Configurazione di un sensore Cisco Secure IDS in CSPM

Sommario

Introduzione

Questo documento spiega la procedura utilizzata per configurare un sensore Cisco Secure Intrusion Detection System (IDS) su Cisco Secure Policy Manager (CSPM). in questo documento si presume che CSPM versione 2.3.I sia stato installato nel computer. La versione "I" consente la gestione di dispositivi IDS (sensori di appliance, router Cisco IOS® o blade IDS) in uno switch Cisco Catalyst® 6000. Nel documento si presume inoltre che i parametri IDS relativi agli uffici postali siano definiti correttamente. Questi includono HOSTID, ORGID, HOSTNAME e ORGNAME. Notare che affinché l'host CSPM comunichi con un sensore, ORGID e ORGNAME devono corrispondere a quanto definito sul sensore.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su CSPM 2.3.I e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

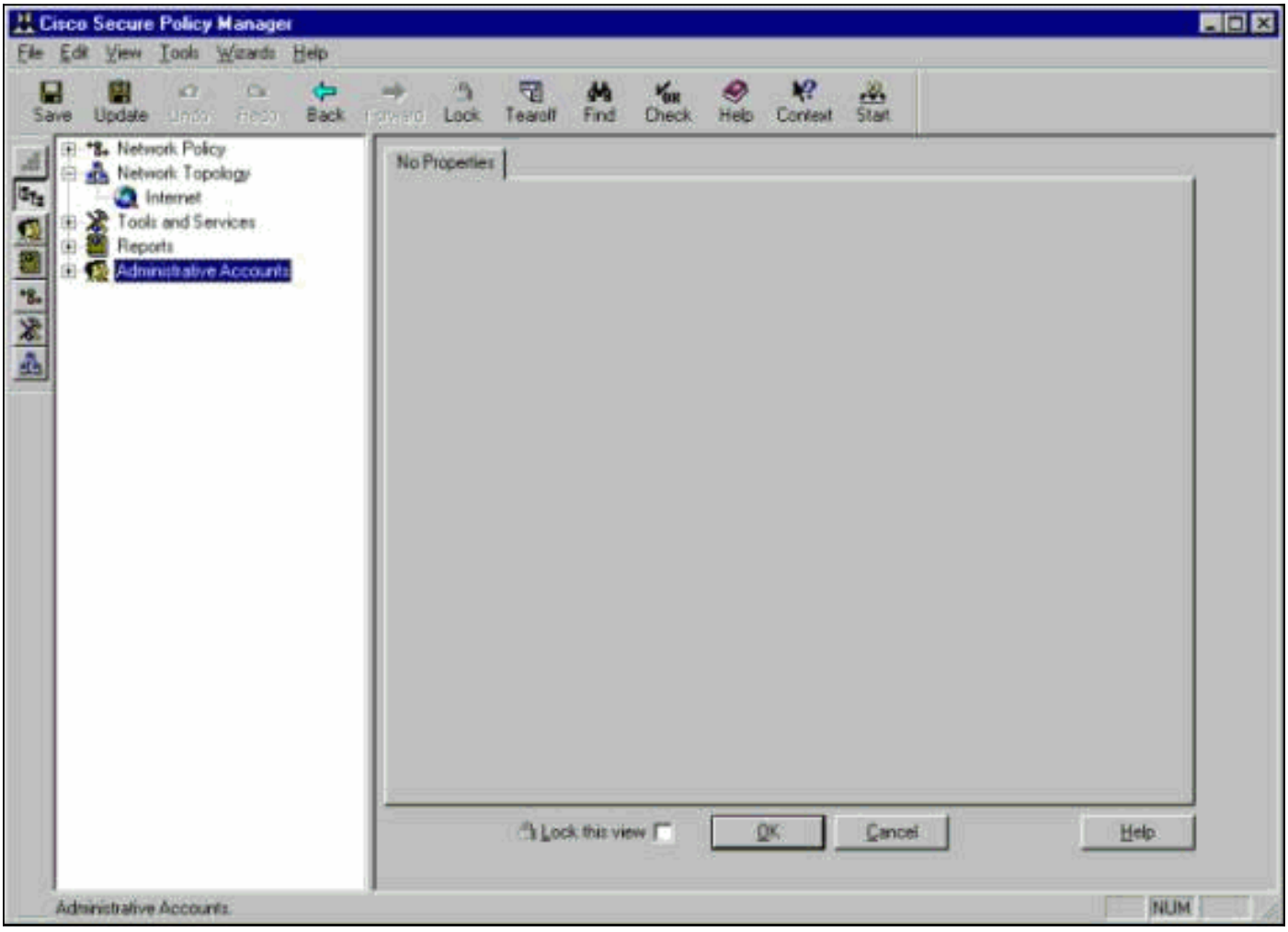
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

Nelle sezioni seguenti viene illustrato il processo utilizzato per configurare un sensore IDS in CSPM.

Avviare CSPM e accedere. Viene visualizzato un modello vuoto (avvio iniziale) che consente di definire la rete.



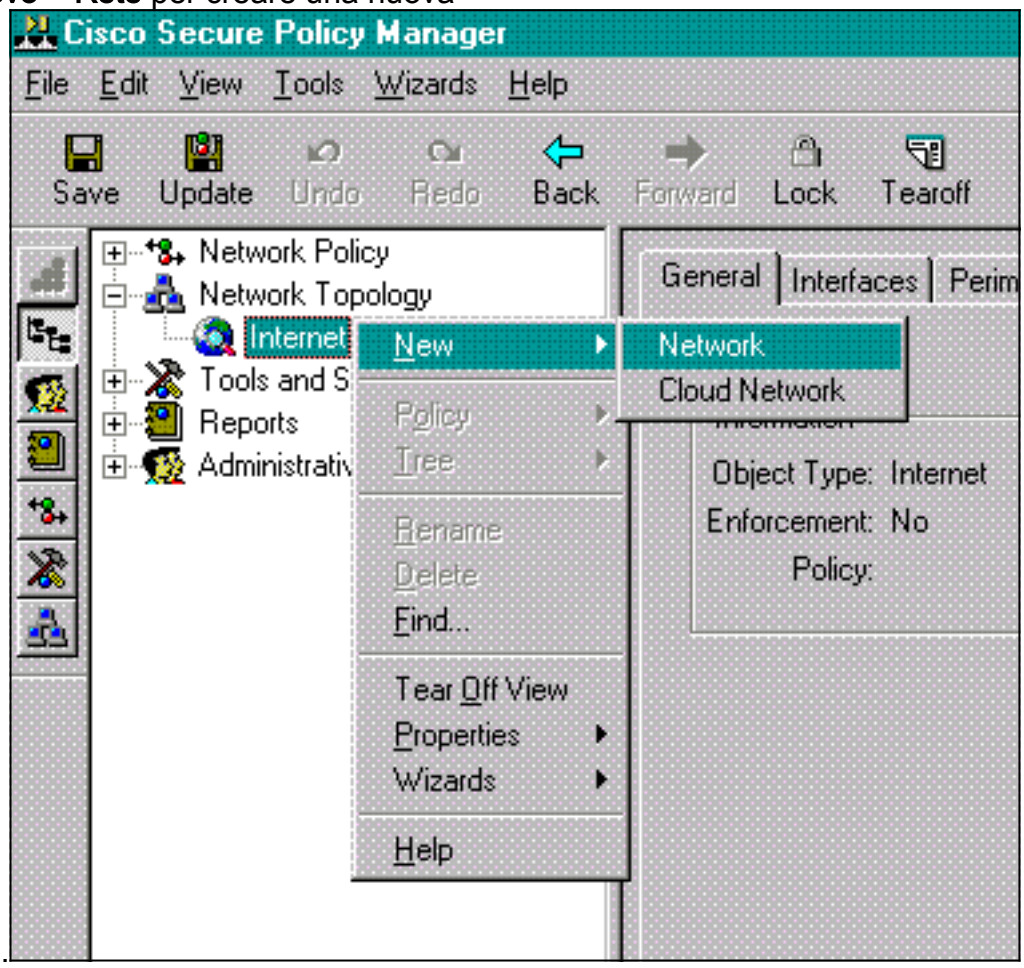
Queste tre definizioni sono richieste nella topologia CSPM per IDS.

1. Definire la rete in cui risiede l'interfaccia di controllo del sensore e la rete in cui risiede l'host CSPM. Se si trovano nella stessa subnet, è necessario definire una sola rete. Definire prima questa rete.
2. Definire l'host CSPM nella relativa rete. Senza la definizione dell'host CSPM, il sensore non può essere gestito.
3. Definire il sensore nella rete.

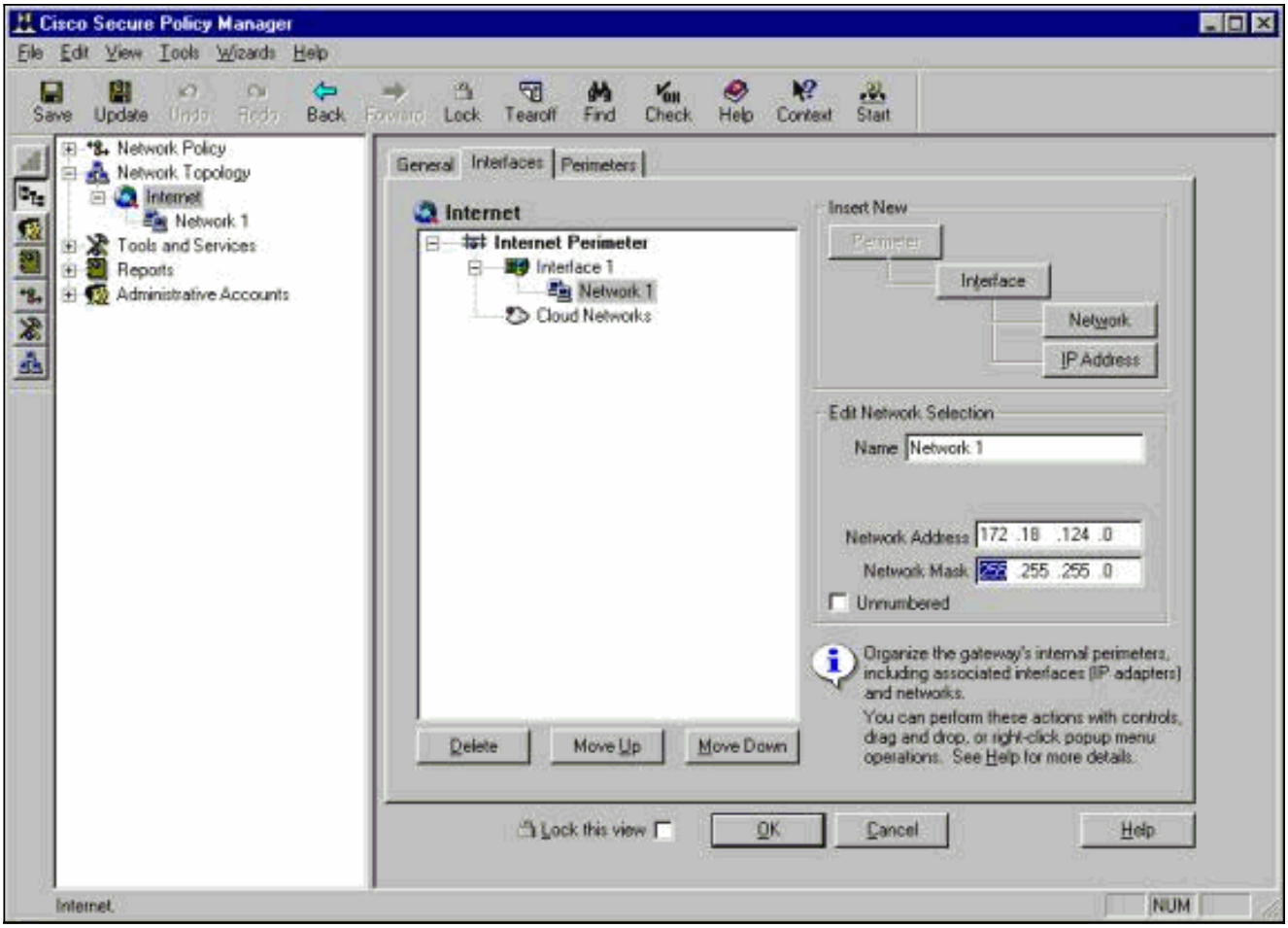
Definizione della rete in cui risiede l'host CSPM

Attenersi alla seguente procedura:

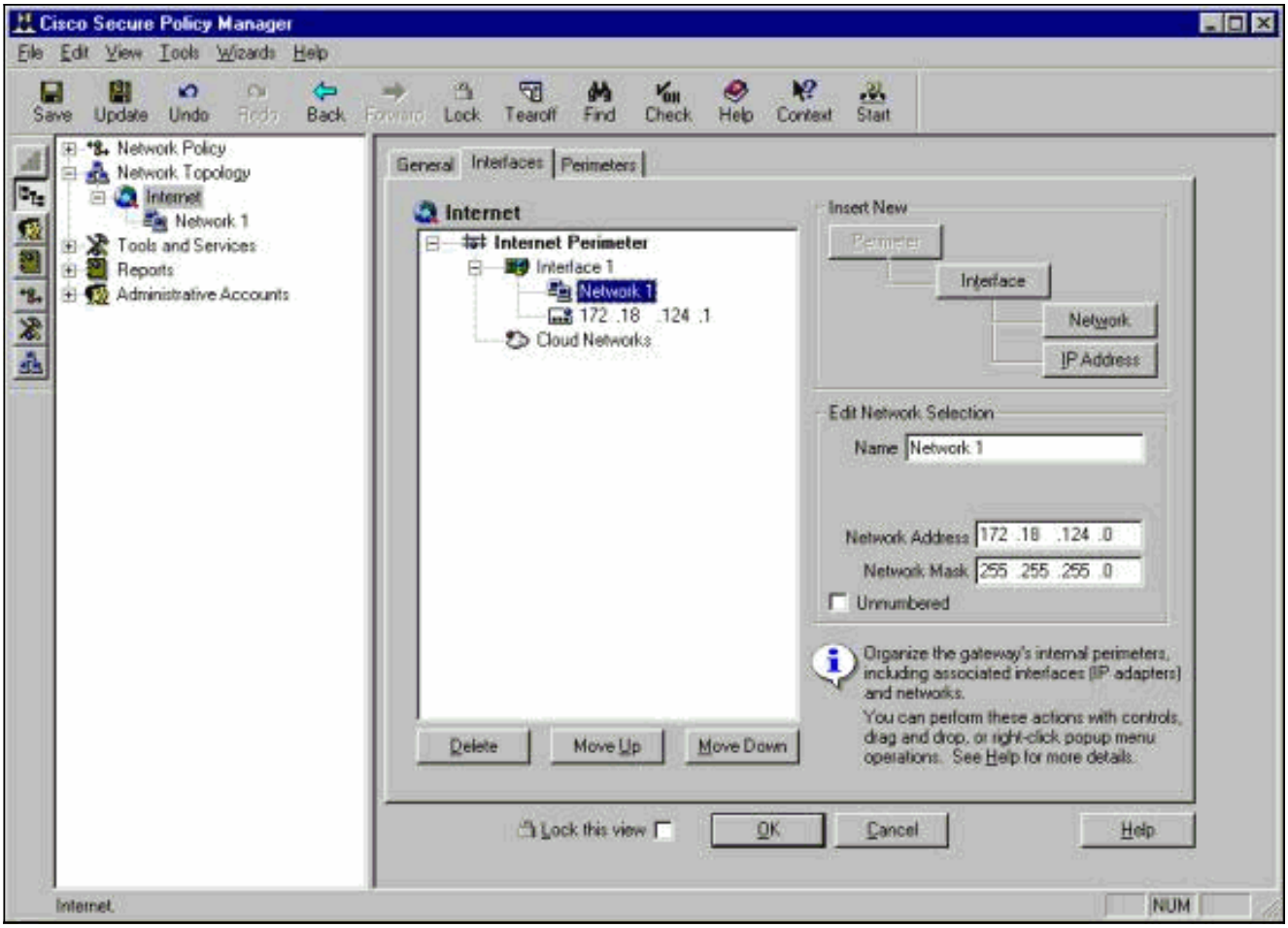
1. Fare clic con il pulsante destro del mouse sull'icona **Internet** nella topologia e selezionare **Nuovo** > **Rete** per creare una nuova rete.



2. Sul lato destro del pannello Rete, aggiungere il nome della nuova rete, l'indirizzo di rete e la netmask che verrà
utilizzata.



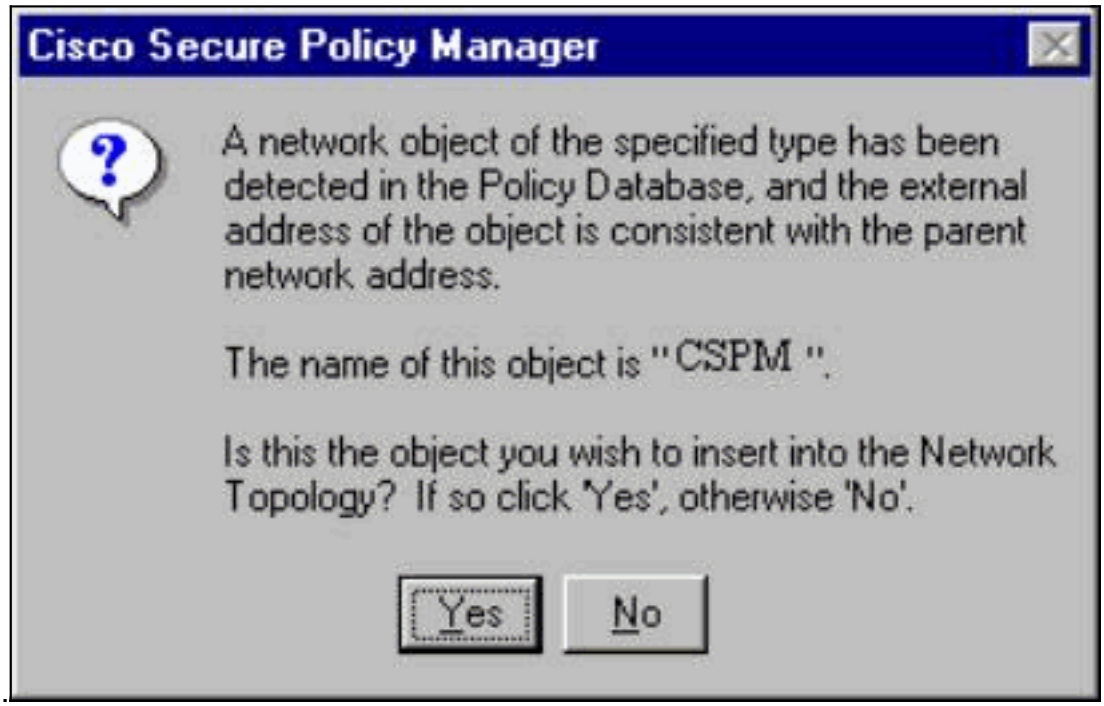
3. Fare clic sul pulsante **Indirizzo IP** e immettere l'indirizzo IP della rete utilizzato per raggiungere Internet.In genere si tratta del gateway predefinito per la rete.**Nota:** quando si gestiscono i sensori, l'indirizzo del gateway non deve essere necessariamente corretto, in quanto al sensore non vengono inviate le informazioni sul gateway predefinito. Dovrebbe già essere definita nel Sensore.
4. Fare clic su **OK**. La rete viene aggiunta alla mappa della topologia senza errori.



Aggiungere l'host CSPM

Utilizzare questa procedura per aggiungere l'host CSPM.

1. Nella Topologia di rete, fare clic con il pulsante destro del mouse sulla rete appena aggiunta e selezionare **Nuovo > Host**.CSPM visualizza una schermata simile a questa. In caso contrario, la rete appena definita non è quella in cui si trova l'host CSPM. Controllare nuovamente l'indirizzo IP sull'host CSPM.

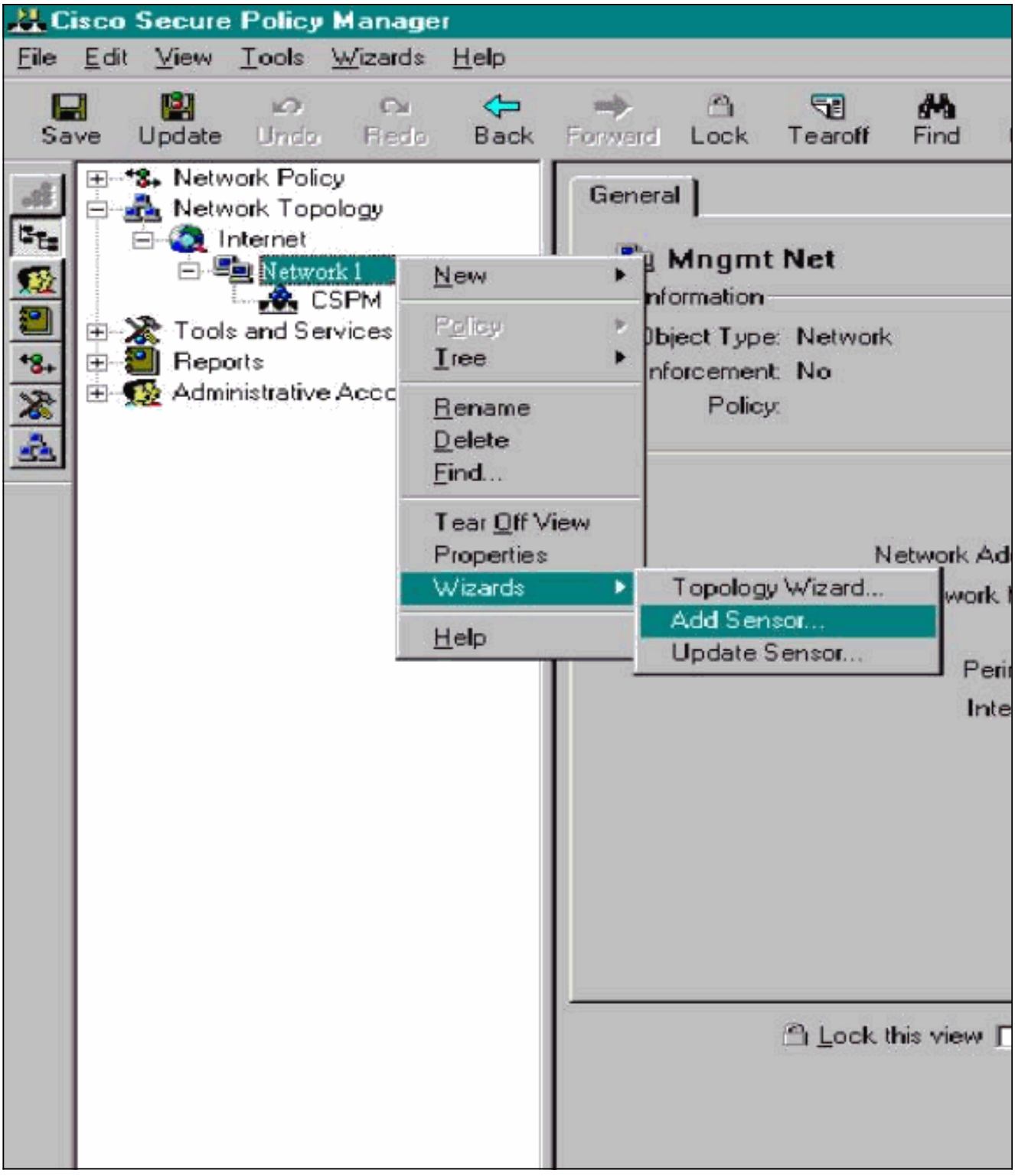


2. Fare clic su **Sì** per installare l'host CSPM nella topologia.
3. Verificare che le informazioni nella schermata Generale per l'host CSPM siano corrette.
4. Fare clic su **OK** nella schermata Generale dell'host CSPM.

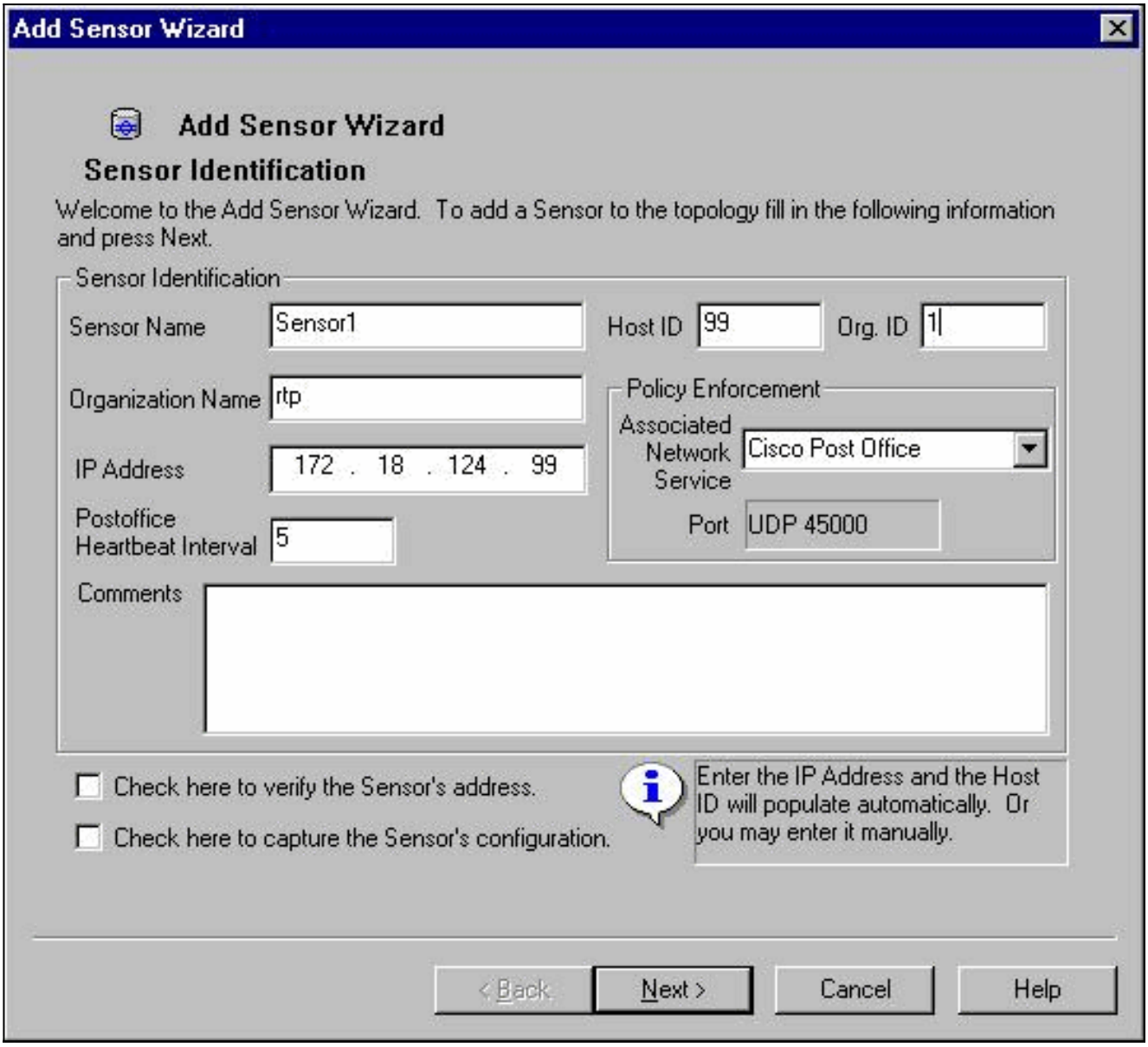
Aggiungi dispositivo sensore

Utilizzare questa procedura per aggiungere la periferica sensore.

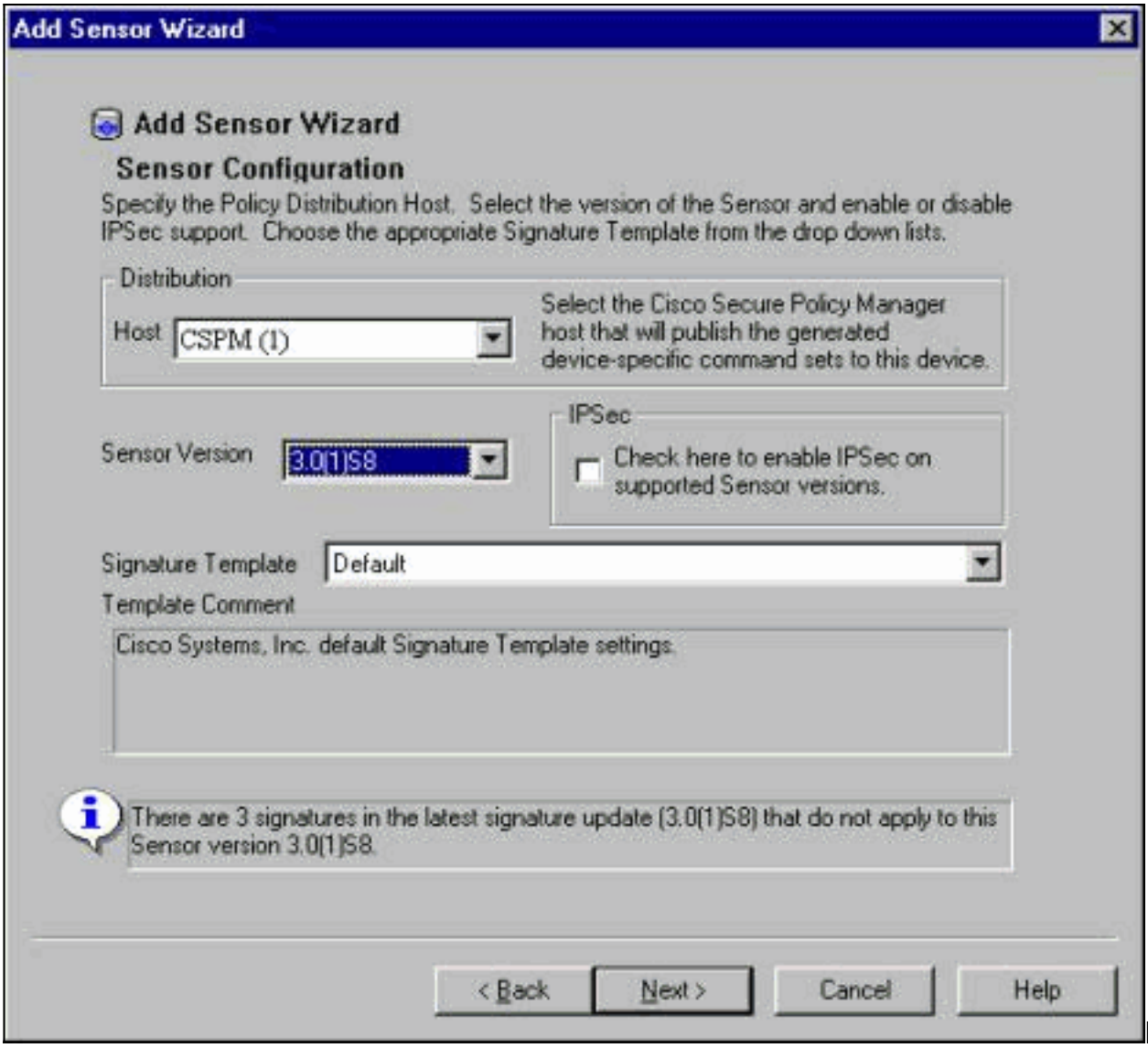
1. Fare clic con il pulsante destro del mouse sulla rete in cui risiede il sensore e selezionare **Procedure guidate > Aggiungi sensore**.**Nota:** se l'host CSPM e l'interfaccia di controllo del sensore non si trovano nella stessa rete, definire la rete in cui risiede il sensore.



2. Immettere i parametri corretti per il sensore.



3. Fare clic su **Controlla qui per verificare l'indirizzo del sensore** nella casella.**Nota:** se è la prima volta che si configura questo sensore, non si desidera acquisire la configurazione del sensore. Se il sensore è stato precedentemente configurato in un'altra posizione tramite un director UNIX o un altro host CSPM e sono state apportate modifiche alla configurazione delle firme dei sensori, acquisire la configurazione del sensore.
4. Fare clic su **Avanti** per definire le versioni della firma sul sensore. Per verificare questa condizione sul sensore, è possibile anche usare il comando **nrvers**.



Nota: se CSPM non dispone della versione corretta del sensore in esecuzione sul sensore, aggiornare le firme sull'host CSPM. Per gli aggiornamenti, vedere Download del software (solo utenti registrati).

5. Per continuare, fare clic sul pulsante **Avanti**.
6. Fare clic su **Fine** per completare l'installazione del sensore nella topologia.
7. Dal menu principale di CSPM, selezionare **File > Salva** e **Aggiorna** per compilare in CSPM le informazioni immesse nella topologia. Questo passaggio è necessario per avviare il protocollo dell'ufficio postale sull'host CSPM.
8. Verificare che tutto funzioni accedendo al sensore come utente netranger.
9. Eseguire il comando **nrconns**.

```
>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

>
```

Nota: se il sensore e l'host CSPM non comunicano, viene visualizzato un output simile a questo:

```
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
```

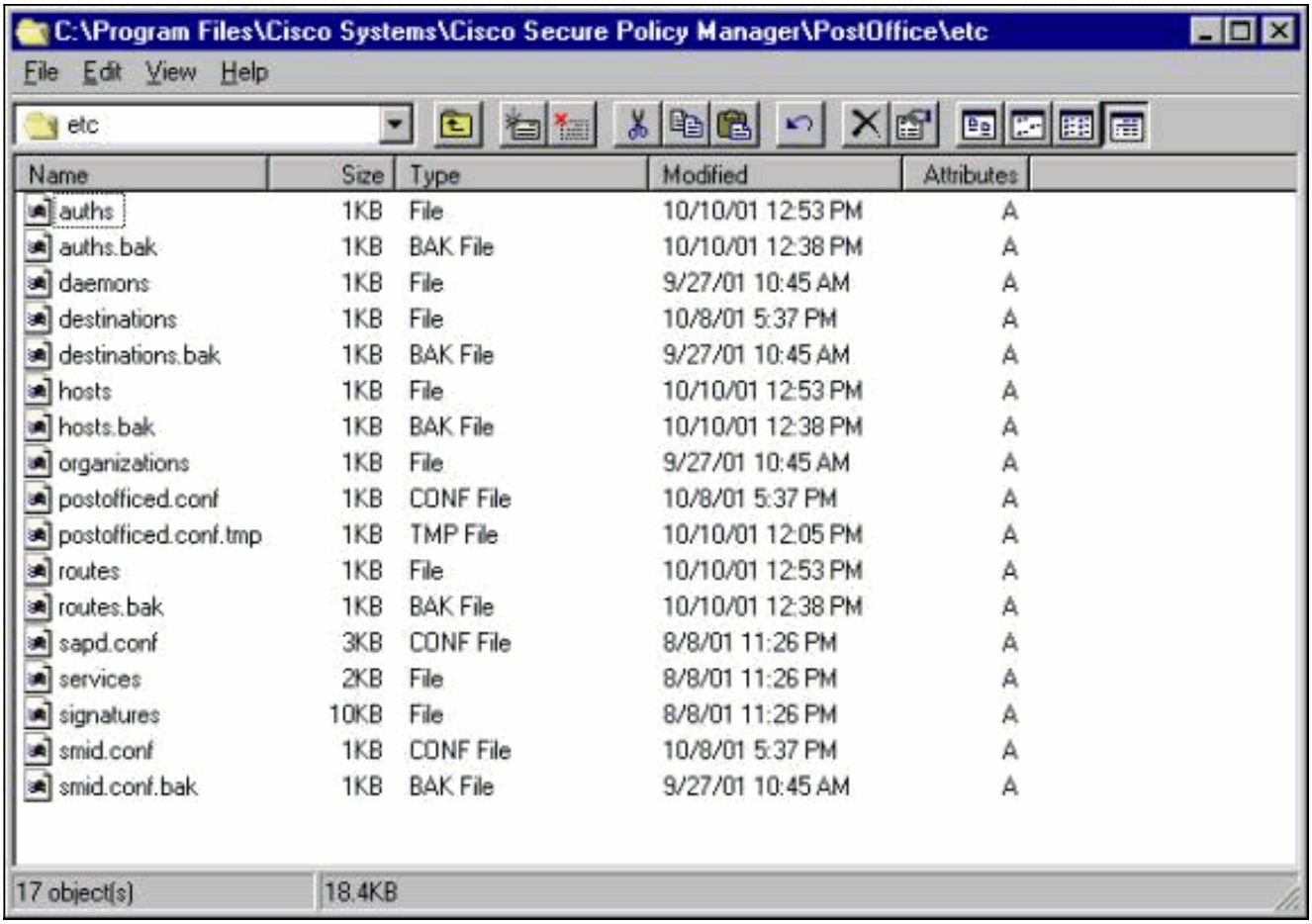
In questo caso, ottenere una traccia dello sniffer per verificare se entrambi i dispositivi inviano pacchetti UDP 4500. UDP 4500 è ciò che i dispositivi IDS utilizzano per comunicare tra loro. Per verificarlo sul sensore, **passare** alla radice e (a seconda del sensore in uso) eseguire **snoop -d iprb1 porta 45000** (per un sensore IDS 4210) e **snoop -d iprb0 porta 45000** (per qualsiasi altro modello di sensore).Utilizzare **<control-c>** per interrompere una sessione snoop.Questo output viene visualizzato se non vi sono comunicazioni tra il sensore e CSPM:

```
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#
```

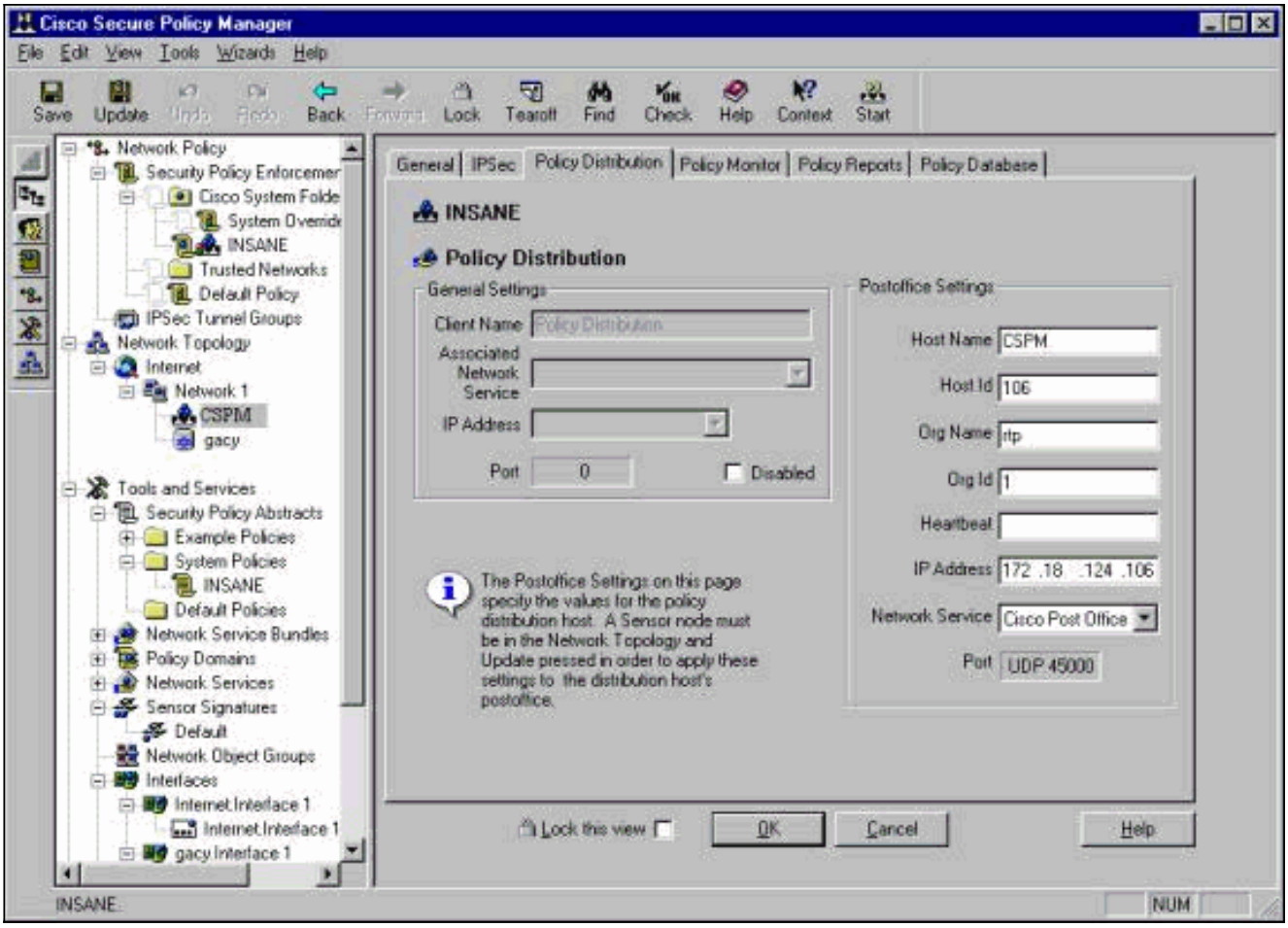
Nell'output precedente, il sensore invia pacchetti UDP 4500, ma non ne riceve alcuno. Una configurazione corretta produce un output simile al seguente:

```
# 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
```

Nell'output precedente, il traffico UDP 4500 va in entrambe le direzioni.Se i pacchetti UDP 4500 vengono trasmessi in entrambe le direzioni e l'output di **nrconns** sul sensore continua a indicare che non è stata stabilita una connessione, i parametri della postazione sul sensore e sull'host CSPM non corrispondono.Per controllare manualmente i parametri di postoffice sull'host CSPM:Utilizzare Esplora risorse per passare alla posizione in cui è installato CSPM nel computer
NT.



Modificare i file dell'host, della route e dell'organizzazione con Write o Wordpad (non utilizzare il Blocco note perché la formattazione risulterà danneggiata).Verificare che i file siano corretti per l'installazione. Se uno dei valori non è corretto, modificarlo e riavviare il computer NT attenendosi alla seguente procedura:Fare clic sull'icona **CSPM** nella topologia di rete.Fare clic sulla scheda Distribuzione dei criteri per immettere i parametri relativi all'ufficio postale.**Salvare** e **aggiornare** le modifiche.Riavviare il computer NT.



