IPS 6.X 以降： IME を使用した E メール通知の設定例

目次

概要

このドキュメントでは、Cisco Intrusion Prevention System（IPS）センサーによってイベント ルールがトリガーされた際に、電子メールによる通知メッセージ（アラート）を送信するように Cisco IPS Manager Express（IME）を設定する手順について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 6.0 およびそれ以降が実行されている Cisco 4200 シリーズ IPS デバイス
- Cisco IPS Manager Express（IME）バージョン 6.1.1 およびそれ以降**注:** IME では、Cisco IPS 5.0 およびそれ以降で実行されているセンサー デバイスの監視に使用でき、IME で提供される新しい機能の一部は、Cisco IPS 6.1 またはそれ以降で実行されているセンサーでのみサポートされます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次のセンサーにも使用できます。

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

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。

背景説明

Cisco Intrusion Prevention System（IPS）には、それ自体で電子メール アラートを送信する機能はありません。 Cisco IPS Manager Express（IME）には、イベント ルールがトリガーされた際に電子メール通知を送信する機能があります。 各イベントの電子メール通知の中で使用できる変数には、署名 ID、アラートの送信元と宛先などの情報が含まれます。

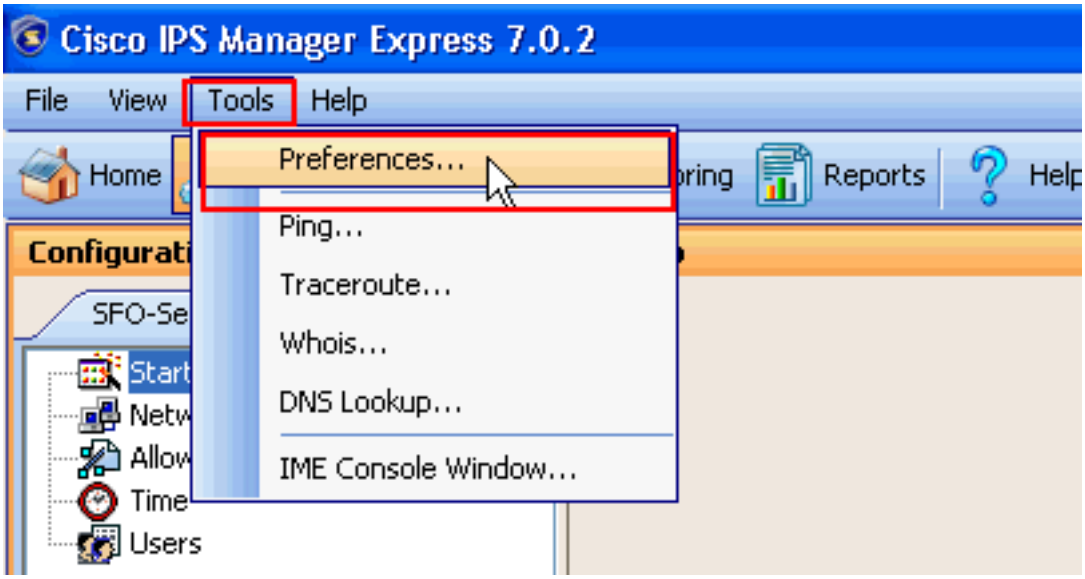
設定

このセクションでは、Cisco IPS Manager Express で電子メール通知を設定するための情報を提供してます。

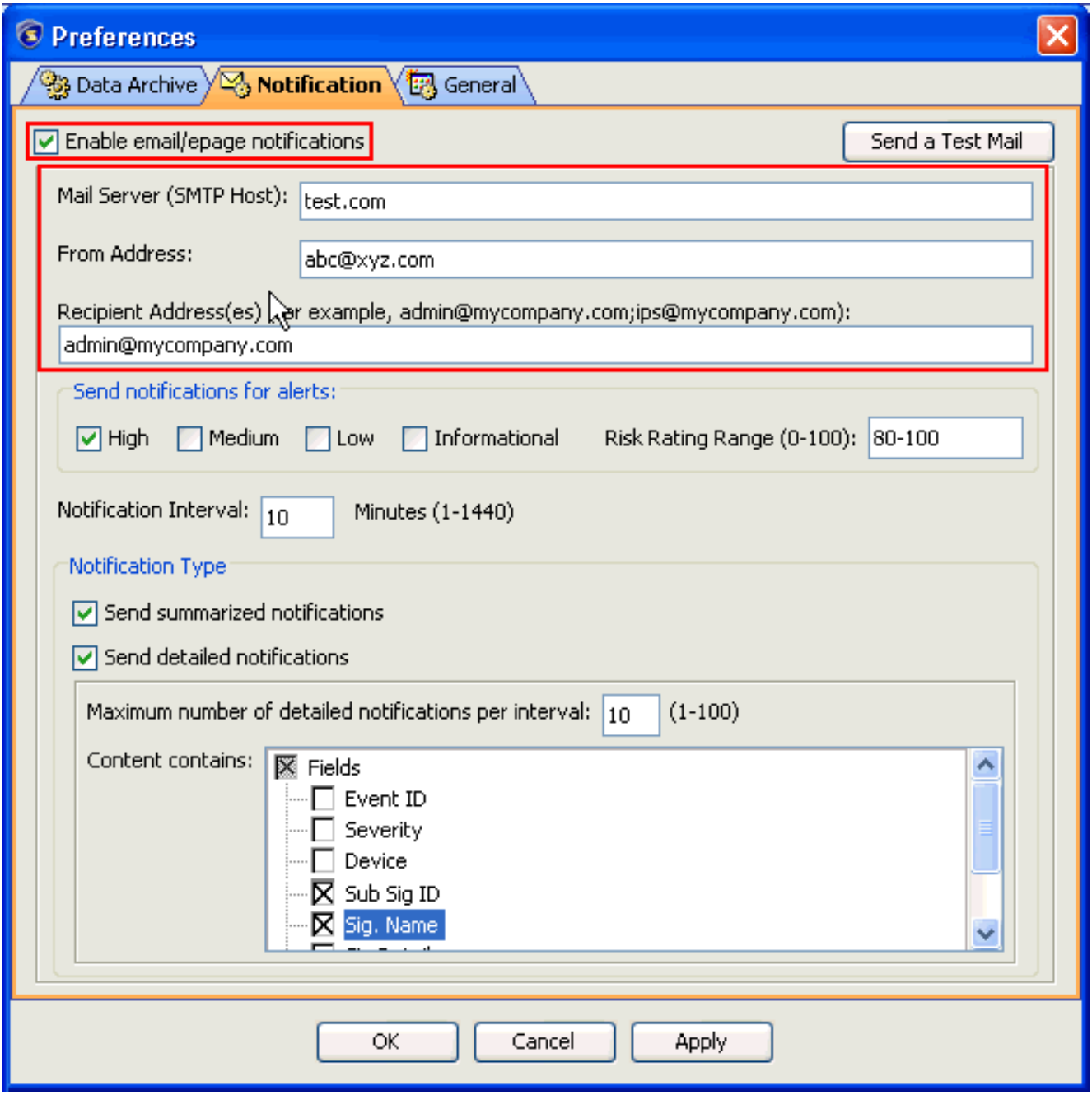
IME での電子メール通知の設定

Cisco IPS Manager Express を使用して電子メール通知を設定するには、次の手順を実行してください。

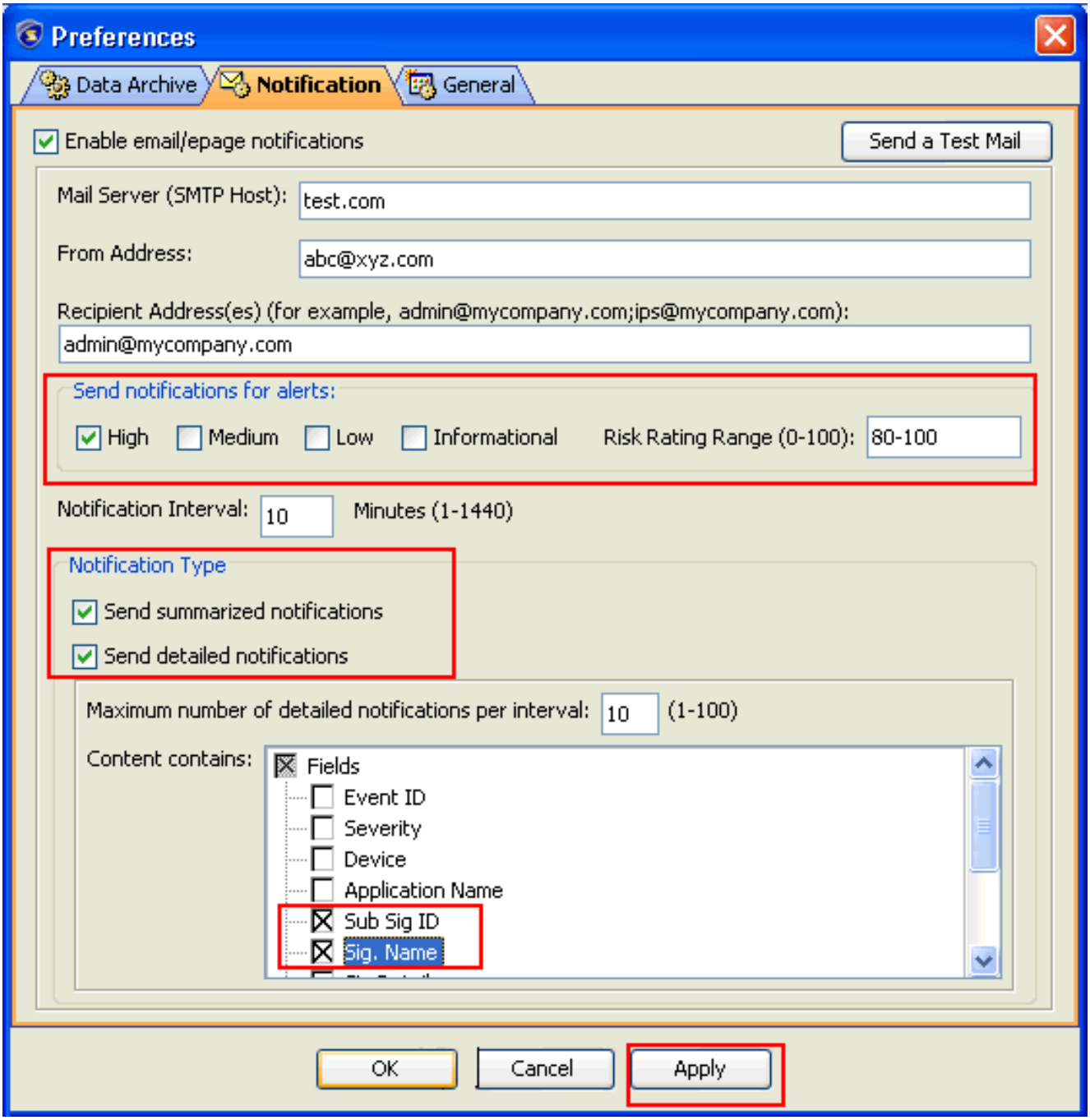
1. スクリーン ショットに従って、[Tools] > [Preferences] の順に選択します。



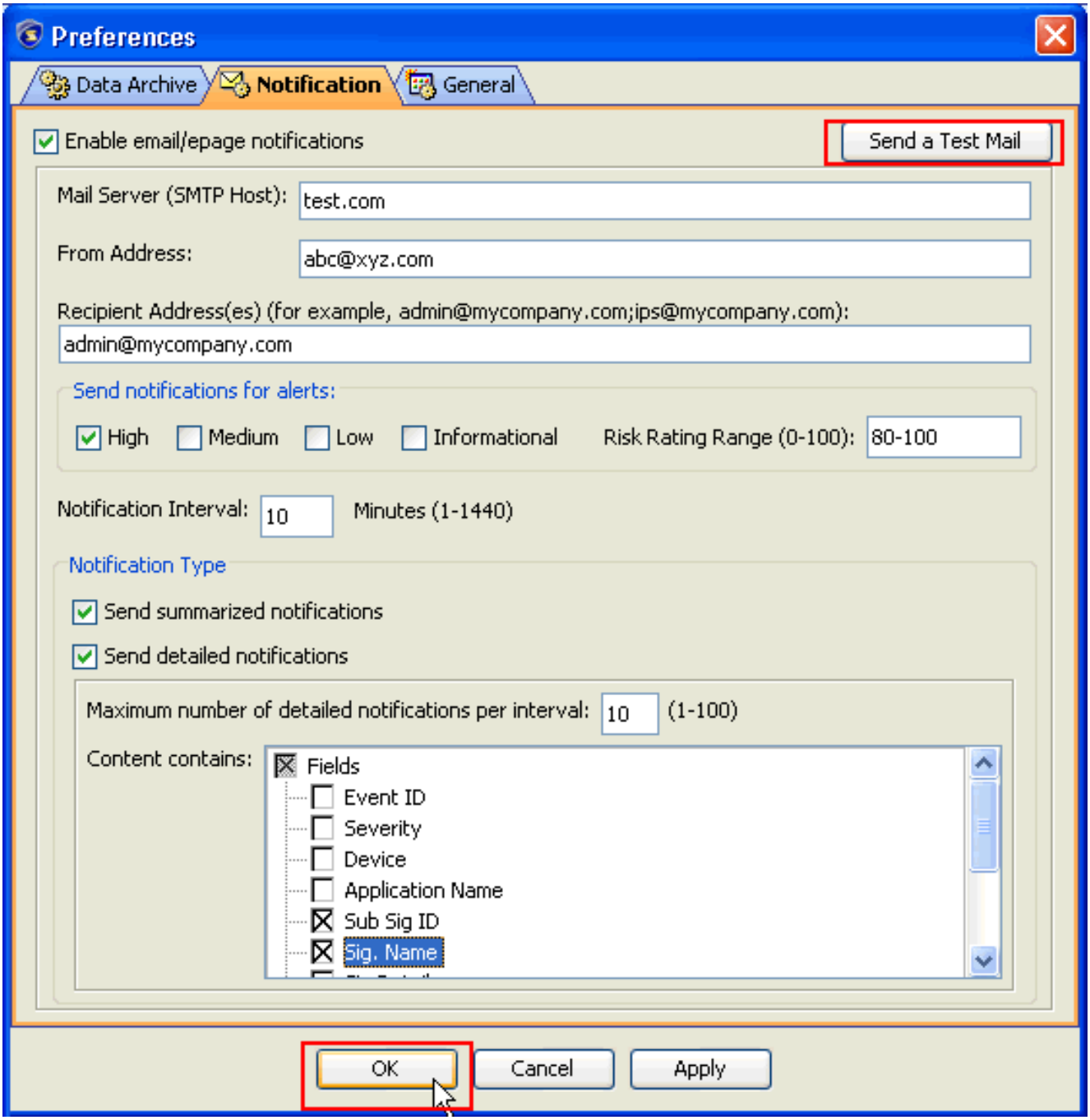
2. 開いた [Preferences] ウィンドウで、[Notification] タブを選択します。 [Enable email/epage notifications] の隣のチェックボックスがオンになっていることを確認します。これは、IME が電子メール通知を送信するのに必須です。 [Mail Server]、[From Address]、および [Recipient Address(es)] の各フィールドにスクリーン ショットに従って必要な情報を入力します。 この例では、使用される [Mail Server] は [test.com]、使用される [From email Address] は [abc@xyz.com]、[Recipient email Address] は [admin@mycompany.com] です。



3. [High]、[Medium]、[Low]、または [Informational level] アラートの隣にあるボックスのいずれかをオンにし、アラートを送信する必要のあるレベルを選択します。 また、通知メールの中に表示されるように選択するには、フィールド名の隣にあるボックスをオンにします。この例では、選択されたフィールドは、[Sub Sig ID] および [Sig Name] です。 その後、表示されているように [send summarized notifications] および [send detailed notifications] の隣にあるチェック ボックスをオンにして、[Notification Type] を選択します。 次に [Apply] をクリックします。



4. [OK] をクリックしてから、[send a Test Mail] ボタンをクリックし、IME が設定に従って電子メール アラートを送信できるかチェックします。 設定した受信者が電子メールを受信すれば、設定は正常に動作しています。



これで電子メール通知の設定手順は完了です。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Intrusion Prevention System に関するサポート ページ
- Cisco IPS Manager Express に関するサポート ページ
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems