Следите за развитием Событий, Генерируемых использованием Системы предотвращения вторжений Cisco IOS IPS Manager Express

Содержание

Введение

Этот документ объясняет, как использовать, следят за развитием событий, генерируемых Системой предотвращения вторжений Cisco IOS (IPS IOS) с помощью IPS Manager Express (IME).

IPS Cisco IOS является программной функцией глубокой проверки пакетов, которая эффективно смягчает широкий диапазон сетевых атак.

Cisco IME является простым, на основе GUI программное обеспечение управления IPS.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам.

- Система предотвращения вторжений Cisco IOS
- IPS Manager Express

Используемые компоненты

Сведения в этом документе основываются на Системе предотвращения вторжений Cisco IOS с помощью IPS Manager Express.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Функции

Требование:

Для IME для поддержки IPS IOS маршрутизатор должен выполнить Cisco IOS Software Release 12.3 (14) T7 и 12.4 (15) T2 или более новый. IME может поддержать до 10 устройств.

Примечание: IME только поддерживает мониторинг событий для IPS IOS. Конфигурация не поддерживается.

!--- конфигурацию

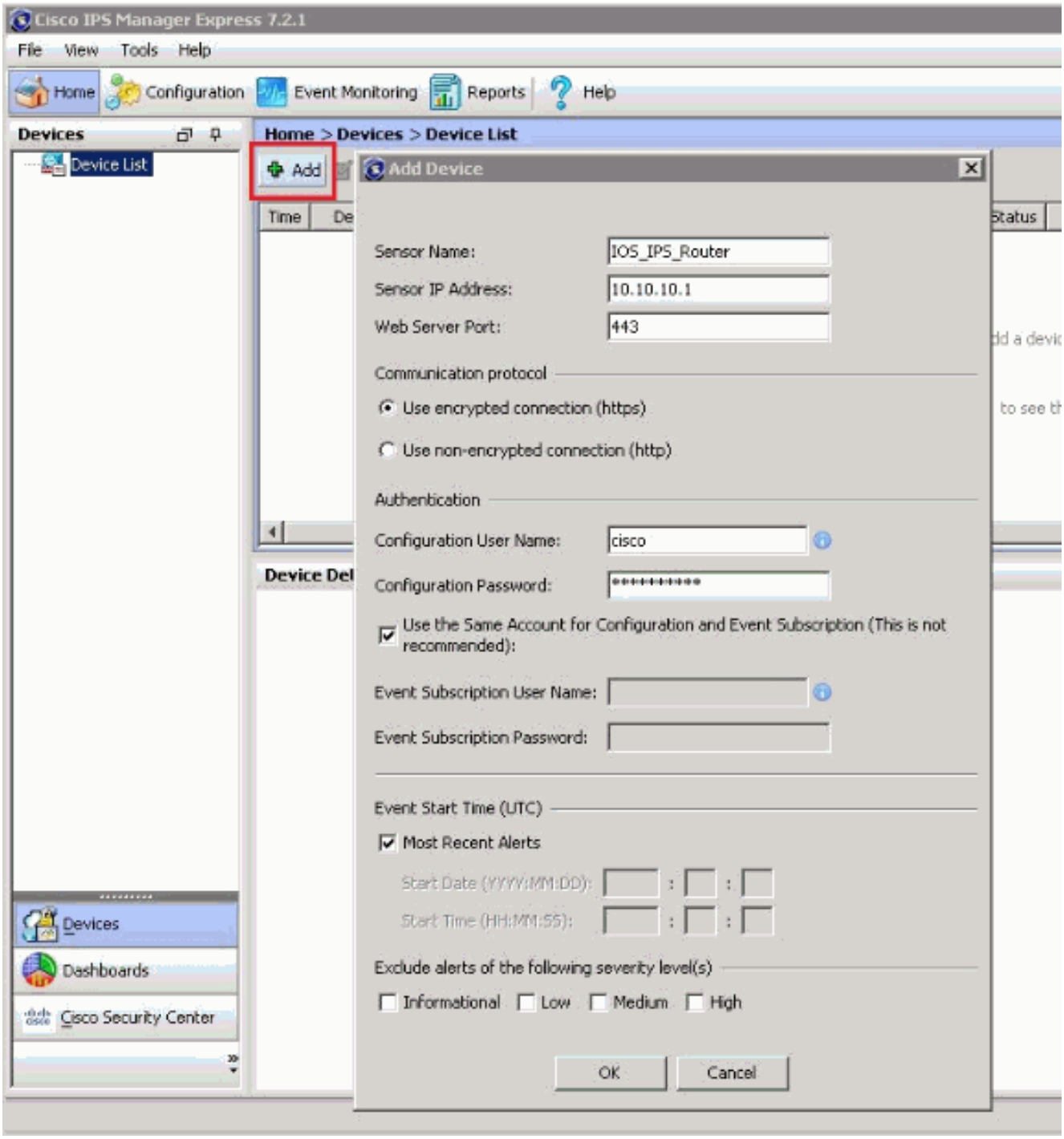
IME использует SDEE для получения событий от IPS IOS. Уведомление SDEE отключено по умолчанию и должно быть вручную включено. Для использования SDEE Web-сервер маршрутизатора должен быть включен. По умолчанию IME пытается установить безопасное соединение с маршрутизатором с помощью HTTPS (TCP 443). Это требует, чтобы цифровой сертификат был настроен на маршрутизаторе. Дополнительно, IME может быть настроен для поддержки небезопасного соединения с помощью HTTP (TCP 80).

