IPS Manager Express を使用した Cisco IOS Intrusion Prevention System で生成されたイベントのモニタ

目次

概要

このドキュメントでは、IPS Manager Express（IME）を使用して Cisco IOS 侵入防御システム（IOS-IPS）によって生成されたモニタ イベントを使用する方法について説明します。

Cisco IOS IPS は効果的にネットワーク攻撃の広範囲を軽減するソフトウェアベースの強度 の パケット インスペクション 機能です。

Cisco IME は簡単な、GUI ベース IPS 管理 ソフトウェアです。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- Cisco IOS 侵入防御システム（IPS）
- IPS Manager Express

使用するコンポーネント

この文書に記載されている情報は IPS Manager Express を使用して IOS 侵入防御システム（IPS） on Cisco 基づいています。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

機能

要件：

IOS IPS をサポートする IME に関してはルータは Cisco IOS ソフトウェア リリース 12.3(14)T7 および 12.4(15)T2 またはより新しいを実行する必要があります。 IME は 10 までのデバイスをサポートできます。

注: IME は IOS IPS のためのイベントモニタリングだけをサポートします。 設定はサポートされません。

設定

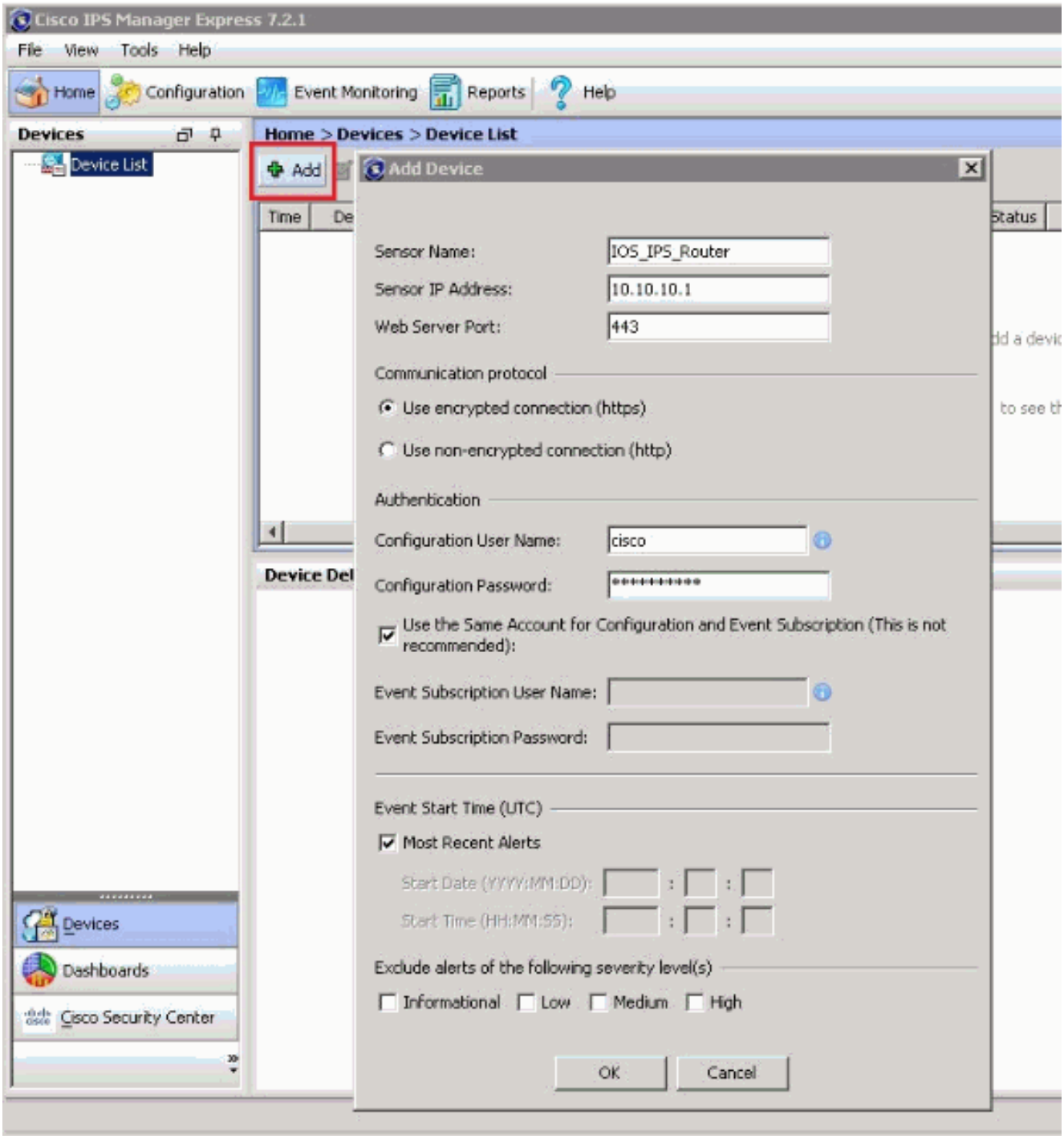
IME は IOS IPS からイベントを得るのに SDEE を使用します。 SDEE 通知はデフォルトでディセーブルにされ、手動で 有効に なる必要があります。 SDEE を使用するために、ルータの Webサーバは有効に する必要があります。 デフォルトで、IME は HTTPS （ 443 ） TCP を使用してルータに信頼できる接続を確立することを試みます。 これはデジタル認証がルータで設定されるように要求します。 任意で、IME は HTTP （ 80 ） TCP を使用して安全でない接続をサポートするために設定することができます。

