IPS 6.X : Activer/Désactiver le résumé d'un événement spécifique à l'aide d'IDM

Contenu

Introduction

Ce document décrit comment activer/le résumé d'un événement spécifique dans la version de logiciel 6.x de Système de prévention d'intrusion (IPS) utilisant le gestionnaire de périphérique IPS (IDM).

Remarque: Des Listes d'accès doivent être configurées dans les appliances IPS afin de permettre l'accès de l'hôte ou du réseau où le logiciel de gestion tel qu'IDM et les IEV (visualisateur d'événements d'ID) sont installés et fonctionnent correctement. Référez-vous à changer la section de liste d'accès de configurer le capteur de Système de protection contre les intrusions Cisco utilisant le pour en savoir plus de l'interface de ligne de commande 5.0.

Conditions préalables

Conditions requises

Ce document est créé avec la supposition qu'IPS 6.x est installé et fonctionne correctement.

Composants utilisés

Les informations dans ce document sont basées sur le capteur IPS de gamme Cisco 4200 qui exécute la version de logiciel 6.0(2)E1.

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 utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

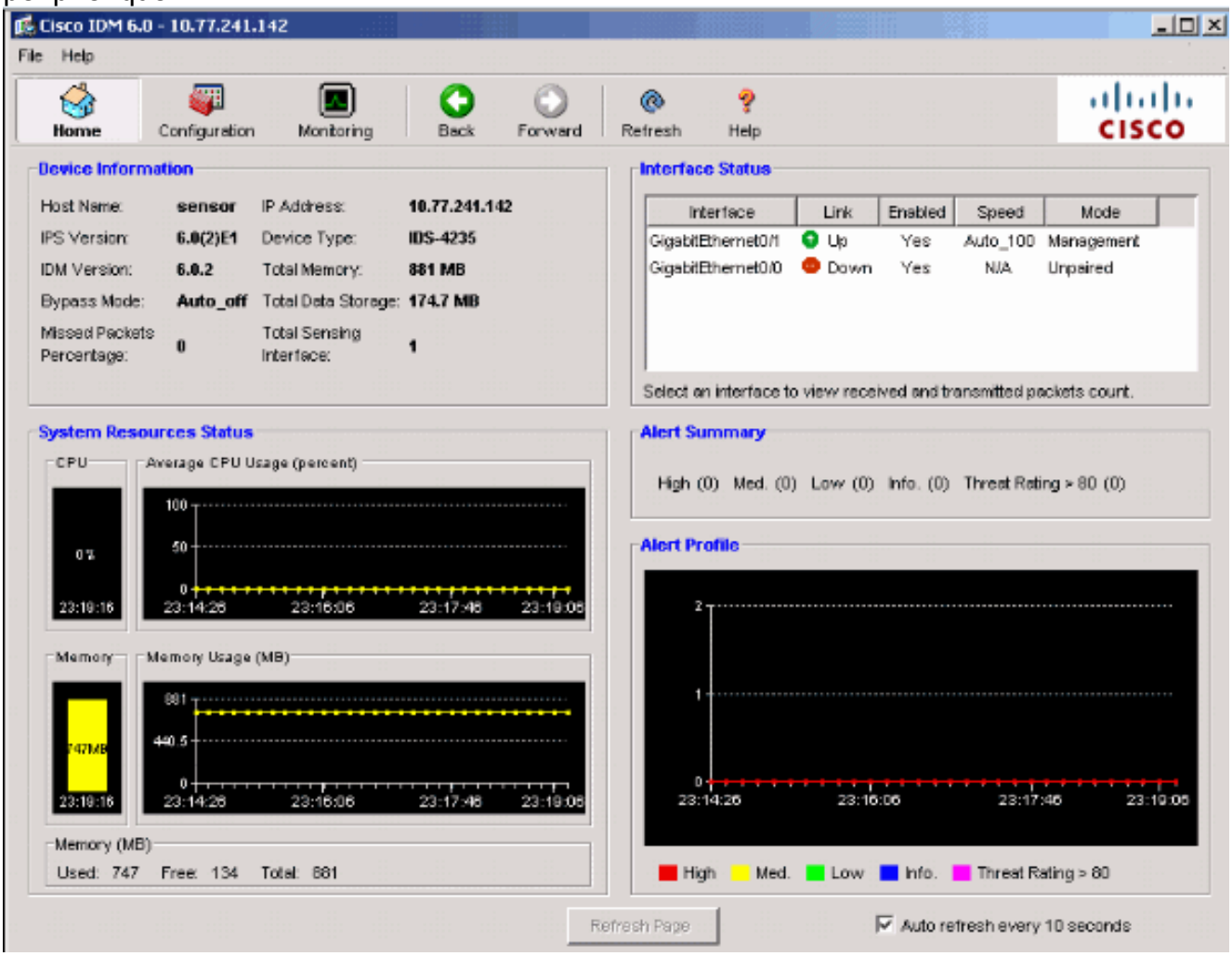
Activer/Désactiver le résumé d'un événement spécifique à l'aide d'IDM

Pour une compréhension claire, cette section fournit un exemple dans lequel vous activer/le résumé pour l'**ID de signature : 5748**.

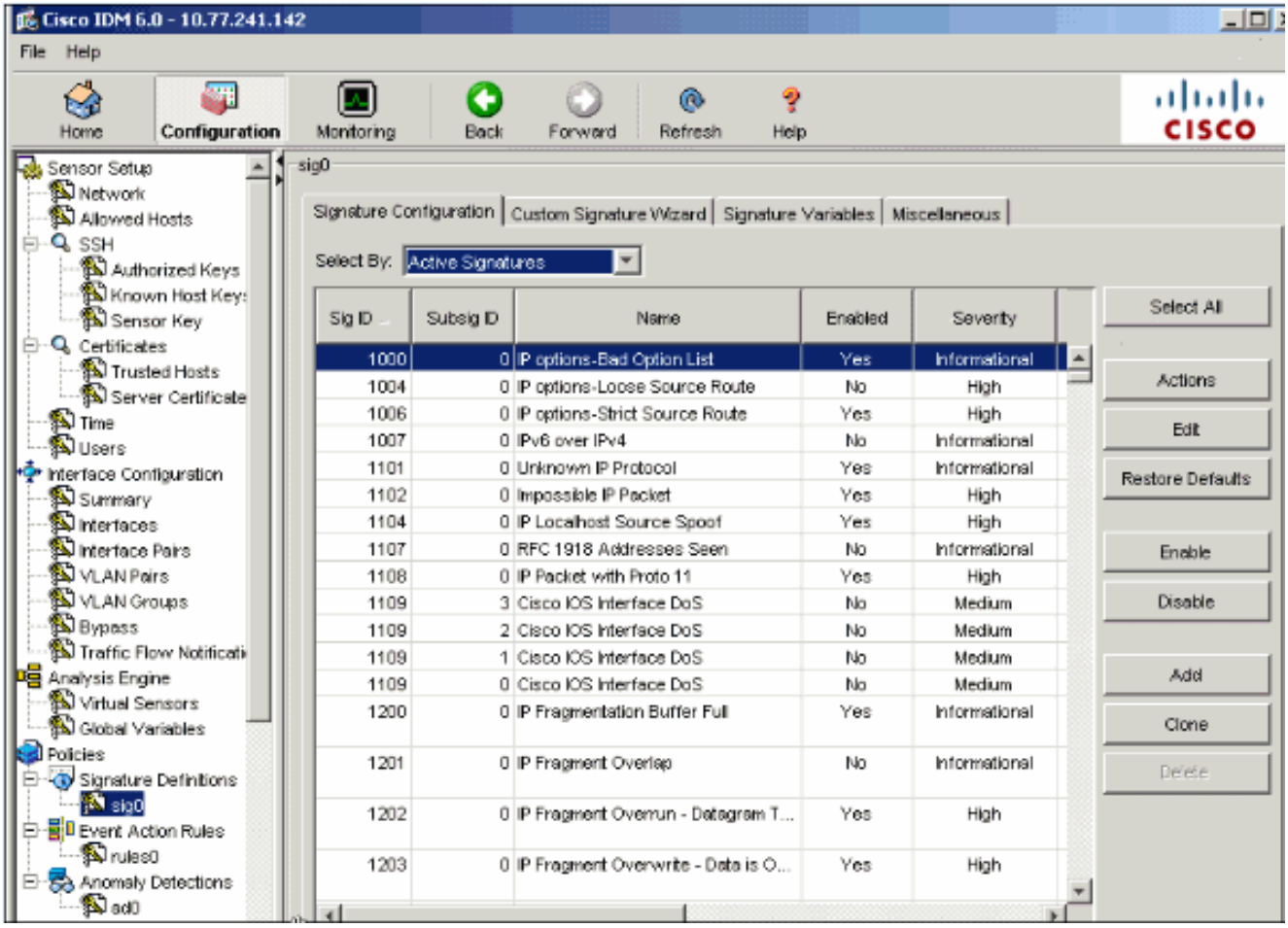
Configuration IDM

Procédez comme suit :

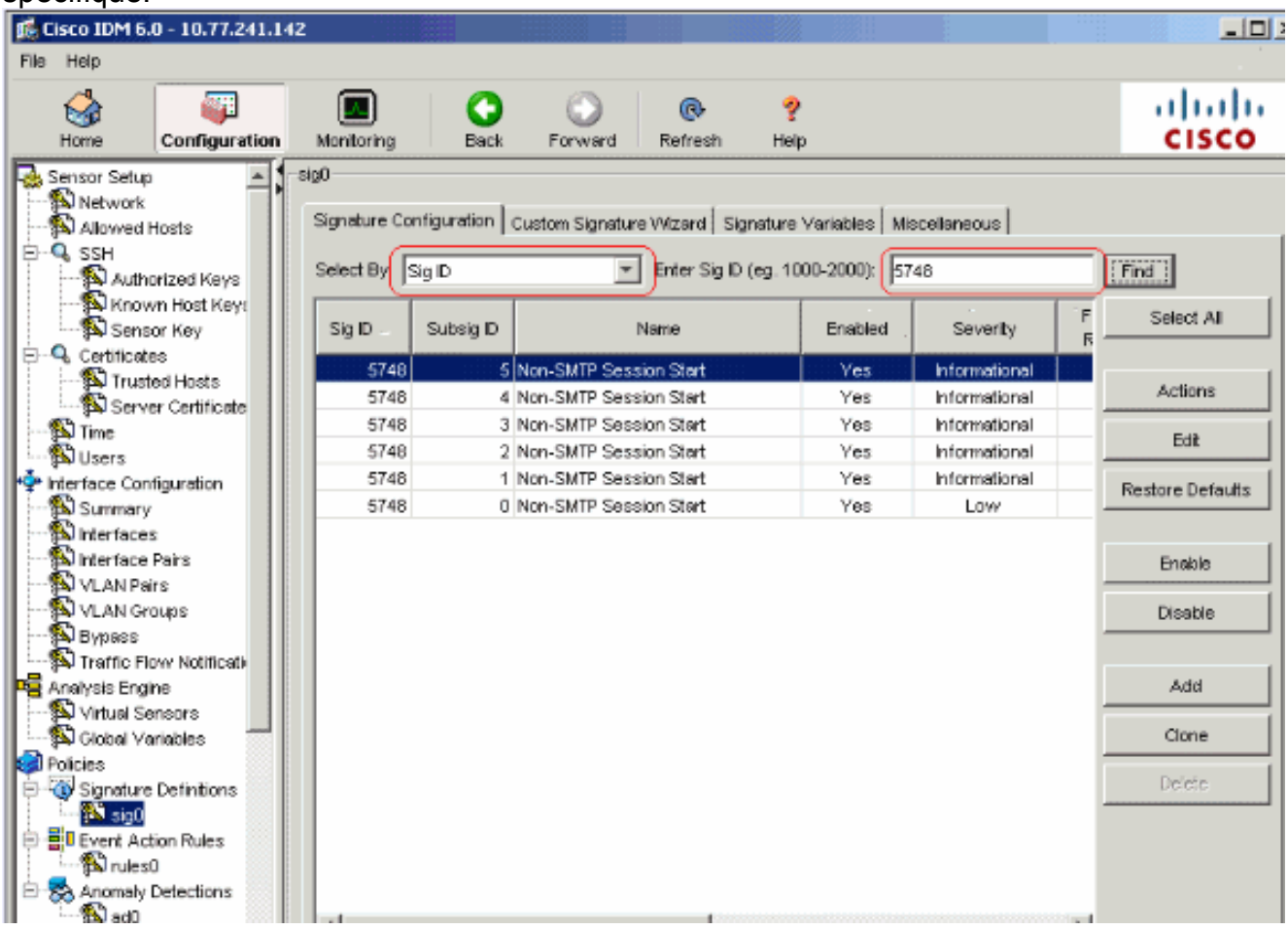
1. Lancement IDM.
2. Cliquez sur **à la maison** afin de voir la page d'accueil de l'IDM. Cette page affiche l'information sur le périphérique.



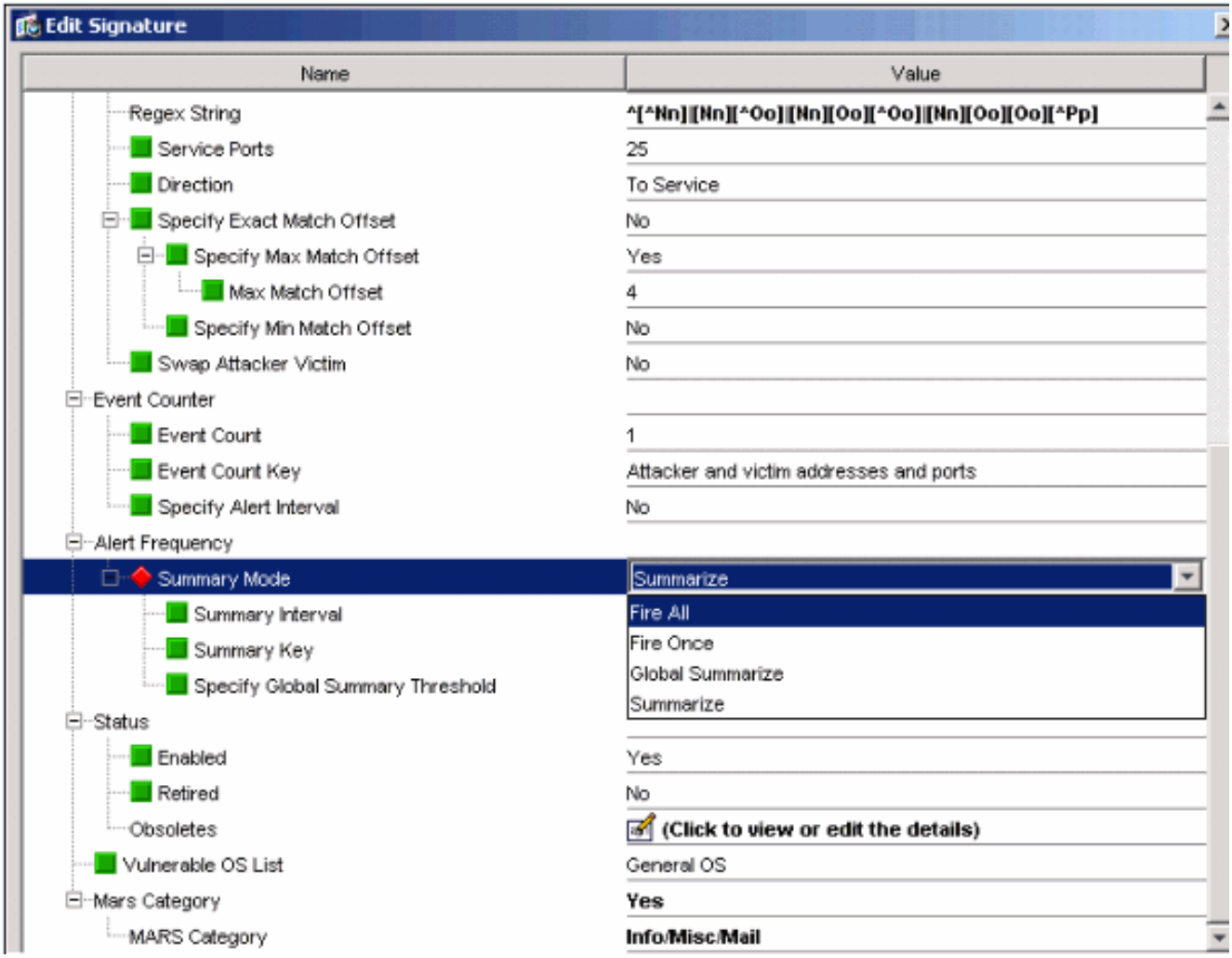
3. Choisissez la **configuration > les stratégies > les définitions de signature > le sig0 > la configuration de signature > sélectionnent par : ID de Sig** afin d'afficher toutes les signatures disponibles dans le capteur.



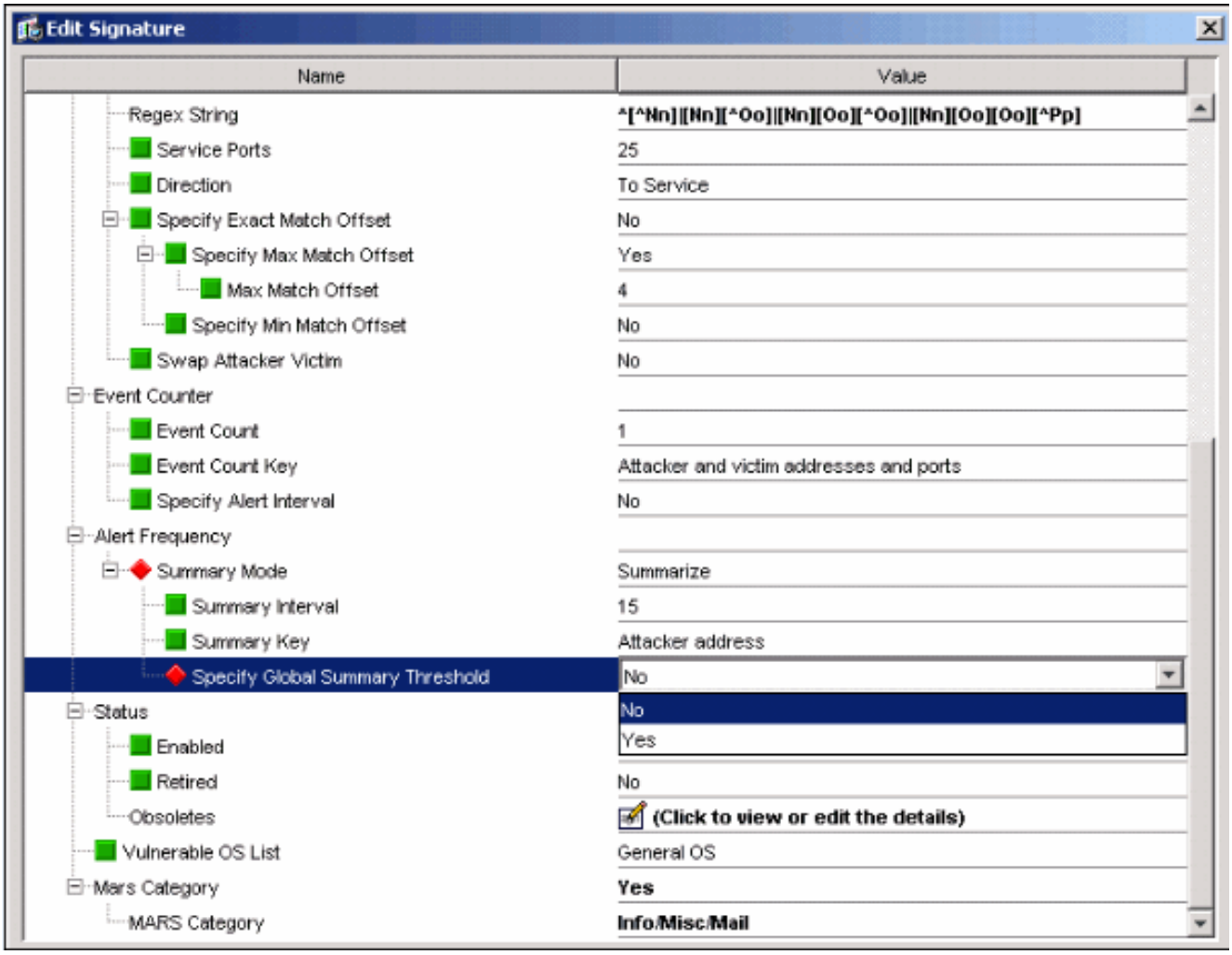
4. Choisissez l'**ID de Sig du** choisi par le menu déroulant et puis écrivez l'ID **5748 de** Sig afin de trouver une signature spécifique.



5. Cliquez sur Edit afin d'éditer la signature.
6. Dans la fenêtre de signature d'éditer, choisissez la **définition de signature > la fréquence d'alerte > mode récapitulatif**, et changez l'action du du **récapitulation pour se déclencher tous** dans le menu déroulant récapitulatif de
mode.



7. Assurez-vous que spécifiez le seuil récapitulatif global est placé à **non.**



Informations connexes

- Page de support de Système de protection contre les intrusions Cisco
- Page de support de Gestionnaire de périphériques Cisco IPS
- Obtenir commencé par l'IOS IPS
- Support et documentation techniques - Cisco Systems