Eventos del monitor generados por el sistema de prevención de intrusiones del Cisco IOS usando el administrador IPS expreso

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Funciones](#)
[Configuración](#)
[‘Configuración del router’](#)
[Configurar IME](#)
[Información Relacionada](#)

Introducción

Este documento explica cómo utilizar los eventos del monitor generados por el sistema de prevención de intrusiones del Cisco IOS (IOS-IPS) usando el administrador IPS expreso (IME).

El Cisco IOS IPS es una característica basada en software del examen del profundo-paquete que atenúa con eficacia una amplia gama de ataques a la red.

Cisco IME es un software simple, GUI basado de la Administración de IPS.

prerrequisitos

Requisitos

Los Quien lea este documento deben tener conocimiento de estos temas.

- Sistema de prevención de intrusiones del Cisco IOS
- Administrador IPS expreso

Componentes Utilizados

La información en este documento se basa en el sistema de prevención de intrusiones del Cisco IOS usando el administrador IPS expreso.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Funciones

Requisito:

Para que IME soporte IOS IPS, el router necesita ejecutar los Cisco IOS Software Releases 12.3(14)T7 y 12.4(15)T2 o más nuevo. IME puede soportar hasta 10 dispositivos.

Nota: IME apoya solamente el monitoreo de evento para IOS IPS. La configuración no se soporta.

Configuración

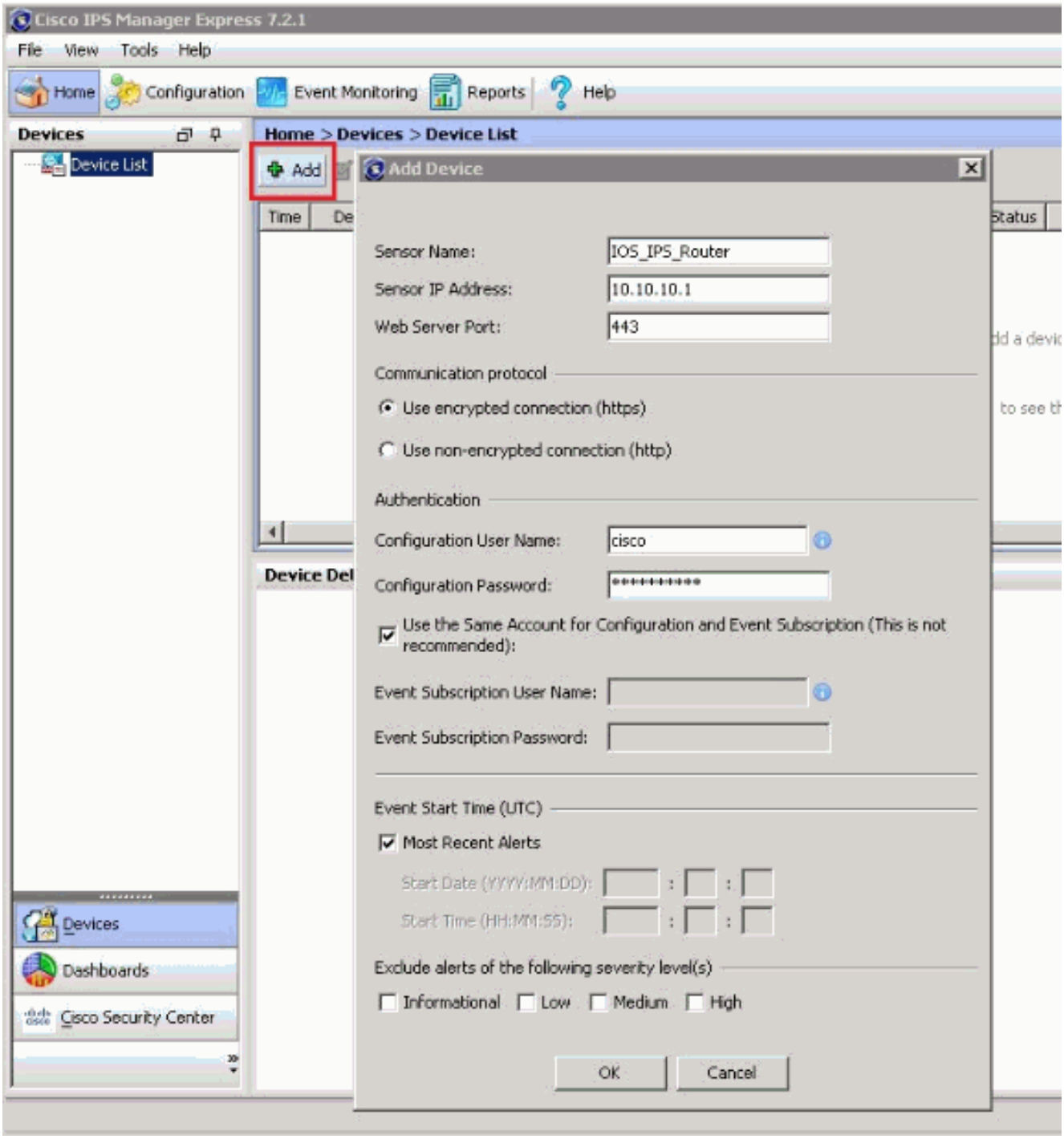
IME utiliza SDEE para conseguir los eventos de IOS IPS. La notificación SDEE se inhabilita por abandono y debe ser habilitada manualmente. Para utilizar SDEE, el servidor Web del router debe ser habilitado. Por abandono, IME intenta establecer una conexión segura al router que usa HTTPS (TCP 443). Esto requiere un certificado digital ser configurada en el router. Opcionalmente, IME se puede configurar para soportar una conexión unsecure usando HTTP (TCP 80).

