IPS 6.X und höher: E-Mail-Benachrichtigungen mit IME-Konfigurationsbeispiel

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Zugehörige Produkte
Konventionen
Hintergrundinformationen
Konfigurieren
Konfiguration von E-Mail-Benachrichtigungen im IME
Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument wird der Konfigurationsvorgang für Cisco IPS Manager Express (IME) erläutert, um die E-Mail-Benachrichtigung (Warnungen) zu senden, wenn Event Rules von Cisco Intrusion Prevention System (IPS)-Sensoren ausgelöst werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IPS-Gerät der Serie 4200 mit Softwareversion 6.0 und höher
- Cisco IPS Manager Express (IME) Version 6.1.1 und höher**Hinweis:** Obwohl IME zum Überwachen von Sensorgeräten verwendet werden kann, auf denen Cisco IPS 5.0 und höher ausgeführt wird, werden einige der neuen Funktionen und Funktionen von IME nur auf Sensoren unterstützt, auf denen Cisco IPS 6.1 oder höher ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Sensoren verwendet werden:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20
- AIP-SSM

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das Cisco Intrusion Prevention System (IPS) kann keine E-Mail-Warnmeldungen allein senden. Cisco IPS Manager Express (IME) kann E-Mail-Benachrichtigungen senden, wenn eine Ereignisregel ausgelöst wird. Die Variablen, die in der E-Mail-Benachrichtigung für jedes Ereignis verwendet werden können, enthalten Variablen wie die Signature-ID, die Quelle und das Ziel der Warnung und viele mehr.

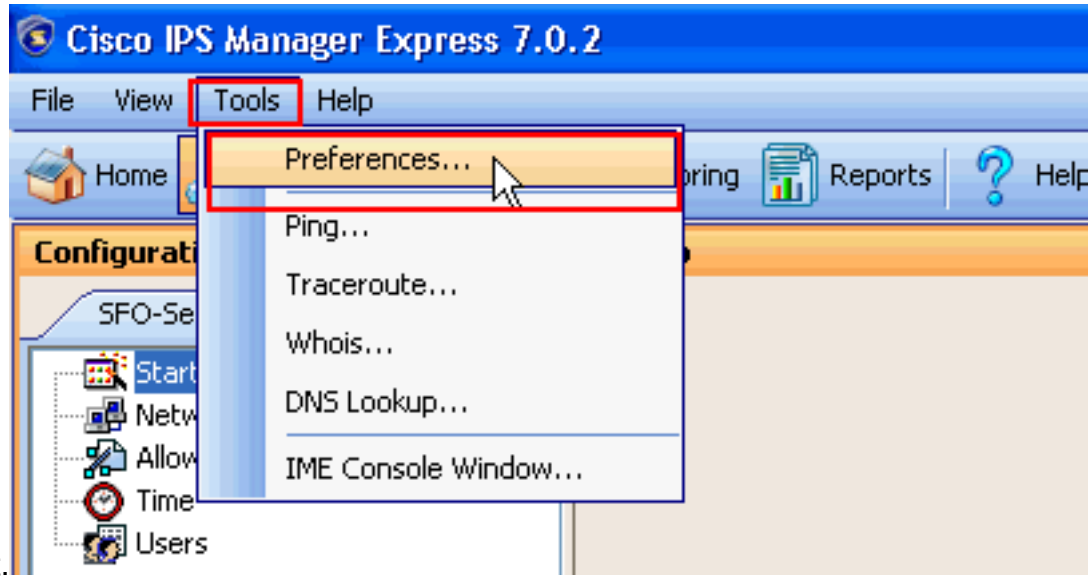
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der E-Mail-Benachrichtigung mit Cisco IPS Manager Express.

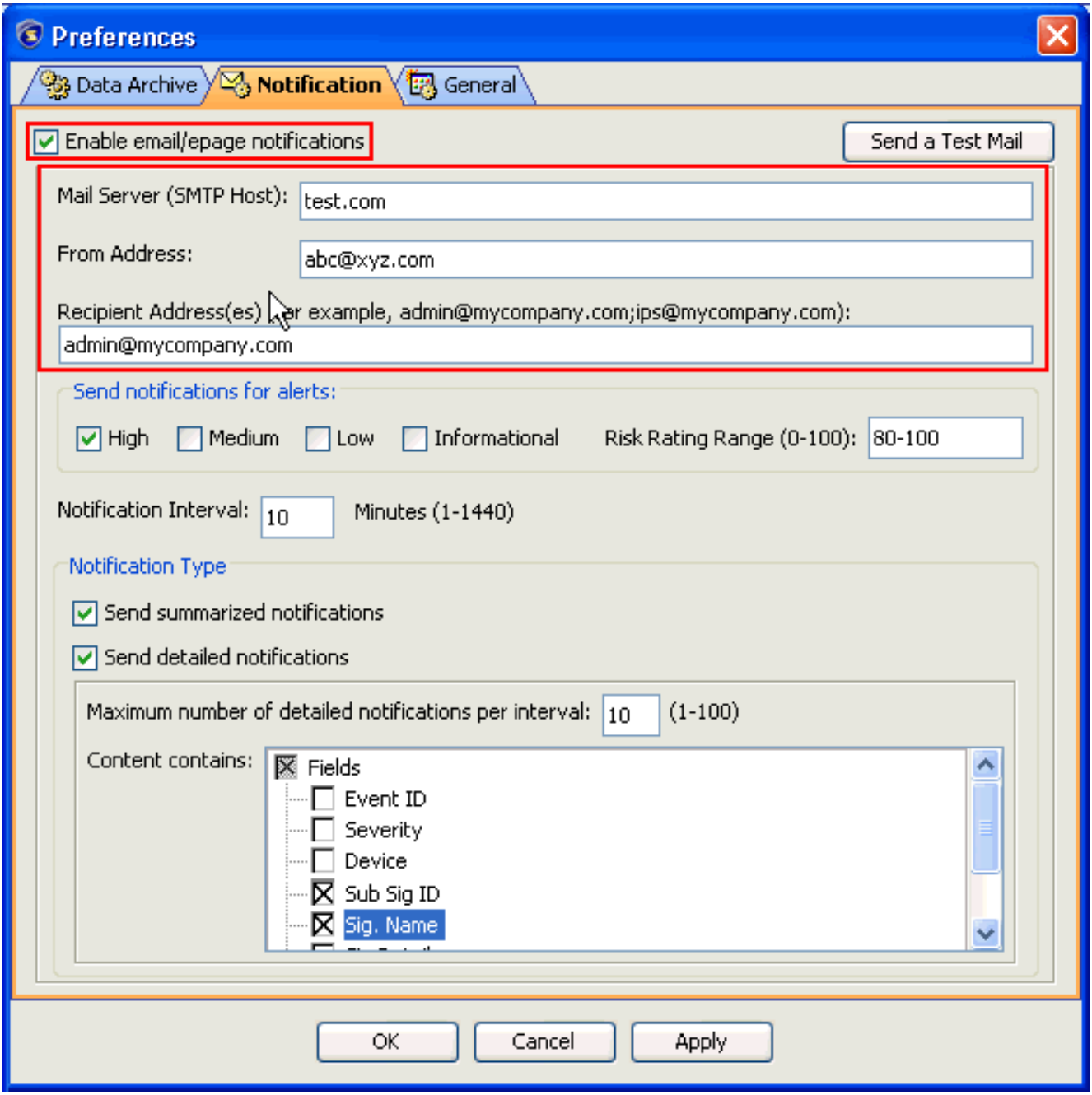
Konfiguration von E-Mail-Benachrichtigungen im IME

Gehen Sie wie folgt vor, um E-Mail-Benachrichtigungen mit Cisco IPS Manager Express zu konfigurieren:

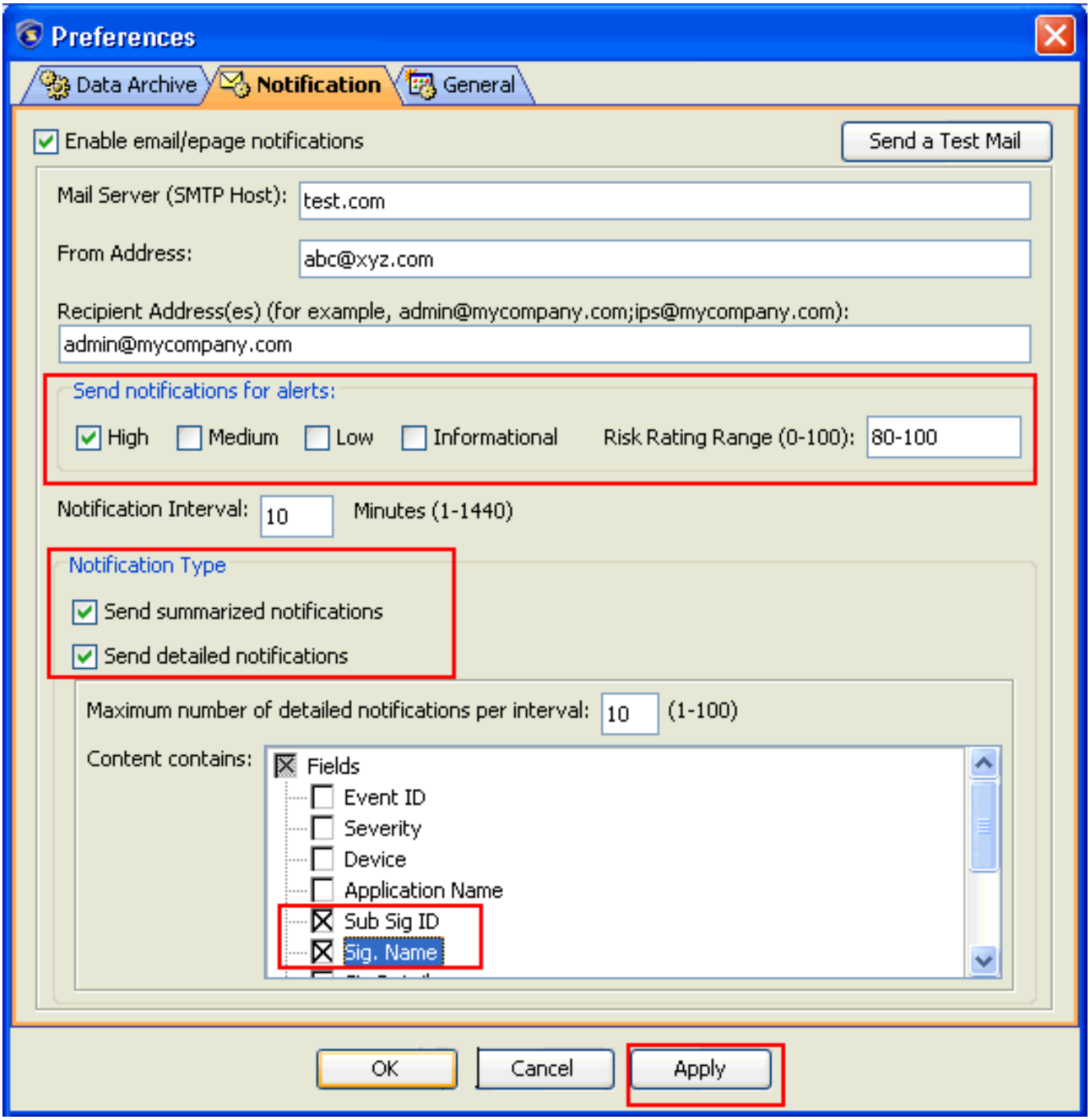
1. Wählen Sie **Extras > Voreinstellungen**, wie im Screenshot

gezeigt. 

