Surveillez les événements générés par le système de prévention des intrusions utilisant le Manager Express IPS

Contenu

Introduction

Ce document explique comment utiliser des événements de moniteur générés par le système de prévention des intrusions (IOS IPS) utilisant le Manager Express IPS (IME).

Le Cisco IOS IPS est une caractéristique articulée autour d'un logiciel d'inspection de profond-paquet qui atténue efficacement un large éventail d'attaques réseau.

Cisco IME est un logiciel simple et basé sur GUI de Gestion IPS.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la connaissance de ces thèmes.

- Système de prévention des intrusions
- Manager Express IPS

Composants utilisés

Les informations dans ce document sont basées sur le système de prévention des intrusions utilisant le Manager Express IPS.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Caractéristiques

Condition requise :

Pour qu'IME prenne en charge l'IOS IPS, le routeur doit exécuter des versions du logiciel Cisco IOS 12.3(14)T7 et 12.4(15)T2 ou plus nouveau. IME peut prendre en charge jusqu'à 10 périphériques.

Remarque: IME prend en charge seulement la surveillance d'événement pour l'IOS IPS. La configuration n'est pas prise en charge.

Configuration

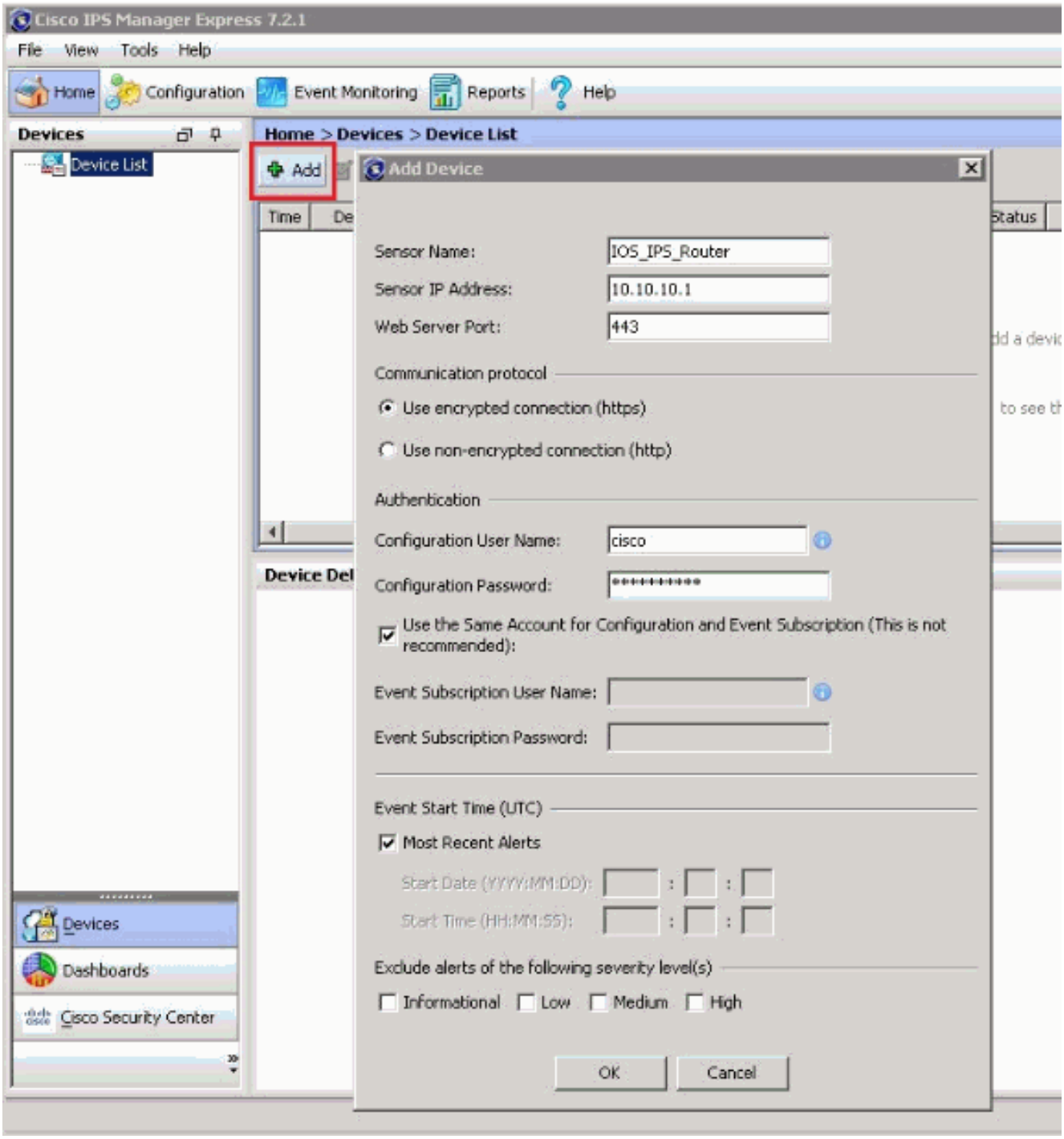
IME emploie SDEE pour obtenir des événements d'IOS IPS. La notification SDEE est désactivée par défaut et doit être manuellement activée. Pour utiliser SDEE, le web server du routeur doit être activé. Par défaut, essais IME pour établir une connexion sécurisée au routeur utilisant HTTPS (TCP 443). Ceci exige d'un certificat numérique d'être configuré sur le routeur. Sur option, IME peut être configuré pour prendre en charge une connexion unsecure utilisant le HTTP (TCP 80).

Configurer le routeur

1. Notification de l'enable SDEE :`Router(config)# ip ips notify sdee`
2. Enable HTTPS :`Router(config)#ip http secure-server`
3. HTTP d'enable (facultatif) :`Router(config)# ip http server`

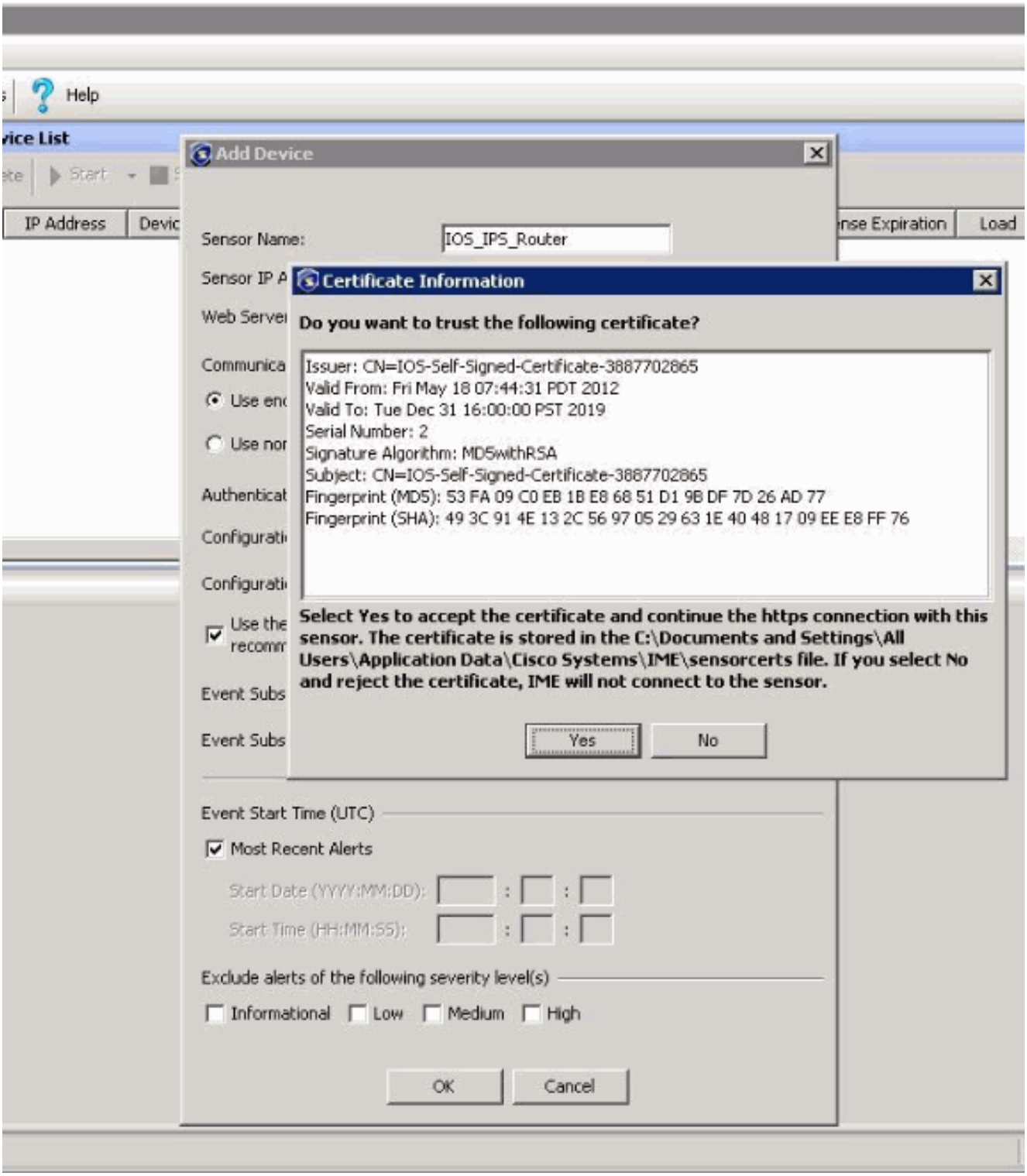
Configurer IME

1. Téléchargez et installez IME. Exécutez IME. Puis, cliquez sur Add.Téléchargement IME :http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460

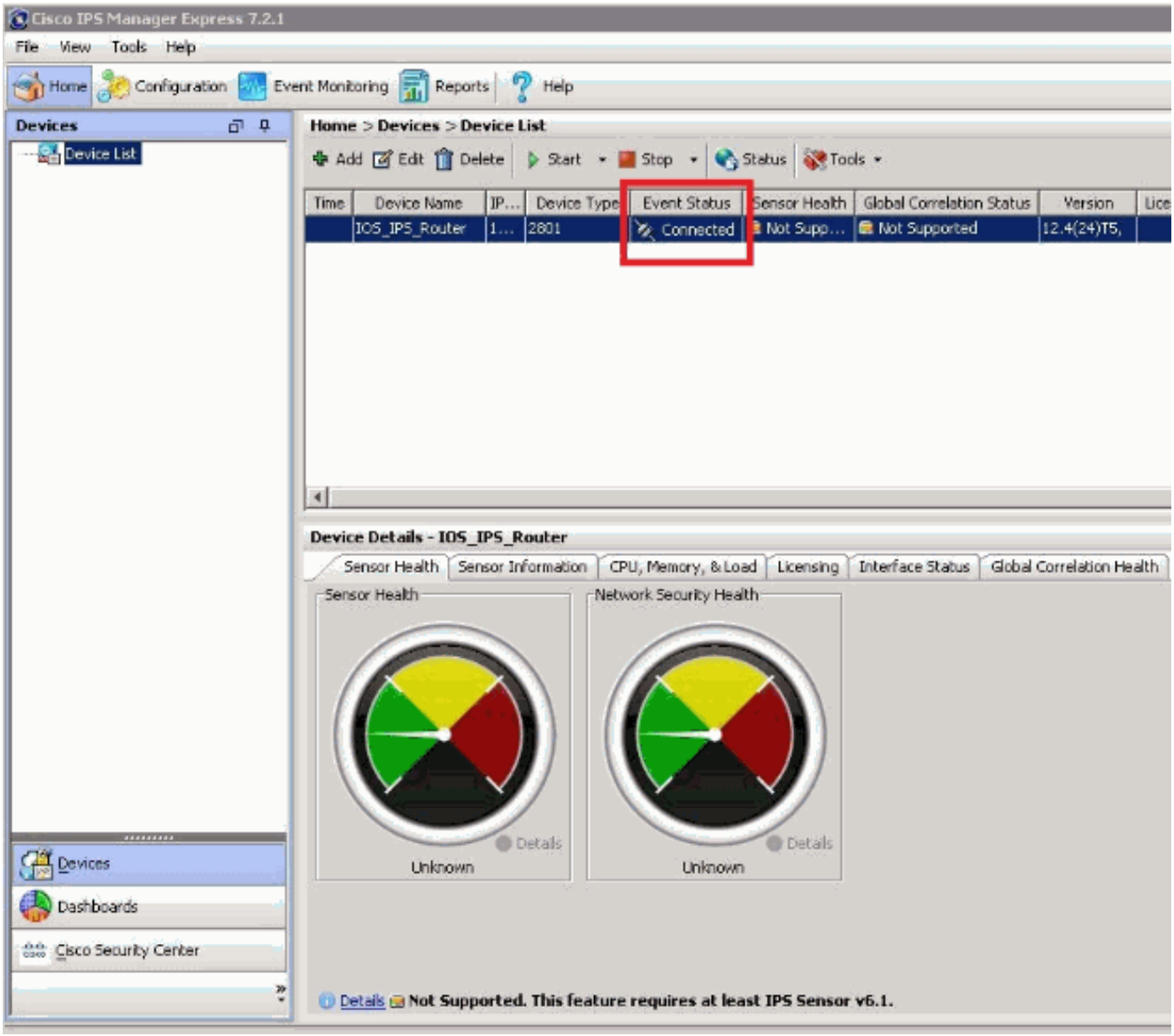


Remarque: La valeur par défaut emploie HTTPS et port 443 pour se connecter au routeur. Vous pouvez également choisir de se connecter utilisant le HTTP seulement, et changez le port à 80.

2. Si utilisant HTTPS, vous êtes présenté avec un écran pour recevoir le certificat auto-signé du routeur. Cliquez sur
Yes.

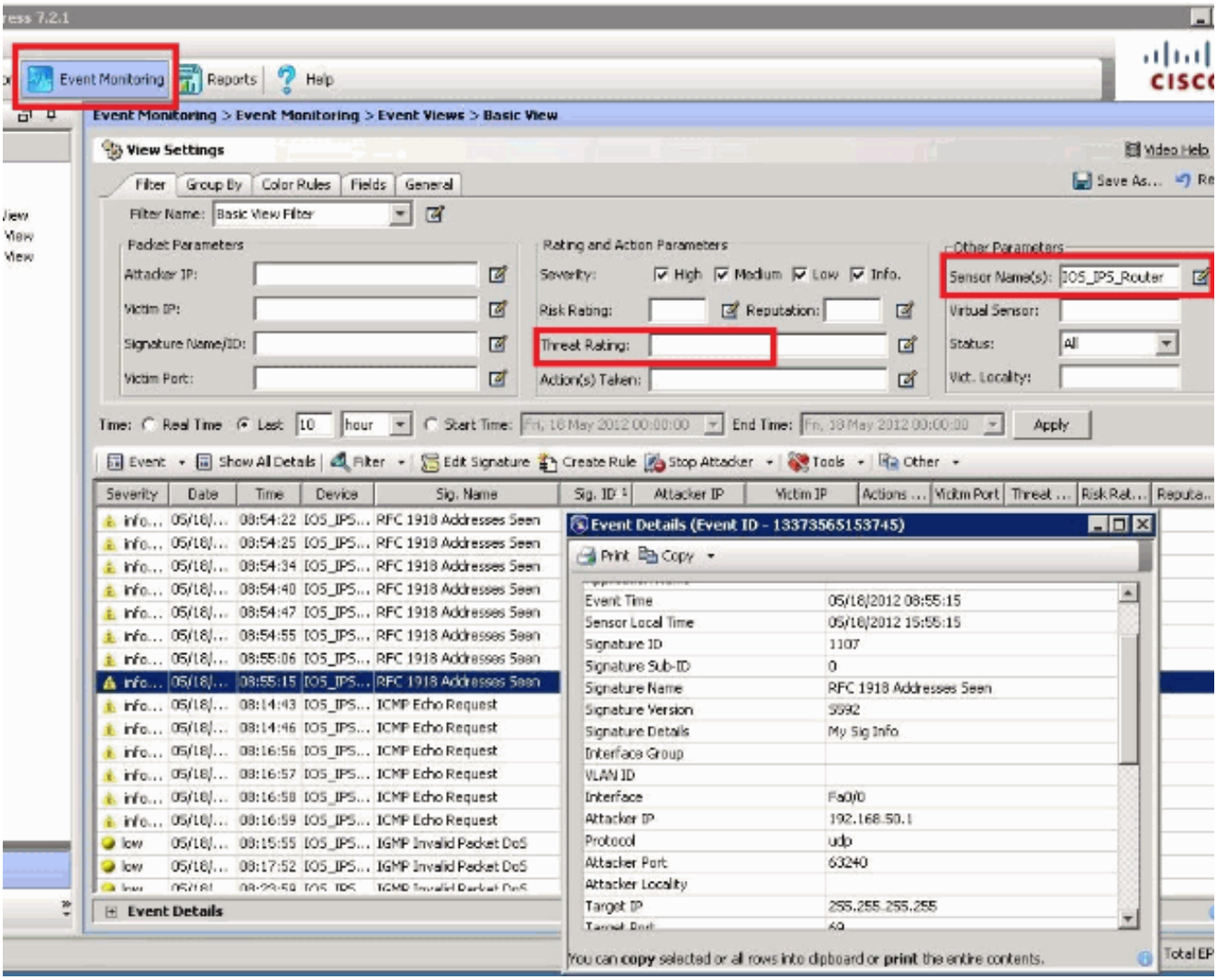


Une fois que correctement ajouté, vous verrez ce qui suit
:



Remarque: Si HTTPS est utilisé pour se connecter au routeur, toutes les modifications au certificat sur le routeur exigeront du périphérique d'être redécouvert dans IME. Pour régénérer le certificat dans IME, double-cliquer le routeur sous la liste de périphériques. Puis, cliquez sur OK pour s'assurer qu'IME se connecte au routeur pour obtenir le nouveau certificat. Cliquez sur **oui** pour recevoir le certificat mis à jour.

3. Visionnement des événements : **Surveillance d'événement de** clic. Veillez-vous pour sélectionner le routeur sous le « nom de capteur ».**Remarque:** Par défaut, dans les configurations de vue sous le champ « d'évaluation de menace », la valeur est placée à ">=70". Cette valeur fait les signatures d'affichage de résultat seulement avec l'évaluation de menace ci-dessus et l'égal à 70.Pour visualiser toutes les signatures de sévérité gardez le champ vide « d'évaluation de
menace ».



Informations connexes

- Système de prévention des intrusions
- Obtenir commencé par l'IOS IPS - Un guide pas à pas
- Cisco IPS Manager Express
- Support et documentation techniques - Cisco Systems