

# **HP-UX Host Intrusion Detection System Release 3.0 Release Notes**

**HP-UX 11i v2, 11i v1.6, and 11i v1**



**Manufacturing Part Number : J5083-90015**

**November 2004**

Printed in U.S.A

© Copyright 2004 Hewlett-Packard Development Company L.P.

---

## Legal Notices

The information in this document is subject to change without notice.

*Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.* Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Please read the Hewlett-Packard Software Product License Agreement and Limited Warranty, printed in Appendix A, "HP Software License," on page 33, before operating this product. Rights in the software are offered only on the condition that the customer accepts all terms and conditions of the License Agreement.

Operating the product indicates your acceptance of these terms and conditions. If you do not agree to the License Agreement, you may return the unused product for a full refund.

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

You are solely responsible for securing your system and for implementing security policies and procedures. This product is not a replacement for comprehensive security policies and procedures.

The product is a detection system. The product does not prevent the onset of attacks. If your system is vulnerable to attacks, those vulnerabilities will remain even after the product is installed. The product does not find static security flaws on a system or authenticate users of a valid account.

Use of this document and any supporting software media (CD-ROMs, flexible disk, and tape cartridges) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

### Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

### U.S. Government License

Proprietary computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Trademarks

UNIX® is a registered trademark of The Open Group.

Java™ is a US trademark of Sun Microsystems, Inc.

MS-DOS® and Microsoft® are U.S. registered trademarks of Microsoft Corporation.

OSF/Motif™ is a trademark of The Open Group.

X Window System™ is a trademark of The Open Group.

---

## Revision History

This document's printing date and part number indicate its edition. The printing date changes when a new edition is printed. (Minor corrections and updates which are incorporated at reprint do not cause the date to change.) New editions of this manual incorporate all material updated since the previous edition.

J5083-90015	November 2004. Software release 3.0.
J5083-90012	September 2003. Software release 2.2.
J5083-90008	June 2002. Software release 2.1.
J5083-90006	December 2001. Software release 2.0.
J5083-90004	March 2001. Software release 1.0. Revised.
J5083-90002	July 2000. Software release 1.0.

---

## Conventions

We use the following typographical conventions.

<i>audit</i> (5)	An HP-UX manpage. <i>audit</i> is the name and <i>5</i> is the section in the <i>HP-UX Reference</i> . On the web and on the Instant Information CD, it may be a hot link to the manpage itself. From the HP-UX command line, you can enter “man audit” or “man 5 audit” to view the manpage. See <i>man</i> (1).
<i>Book Title</i>	The title of a book. On the web and on the Instant Information CD, it may be a hot link to the book itself.
<b>KeyCap</b>	The name of a keyboard key. Note that <b>Return</b> and <b>Enter</b> both refer to the same key.
<i>Emphasis</i>	Text that is emphasized.
<b>Emphasis</b>	Text that is strongly emphasized.
<b>Term</b>	The defined use of an important word or phrase.
ComputerOutput	Text displayed by the computer.
<b>User Input</b>	Commands and other text that you type.
Command	A command name or qualified command phrase.
<i>Variable</i>	The name of a variable that you may replace in a command or function or information in a display that represents several possible values.
[ ]	The contents are optional in formats and command descriptions. If the contents are a list separated by  , you may choose one of the items.
{ }	The contents are required in formats and command descriptions. If the contents are a list separated by  , you must choose one of the items.
...	The preceding element may be repeated an arbitrary number of times.
	Separates items in a list of choices.

**1. Announcement**

New and Changed Features .....	2
What's New in Release 3.0 .....	2
Compatibility with Previous Releases .....	2
Compatibility with Other Products .....	3
Localization .....	3
What Is HP-UX HIDS? .....	4
Benefits .....	5
Standard Surveillance Groups and Schedules .....	5
Documentation .....	6
Manuals .....	6
Manpages .....	6
HP OpenView SMART Plug-In .....	6
IDS Mailing List .....	7
ITRC Security Forum .....	7
Support Model .....	7
Known Problems, Limitations, and Fixes .....	8
Clarifications .....	8
Known Problems .....	8
Limitations .....	9
Fixes and Enhancements in Release 3.0 .....	10

**2. Installation**

Introduction .....	14
Installation Summary .....	16
Hardware and Software Requirements .....	17
Administration and Agent Systems .....	17
Administration System .....	17
Agent Systems .....	17
Dual System .....	17
When Updating from Release 2.x .....	18
Pre-Installation .....	19
Making Depots .....	20
Create the Depot Directory .....	20
Get Patches for HP-UX 11i v1 .....	20
Get the HP-UX HIDS Product .....	23
Get Patches for Java .....	25
Get the Java Software .....	25
Installing OpenSSL .....	26
Installing the Depots .....	28
Will Installing HP-UX HIDS Release 3.0 Reboot My Agent System? .....	29
Post-Installation .....	30
Updating from Release 2.x .....	30
Configuration .....	32
Required .....	32
Optional .....	32

---

# Contents

## A. HP Software License

Attention.....	34
LICENSE ISSUES .....	34
OpenSSL License .....	34
Original SSLeay License .....	35
HP Software License Terms .....	37

---

# **1**      **Announcement**

The HP-UX Host Intrusion Detection System Release 3.0 Release Notes describes the new features, fixes, limitations, and known issues in the HP-UX Host Intrusion Detection System (HP-UX HIDS) Release 3.0. HP-UX HIDS Release 3.0 is a major product release, which provides improved product performance and incorporates several usability enhancements.

## New and Changed Features

HP-UX HIDS Release 3.0 runs on HP-UX 11i v2, 11i v1.6, and 11i v1. It is available in the installation bundles for HP-UX 11i v2, in the Operating Environment bundles for HP-UX 11i v1, in the Application Releases, and from the HP Software Depot. In this document, “11i” unqualified encompasses all the supported 11i versions.

