

IPS 6.X: Enable/Disable the Summary of a Specific Event Using IDM

Document ID: 91527

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Enable/Disable the Summary of a Specific Event Using IDM

- IDM Configuration

Related Information

Introduction

This document describes how to enable/disable the summary of a specific event in Intrusion Prevention System (IPS) software version 6.x using the IPS Device Manager (IDM).

Note: Access lists must be configured in the IPS appliances in order to allow the access from the host or network where management software such as IDM and IEV (IDS Event Viewer) are installed and work properly. Refer to the Changing the Access List section of the Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.0 for more information.

Prerequisites

Requirements

This document is created with the assumption that IPS 6.x is installed and works properly.

Components Used

The information in this document is based on the Cisco 4200 Series IPS Sensor that runs software version 6.0(2)E1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Enable/Disable the Summary of a Specific Event Using IDM

For a clear understanding, this section provides an example in which you enable/disable the summary for the **Signature ID: 5748**.

IDM Configuration

Complete these steps.

1. Launch IDM.
2. Click **Home** in order to see the homepage of the IDM. This page shows the device information.

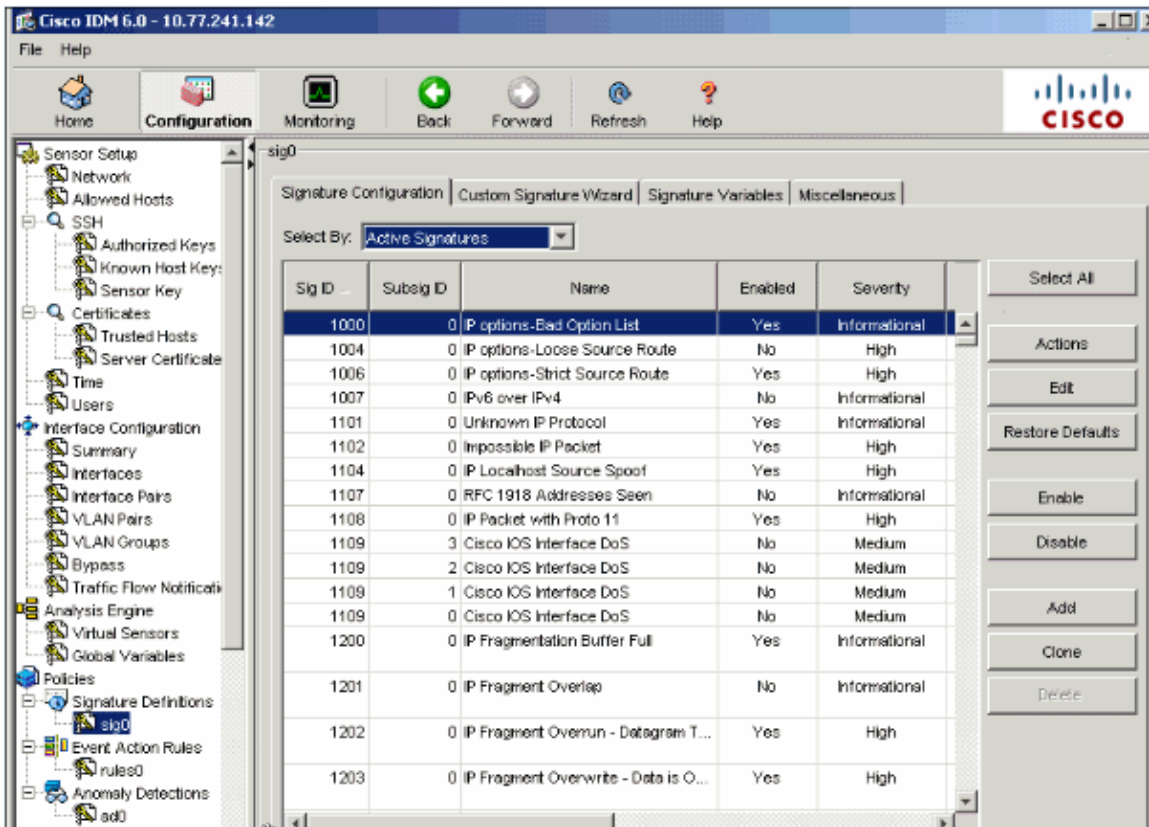
The screenshot displays the Cisco IDM 6.0 web interface. The browser title is "Cisco IDM 6.0 - 10.77.241.142". The interface includes a navigation bar with "Home", "Configuration", "Monitoring", "Back", "Forward", "Refresh", and "Help" buttons. The main content area is divided into several sections:

- Device Information:** Host Name: sensor, IP Address: 10.77.241.142, IPS Version: 6.0(2)E1, Device Type: IDS-4235, IDM Version: 6.0.2, Total Memory: 881 MB, Bypass Mode: Auto_off, Total Data Storage: 174.7 MB, Missed Packets Percentage: 0, Total Sensing Interface: 1.
- Interface Status:** A table showing interface status:

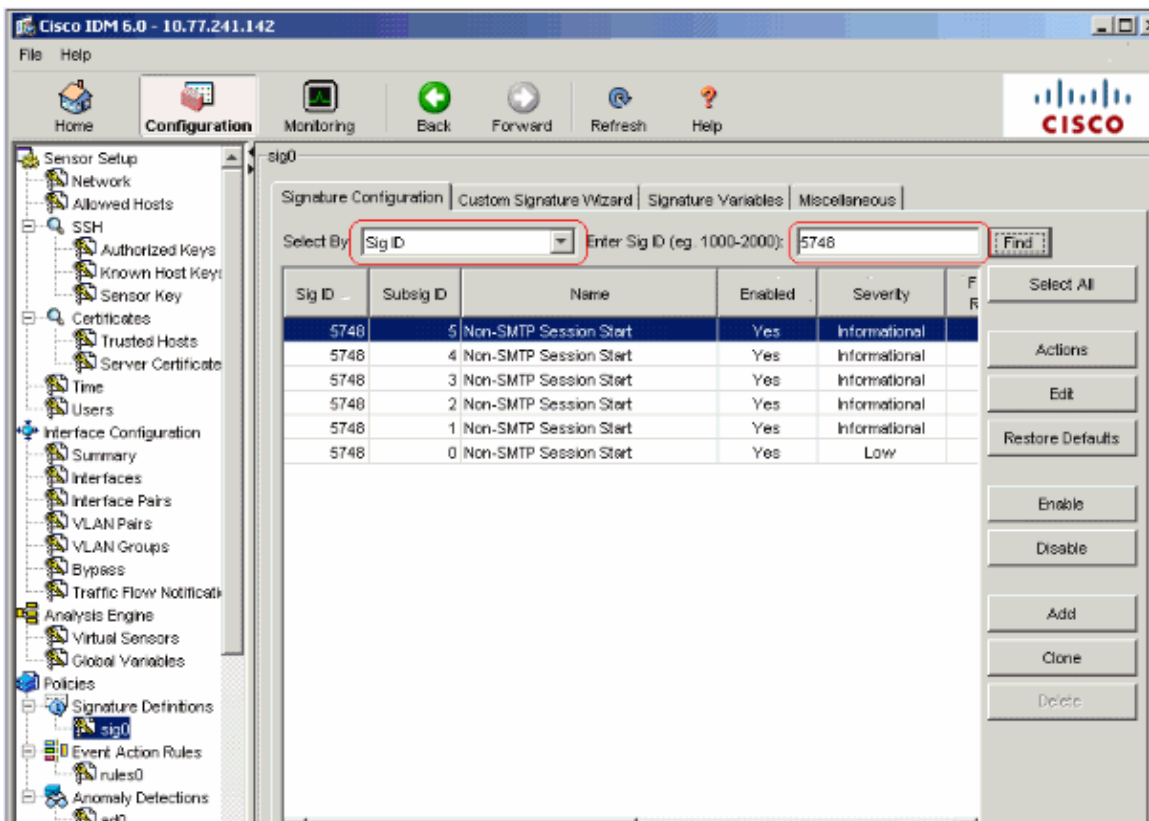
Interface	Link	Enabled	Speed	Mode
GigabitEthernet0/1	Up	Yes	Auto_100	Management
GigabitEthernet0/0	Down	Yes	N/A	Unpaired
- System Resources Status:** CPU usage is 0%. Memory usage is 74.7 MB. A line graph shows average CPU usage and memory usage over time.
- Alert Summary:** High (0), Med. (0), Low (0), Info. (0), Threat Rating > 80 (0).
- Alert Profile:** A line graph showing alert counts over time.

At the bottom, there is a "Refresh Page" button and a checkbox for "Auto refresh every 10 seconds".

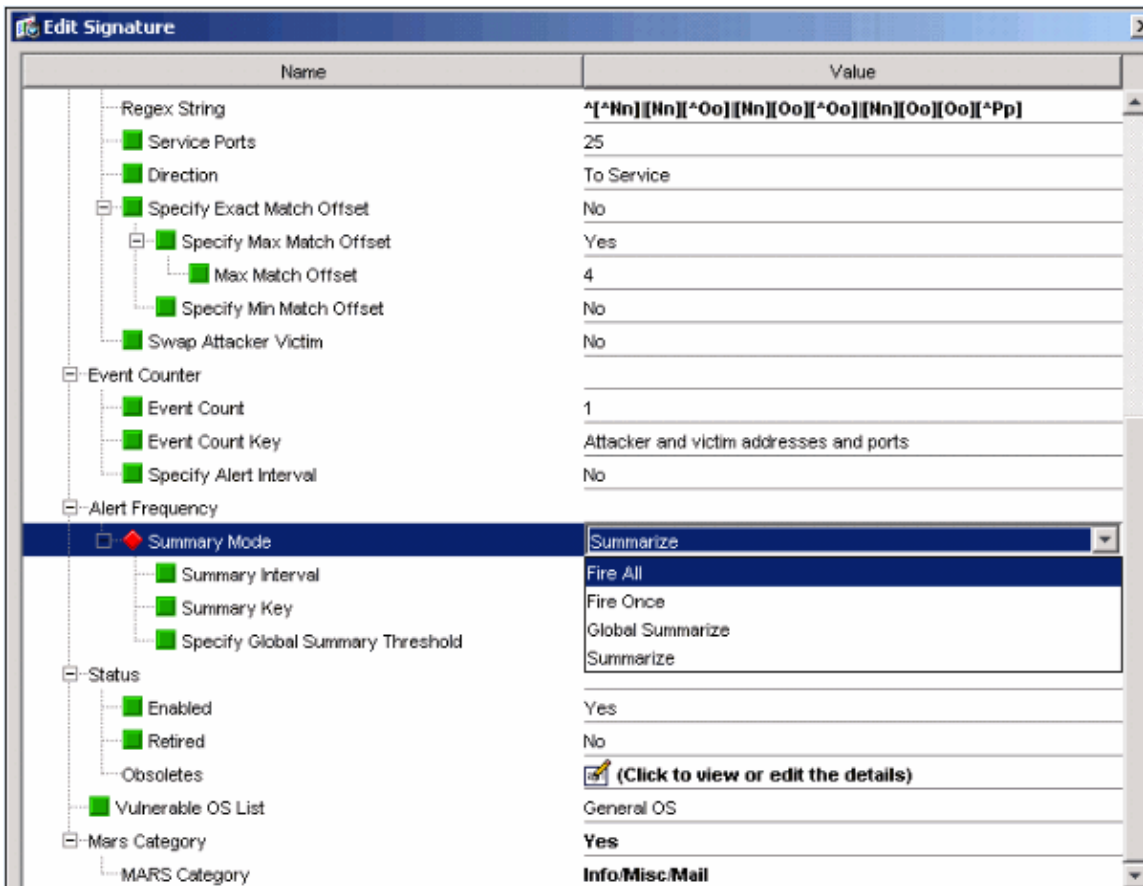
3. Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration > Select By: Sig ID** in order to display all the signatures available in the Sensor.



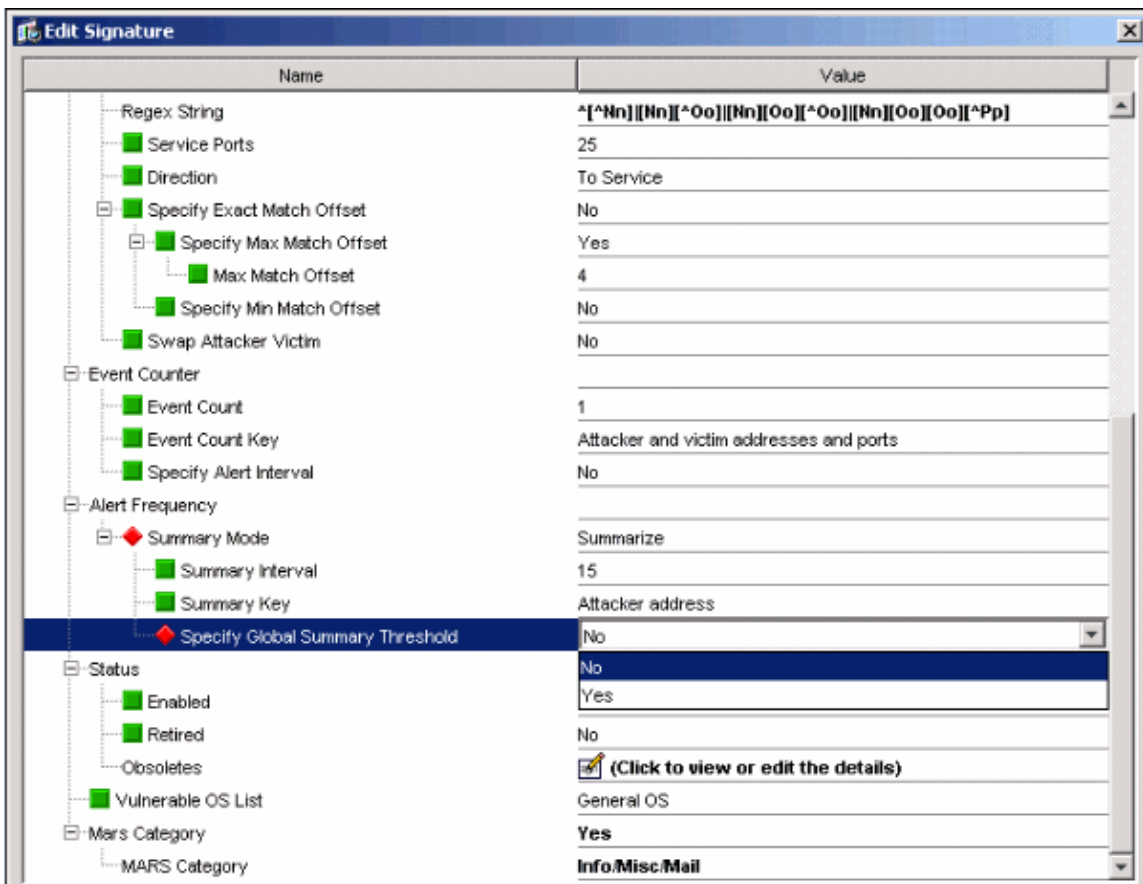
4. Choose **Sig ID** from the Select By drop-down menu and then enter Sig ID **5748** in order to find a specific signature.



5. Click **Edit** in order to edit the signature.
6. In the Edit Signature window, choose **Signature Definition > Alert Frequency > Summary Mode**, and change the action from **Summarize** to **Fire all** in the Summary Mode drop-down menu.



7. Make sure that Specify Global Summary Threshold is set to No.



Related Information

- [Cisco Intrusion Prevention System Support Page](#)
 - [Cisco IPS Device Manager Support Page](#)
 - [Getting Started with IOS IPS](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 31, 2007

Document ID: 91527
