# CSPM での Cisco Secure IDS センサーの設定

## 目次



## 概要

このドキュメントは、Cisco Secure Policy Manager（CSPM）で Cisco Secure Intrusion Detection System（IDS）センサーを設定するための手順について説明します。 コンピュータに CSPM バージョン 2.3.I がインストール済みであることを前提としています。 バージョン "I" では、Cisco Catalyst(R) 6000 スイッチの IDS 装置（センサー装置、Cisco IOS(R) ルータ、または IDS ブレード）の管理が可能です。 また、IDS postoffice パラメータが正しく定義されていることも前提となります。 パラメータには、HOSTID、ORGID、HOSTNAME、および ORGNAME などが含まれます。 CSPM ホストがセンサーと通信するには、ORGID および ORGNAME などのパラメータがセンサーに定義されているパラメータと一致する必要があります。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

この文書に記載されている情報は CSPM 2.3.I およびそれ以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

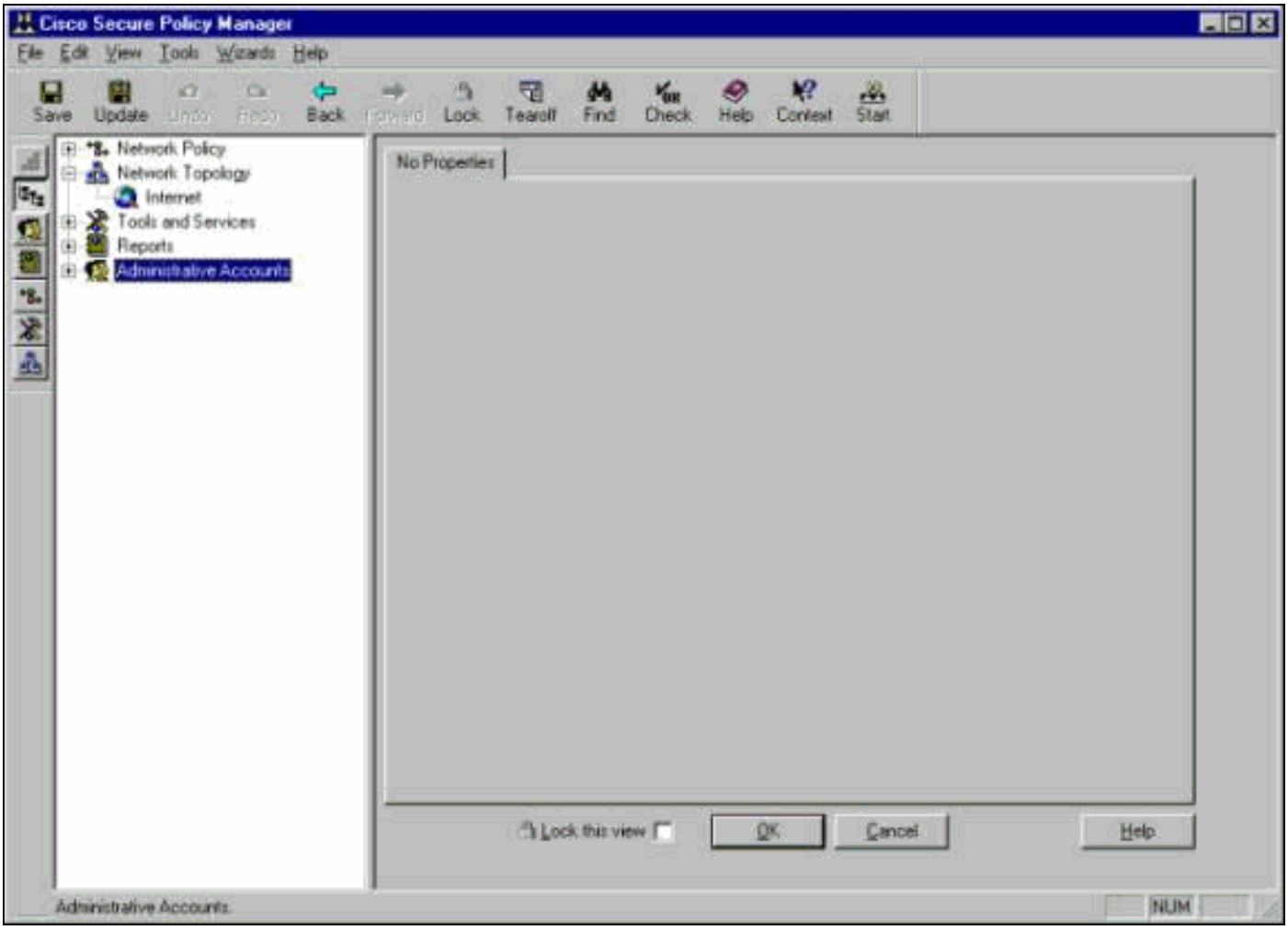
### 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

これらのセクションは CSPM の IDS センサを設定するのに使用されるプロセスを説明します。

起動 CSPM およびログイン。 初期起動で表示される空白のテンプレートに、ネットワークを定義します。



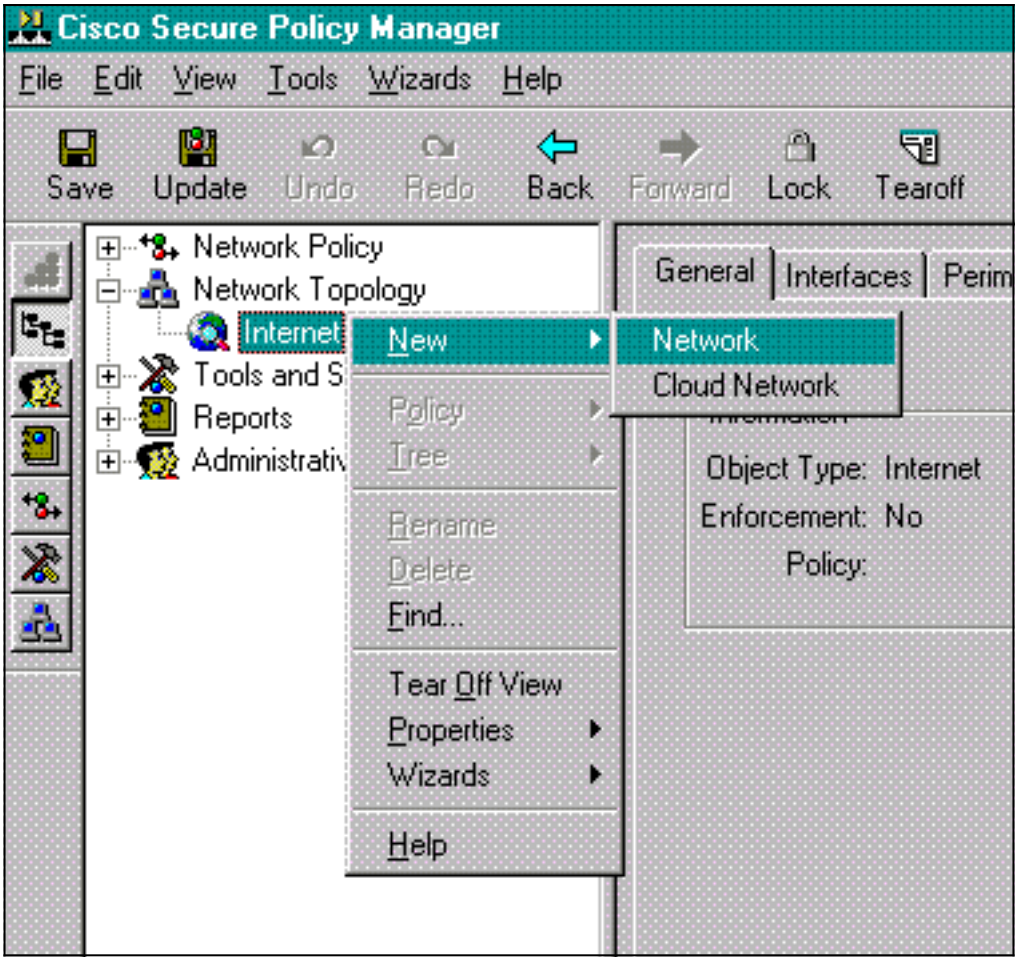

IDS に CSPM トポロジーにこの 3 つの定義が必要となります。

1. センサーの制御インターフェイスが存在するネットワーク、および CSPM ホストが常駐するネットワークの定義。 この 2 つが同じサブネットにある場合、定義する必要があるのは 1 つのネットワークだけです。 このネットワークを最初に定義します。
2. 最初に定義したネットワークでの CSPM ホストの定義。 CSPM ホストが定義されていないと、センサーは管理できません。
3. 定義したネットワークでのセンサーの定義。

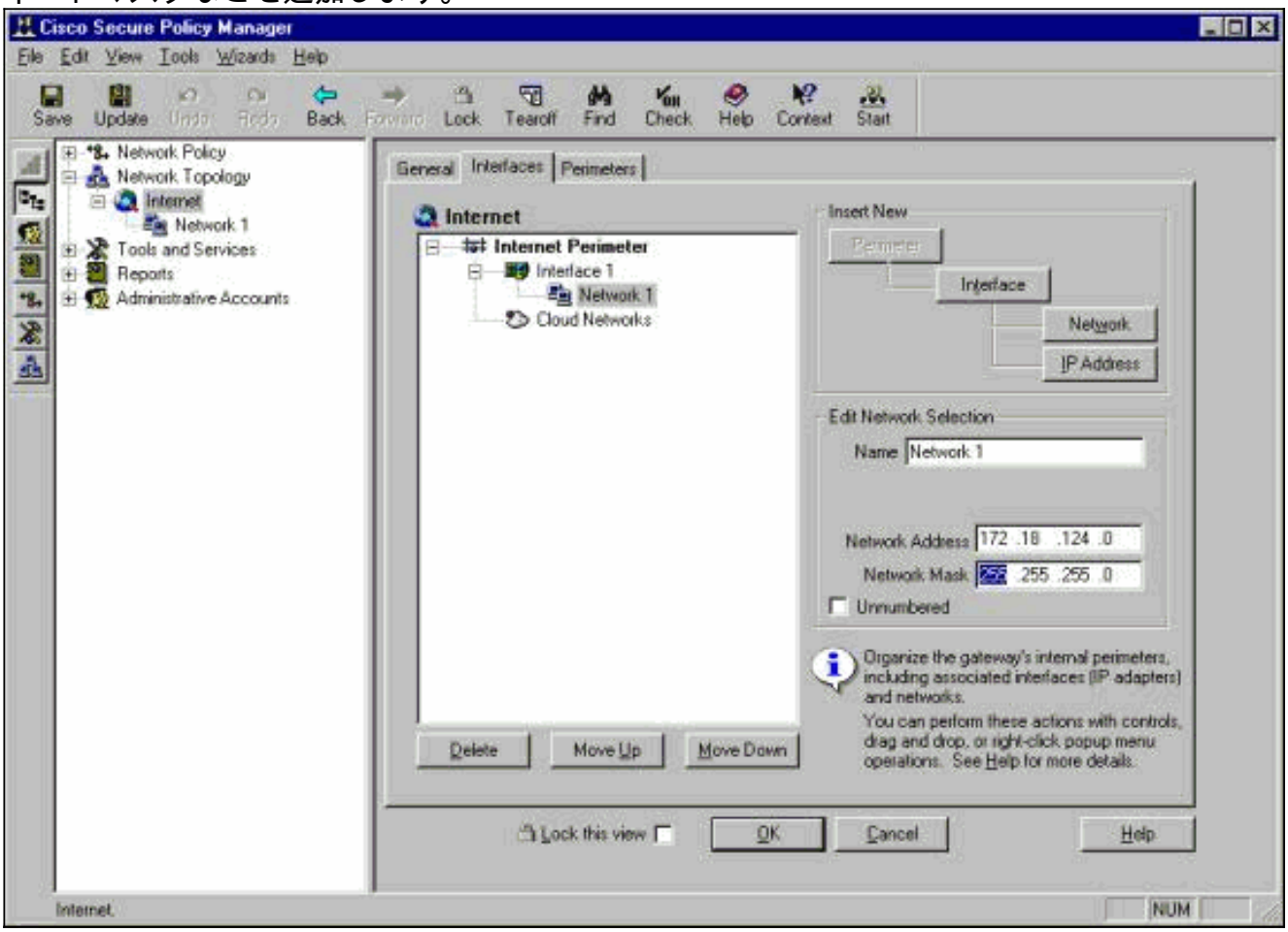
## CSPM ホストが常駐するネットワークの定義

次の手順を実行します。

1. トポロジの Internet アイコン上で右クリックして、New > Network 順に選択して新しいネットワークを作成します。



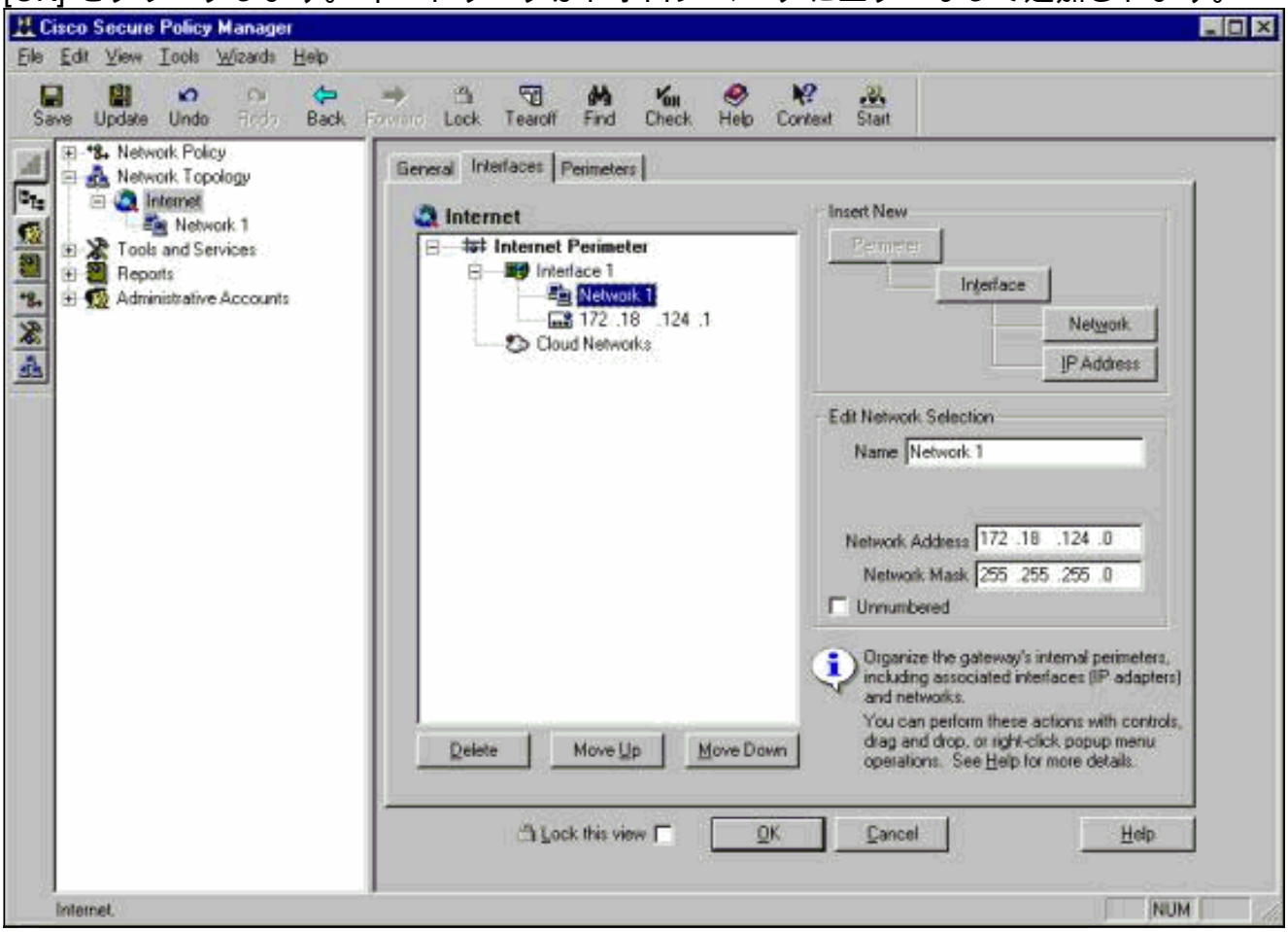

2. Network Panel の右側に、使用する新しいネットワーク名、ネットワーク アドレス、およびネットマスクなどを追加します。




3. IP Address ボタンをクリックし、インターネットに接続する際に使用するネットワークの

IP アドレスを入力します。通常は、ネットワークのデフォルト ゲートウェイを入力します。**注:** センサーを管理するとき、ゲートウェイアドレスは必ずしもセンサーがこのデフォルトゲートウェイ情報 送信 されないので正しくなくてもよろしくないです。 センサーにはすでにゲートウェイ アドレスが定義されています。

4. [OK] をクリックします。 ネットワークはトポロジ マップにエラーなしで追加されます。

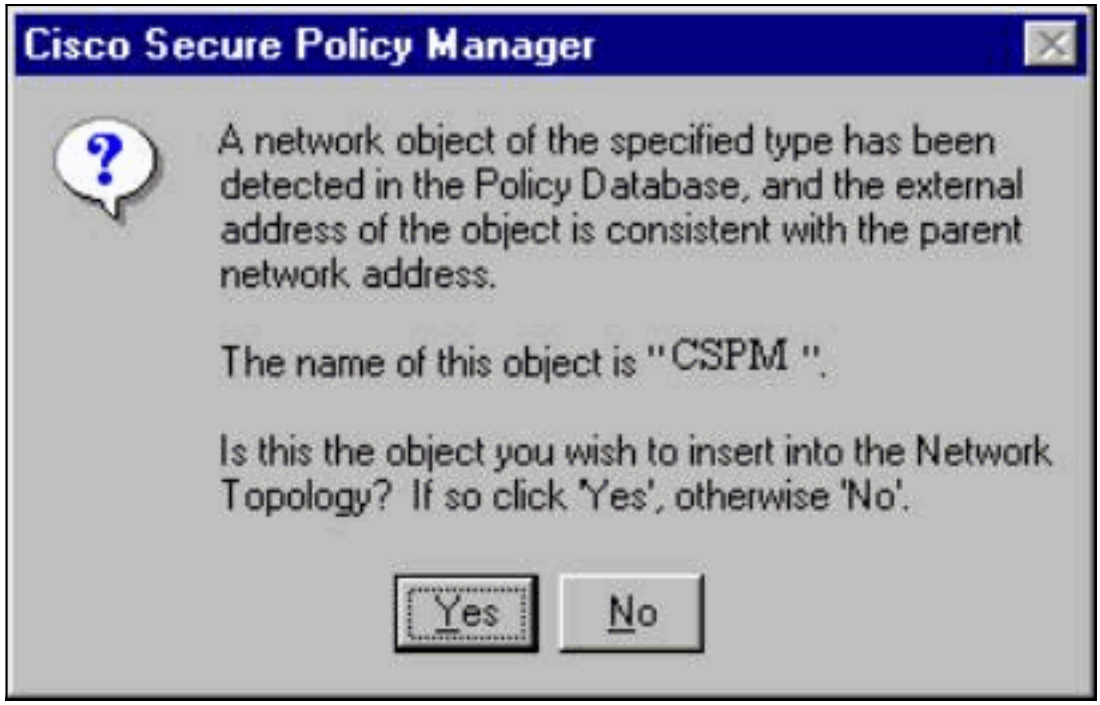



## CSPM ホストの追加

CSPM ホストを追加するのにこのプロシージャを使用して下さい。

1. Network Topology で、追加したネットワークを右クリックし、New > Host の順に選択します。CSPM はこれと同じような画面を表示します。 画面が表示されない場合は、定義したネットワークに CSPM ホストが見つかりません。 CSPM ホストの IP アドレスを再度チェ

ックします。

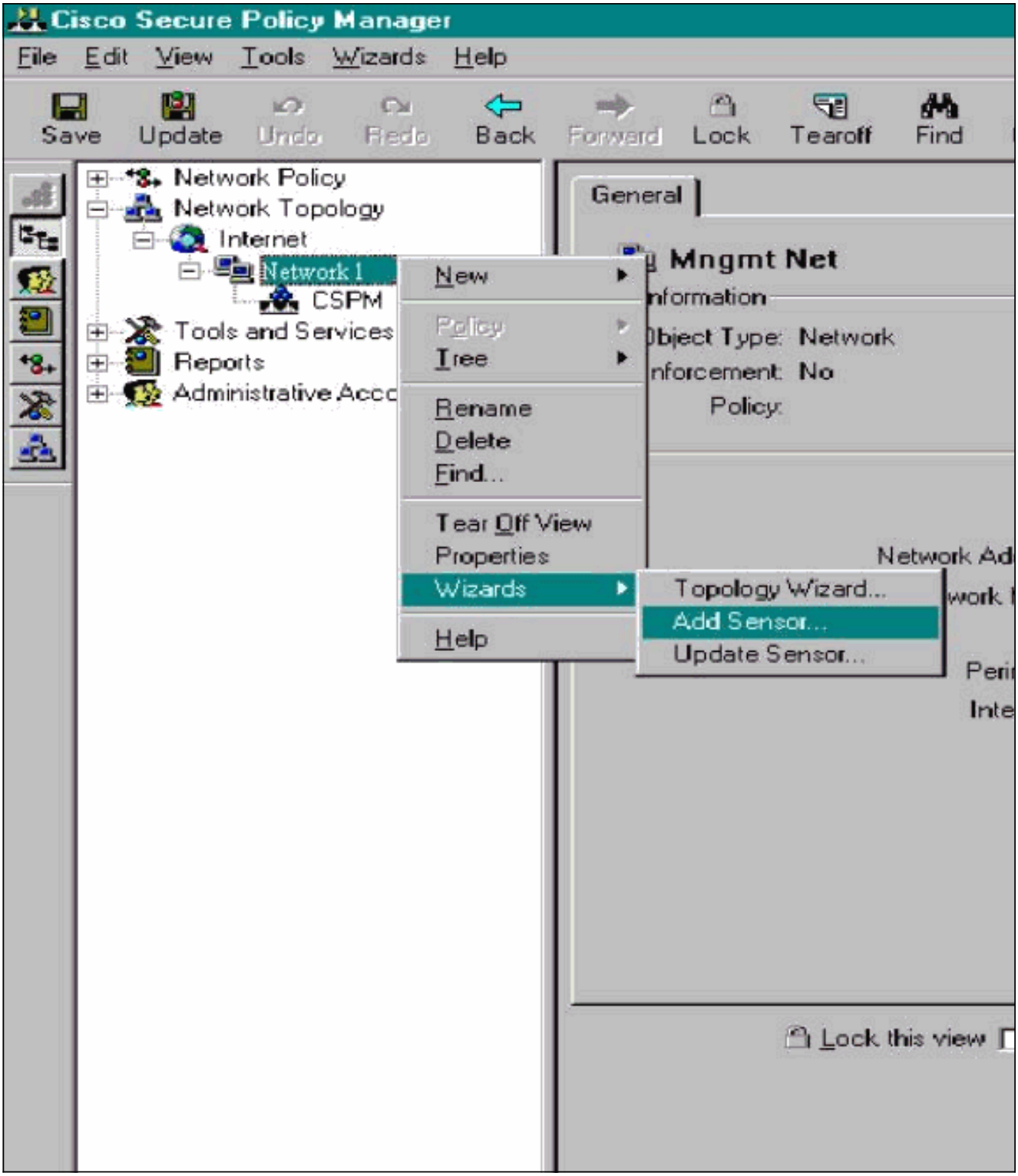



2. Yes をクリックして、トポロジに CSPM ホストをインストールします。
3. CSPM ホストの General 画面で情報が正しいことを確認します。
4. CSPM ホストの General 画面で OK をクリックします。

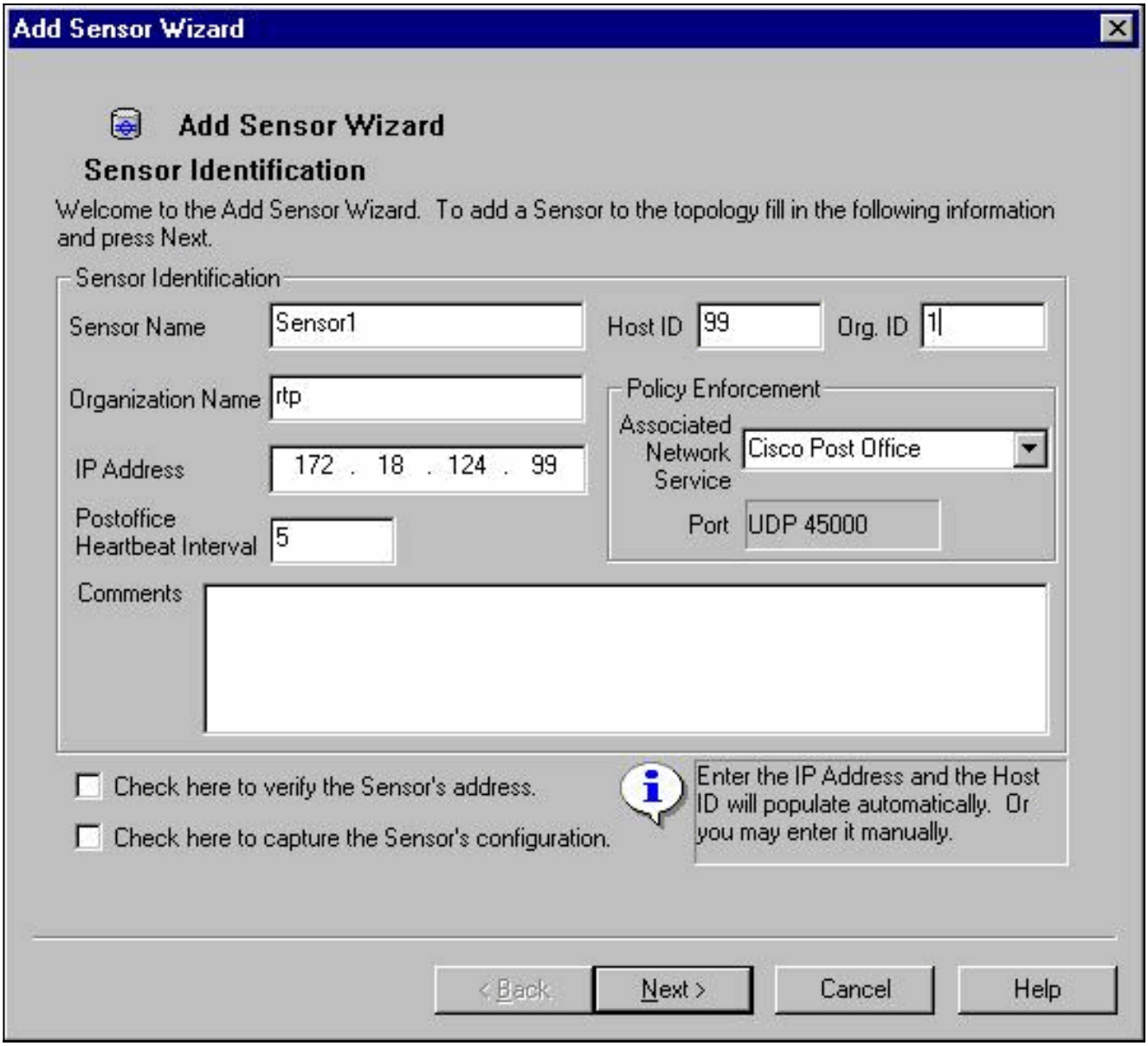
## センサー装置の追加

センサ デバイスを追加するのにこのプロシージャを使用して下さい。

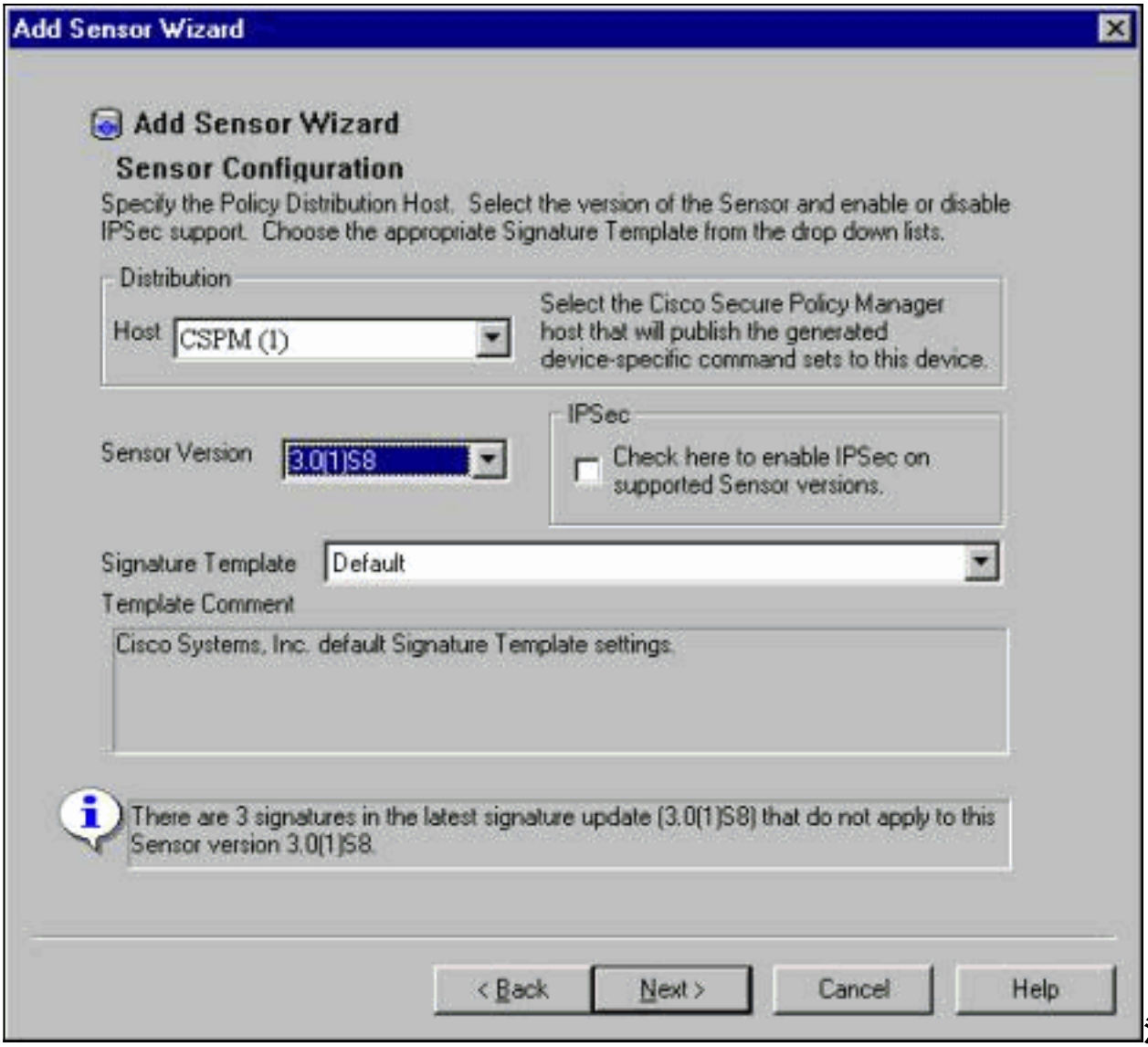
1. センサーが常駐する右クリックし、Wizards > Add Sensor の順に選択 して下さいネットワークを。**注:** センサーの CSPM ホストおよび制御 インタフェースが同じネットワークにない場合、センサーが常駐するネットワークを定義して下さい。




2. センサーの正しい postoffice パラメータを入力します。




3. Check here to verify the Sensor's address ボックスをクリックします。**注:** センサーを初めて設定するときは、センサーの設定は取り込みません。 センサーの設定を取り込むのは、UNIX ダイレクタまたは別の CSPM ホスト経由で、このセンサーに関する設定を以前に行ったものの、センサーのシグニチャに新たに設定変更を加えた場合です。
4. Next をクリックして、センサーのシグニチャ バージョンを定義します。 またセンサーでこれをチェックする **nrvers コマンドを**発行できます。




**注**: CSPM にセンサーで実行している正しいセンサ バージョンがなかったら、CSPM ホストのシグニチャをアップデートして下さい。 [更新の詳細は、「ソフトウェアのダウンロード」を参照してください。]

5. Next ボタンをクリックして、処理を続けます。
6. Finish をクリックして、トポロジへのセンサーのインストールを終了します。
7. CSPM のメイン メニューから、File > Save and Update の順に選択して、トポロジに入力した情報を CSPM にコンパイルします。 CSPM ホストで postoffice プロトコルを開始するには、このステップが必要であることに注意してください。
8. すべてが netrangr ユーザことをとしてセンサーにログイン することによってはたらくことを確認して下さい。
9. nrconns コマンドを実行します。`>`**`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 >` **注:** センサーおよび CSPM ホストが通信しない場合、これと同じような出力は代りに現われます:`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` これが事実である場合、両側が UDP 45000 パケットを送信 して いるかどうか見るためにスニファートレースを得て下さい。 UDP 45000 は、IDS 装置が相互に通信するときに使用するパケットです。 どんなセンサーが（によって）あるかこれを**スヌープを**定着させ、実行するためにセンサー、**SU** でテストするため**- d iprb1 ポート 45000**（IDS 4210 センサーのために）および**スヌーピングするため- d iprb0 ポート 45000**（センサーの他のどのモデルのためにも）。<control-c> を使用し

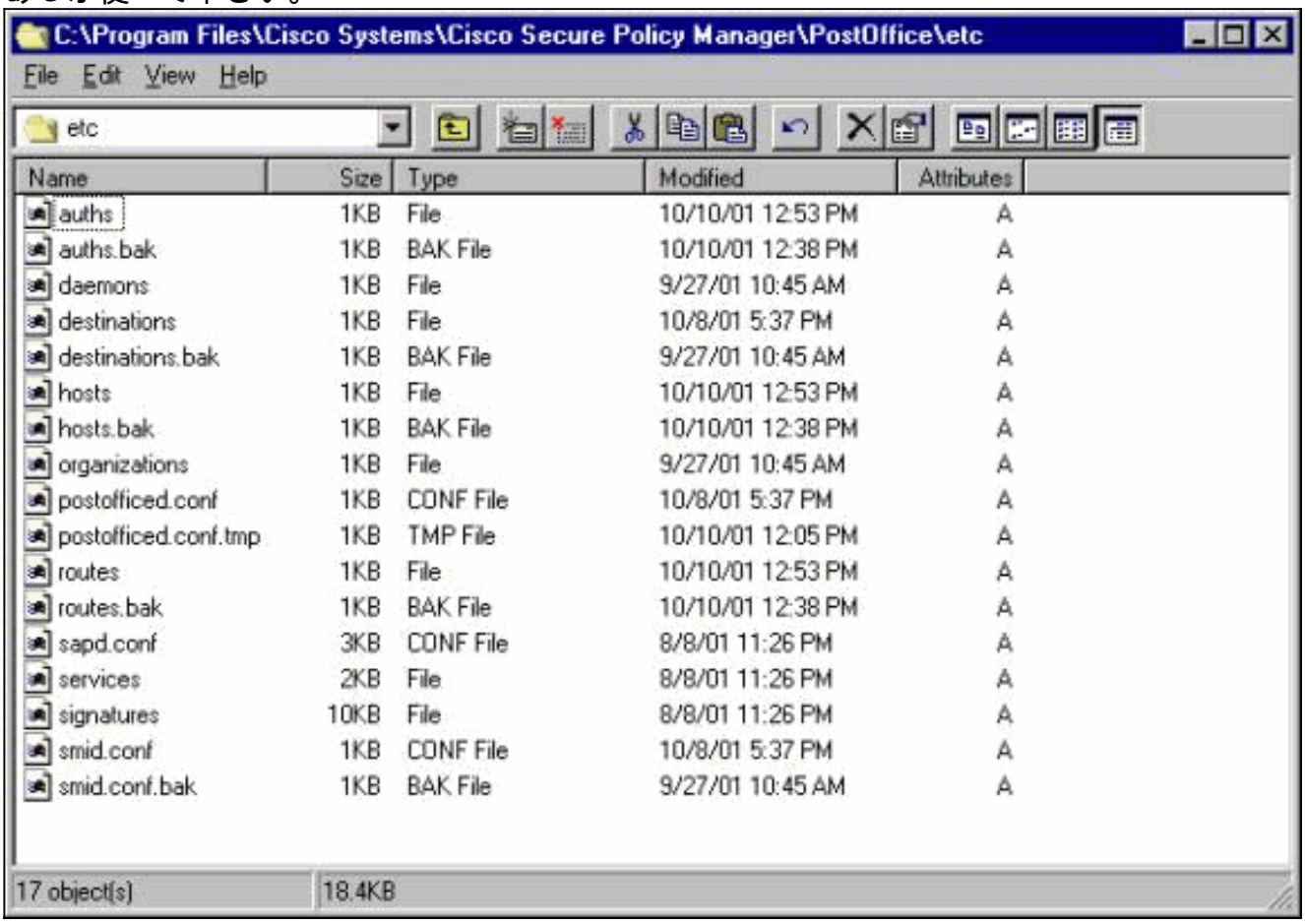
て、スヌープ セッションから抜け出します。この出力はセンサーと CSPM 間に通信がない場合現われます:netrangr@gacy:/usr/nr

```
>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#
```

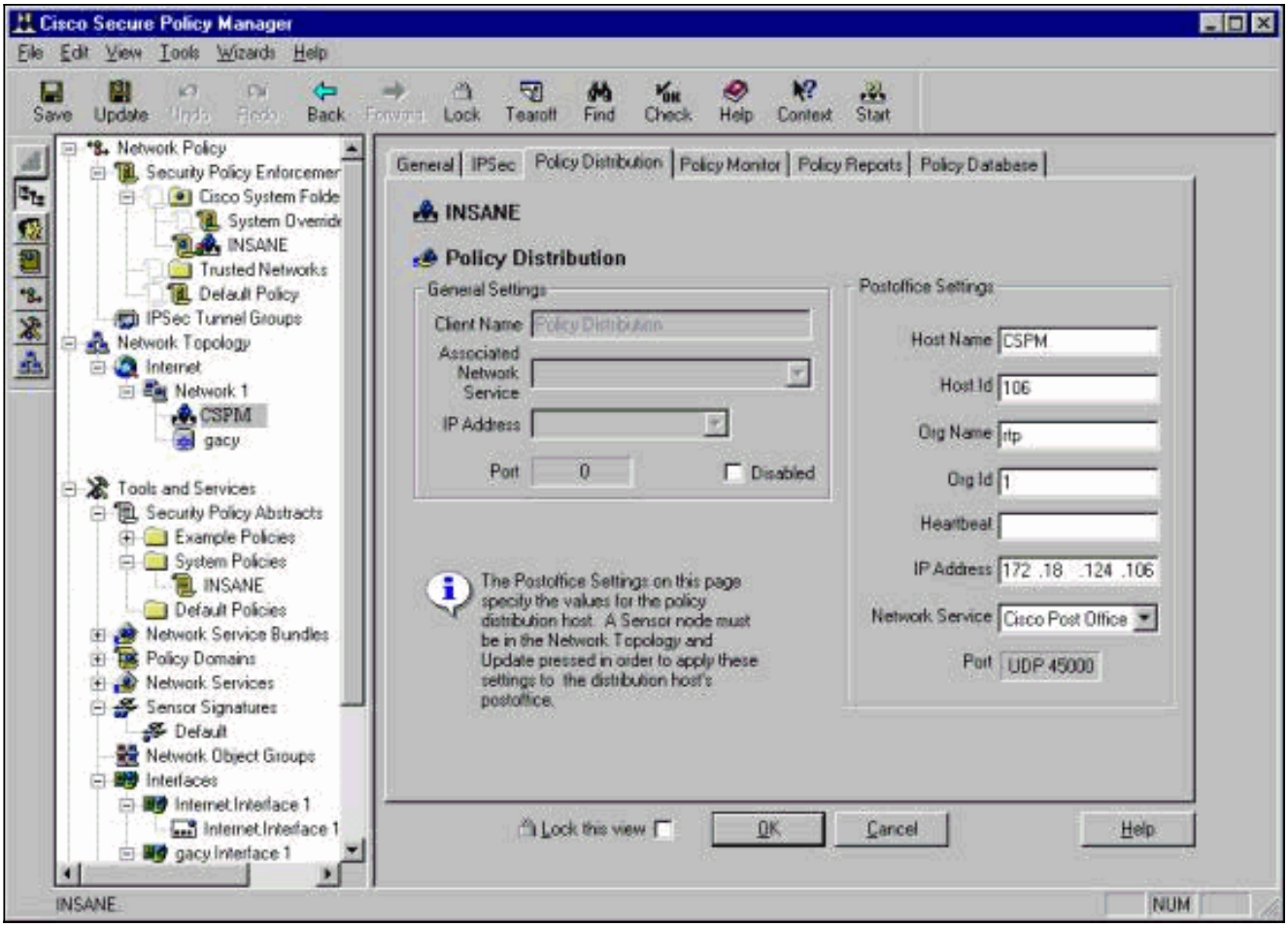
上記の出力では、センサー送信 UDP 45000 パケットは、しかし受け取りません。 正しい設定はこれと同じような出力を生成 します:

```
# 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
```

上記の出力では、UDP 45000 トラフィックは両方向で入ります。確立される接続がないと UDP 45000 パケットが両方向で流れればおよびセンサーの **nrconns** の出力がそれでも言えばセンサーのポストオフィス パラメータおよび CSPM ホストは一致する。CSPM ホストの postoffice パラメータを手作業でチェックするには、次の処理を実行します。ナビゲート するのに Windowsエクスプローラを NT搭載マシンでインストールされる CSPM がどこににあるか使って下さい。




ホストを、ルート編集すれば、フォーマッティングが破損しているので ) 学術団体資料はとのまたはワードパッド書きます ( Notepad を使用しないで下さい。これらのファイルが正しくインストールされていることを確認します。 値のうちのどれかが正しくない場合、それらを編集し、これらのステップを使用して NT コンピュータをリブートして下さい:Network Topology で CSPM アイコンをクリックします。Policy Distribution タブをクリックして、postoffice パラメータを入力します。変更を Save および Update します。NT コンピュータをリブートします。



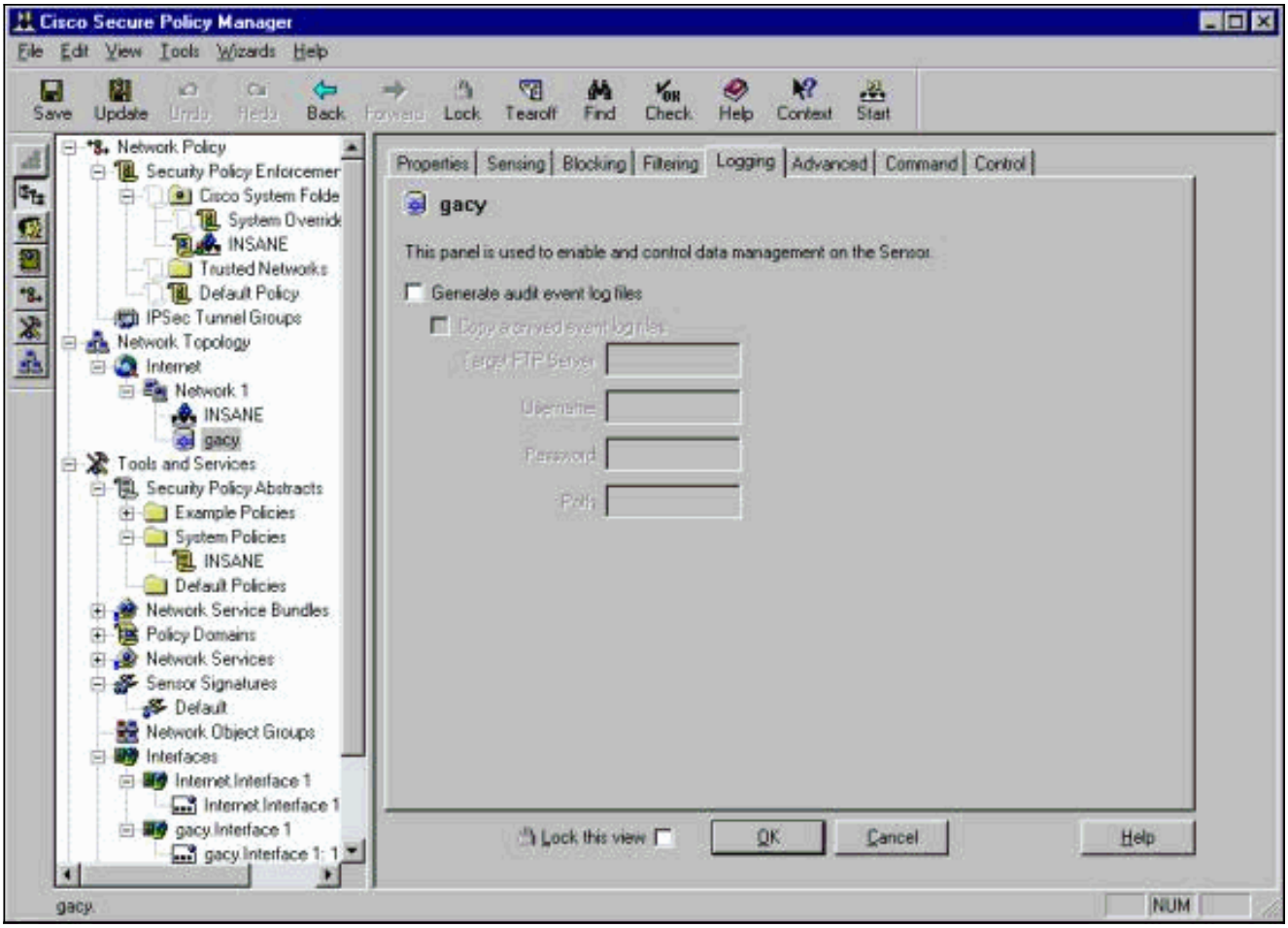

## Sensor の設定

CSPM に設定を保存したら、センサーを設定します。 これをするために、最初に自身のログに参照するアラームを書くためにセンサーを設定 して下さい。 それから正しいインターフェイスで」スニッフィングするためにセンサーを「設定 して下さい。

## ログへのアラームの書き込み

ログにアラームを書くのにこのプロシージャを使用して下さい。

1. Generate audit event log files ボックスをクリックし、アラームをローカル ログに送信するようにセンサーに指示を出します。それはまたデフォルトで CSPM ボックスにそれに設定を押下げた後アラームを送信 します。

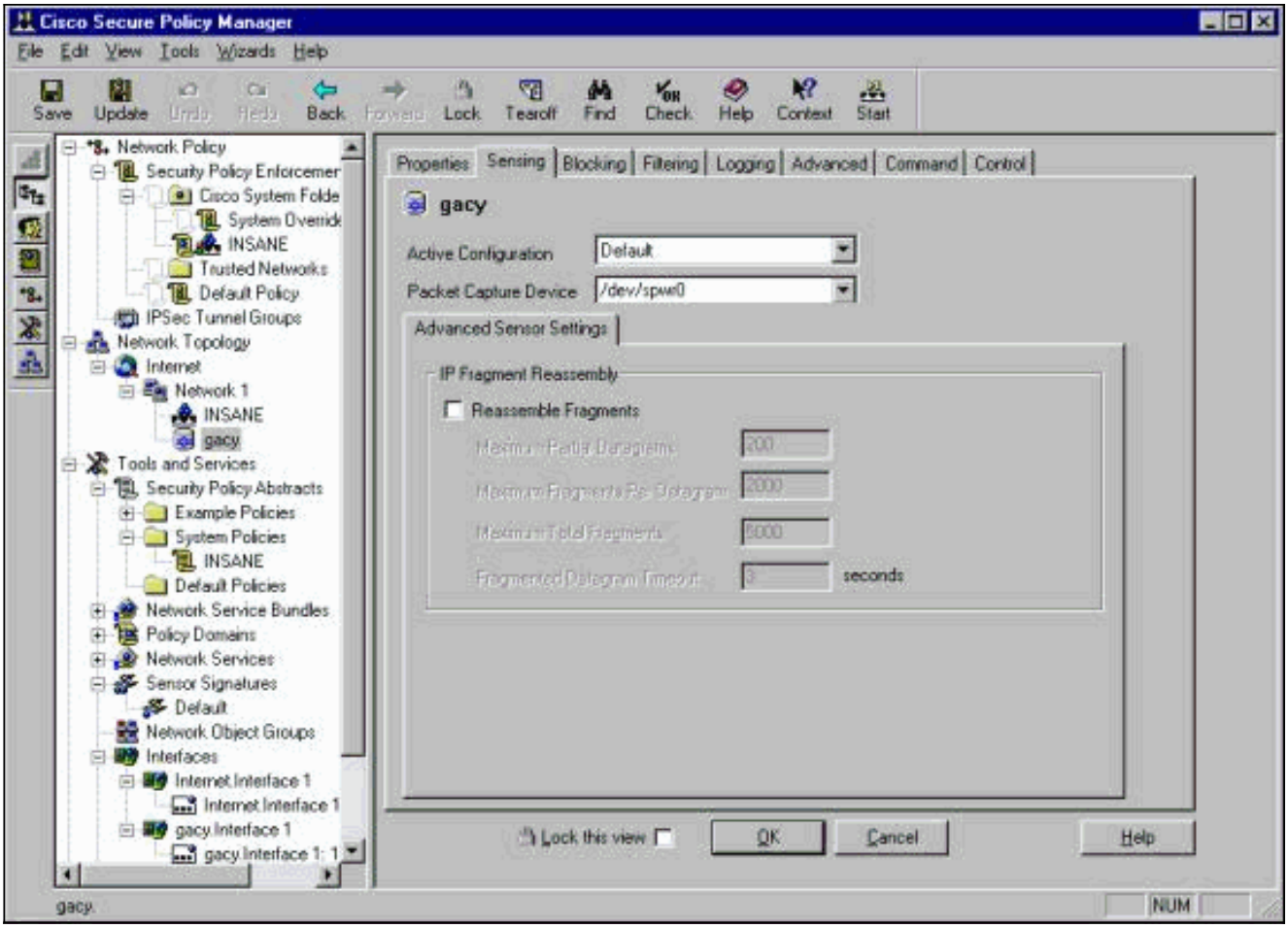



2. [OK] をクリックして、次に進みます。

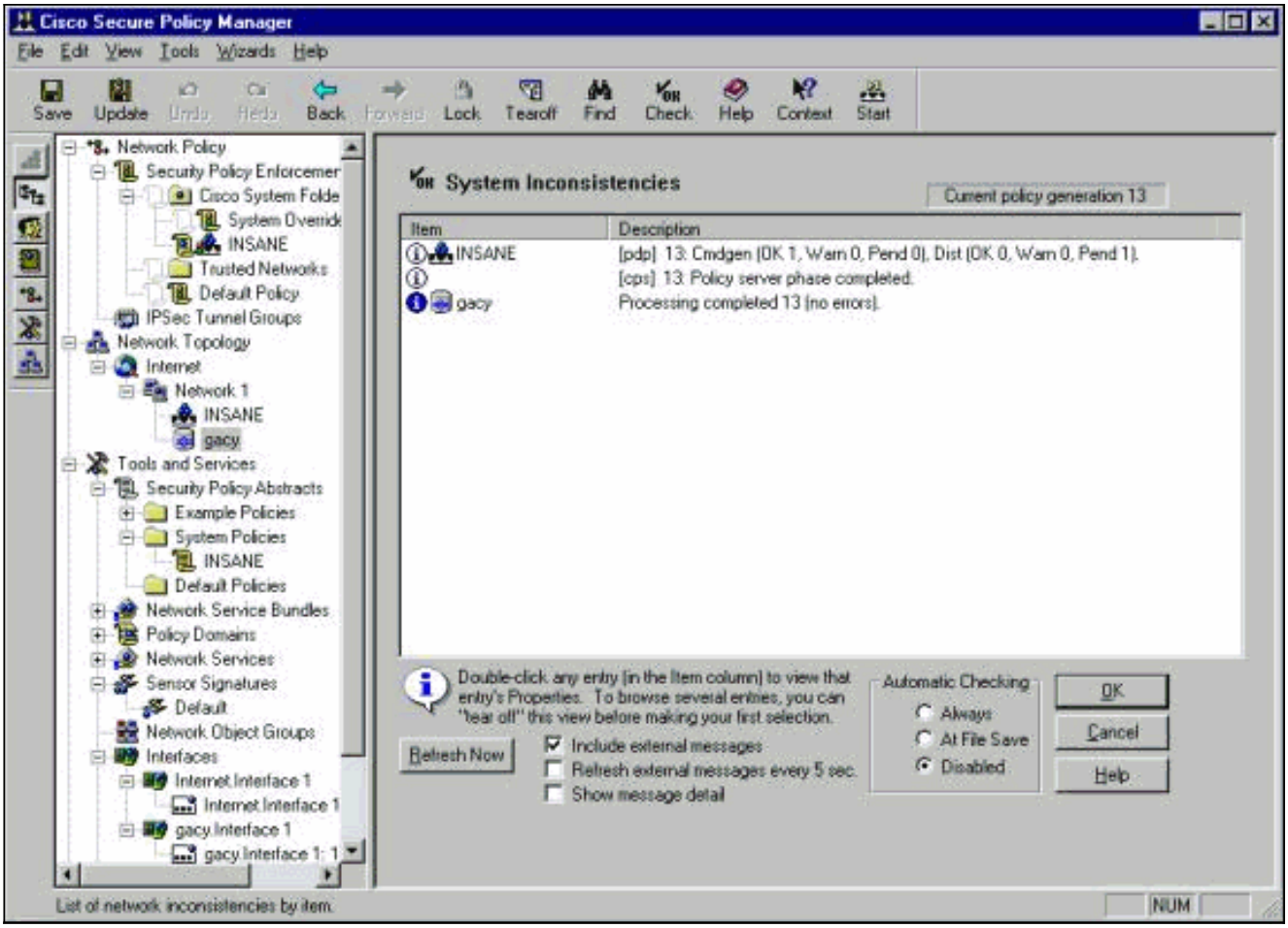
## センサーの「スニファ」への設定

センサーを」スニッフィングするために設定 するのにこのプロシージャを「使用して下さい。

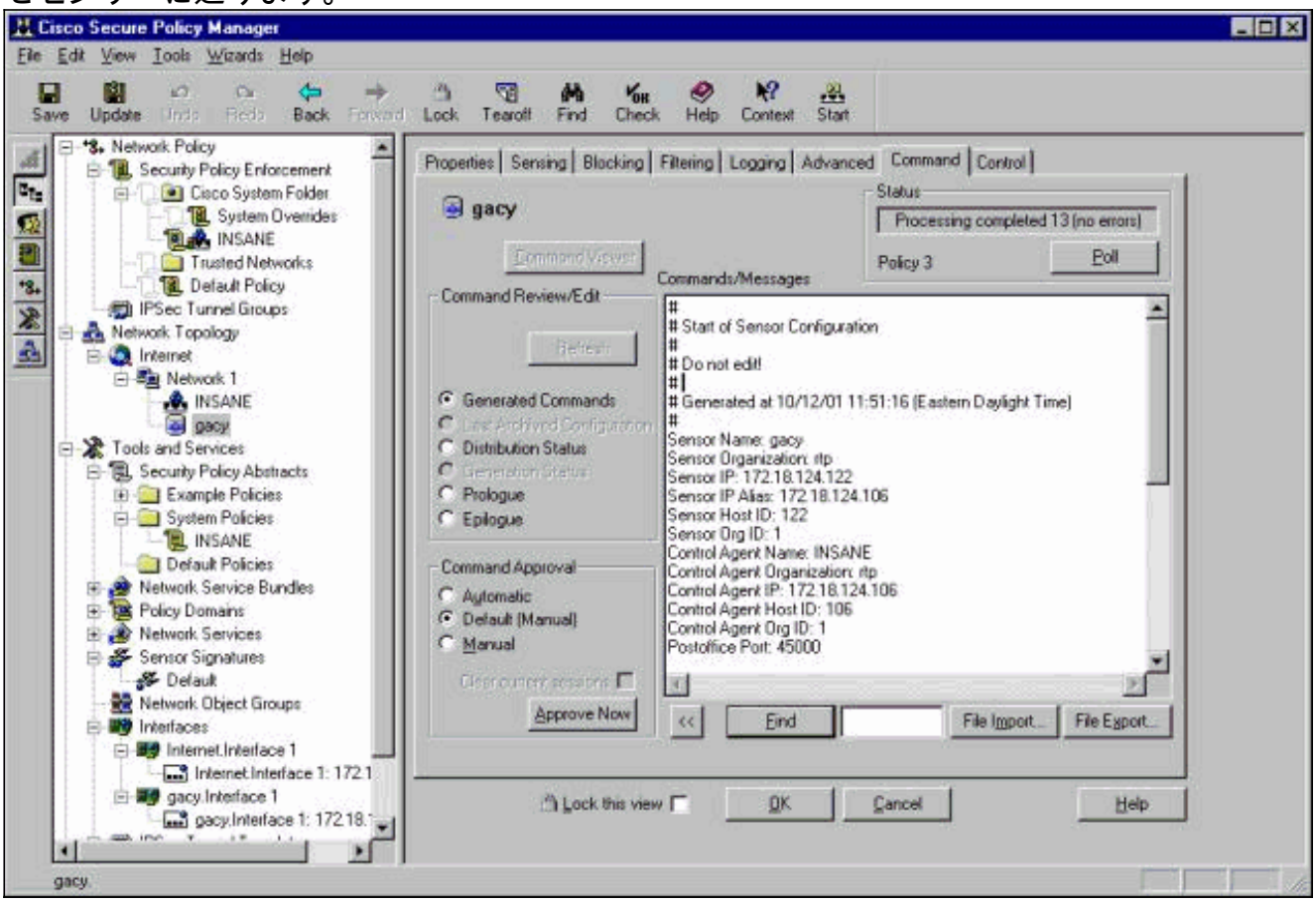
1. CSPM トポロジでセンサーを選択して、Sensing タブをクリックします。
2. 次のように Packet Capture Device を定義します。iprb0 - IDS 4210 センサーのための
   …spwr0 -他のセンサー モデルのための
   …



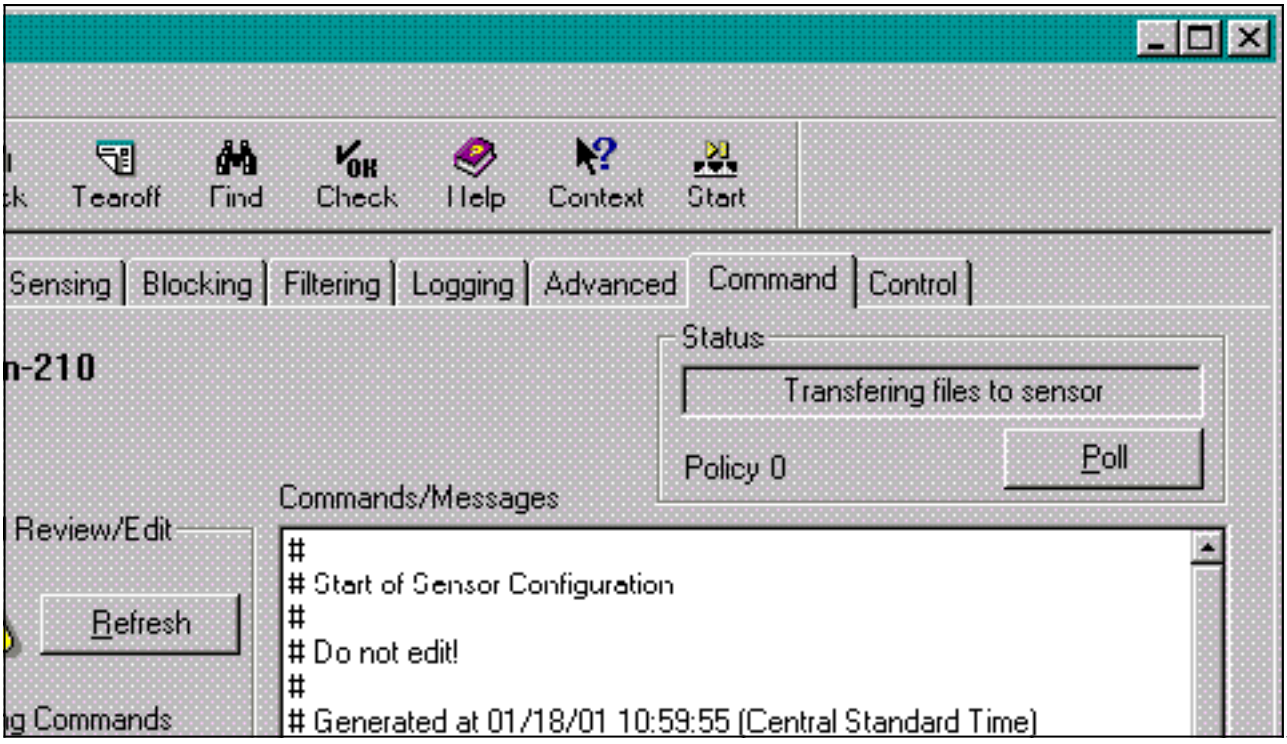

3. [OK] をクリックして、次に進みます。
4. CSPM メニュー バー上で Update アイコンをクリックし、CSPM の情報を更新します。**注**：すべてがうまくいく場合、これと同じような画面は現われます。 赤字のエラーがないことに注意してください。 黄色い警告は通常は心配ありません。



