

# IPS 6: Включение/отключение сводки определенных событий с помощью IDM

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Включение/отключение сводки определенных событий с помощью IDM](#)

[Конфигурация IDM](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает как к позволить/запретить сводка определенного события в версии программного обеспечения 6.x Системы предотвращения вторжений (IPS) с помощью диспетчера устройств IPS (IDM).

**Примечание:** Списки доступа должны быть настроены в устройствах IPS для предоставления доступа от хоста или сети, где программное обеспечение для управления, такое как IDM и [IEV \(IDS Event Viewer\)](#) установлено и работает должным образом. См. [Изменение раздела Списка доступа Настройки Датчик системы предотвращения вторжений Cisco \(IPS\) Использование Интерфейса командной строки 5.0](#) для получения дополнительной информации.

## Предварительные условия

### Требования

Этот документ создан учитывая, что IPS 6.x установлен и работает должным образом.

### Используемые компоненты

Сведения в этом документе основываются на Cisco Сенсор IPS серии 4200, который работает под управлением ПО версии 6.0 (2) E1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Включение/отключение сводки определенных событий с помощью IDM

Для четкого представления этот раздел предоставляет пример в который вы позволить/запретить сводка для Идентификатора подписи: 5748.

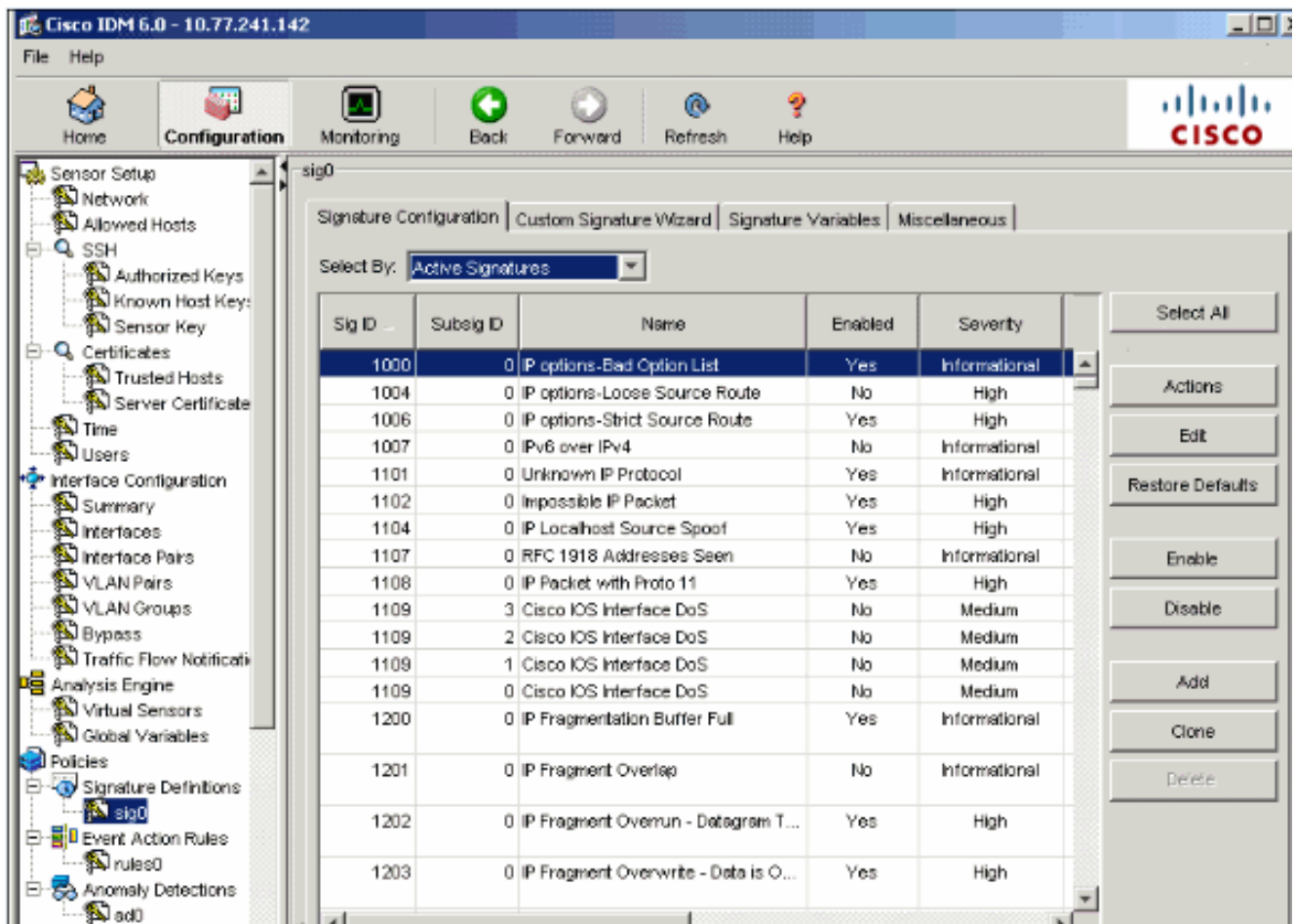
## Конфигурация IDM

Выполните следующие действия.

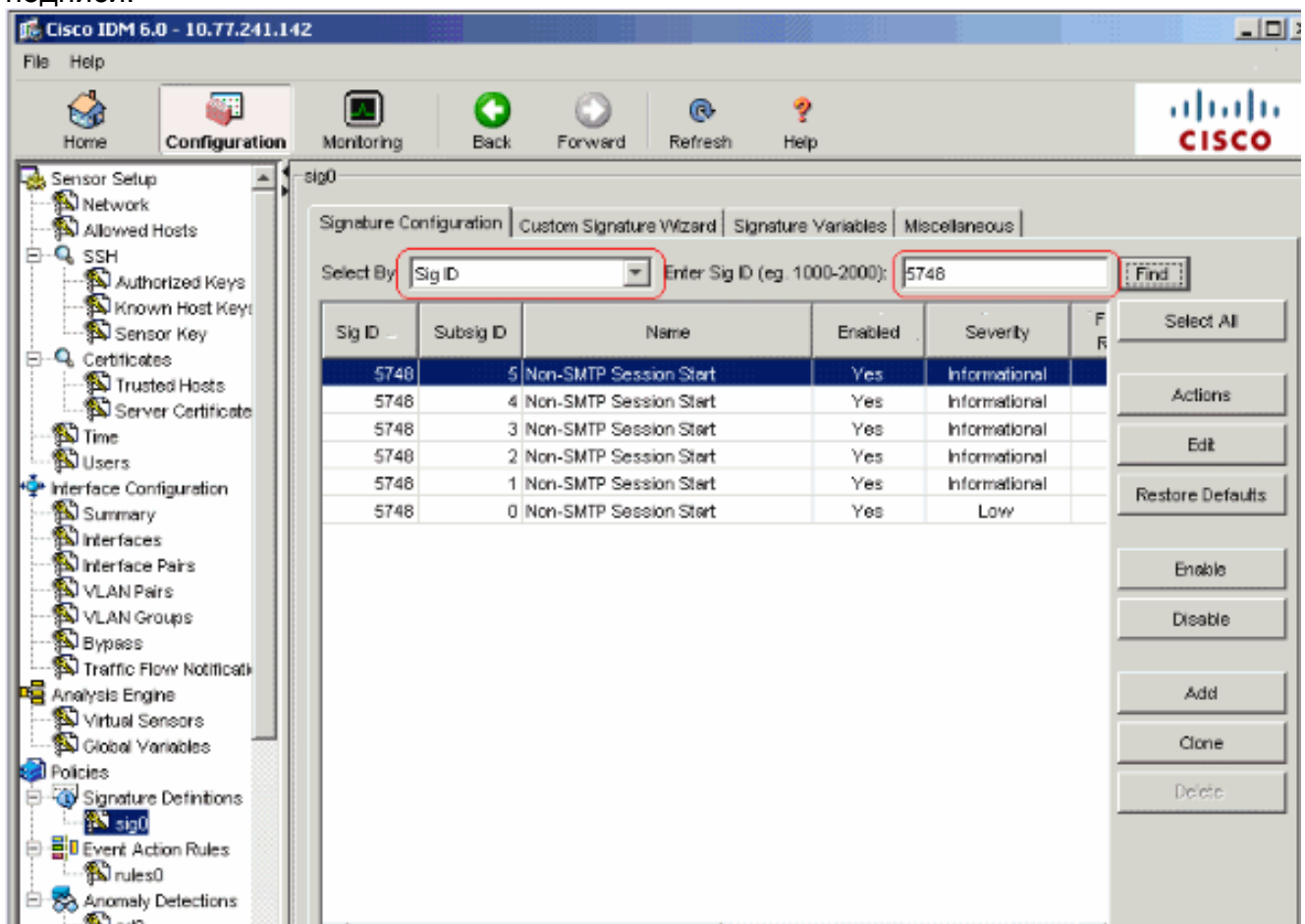
1. IDM запуска.
2. Нажмите **Home** для наблюдения домашней страницы IDM. Эта страница показывает сведения об устройстве.



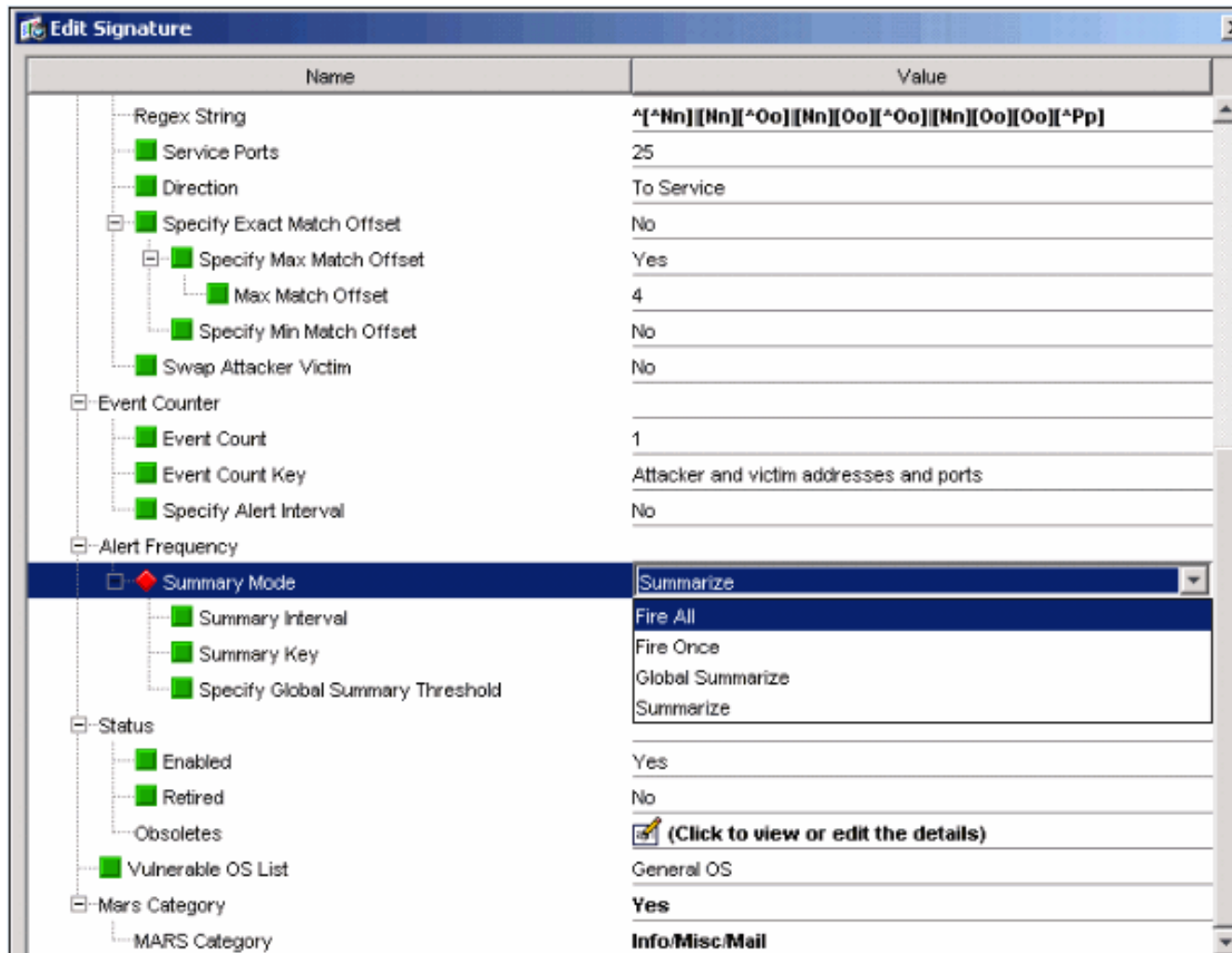
3. Выберите **Configuration> Policies> Signature Definitions> sig0>**, Конфигурация Подписи> Выбирает **By: ID Сигнала** для отображения всех подписей, доступных в Датчике.



4. Выберите Sig ID из Выбрать раскрывающегося меню Ву и затем введите ID 5748  
Сигнала для обнаружения определенной подписи.



5. Нажмите **Edit** для редактирования подписи.
6. В окне Edit Signature выберите **Signature Definition > Alert Frequency > Summary Mode** и измените действие от **Суммируют** для **Увольнения всех** в Итоговое раскрывающееся меню Режима.



7. Удостоверьтесь, что Указывают, что Глобальный Итоговый Порог установлен к **Нет**.

Name	Value
Regex String	*[^\n][\n][^\o][\o][^\o][\o][^\p][\p]
Service Ports	25
Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	Yes
Max Match Offset	4
Specify Min Match Offset	No
Swap Attacker Victim	No
Event Counter	
Event Count	1
Event Count Key	Attacker and victim addresses and ports
Specify Alert Interval	No
Alert Frequency	
Summary Mode	Summarize
Summary Interval	15
Summary Key	Attacker address
Specify Global Summary Threshold	No
Status	No
Enabled	Yes
Retired	No
Obsoletes	(Click to view or edit the details)
Vulnerable OS List	General OS
Mars Category	Yes
MARS Category	Info/Misc/Mail

## Дополнительные сведения

- [Страница технической поддержки системы предотвращения вторжений Cisco \(IPS\)](#)
- [Страница технической поддержки Cisco IPS Device Manager](#)
- [Начало работы с IPS IOS](#)
- [Cisco Systems – техническая поддержка и документация](#)