Выбор конфигурации маршрутизатора

1. Включите уведомление SDEE:`Router(config)# ip ips notify sdee`
2. Включите HTTPS:`Router(config)#ip http secure-server`
3. Включите HTTP (Необязательно):`Router(config)# ip http server`

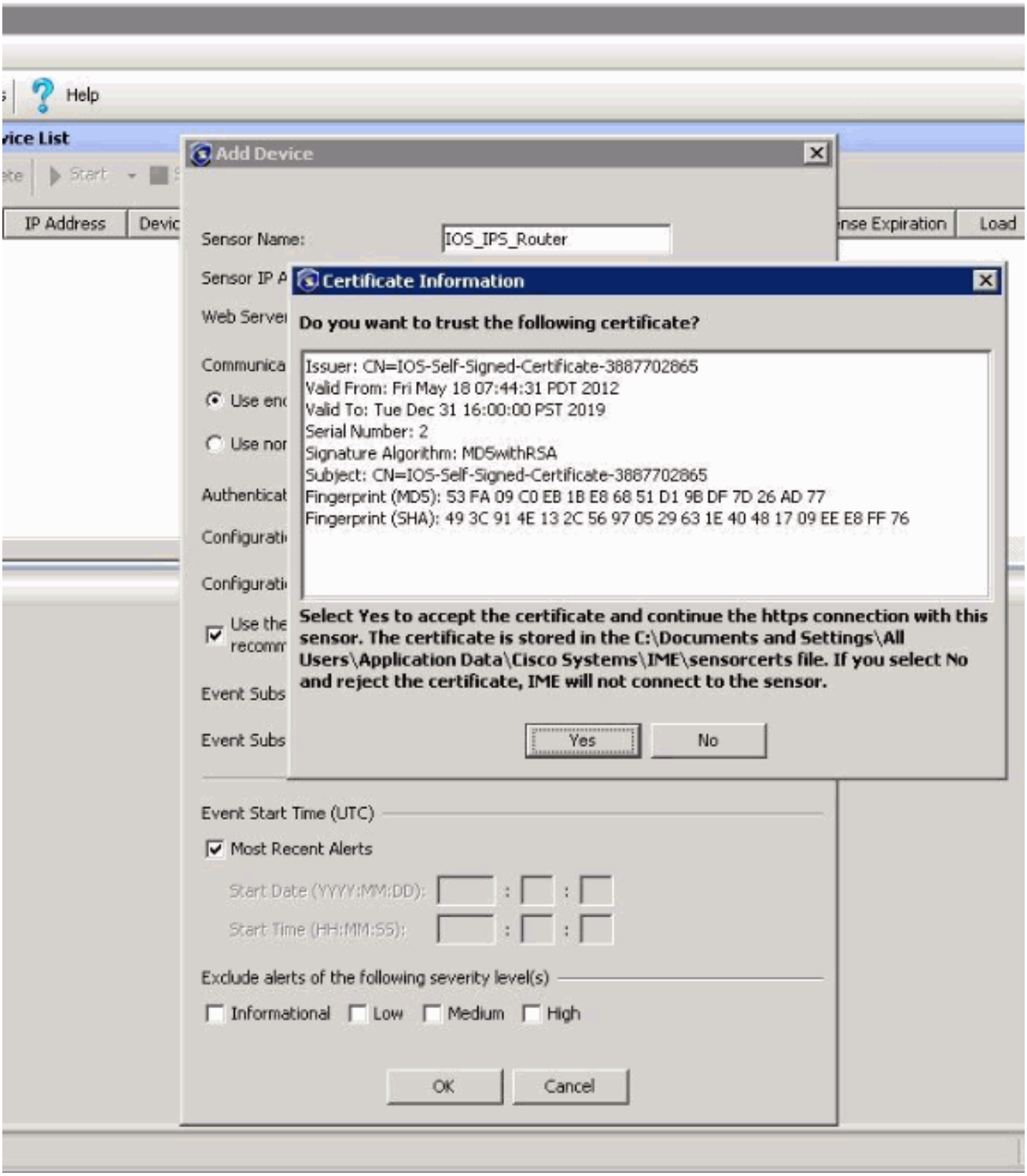
Настройка IME

1. Загрузка и установка IME. Выполните IME. **Потом нажмите кнопку Add (добавить).**Загрузка IME:http://www. cisco . com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

