IPS 6.x: Aktivieren/Deaktivieren der Zusammenfassung eines bestimmten Ereignisses mit IDM

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Zusammenfassung eines bestimmten Ereignisses in der IPS-Softwareversion 6.x mithilfe des IPS Device Manager (IDM) aktivieren/deaktivieren.

Hinweis: Zugriffslisten müssen in den IPS-Appliances konfiguriert werden, um den Zugriff vom Host oder vom Netzwerk aus zu ermöglichen, in dem Managementsoftware wie IDM und IEV (IDS Event Viewer) installiert sind und ordnungsgemäß funktionieren. Weitere Informationen finden Sie im Abschnitt Ändern der Zugriffsliste im Abschnitt Konfigurieren des Cisco Intrusion Prevention System-Sensors mithilfe der Befehlszeilenschnittstelle 5.0.

Voraussetzungen

Anforderungen

Dieses Dokument wird unter der Annahme erstellt, dass IPS 6.x installiert ist und ordnungsgemäß funktioniert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco IPS Sensor der Serie 4200, der die Softwareversion 6.0(2)E1 ausführt.

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.

Konventionen

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

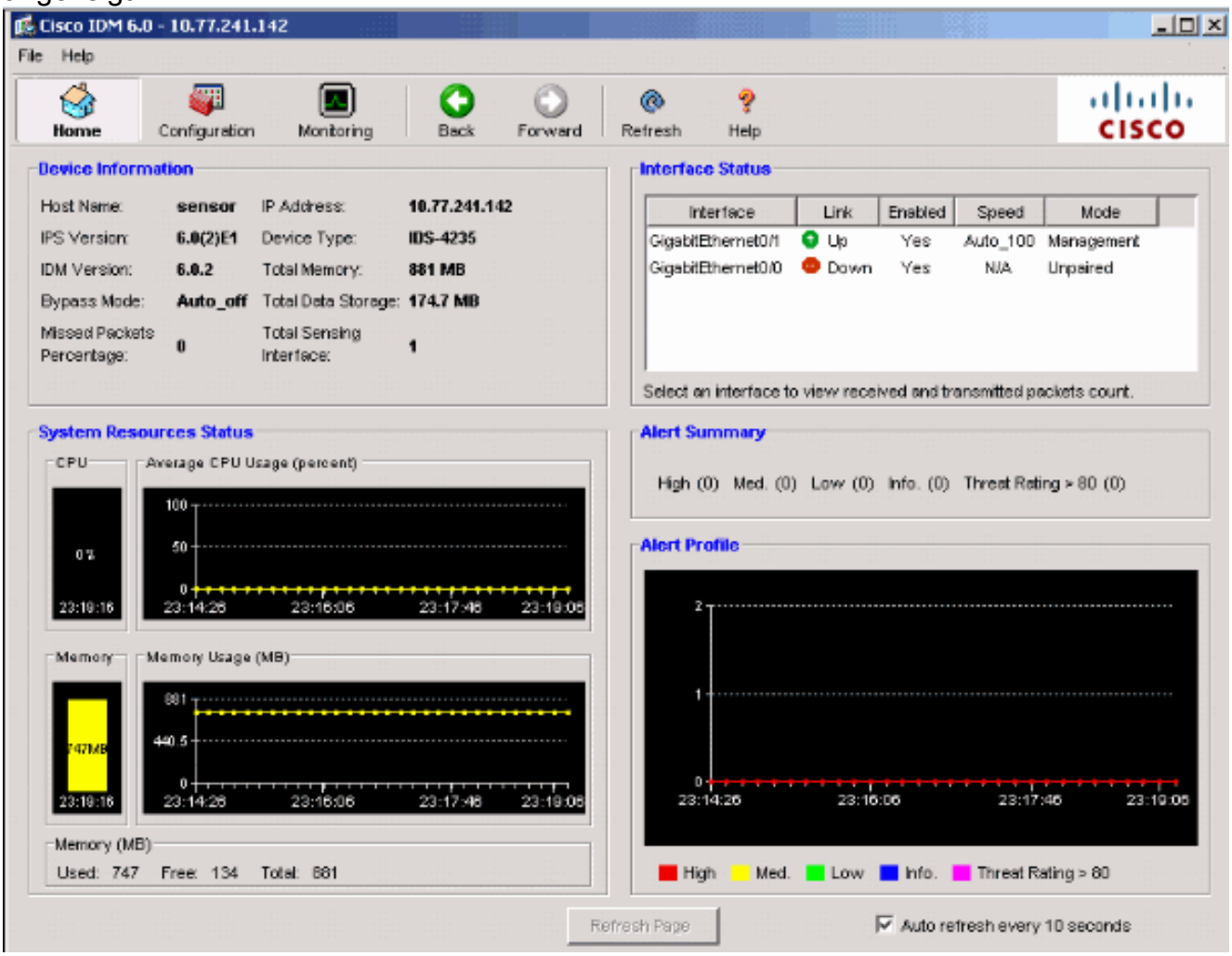
Aktivieren/Deaktivieren der Zusammenfassung eines bestimmten Ereignisses mit IDM

Dieser Abschnitt enthält ein Beispiel, in dem Sie die Zusammenfassung für die **Signature-ID** aktivieren/deaktivieren können**: 5748**.

IDM-Konfiguration

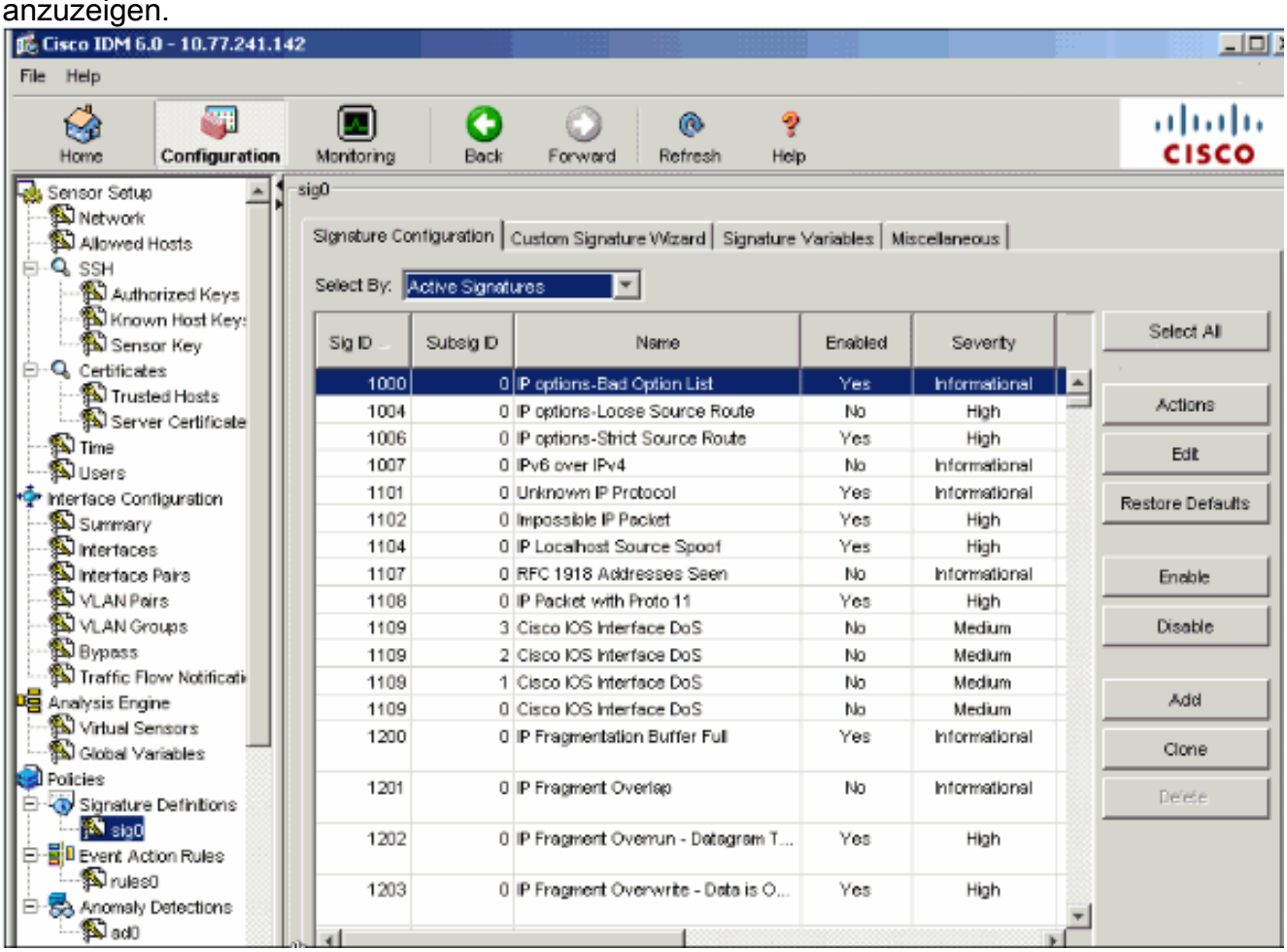
Führen Sie diese Schritte aus.

1. Starten Sie IDM.
2. Klicken Sie auf **Home**, um die Startseite des IDM anzuzeigen. Auf dieser Seite werden die Geräteinformationen
   angezeigt.

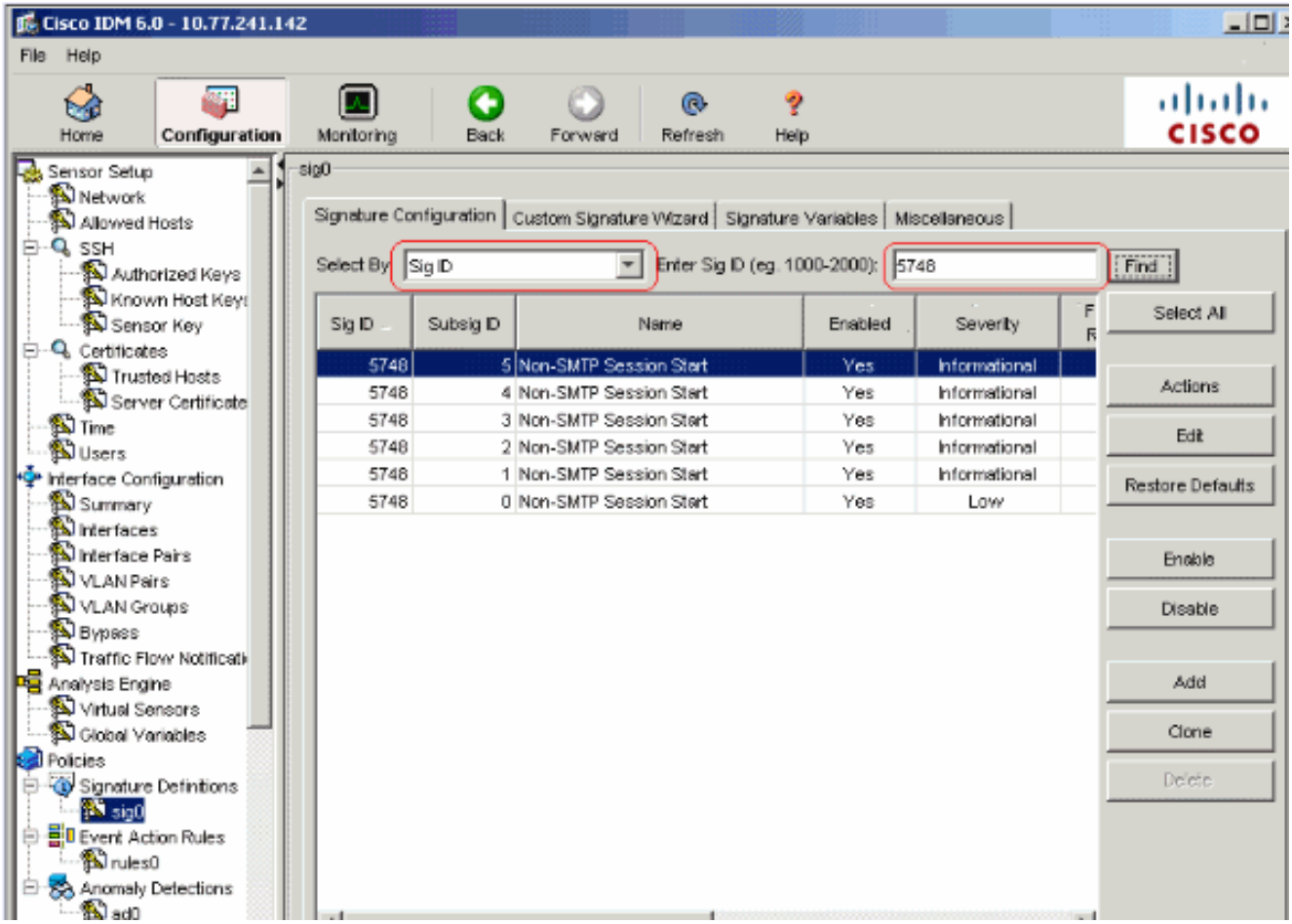


3. Wählen Sie **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration > Select By: Signature-ID**, um alle im Sensor verfügbaren Signaturen

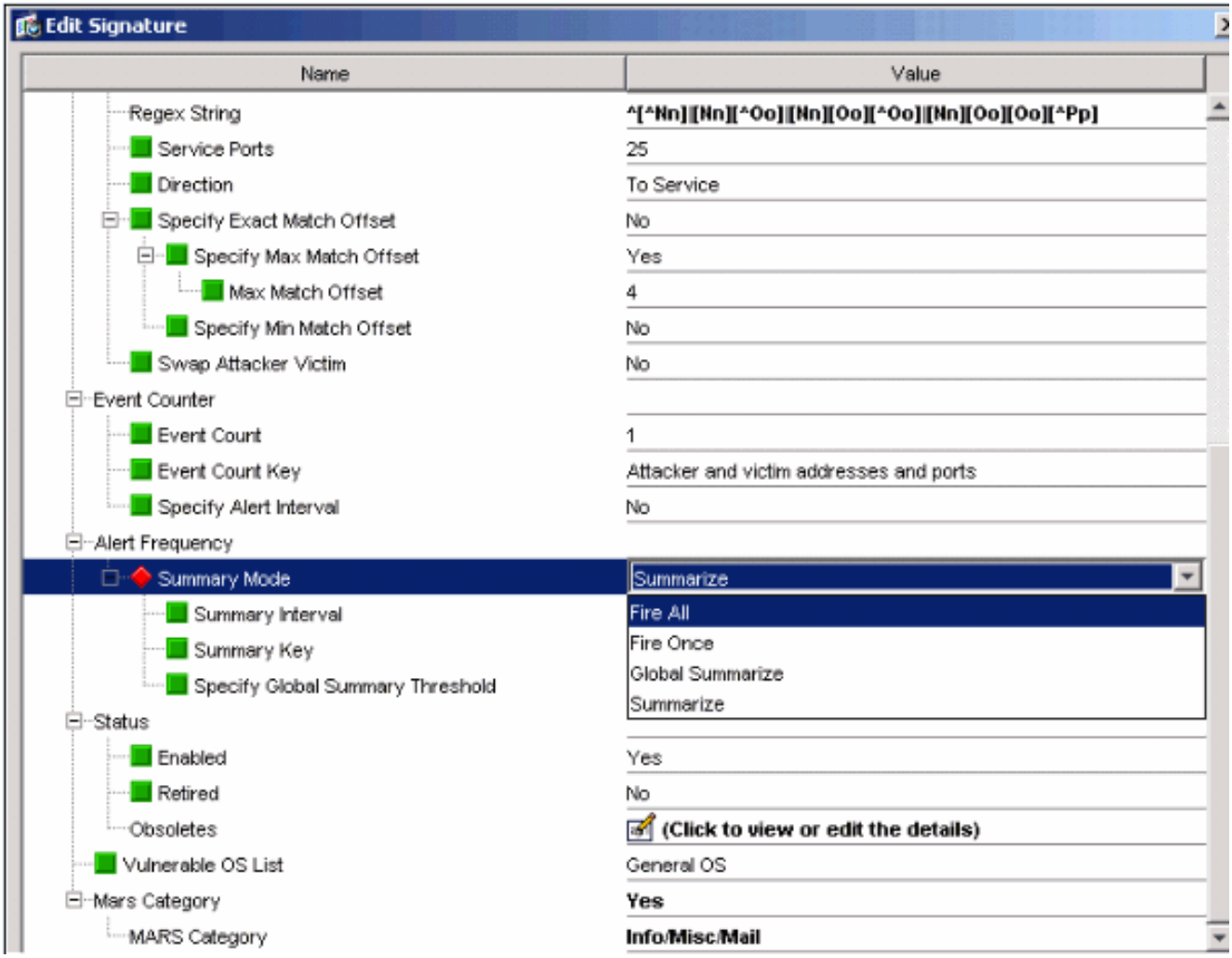
anzuzeigen.



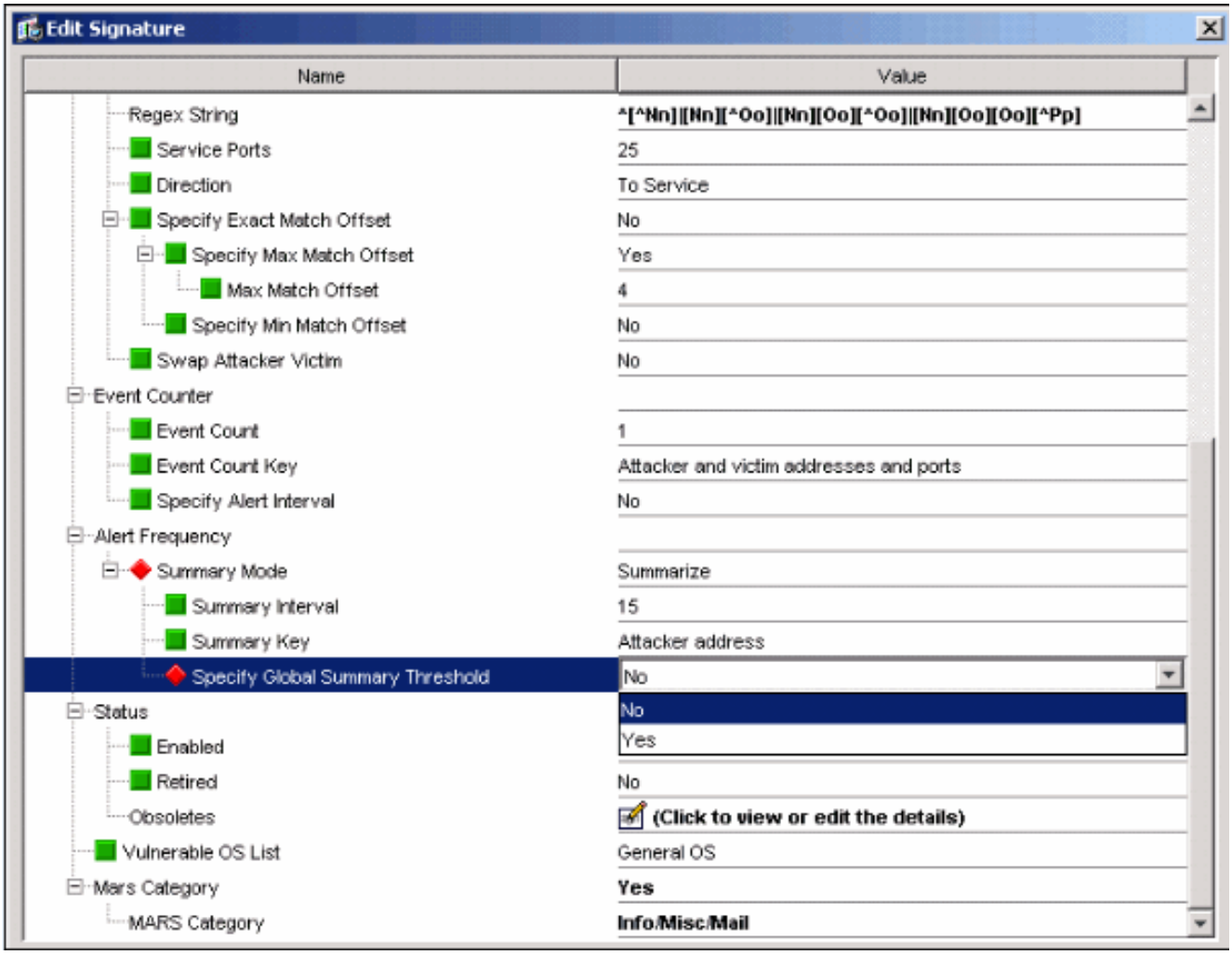
4. Wählen Sie **Signature-ID** aus dem Dropdown-Menü Wählen Sie Nach aus, und geben Sie dann die Signature-ID **5748** ein, um eine bestimmte Signatur zu suchen.



5. Klicken Sie auf **Bearbeiten**, um die Signatur zu bearbeiten.
6. Wählen Sie im Fenster Signatur bearbeiten die Option **Signaturdefinition > Warnfrequenz > Zusammenfassungsmodus aus**, und ändern Sie die Aktion im Dropdown-Menü Zusammenfassen von **Zusammenfassen** in **Feuer**.



7. Vergewissern Sie sich, dass Globalen Übersichtsschwellenwert angeben auf **Nein** festgelegt ist.



Zugehörige Informationen

- Support-Seite für das Cisco Intrusion Prevention System
- Support-Seite für Cisco IPS Geräte-Manager
- Erste Schritte mit IOS IPS
- Technischer Support und Dokumentation - Cisco Systems