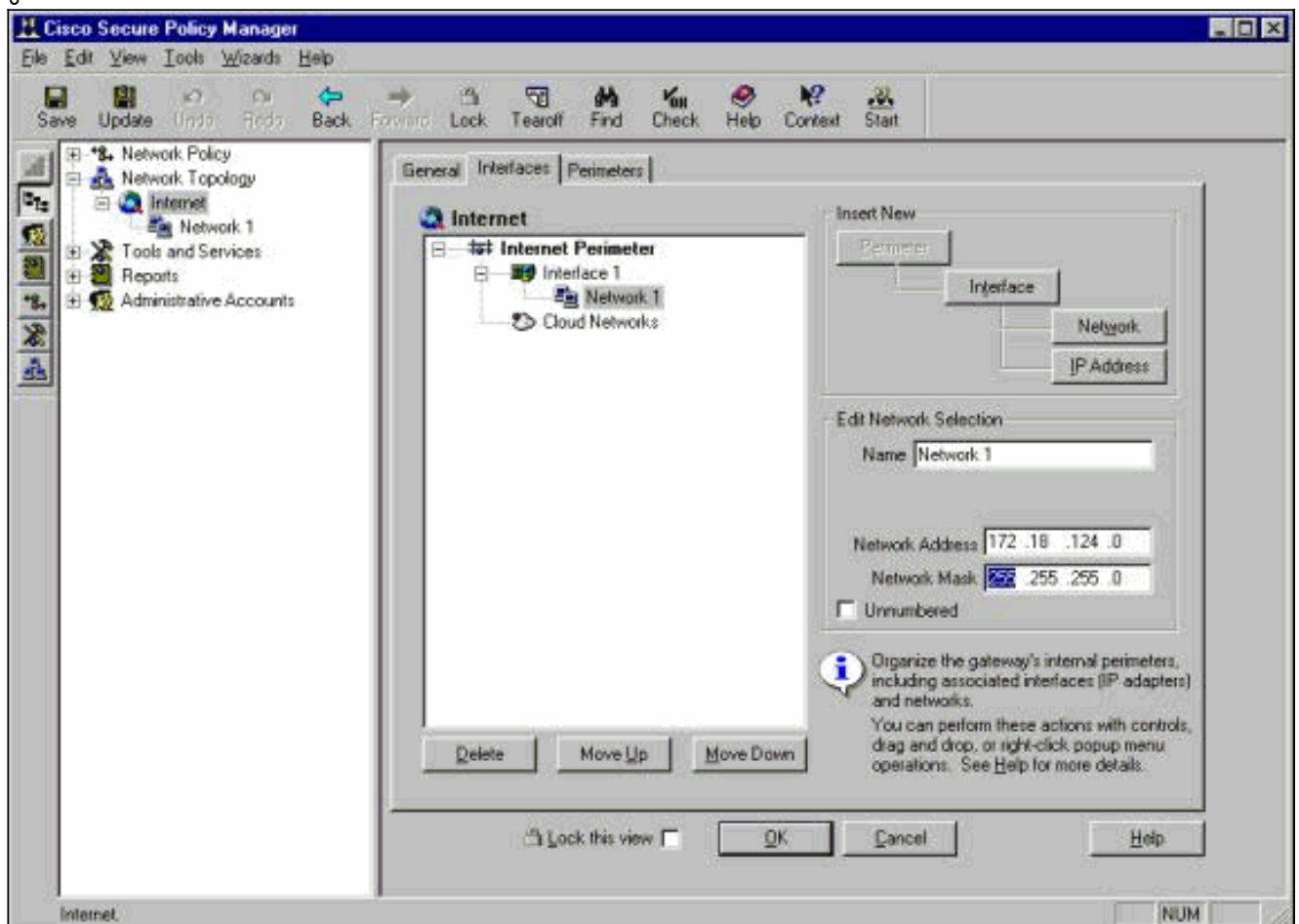
定義CSPM主機所在的網路

請完成以下步驟：

1. 按一下右鍵拓撲中的Internet圖示，然後選擇**New > Network**以建立新網路。



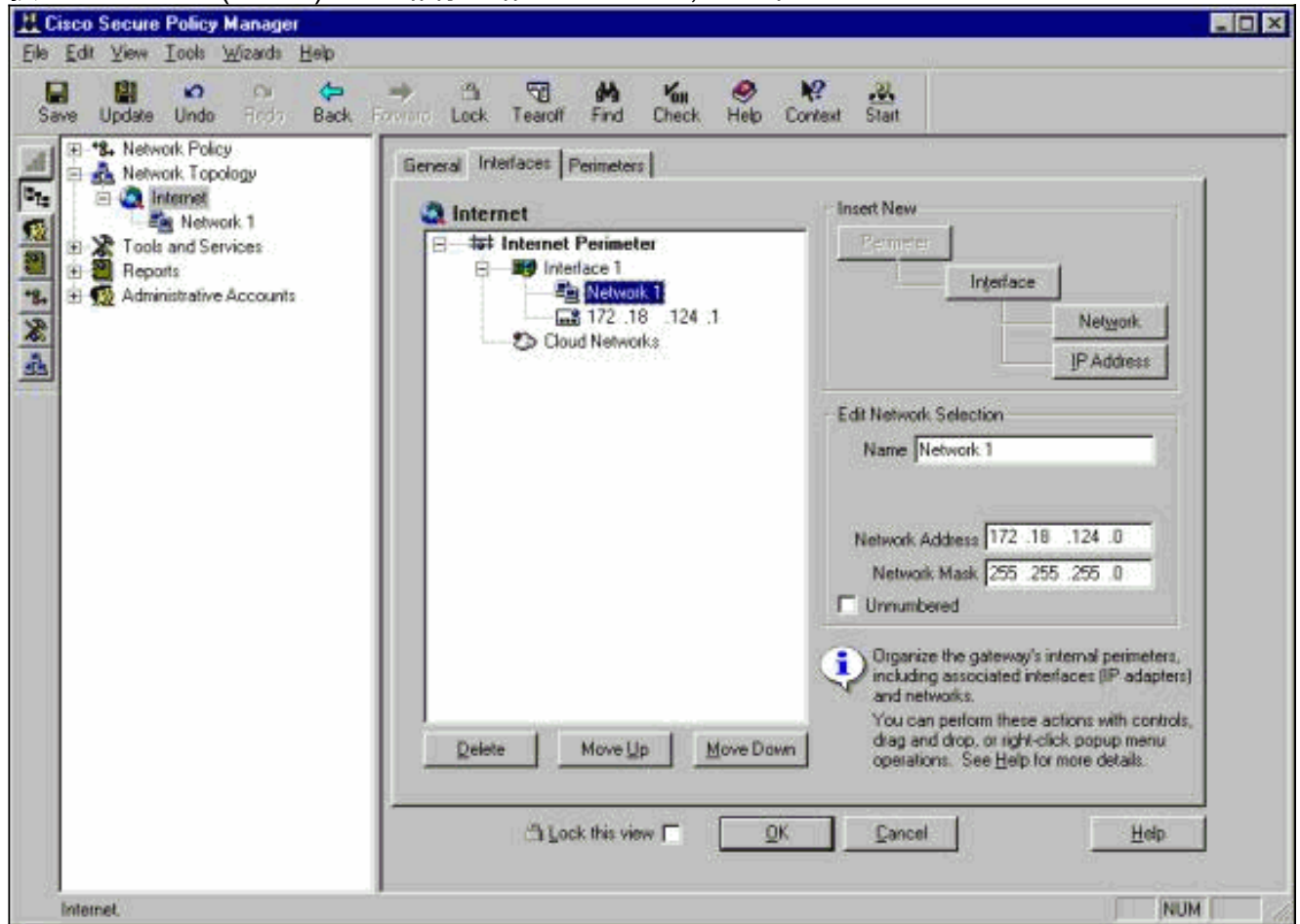
2. 在「Network Panel (網路面板)」的右側，新增要使用的新網路名稱、網路地址和網路掩碼。