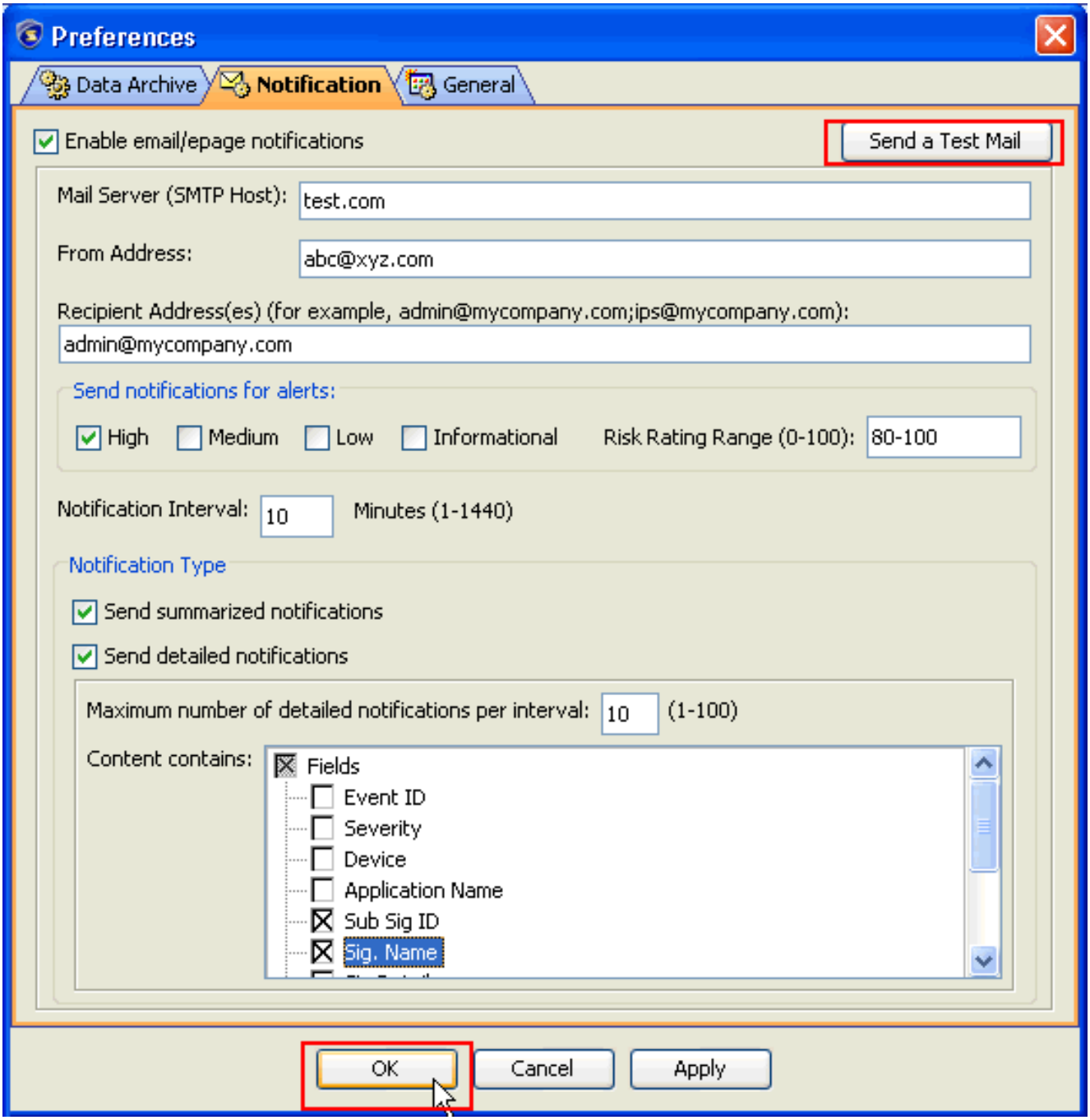
2. Wählen Sie nun im sich öffnenden Fenster Preferences (Voreinstellungen) die Registerkarte **Notification (Benachrichtigung)** aus. Stellen Sie sicher, dass das Kontrollkästchen neben **E-Mail-/Seiten-Benachrichtigungen aktivieren** aktiviert ist. Dies ist ein Muss, damit IME E-Mail-Benachrichtigungen senden kann. Geben Sie die erforderlichen Informationen in den Feldern Mail-Server, Von-Adresse und Empfängeradresse(n) an, wie im Screenshot gezeigt. In diesem Beispiel wird der **Mail-Server test.com** verwendet, die verwendete **Von-E-Mail-Adresse** lautet **abc@xyz.com**, und die **Empfänger-E-Mail-Adresse ist admin@mycompany.com.**



3. Aktivieren Sie eines der Kästchen neben **Warnungen auf hoher**, **mittlerer**, **niedriger** oder **Informations-**Ebene, um die Stufe auszuwählen, für die Warnungen gesendet werden müssen. Aktivieren Sie außerdem die Kontrollkästchen neben den erforderlichen Feldnamen, um die Felder auszuwählen, die in der Benachrichtigungs-E-Mail enthalten sein sollen. In diesem Beispiel werden die Felder **Sub Sig ID** und **Sig Name** ausgewählt. Aktivieren Sie dann die Kontrollkästchen neben dem **Senden** von **zusammengefassten Benachrichtigungen** und **Senden detaillierter Benachrichtigungen** wie gezeigt, um **Benachrichtigungstyp** auszuwählen. Klicken Sie anschließend auf **Übernehmen.**



4. Klicken Sie auf **OK**, und klicken Sie dann auf **die** Schaltfläche **Testmail senden**, um zu überprüfen, ob das IME eine E-Mail-Benachrichtigung entsprechend der Konfiguration senden kann. Wenn die konfigurierten Empfänger eine E-Mail empfangen, funktioniert die Konfiguration
einwandfrei.



Damit ist das Konfigurationsverfahren für die E-Mail-Benachrichtigung abgeschlossen.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Support-Seite für das Cisco Intrusion Prevention System
- Support-Seite für Cisco IPS Manager Express
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems