Configuration d'un détecteur IDS sécurisé Cisco dans CSPM

Contenu

Introduction

Ce document explique la procédure utilisée pour configurer un capteur Cisco Secure de système de détection d'intrusion (ID) sur le Cisco Secure Policy Manager (CSPM). Ce document suppose que vous avez installé la version 2.3.I CSPM sur votre ordinateur. Version « je » permet la Gestion des périphériques d'ID (des Routeurs de capteurs, de Cisco IOS® d'appareils, ou des lames d'ID) dans un commutateur du Cisco Catalyst® 6000. Ce document suppose également que les paramètres de bureau de poste d'ID sont correctement définis. Ceux-ci incluent le HOSTID, l'ORGID, l'ADRESSE INTERNET, et l'ORGNAME. Veuillez noter que pour que l'hôte CSPM communique avec un capteur, l'ORGID et l'ORGNAME doivent apparier ce qui est défini sur le capteur.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur CSPM 2.3.I et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

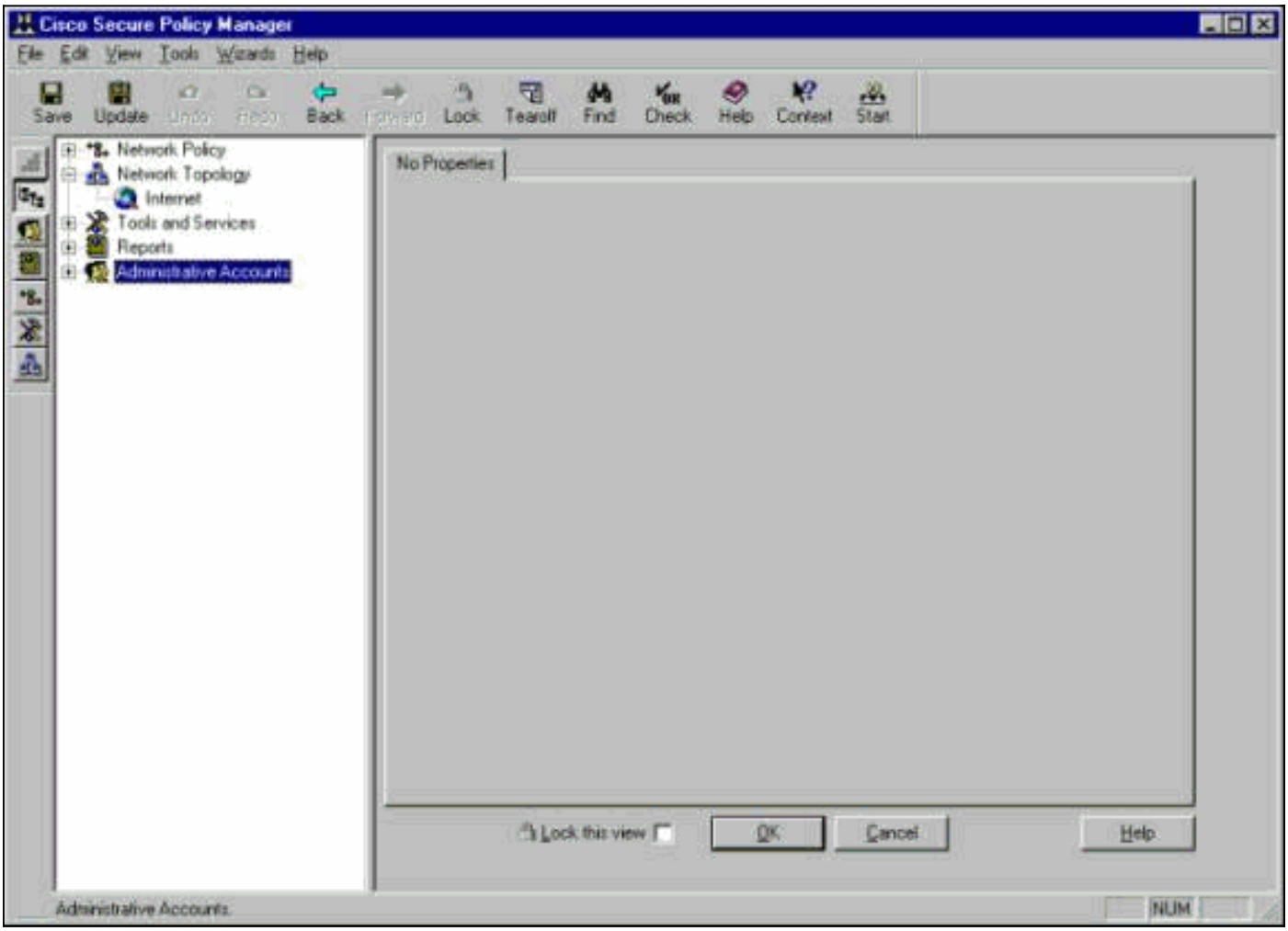
Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Ces sections expliquent le processus utilisé pour configurer un capteur d'ID dans CSPM.

Lancement CSPM et procédure de connexion. Un modèle vide apparaît (lancement initial) qui te permet pour définir votre réseau.



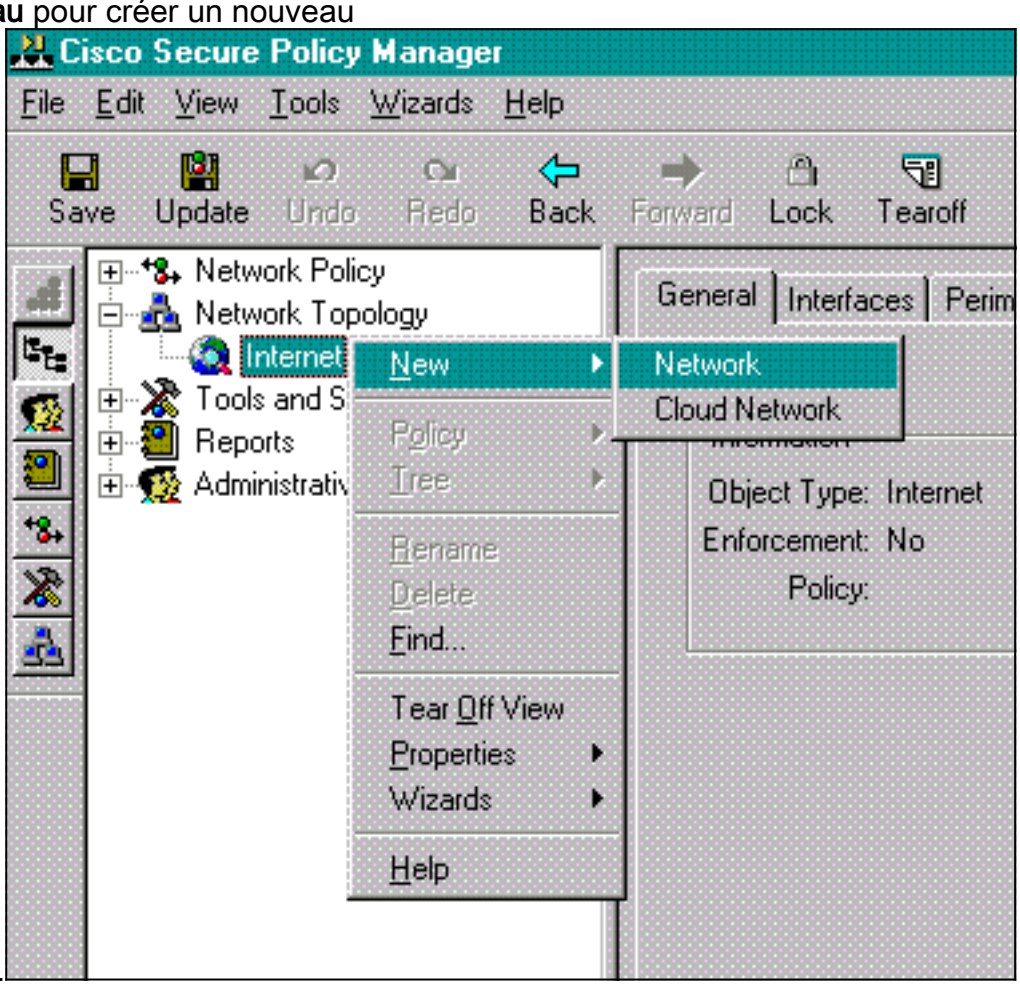
Ces trois définitions sont exigées dans la topologie CSPM pour des ID.

1. Définissez le réseau dans lequel l'interface de contrôle du capteur réside et le réseau dans lequel l'hôte CSPM réside. S'ils sont sur le même sous-réseau, alors seulement un réseau doit être défini. Définissez ce réseau premier.
2. Définissez l'hôte CSPM dans son réseau. Sans définition d'hôte CSPM, le capteur ne peut pas être géré.
3. Définissez le capteur dans son réseau.

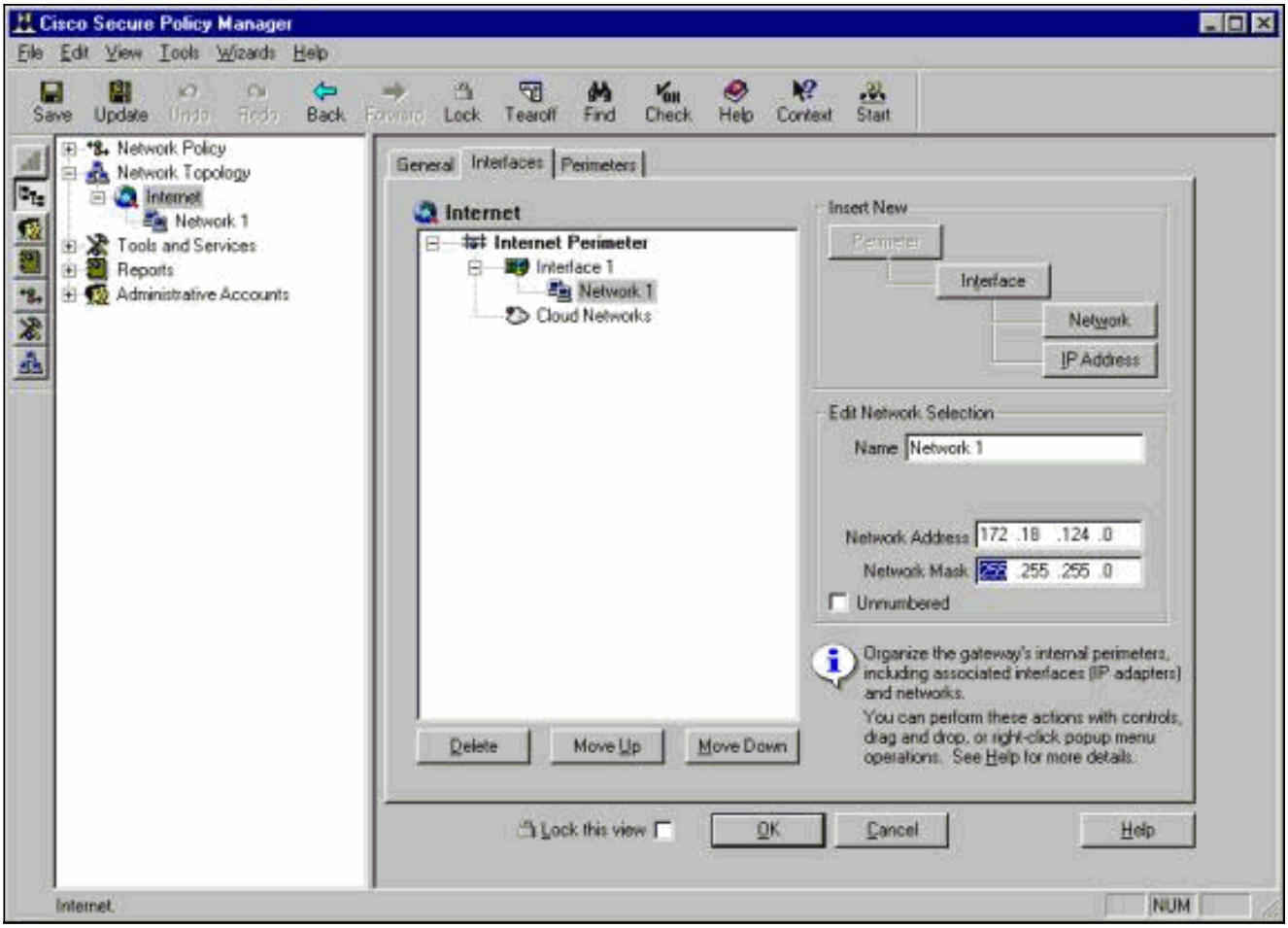
Définissez le réseau sur lequel l'hôte CSPM réside

Procédez comme suit :

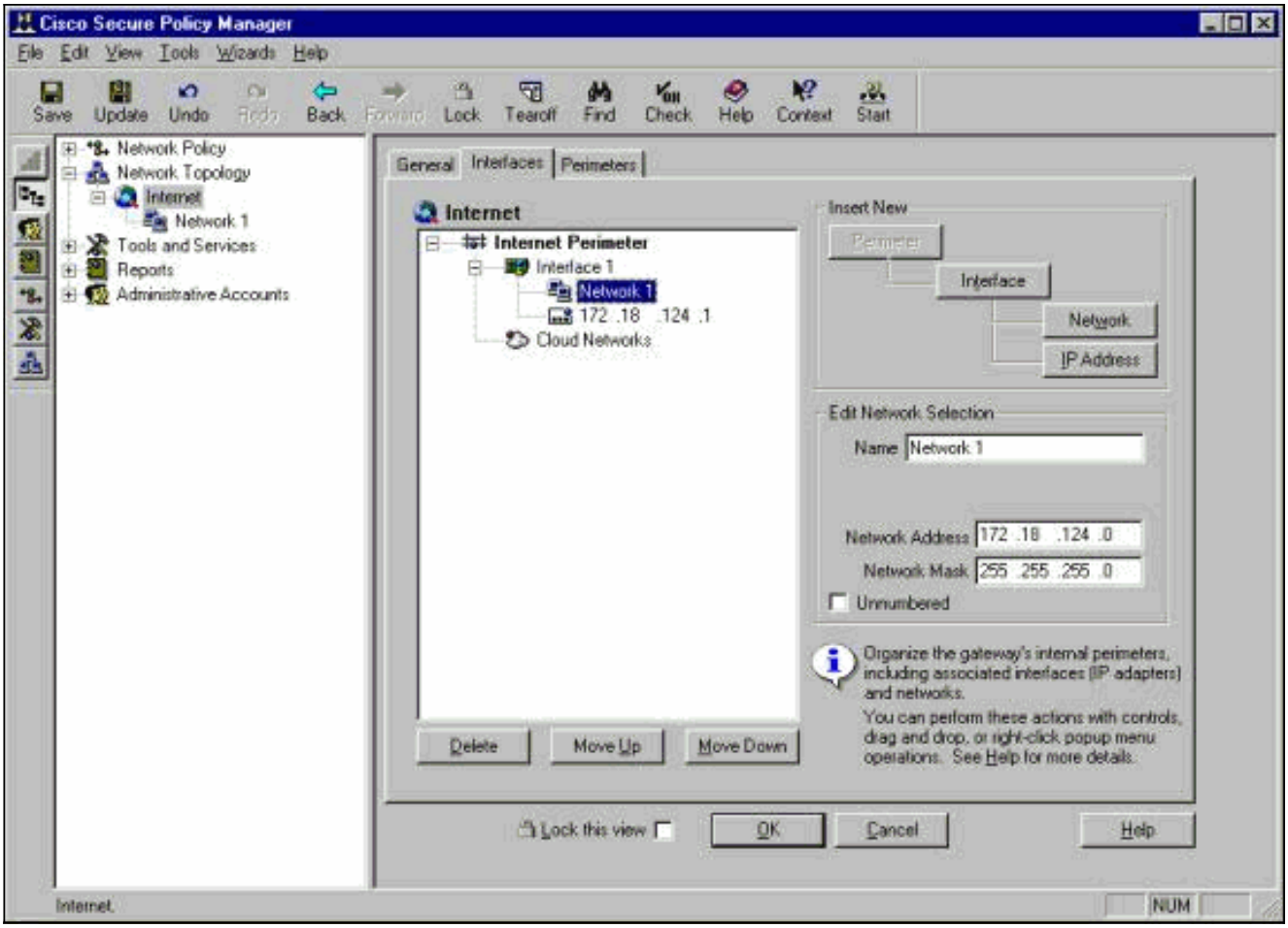
1. Cliquez avec le bouton droit sur l'icône d'**Internet** dans la topologie et sélectionnez **nouveau > réseau** pour créer un nouveau réseau.



2. Du côté droit du panneau de réseau, ajoutez le nom du nouveau réseau, de l'adresse réseau, et du netmask qui sera utilisé.