3. 按一下IP Address按鈕，然後輸入網路用於訪問Internet的IP地址。通常它是網路的預設網關。

注意：管理感測器時，由於未向感測器傳送此預設網關資訊，因此網關地址不必正確。應在感測器中定義。

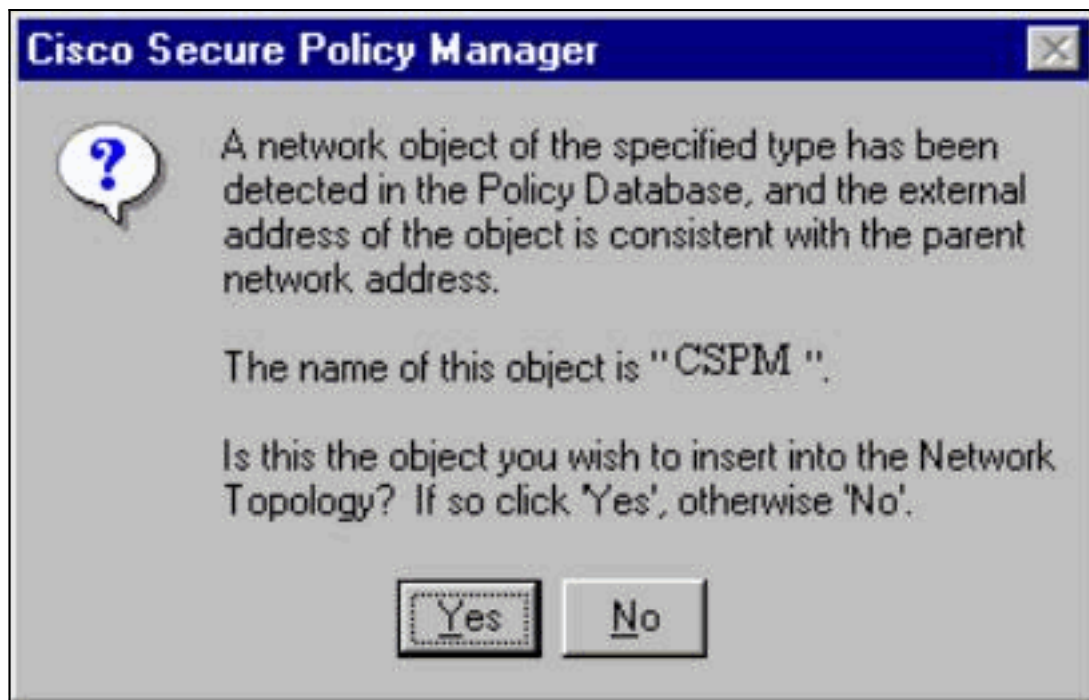
4. 按一下「OK」（確定）。網路將新增到拓撲圖中，沒有任何錯誤。



新增CSPM主機

使用此過程新增CSPM主機。

1. 在網路拓撲中，按一下右鍵剛新增的網路，然後選擇**New > Host**。CSPM將顯示類似以下的螢幕。如果不是，則您剛定義的網路不是CSPM主機所在的網路。再次檢查CSPM主機上的IP地