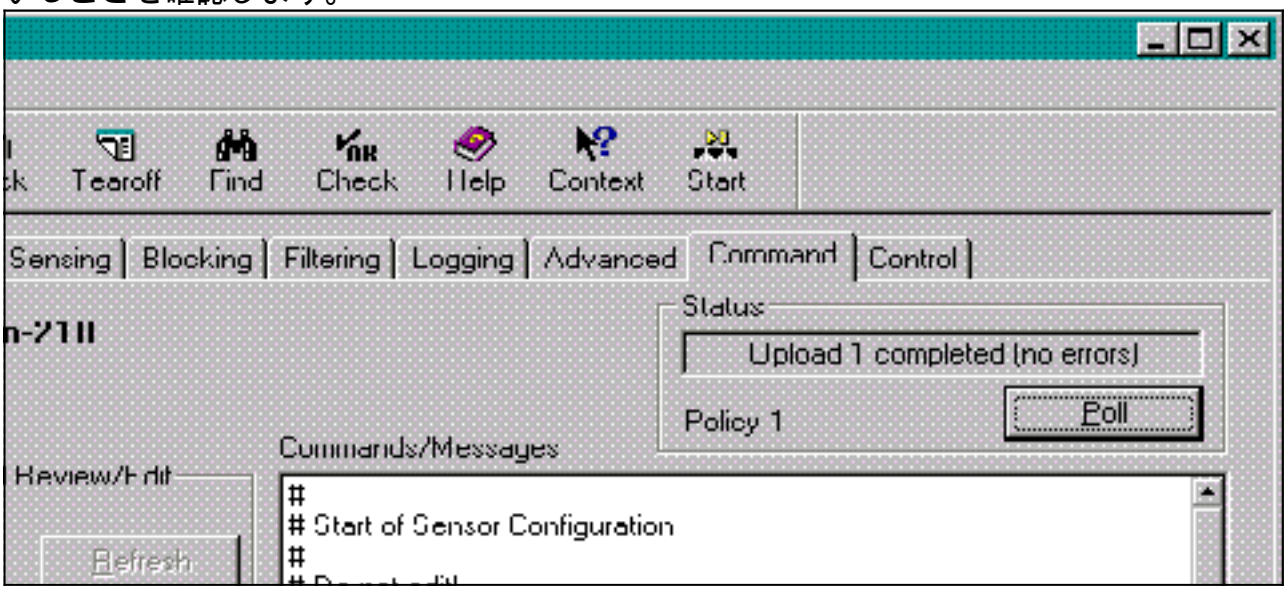

5. Network Topology でセンサーを選択したら、Command タブをクリックして、更新した設定をセンサーに送ります。



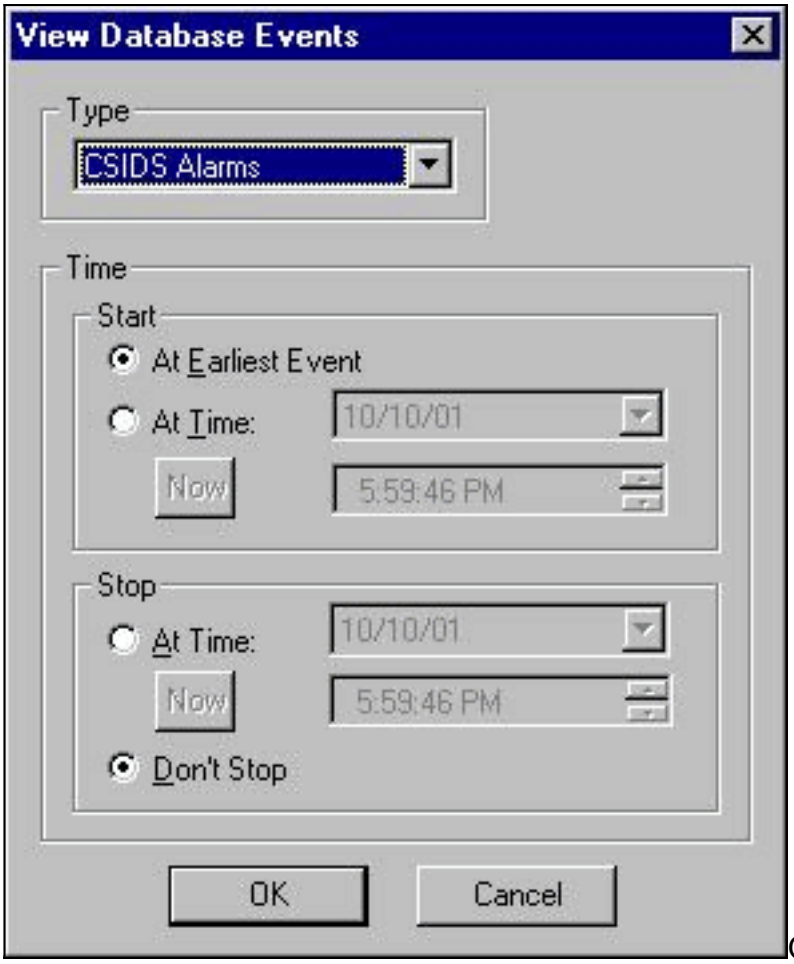

6. センサーに設定を送信 するために **Approve Now ボタンを**クリックして下さい。



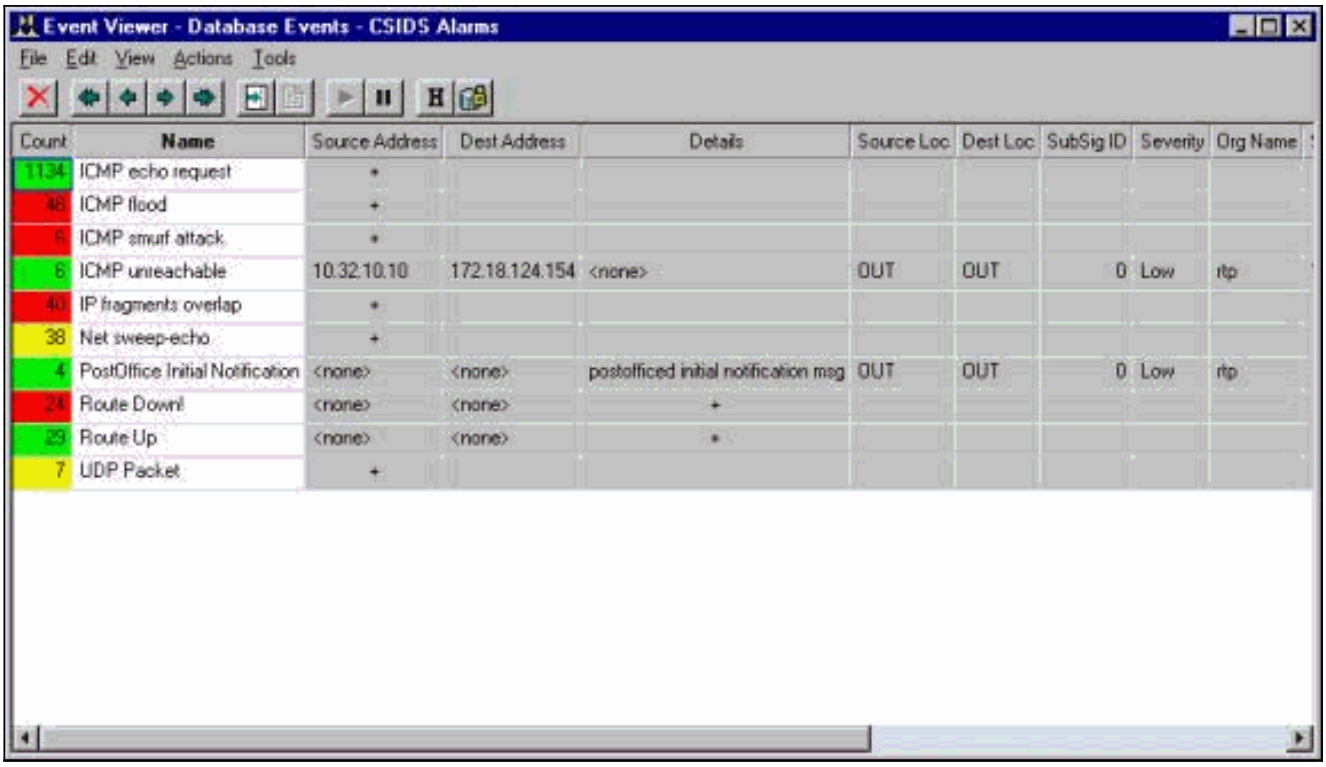
ステータス バー ペインは「アップロード <#> によって完了される」メッセージを表示する。これは有効なを示し、転送プロセスを完了します。 センサーは今今アップデートされ、正常に動作する必要があります。センサーが正常に動作しないときは、センサーに戻り、nrconns コマンドの出力結果をチェックし、CSPM ホストとセンサーの間に接続が確立していることを確認します。



この処理が終了したら、センサーが CSPM ホストに送信するアラームを Event Viewer で探すことができます。 CSPM メインメニューからのイベント ビューアを、表示することは > **ビュー センサー イベント > データベース** 『Tools』 を選択 します。



OK をクリックして、Events Database ウィンドウを表示します。 画面は得るかもしれないアラームによって変わります。




## 関連情報

- テクニカルサポートとドキュメント - Cisco Systems