### What’s New in Release 3.0

- Significant reduction in CPU consumption and better performance throughput by the HIDS idscor correlator process.
- Template consolidation and property changes. Prior to this version the "Monitor Logins/Logouts" template and the "Monitor Start of Interactive Sessions" template has provided overlapping functionality. The overlapping facility has been rectified and the two templates have been consolidated into one template called Monitoring Logins/Logouts.
- A number of new template properties to allow better filtering of unwanted alerts.
- Further fine tuning of default template settings for "out of the box" configurations to reduce the alert volume generated.
- A supported command-line interface tool (`idsadmin`) for end users who wish to automate their HIDS deployment and management processes.
- More descriptive alerts to assist in developing more comprehensive filtering within template properties.
- New conversion utilities to migrate v2.x customizations to the new v3.0 template format to preserve existing deployment efforts.
- Use of OpenSSL for securing agent-admin communication. As a result, HIDS has a new dependency on the OpenSSL product available in HP-UX OEs (as well as at <http://software.hp.com>). The main benefit is that any SSL-related vulnerability fixes can be made readily available to HIDS customers without the need for a new release of HIDS.
- The HP-UX HIDS bundle has been split into two products (IDS and IDS-KERN) to reduce the likelihood of a system reboot for future HIDS updates.

### Compatibility with Previous Releases

HP-UX HIDS software Release 3.0 is not backward compatible with Release 2.0, 2.1, 2.2 (collectively referred to as 2.x henceforth) and 1.0. Specifically, HIDS Release 3.0 agents and GUI cannot communicate with 2.x and 1.0 GUI and agents. This means that 2.x and 1.0 agents cannot be managed by the 3.0 system manager GUI, and *vice versa*. Release 2.x communication keys and certificates are recognized and valid in Release 3.0 and new keys and certificates need not be generated after migrating to Release 3.0.

The templates in v3.0 differ significantly from v2.x. In order to use existing V2.x schedules, you must use the `guiSchedConvert` migration tool (see “The `guiSchedConvert` Migration Tool” on page 30) to convert schedule files used by the

System Manager and the `adminSchedConvert` migration tool (see “The `adminSchedConvert` Migration Tool” on page 31) to convert text schedule files used by the `idsadmin` command..

HP recommends that you upgrade all systems to Release 3.0.

---

**NOTE**

You cannot directly migrate HP-UX HIDS Release 1.0 schedules to HP-UX HIDS Release 3.0 schedules. You must first migrate to HP-UX HIDS Release 2.2 schedules and then migrate to HP-UX HIDS Release 3.0 schedules.

---

## Compatibility with Other Products

HP-UX HIDS is not compatible with all HP software products, as listed in Table 1-1. Do not run HP-UX HIDS on systems that are running unsupported products (or vice versa).

**Table 1-1 HP-UX HIDS Product Compatibility**

Product	Supported?
HP-UX 11i v2	Yes
HP-UX 11i v1.6	Yes
HP-UX 11i v1.5	No
HP-UX 11i v1	Yes
HP-UX 11.0	No
HP-UX 10.26	No
HP-UX 10.x	No
NIS, NIS+	Yes
OpenView	Yes
ServiceGuard	Not tested
Third-party EMS	Not tested
Trusted Mode operation	Yes
Virtual Vault	No

## Localization

The HP-UX HIDS software and documentation are *not* localized in non-English languages.

## What Is HP-UX HIDS?

HP-UX HIDS is a host-based HP-UX security product for HP computers running HP-UX 11i. HP-UX HIDS enables security administrators to proactively monitor, detect, and respond to attacks targeted at specific hosts. Since there are many types of attacks that can bypass network-based detection systems, HP-UX HIDS complements existing network-based security mechanisms, bolstering enterprise security.

HP-UX HIDS seeks out patterns that might suggest security breaches or misuses by examining information about system activity from a variety of data sources. Such illicit activities might include, for example, an intruder attempting to break into or disrupt your system, subversive “insider” activities, or someone trying to spread a virus. Once HP-UX HIDS has been activated for a given host system, and it detects an intrusion attempt, it issues an alert to the administrative interface where you can immediately investigate the situation, and when necessary, take action against the intrusion. In addition, you can customize a local response to an alert using one of the sample programs described in Appendix B, “Response Programs”, of the *HP-UX Host Intrusion Detection System Administrator's Guide* or a program you write yourself.

HP-UX HIDS is particularly useful for enterprise environments where centralized management tools control networks of heterogeneous systems. These environments include, for example, web servers, transaction processors, application servers, and database systems.

## Benefits

- HP-UX HIDS is an HP-UX intrusion detection product that can enhance local host-level security within your network. It does this by automatically monitoring each configured host system within the network for possible signs of unwanted and potentially damaging intrusions. If successful, such intrusions can lead to the loss of availability of key systems or compromise system integrity.
- HP-UX HIDS provides continuous surveillance against inappropriate system usage that is characteristic of hacker break-in attempts, subversive inside activities, and viruses.
- HP-UX HIDS is a perfect complement to network-based security solutions, and as such, can bolster the overall security of the computing infrastructure. HP-UX HIDS is designed to detect intrusions that network-based offerings cannot identify, thereby bolstering the integrity of the host system as the last line of defense.
- As HP-UX HIDS continuously examines ongoing activity on a system, it seeks out patterns that might suggest security breaches or misuses. The types of threats which HP-UX HIDS monitors include the following:

<b>System Critical</b>	Unauthorized access Privilege violations Trojan horse “Root” exploits
<b>HP-UX OS</b>	Race condition Buffer overflow Password guessing
<b>User security</b>	Failed logins Failed SU attempts User A modifying User B’s file
<b>Files</b>	Modification of critical system files and directories Creation of world writable files Creation of setuid files Critical file creation and deletion

- HP-UX HIDS can provide immediate notification in the event of suspicious activity that might *precede* an attack.

## Standard Surveillance Groups and Schedules

HP-UX HIDS provides a set of (read-only) standard (preconfigured) surveillance groups and schedules that will appear when you start the HP-UX HIDS System Manager. You can use them directly or as basis for the development of your own customized schedules and groups.

