IPS 6.X - Abilitazione/disabilitazione di un riepilogo di un evento specifico tramite IDM

Sommario

Introduzione

In questo documento viene descritto come abilitare/disabilitare il riepilogo di un evento specifico nel software Intrusion Prevention System (IPS) versione 6.x utilizzando IPS Device Manager (IDM).

Nota: gli elenchi degli accessi devono essere configurati negli accessori IPS in modo da consentire l'accesso dall'host o dalla rete in cui sono installati e funzionano correttamente software di gestione quali IDM e IEV (IDS Event Viewer). Per ulteriori informazioni, consultare la sezione Modifica dell'elenco degli accessi in Configurazione del sensore Cisco Intrusion Prevention System (Cisco) tramite l'interfaccia della riga di comando 5.0.

Prerequisiti

Requisiti

Per la creazione di questo documento si presume che IPS 6.x sia installato e funzioni correttamente.

Componenti usati

Per la stesura del documento, è stato usato un sensore Cisco IPS serie 4200 con software versione 6.0(2)E1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

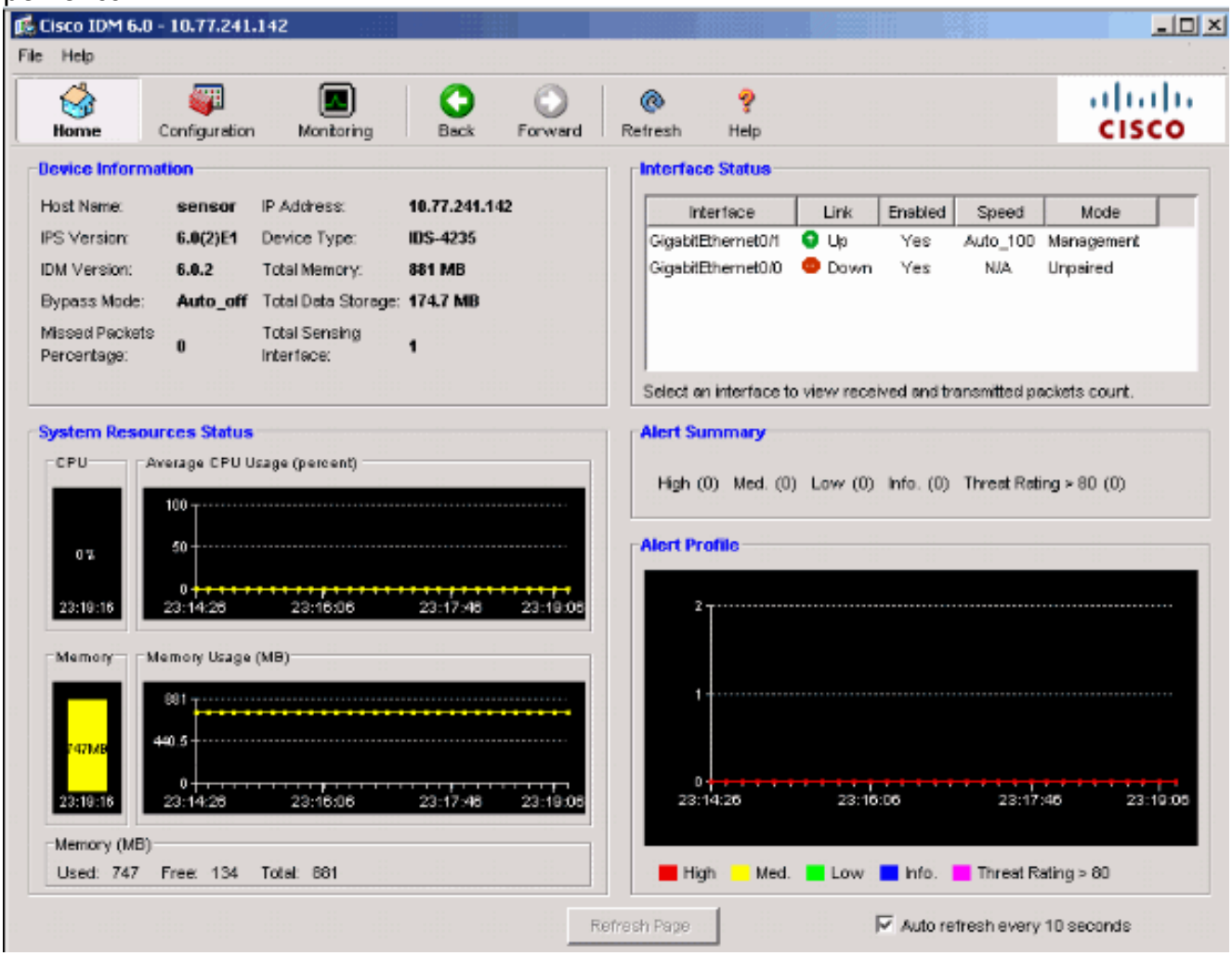
Attivare/disattivare il riepilogo di un evento specifico utilizzando IDM

Per una comprensione più approfondita, in questa sezione viene fornito un esempio in cui è possibile attivare/disattivare il riepilogo per il **Signature ID: 5748.**

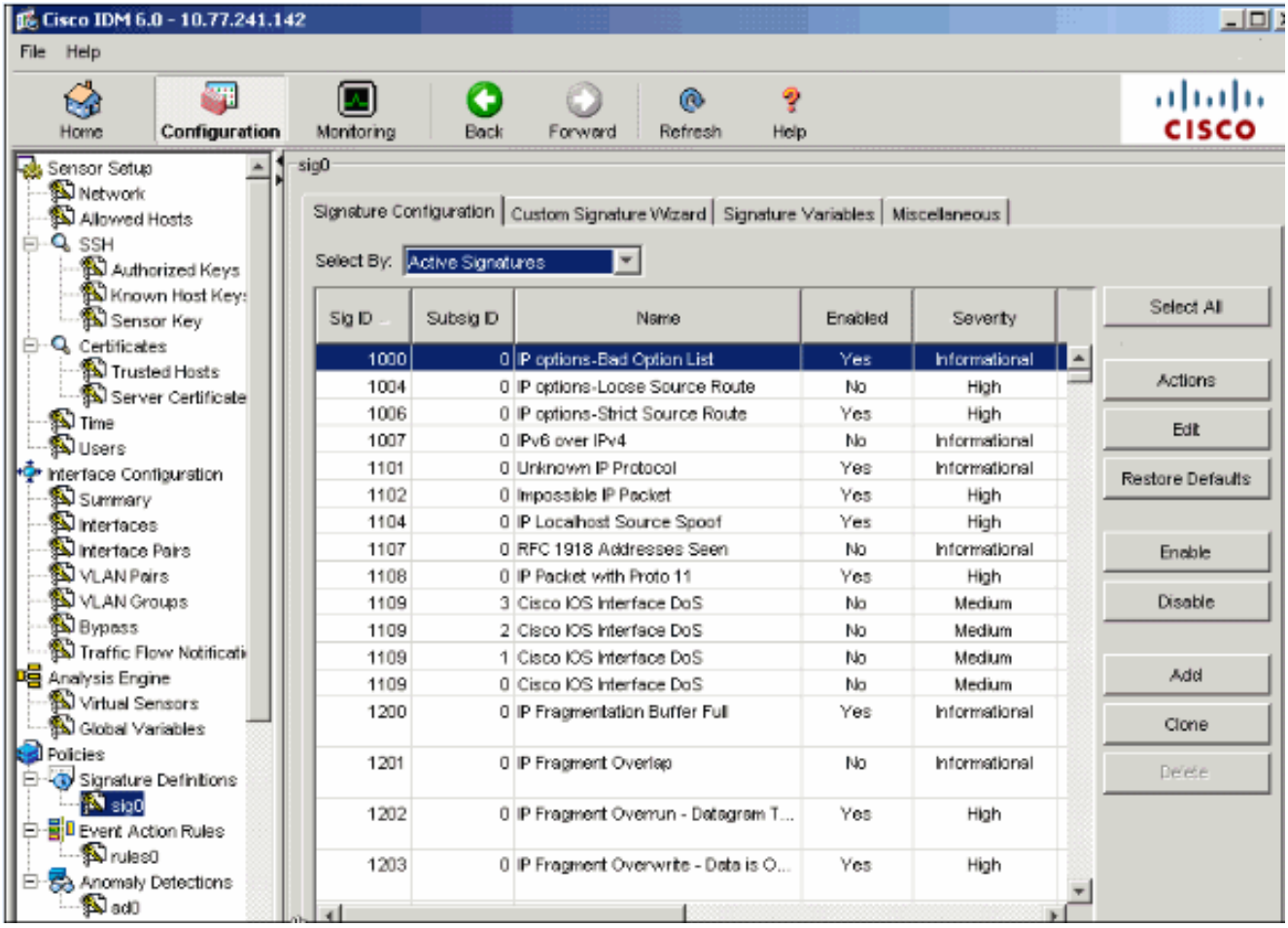
Configurazione IDM

Attenersi alla seguente procedura.