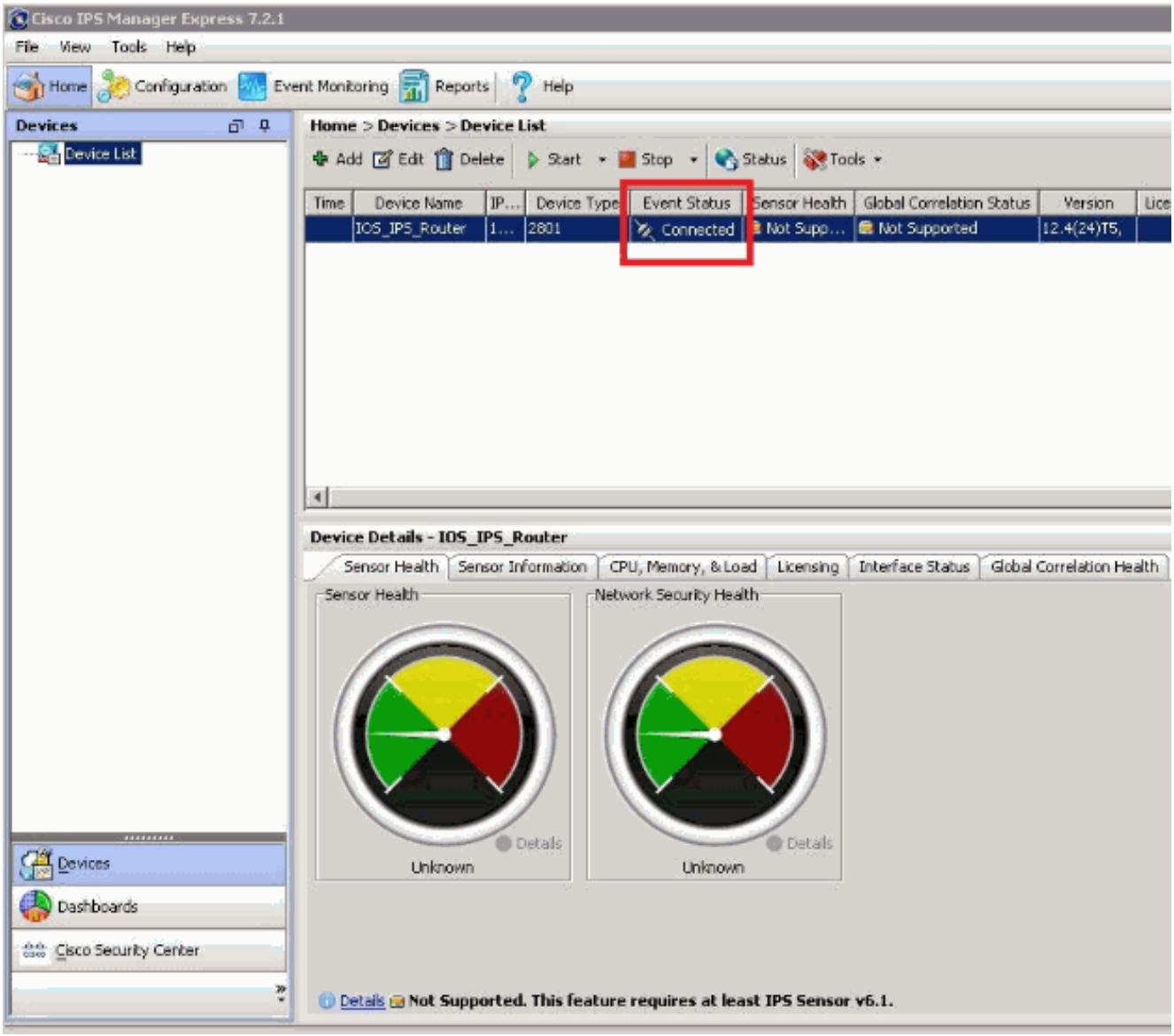


Примечание: Настройка по умолчанию использует HTTPS и порт 443 для соединения с маршрутизатором. Можно также принять решение подключить HTTP использования только и изменить порт на 80.