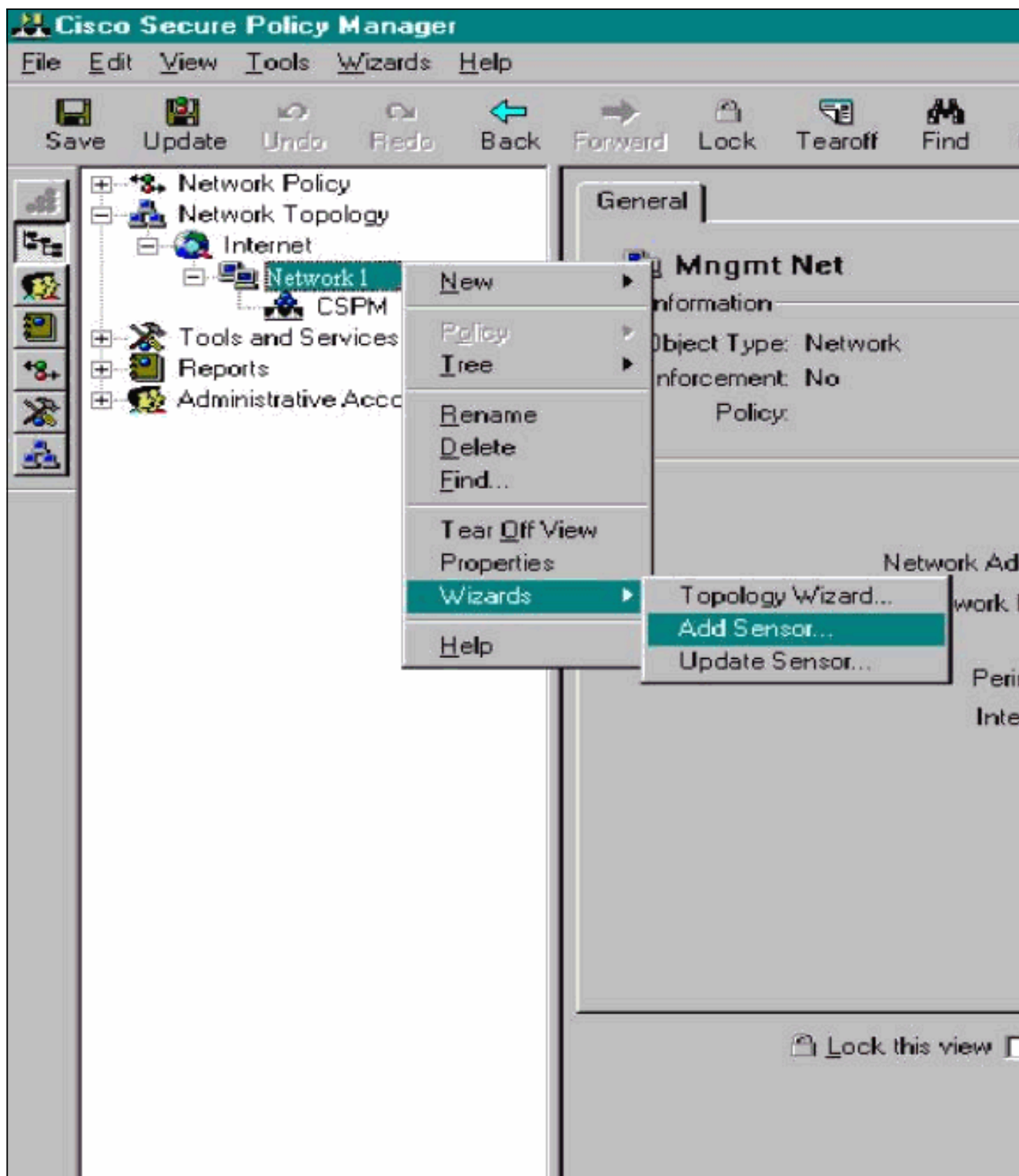
址。

2. 按一下**Yes**將CSPM主機安裝到拓撲中。
3. 驗證CSPM主機的「General (常規)」螢幕上的資訊是否正常。
4. 在CSPM主機的General螢幕上按一下**OK**。

新增感測器裝置

使用此過程新增感測器裝置。

1. 按一下右鍵感測器所在的網路並選擇**Wizards > Add Sensor**。注意：如果CSPM主機和感測器的控制介面不在同一網路中，請定義感測器所在的網路。



2. 輸入感測器的正確郵局引數。

Add Sensor Wizard

Sensor Identification

Welcome to the Add Sensor Wizard. To add a Sensor to the topology fill in the following information and press Next.

Sensor Identification

Sensor Name Host ID Org. ID

Organization Name

IP Address

Postoffice Heartbeat Interval

Policy Enforcement


Associated Network Service

Port

Comments

Check here to verify the Sensor's address.

Check here to capture the Sensor's configuration.

 Enter the IP Address and the Host ID will populate automatically. Or you may enter it manually.

< Back Next > Cancel Help

- 按一下 **Check here to verify the Sensor's address** 框。注意：如果這是第一次設定此感測器，則不需要捕獲感測器的配置。如果您以前通過UNIX導向器或其他CSPM主機配置過此感測器並對感測器特徵碼進行了配置更改，則您需要捕獲感測器的配置。
- 按一下下一步以定義感測器上的特徵碼版本。您也可以發出 `nrvrs` 命令在感測器上檢查此情況

Add Sensor Wizard

Sensor Configuration

Specify the Policy Distribution Host. Select the version of the Sensor and enable or disable IPSec support. Choose the appropriate Signature Template from the drop down lists.

Distribution
Host: **CSPM (1)** Select the Cisco Secure Policy Manager host that will publish the generated device-specific command sets to this device.

Sensor Version: **3.0(1)S8**

IPSec
 Check here to enable IPSec on supported Sensor versions.

Signature Template: **Default**

Template Comment
Cisco Systems, Inc. default Signature Template settings.

i There are 3 signatures in the latest signature update (3.0(1)S8) that do not apply to this Sensor version 3.0(1)S8.

< Back Next > Cancel Help

。 **注**：如果CSPM的感測器版本不正確，則請更新CSPM主機上的簽名。如需更新，請參閱[軟體下載](#)(僅限註冊客戶)。

5. 按一下**Next**按鈕繼續。
6. 按一下**Finish**完成將感測器安裝到拓撲結構中的過程。
7. 在CSPM主選單中，選擇**File > Save and Update**，將拓撲中輸入的資訊編譯為CSPM。請注意，在CSPM主機上啟動郵局協定需要執行此步驟。
8. 以網路使用者身份登入感測器，驗證一切是否正常。
9. 執行nrconns命令。

>nrconns

Connection Status for gacy.rtp

```
cspm.rtp Connection 1: 172.18.124.106 45000 1
[Established] sto:0004 with Version 1
```

netrangr@gacy:/usr/nr

>

註：如果感測器和CSPM主機沒有通訊，將顯示類似以下內容的輸出：

netrangr@gacy:/usr/nr

>nrconns

Connection Status for gacy.rtp


```
insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent]
sto:5000 syn NOT rcvd!
```

```
netrangr@gacy:/usr/nr
```

