IPS 6.X - Een overzicht van specifieke gebeurtenissen inschakelen/uitschakelen via IDM

Inhoud

Inleiding

Dit document beschrijft hoe u de samenvatting van een specifieke gebeurtenis in IPS-softwareversie 6.x (Inbraakpreventiesysteem) kunt in/uitschakelen met behulp van IPS Apparaatbeheer (IDM).

Opmerking: Toegangslijsten moeten in de IPS-apparaten worden geconfigureerd om toegang te bieden vanaf de host of het netwerk waar beheersoftware zoals IDM en IEV (IDS Event Viewer) geïnstalleerd zijn en goed werken. Raadpleeg het gedeelte Toegangslijst wijzigen van de Cisco-inbraakpreventiesysteem-sensor die de Opdrachtlijn Interface 5.0 gebruikt voor meer informatie.

Voorwaarden

Vereisten

Dit document wordt gemaakt met de aanname dat IPS 6.x geïnstalleerd is en correct werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 4200 Series IPS Sensor die softwareversie 6.0(2)E1 draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

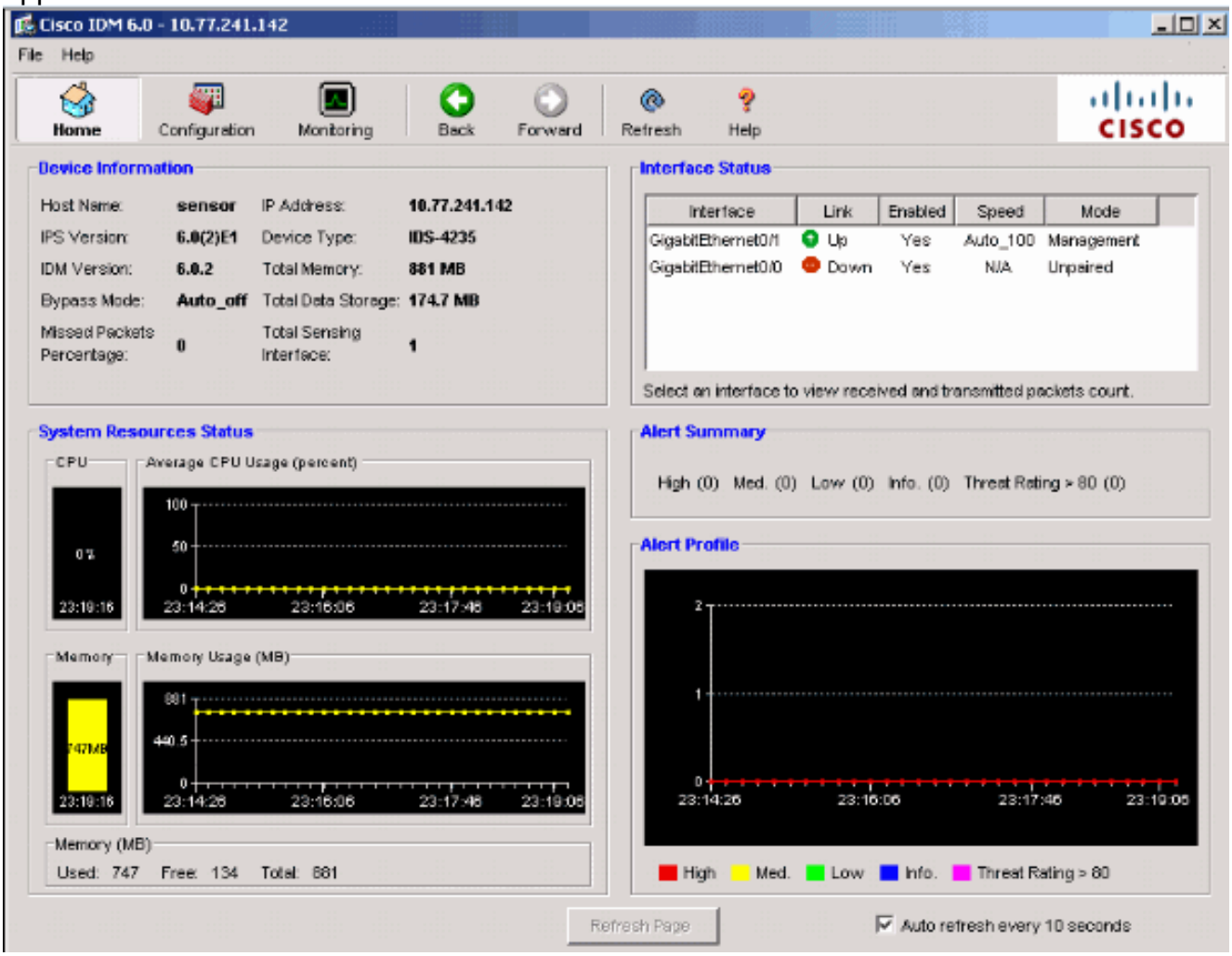
De samenvatting van een specifieke gebeurtenis inschakelen/uitschakelen met IDM

Voor een duidelijk begrip, verstrekt dit gedeelte een voorbeeld waarin u de samenvatting voor de **Ondertekening-ID** in- of uitschakelen**: 5748.**

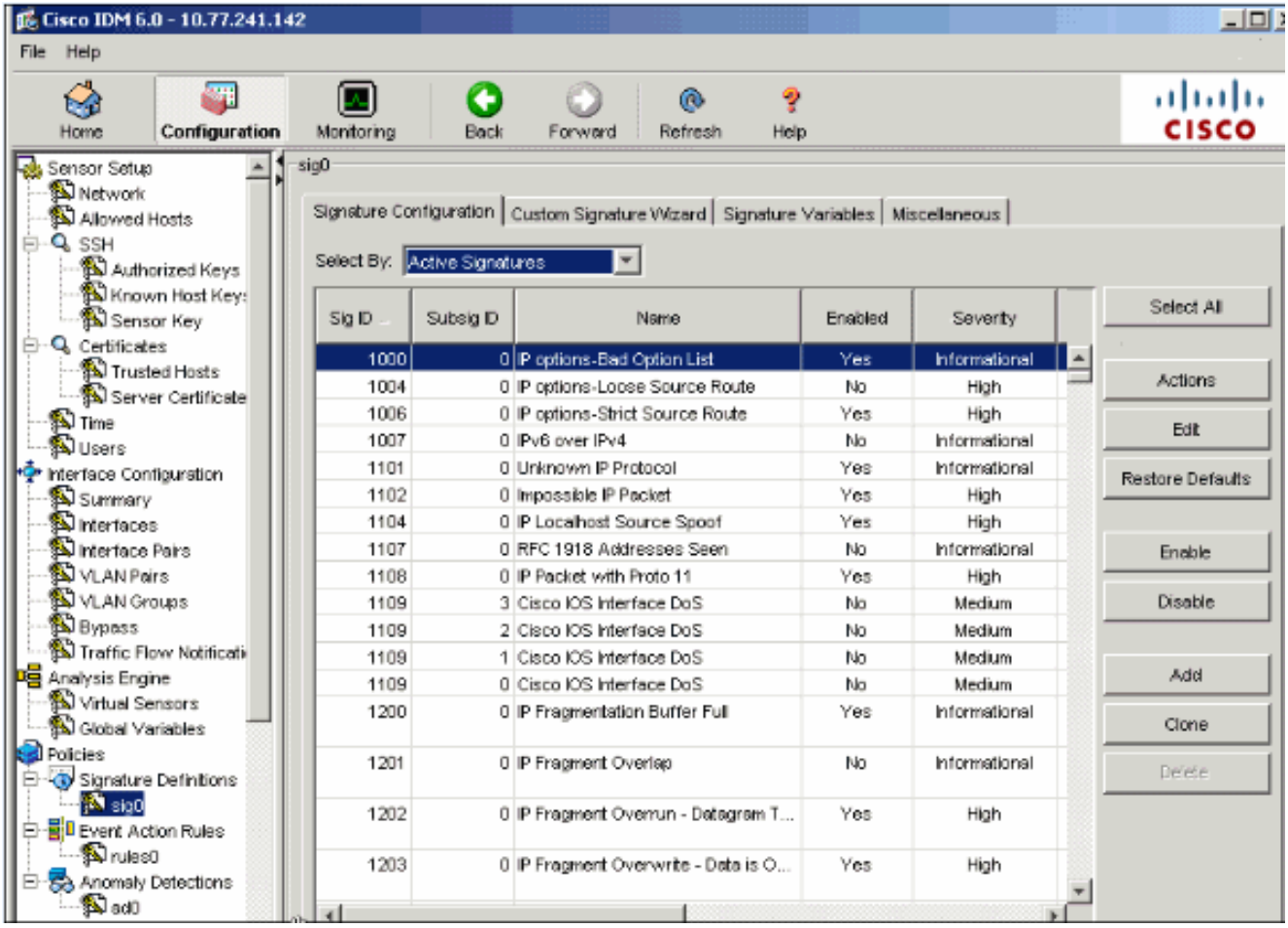
IDM-configuratie

Voer de volgende stappen uit.

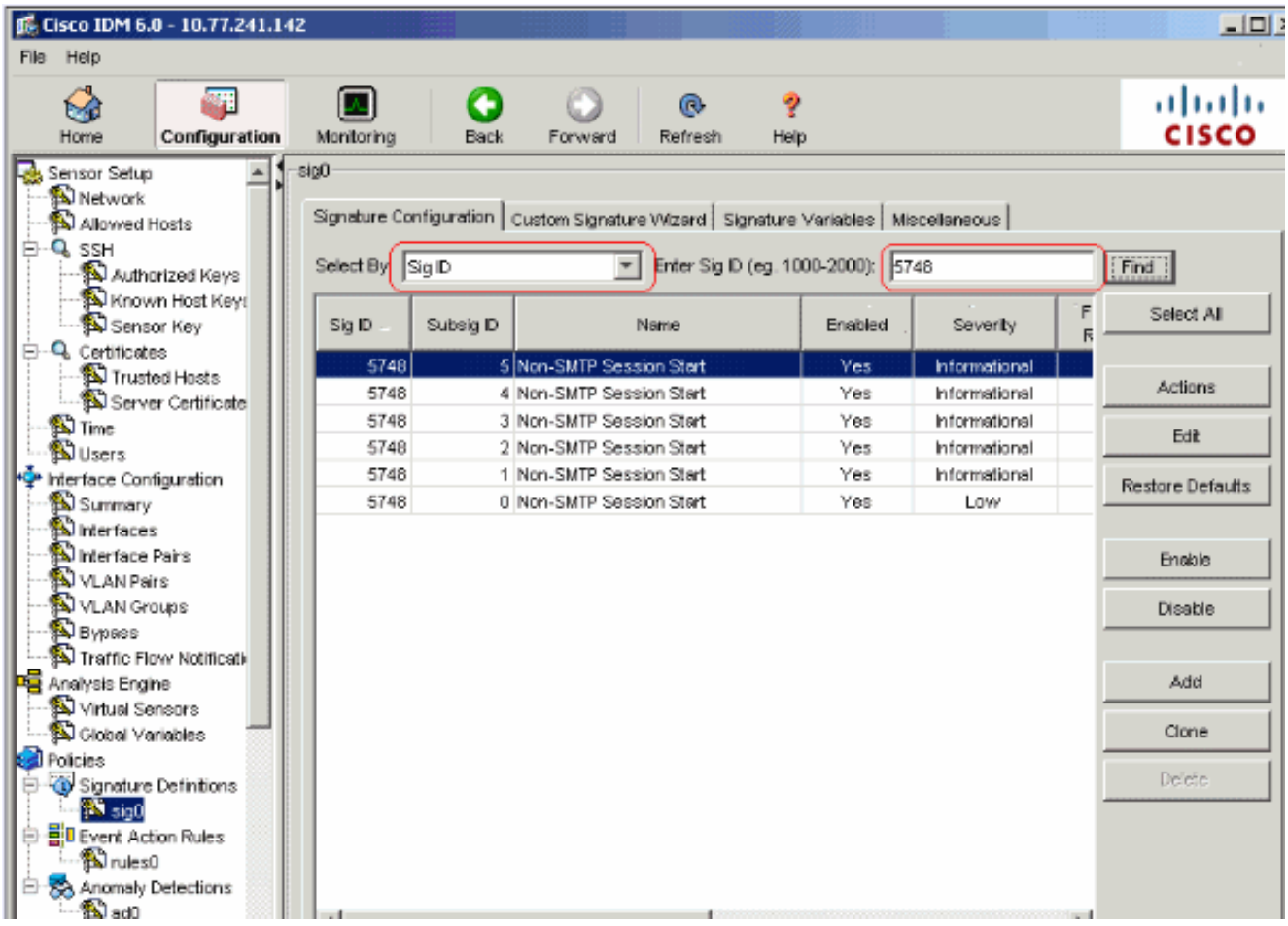
1. Start IDM.
2. Klik op **Home** om de startpagina van de IDM te zien. Deze pagina toont de apparaatinformatie.



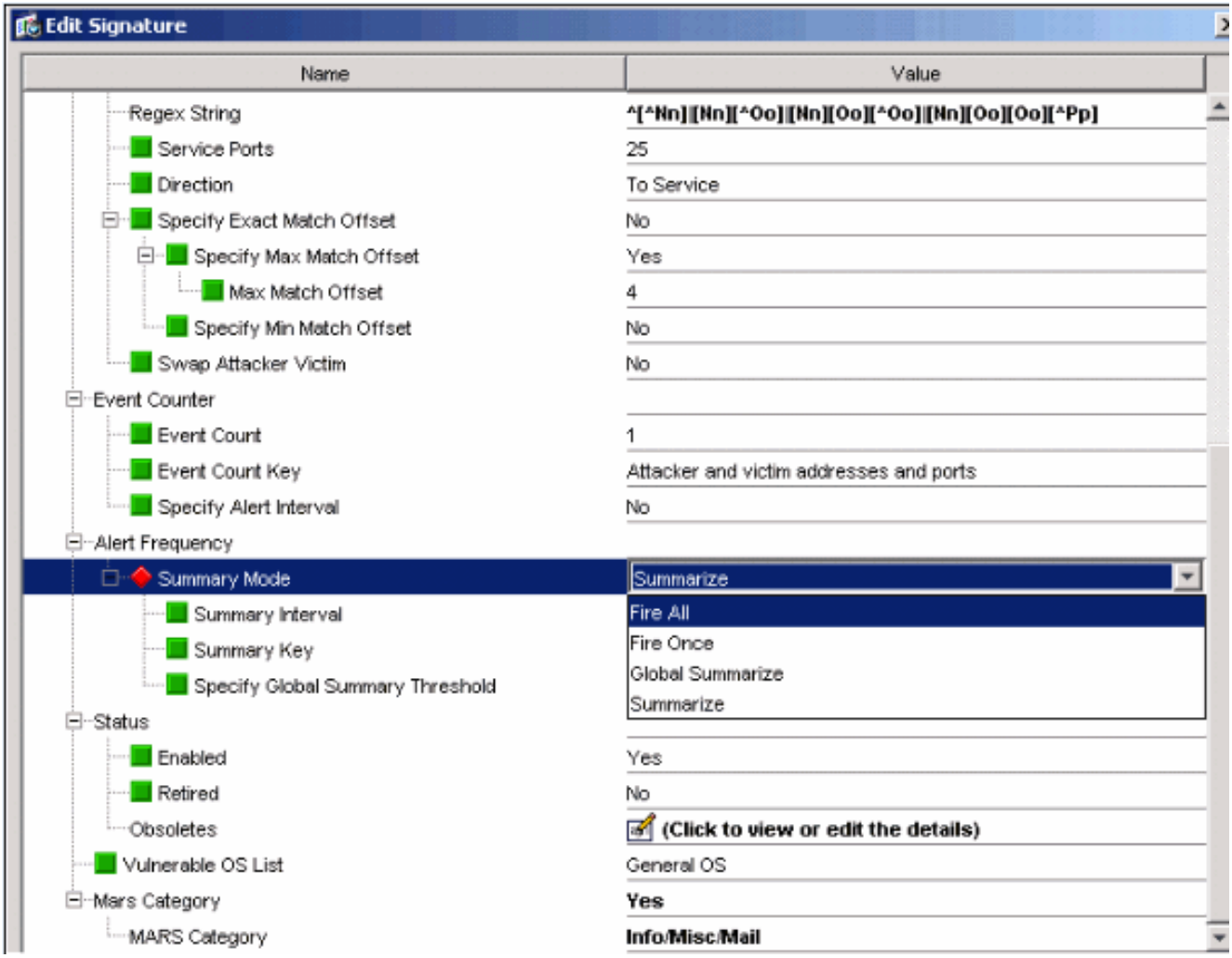
3. Kies **Configuration > Policy > Signature Definitions > sig0 > Signature Configuration > Select by: ID** Sig om alle handtekeningen die in de sensor beschikbaar zijn weer te geven.



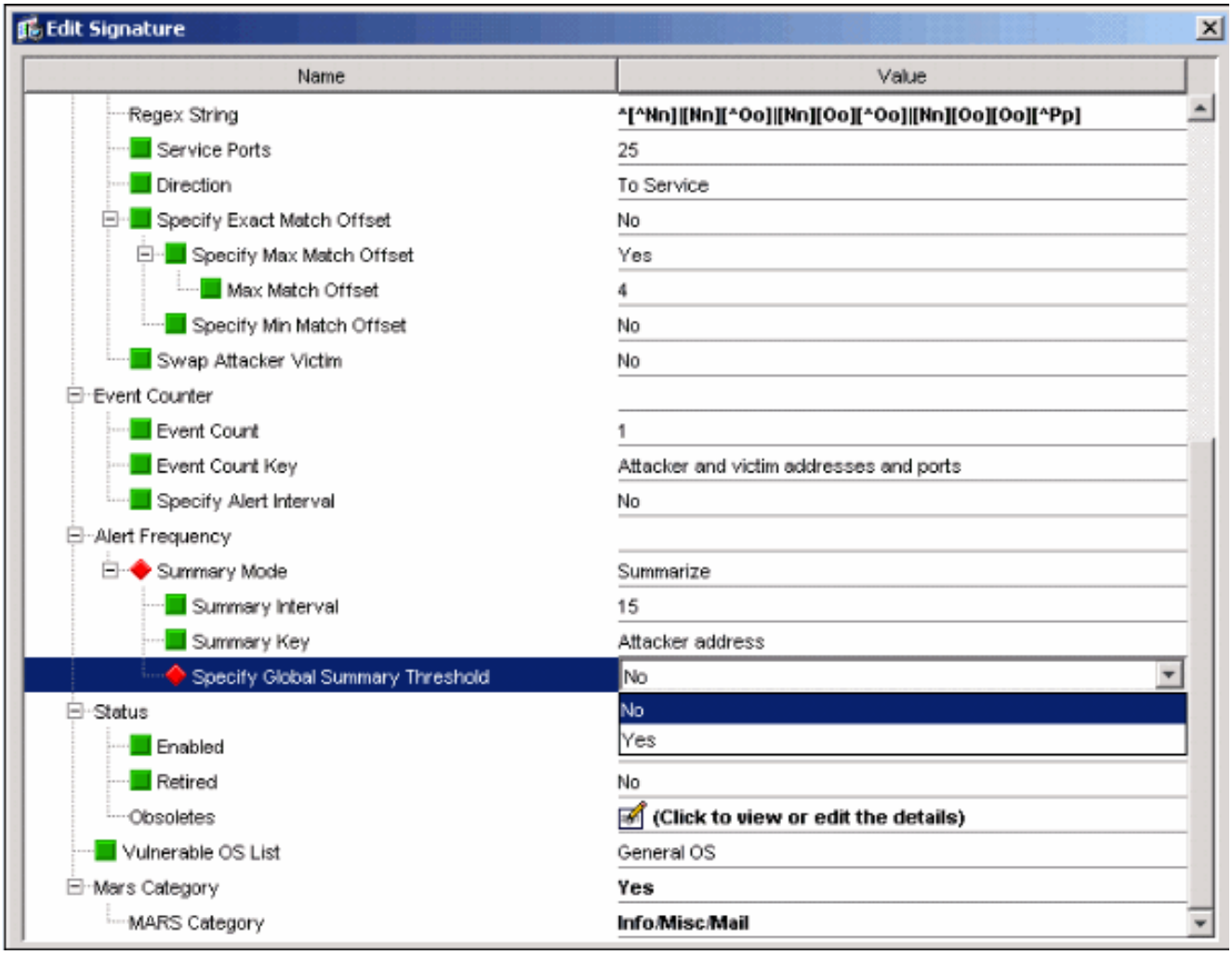
4. Kies **SIG-ID** in het vervolgkeuzemenu Selecteren en voer vervolgens Sig-ID **5748 in** om een specifieke handtekening te vinden.



5. Klik op **Bewerken** om de handtekening te bewerken.
6. Selecteer in het venster Handtekening bewerken de optie **Definitie handtekeningen > Frequentie signaleren > Samenvatting Mode** en wijzig de actie van **Samenvatting** in **Alle** in het vervolgkeuzemenu Samenvatting
   Mode.



7. Zorg ervoor dat de Drempel voor globale samenvatting opgeven op **Nee** is ingesteld.



Gerelateerde informatie

- Categoriepagina voor Cisco-inbraakpreventiesysteem
- Ondersteuning voor Cisco IPS apparaatbeheer
- Introductie met IOS IPS
- Technische ondersteuning en documentatie – Cisco Systems