IPS 6.X: Habilite/neutralización el resumen de un evento específico usando el IDM

Contenido

Introducción

Este documento describe cómo habilitar/neutralización el resumen de un evento específico en la versión de software 6.x del Sistema de prevención de intrusiones (IPS) usando el administrador de dispositivo IPS (IDM).

Note: Las Listas de acceso se deben configurar en los dispositivos IPS para permitir el acceso del host o de la red donde el software de administración tal como IDM y el IEV (IDS Event Viewer) están instalados y trabajan correctamente. Refiera a cambiar la sección de la lista de acceso de configurar el sensor de Cisco Intrusion Prevention System usando la interfaz de línea de comando 5.0 para más información.

prerrequisitos

Requisitos

Este documento se crea con la suposición que el IPS 6.x está instalado y trabaja correctamente.

Componentes Utilizados

La información en este documento se basa en el sensor IPS de las Cisco 4200 Series que funciona con la versión de software 6.0(2)E1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

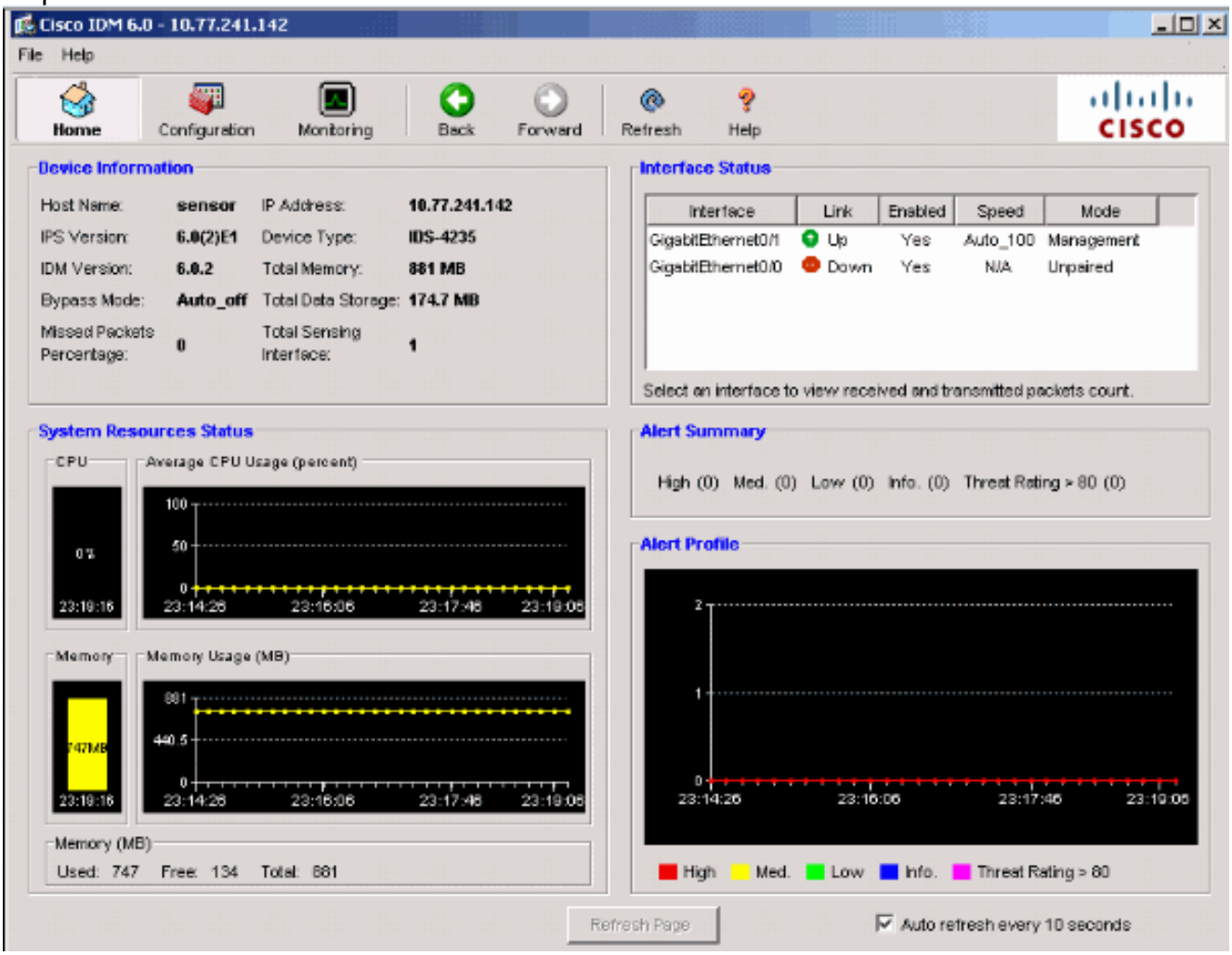
Habilite/neutralización el resumen de un evento específico usando el IDM

Para un conocimiento, esta sección proporciona un ejemplo en el cual usted habilite/neutralización el resumen para el **ID de la firma: 5748**.

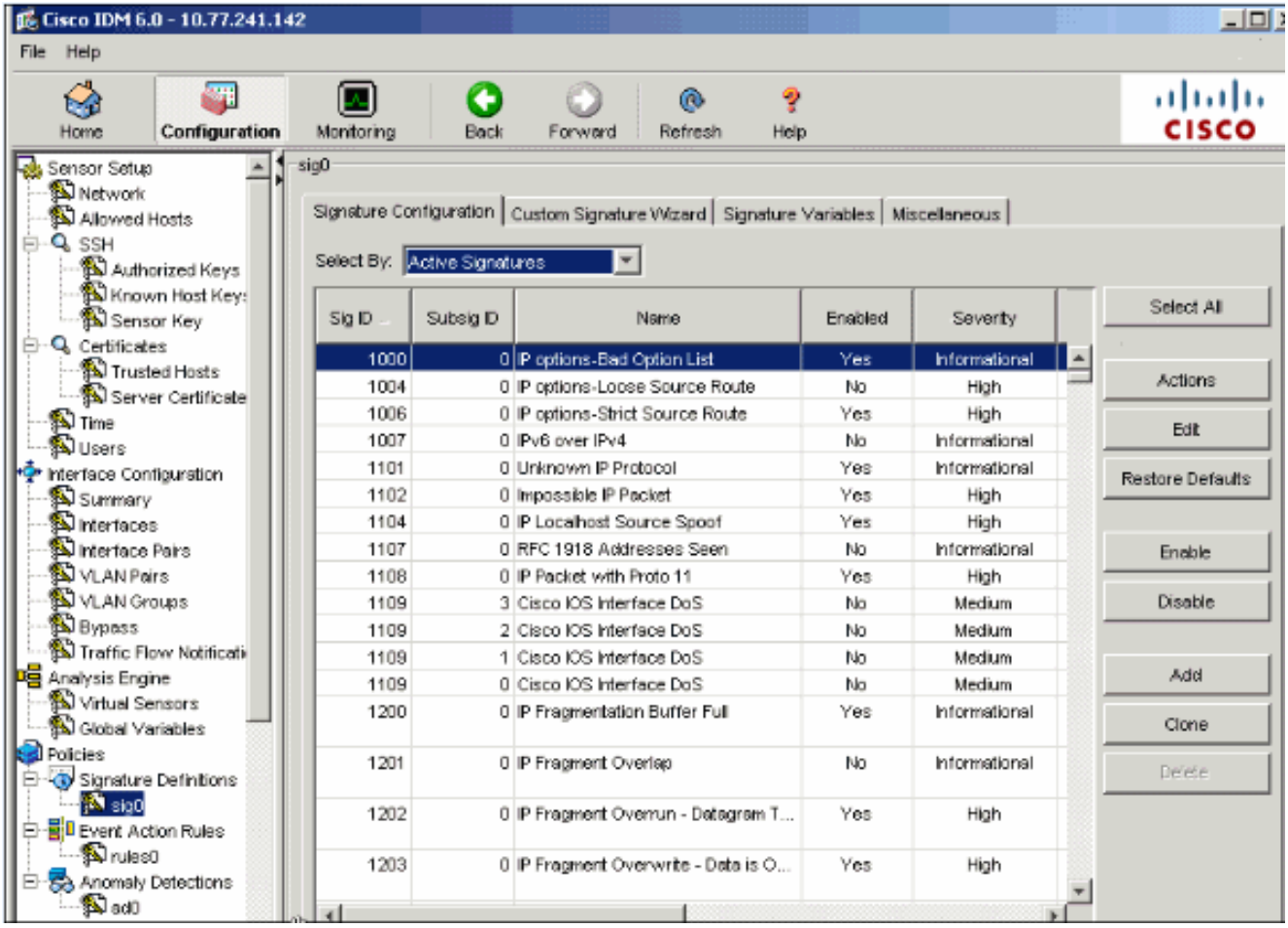
Configuración IDM

Complete estos pasos.

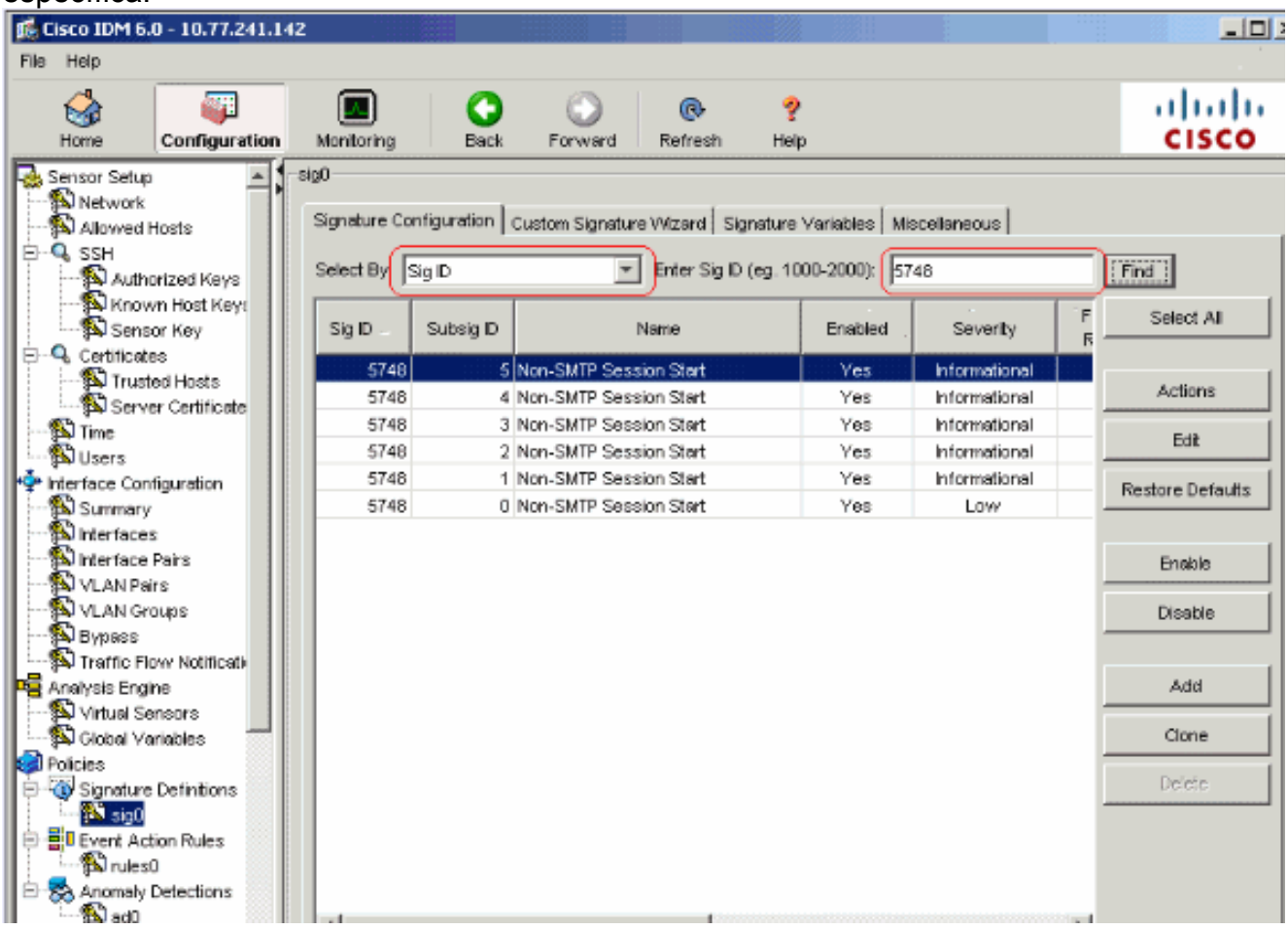
1. Inicie el IDM.
2. Haga clic **a casa** para ver el homepage del IDM. Esta página muestra la información del dispositivo.



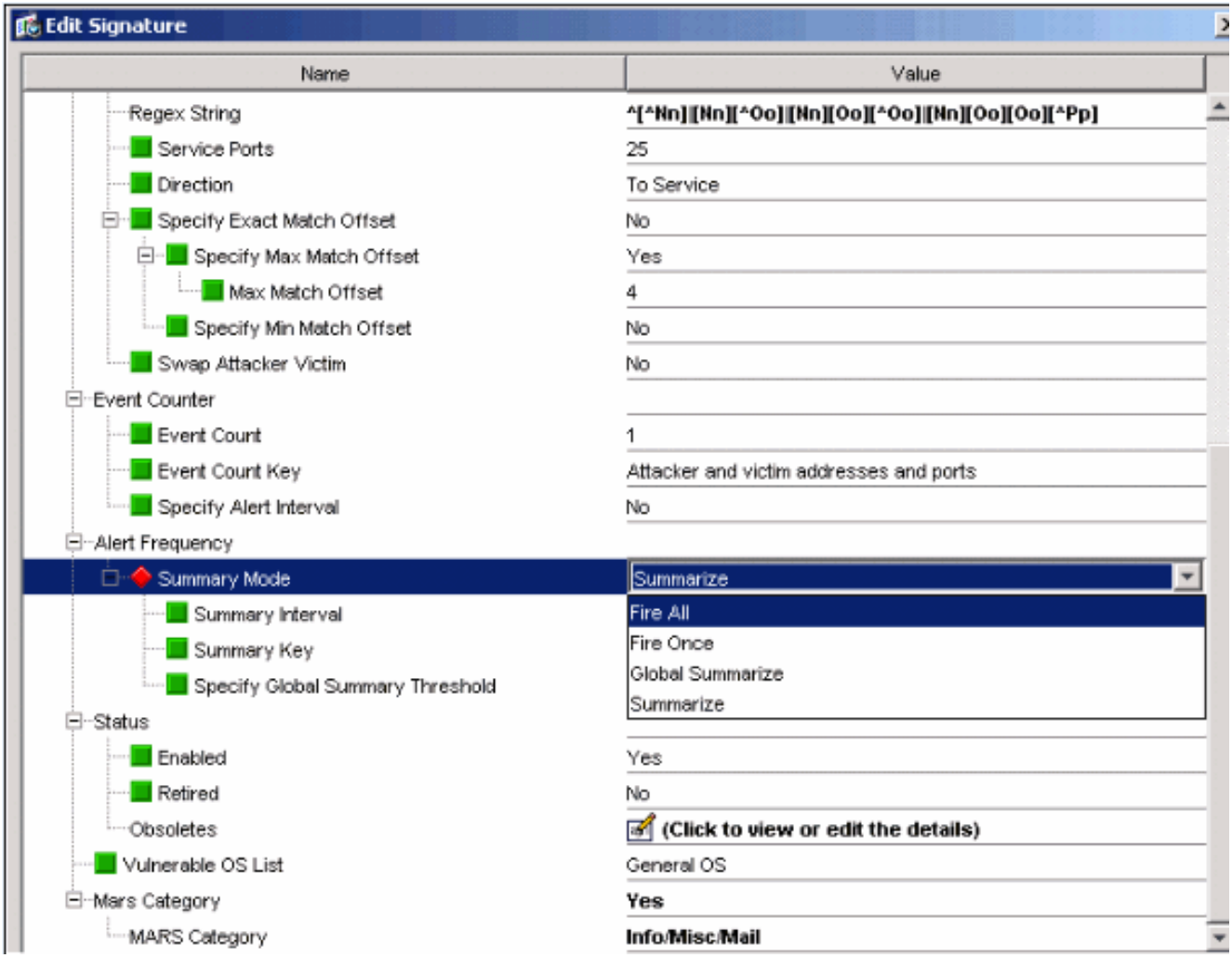
3. Elija la **configuración > las directivas > las definiciones de la firma > sig0 > la configuración de la firma > seleccionan por: Sig ID** para visualizar todas las firmas disponibles en el sensor.



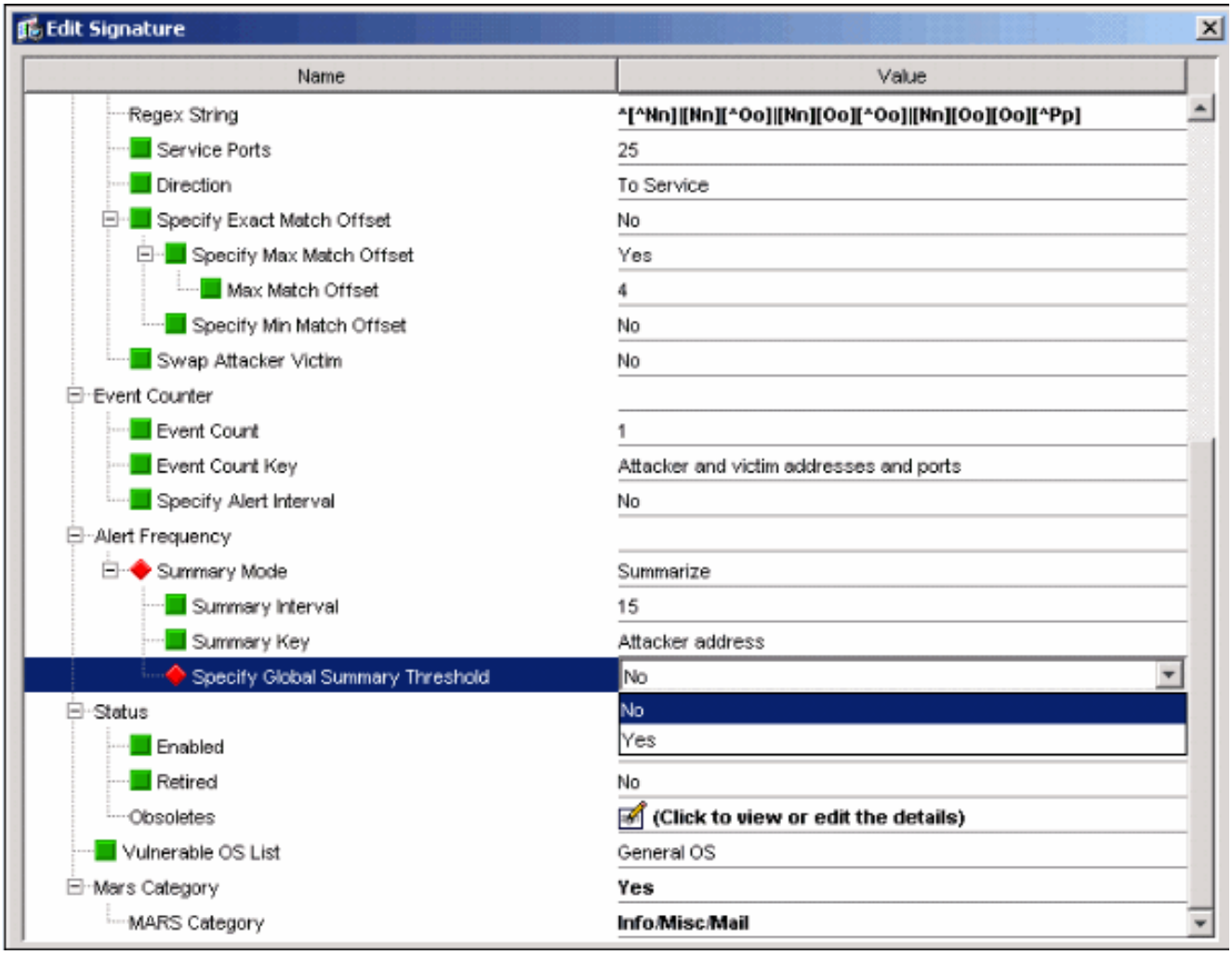
4. Elija los **Sig ID del** selecto por el menú desplegable y después ingrese los Sig ID **5748** para encontrar una firma
específica.



5. El tecleo **edita** para editar la firma.
6. En la ventana de la firma del editar, elija la **definición de la firma > la frecuencia de la alerta > modo sumario**, y cambie la acción del **resumen para encender todos** en el menú desplegable sumario del
   modo.



7. Aseegurese que especifique el umbral sumario global está fijado a **no.**



Información Relacionada

- Página de soporte del Cisco Intrusion Prevention System
- Página de soporte del Cisco IPS Device Manager
- Introducción con IOS IPS
- Soporte Técnico y Documentación - Cisco Systems