如果是這種情況，請取得監聽器追蹤軌跡，看看兩端是否正在傳送UDP45000封包。UDP通45000是IDS裝置用於相互通訊的內容。要在感測器上測試此情況，請將su根和（取決於您使用的感測器）執行snoop -d iprb1埠45000（對於IDS 4210感測器）和snoop -d iprb0埠4500（對於任何其他感測器型號）。使用<control-c>中斷監聽會話。如果感測器和CSPM之間沒有通訊，則顯示此輸出：

```
netrangr@gacy:/usr/nr
```

```
>su -
```

```
Password:
```

```
Sun Microsystems Inc. SunOS 5.8 Generic February 2000
```

```
# snoop -d spwr0 port 45000
```

```
Using device /dev/spwr (promiscuous mode)
```

```
172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52
```

```
172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52
```

```
172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52
```

```
172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52
```

```
^C#
```

在上面的輸出中，感測器傳送UDP數45000包，但不會收到任何資料包。正確的配置會產生類似以下的輸出：

```
# snoop -d spwr0 port 45000
```

```
Using device /dev/iprb (promiscuous mode)
```

```
172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56
```

```
gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56
```

```
172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56
```

```
gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56
```

在上面的輸出中，UDP 45000流量雙向傳輸。如果UDP 45000資料包雙向流動，感測器上的nrconns輸出仍顯示未建立連線，則感測器和CSPM主機上的郵局引數不匹配。手動檢查CSPM主機上的郵局引數：使用Windows資源管理器導航到NT電腦上安裝CSPM的位置。

C:\Program Files\Cisco Systems\Cisco Secure Policy Manager\PostOffice\etc

File Edit View Help

etc

Name	Size	Type	Modified	Attributes
auths	1KB	File	10/10/01 12:53 PM	A
auths.bak	1KB	BAK File	10/10/01 12:38 PM	A
daemons	1KB	File	9/27/01 10:45 AM	A
destinations	1KB	File	10/8/01 5:37 PM	A
destinations.bak	1KB	BAK File	9/27/01 10:45 AM	A
hosts	1KB	File	10/10/01 12:53 PM	A
hosts.bak	1KB	BAK File	10/10/01 12:38 PM	A
organizations	1KB	File	9/27/01 10:45 AM	A
postofficed.conf	1KB	CONF File	10/8/01 5:37 PM	A
postofficed.conf.tmp	1KB	TMP File	10/10/01 12:05 PM	A
routes	1KB	File	10/10/01 12:53 PM	A
routes.bak	1KB	BAK File	10/10/01 12:38 PM	A
sapd.conf	3KB	CONF File	8/8/01 11:26 PM	A
services	2KB	File	8/8/01 11:26 PM	A
signatures	10KB	File	8/8/01 11:26 PM	A
smid.conf	1KB	CONF File	10/8/01 5:37 PM	A
smid.conf.bak	1KB	BAK File	9/27/01 10:45 AM	A

17 object(s) 18.4KB

使用寫或寫字板編輯主機、路由和組織檔案（請勿使用記事本，因為格式將損壞）。確保這些檔案對於您的安裝看起來正確。如果任何值不正確，請按照以下步驟對其進行編輯並重新啟動 NT 電腦：按一下網路拓撲中的 **CSPM** 圖示。點選 Policy Distribution 頁籤以輸入郵局引數。儲存和更新您的變更。重新啟動 NT 電腦。

Cisco Secure Policy Manager

File Edit View Tools Wizards Help

Save Update Undo Redo Back Forward Lock Tearoff Find Check Help Context Start

INSANE

Policy Distribution

General Settings

Client Name: Policy Distribution

Associated Network Service: [Dropdown]

IP Address: [Dropdown]

Port: 0 Disabled

Postoffice Settings

Host Name: CSPM

Host Id: 106

Org Name: rtp

Org Id: 1

Heartbeat: [Text]

IP Address: 172.18.124.106

Network Service: Cisco Post Office

Port: UDP 45000

The Postoffice Settings on this page specify the values for the policy distribution host. A Sensor node must be in the Network Topology and Update pressed in order to apply these settings to the distribution host's postoffice.