'Configuración del router'

1. Notificación del permiso SDEE:`Router(config)# ip ips notify sdee`
2. Permiso HTTPS:`Router(config)#ip http secure-server`
3. Permiso HTTP (opcional):`Router(config)# ip http server`

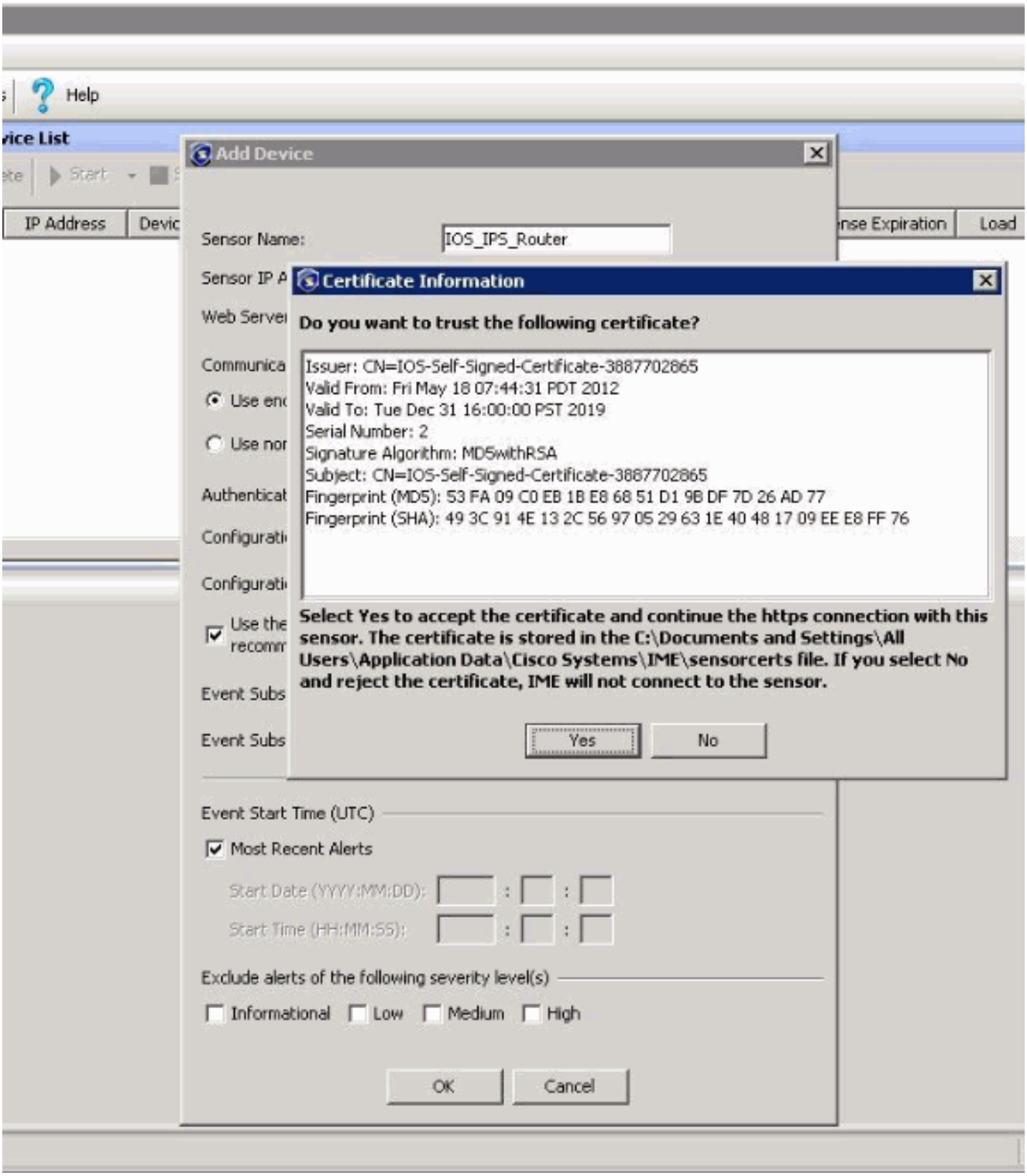
Configurar IME

1. Descargue y instale IME. Ejecute IME. Entonces, haga click en AddDescarga IME:http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

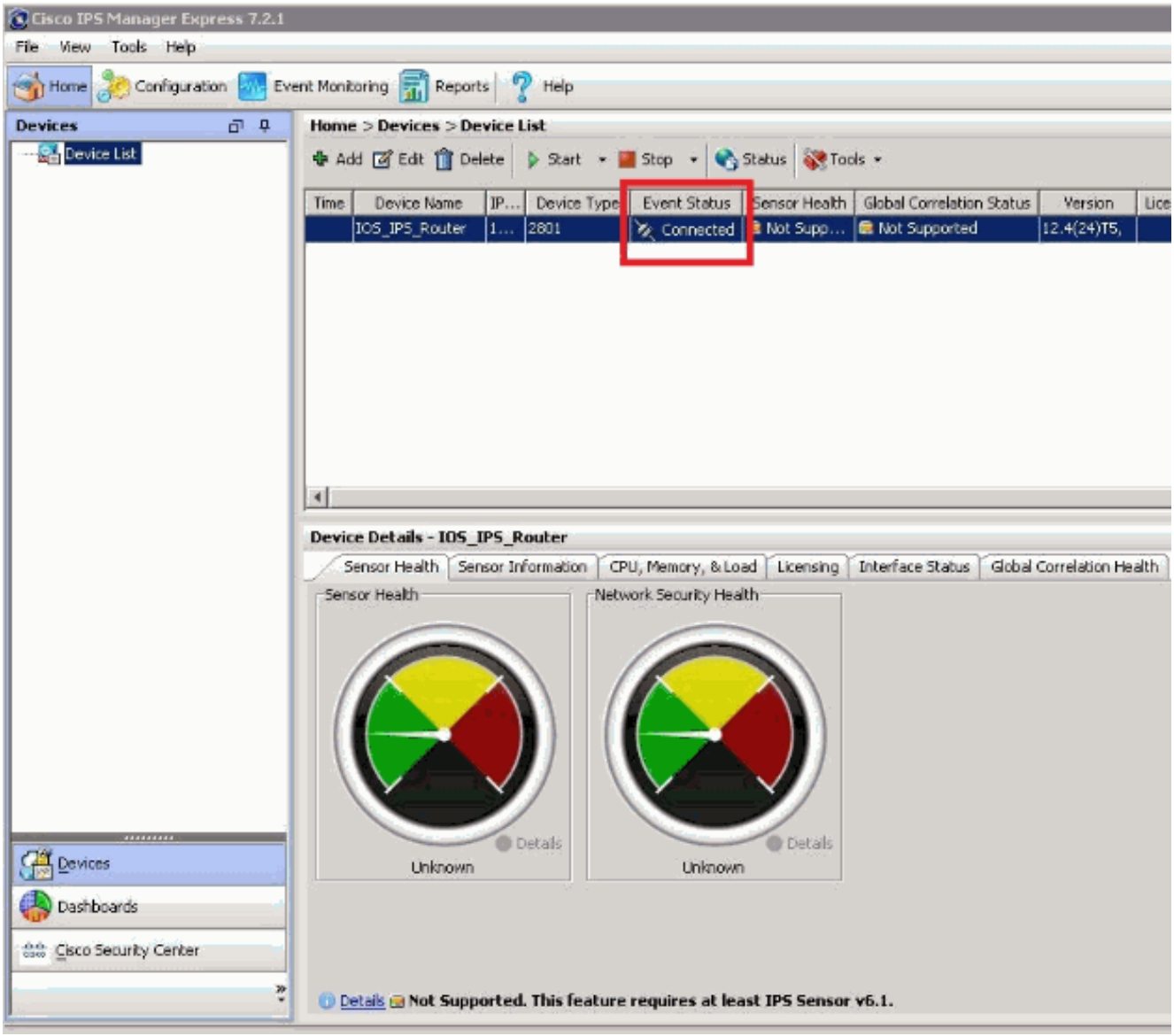


Nota: La configuración predeterminada utiliza HTTPS y el puerto 443 para conectar con el router. Usted puede también elegir conectar usando el HTTP solamente, y cambia el puerto a 80.

2. Si usa el HTTPS, le presentan con una pantalla para validar el certificado autofirmado del router. Haga clic en
   Sí

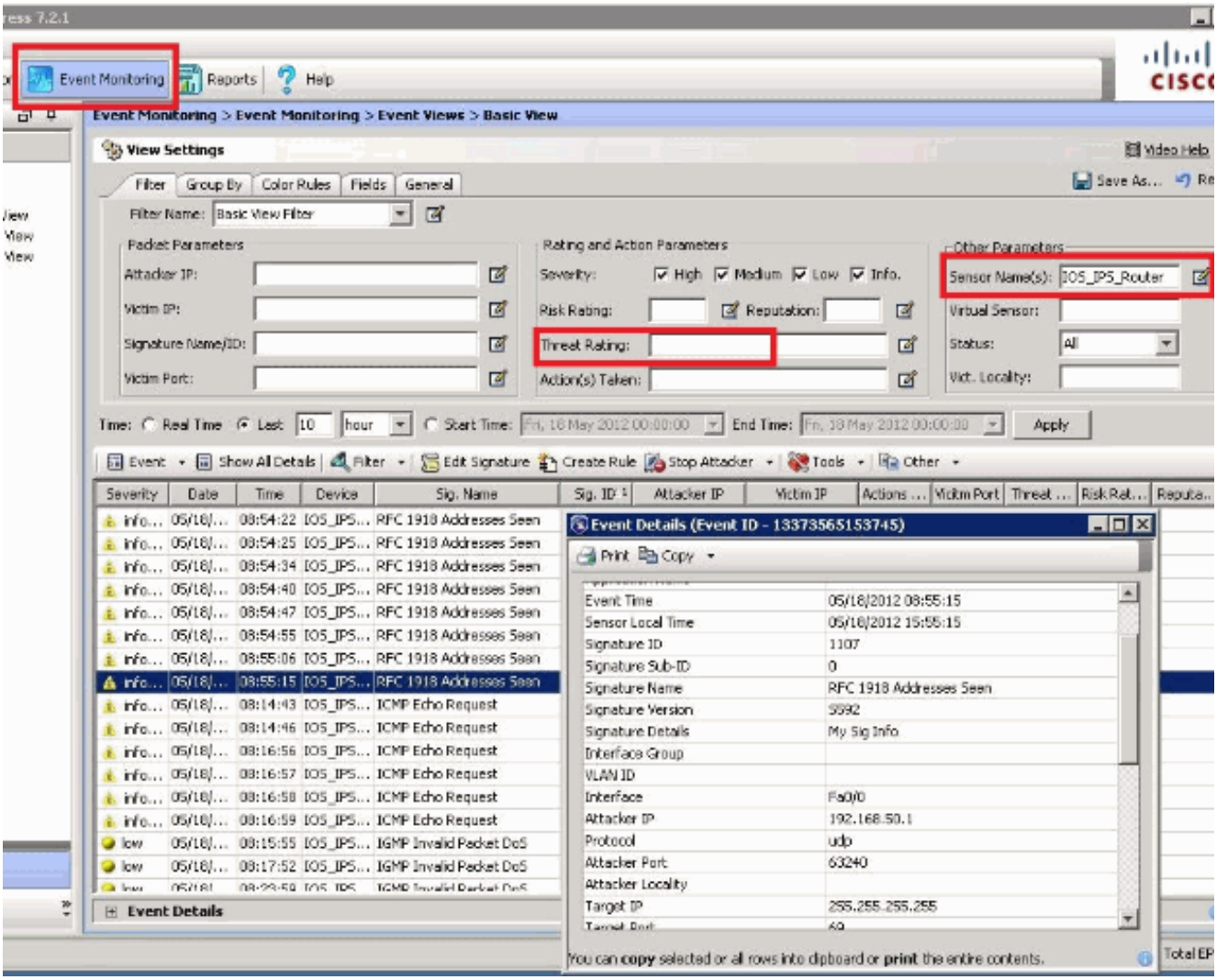


Una vez que está agregado correctamente, usted verá el siguiente:



Nota: Si el HTTPS se utiliza para conectar con el router, cualquier cambio al certificado en el router requerirá el dispositivo ser redescubierto en IME. Para restaurar el certificado en IME, tecleo doble el router conforme a la lista de dispositivos. Entonces, la **AUTORIZACIÓN del** tecleo para aseegurarse IME conecta con el router para conseguir el nuevo certificado. Haga clic **sí** para validar el certificado actualizado.

3. Ver los eventos: **Supervisión del** evento click. Aseegurese le seleccionar al router bajo “nombre del sensor”.**Nota:** Por abandono, en las configuraciones de la visión bajo “campo del grado de la amenaza”, el valor se fija hasta el ">=70". Este valor hace las firmas de la visualización del resultado solamente con el grado de la amenaza arriba y el igual a 70.Para ver todas las firmas de la gravedad guarde “el espacio en blanco del campo del grado de la amenaza”.



Información Relacionada

- Sistema de prevención de intrusiones del Cisco IOS
- Introducción con IOS IPS - Un guía paso a paso
- Administrador del IPS de Cisco expreso
- Soporte Técnico y Documentación - Cisco Systems