---

## Documentation

HP-UX HIDS documentation includes Manuals, Manpages, information on the HP OpenView SMART Plug-In, an IDS Mailing List, and the ITRC Security Forum.

### Manuals

The following documents are available at the HP Technical Documentation website in the Internet and Security Solutions collection, <http://docs.hp.com/hpux/internet>, and on the Instant Information CD in the Internet and Security Solutions collection.

HP Part No.	Title
J5083-90015	<i>HP-UX Host Intrusion Detection System Release 3.0. Release Notes</i> (the document you are reading now)
J5083-90013	<i>HP-UX Host Intrusion Detection System Administrator's Guide, Software Release 3.0.</i>

### Manpages

After installation, you can access the following manpages online using the `man` command. Before accessing these manpages, add `/opt/ids/share/man` to your `MANPATH` environment variable as follows:

```
export MANPATH=/opt/ids/share/man:$MANPATH
```

Directory	Manpages
<code>/opt/ids/share/man/man1m</code>	<i>IDS_checkAdminCert</i> (1M) <i>IDS_checkAgentCert</i> (1M) <i>IDS_checkInstall</i> (1M) <i>IDS_genAdminKeys</i> (1M) <i>IDS_genAgentCerts</i> (1M) <i>IDS_importAgentKeys</i> (1M) <i>idsadmin</i> (1M) <i>idsagent</i> (1M) <i>idsgui</i> (1M)
<code>/opt/ids/share/man/man5</code>	<i>ids.cf</i> (5)

### HP OpenView SMART Plug-In

The following document is available at the HP OpenView web site in the SPI Gallery at <http://openview.hp.com/products/spi/index.html>.

HP Part No.	Title
(none)	<i>HP OpenView Operations SMART Plug-In for HP-UX HIDS</i>

## IDS Mailing List

To receive the latest news about HP-UX HIDS, send an e-mail message to `majordomo@hpuxmail.cup.hp.com`. The body of the message should contain only:

`subscribe ids9000-news`

This address is for subscription requests only; do not send product questions or other inquiries.

To unsubscribe, send the message:

`unsubscribe ids9000-news`

## ITRC Security Forum

Get help from your peers in the HP Information Technology Resource Center (ITRC) security forum. It is on the web at

`http://forums.itrc.hp.com/cm`

From there, select the `hp-ux` area and then the `security` category.

## Support Model

In the future, HP-UX HIDS customers can expect to receive maintenance/minor versions of HP-UX HIDS, instead of individual patches for various defect fixes. HP recommends customers to adopt the latest version to take advantage of defect fixes (for a maintenance/minor release) and new functionality (for a major release).

The support model, in light of this approach (product versioning instead of individual patches), is as follows: The latest maintenance/minor version is the actively supported release. Customers using a prior major release (or any of its minor versions) will be supported on a best-effort basis: they will be asked to adopt the latest version, especially if a problem they are experiencing has been corrected in the latest version. Specifically, this means that version 3.0 is now the actively supported release and all older versions are supported on a best-effort basis.

---

### NOTE

Starting May 2005, the support for Release 1.0 of HP-UX HIDS will be discontinued. HP recommends that all customers using HIDS Release 1.0 upgrade to Release 3.0.

---

## Known Problems, Limitations, and Fixes

For a current and complete list of HP-UX HIDS problems and their fixes, see the Technical Knowledge Database on the HP IT Resource Center websites:

<http://us-support.external.hp.com> for Americas/Asia-Pacific customers

<http://europe-support.external.hp.com> for European customers

The Technical Knowledge Database is available to customers with support contracts.

### Clarifications

#### Update Preferred Over Cold Reinstall

HP-UX HIDS is designed to support updates. If you cold reinstall the newer version by first removing the older version (`swremove`), you will incur two reboots (instead of just one or possibly none) and the probable loss of some of your configuration data.

#### Do Not Change Permissions

Do not change the permissions on files and directories owned by `ids`. Opening up the permissions to be world writable/readable will cause the agent to fail security checks and exit. Changing file permissions will also result in `swverify` errors.

#### HUP After Log File Rotation

When you rotate the error or alert log files on an agent, you must send a HUP signal to the `idsagent` process so it can reset its file descriptors and begin writing to the new logs.

### Known Problems

#### Problem: Java Virtual Machine Runs Out of Memory for the System Manager GUI

When the System Manager GUI has alerts in the range of tens of thousands, it might die or hang as the Java Virtual Machine (JVM) eventually runs out of memory. You can increase the maximum heap size of JVM by adding a `-Xmx<size>` option after the line `"$JAVA_RUN \"` in `idsgui`. For example:

```
-Xmx256m \
```

This increases the maximum heap size to 256MB.

#### Problem: The Buffer Overflow Template cannot Filter Certain Alerts

The Buffer Overflow template does not correctly report the full pathname of the program that attempted to execute on its stack as part of a stack buffer overflow attack. As a result, the `programs_to_not_watch` template property cannot be used to filter out those alerts for buffer overflow attacks detected by the kernel. All other types of buffer overflow alerts (i.e., unusually long argument or use of non-printable character(s)) can be filtered using the `programs_to_not_watch` template property.

**Problem: The Creation of Setuid File template creates an alert with the wrong severity level**

When an empty setuid file is created using the `mknod()` system call, the setuid template incorrectly reports an alert with severity 3 instead of severity 1.

**Problem: The default value of the fail\_interval template property is incorrect**

The default value of the `fail_interval` template property for the Repeated Failed Su Commands template is incorrectly set to 1440 (seconds) in the predefined Surveillance Groups. The default value should be 86400 seconds (= 24 hours) instead.

**Problem: SSH does not perform a clean exit after idsagent is started**

After starting `idsagent` from a `ssh` login, logging out of the agent system results in the `ssh` session hanging indefinitely. As a workaround, login by entering:

```
ssh -l root <machine> /usr/dt/bin/dtterm; then type in the  
"/sbin/init.d/idsagent start" commands interactively.
```

## Limitations

**Limitation: Predefined Schedules and Groups Are Not Clearly Marked**

The predefined (read-only) surveillance schedules and groups are not well distinguished in the System Manager screens. You are allowed to modify them for the purpose of creating a new schedule, but you cannot save the modified schedule or group over the original predefined schedule or group. The program does *not* notify you that a predefined group was not saved when you press the Save button in the Schedule Manager screen.

**Limitation: Agents and Kernel Parameters**

The administration System Manager can monitor up to 23 agent systems unless you make kernel parameter changes, as described in Chapter 2, “Configuration,” of the *HP-UX Host Intrusion Detection System Administrator's Guide*.

**Limitation: Dropped Kernel Audit Records**

Depending on the system profile and product configuration, and under heavy loads, HP-UX HIDS can drop kernel audit records and therefore miss potential intrusions. The `IDDS_MODE` configuration parameter for the kernel `dsp` in the `ids.cf` configuration file only controls whether the kernel auditing subsystem (IDDS) either blocks or drops audit records under heavy loads. Currently, the user space component of HP-UX HIDS (`idskerndsp`), which collects audit data from IDDS, cannot be configured to either block or drop audit records under heavy loads. Instead, the product displays a notice in the Network Browser error panel that audit records are being dropped. The kernel `dsp` parameters, `DROP_NOTIFY_INTERVAL` and `LOW_WATERMARK`, control (1) the frequency that reminder notices are sent and (2) the point at which a notice is sent that audit records are no longer being dropped, respectively. See Appendix D, “The Agent Configuration File,” in the *HP-UX Host Intrusion Detection System Administrator's Guide* for more details.

**Limitation: The adminSchedConvert Migration Tool**

The text-based migration tool `/opt/ids/bin/adminSchedConvert` fails to migrate 2.x schedules that contain properties with the following:

- Regular expressions that contain escaped square bracket ([ or ]), or angle bracket (< or >) characters.
- Regular expressions that contain special patterns, such as <S>, <@>.
- Regular expressions that contain the expression group [...], the OR operator with the expression group [... | ...], or the NOT operator with the regular expression <![...]>.

If your text schedules contain these characters in regular expressions, you must manually convert them to the equivalent UNIX regular expressions.

#### **Limitation: The guiSchedConvert Schedule Migration Tool**

The GUI schedules migration tool, /opt/ids/bin/guiSchedConvert, fails to migrate when the 2.x schedule file has properties with <S> or <@> in their regular expressions.

If your GUI schedules contain these characters in regular expressions, you must manually convert them to use the UNIX regular expression equivalent.

#### **Limitation: Idsadmin Does Not Automatically Overwrite Existing Schedule**

Idsadmin [-f ascii\_schedule] option does not automatically overwrite existing schedule. Stop and remove the existing schedule (if there is one), and then start a new schedule using the -f option.

#### **Limitation : System Manager with Java 1.4.x**

The System Manager does not work properly with Java 1.4.x. There are no known problems running the System Manager with JDK 1.3.1. Please use the latest available version of JDK 1.3.1.

#### **Limitation: Granularity of sulog entries**

You should specify a multiple of sixty seconds in the fail\_interval template property of the Repeated Failed Su Commands template because sulog entries are time stamped with a granularity of minutes and not seconds.

#### **Limitation: Time units can not be specified for template properties in Schedule Manager**

In the Schedule Manager's template property editing windows, you can not specify time units (i.e., s=seconds, m=minutes, d=days, w=weeks) for template property time values. Because the default time unit is seconds, all time related template properties will be interpreted as being in seconds.

### **Fixes and Enhancements in Release 3.0**

Release 3.0 corrects defects and includes enhancements in the following areas:

#### **Fixes: Significant Reduction in CPU Consumption by Idscor and Better Performance Throughput**

HIDS now provides reduced CPU consumption by Idscor and better performance throughput.

**Fixes: Enhanced Default Tuning of Templates to Improve Alert Reduction**

All product templates have been rewritten and fine-tuned to detect intrusions resulting in the consolidation of two templates and introduction of new templates properties. The new correlator, along with other optimizations and performance enhancements result in faster and more efficient processing by the agent, thereby allowing for increased throughput and reduced CPU utilization as compared to older versions. A number of new template properties have been introduced to reduce the number of unnecessary alerts.

**Fixes: Enhanced Option for idsadmin**

A [-f schedule\_file] option is added to `idsadmin` to improve administration via supported command line interface; `idsadmin` is now fully supported to assist customers interested in automated provisioning of large number of agents.

Announcement

**Known Problems, Limitations, and Fixes**

---

## **2** **Installation**

---

### **IMPORTANT**

*Read this entire chapter before installing, or updating to, HP-UX HIDS release 3.0.*

## Introduction

Release 3.0 of HP-UX HIDS is available from three sources.

- As a depot directory on the server Operating Environment media, beginning with HP-UX 11i v2 and OEUR 2005 (HP-UX 11i v1). HP-UX HIDS is a selectable product on the OE media, and you may install it at system install/update time, or at a later time using these instructions.
- As a depot directory on an Application Release CD, beginning with 2005 (HP-UX 11i).
- As a depot file you download from the HP Software Depot web site (HP-UX 11i).

The HP-UX HIDS software product bundle, HP-UX-HIDS, contains the IDS and IDS-KERN products. The IDS-KERN product is used to reduce the likelihood of a system reboot for future HIDS software updates. The IDS product comprises three subproducts. You may choose to install the following subproducts:

**Table 2-1**

### Filesets of HIDS

Software	Description
IDS . IDS-AGT-RUN	The agent software. The agent runs on servers to help protect them from intrusions.
IDS . IDS-ADM-RUN and IDS . IDS-ADM-SHLIB	The administration software and the shared libraries for the administration software. The HP-UX HIDS administration System Manager manages and monitors the HP-UX HIDS agents.
IDS . IDS-ENG-A-MAN	The manpages for HP-UX HIDS.