Lock this view OK Cancel Help

INSANE NUM

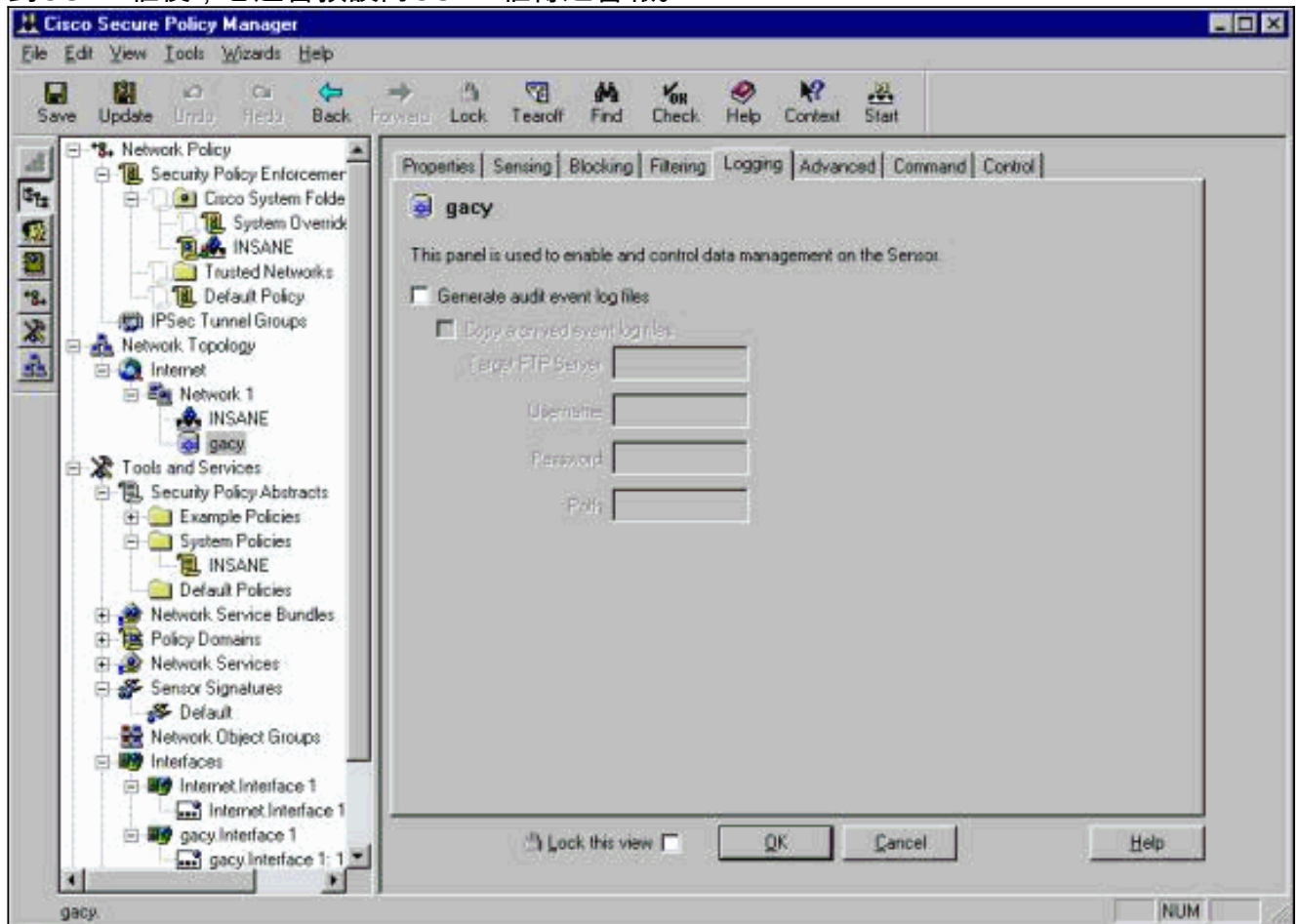
配置感測器

在CSPM中儲存配置後，配置感測器。為此，請首先將感測器設定為將它看到的警報寫入其自己的日誌。然後在正確的介面上將感測器設定為「嗅探」。

將警報寫入日誌

使用此過程將警報寫入日誌。

1. 按一下**Generate audit event log files**框以指示感測器將警報傳送到其本地日誌。在將配置下推到CSPM框後，它還會預設向CSPM框傳送警報。