2. При использовании HTTPS вам предоставляют экран для принятия подписанного сертификата от маршрутизатора. **Нажмите кнопку YES.**

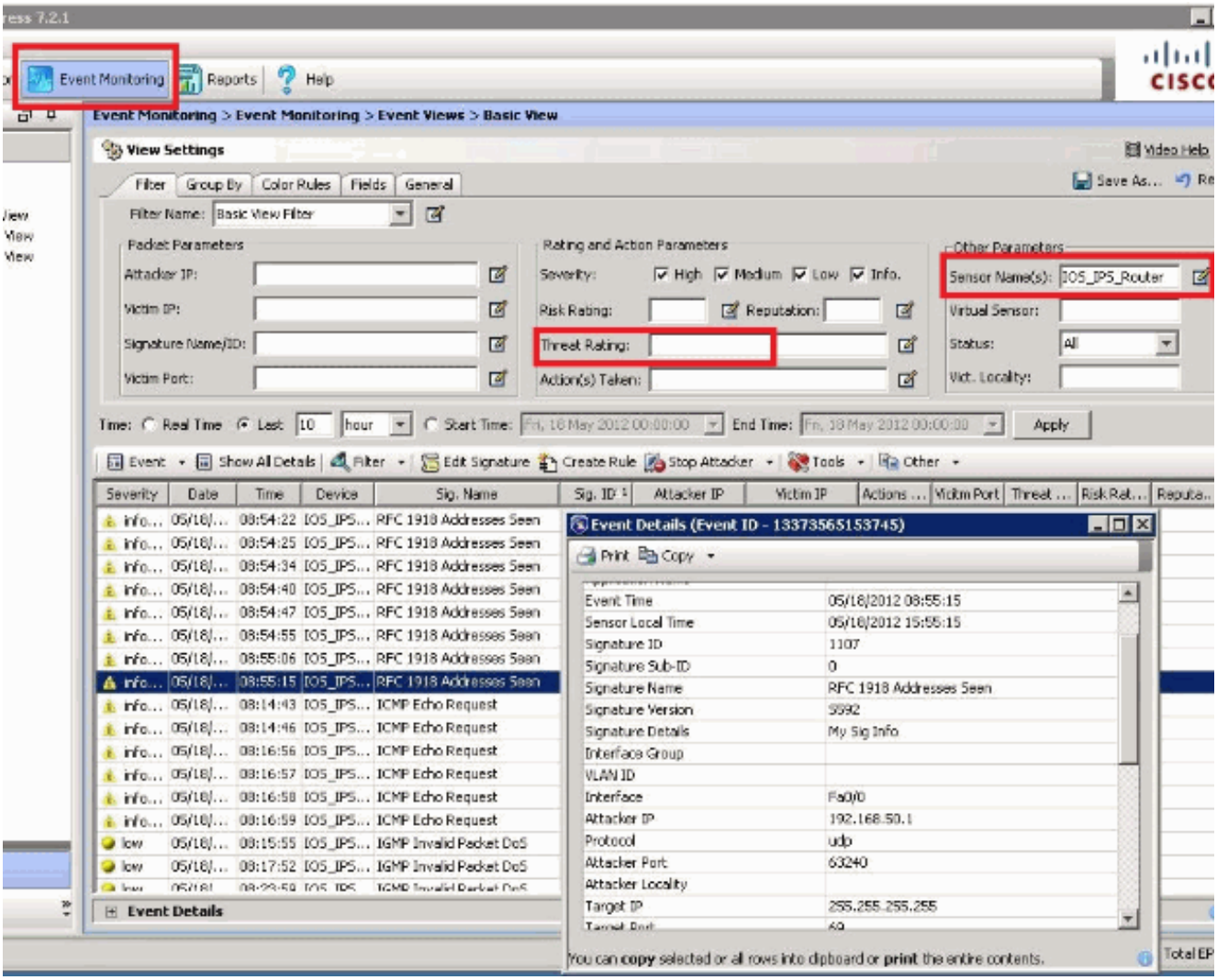


После того, как правильно добавленный, вы будете видеть придерживающееся:



Примечание: Если HTTPS будет использоваться для соединения с маршрутизатором, то любые изменения к сертификату на маршрутизаторе потребуют, чтобы устройство было открыто вновь в IME. Для обновления сертификата в IME, дважды щелкают маршрутизатор под Списком устройств. Затем нажмите **OK** для проверки подключений IME к маршрутизатору для получения нового сертификата. Нажмите **Yes** для принятия обновленного сертификата.

3. Просмотр Событий: Нажмите **Event Monitoring**. Удостоверьтесь, что вы выбираете маршрутизатор под "Названием Датчика".**Примечание:** По умолчанию, в обзорных параметрах настройки под полем "Threat Rating", значение установлено в"> =70". Это значение заставляет результат отобразить подписи только с оценкой угрозы выше и равный 70.Для просмотра всех подписей степеней серьезности ошибки поддерживают пробел поля "Threat
Rating".



Дополнительные сведения

- Система предотвращения вторжений Cisco IOS
- Начало работы с IPS IOS - пошаговые инструкции
- Cisco IPS Manager Express
- Cisco Systems – техническая поддержка и документация