Table 2-2 shows which software is required on the administration and agent systems as well as on a dual or evaluation system where you would run administration and agent software together. The “Installation Summary” on page 16 describes how to package the software into software depots and install it on your administration and agent systems.

**Table 2-2**

### Software to Install

Software	Evaluation or Dual System	Agent System	Administration System
IDS . IDS-AGT-RUN	YES	YES	NO
IDS . IDS-ADM-RUN and IDS . IDS-ADM-SHLIB	YES	NO	YES
IDS . IDS-ENG-A-MAN	YES	YES	YES
HP-UX-required kernel patches	YES	YES	NO
Java JRE 1.3.1	YES	NO	YES
Java-required patches	YES	NO	YES

**Table 2-2**      **Software to Install (Continued)**

<b>Software</b>	<b>Evaluation or Dual System</b>	<b>Agent System</b>	<b>Administration System</b>
IDS-KERN	YES	YES	NO

## Installation Summary

---

### IMPORTANT

---

***Read this entire chapter before installing, or updating to, HP-UX HIDS, release 3.0.***

The sections that follow provide step-by-step instructions for updating to or cold-installing HP-UX HIDS release 3.0. This section provides a summary of the tasks.

In addition to these *Release Notes*, you will need the *HP-UX Host Intrusion Detection System Administrator's Guide Software Release 3.0* for information on configuration and initial startup.

- Step 1.** Ensure that your administration and agent systems meet the requirements as described in **“Hardware and Software Requirements” on page 17.**
- Step 2.** If you are currently using release 2.x, follow the instructions in **“When Updating from Release 2.x” on page 18.**
- Step 3.** Perform the pre-installation tasks described in **“Pre-Installation” on page 19.**
- Step 4.** Create software depots for the administration system and the agent systems, as described in **“Making Depots” on page 20.**
- Step 5.** Install the software on your administration and agent systems, as described in **“Installing the Depots” on page 28.**
- Step 6.** Perform the post-installation tasks described in **“Post-Installation” on page 30.**
- Step 7.** Create secure communication certificates and perform other configuration tasks, as outlined in **“Configuration” on page 32.**
- Step 8.** If you are updating from release 1.0, you must first update to version 2.2 and then follow the instructions in **“Updating from Release 2.x” on page 30.**

---

## Hardware and Software Requirements

Check that your systems meet the requirements for installing HP-UX HIDS.

### Administration and Agent Systems

For each administration and agent system:

- You must be running HP-UX 11i v1, 11i v1.6, or 11i v2. To check, enter:

```
uname -r
```

It will display B.11.11, B.11.22, or B.11.23, respectively.

- The system must be at least a PA-RISC system for HP-UX 11i v1 or Itanium-based for HP-UX 11i v1.6 and 11i v2.
- You must be superuser to do the installation.

### Administration System

For the system where you plan to install the administration software:

- You must have 26 MB of free disk space in `/opt/ids` and space for configuration files in `/etc/opt/ids` and log files in `/var/opt/ids`.
- You must have Java SDK or RTE 1.3.1.x (version 1.3.1.13 or later is recommended) and all the corresponding Java patches. Java installation is part of these installation instructions. (Java 1.4.x may co-exist with 1.3.1.x, but it does not work with the System Manager. Therefore, 1.3.1.x is used by default when the System Manager starts.)

### Agent Systems

On each system, which you plan to install the agent software for monitoring the system for security breaches or system misuse:

- You must have 8 MB of free disk space in `/opt/ids`.
- The memory mapped file (`/var/opt/ids/ids_*`) has increased in size from 10M to 20M in v3.0. HP recommends that you have at least 50M of free space in `/var` for the memory mapped files and log files.
- For HP-UX 11i v1, you must have certain patches for both the operating system and the kernel audit system. Patch installation is part of these installation instructions.
- The `cron` daemon must be enabled. See `cron(1M)` for more information.
- Virtual memory usage of `idscor` process can be as high as 200 M. You may need to increase the `maxdsiz` tunable for your system.

### Dual System

If a system is both an administration system and agent system, combine the requirements for both.

## **When Updating from Release 2.x**

HP-UX HIDS software release 3.0 is not backward compatible with any 2.x releases. The Release 3.0 system manager cannot manage Release 2.x agents and vice versa. Release 2.x communication keys and certificates are recognized and valid in Release 3.0 and new keys and certificates need not be generated after migrating to Release 3.0.

---

## Pre-Installation

HP recommends that you stop the `idsagent` before upgrading to HP-UX HIDS Release 3.0.

---

### IMPORTANT

We recommend that you make a full backup of all administration and agent systems before you install HP-UX HIDS. Installation on agent systems requires a kernel rebuild (automatic) and reboot.

## Making Depots

It is a good idea to gather the various pieces of software into depots that you can use with the `swinstall` command. These instructions tell you how to prepare three combination depots. You will need *at most three* of them: one administration depot and one or two agent depots. The three depots are described in Table 2-3.

After you select the two or three that you need, we recommend you go through the rest of this section and the next one (“Installing the Depots” on page 28) and mark the substeps that you will need to complete.

**Table 2-3**      **Software Depots**

Depot	Contents
<b>11i Admin+Agent Depot</b> <code>/var/depot/ids_11i_admin+agent</code> For an HP-UX 11i system supporting the HP-UX HIDS administration <i>and</i> agent software	Required system patches Required Java patches Java 1.3.1 IDS.IDS-ADM-RUN and IDS.IDS-ADM-SHLIB subproducts IDS.IDS-AGT-RUN subproduct IDS.IDS-ENG-A-MAN subproduct IDS-KERN product
<b>11i Admin Depot</b> <code>/var/depot/ids_11i_admin</code> For an HP-UX 11i system supporting the HP-UX HIDS administration software	Required Java patches Java 1.3.1 IDS.IDS-ADM-RUN and IDS.IDS-ADM-SHLIB subproduct IDS.IDS-ENG-A-MAN subproduct
<b>11i Agent Depot</b> <code>/var/depot/ids_11i_agent</code> For an HP-UX 11i system supporting the HP-UX HIDS agent software	Required system patches IDS.IDS-AGT-RUN subproduct IDS.IDS-DOC subproduct

### Create the Depot Directory

- Step 1.** Log in as superuser (root) on a system where you can build a software depot. The current or intended HP-UX HIDS administration system is a good choice.
- Step 2.** If it does not exist, create the base directory for the depots now.

```
mkdir /var/depot
```

### Get Patches for HP-UX 11i v1

Perform this procedure only if one or more of your agent systems is running HP-UX 11i v1 (PA).

