

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

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Recursos](#)

[Configuração](#)

[Configurando o Roteador](#)

[Configurando IME](#)

[Informações Relacionadas](#)

## 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 abrange 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](#)

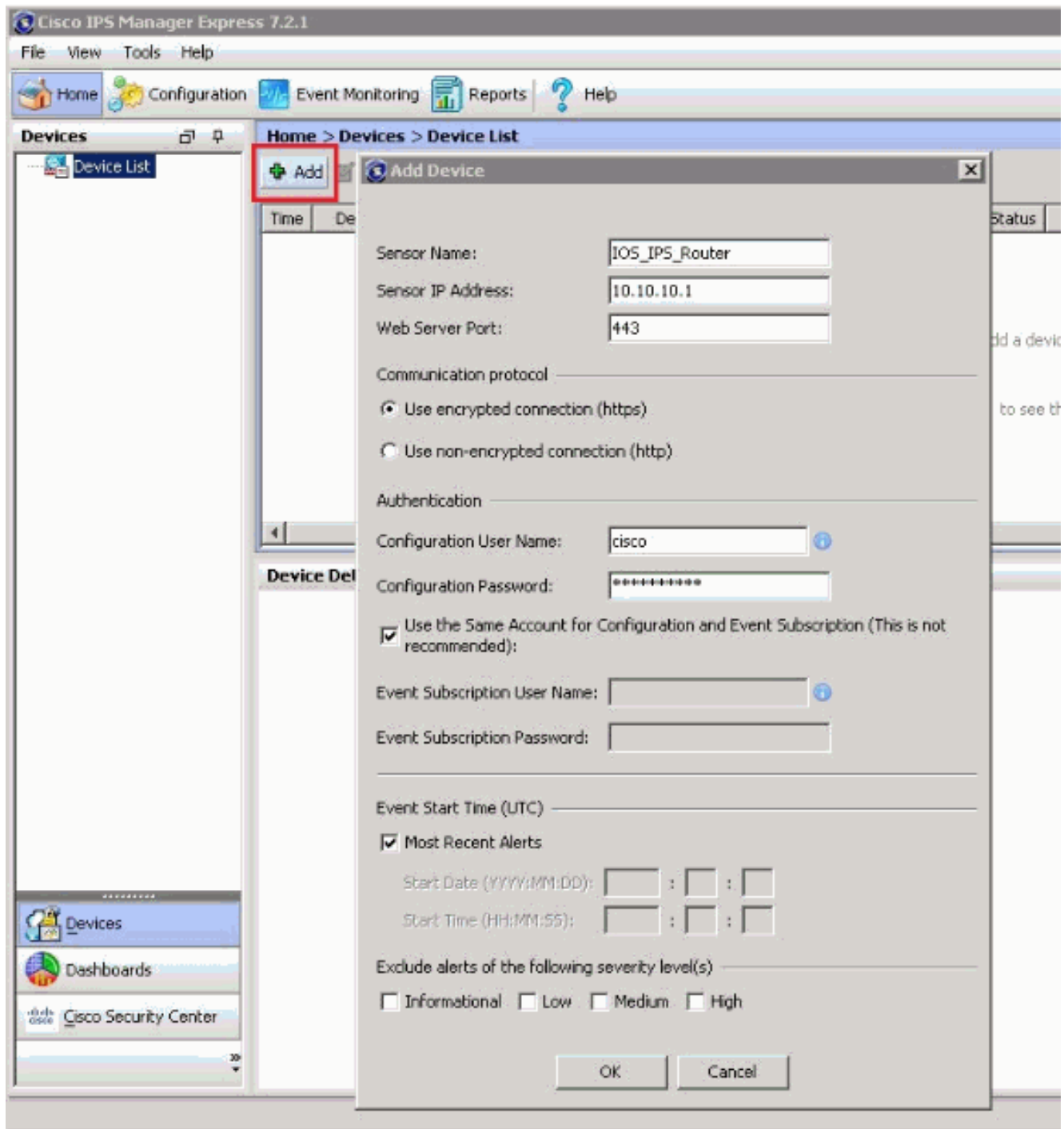
IME usa SDEE para obter eventos de IO IPS. A notificação SDEE é desabilitada à revelia e deve manualmente ser permitida. Para usar SDEE, o servidor de Web do roteador deve ser permitido. À revelia, IME tenta estabelecer uma conexão segura ao roteador que usa HTTPS (TCP 443). Isto exige um certificado 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`

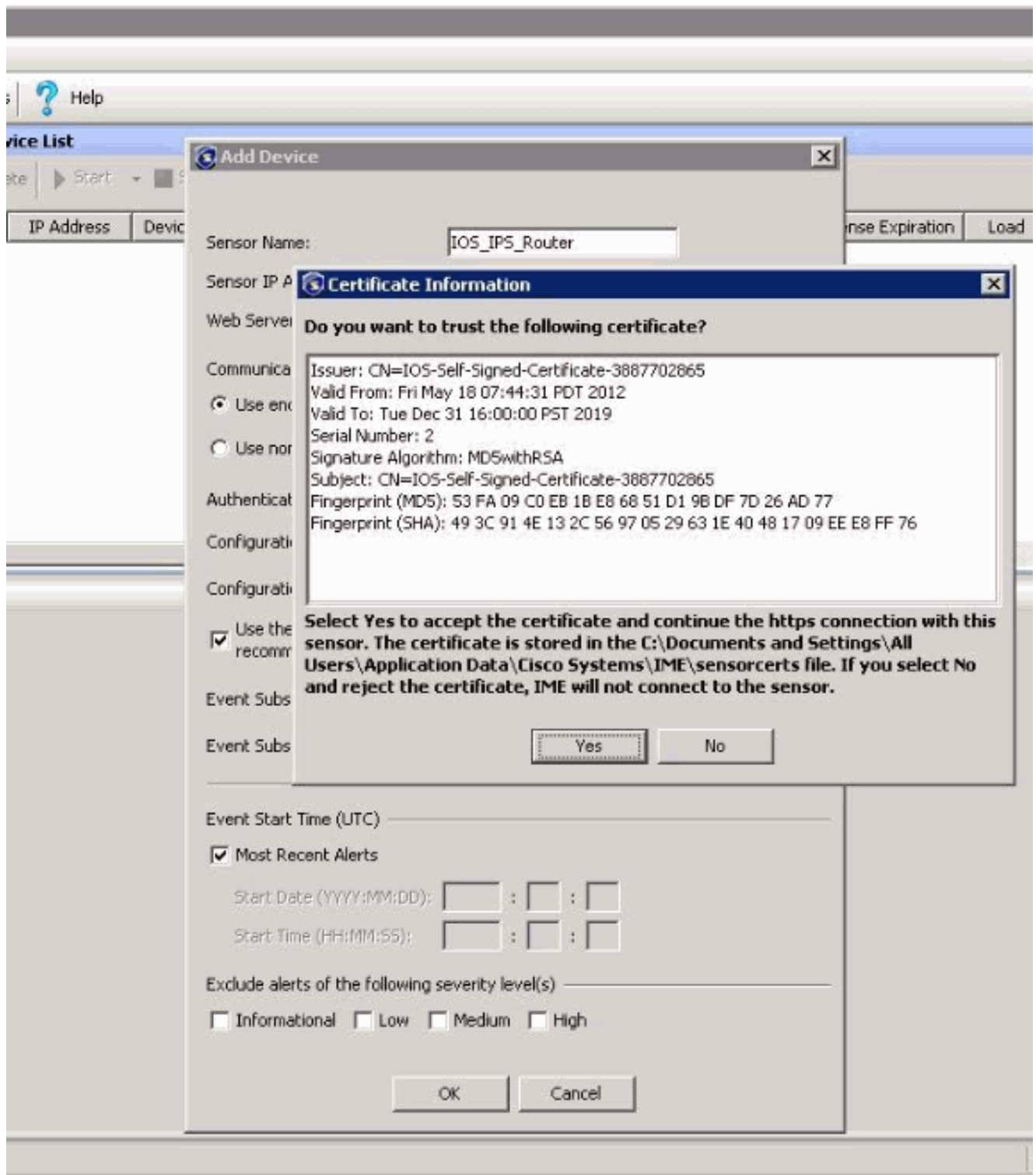
### [Configurando IME](#)

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>

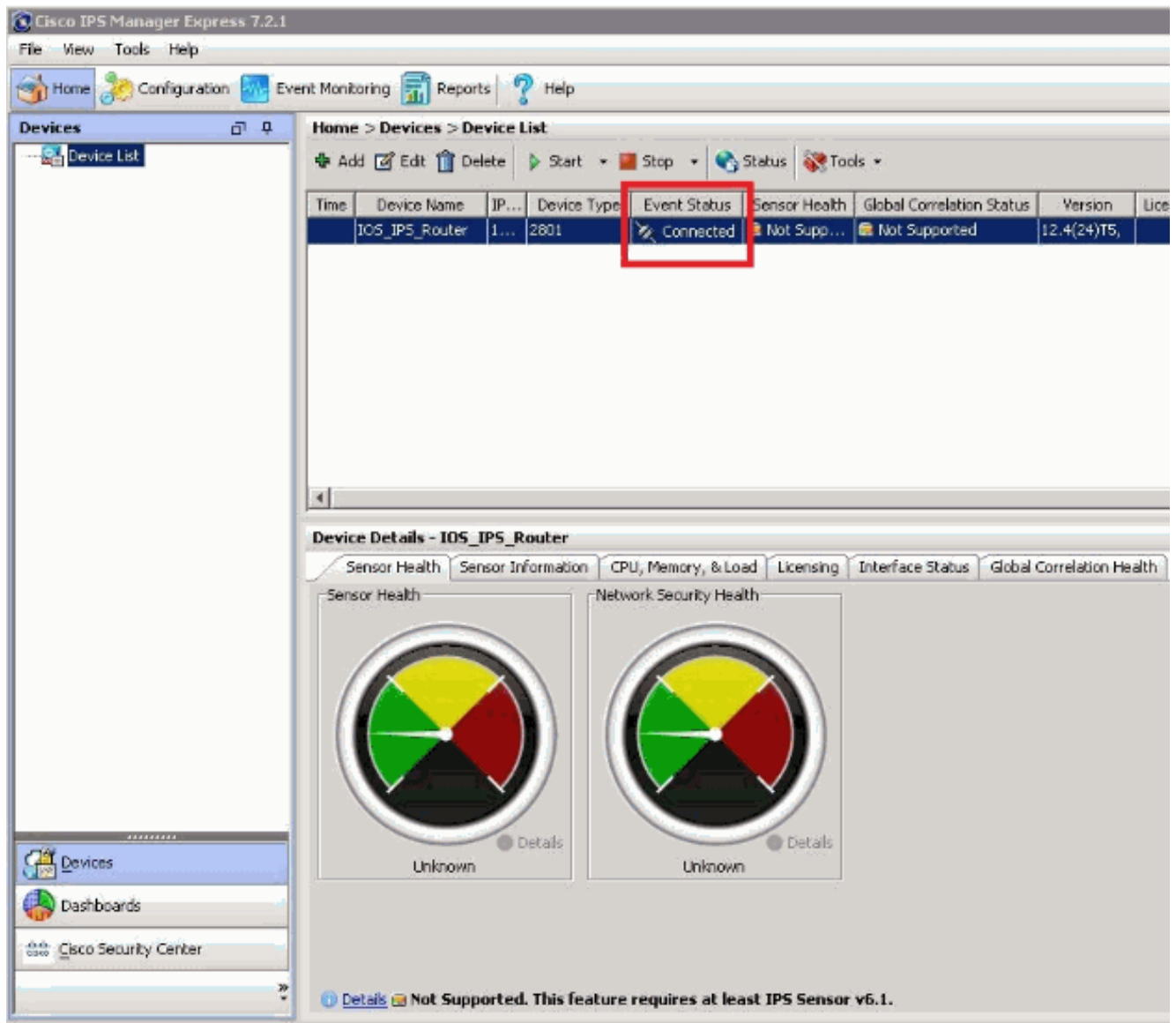


**Nota:** A configuração padrão usa HTTPS e porta 443 para conectar ao roteador. Você pode igualmente escolher conectar usando o HTTP somente, e muda a porta a 80.

2. Se usando o HTTPS, você é apresentado 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.

- Vendo eventos: **Monitoramento de evento do clique.** Certifique-se de você seleccionar 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 " $\geq 70$ ". 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".

Cisco IOS 7.2.1

Event Monitoring | Reports | Help

Event Monitoring > Event Monitoring > Event Views > Basic View

View Settings

Filter: Basic View Filter

Packet Parameters: Attacker IP, Victim IP, Signature Name/ID, Victim Port

Rating and Action Parameters: Severity (High, Medium, Low, Info), Risk Rating, Reputation, Threat Rating, Action(s) Taken

Other Parameters: Sensor Name(s): IOS\_IPS\_Router, Virtual Sensor, Status: All, Vict. Locality

Time: Real Time | Last: 10 hour | Start Time: Fri, 18 May 2012 00:00:00 | End Time: Fri, 18 May 2012 00:00:00 | Apply

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Actions	Victim Port	Threat	Risk Rel.	Reputa...
Info...	05/18/...	08:54:22	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:25	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:34	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:40	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:47	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:55	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:55:06	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:55:15	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:14:43	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:14:46	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:56	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:57	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:58	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:59	IOS_IPS...	ICMP Echo Request								
low	05/18/...	08:15:55	IOS_IPS...	IGMP Invalid Packet DoS								
low	05/18/...	08:17:52	IOS_IPS...	IGMP Invalid Packet DoS								
low	05/18/...	08:22:50	IOS_IPS...	IGMP Invalid Packet DoS								

Event Details (Event ID - 13373565153745)

Print | Copy

Event Time: 05/18/2012 08:55:15  
 Sensor Local Time: 05/18/2012 15:55:15  
 Signature ID: 1107  
 Signature Sub-ID: 0  
 Signature Name: RFC 1918 Addresses Seen  
 Signature Version: 5392  
 Signature Details: My Sig Info  
 Interface Group:  
 VLAN ID:  
 Interface: Fa0/0  
 Attacker IP: 192.168.50.1  
 Protocol: udp  
 Attacker Port: 63240  
 Attacker Locality:  
 Target IP: 255.255.255.255  
 Target Port: 60

You can copy selected or all rows into clipboard or print the entire contents.

## 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](#)