ルータの設定

1. イネーブル SDEE 通知:`Router(config)# ip ips notify sdee`
2. イネーブル HTTPS:`Router(config)#ip http secure-server`
3. イネーブル HTTP （ オプションの ）:`Router(config)# ip http server`

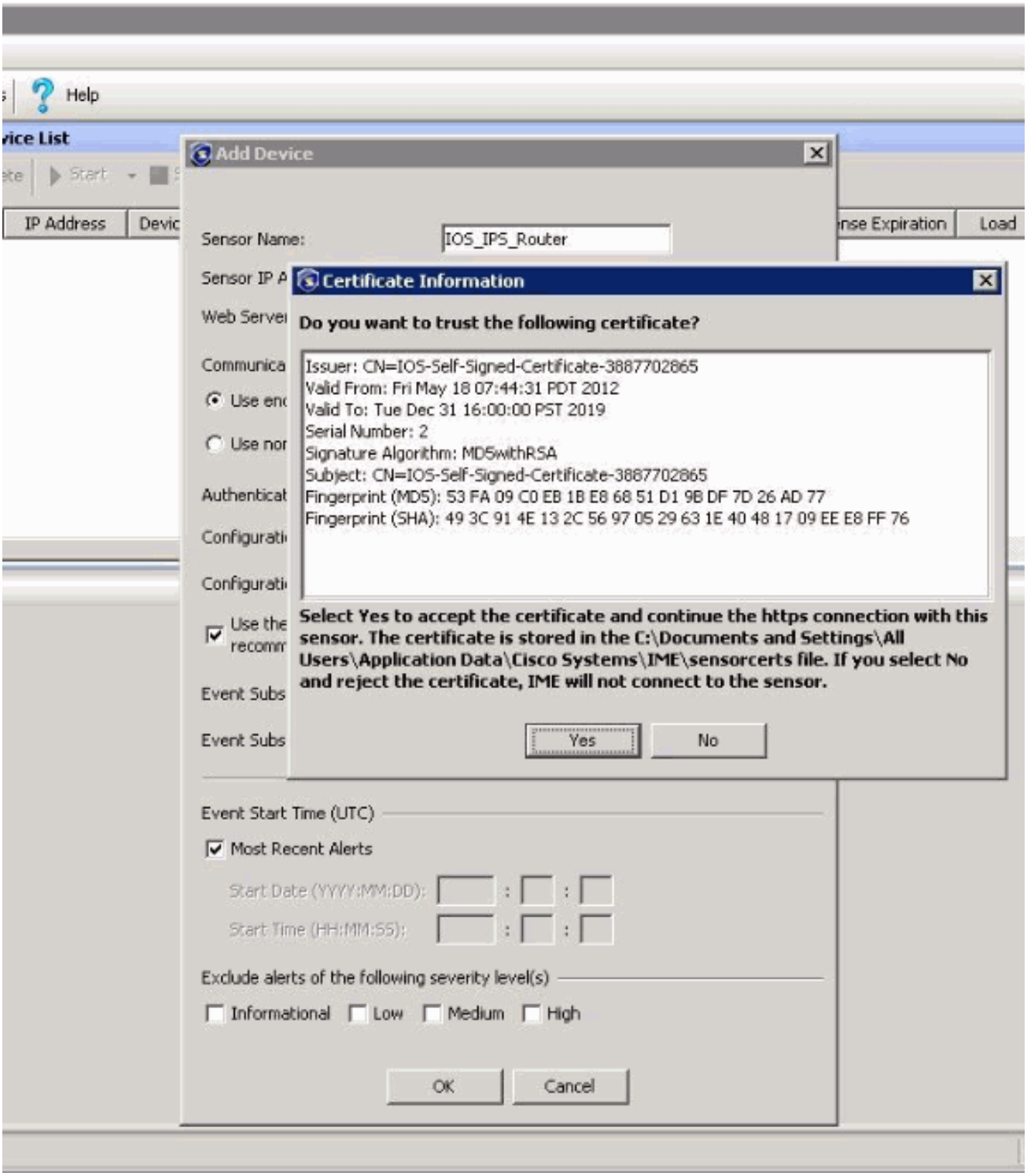
IME の設定

1. ダウンロードおよびインストール IME。 IME を実行して下さい。 次に、[Add] をクリックします。ダウンロード IME:http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

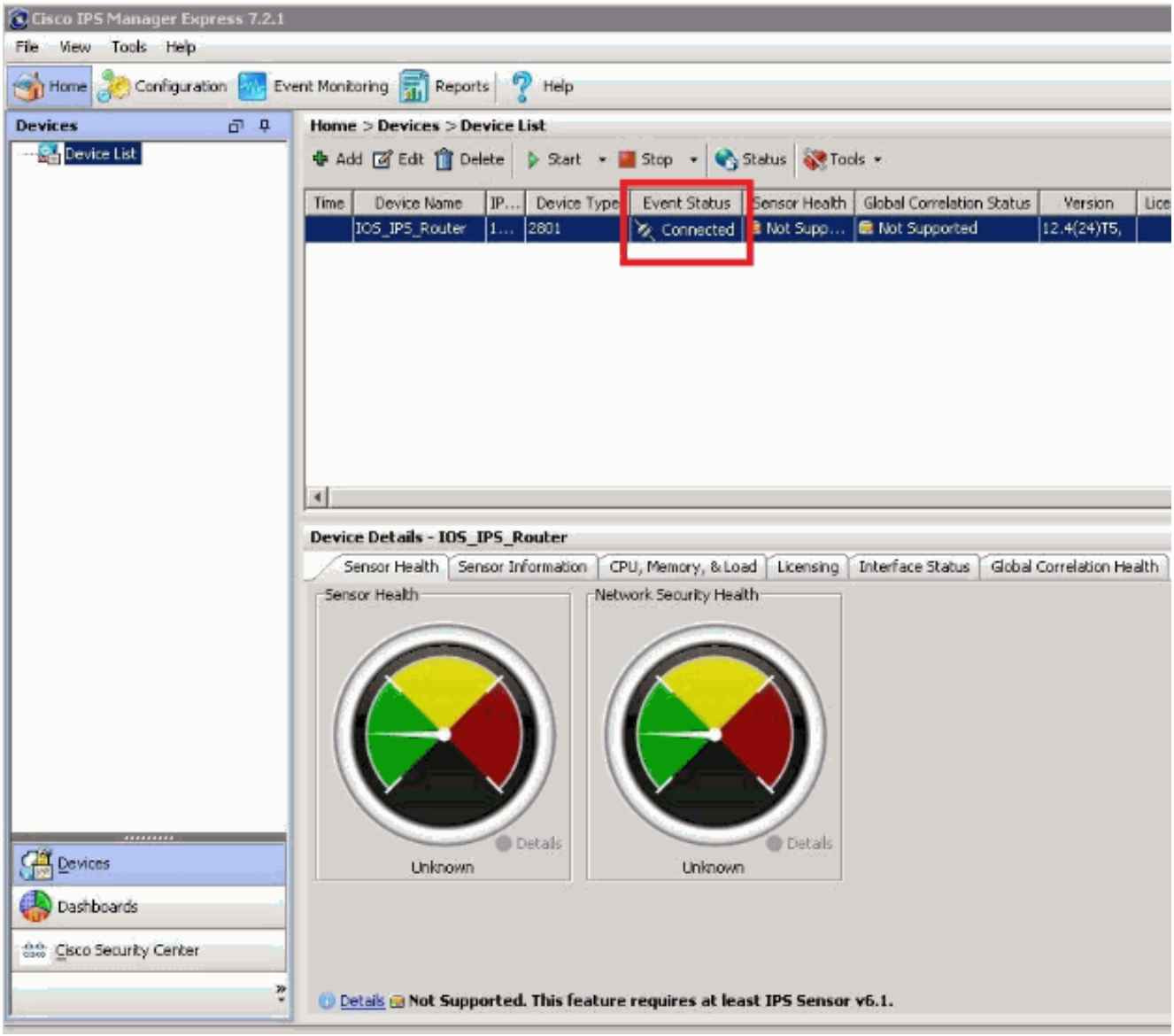


注: デフォルト設定はルータに接続するのに HTTPS およびポート 443 を使用します。 また HTTP だけを使用して接続することを選択でき 80 にポートを変更します。

