



# Cisco IOS IPS Support for Microsoft Engines

---

**First Published: June 28, 2007**

**Last Updated: June 28, 2007**

The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IOS Intrusion Prevention Systems (IPS) to support Microsoft RPC (Remote Procedure Call) and Microsoft SMB (Server Message Block) protocols. IPS signatures can now scan for, detect, and take proper action against vulnerabilities in MSRPC and SMB protocols.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Cisco IOS IPS Support for Microsoft Engines” section on page 7](#).

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Information About Cisco IOS IPS Support for Microsoft Engines, page 2](#)
- [How to Use Cisco IOS IPS, page 2](#)
- [Configuration Examples for Cisco IOS IPS, page 2](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for Cisco IOS IPS Support for Microsoft Engines, page 7](#)



---

Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

# Information About Cisco IOS IPS Support for Microsoft Engines

Before using IPS, you should understand the following concept:

- [Cisco IOS IPS Overview, page 2](#)

## Cisco IOS IPS Overview

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured via CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

## How to Use Cisco IOS IPS

The addition of the MSRPC and MSB protocol support does not change the way in which Cisco IOS IPS is defined and enabled in your network. For information on how to enable IPS on your network via command-line interface (CLI), see the section “[How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS](#)” within the document *Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements*.

## Configuration Examples for Cisco IOS IPS

This section contains the following example:

- [show ip ips signature Output to Verify MS Engines:Example, page 3](#)

## show ip ips signature Output to Verify MS Engines:Example

The following sample output from the **show ip ips signature** command displays output for the service-msrpc and service-smb-advanced signatures:

```
Signature Micro-Engine: service-msrpc: Total Signatures 21
service-msrpc enabled signatures: 21
service-msrpc compiled signatures: 21
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
-----
3330:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S148
3332:0 Y Y A HIGH 0 35 0 0 0 FA N 100 S148
3337:0 Y Y A HIGH 0 8 2 0 0 FA N 100 S85
3331:2 Y Y A HIGH 0 1 0 0 0 FA N 90 S215
3327:12 Y Y A HIGH 0 1 0 0 0 FA N 85 S214
3328:3 Y Y A MED 0 1 0 0 0 FA N 85 S170
3328:1 Y Y A MED 0 1 0 0 0 FA N 85 S148
3327:8 Y Y A INFO 0 1 0 0 0 FA N 85 S214
3334:6 Y Y A HIGH 0 1 0 0 0 FA N 80 S215
3327:0 Y Y A HIGH 0 1 0 0 0 FA N 80 S165
6232:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S209
3327:4 Y Y A HIGH 0 1 0 0 0 FA N 75 S188
3334:5 Y Y A HIGH 0 2 2 0 0 FA N 75 S179
3338:2 Y Y A HIGH 0 40 3 0 0 FA N 75 S175
3338:3 Y Y A HIGH 0 1 0 0 0 FA N 75 S175
6130:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S167
6130:6 Y Y A INFO 0 1 0 0 0 FA N 75 S192
5567:1 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:2 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:3 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:4 Y Y A INFO 0 1 0 0 0 FA N 55 S187

Signature Micro-Engine: service-smb-advanced: Total Signatures 31
service-smb-advanced enabled signatures: 31
service-smb-advanced compiled signatures: 31
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
-----
5593:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5592:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5582:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5599:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5595:0 Y Y A MED 0 1 0 0 0 FA N 100 S262
5579:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5581:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5580:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5584:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5576:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5577:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5583:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5591:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5590:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5598:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S264
5588:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5586:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5585:0 Y Y A MED 0 1 0 0 0 FA N 85 S264
5579:1 Y Y A MED 0 1 0 0 0 FA N 85 S264
5602:0 Y Y A MED 0 1 0 0 0 FA N 85 S262
5589:0 Y Y A LOW 0 1 0 0 0 FA N 85 S262
5578:0 Y Y A INFO 0 1 0 0 0 FA N 85 S264
5605:0 Y Y A INFO 0 1 0 0 0 FA N 85 S262
5600:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5597:0 Y Y A HIGH 0 50 0 0 0 FA N 75 S262
5594:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
```

```

5587:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5603:0 Y Y A MED 0 1 0 0 0 FA N 75 S262
5591:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5575:0 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5590:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262

```

## Additional References

The following sections provide references related to the Cisco IOS IPS Support for Microsoft Engines feature.

## Related Documents

| Related Topic                                  | Document Title                                                                                                                     |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS IPS configuration tasks and commands | <a href="#">Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements</a> , Cisco IOS Release 12.4(11)T feature module |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

This section documents only commands modified.

- [debug ip ips](#)

# debug ip ips

To enable debugging messages for Cisco IOS Intrusion Prevention System (IPS), use the **debug ip ips** command in privileged EXEC mode. To disable debugging messages, use the **no** form of this command.

**debug ip ips** [*engine*] [**detailed**] [**service-msrpc**] [**service-sm**]

**no debug ip ips** [*engine*] [**detailed**]

## Syntax Description

|                      |                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------|
| <i>engine</i>        | (Optional) Displays debugging messages only for a specific signature engine.                               |
| <b>detailed</b>      | (Optional) Displays detailed debugging messages for the specified signature engine or for all IPS actions. |
| <b>service-msrpc</b> | (Optional) Displays debugging messages for Microsoft RPC (Remote Procedure Call) (MSRPC) actions.          |
| <b>service-sm</b>    | (Optional) Displays debugging messages for Microsoft SMB(Server Message Block) actions.                    |

## Command Modes

Privileged EXEC

## Command History

| Release   | Modification                                                                                                                       |
|-----------|------------------------------------------------------------------------------------------------------------------------------------|
| 12.3(8)T  | This command was introduced.                                                                                                       |
| 12.4(15)T | The <b>service-msrpc</b> and the <b>service-sm</b> keywords were added to support Microsoft communication protocols MSRPC and SMB. |

## Examples

The following example shows how to enable debugging messages for the Cisco IOS IPS:

```
Router# debug ip ips
```

# Feature Information for Cisco IOS IPS Support for Microsoft Engines

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Cisco IOS IPS Support for Microsoft Engines

| Feature Name                                | Releases  | Feature Information                                                                                           |
|---------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------|
| Cisco IOS IPS Support for Microsoft Engines | 12.4(15)T | The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IPS to support MSRPC and SMB protocols. |

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

