

IPS 6.X en hoger - E-mailberichten configureren met IME

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuratie van e-mailmelding in IME](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document legt het proces uit van de configuratie van Cisco IPS Manager Express (IME) om het e-mailwaarschuwing te verzenden (waarschuwingen) wanneer Event Regels worden geactiveerd door Cisco IPS-sensoren (Inbraakpreventiesysteem).

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke voorwaarden van toepassing op dit document.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4200 Series IPS-apparaat waarmee softwareversie 6.0 en hoger wordt uitgevoerd
- Cisco IPS Manager Express (IME) versie 6.1.1 en hoger**Opmerking:** Hoewel IME kan worden gebruikt om sensorapparaten te bewaken die Cisco IPS 5.0 en hoger uitvoeren, worden sommige nieuwe functies en functies die in IME worden geleverd alleen ondersteund op sensoren die Cisco IPS 6.1 of hoger uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Verwante producten](#)

Deze configuratie kan ook met deze sensoren worden gebruikt:

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

[Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

[Achtergrondinformatie](#)

Het Cisco Inbraakpreventiesysteem (IPS) heeft de mogelijkheid niet om e-mailwaarschuwingen op zichzelf te verzenden. Cisco IPS Manager Express (IME) heeft de mogelijkheid e-mailberichten te verzenden als er een Event Rule wordt geactiveerd. De variabelen die in de e-mailkennisgeving voor elke gebeurtenis kunnen worden gebruikt, omvatten variabelen zoals de Signature ID, de bron en de bestemming van de signalering en nog veel meer.

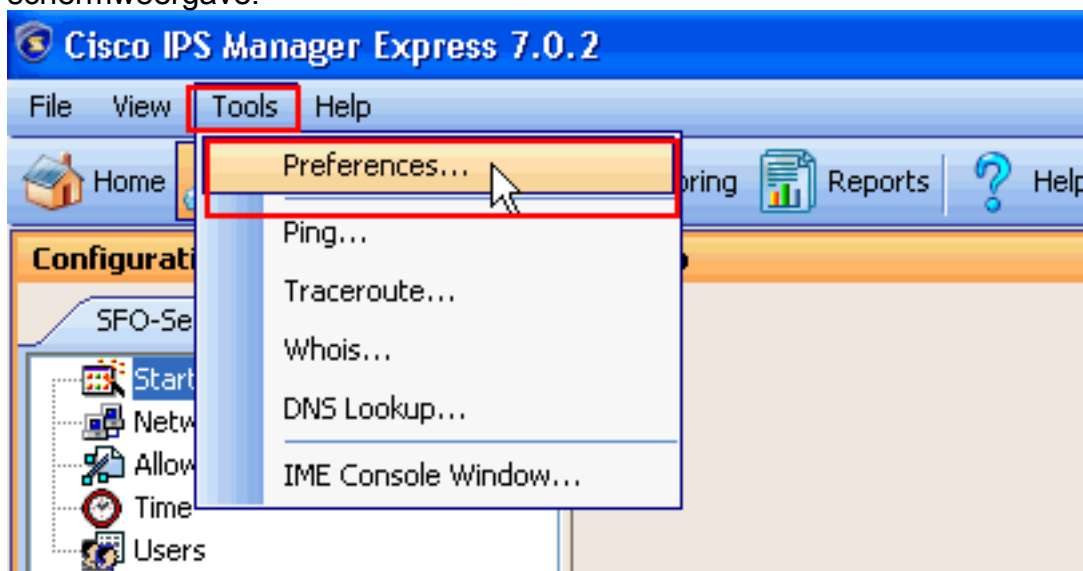
[Configureren](#)

In deze sectie, wordt u voorgesteld met de informatie om e-mailbericht met de Cisco IPS Manager Express te vormen.

[Configuratie van e-mailmelding in IME](#)

Voltooi deze stappen om e-mailmeldingen te configureren met behulp van Cisco IPS Manager Express:

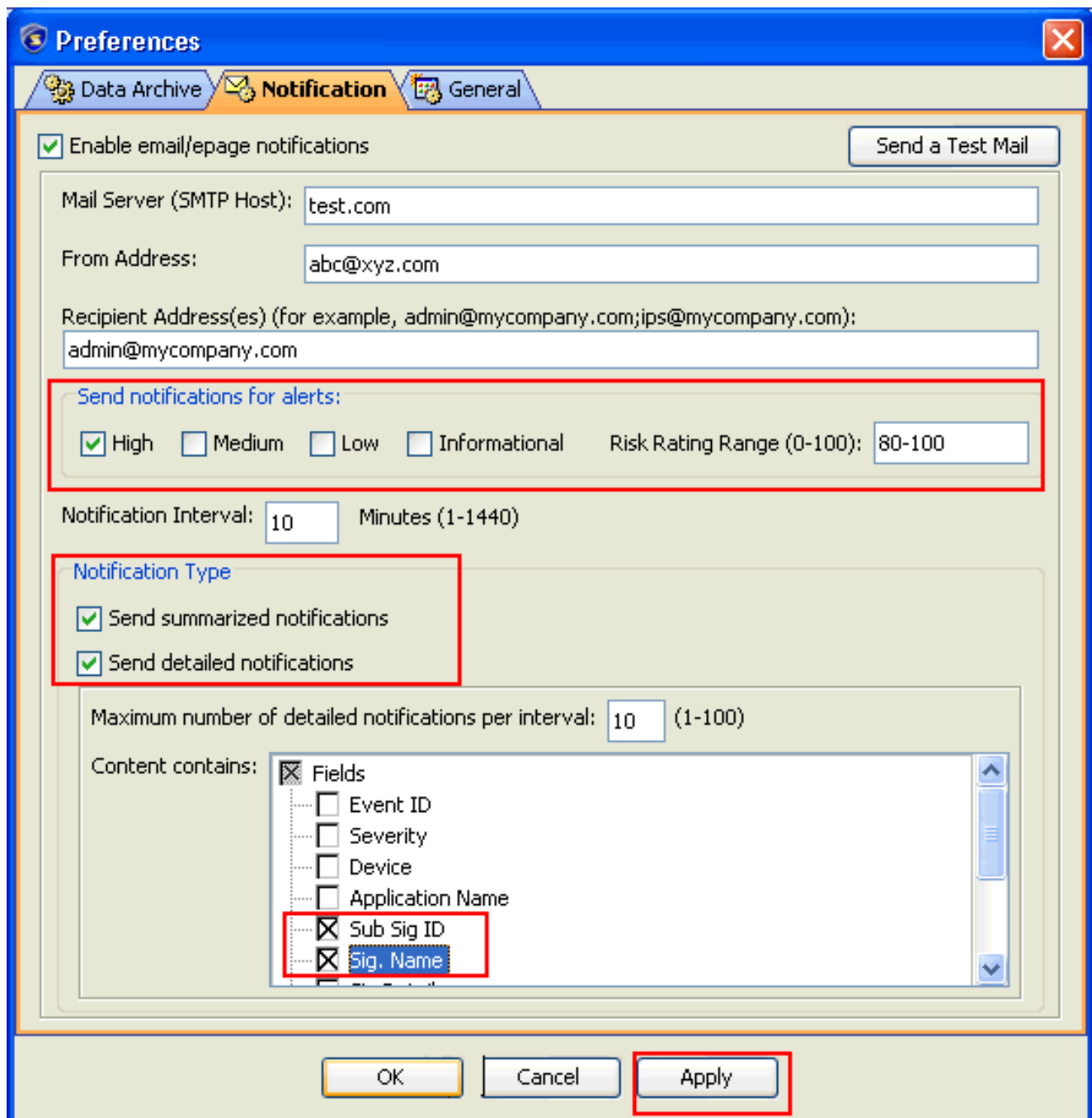
1. Kies **Gereedschappen > Voorkeuren** zoals in de schermweergave.



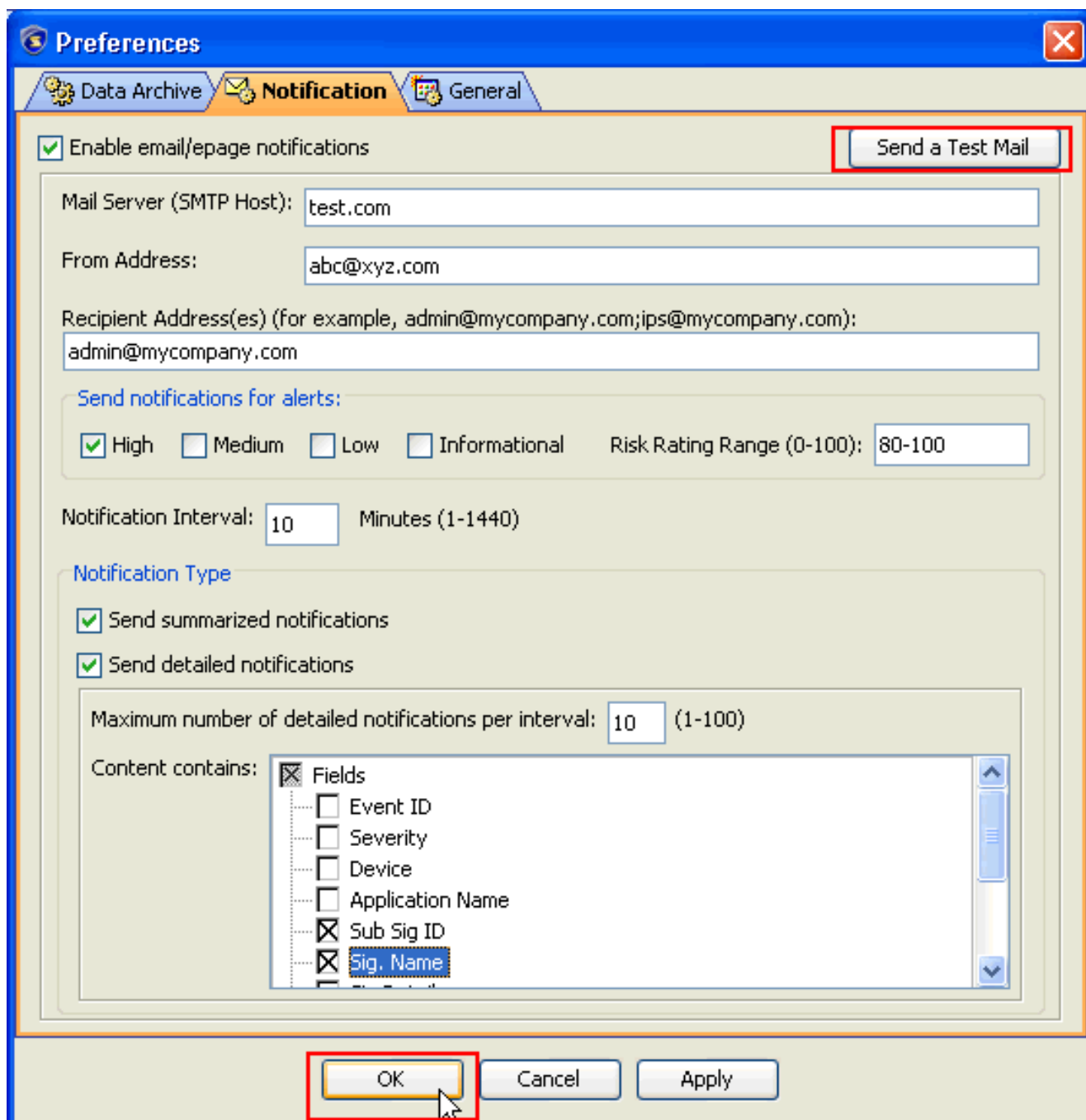
2. Kies nu in het venster Voorkeuren dat is geopend het tabblad **Kennisgeving**. Zorg dat het aankruisvakje naast **Bericht per e-mail/pagina inschakelen** is ingeschakeld, wat een vereiste is voor de IME om e-mailberichten te verzenden. Geef de gewenste informatie op in de velden Mail Server, Vanaf Adres en Adres(sen) van de ontvanger zoals getoond in de screenshot. In dit voorbeeld is de gebruikte **Mail Server test.com**, het **Van e-mail adres abc@xyz.com** en het **Ontvangende e-mailadres is admin@mycompany.com**.

The screenshot shows the 'Preferences' dialog box with the 'Notification' tab selected. The 'Enable email/epage notifications' checkbox is checked. The 'Mail Server (SMTP Host)' field contains 'test.com', the 'From Address' field contains 'abc@xyz.com', and the 'Recipient Address(es)' field contains 'admin@mycompany.com'. Below these fields, there is a section for 'Send notifications for alerts' with radio buttons for 'High', 'Medium', 'Low', and 'Informational', and a 'Risk Rating Range (0-100)' field set to '80-100'. The 'Notification Interval' is set to '10' minutes. Under 'Notification Type', both 'Send summarized notifications' and 'Send detailed notifications' are checked. The 'Maximum number of detailed notifications per interval' is set to '10'. The 'Content contains' section has a list of fields with checkboxes: 'Fields' (checked), 'Event ID' (unchecked), 'Severity' (unchecked), 'Device' (unchecked), 'Sub Sig ID' (checked), and 'Sig. Name' (checked).

3. Controleer een van de vakken naast **signaleringen op hoog, middelgroot, laag of informatief niveau** om het niveau te kiezen waarvoor signaleringen moeten worden verzonden. Controleer ook de vakjes naast de vereiste veldnamen om de velden in de e-mail te selecteren. In dit voorbeeld zijn de velden **Sub Sig ID** en **Naam Sig**. Controleer vervolgens de vakjes naast het **verzenden van samengevatte kennisgevingen** en **verstuur gedetailleerde kennisgevingen** zoals aangegeven om het **kennisgevingstype** te kiezen. Klik vervolgens op **Toepassen**.



4. Klik op **OK** en vervolgens op een **Test Mail** - knop **verzenden** om te controleren of de IME in staat is om een e-mailbericht te verzenden volgens de configuratie. Als een e-mail wordt ontvangen door de ontvangers die zijn ingesteld, werkt de configuratie prima.



Dit voltooit de procedure voor het configureren van e-mailberichten.

[Problemen oplossen](#)

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

[Gerelateerde informatie](#)

- [Categoriepagina voor Cisco-inbraakpreventiesysteem](#)
- [Ondersteuning van Cisco IPS Manager Express](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)