IPS 6.X: Permita/desabilitação o sumário de um evento específico usando o IDM

Índice

Introdução

Este documento descreve como permitir/desabilitação o sumário de um evento específico na versão de software 6.x do Intrusion Prevention System (IPS) usando o gerenciador de dispositivo IPS (IDM).

Nota: As Listas de acesso devem ser configuradas nos dispositivos IPS a fim permitir o acesso do host ou da rede onde o software de gestão tal como o IDM e o IEV (IDS Event Viewer) são instalados e trabalham corretamente. Refira a mudança da seção da lista de acessos de configurar o sensor de Sistema de prevenção de intrusões da Cisco usando a interface da linha de comando 5.0 para mais informação.

Pré-requisitos

Requisitos

Este documento é criado com a suposição que o IPS 6.x está instalado e trabalha corretamente.

Componentes Utilizados

A informação neste documento é baseada no sensor IPS do Cisco 4200 Series que executa a versão de software 6.0(2)E1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

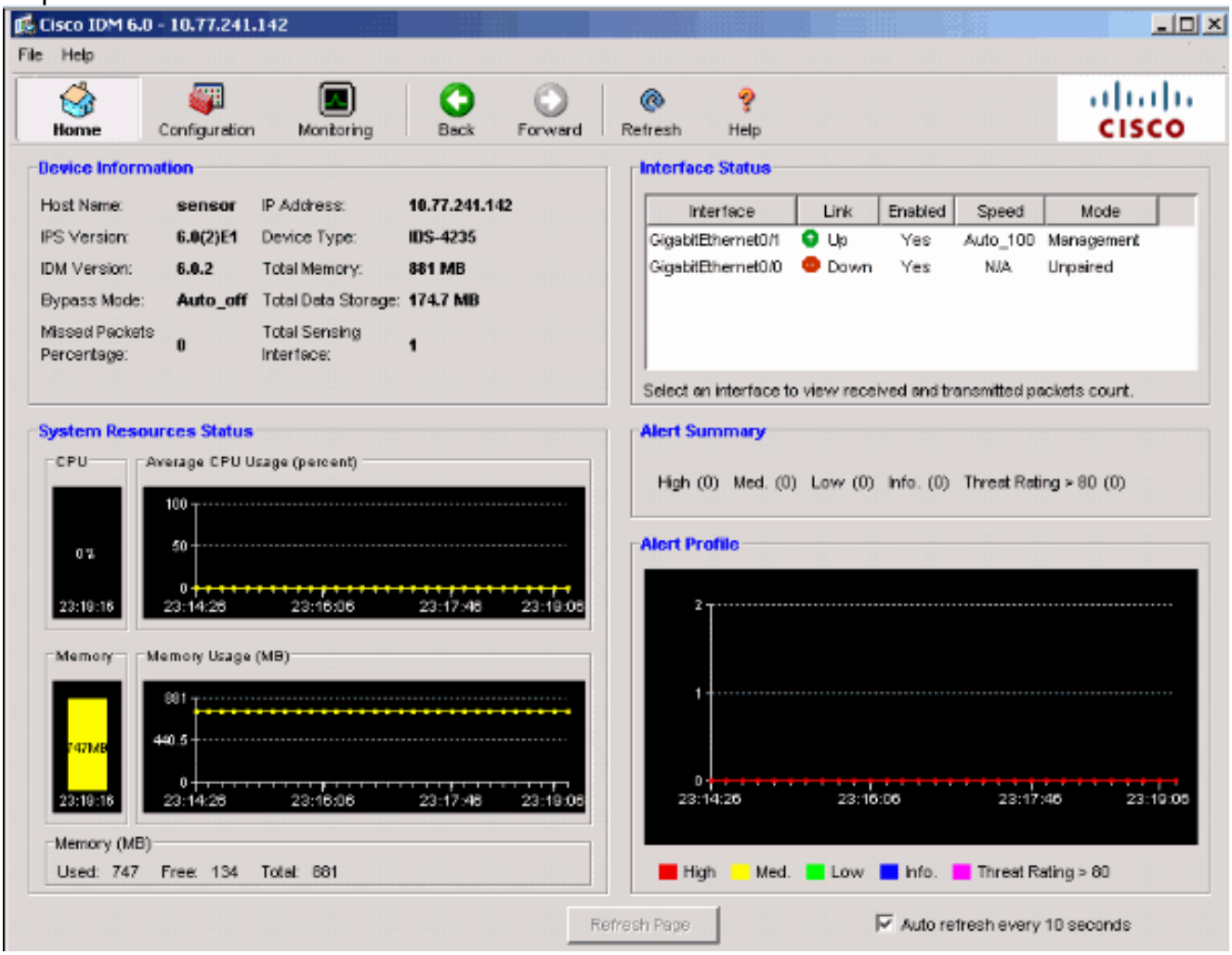
Permita/desabilitação o sumário de um evento específico usando o IDM

Para um entendimento claro, esta seção fornece um exemplo em que você permite/desabilitação o sumário para o **ID de assinatura: 5748**.

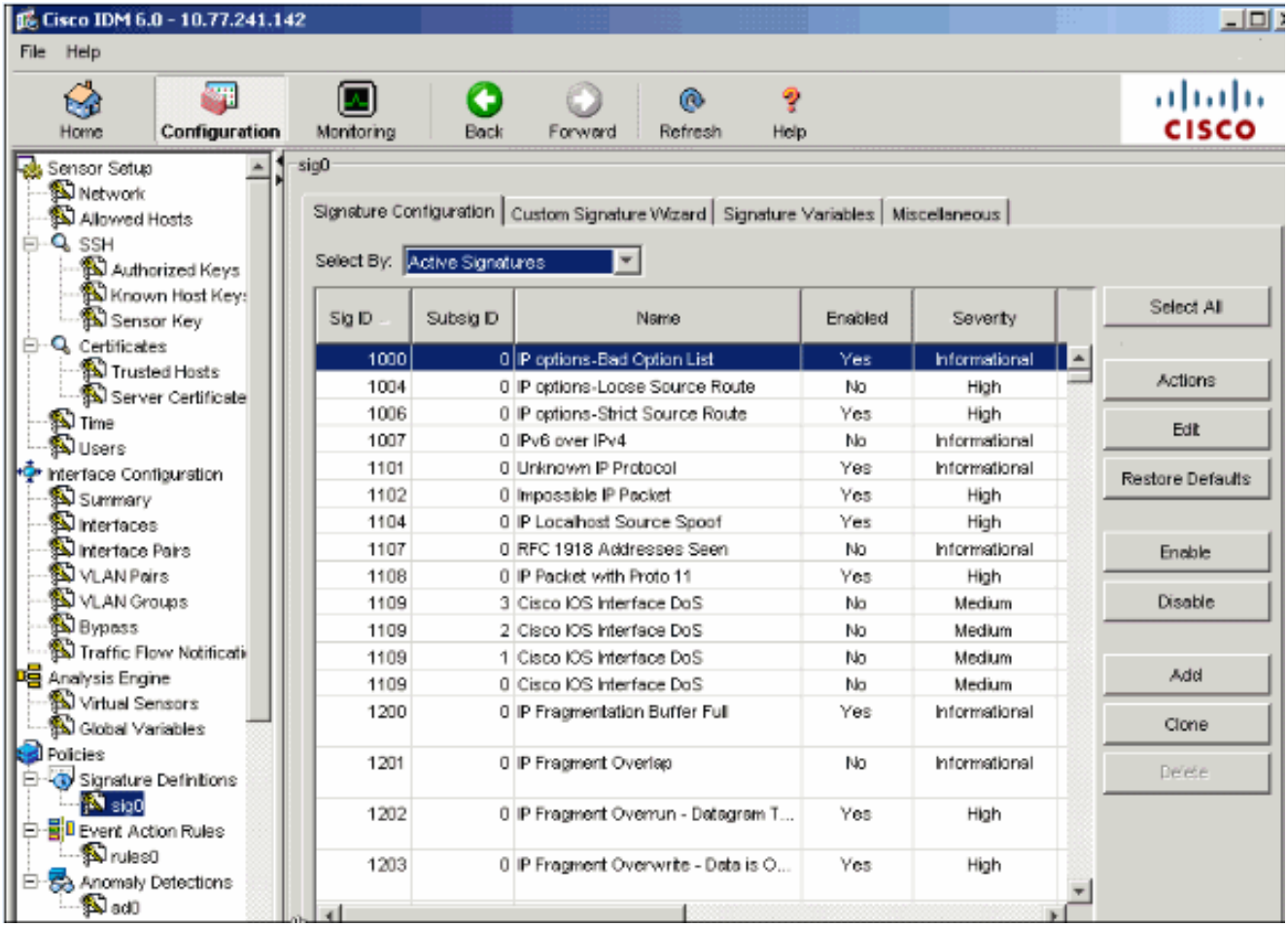
Configuração IDM

Termine estas etapas.

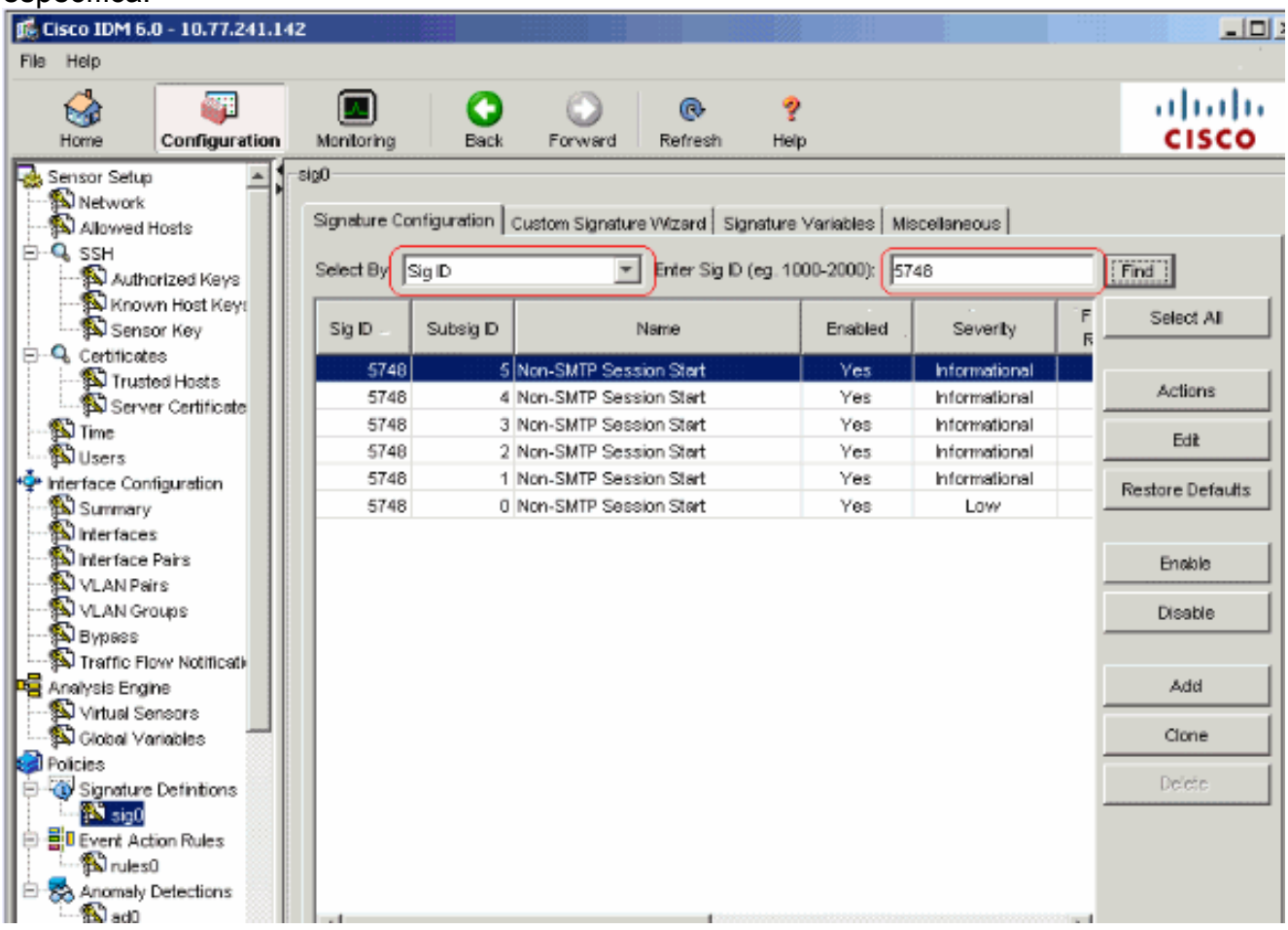
1. Lance o IDM.
2. Clique **em casa** a fim ver o homepage do IDM. Esta página mostra a informação do dispositivo.



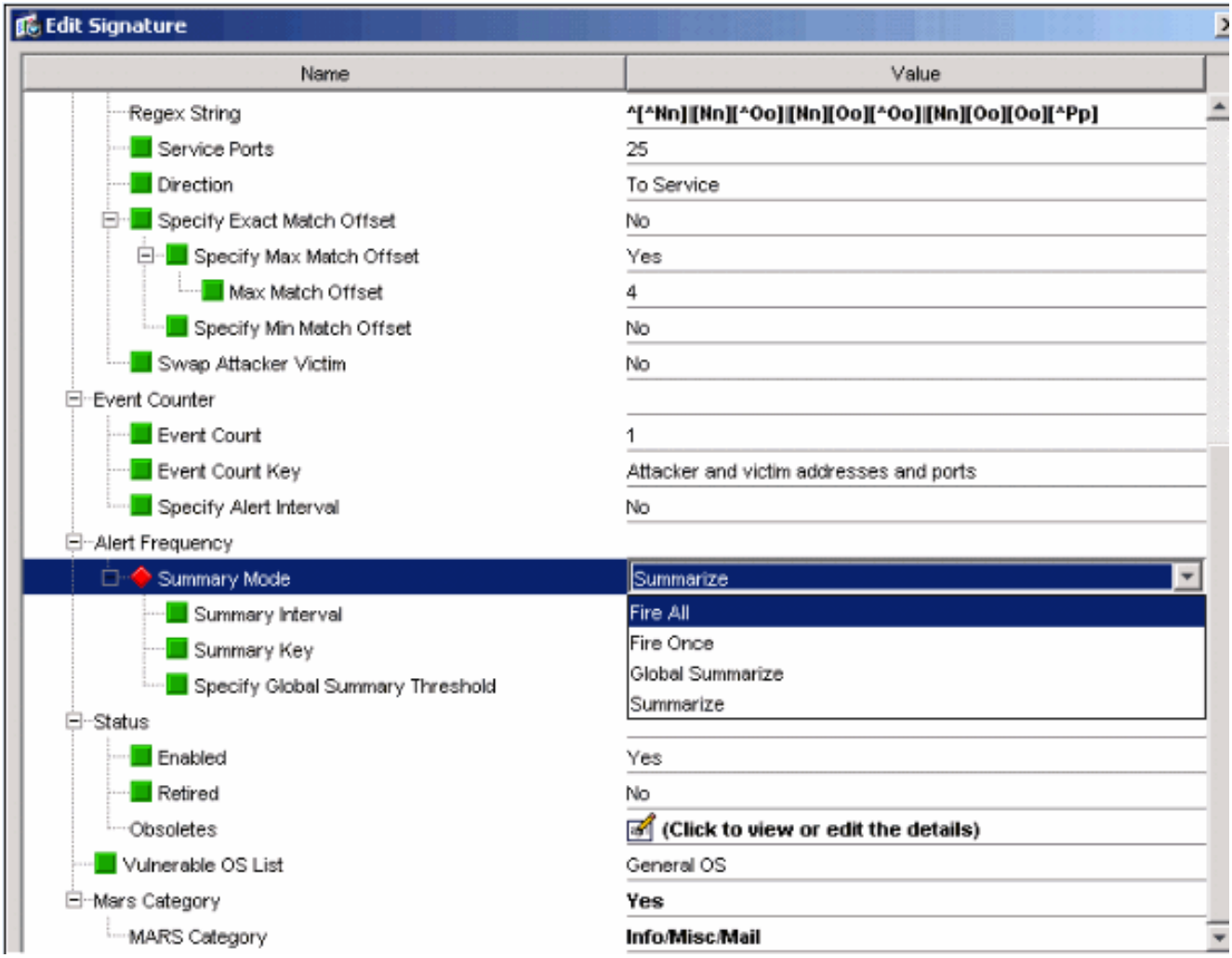
3. Escolha a **configuração > as políticas > as definições da assinatura > o sig0 > a configuração da assinatura > selecionam por: Sig ID** a fim indicar todas as assinaturas disponíveis no
sensor.



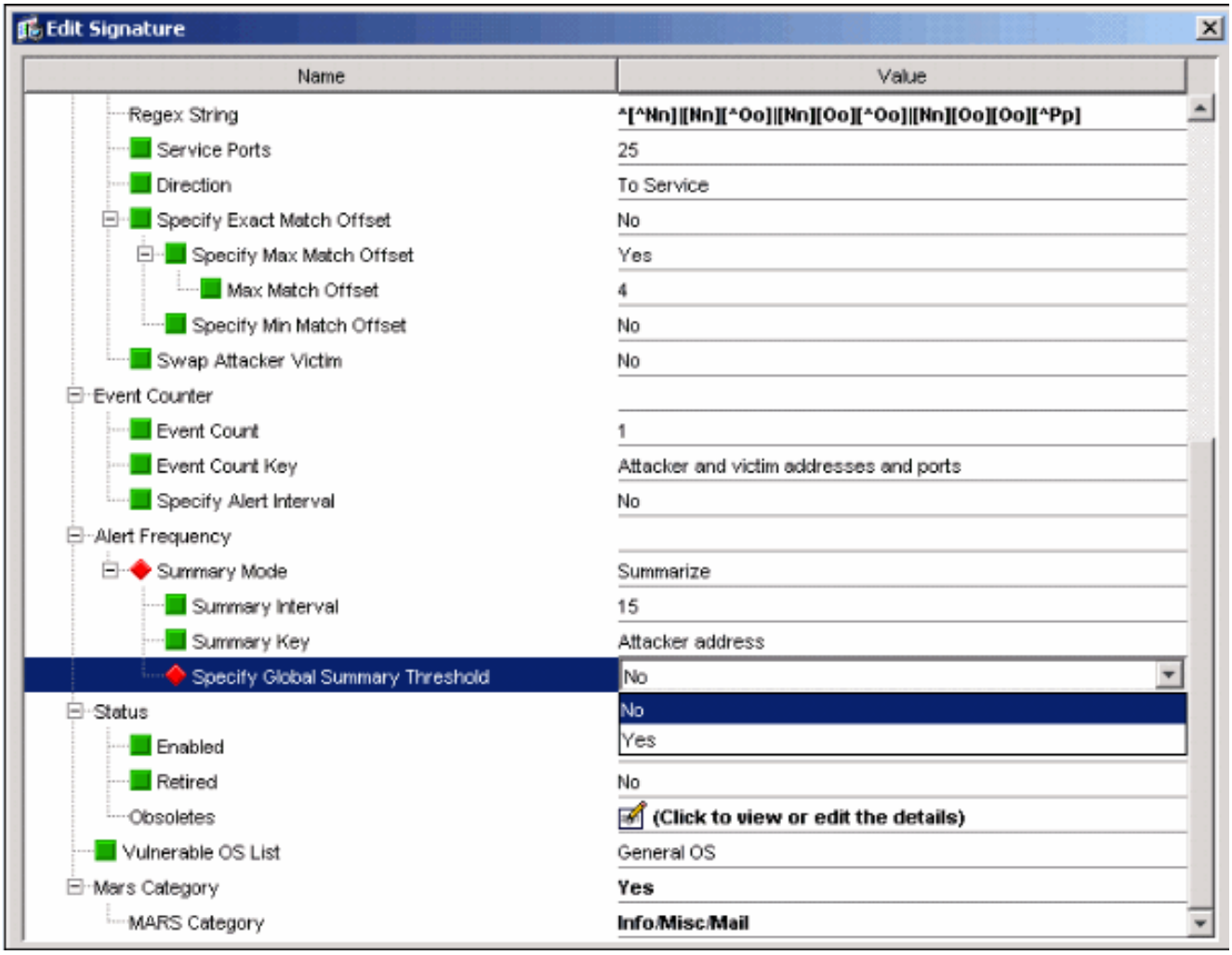
4. Escolha os **Sig ID do** seleto pelo menu suspenso e entre então nos Sig ID **5748** a fim encontrar uma assinatura
específica.



5. O clique **edita** a fim editar a assinatura.
6. No indicador da assinatura da edição, escolha a **definição da assinatura > a frequência do alerta > modo sumário**, e mude a ação do **resumem para atear fogo a tudo no** menu suspenso sumário do
   modo.



7. Certifique-se de que especifique o ponto inicial sumário global está ajustado a **não.**



Informações Relacionadas

- Página de suporte do Sistema de prevenção de intrusões da Cisco
- Página de suporte do Cisco IPS Device Manager
- Obtenção começado com IO IPS
- Suporte Técnico e Documentação - Cisco Systems