IPS 6.X e mais tarde: Notificações de Email usando o exemplo de configuração IME

Índice

Introdução

Este documento explica o processo da configuração do gerente do ips Cisco expresso (IME) a fim enviar a mensagem da notificação de Email (alertas) quando as regras do evento estão provocadas por sensores do Sistema de prevenção de intrusões da Cisco (IPS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo IPS do Cisco 4200 Series que executa a versão de software 6.0 e mais atrasado
- Versão 6.1.1 e mais recente expressa do gerente do ips Cisco (IME)**Nota:** Quando IME puder ser usado para monitorar os dispositivos de sensor que executam o ips Cisco 5.0 e mais atrasado, alguma dos novos recursos e da funcionalidade entregados em IME é apoiada somente nos sensores que executam o ips Cisco 6.1 ou mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com estes sensores:

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

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O Sistema de prevenção de intrusões da Cisco (IPS) não tem a capacidade para enviar alertas do email no seus próprios. O gerente do ips Cisco expresso (IME) tem a capacidade para enviar notificações de E-mail quando uma regra do evento é provocada. As variáveis que podem ser usadas dentro da notificação de E-mail para cada evento incluem variáveis tais como o ID de assinatura, a fonte e o destino do alerta, e muito mais.

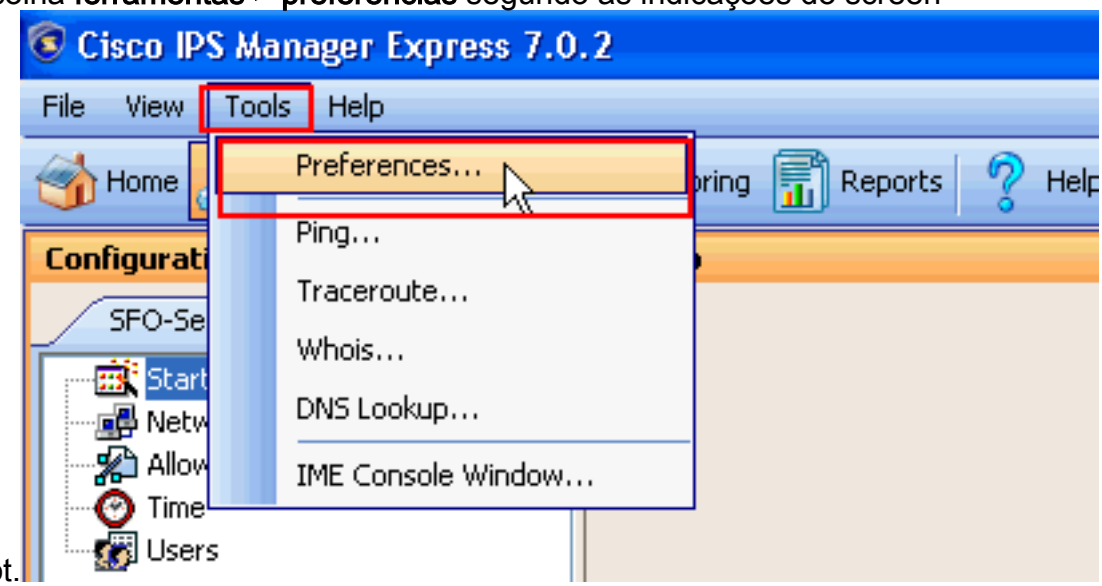
Configurar

Nesta seção, você é presentado com a informação para configurar a notificação de Email com o gerente do ips Cisco expresso.

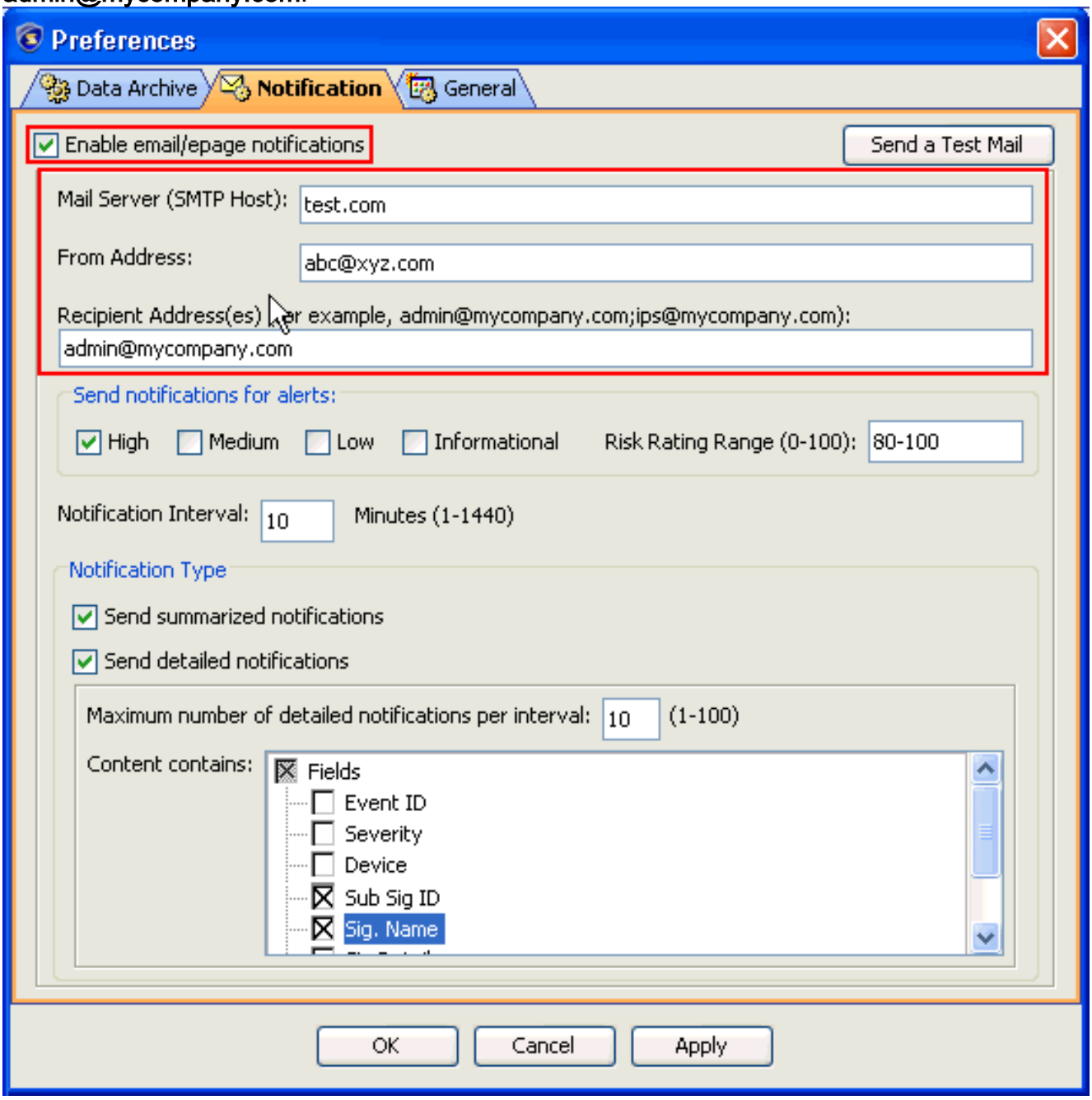
Configuração da notificação de Email em IME

Termine estas etapas a fim configurar notificações de Email usando o gerente do ips Cisco expresso:

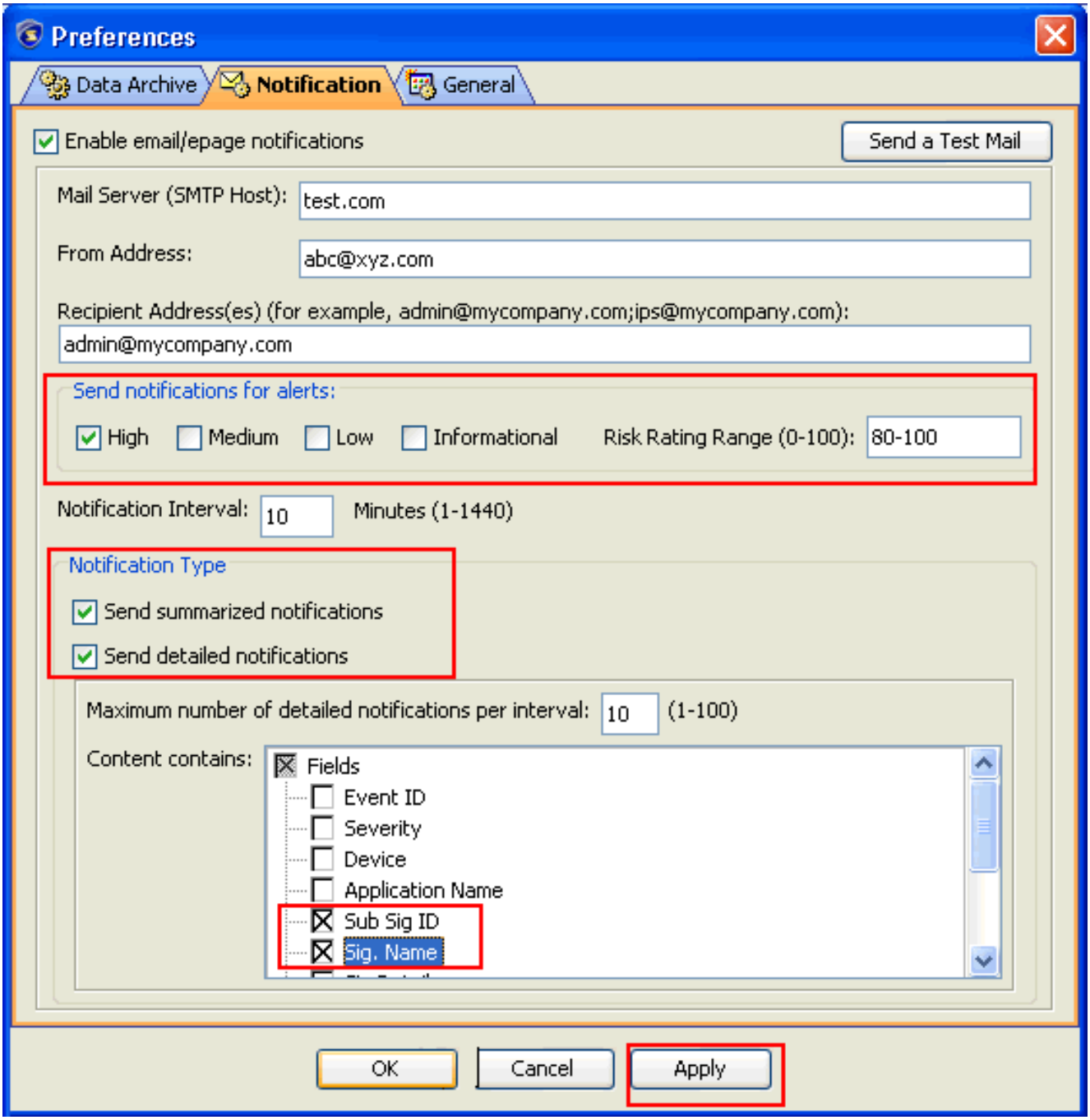
1. Escolha **ferramentas > preferências** segundo as indicações do screen shot.



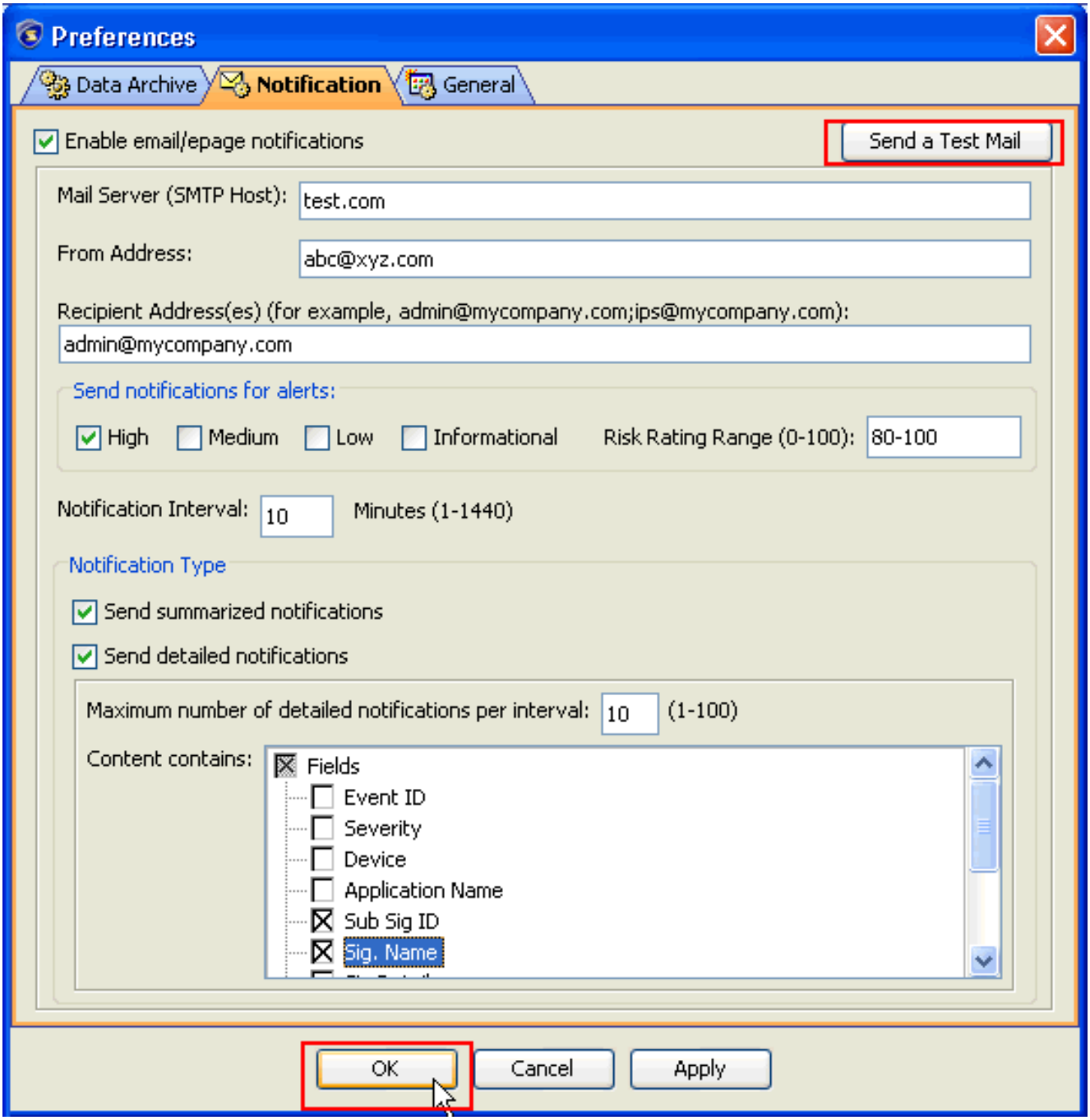
2. Agora na janela de preferências que abriu, escolha a aba da **notificação**. Certifique-se de que a caixa de verificação ao lado de **permite notificações do email/epage** está verificada, que é uma obrigação para que o IME envie notificações de Email. Forneça a informação requerida no mail server, do endereço, e campos de endereço destinatários segundo as indicações do screen shot. Neste exemplo, o **mail server** usado é **test.com**, do **endereço email** usado é **abc@xyz.com** e o **endereço email destinatário** é **admin@mycompany.com**.



3. Verifique uma das caixas ao lado de **alto**, **médio**, **ponto baixo**, ou os alertas do **nível informacional** a fim escolher o nível para que alerta têm que enviado. Igualmente verifique as caixas ao lado dos nomes arquivados exigidos em ordem escolhem os campos a estam presente no correio da notificação. Neste exemplo, os campos escolhidos são os **Sig secundários ID** e o **nome dos Sig**. Verifique então as caixas ao lado de **enviam notificações resumidas** e **enviam notificações detalhadas** segundo as indicações da ordem para escolher o **tipo de notificação**. Clique então **aplicam-se.**



4. Clique a **APROVAÇÃO**, e clique-a então **enviam** sobre um botão do **correio do teste** a fim verificar se o IME pode enviar um alerta do email de acordo com a configuração. Se um email é recebido pelos receptores configurou então os trabalhos da configuração muito bem.



Isto termina o procedimento de configuração da notificação de Email.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Página de suporte do Sistema de prevenção de intrusões da Cisco
- Página de suporte expressa do gerente do ips Cisco
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems