

# Intrusion Prevention System Device Manager 5.1 – Tune Signature

Document ID: 91210

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Background Information

### Tune Signatures

Step-by-Step Procedure

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

Intrusion Prevention System (IPS) 5.1 contains over 1000 built-in default signatures. You cannot rename or delete signatures from the list of built-in signatures, but you can retire signatures to remove them from the sensing engine. You can later activate retired signatures. However, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic. You can tune built-in signatures when you adjust several signature parameters. Built-in signatures that have been modified are called *tuned signatures*.

This document illustrates the steps to use in order to tune the signature using the IPS Device Manager (IDM). IDM is a web-based, Java application that enables you to configure and manage your Sensor. The web server for IDM resides on the Sensor. You can access it through Internet Explorer, Netscape, or Mozilla web browsers.

**Note:** You can create signatures, which are called *custom signatures*. Custom signature IDs begin at 60000. You can configure them for several things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic that is monitored.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the Cisco Intrusion Prevention System Device Manager 5.x.

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.

## Background Information

In order to configure a Sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install the signature update. When an attack is detected that matches an enabled signature, the Sensor generates an alert, which is stored in the Sensor's event store. The alerts, as well as other events, can be retrieved from the event store by web-based clients. By default, the Sensor logs all informational alerts or higher.

Some signatures have sub-signatures. That is, the signature is divided into sub-categories. When you configure a sub-signature, changes made to the parameters of one sub-signature apply only to that sub-signature. For example, if you edit signature 3050 sub-signature 1 and change the severity, the severity change applies only to sub-signature 1 and not to 3050 2, 3050 3, and 3050 4.

## Tune Signatures

A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

A green icon indicates that the parameter currently uses the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

## Step-by-Step Procedure

Complete these steps in order to tune signatures:

1. Log in to IDM using an account with administrator or operator privileges.
2. Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

3. In order to locate a signature, choose a sorting option from the **Select By** list.

For example, if you search for a UDP Flood signature, choose **L2/L3/L4 Protocol** and then **UDP Floods**.

The Signature Configuration pane refreshes and displays only those signatures that match your sorting criteria.

4. In order to tune an existing signature, select the signature and complete these steps:

- a. Click **Edit** to open the Edit Signature dialog box.
- b. Review the parameter values and change the value of any parameter you want to tune.

**Note:** In order to choose more than one event action, hold down the **Ctrl** key.

- c. Under Status, choose **Yes** to enable the signature.

**Note:** The signature must be enabled for the Sensor to actively detect the attack specified by the signature.

d. Under Status, specify if this signature is retired. Click **No** to activate the signature. This places the signature in the engine.

**Note:** A signature must be activated for the Sensor to actively detect the attack specified by the signature.

**Note:** Click **Cancel** in order to undo your changes and close the Edit Signature dialog box.  
e. Click **OK**.

The edited signature now appears in the list with the Type set to Tuned.

**Note:** If you want to undo your changes, click **Reset**.

5. Click **Apply** to apply your changes and save the revised configuration.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [Cisco Intrusion Prevention System](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 19, 2007

Document ID: 91210

---