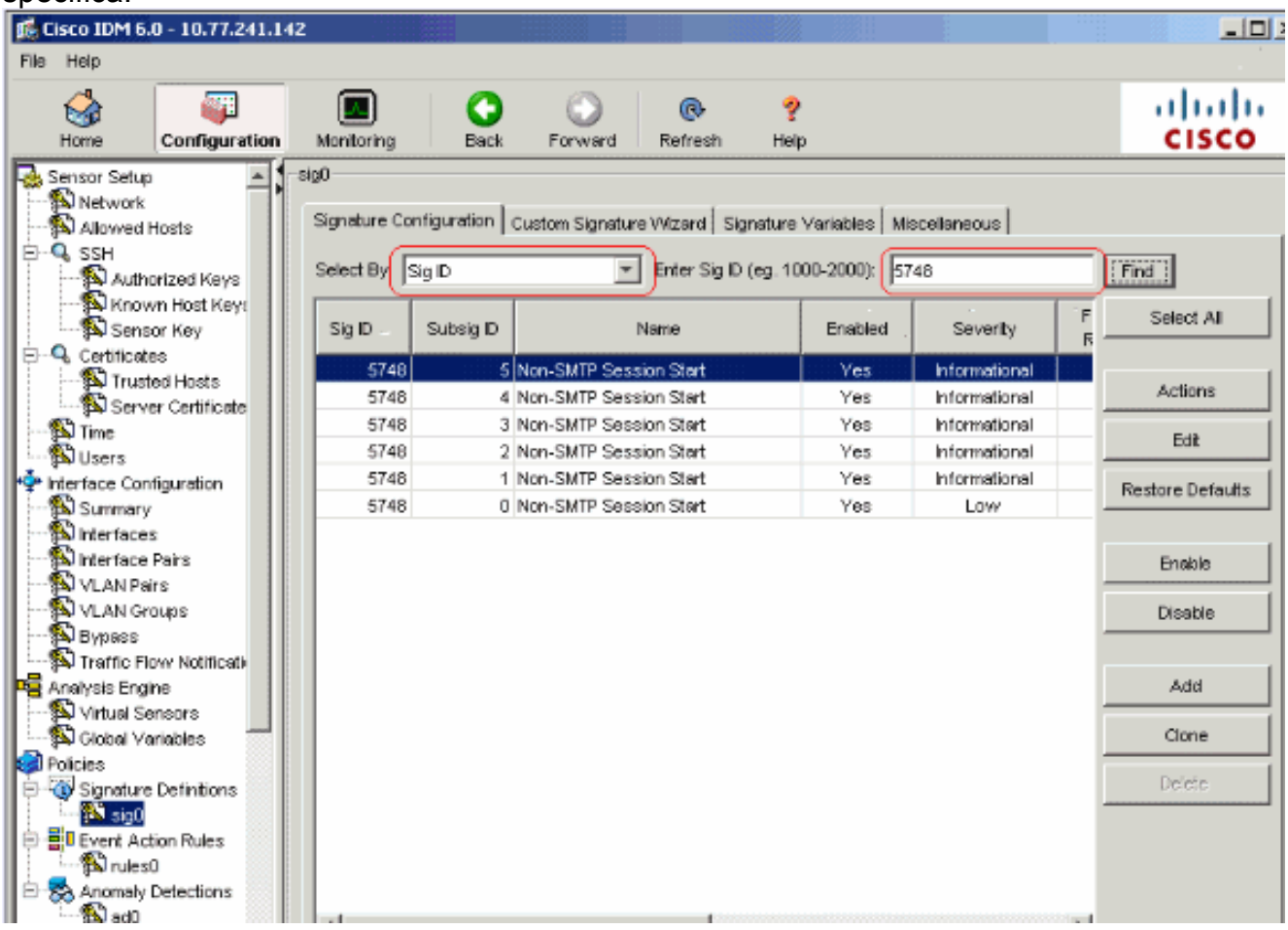
1. Avviare IDM.
2. Fare clic su **Home page** per visualizzare la home page di IDM. In questa pagina vengono visualizzate le informazioni sulla periferica.



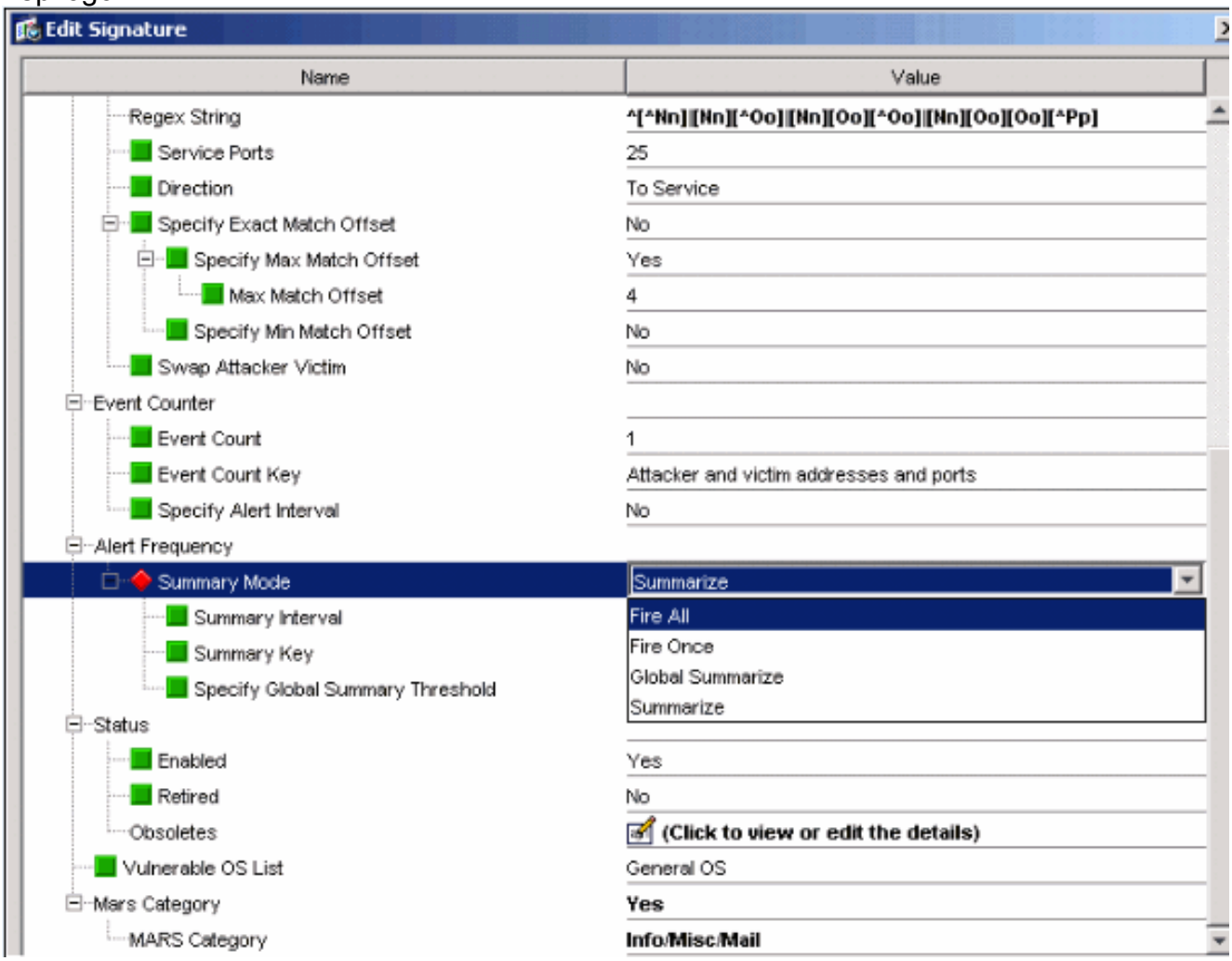
3. Scegliere **Configurazione > Criteri > Definizioni firma > sig0 > Configurazione firma > Seleziona per: Signature ID** per visualizzare tutte le firme disponibili nel sensore.



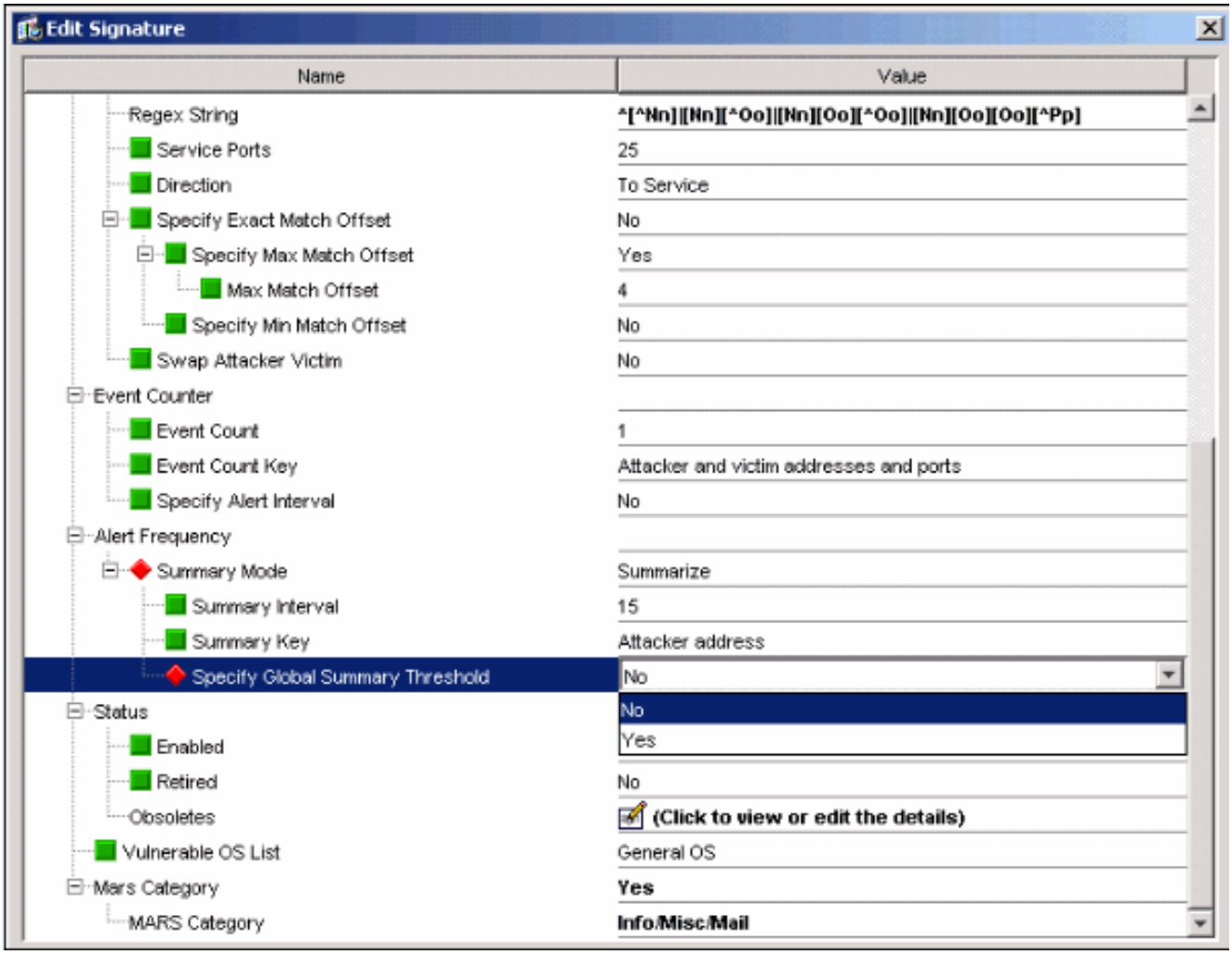
4. Scegliere **Signature ID** dal menu a discesa Seleziona per, quindi immettere Signature ID **5748** per trovare una firma specifica.



5. Per modificare la firma, fare clic su **Modifica**.
6. Nella finestra Modifica firma, scegliere **Definizione firma > Frequenza avviso > Modalità riepilogo**, quindi modificare l'azione da **Riepiloga** a **Attiva tutto** nel menu a discesa Modalità riepilogo.



7. Assicurarsi che l'opzione Specifica soglia di riepilogo globale sia impostata su **No**.



Informazioni correlate

- Pagina di supporto di Cisco Intrusion Prevention System
- Pagina di supporto di Cisco IPS Device Manager
- Guida introduttiva a IOS IPS
- Documentazione e supporto tecnico – Cisco Systems