Monitore os eventos gerados pelo sistema da prevenção de intrusão do Cisco IOS usando o gerente IPS expresso

Índice

Introdução

Este documento explica como usar os eventos do monitor gerados pelo sistema da prevenção de intrusão do Cisco IOS (IOS-IPS) que usa o gerente IPS expresso (IME).

O Cisco IOS IPS é uma característica com base no software da inspeção do profundo-pacote que abrande eficazmente um amplo intervalo dos ataques de rede.

Cisco IME é um software simples, com base em GUI do Gerenciamento de IPS.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter o conhecimento destes assuntos.

- Sistema da prevenção de intrusão do Cisco IOS
- Gerente IPS expresso

Componentes Utilizados

A informação neste documento é baseada no sistema da prevenção de intrusão do Cisco IOS usando o gerente IPS expresso.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Recursos

Exigência:

Para que IME apoie IO IPS, o roteador precisa de executar Cisco IOS Software Releases 12.3(14)T7 e 12.4(15)T2 ou mais novo. IME pode apoiar até os dispositivos 10.

Nota: IME apoia somente o monitoramento de evento para IO IPS. A configuração não é apoiada.

Configuração

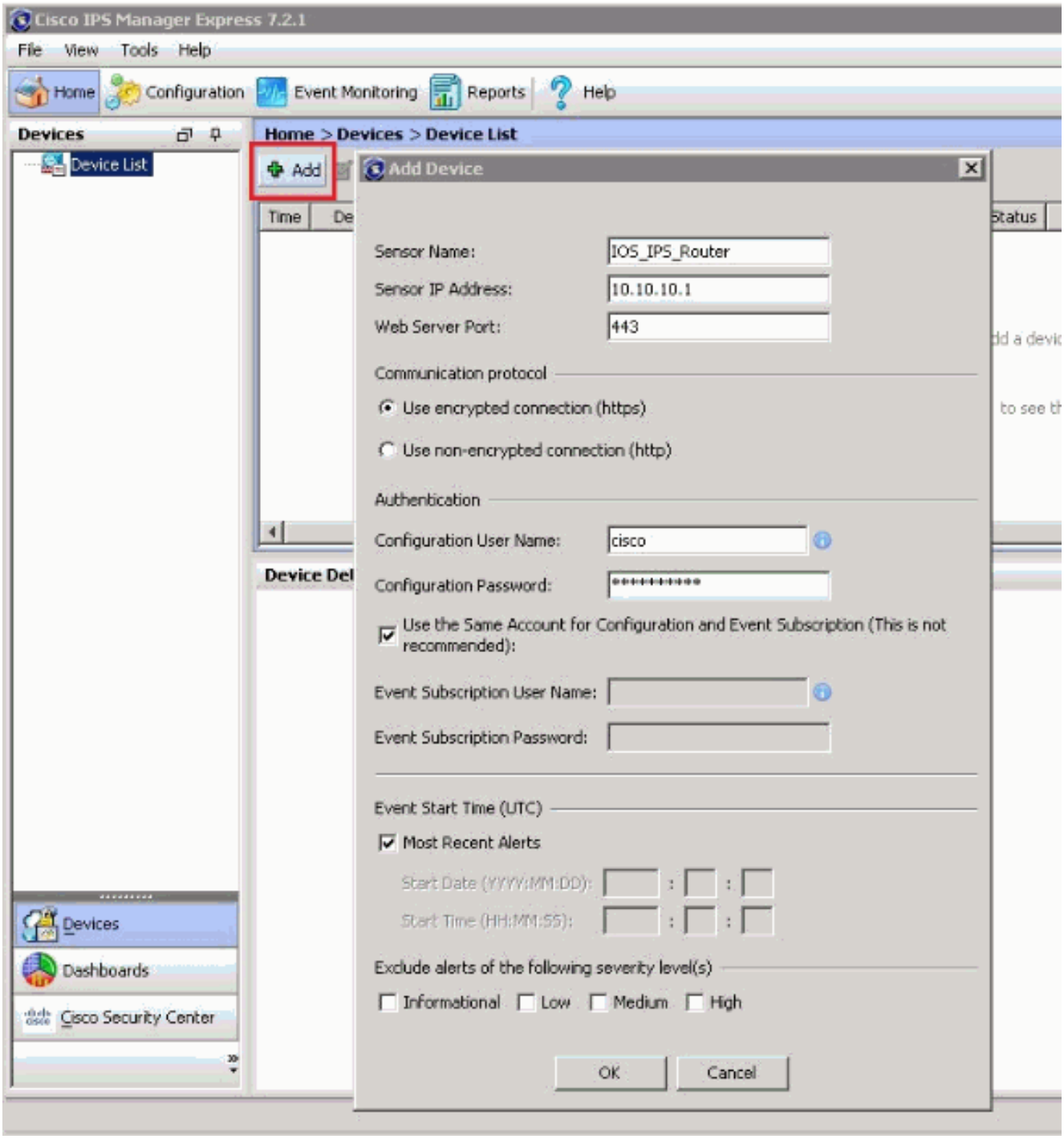
IME usa SDEE para obter eventos de IO IPS. A notificação SDEE é desabilitada à revelia e deve manualmente ser permitida. Para usar SDEE, o servidor de Web do roteador deve ser permitido. À revelia, IME tenta estabelecer uma conexão segura ao roteador que usa HTTPS (TCP 443). Isto exige um certificado digital ser configurado no roteador. Opcionalmente, IME pode ser configurado para apoiar uma conexão inseguro usando HTTP (TCP 80).

Configurando o Roteador

1. Permita a notificação SDEE:`Router(config)# ip ips notify sdee`
2. Permita o HTTPS:`Router(config)#ip http secure-server`
3. Permita o HTTP (opcional):`Router(config)# ip http server`

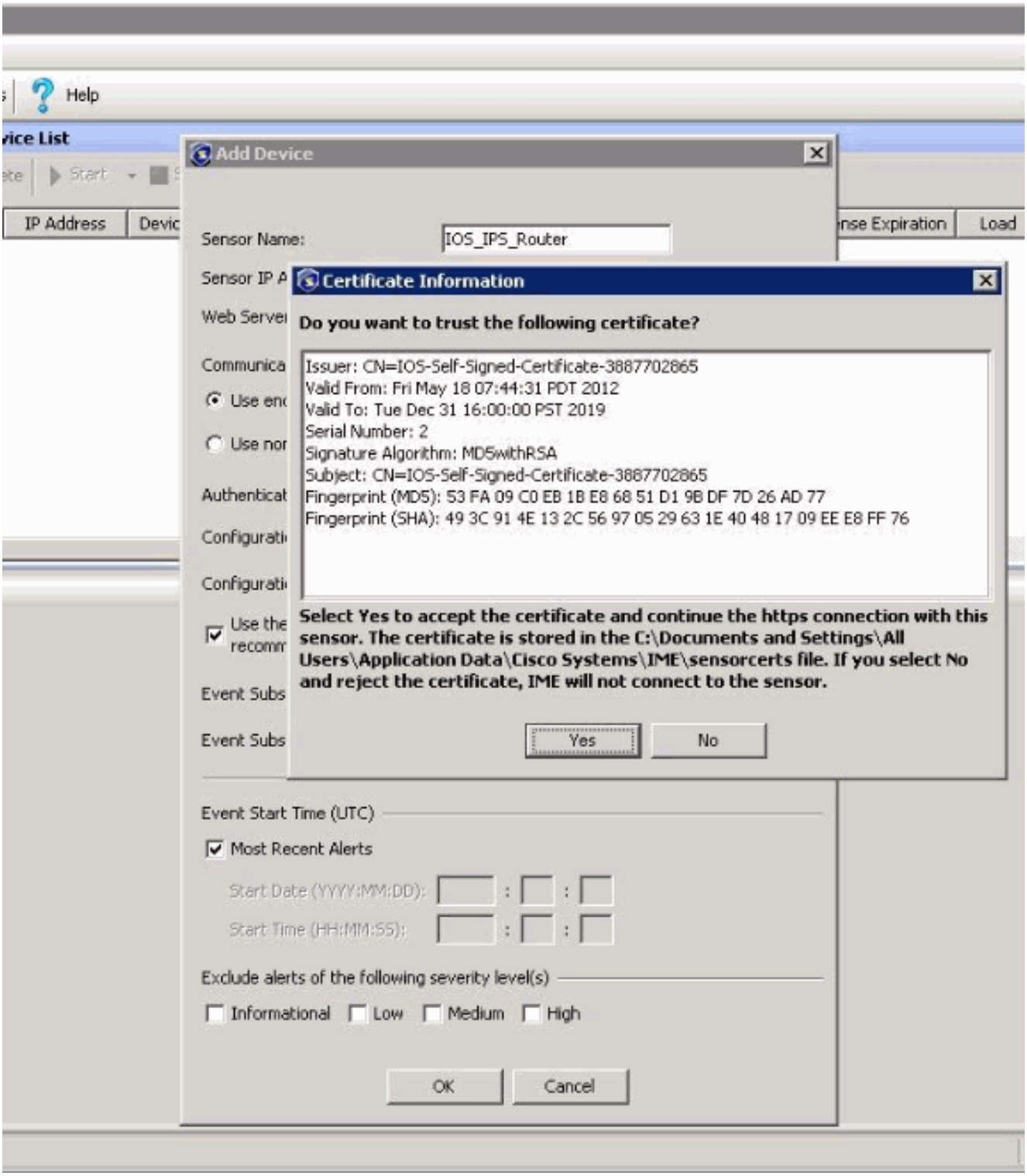
Configurando IME

1. Transfira e instale IME. Execute IME. Então, o clique **adiciona**.Transferência IME:http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

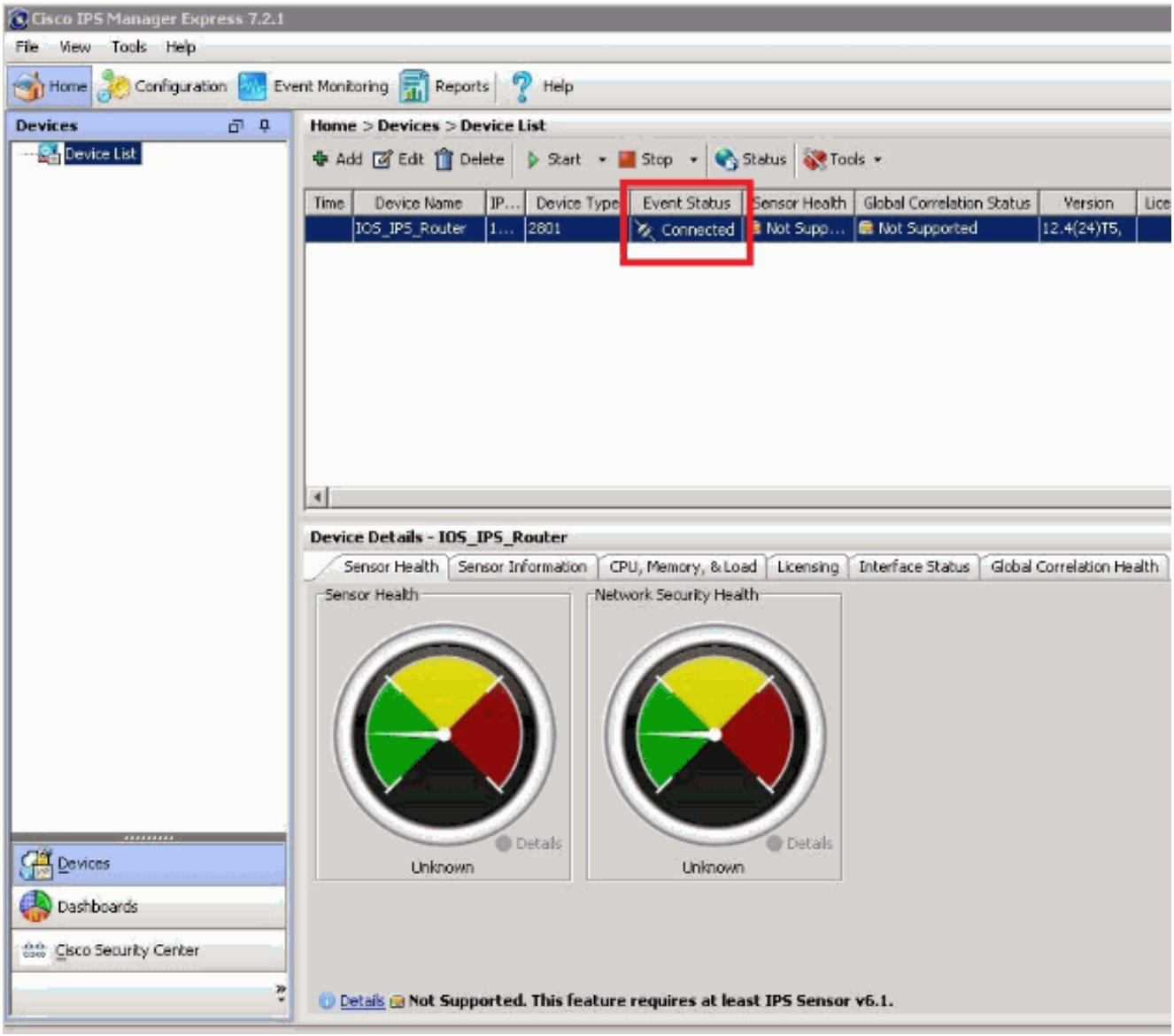


Nota: A configuração padrão usa HTTPS e porta 443 para conectar ao roteador. Você pode igualmente escolher conectar usando o HTTP somente, e muda a porta a 80.

2. Se usando o HTTPS, você é presentado com uma tela para aceitar o certificado auto-assinado do roteador. Clique em
Sim.

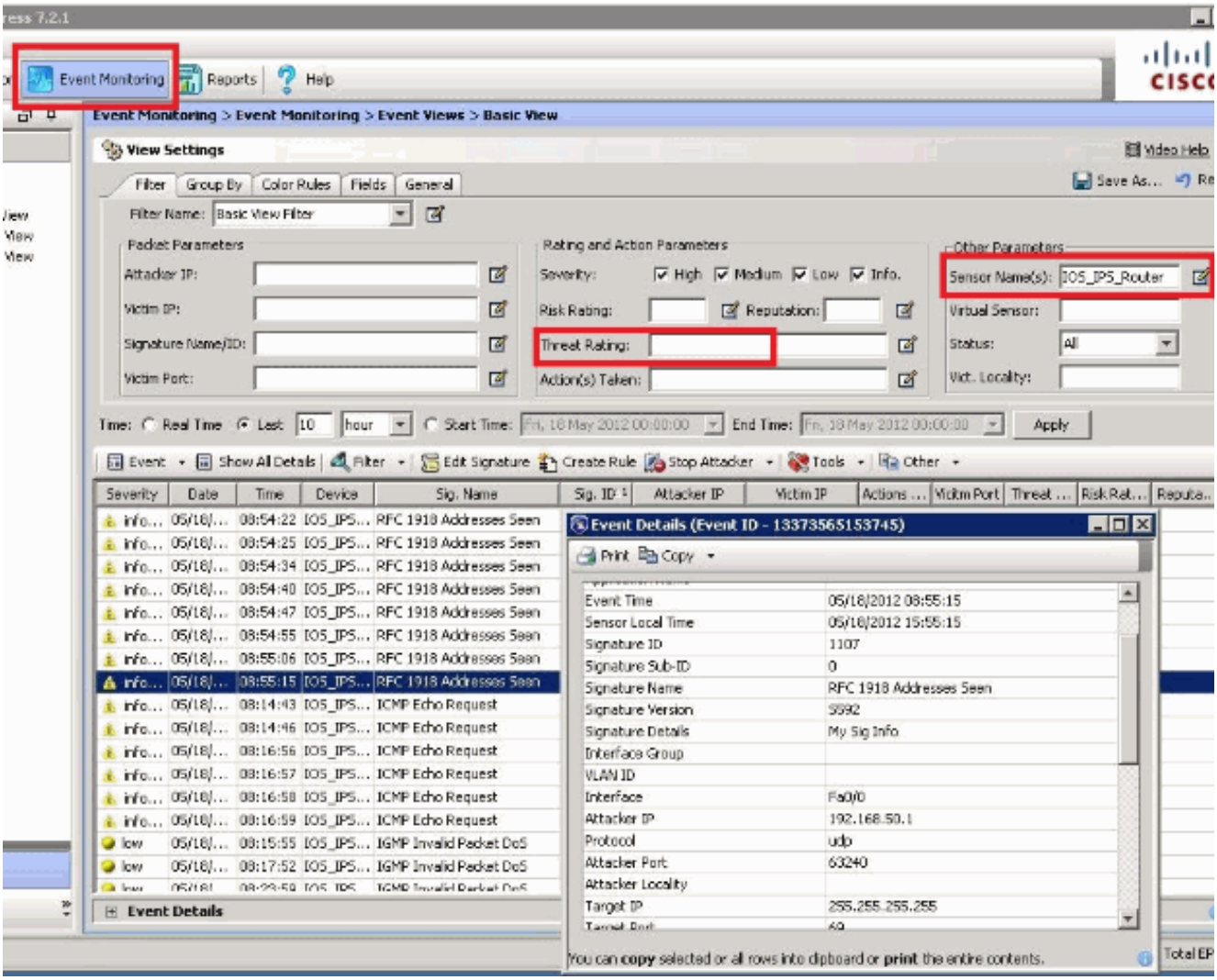


Uma vez que adicionado corretamente, você verá o seguinte:



Nota: Se o HTTPS é usado para conectar ao roteador, todas as mudanças ao certificado no roteador exigirão o dispositivo ser redescobertas em IME. Para refrescar o certificado em IME, fazer duplo clique o roteador sob a lista de dispositivos. Então, a **APROVAÇÃO do** clique para certificar-se de IME conecta ao roteador para obter o certificado novo. Clique **sim** para aceitar o certificado actualizado.

3. Vendo eventos: **Monitoramento de evento do** clique. Certifique-se de você selecionar o roteador sob do “o nome sensor”.**Nota:** À revelia, nos ajustes da vista sob da “o campo da avaliação ameaça”, o valor é ajustado a ">=70". Este valor faz as assinaturas do indicador do resultado somente com avaliação da ameaça acima e igual a 70.Para ver todas as assinaturas da severidade mantenha da “a placa do campo da avaliação ameaça”.



Informações Relacionadas

- Sistema da prevenção de intrusão do Cisco IOS
- Obter começados com IO IPS - Um guia passo a passo
- Gerente do ips Cisco expresso
- Suporte Técnico e Documentação - Cisco Systems