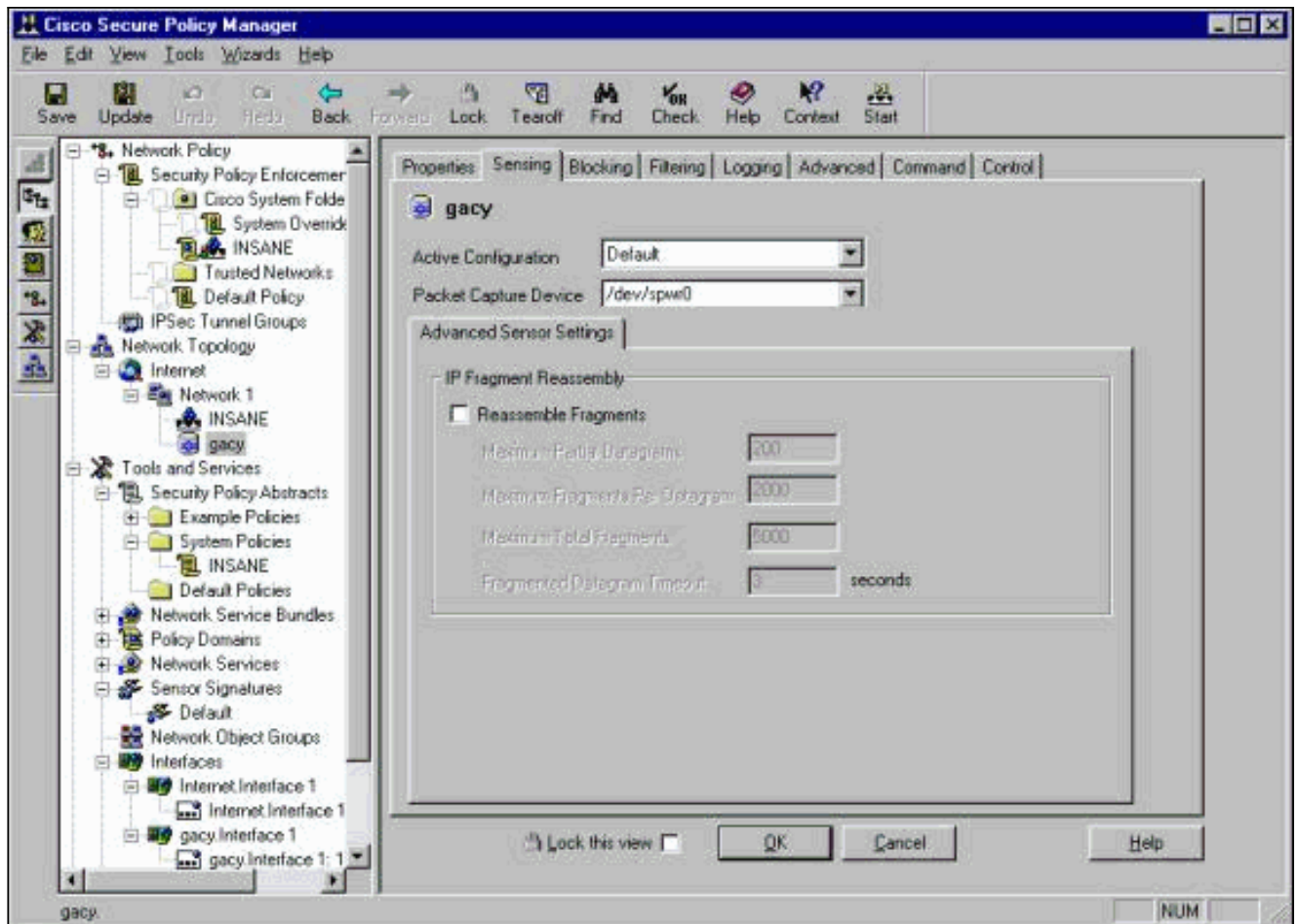


2. 按一下**OK**繼續。

將感測器設定為「嗅探」

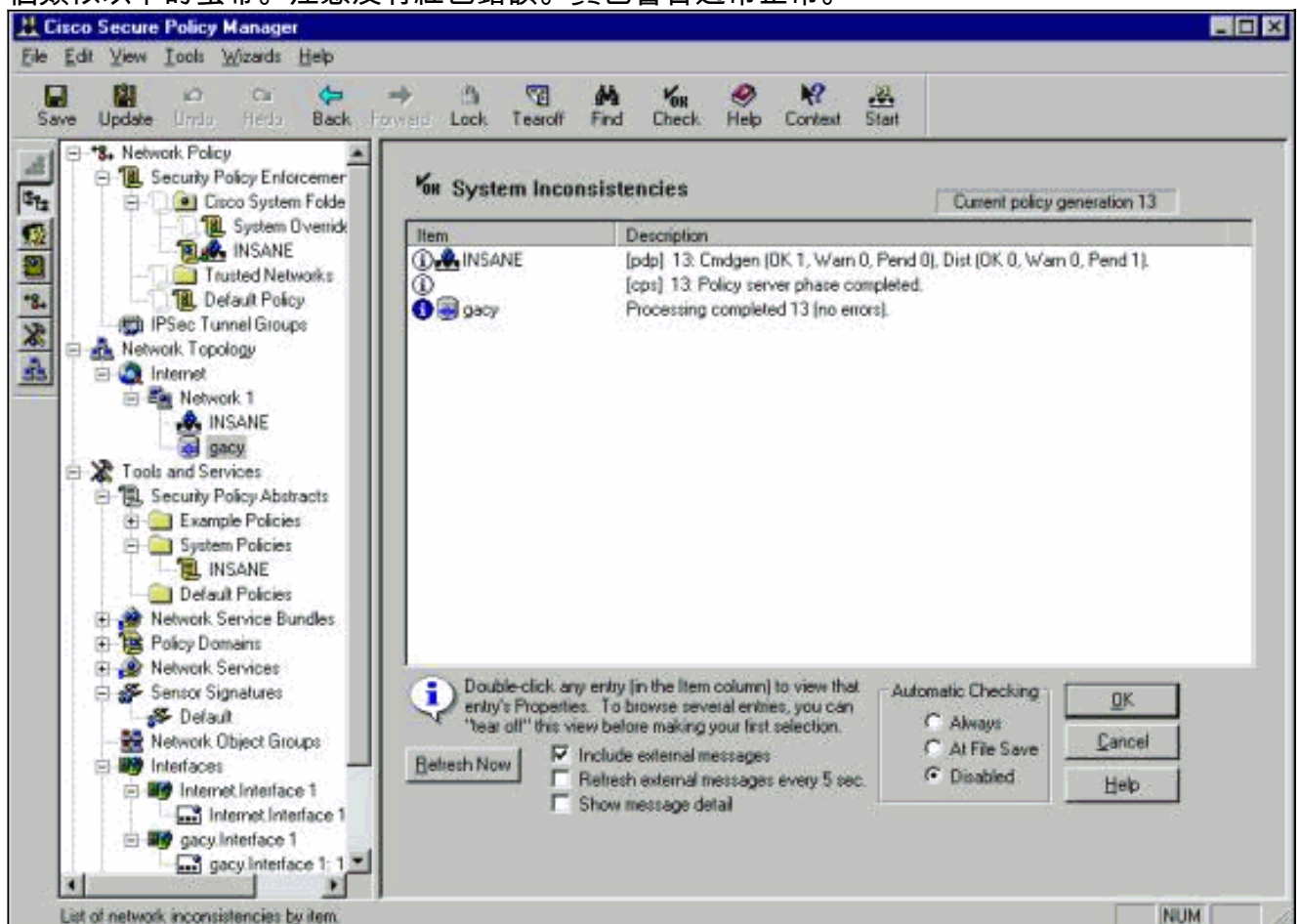
使用此過程將感測器設定為「嗅探」。

1. 選擇CSPM拓撲中的感測器，然後按一下「感應」頁籤。
2. 定義資料包捕獲裝置：iprb0 — 用於IDS 4210感測器spwr0 — 適用於任何其他感測器型號

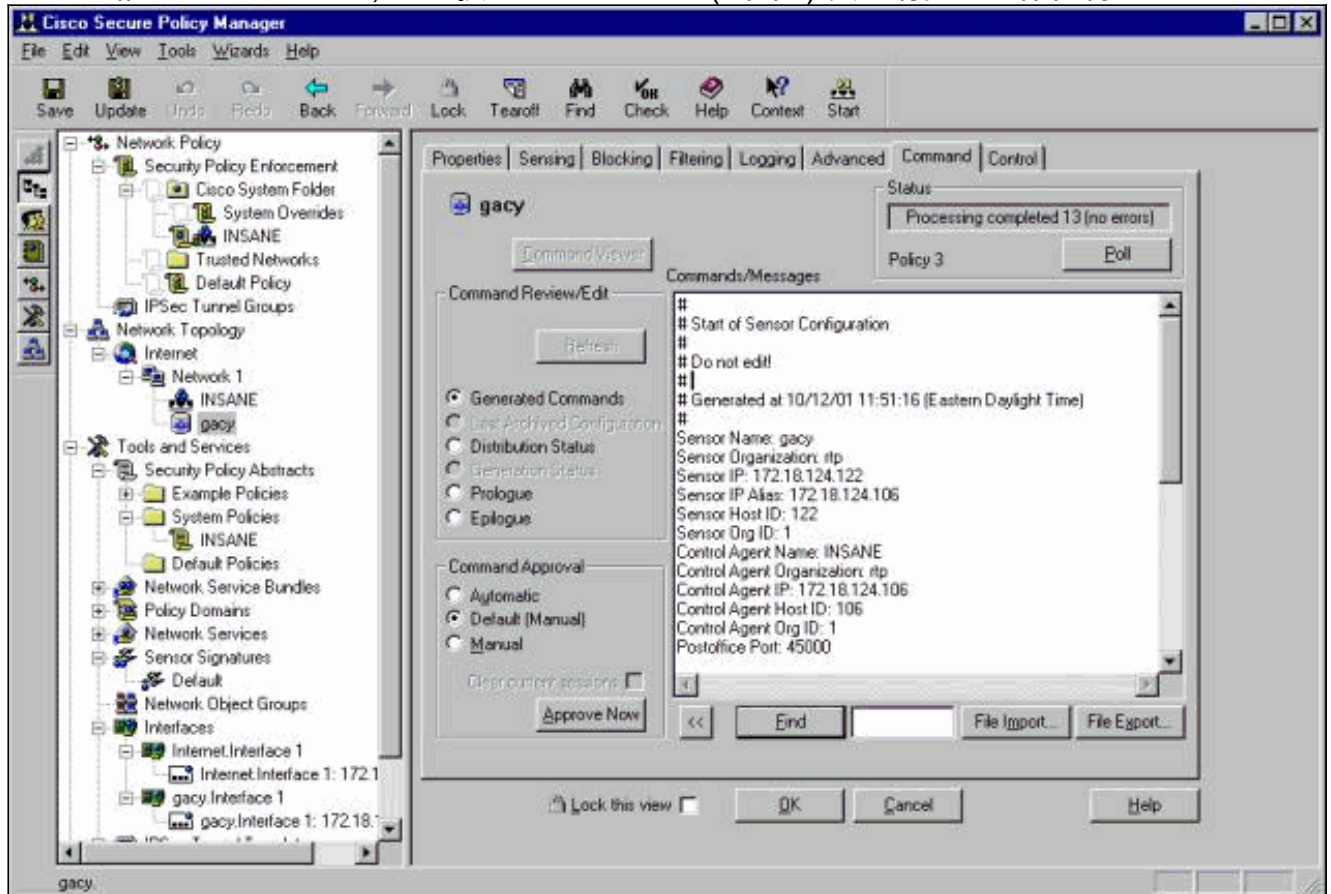


3. 按一下OK繼續。

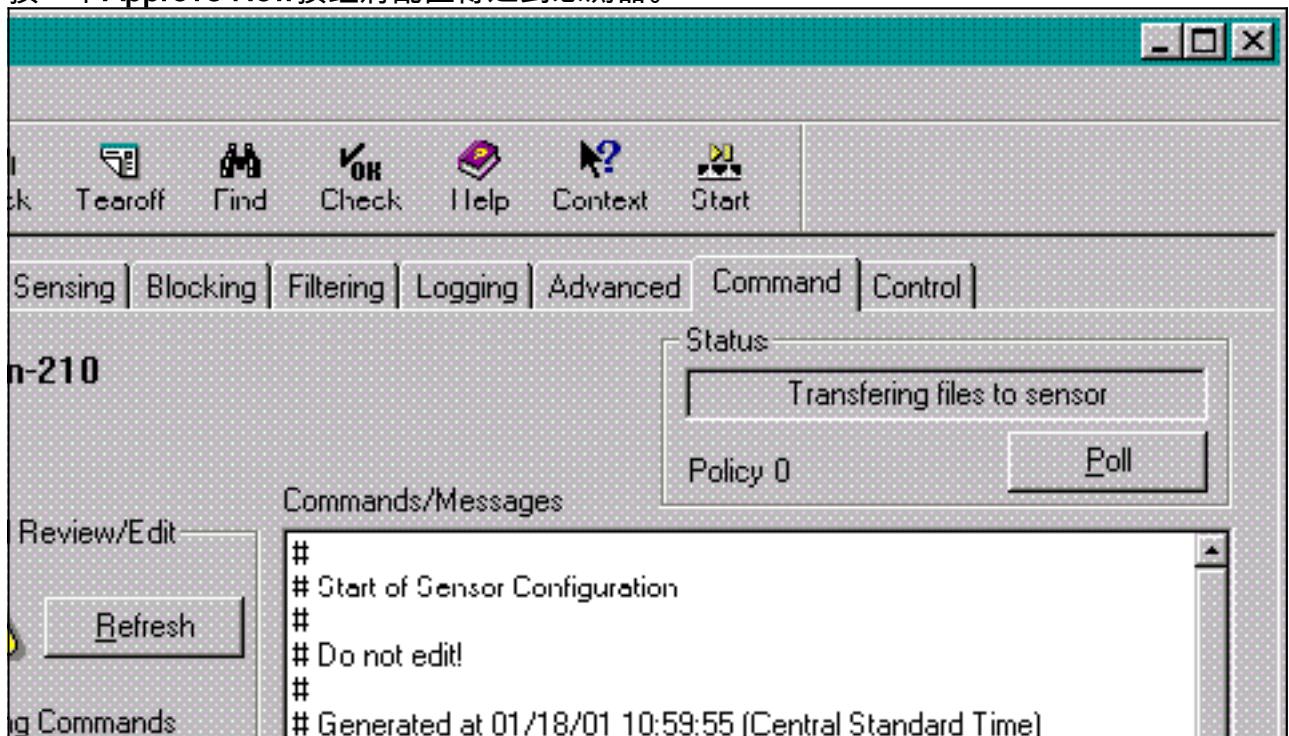
4. 按一下CSPM選單欄上的Update圖示以使用資訊更新CSPM。注意：如果一切順利，將顯示一個類似以下的螢幕。注意沒有紅色錯誤。黃色警告通常正常。



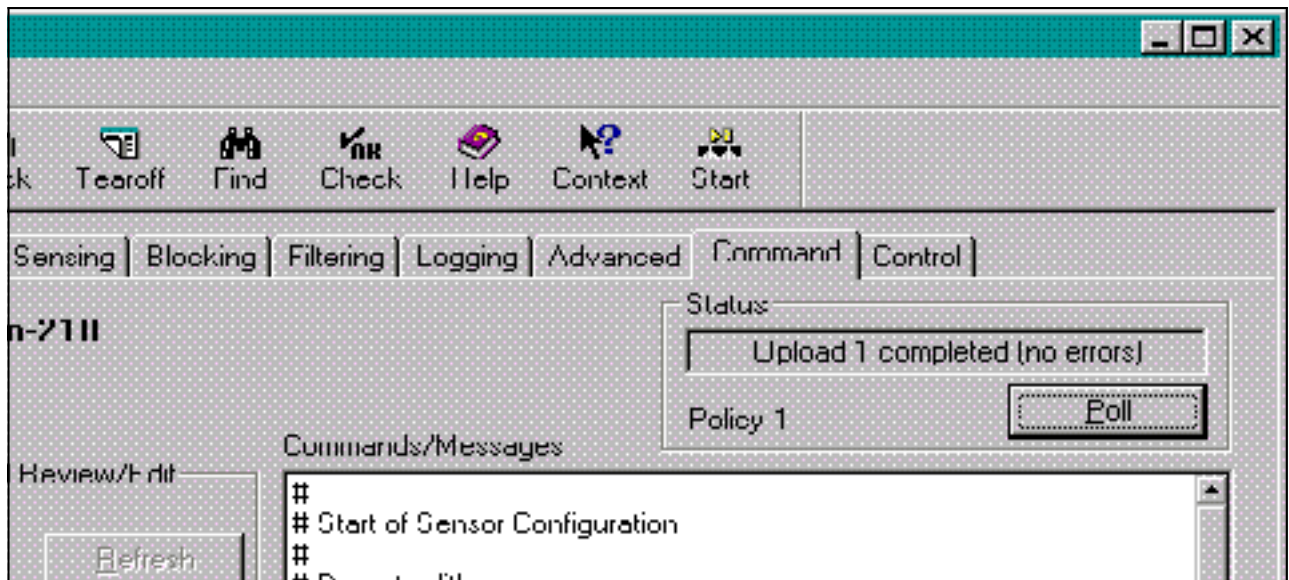
5. 選擇網路拓撲中的感測器，然後按一下Command (命令) 頁籤將更新的配置傳送到感測器。



6. 按一下Approve Now按鈕將配置傳送到感測器。

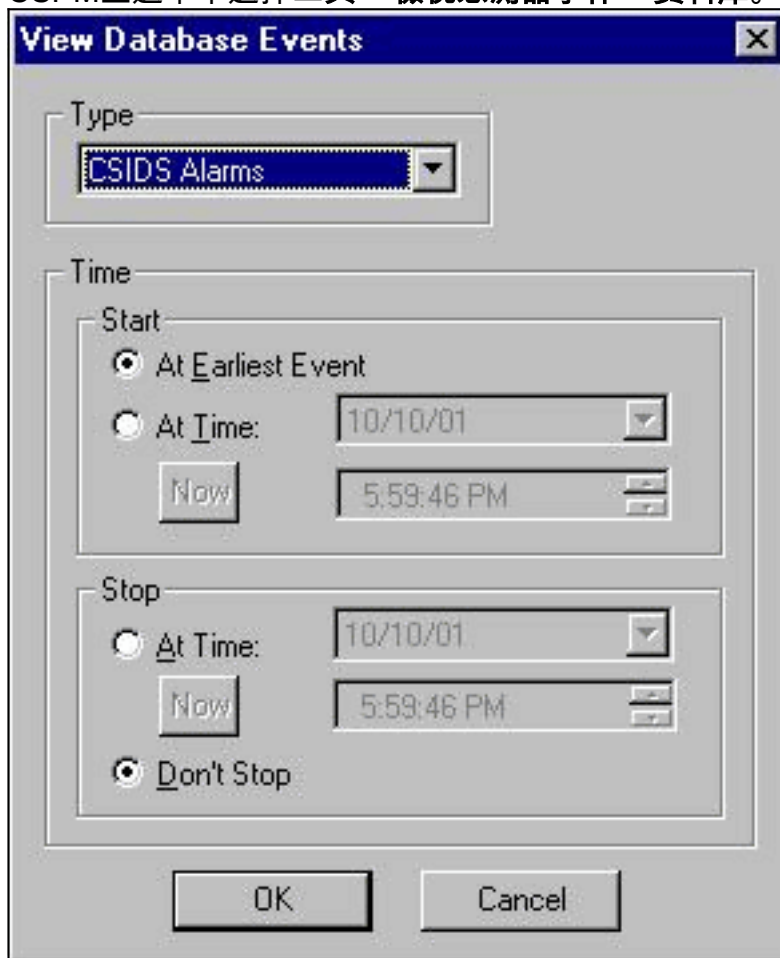


狀態窗格顯示「Upload <#> completed」(上傳<#>已完成)消息。這表示有效且完整的傳輸過程。感測器現在已更新，現在應能正常運行。如果感測器未正常運行，請返回感測器並檢查nrconns命令的輸出，以確保CSPM主機與感測器之間建立連線。



完

成後，您可以在事件檢視器中查詢感測器傳送到CSPM主機的警報。要檢視事件檢視器，請從CSPM主選單中選擇工具 > 檢視感測器事件 > 資料庫。



按一下OK以顯示事件資料庫視窗。根

據可能收到的警報，螢幕會有所不同。

Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	*							
48	ICMP flood	+							
6	ICMP smurf attack	+							
6	ICMP unreachable	10.32.10.10	172.18.124.154	<none>	OUT	OUT	0	Low	rtp
40	IP fragments overlap	+							
38	Net sweep-echo	+							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
24	Route Down!	<none>	<none>	+					
29	Route Up	<none>	<none>	+					
7	UDP Packet	+							

相關資訊

- [技術支援與文件 - Cisco Systems](#)