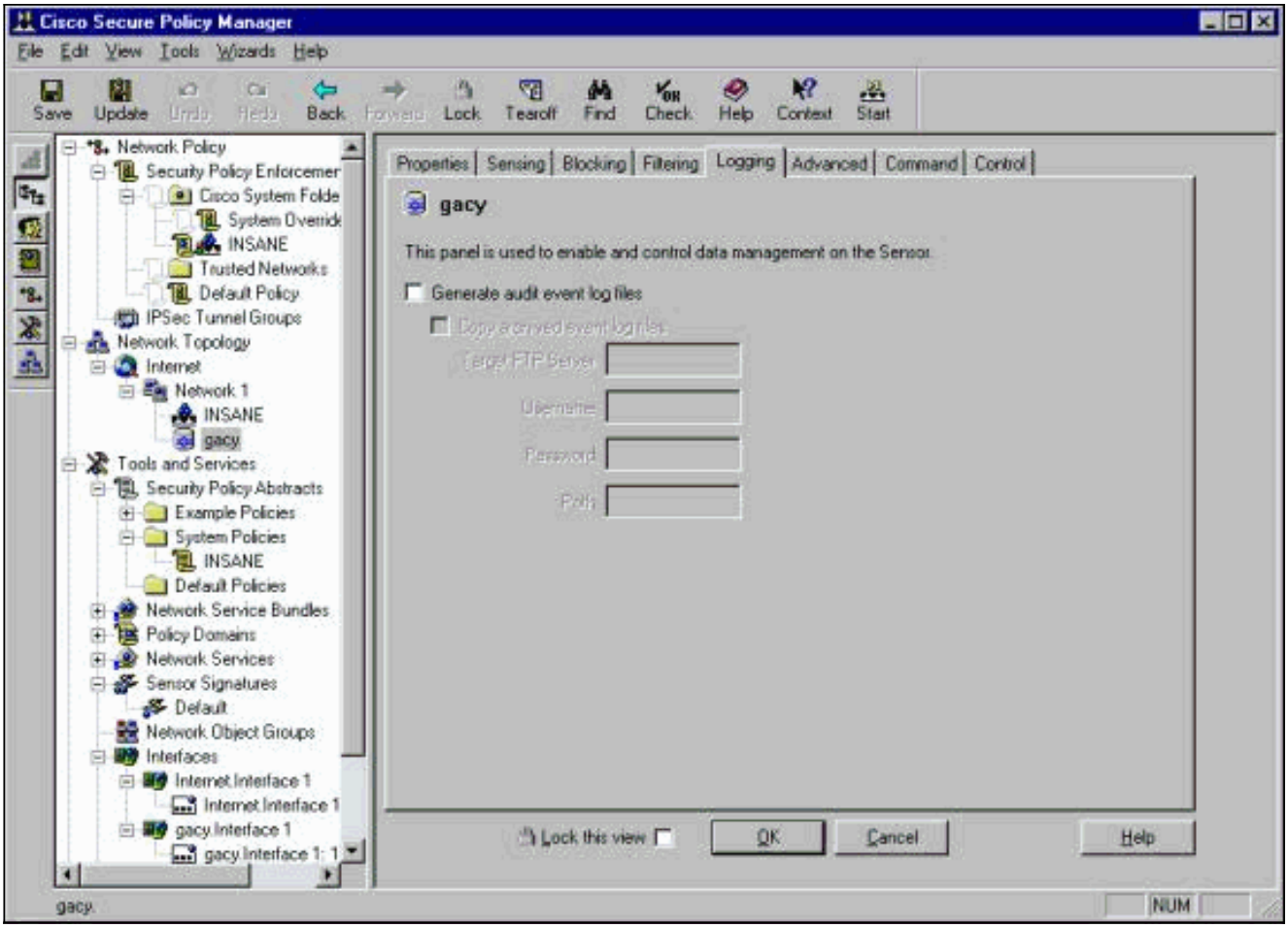
Configurazione del sensore

Dopo aver salvato la configurazione in CSPM, configurare il sensore. A tale scopo, impostare il sensore in modo che scriva gli allarmi rilevati sul proprio registro. Quindi impostare il sensore su "sniff" sull'interfaccia corretta.

Scrivi avvisi nel registro

Utilizzare questa procedura per scrivere gli allarmi nel registro.

1. Fare clic sulla casella **Genera file registro eventi di controllo** per indicare al sensore di inviare gli allarmi ai registri locali.Per impostazione predefinita, invia inoltre allarmi al modulo CSPM dopo aver eseguito il push di una configurazione.

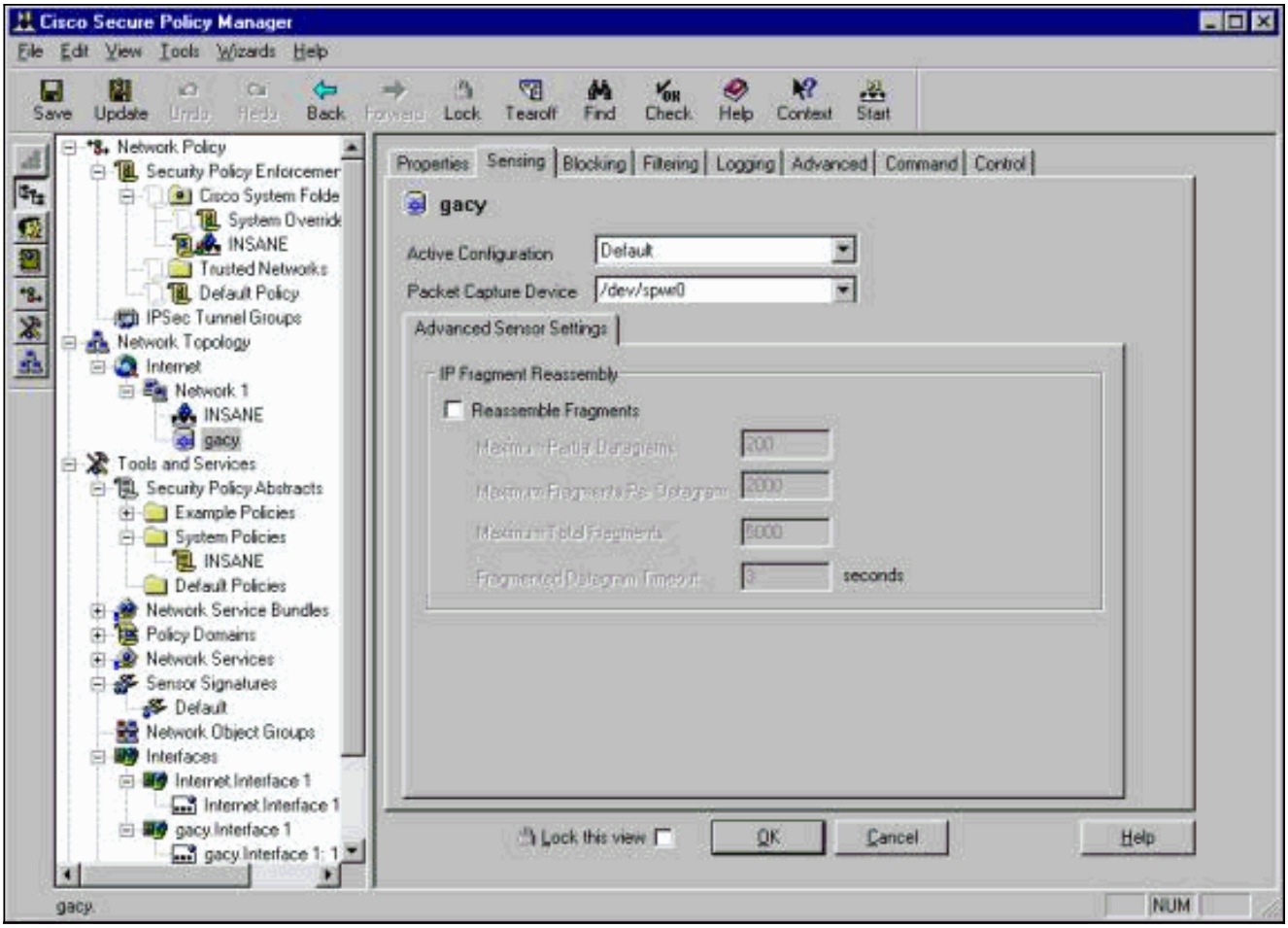


2. Fare clic su **OK** per continuare.

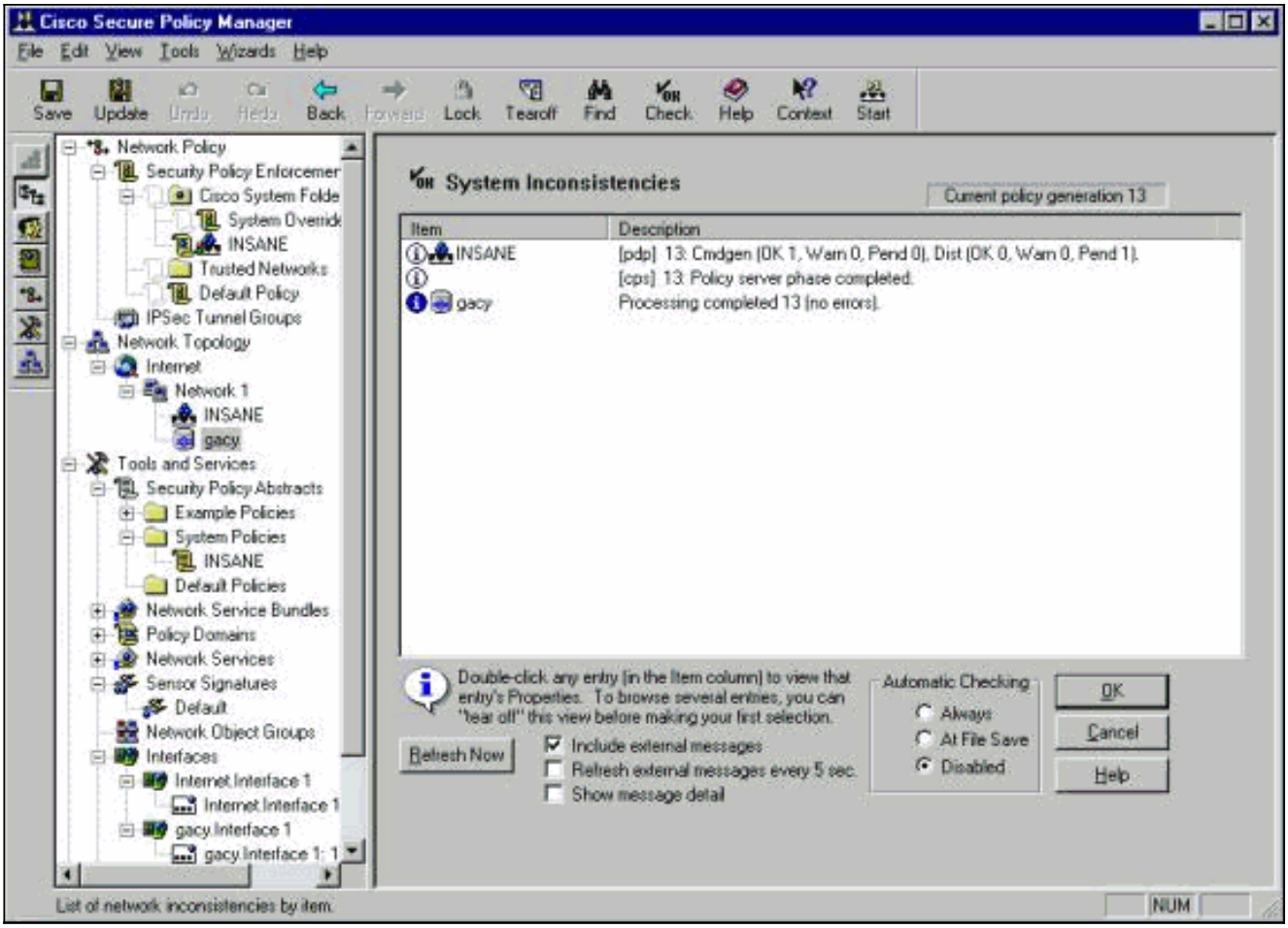
Impostare il sensore su "Sniffa"

Utilizzare questa procedura per impostare il sensore su "Sniffing".

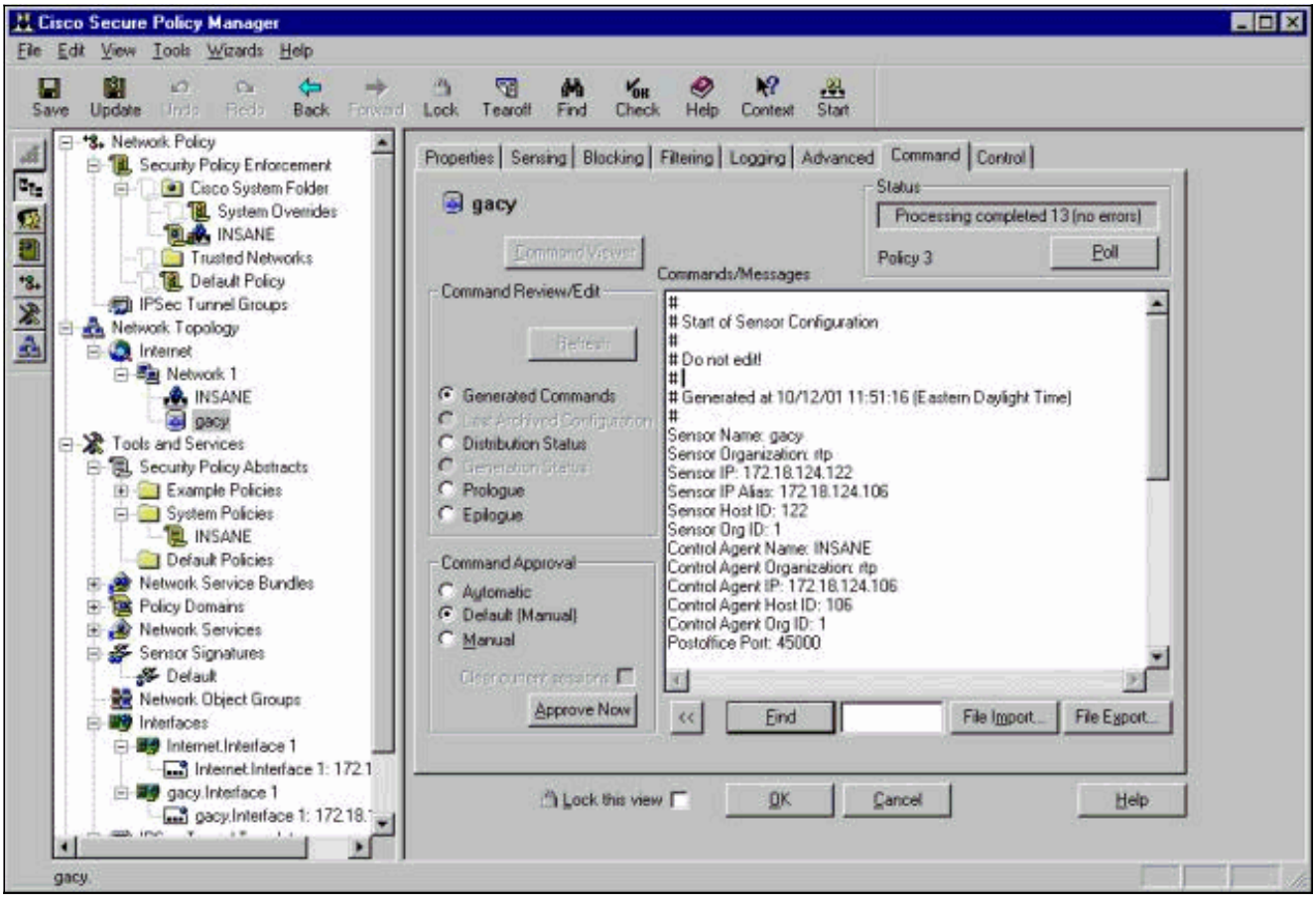
1. Selezionare il sensore nella topologia CSPM e fare clic sulla scheda Rilevamento.
2. Definire il dispositivo di acquisizione pacchetti:iprb0 - per sensore IDS 4210spwr0 - per qualsiasi altro modello di
   sensore



3. Fare clic su **OK** per continuare.
4. Fare clic sull'icona **Aggiorna** nella barra dei menu di CSPM per aggiornare CSPM con le informazioni.**Nota:** se tutto va bene, appare una schermata simile a questa. Si noti che non sono presenti errori rossi. Le avvertenze gialle sono in genere corrette.

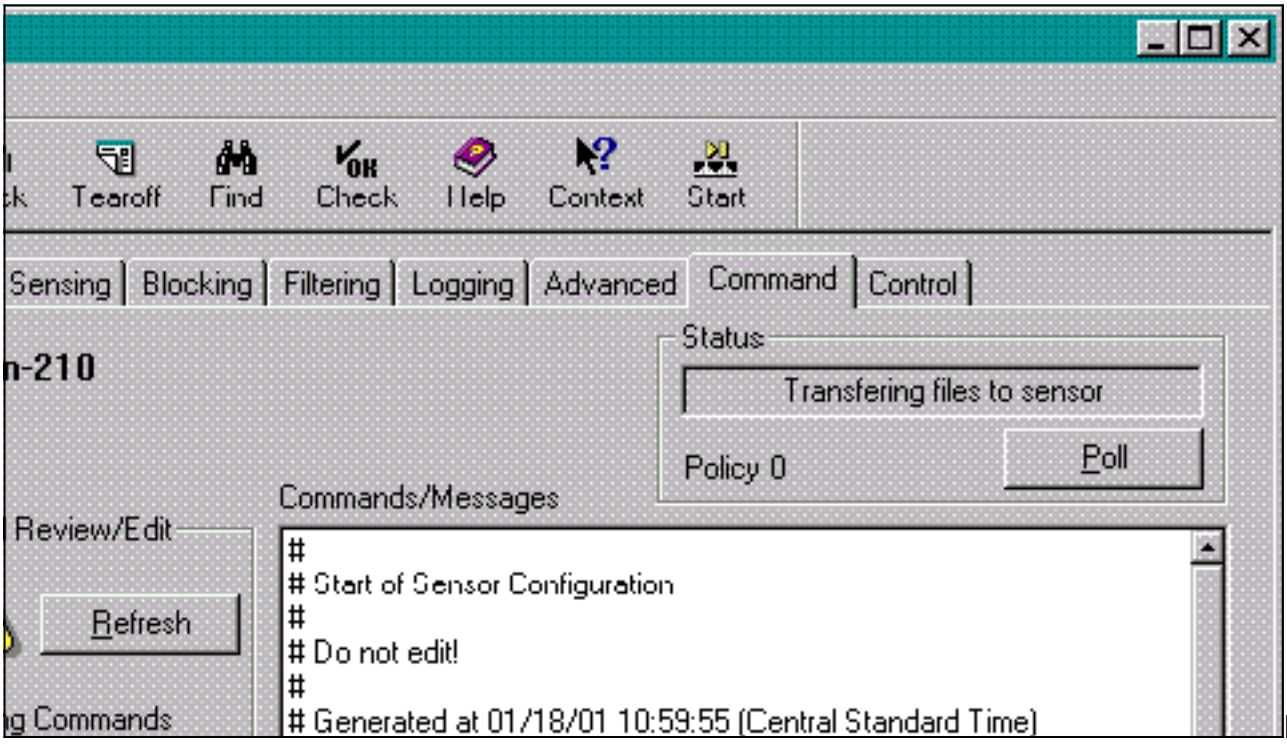


5. Selezionare il sensore nella topologia di rete e fare clic sulla scheda Comando per inviare la configurazione aggiornata al
sensore.

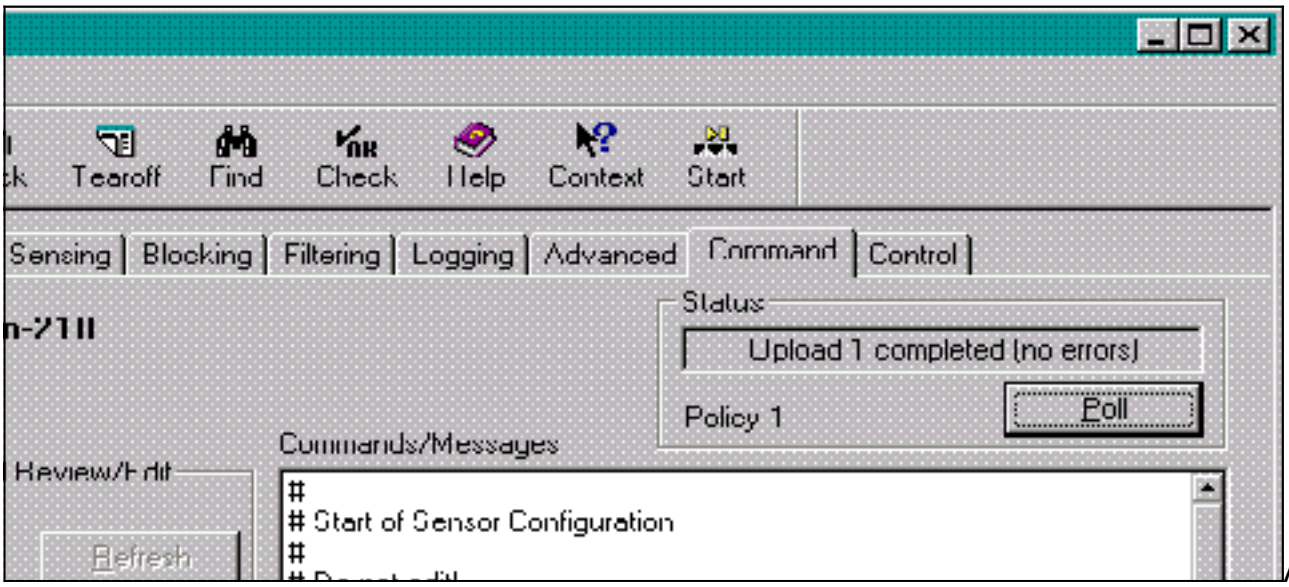


6. Fare clic sul pulsante **Approva ora** per inviare la configurazione al

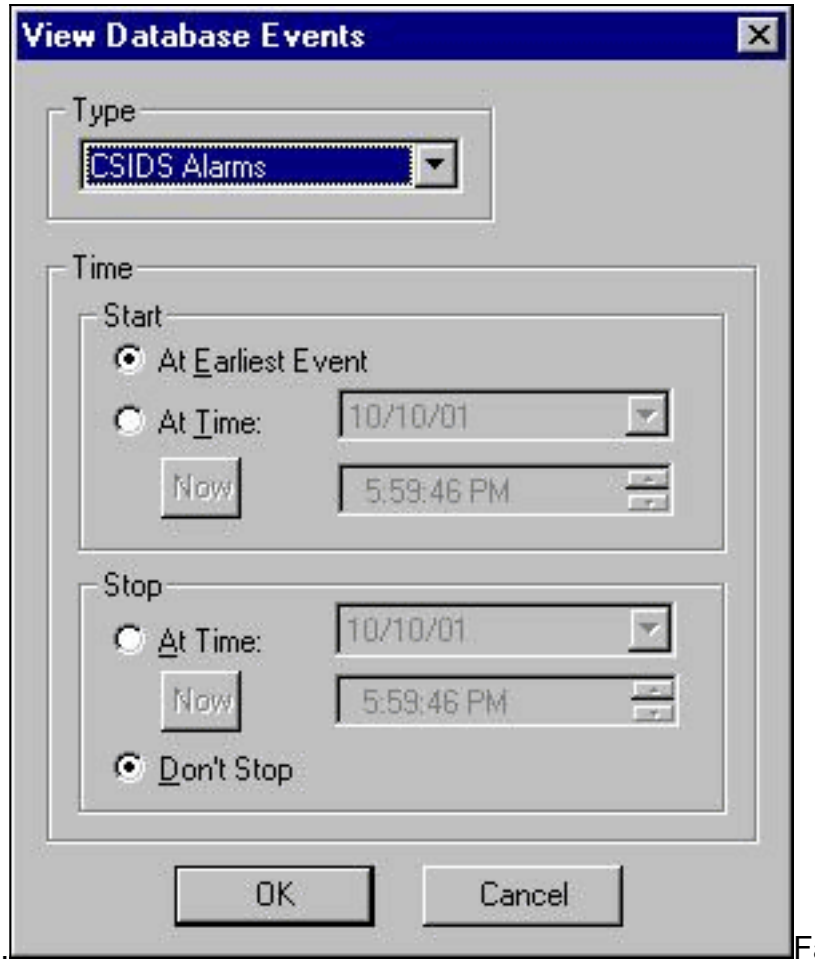
sensore.



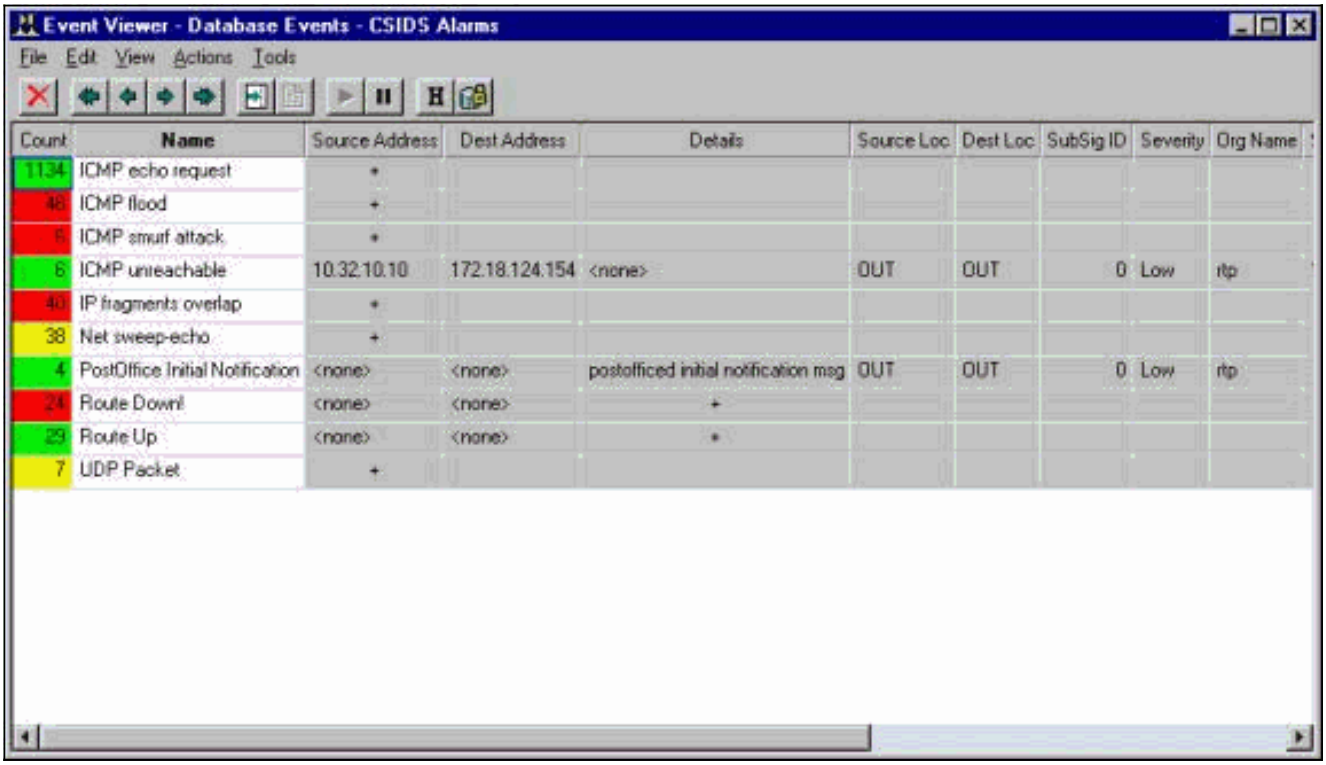
Nel riquadro di stato viene visualizzato il messaggio "Caricamento <#> completato". Indica un processo di trasferimento valido e completo. Il sensore è stato aggiornato e ora dovrebbe funzionare normalmente.Se il sensore non funziona normalmente, tornare al sensore e controllare l'output del comando **nrconns** per verificare che la connessione tra l'host CSPM e il sensore sia stata
stabilita.



Al termine, è possibile cercare gli allarmi inviati dal sensore all'host CSPM nel visualizzatore eventi. Per visualizzare il Visualizzatore eventi, dal menu principale di CSPM selezionare **Strumenti > Visualizza eventi sensore >**



Database.Fare clic su **OK** per visualizzare la finestra del database degli eventi. Lo schermo varia a seconda degli allarmi che si
ricevono.



Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems