Cisco IOS入侵防御系统生成的箴言报事件使用IPS管理器Express

目录

简介

本文解释如何使用Cisco IOS入侵防御系统生成的监视器事件(IOS-IPS)使用IPS管理器Express (IME)。

Cisco IOS IPS是有效减轻各种各样的网络攻击的一个基于软件的深度信息包检验功能。

思科IME是一简单，基于GUI的IPS管理软件。

先决条件

要求

本文读者应该有这些主题知识。

- Cisco IOS入侵防御系统
- IPS管理器Express

使用的组件

使用IPS管理器Express，本文档中的信息根据Cisco IOS入侵防御系统。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能

需求：

为了使支持的IME IOS IPS，路由器需要运行Cisco IOS软件版本12.3(14)T7和12.4(15)T2或者更新。IME可以支持10个设备。

注意： IME只支持IOS IPS的事件监控。不支持配置。

配置

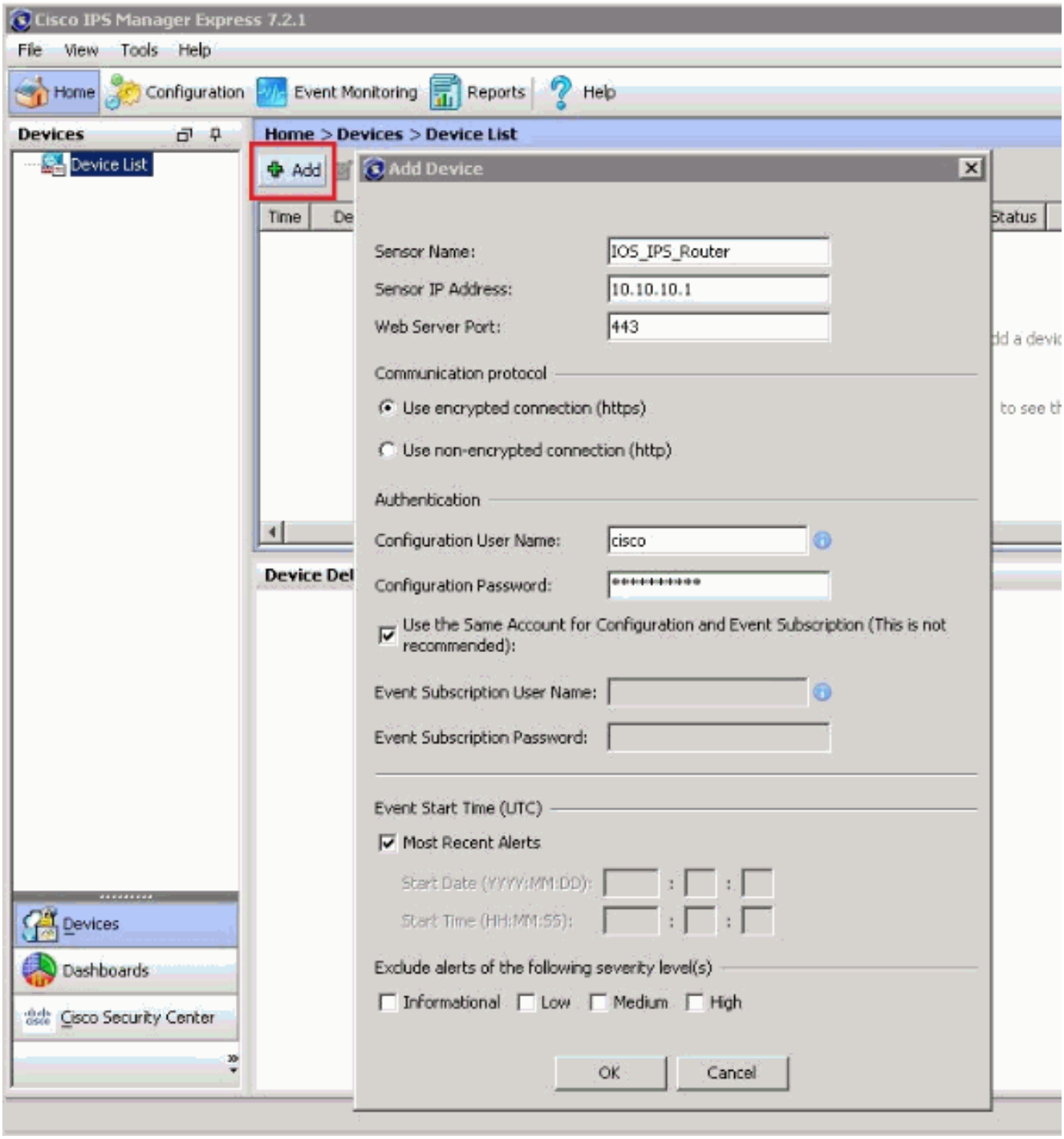
IME使用SDEE从IOS IPS获得事件。默认情况下SDEE通知禁用并且必须手工启用。要使用SDEE，必须启用路由器的Web服务器。默认情况下，使用HTTPS (TCP 443)， IME设法建立对路由器的一个安全连接。这要求在路由器将配置的数字证书。随意地，使用HTTP (TCP 80)， IME可以配置支持不安全的连接。

配置路由器

1. Enable (event) SDEE通知：`Router(config)# ip ips notify sdee`
2. Enable (event) HTTPS ：`Router(config)#ip http secure-server`
3. Enable (event) HTTP (可选) ：`Router(config)# ip http server`

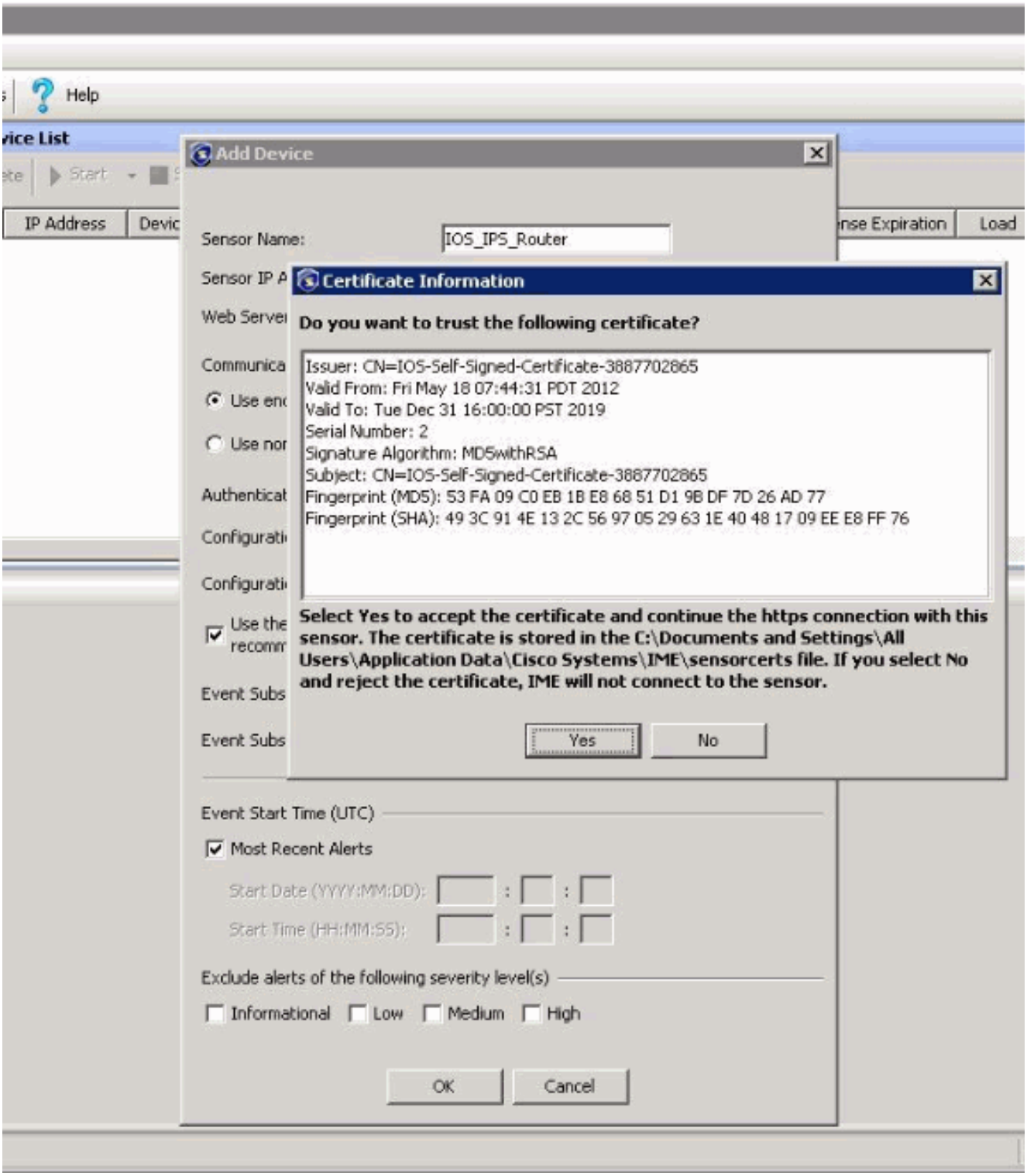
配置IME

1. 下载和安装IME。运行IME。然后，请单击**添加**。下载IME：http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

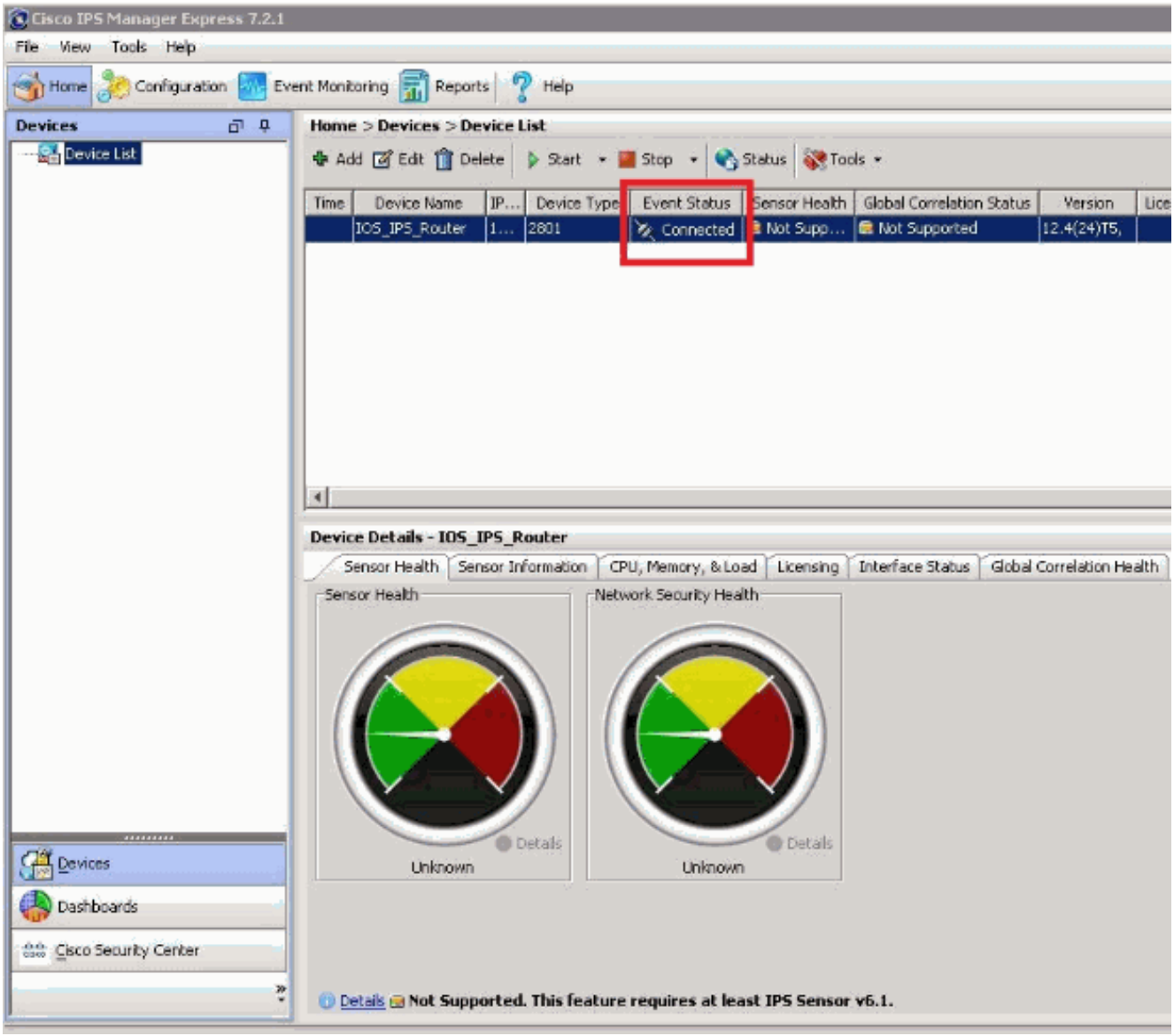


注意： 默认设置使用HTTPS和端口443连接到路由器。您能也选择连接使用仅HTTP，并且更换端口到80。

2. 如果曾经HTTPS，您提交以屏幕接受从路由器的自签名证书。单击 **Yes**。

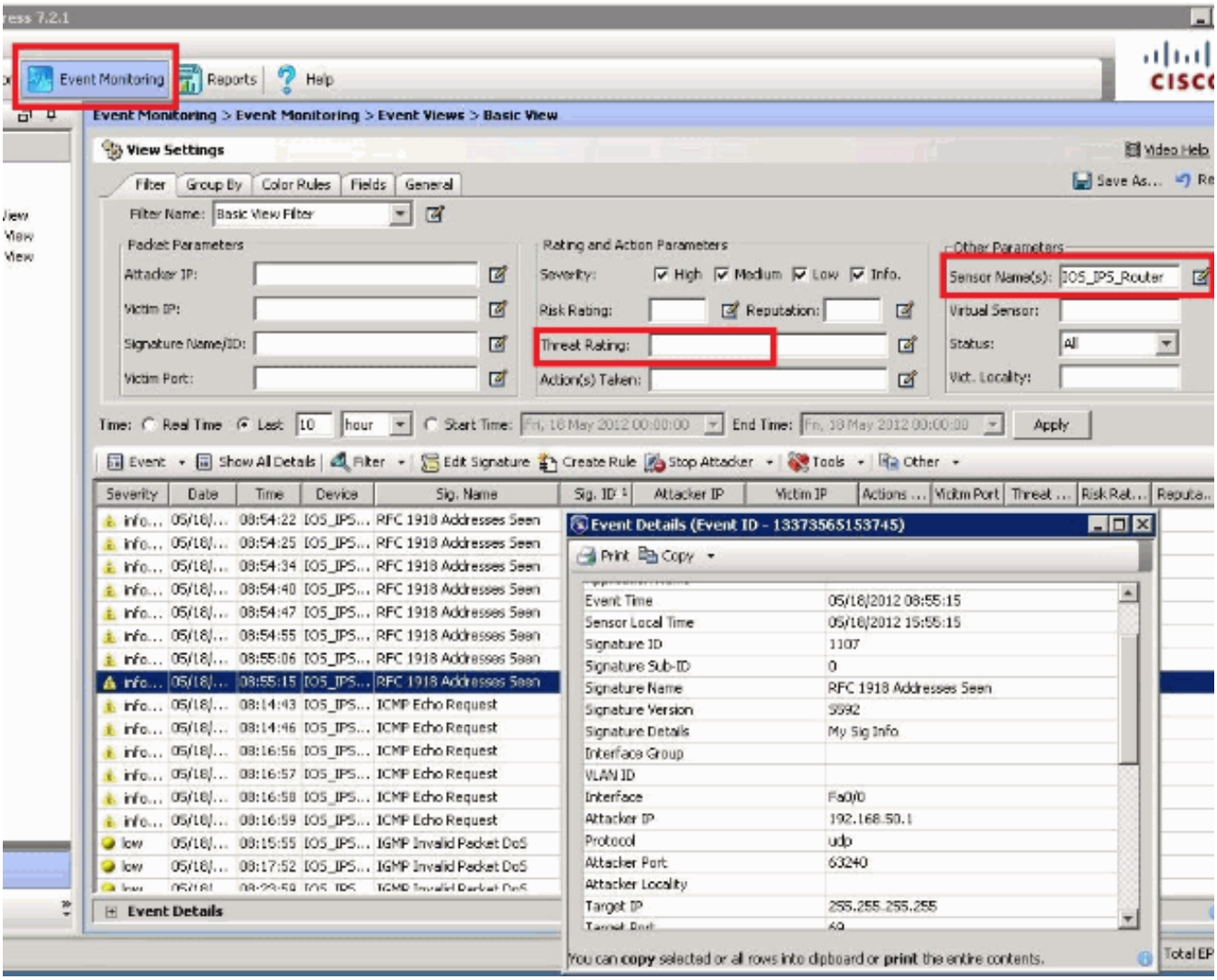


一旦正确地添加，您将看到以下
：



注意： 如果HTTPS用于连接到路由器，对证书的所有更改在路由器将要求将被再发现的设备到IME。要刷新在IME的证书，请双击路由器在设备清单下。然后，请点击OK键确保IME连接到路由器获得新证书。点击**是**接受更新证书。

3. 查看事件：点击**事件监控**。确保您选择路由器在“传感器下命名”。**注意：** 默认情况下，在“威胁分级的”字段下的视图设置，值设置到">=70"。此值做结果显示仅签名与威胁上面规定值和等于到70。要查看所有严重性签名请保持“威胁分级的”字段空白。



相关信息

- Cisco IOS入侵防御系统
- 开始与IOS IPS -一分步指南
- Cisco IPS Manager Express
- 技术支持和文档 - Cisco Systems