2. HTTPS を使用している場合ルータからの自己署名証明書を受け入れるために、画面が表示されます。 [Yes] をクリックします。

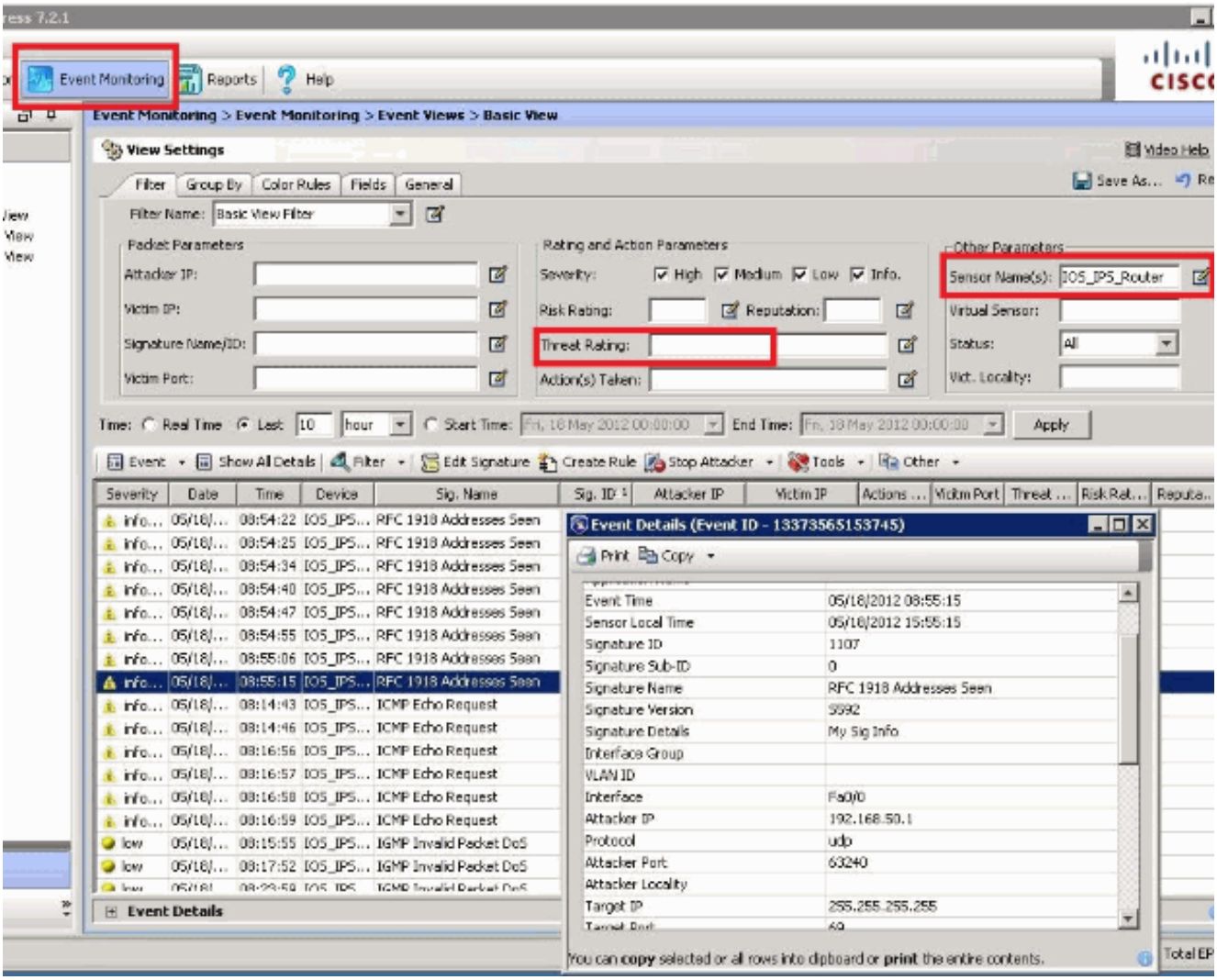


正しく追加されて、次が表示されます
:



注: HTTPS がルータに接続すればのに使用されている場合ルータの認証へのどの変更でもデバイスが IME に再発見されるように要求します。 IME の認証をリフレッシュするために、デバイス リストの下でルータをダブル クリックして下さい。 それから、新しい認証を得るために IME がルータに接続することを確かめるために『OK』 をクリック して下さい。 更新済認証を受け入れるために『Yes』 をクリック して下さい。

3. イベントの表示: クリック イベント **モニタリング**。 「センサー名前」の下でルータを選択するために確かめて下さい。**注:** デフォルトで」、フィールドを評価する「脅威の下のビュー設定で値は ">=70" に設定 されます。 この値は 70 におよび等号上で評価する脅威が付いているだけ結果ディスプレイ シグニチャを作ります。すべての重大度 シグニチャを表示するために「脅威を」フィールドは空白を評価させ続けて下さい。



関連情報

- Cisco IOS 侵入防御システム（IPS）
- IOS IPS との開始-詳細なガイド
- Cisco IPS Manager Express
- テクニカルサポートとドキュメント - Cisco Systems