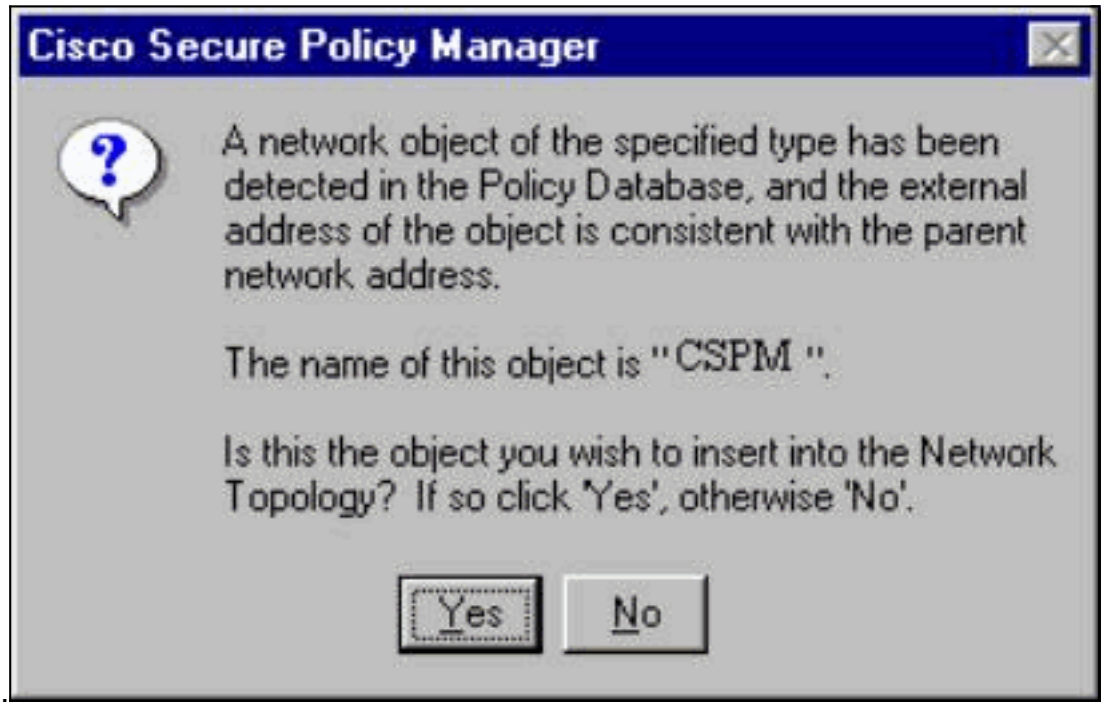
3. Cliquez sur le bouton d'**adresse IP**, et écrivez l'adresse IP pour votre réseau qu'il l'utilise pour atteindre l'Internet.Normalement c'est la passerelle par défaut pour le réseau.**Remarque:** Quand vous gérez des capteurs, l'adresse de passerelle ne doit pas nécessairement être correcte puisque le capteur n'est pas envoyé à ces informations sur la passerelle par défaut. Il devrait déjà être défini dans le capteur.
4. Cliquez sur **OK**. Le réseau n'est ajouté à la carte de topologie sans aucune erreur.



Ajoutez l'hôte CSPM

Employez cette procédure pour ajouter l'hôte CSPM.

1. En topologie du réseau, clic droit sur le réseau que vous avez juste ajouté et **nouveau** choisi **> hôte**.CSPM apporte un écran semblable à ceci. Sinon, puis le réseau que vous avez juste défini n'est pas le réseau dans lequel votre hôte CSPM se trouve. Vérifiez l'adresse IP sur votre hôte CSPM de nouveau.

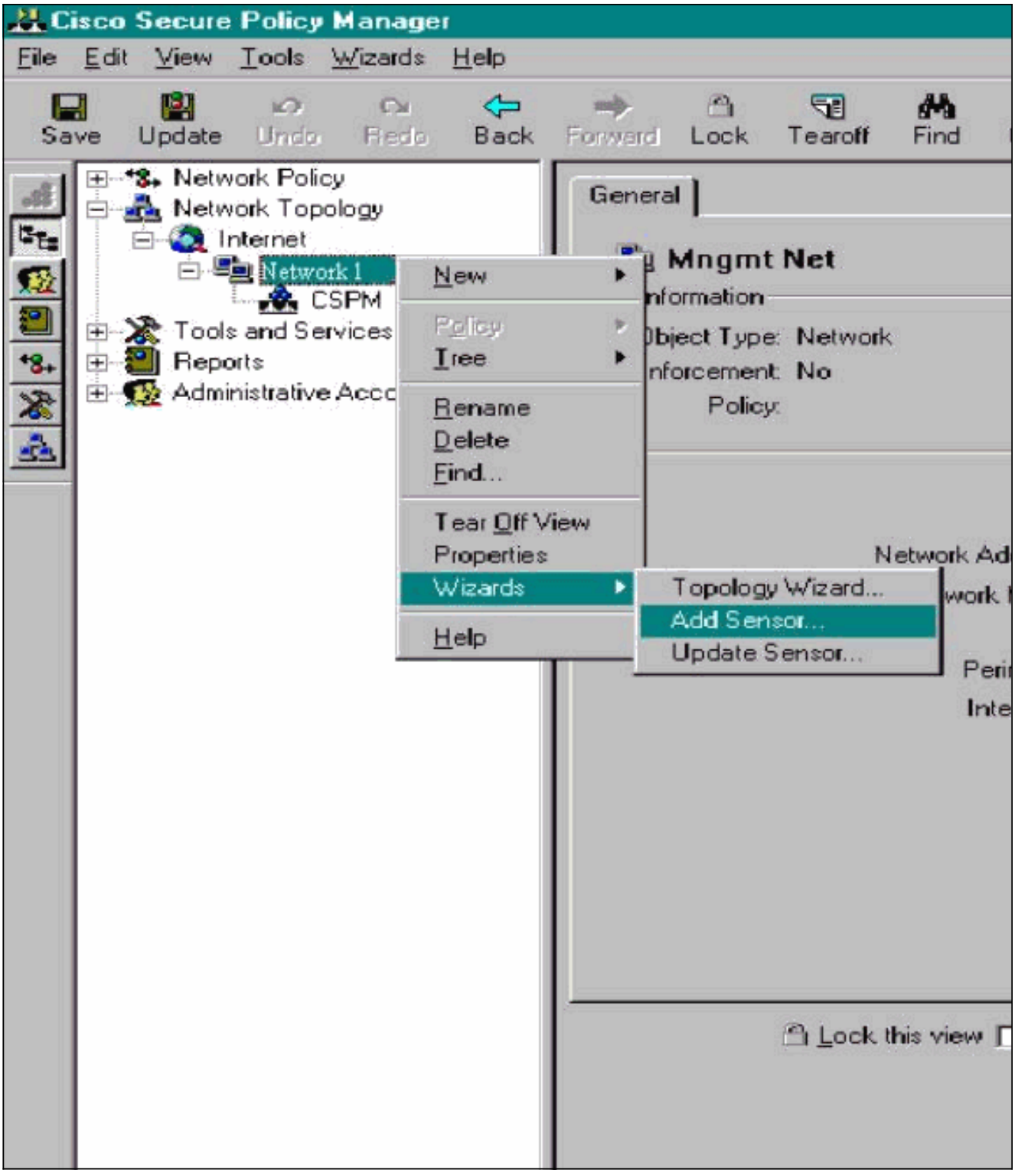


2. Cliquez sur **oui** pour installer l'hôte CSPM dans la topologie.
3. Vérifiez que les informations sur l'écran général pour l'hôte CSPM sont correctes.
4. Cliquez sur OK sur l'écran général de l'hôte CSPM.

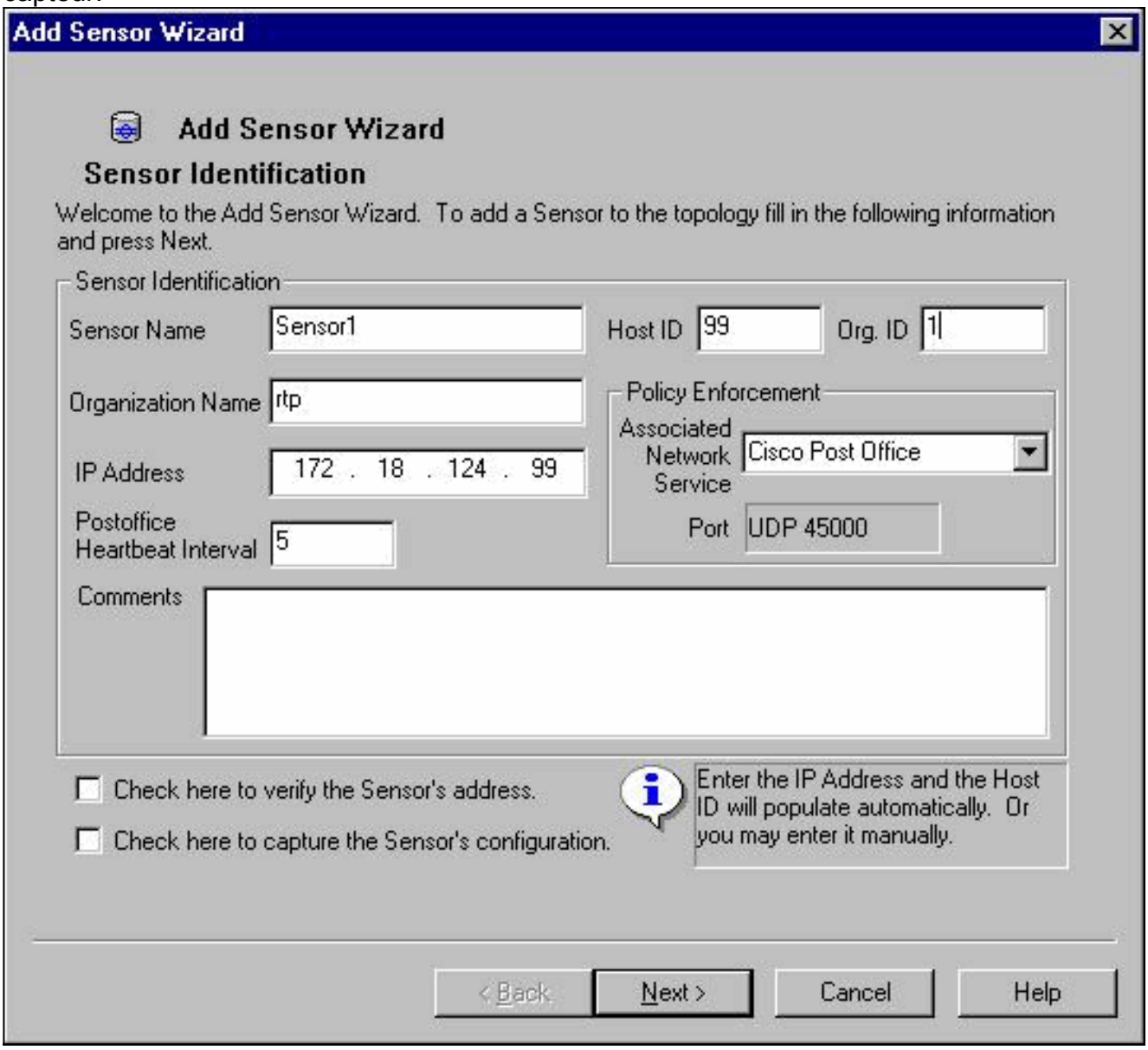
Ajoutez le périphérique de capteur

Employez cette procédure pour ajouter le périphérique de capteur.

