

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

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Aktivieren/Deaktivieren der Zusammenfassung eines bestimmten Ereignisses mit IDM](#)

[IDM-Konfiguration](#)

[Zugehörige Informationen](#)

## [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.

The screenshot shows the Cisco IDM 6.0 web interface. The top navigation bar includes 'Home', 'Configuration', 'Monitoring', 'Back', 'Forward', 'Refresh', and 'Help'. The left sidebar contains a tree view with categories like 'Sensor Setup', 'Interface Configuration', 'Policies', and 'Signature Definitions'. The main content area is titled 'sig0' and shows the 'Signature Configuration' page. A dropdown menu is set to 'Active Signatures'. Below it is a table of signatures:

Sig ID	Subsig ID	Name	Enabled	Severity
1000	0	IP options-Bad Option List	Yes	Informational
1004	0	IP options-Loose Source Route	No	High
1006	0	IP options-Strict Source Route	Yes	High
1007	0	IPv6 over IPv4	No	Informational
1101	0	Unknown IP Protocol	Yes	Informational
1102	0	Impossible IP Packet	Yes	High
1104	0	IP Localhost Source Spoof	Yes	High
1107	0	RFC 1918 Addresses Seen	No	Informational
1108	0	IP Packet with Proto 11	Yes	High
1109	3	Cisco IOS Interface DoS	No	Medium
1109	2	Cisco IOS Interface DoS	No	Medium
1109	1	Cisco IOS Interface DoS	No	Medium
1109	0	Cisco IOS Interface DoS	No	Medium
1200	0	IP Fragmentation Buffer Full	Yes	Informational
1201	0	IP Fragment Overlap	No	Informational
1202	0	IP Fragment Overrun - Datagram T...	Yes	High
1203	0	IP Fragment Overwrite - Data is O...	Yes	High

On the right side of the table, there are several action buttons: 'Select All', 'Actions', 'Edit', 'Restore Defaults', 'Enable', 'Disable', 'Add', 'Clone', and 'Delete'.

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.

The screenshot shows the Cisco IDM 6.0 configuration interface. The main window is titled 'Signature Configuration' and is set to 'Custom Signature Wizard'. The 'Select By' dropdown is set to 'Sig ID', and the 'Enter Sig ID (eg. 1000-2000):' field contains '5748'. A table lists the following signature entries:

Sig ID	Subsig ID	Name	Enabled	Severity	F R
5748	5	Non-SMTP Session Start	Yes	Informational	
5748	4	Non-SMTP Session Start	Yes	Informational	
5748	3	Non-SMTP Session Start	Yes	Informational	
5748	2	Non-SMTP Session Start	Yes	Informational	
5748	1	Non-SMTP Session Start	Yes	Informational	
5748	0	Non-SMTP Session Start	Yes	Low	

On the right side of the table, there are several action buttons: 'Select All', 'Actions', 'Edit', 'Restore Defaults', 'Enable', 'Disable', 'Add', 'Clone', and 'Delete'.

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**.

Name	Value
Regex String	<code>^[^Nn][Nn][^Oo][Oo][^Pp]</code>
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	Fire All
Summary Key	Fire Once
Specify Global Summary Threshold	Global Summarize
Status	Summarize
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

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

Name	Value
Regex String	<code>^[^Nn][Nn][^Oo][Oo][Nn][Oo][^Oo][Nn][Oo][Oo][^Pp]</code>
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

## 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](#)