

# Table of Contents

<b><u>Cisco Secure IDS Version 3.1 and Earlier Raw Log Files</u></b> .....	1
<u>Document ID: 15253</u> .....	1
<u>Cisco has announced the end-of-sales for the Cisco Secure IDS Director and the end-of-sales and end-of-life for Cisco IDS 3.x Sensor Software.</u> .....	1
<u>Introduction</u> .....	1
<u>Prerequisites</u> .....	1
<u>Requirements</u> .....	1
<u>Components Used</u> .....	1
<u>Conventions</u> .....	2
<u>Sample Event Log File</u> .....	2
<u>NetPro Discussion Forums – Featured Conversations</u> .....	4
<u>Related Information</u> .....	5

# Cisco Secure IDS Version 3.1 and Earlier Raw Log Files

Document ID: 15253

---

**Cisco has announced the end-of-sales for the Cisco Secure IDS Director and the end-of-sales and end-of-life for Cisco IDS 3.x Sensor Software.**

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Sample Event Log File**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

Cisco Secure IDS provides four levels of logging: events, errors, commands, and sessions. All event, error, command, and session log data is stored in a common, comma-delimited, flat file that can be imported into any database. Level 1 and higher events are logged on the Sensor, and Level 2 through 5 events are forwarded to the log file on the Director. The active Cisco Secure IDS log file on the Sensor and the Director is located in /usr/nr/var and is named log.YYYYMMDDHHMM. When the active log file reaches 300 KB, or after 240 minutes have elapsed (whichever comes first), the active log file is closed and archived, and a new active log file is created. You can change the size or time limit of the active log file. Refer to Cisco IDS Director for UNIX Configuration and Operations Guide Version 2.2.3, Configuration Management, Data Management for details. Archived log files are stored in /usr/nr/var/new.

The format of the log file is documented in Cisco IDS Director for UNIX Configuration and Operations Guide Version 2.2.3, Data and File Management.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- IDS Sensors running software version 3.1 or earlier.
- IDS UNIX Director running software version 2.2.3 or earlier.

**Note:** Version 2.3.3 is the last release of IDS Director software. This release supports Cisco IDS Sensors running versions 3.x and earlier.

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Sample Event Log File

A sample event log file entry is provided here. An explanation of each field is displayed in the table after the log entry.

```
4,1028109,1998/12/23,22:07:00,1998/12/23,16:07:00,10008,5,100,
OUT,IN, 5,8000, 51304,TCP/IP, 131.215.210.2,207.18.164.70,1034,21,
0.0.0.0, hacked in, 75736 ? EOD0A
```

Data	Field	Comments
4	Record type	The numbers correspond to the logging levels: 2 is error, 3 is command, 4 is events or alarms, and 5 is IP (or sessions).
1028109	Record number	Begins at 1,000,000. Each time the sensor/packetd process is started, the record number is incremented by one.
1998/12/23	Greenwich Mean Time (GMT) date	
22:07:00	GMT	
1998/12/23	Local date	
16:07:00	Local time	
10008	The application ID of the process that generated the log record. 10008 is the packetd service.	The /usr/nr/etc/services file on both the Directors and Sensors provides the mapping of application IDs
5	Host ID of the Sensor or Director that generated the log record.	to Cisco Secure IDS services. The user assigns the host ID during system initialization (that is, through sysconfig-sensor). A mapping of the host ID to host names is provided

		in the /usr/nr/etc/hosts file on both the Directors and Sensors.
100	Organization ID of the Sensor or Director that generated the log record.	The user assigns the organization ID during system initialization. A mapping of the organization ID to organization names is provided in the /usr/nr/etc/organizations file on the Directors and Sensors.
OUT	Event source location	The location is either inside or outside of the defined protected networks.
IN	Event destination location	The location is either inside or outside of the defined protected networks.
5	Alarm level	By default Cisco Secure IDS has five alarm levels. The user can configure up to 255 levels.
8000	Signature ID	A mapping of signature IDs to signature names is provided in the /usr/nr/etc/signatures file on the Directors and Sensors. Signature IDs range from 1000 to 10,000.
51304	Sub-signature ID	This ID is primarily found with string match signatures, which are user-customizable. String match sub-signature names can be found in the optional event detail field. In this example, the string "hacked in" triggered the logging of this event. For signatures that do not have sub-signatures, this field is "0." Sub-signature IDs are assigned by the system and user-defined string match signatures start with sub-signature ID 51304.

TCP/IP	Indicates IP traffic	IP traffic is the only traffic supported at this time.
31.215.210.2	Source IP address that triggered the event.	
207.18.164.70	Destination IP address of the triggered event.	
1034	Source port	
21	Destination port	
0.0.0.0	External data source IP address	IP address of the network device that detected the event when external data sources are used (for example, ACL syslog from a router). 0.0.0.0 signifies that the Sensor specified by the recorded host and organization ID detected this event.
hacked in	Optional event detail	This field is not always populated. In this example, the string "hacked in" triggered the logging of this event.
75736 ? E0D0A	Optional context data	This field is not always populated. In this example, it provides a snapshot of incoming and outgoing binary TCP traffic up to a maximum of 256 bytes in both directions that proceed the trigger of the signature.

## 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 IDS Sensor Software Product Support Information**
  - **Cisco Intrusion Detection System Technical Documentation**
  - **End-of-Sale for the Cisco IDS Director**
  - **End-of-Life for Cisco IDS Sensor Software Version 3.x**
  - **Technical Support – Cisco Systems**
- 

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jun 27, 2005

Document ID: 15253

---