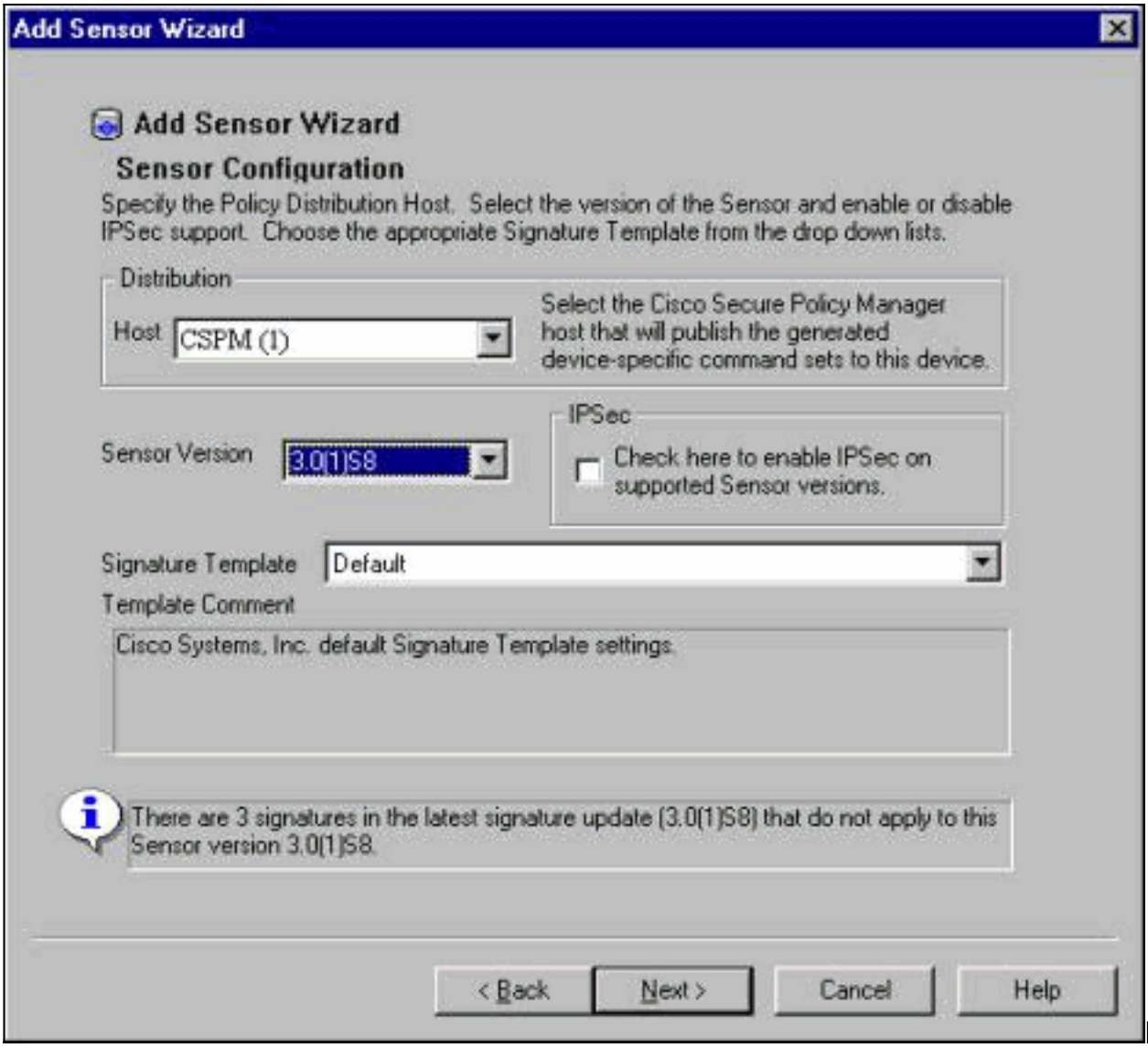
1. Cliquez avec le bouton droit sur le réseau dans lequel votre capteur réside et les **assistants** choisis > **ajoutent le capteur**.**Remarque:** Si l'hôte CSPM et l'interface de contrôle de votre capteur ne sont pas dans le même réseau, définissez le réseau dans lequel votre capteur réside.



2. Entrez les paramètres corrects de bureau de poste pour le capteur.



3. Cliquez sur le **contrôle ici pour vérifier la** case de l'**adresse du capteur**.**Remarque:** Si c'est la première fois vous installez ce capteur, vous ne voulez pas capturer la configuration du capteur. Si vous avez précédemment configuré ce capteur ailleurs par l'intermédiaire d'un directeur UNIX ou d'un hôte différent CSPM et avez apporté des modifications de configuration aux signatures de capteurs, alors vous voulez capturer la configuration du capteur.
4. Le clic **à côté de** définissent les versions de signature sur le capteur. Vous pouvez également émettre les **nrvers** commandez de vérifier ceci sur le capteur.



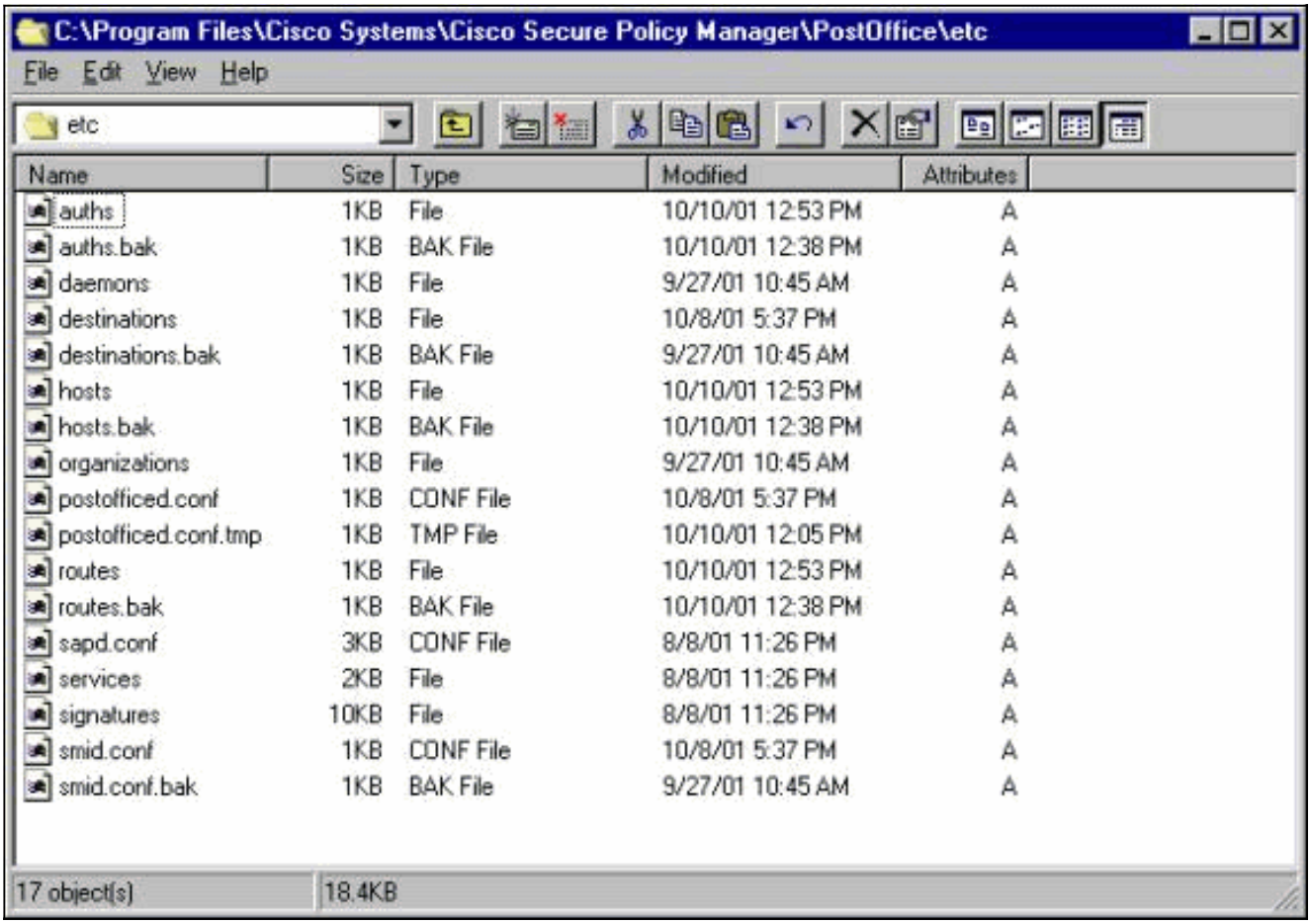
Remarque: Si CSPM n'a pas la version correcte de capteur que vous vous exécutez sur votre capteur, mettez à jour les signatures sur votre hôte CSPM. Veuillez voir le téléchargement logiciel (clients enregistrés seulement) pour des mises à jour.

5. Cliquez sur le **bouton suivant** pour continuer.
6. Cliquez sur Finish pour se terminer l'installation du capteur dans la topologie.
7. Du menu principal CSPM, du **fichier** choisi > de la **sauvegarde** et **mise à jour** pour compiler l'information saisie dans la topologie dans CSPM. Veuillez noter que cette étape est nécessaire pour commencer le Post Office Protocol sur l'hôte CSPM.
8. Vérifiez que tout fonctionne à côté de se connecter dans votre capteur en tant qu'utilisateur de netrangr.
9. Exécutez la commande de **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 >` **Remarque:** Si le capteur et l'hôte CSPM ne communiquent pas, la sortie semblable à ceci apparaît à la place :`netrangr@gacy:/usr/nr`

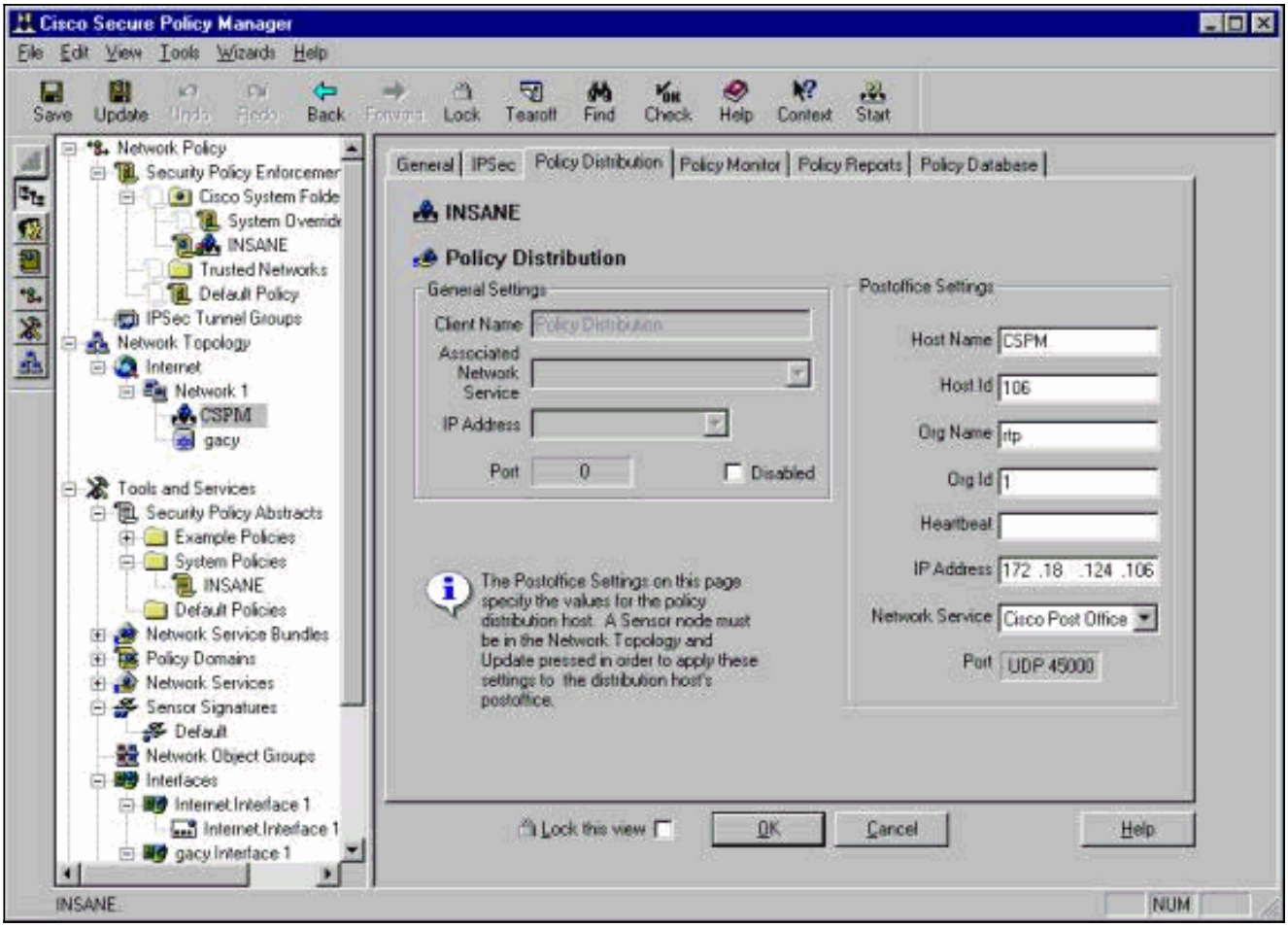
   `>nrconns Connection Status for gacy.rtp insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent] sto:5000 syn NOT rcvd! netrangr@gacy:/usr/nr` Si c'est le cas, obtenez un tracé de renifleur pour voir si les deux côtés envoient à UDP 45000 paquets. Est l'UDP 45000 ce que les périphériques d'ID les utilisent pour communiquer les uns avec les autres. Pour tester ceci sur le capteur, le **su** pour enraciner et (selon quel capteur vous avez) pour exécuter le **fureteur - port 45000 d iprb1** (pour un capteur d'ID 4210) et **piller - port 45000 d iprb0** (pour tout autre modèle de capteur).Employez le **<control-c>** pour éclater d'une session de

fureteur.Cette sortie apparaît s'il n'y a aucune transmission entre le capteur et le 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#` Dans la sortie ci-dessus, le capteur en envoie à UDP 45000 paquets, mais ne reçoit pas. Une configuration correcte produit la sortie semblable à ceci :`# 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` Dans la sortie ci-dessus, le trafic de l'UDP 45000 va dans les deux directions.Si l'UDP 45000 paquets entrent dans les deux directions et la sortie des **nrconns** sur le capteur indique toujours qu'il n'y a aucune connexion établie, les paramètres de bureau de poste sur le capteur et l'hôte CSPM ne s'assortissent pas.Pour vérifier les paramètres de bureau de poste sur le CSPM hébergez manuellement :Utilisez l'Explorateur Windows pour naviguer vers où vous avez CSPM installé sur l'ordinateur sous NT.



Éditez l'hôte, artère, et les fichiers d'organisation avec écrivent ou Wordpad (n'utilisez pas Notepad parce que le formatage sera corrompu).Assurez-vous que ces fichiers semblent corrects pour votre installation. Si les valeurs l'unes des ne sont pas correctes, éditez-les et redémarrez votre ordinateur de NT utilisant ces étapes :Cliquez sur en fonction l'icône **CSPM** en topologie du réseau.Cliquez sur en fonction l'onglet de distribution de stratégie pour entrer vos paramètres de bureau de poste.**Sauvegardez** et **mettez à jour** vos modifications.Redémarrez l'ordinateur de NT.



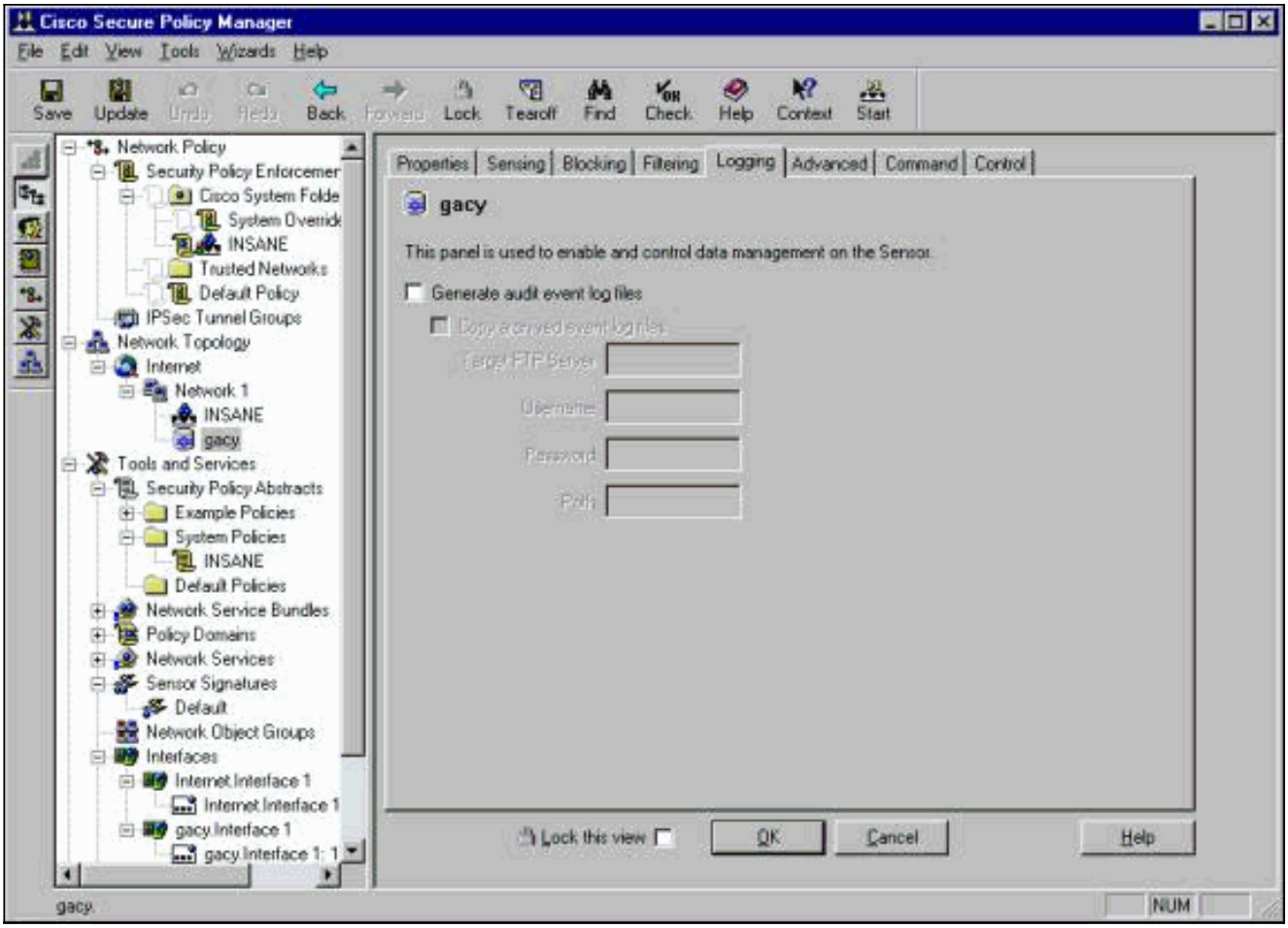
Configurez le capteur

Après que la configuration soit enregistrée dans CSPM, configurez le capteur. Afin de faire ceci, placez d'abord le capteur pour écrire les alarmes qu'elles voient à son propre log. Placez alors le capteur « pour renifler » sur l'interface appropriée.

Écrivez les alarmes au log

Employez cette procédure pour écrire des alarmes au log.

1. Cliquez sur la case de **fichiers de consignation de journal d'événements d'audit de générer** pour dire le capteur d'envoyer les alarmes à ses logs locaux.Il envoie également des alarmes dans la case CSPM par défaut après que vous abaissiez une configuration à elle.

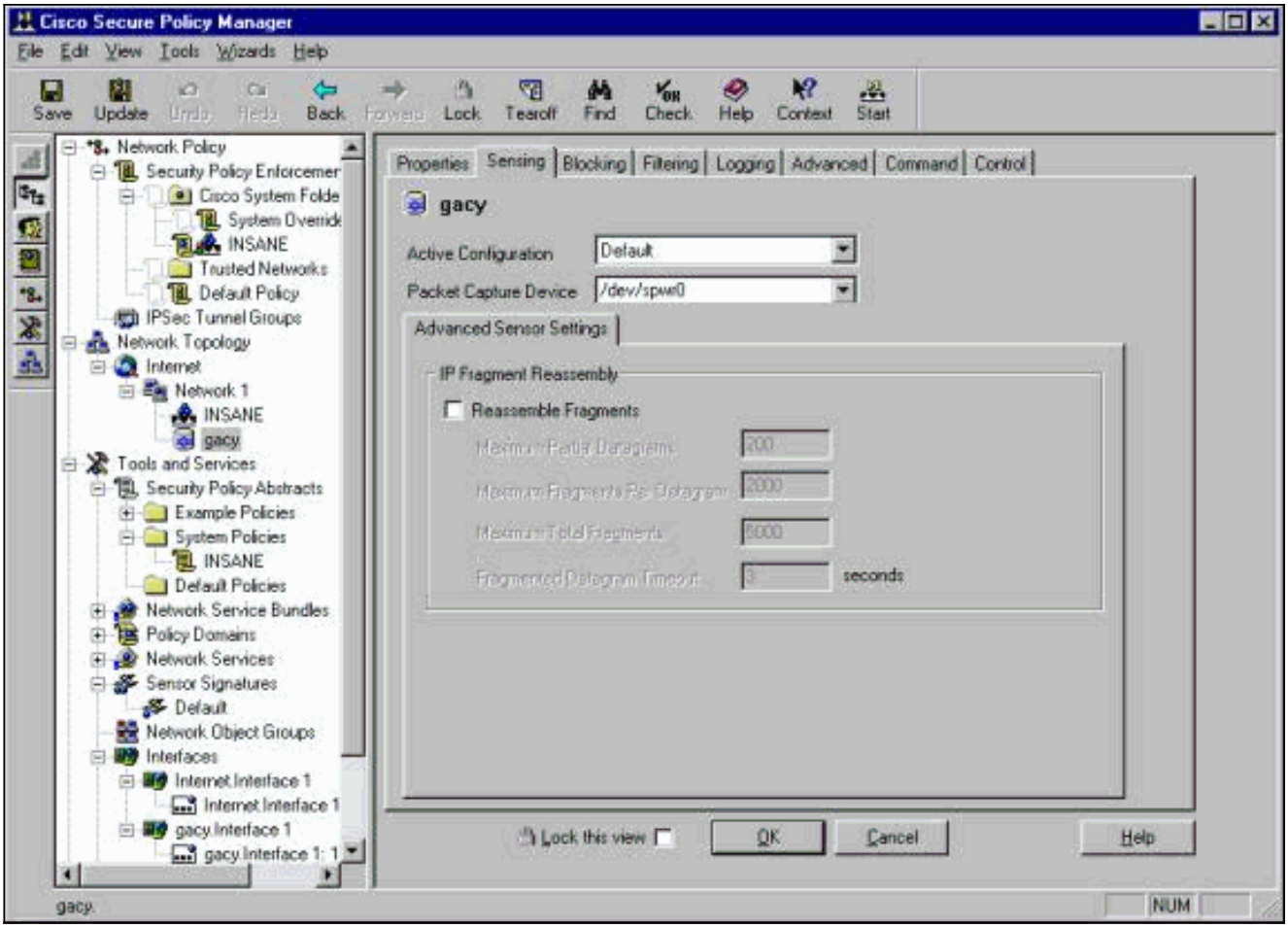


2. Cliquez sur **OK** pour continuer.

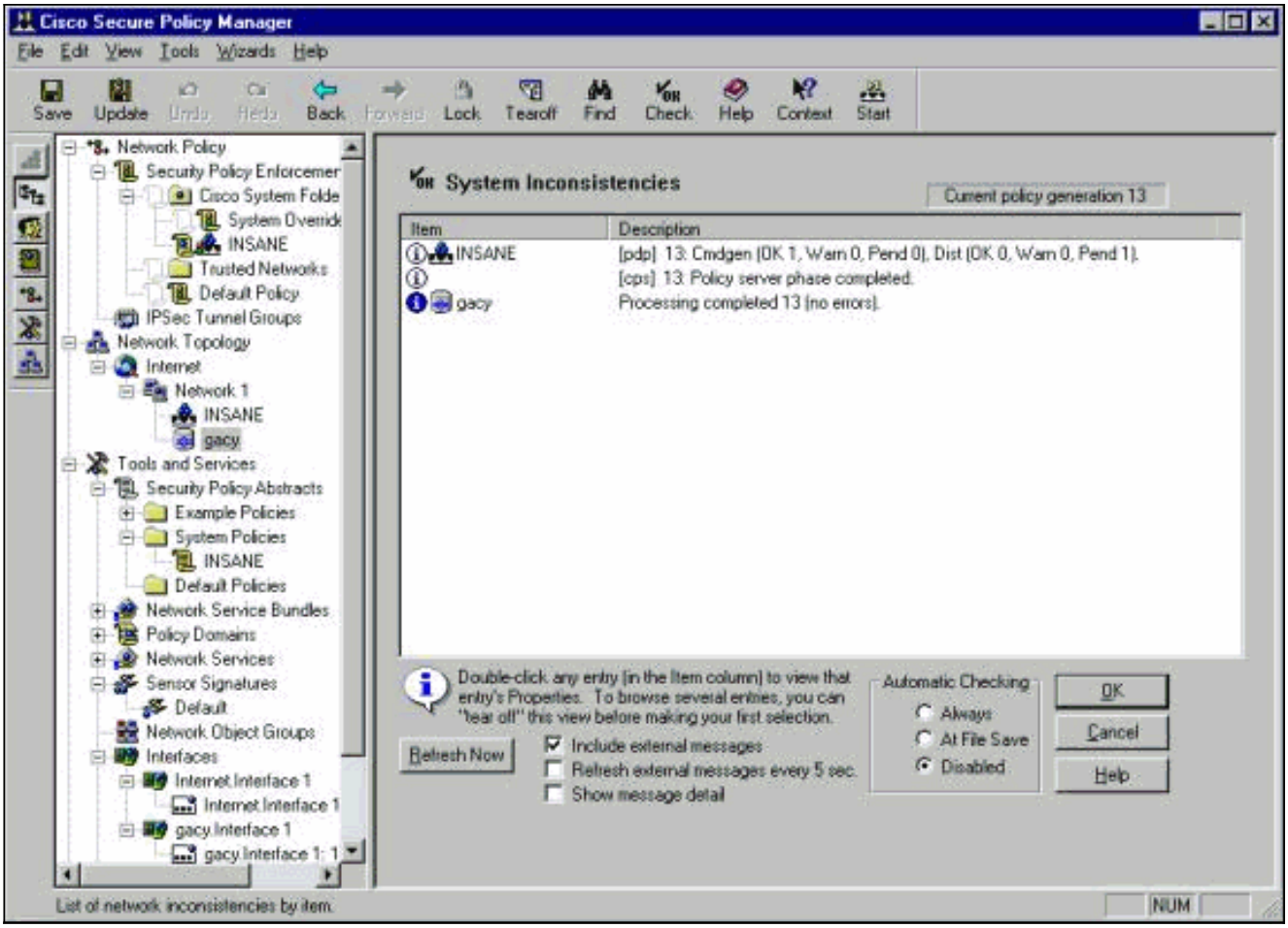
Placez le capteur « pour renifler »

Employez cette procédure pour placer le capteur « pour renifler ».

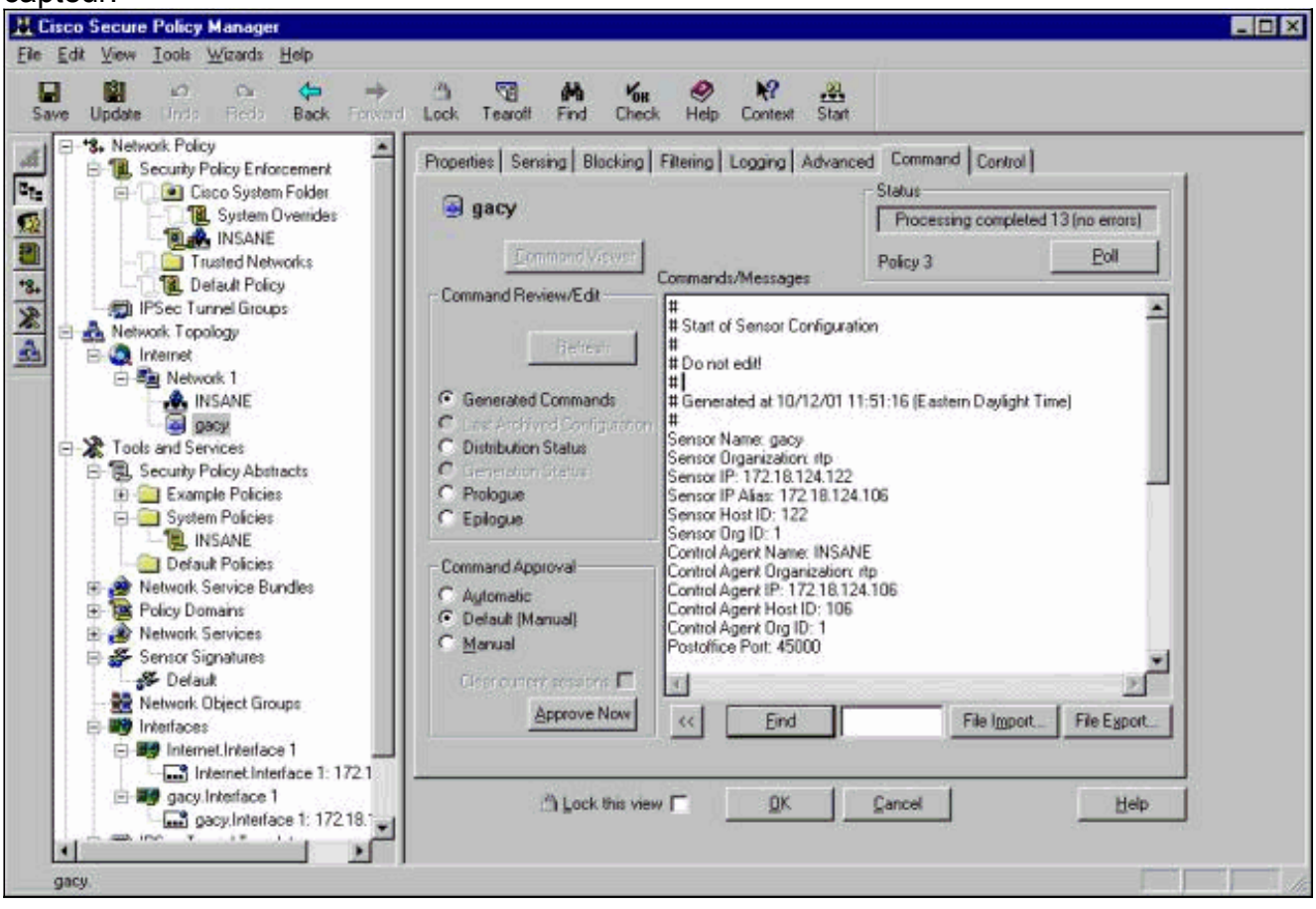
1. Sélectionnez le capteur dans votre topologie CSPM et cliquez sur l'onglet de détection.
2. Définissez le périphérique de capture de paquet :iprb0 - pour un capteur des ID 4210spwr0 - pour tout autre modèle de
   capteur



3. Cliquez sur **OK** pour continuer.
4. Cliquez sur l'icône de **mise à jour** sur la barre de menus CSPM pour mettre à jour CSPM avec les informations.**Remarque:** Si tout va bien, un écran semblable à ceci apparaît. L'avis là ne sont aucune erreur rouge. Les avertissements jaunes sont en général corrects.

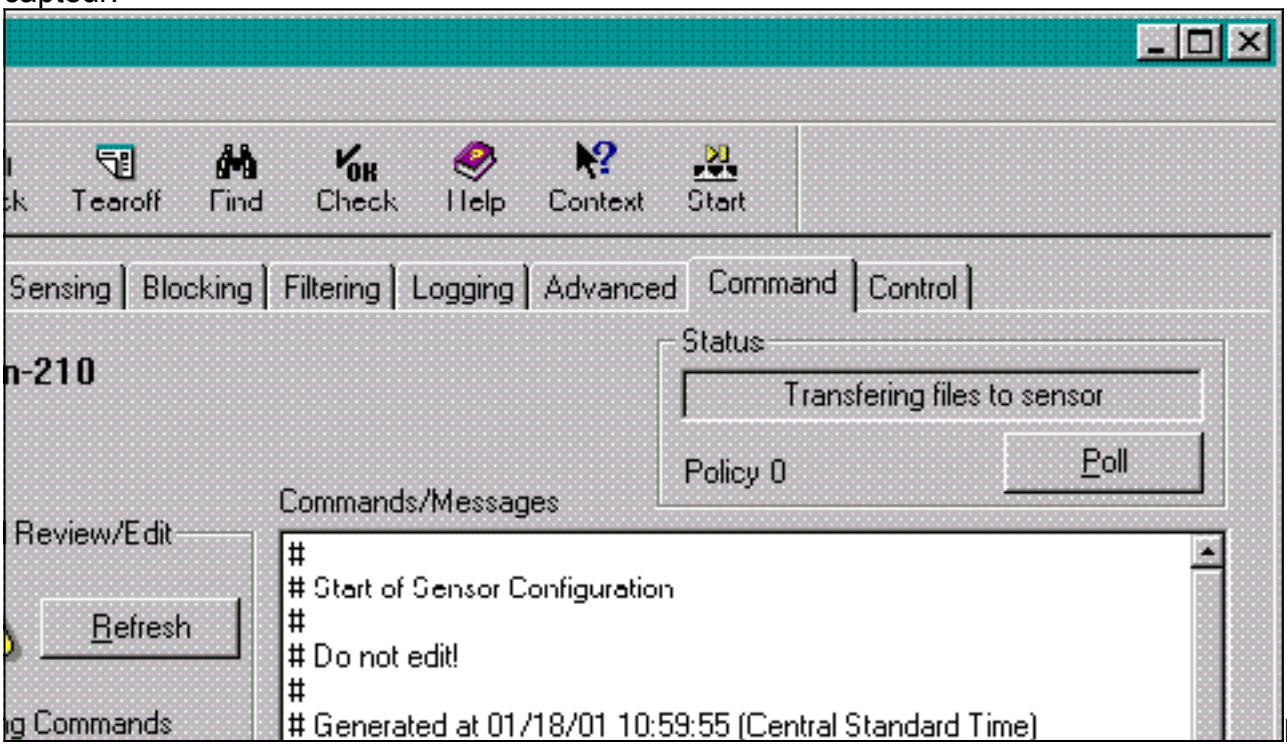


5. Sélectionnez le capteur en topologie du réseau et cliquez sur l'onglet de commande pour envoyer la configuration mise à jour au capteur.

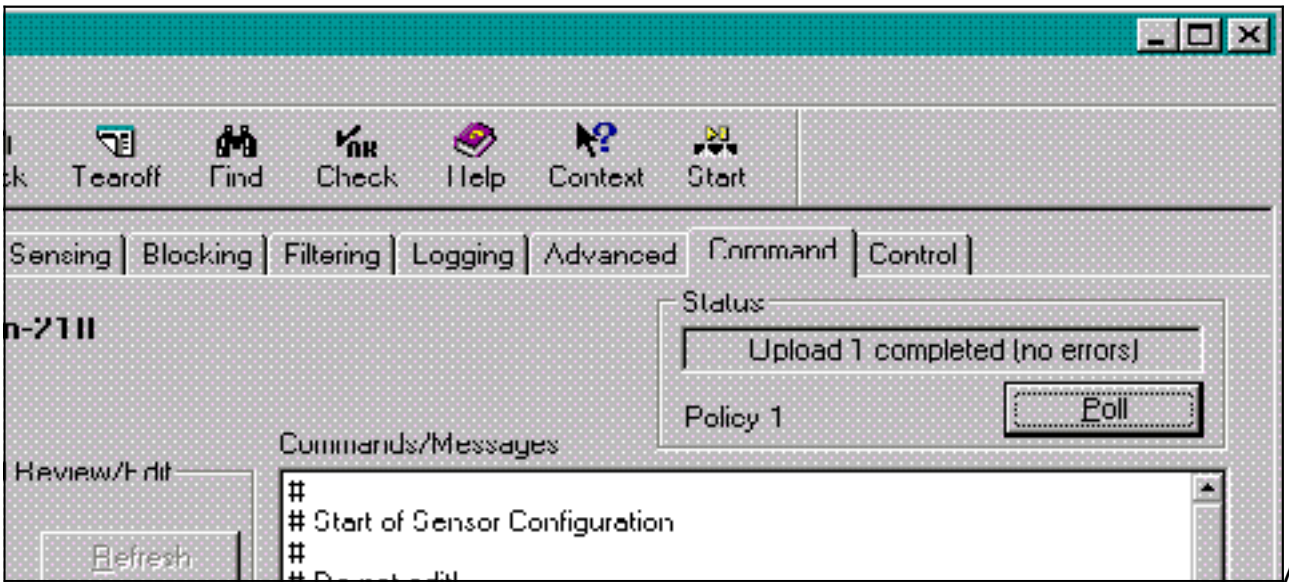


6. Cliquez sur l'**approbation** se boutonnent **maintenant** pour envoyer la configuration au

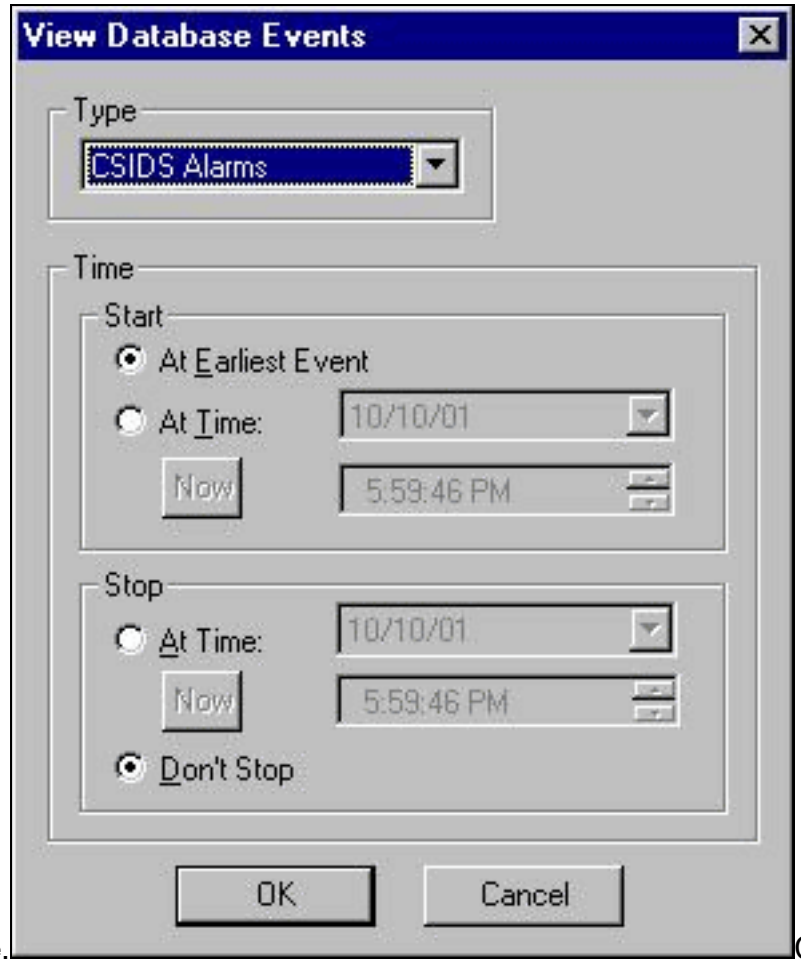
capteur.



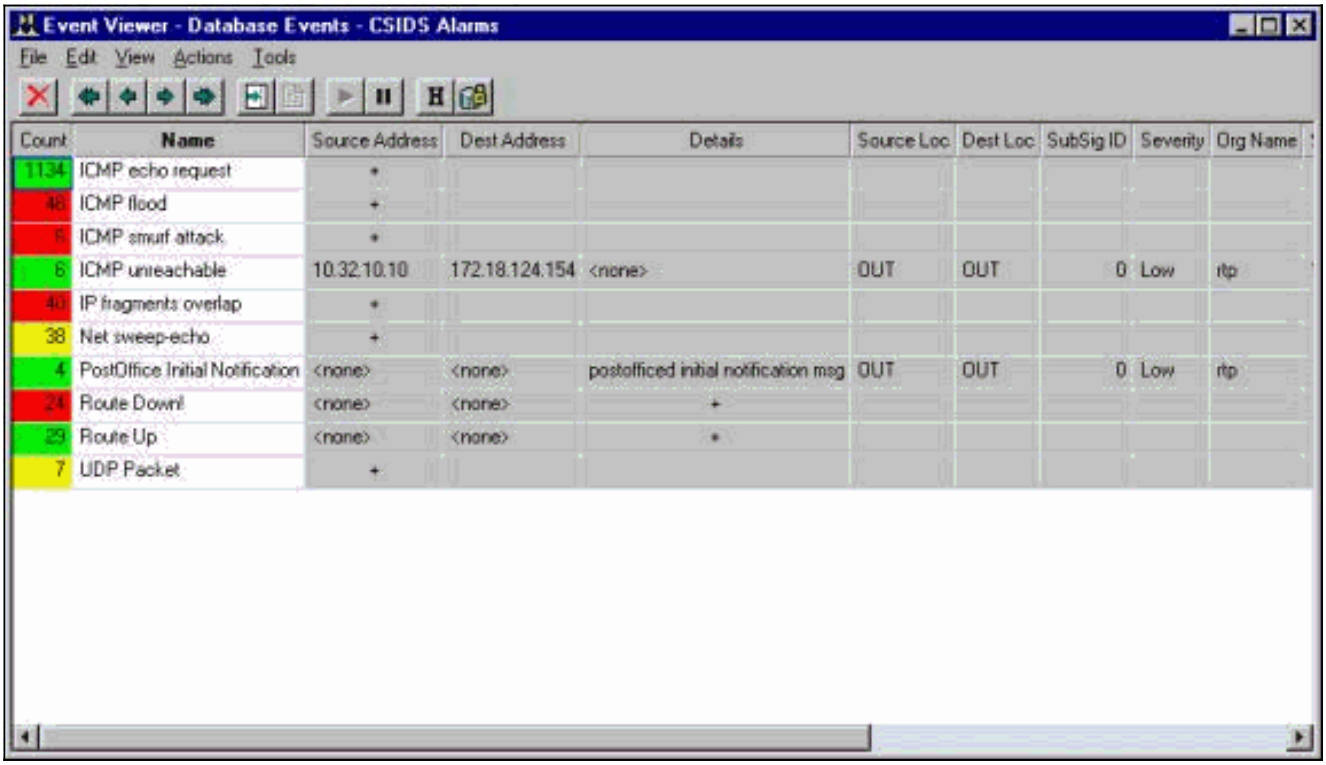
Le volet d'état affiche le message terminé par **<#>** de « téléchargement ». Ceci indique un processus valide et complet de transfert. Le capteur est maintenant mis à jour et devrait maintenant s'exécuter normalement.Si le capteur ne s'exécute pas normalement, retournez au capteur et vérifiez la sortie des **nrconns** commandent de s'assurer que la connexion entre l'hôte CSPM et le capteur est
établie.



Après que ce soit complet, vous pouvez rechercher les alarmes que le capteur envoie au visualiseur d'hôte CSPM en cas. Pour visualiser le visualisateur d'événements, des **outils de** menu principal CSPM **>** des **événements >** de la **base de données** choisis de **capteur de**



vue.Cliquez sur OK pour afficher la fenêtre de base de données d'événements. Votre écran variera selon les alarmes que vous pouvez
obtenir.



Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	*							
46	ICMP flood	*							
5	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	*							

Informations connexes

- Support et documentation techniques - Cisco Systems