---

**NOTE** If you have installed any software updates, some of these patches may already be present on your systems. You can first install the HP-UX HIDS software and run the `/opt/ids/bin/IDS_checkInstall` command to check the patches that you do not need to download.

If you attempt to install a patch that is already there, the `swinstall` command will note that fact and just install the other patches.

---

- Step 1.** Log in as superuser (root) on the depot system; see “Create the Depot Directory” on page 20.
- Step 2.** Create a directory where you can save the patches and make a temporary depot. We'll use `/var/tmp/idspatch_11i`.
- Step 3.** Using the Internet, go to the HP Support web site <http://itrc.hp.com>.
- Step 4.** Click on the link individual patches.

---

**NOTE** You must be registered before you can download patches.

---

- Step 5.** Using the instructions on the web site, download the patches listed in Table 2-4 on page 22 into `/var/tmp/idspatch_11i`.

---

**NOTE** Note the following:

- Some patches may have dependency patches: patches that must be installed first. Click the dependency links and download the dependency patches, too.
- Some patches may be superseded. You can choose either the patch we list or the superseded patch.

---

- Step 6.** Unpack the patch file sets into their separate depots:

```
# sh -c 'for i in /var/tmp/idspatch_11i/PH*; do sh $i; done'
```

- Step 7.** Copy the patches to your agent and administration depots as appropriate:

**a. 11i Agent Depot**

If any of your agent systems is running HP-UX 11i v1, copy the 11i IDS-KERN product and IDS agent subproducts into the `ids_11i_agent` depot:

```
# swcopy -s /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS-KERN
IDS.IDS-AGT-RUN \
IDS.IDS-ENG-A-MAN @ /var/depot/ids_11i_agent
```

**b. 11i Admin Depot**

If your administration system will *not* be running an agent, skip this step.

**c. 11i Admin+Agent Depot**

If your administration system is running HP-UX i v1 and *will* be running an agent, copy the patch depots into the `ids_11i_admin+agent` depot:

```
# sh -c 'for i in /var/tmp/idspatch_11i/PH*.depot; \
do swcopy -s $i \* @ /var/depot/ids_11i_admin+agent; done'
```

### Patches Required for HP-UX 11i

The patch listed in Table 2-4 must be installed on all HP-UX 11i v1 (PA) systems that will run the HP-UX HIDS agent software

---

**NOTE**

These patches are *necessary* for HP-UX 11i v1 (PA systems). It does *not* apply to HP-UX 11i v.1.6 or 11i v2 (Itanium-based systems).

---

**You must install all the patches *before* or at the same time you install HP-UX HIDS on HP-UX 11iv1.**

**Table 2-4**

**Patches Required for HP-UX 11i v1 HIDS Agent Systems**

Patch	Description
PHKL_26749	s700_800 11.11 vn_rename to skip PXSEMA(), creat(2) ENOENT
PHKL_30588	libaudit.a cumulative patch

## Get the HP-UX HIDS Product

HP-UX HIDS release 3.0 for HP-UX 11i is available online from the HP Software Depot as of December 2004, as well as various Application Release and Operating Environment media updates starting in 2005.

### From the HP-UX 11i v2 System Release

See the *HP-UX 11i Version 2 Installation and Update Guide* for information on installing HP-UX HIDS with a system installation or update. If the system is already installed, you can use the method described in “From an Application Release CD or an Operating Environment CD” on page 23.

### From the HP Software Depot

- Step 1.** Log in as superuser (`root`) on the depot system; see “Create the Depot Directory” on page 20.
- Step 2.** Open the HP Software Depot web site <http://software.hp.com>, select the “Security and Manageability” section, and choose the “HP-UX Host Intrusion Detection System (HP-UX HIDS) version 3.0” product.
- Step 3.** Using the instructions on the web site, download the 11i product depot into `/var/tmp/HPUX-HIDS_11i.depot`.
- Step 4.** Copy the HP-UX HIDS product to your administration and agent depots, as appropriate.

#### a. 11i Agent Depot

If any of your agent systems is running HP-UX 11i, copy the 11i IDS-KERN product and IDS agent subproducts into the `ids_11i_agent` depot:

```
# swcopy -s /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS-KERN
IDS.IDS-AGT-RUN \
IDS.IDS-ENG-A-MAN @ /var/depot/ids_11i_agent
```

#### b. 11i Admin Depot

If your administration system is running HP-UX 11i and will *not* be running an agent, copy the 11i administration subproducts into the `ids_11i_admin` depot:

```
# swcopy -s /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS.IDS-ADM-RUN \
IDS.IDS-ENG-A-MAN @ /var/depot/ids_11i_admin
```

#### c. 11i Admin+Agent Depot

If your administration system is running HP-UX 11i and *will* be running an agent, copy the entire 11i product into the `ids_11i_admin+agent` depot:

```
# swcopy -s /var/tmp/idsprod/HPUX-HIDS_11i.depot \* \
@ /var/depot/ids_11i_admin+agent
```

### From an Application Release CD or an Operating Environment CD

- Step 1.** Log in as superuser (`root`) on the depot system; see “Create the Depot Directory” on page 20.
- Step 2.** Do the following:

- a. Locate the HP-UX 11i Application Release CD or HP-UX 11i Operating Environment CD that contains the HP-UX-HIDS product bundle and load it into your CD reader. We'll assume it's mounted on `/SD_CDROM`.

**b. 11i Agent Depot**

If any of your agent systems is running HP-UX 11i, copy the 11i IDS-KERN product and IDS agent subproducts into the `ids_11i_agent` depot:

```
# swcopy -s /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS-KERN
IDS.IDS-AGT-RUN \
IDS.IDS-ENG-A-MAN @ /var/depot/ids_11i_agent
```

**c. 11i Admin Depot**

If your administration system is running HP-UX 11i and will *not* be running an agent, copy the 11i administration subproducts into the `ids_11i_admin` depot:

```
# swcopy -s /SD_CDROM HPUX-HIDS.IDS.IDS-ADM-RUN
HPUX-HIDS.IDS.IDS-ENG-A-MAN \
    @ /var/depot/ids_11i_admin
```

**d. 11i Admin+Agent Depot**

If your administration system is running HP-UX 11i and *will* be running an agent, copy the entire 11i product into the `ids_11i_admin+agent` depot:

```
# swcopy -s /SD_CDROM HPUX-HIDS.IDS @ /var/depot/ids_11i_admin+agent
```

## Get Patches for Java

- Step 1.** Log in as superuser (`root`) on the depot system; see “Create the Depot Directory” on page 20.
- Step 2.** Create a directory where you can save the patches and make a depot. We’ll use `/var/tmp/javapatch`.
- Step 3.** Open the HP Java web site <http://www.hp.com/go/java>,
- Step 4.** Click on the link `patches`.
- Step 5.** Take note of the list of patches that you need, based on your administration system; that is, the HP-UX 11i set.
- Step 6.** Open the HP Support web site <http://itrc.hp.com>,
- Step 7.** Click on the link `individual patches`.
- Step 8.** Using the instructions on the web site, download the 11i Java patches into `/var/tmp/javapatch`.

You must be registered before you can download patches.

Some patches may have dependency patches: patches that must be installed first. Click the dependency links and download the dependency patches, too.

- Step 9.** Unpack the patch file sets:

```
# sh -c 'for i in /var/tmp/javapatch/PH*; do sh $i; done'
```

- Step 10.** Copy the patch file sets into your administration depot, using *one* of the following steps:

### a. 11i Admin Depot

If your administration system is running HP-UX 11i and will *not* be running an agent, copy the 11i Java patches into the `ids_11i_admin` depot:

```
# sh -c 'for i in /var/tmp/javapatch/PH*.depot; \
do swcopy -s $i \* @ /var/depot/ids_11i_admin; done'
```

### b. 11i Admin+Agent Depot

If your administration system is running HP-UX 11i and *will* be running an agent, copy the 11i Java patches into the `ids_11i_admin+agent` depot:

```
# sh -c 'for i in /var/tmp/javapatch/PH*.depot; \
do swcopy -s $i \* @ /var/depot/ids_11i_admin+agent; done'
```

## Get the Java Software

- Step 1.** Log in as superuser (`root`) on the depot system; see “Create the Depot Directory” on page 20.
- Step 2.** Open the HP Java web site <http://www.hp.com/go/java>,
- Step 3.** Click on the link `SDK and RTE 1.3.1`.
- Step 4.** Click on the link `downloads`.

- Step 5.** Choose the SDK or RTE 1.3.1 version.
- Step 6.** Using the instructions on the web site, download the software, for example, to  
`/var/tmp/sdk_13101os11.depot`.
- Step 7.** Transfer the software to the administration depot using one of the following steps.

**a. 11i Admin Depot**

If your administration system is running HP-UX 11i and will *not* be running an agent, copy the 11i Java software into the `ids_11i_admin` depot:

```
# swcopy -s /var/tmp/sdk_13101os11.depot \* \  
@ /var/depot/ids_11i_admin
```

**b. 11i Admin+Agent Depot**

If your administration system is running HP-UX 11i and *will* be running an agent, copy the 11i Java software into the `ids_11i_admin+agent` depot:

```
# swcopy -s /var/tmp/sdk_13101os11.depot \* \  
@ /var/depot/ids_11i_admin+agent
```

## Installing OpenSSL

In addition to Java, you must also install OpenSSL on your system. OpenSSL A.00.09.07 is the latest version of OpenSSL available at <http://www.software.hp.com>.

The following are the steps to install the OpenSSL A.00.09.07-d software:

1. Log in as `root`.
2. Insert the software CD into the appropriate drive if you are installing from the Application Software CD. If you are downloading the software package from <http://www.software.hp.com>, download the depot and follow the instructions provided in the installation page of the OpenSSL software.
3. Run the following command to install the OpenSSL software:  

```
$ swinstall -s <fully-qualified depot source path> OpenSSL
```
4. Enter the drive mount point in the Source Depot Path field and click **OK**. Change the Source Host Name, if required.
5. Select **OpenSSL** from the list of available software and choose **Mark for Install** from the Actions menu.
6. Select **Install** from the Actions menu to start the installation.
7. Click **OK** in the Install Analysis window when the Status field displays a Ready message.
8. Select **Yes** to start the installation. `swinstall` loads the OpenSSL files in approximately 3 to 5 minutes.

The `swinstall` command installs the OpenSSL A.00.09.07-d software in the `/opt/openssl` directory.

---

**IMPORTANT**

You cannot install OpenSSL A.00.09.07-d on a system containing the Internet Express OpenSSL 0.9.7c software. If the Internet Express OpenSSL 0.9.7c software is installed on your system, you must remove the Internet Express OpenSSL 0.9.7c software before installing OpenSSL A.00.09.07-d.

On HP-UX 11i v1 systems that do not contain the `/dev/random` file, OpenSSL automatically uses `prngd` to generate random numbers.

---

## Installing the Depots

---

### CAUTION

If you choose to not follow the installation instructions in this section, it is vitally important that you install the required kernel patches *before* you install the HP-UX HIDS software. *Do not reinstall any patches without consulting HP Support first.*

---

### NOTE

In the commands below, `swinstall` will not reinstall any patches or software that are already installed. You can ignore messages to that regard. The software you need will be installed properly.

The `swinstall` option “`-x autoreboot=true`” in the following commands ensures that any software that requires a system reboot will be installed. If none of the installed software requires a reboot, the system will not be rebooted. See also “Will Installing HP-UX HIDS Release 3.0 Reboot My Agent System?” on page 29.

- Step 1.** Log in as superuser (root) on the HP-UX HIDS administration system.
- Step 2.** Make sure you are the only user on the system; the installation *may* require a reboot.
- Step 3.** Install the software on your administration system. In this procedure, we assume that you are installing one of the admin software depots described in “Making Depots” on page 20. Perform one only of the next two substeps:

- a. 11i Admin Depot**

**Either**

If your administration system is running HP-UX 11i and will *not* be running an agent, install the `ids_11i_admin` depot (a reboot *may* occur):

```
# swinstall -x autoreboot=true \  
-s depotsys:/var/depot/ids_11i_admin \*
```

- b. 11i Admin+Agent Depot**

**Or**

If your administration system is running HP-UX 11i and *will* be running an agent, install the `ids_11i_admin+agent` depot (a reboot *will* occur):

```
# swinstall -x autoreboot=true \  
-s depotsys:/var/depot/ids_11i_admin+agent \*
```

- Step 4.** Install the software on each of your agent systems. In this procedure, we assume that you are installing one of the agent software depots described in “Making Depots” on page 20.
  - a.** Log in as superuser (root) on each HP-UX HIDS agent system.
  - b.** Make sure you are the only user on the system; the installation *will* require a reboot.
  - c. 11i Agent Depot**

**Either**

If your agent system is running HP-UX 11i, install the `ids_11i_agent` depot:

```
# swinstall -x autoreboot=true \  
-s depotsys:/var/depot/ids_11i_agent \*
```

## Will Installing HP-UX HIDS Release 3.0 Reboot My Agent System?

The installation scripts for HP-UX HIDS try to avoid unnecessary system reboots. However, in some circumstances, a system reboot may be required. Those circumstances are (in order of priority):

1. If the `Reinstall Filesets` option is selected in the graphical interface to `swinstall`, all HP-UX HIDS filesets will be installed, and a system reboot *will* occur.
2. If the `-x reinstall=true` option is passed to the command line invocation of `swinstall`, all HP-UX HIDS filesets will be installed, and a system reboot *will* occur.
3. If HP-UX HIDS version 3.0 is being installed on a system for the first time (a fresh install), a reboot *will* occur.
4. If HP-UX HIDS is being upgraded to version 3.0 from a previous version, a reboot will occur.

**Table 2-5**

**Reboot Matrix**

Update from:	Update to v3.0
Not installed	Reboot
<b>v3.0</b>	Reboot
<b>v2.2</b>	Reboot
<b>v2.1</b>	Reboot
<b>v2.0</b>	Reboot
<b>v1.0</b>	Reboot

## Post-Installation

- When an agent system reboots after an upgrade from HP-UX HIDS version 2.x to version 3.0, the “HP-UX Startup in progress” list should display “OK” for the “Starting HP-UX HIDS agent” entry.
- When an agent system reboots after a cold installation, the “HP-UX Startup in progress” list should display “N/A” for the “Starting HP-UX HIDS agent” entry. That is, system boot will not automatically start `idsagent` until after the secure communication keys and certificates have been installed on the agent system (see “Configuration” on page 32).
- On each agent system, after the system has rebooted, run the `IDS_checkInstall` script.

```
# /opt/ids/bin/IDS_checkInstall
```

This script checks that the Intrusion Detection Data Source (`idds`) kernel driver is configured and enabled. On all systems, it also checks that all the *necessary* and superseding patches have been installed; it does not verify superseding patches.

## Updating from Release 2.x

This section contains instructions on the use of conversion utilities for v2.x migrations:

### The `guiSchedConvert` Migration Tool

Delivered as: `/opt/ids/bin/guiSchedConvert`

Usage: `guiSchedConvert [java executable path name]`

What it does: The migration tool will migrate any System Manager v2.x schedule and group file to a corresponding v3.0 syntax. As noted in v3.0 feature announcements, templates differ significantly from v2.x. Highlights of the change include template name change, modification in properties offered and changes in the name of the new property sets. If you have an existing v2.x installation with customer schedules/groups (apart from what was shipped with the product), you should use the migration tool to convert these schedules to be compliant with the v3.0 architecture.

The tool checks whether the groups present in the system belong to v3.0 or v2.x. In case any group belongs to v2.x, it will be migrated. Any v3.0 group will not be changed. For every group that exist in the system (in `/var/opt/ids/gui/SurveillanceGroups`), the `guiSchedConvert` outputs whether the group is being migrated or not.

Steps:

Please back up the original schedules and groups files before installing/updating to v3.0 and the running migration tool.

After installing/updating to the new v3.0 HIDS software, invoke the tool in one of the following ways (before starting the `idsgui` process):

```
# /opt/ids/bin/guiSchedConvert
```

Or

```
$ /opt/ids/bin/guiSchedConvert /opt/java1.3/bin/java
```

If the schedule fails to be activated successfully after 3.0 conversion, the failure is probably due to the limitation described on p10 with the title “The adminSchedConvert Migration Tool” on page 31. If successful, reset the "File modification template" to its prescanned default and add custom changes to it manually.

### **The adminSchedConvert Migration Tool**

Delivered as: /opt/ids/bin/adminSchedConvert

Usage:

```
/opt/ids/bin/adminSchedConvert [file_1] [file_2] ... [file_n]
```

where:

[file\_x] is a Release 2.x text schedule file.

**What it does:** The adminSchedConvert tool converts HIDS Release 2.x text schedule files (for use with the idsadmin -f option) to the HIDS Release 3.0 format. For each [file\_x], the script creates a file with the same name and extension 3\_x.

## Configuration

Once you have installed or updated your HP-UX HIDS software, you need to complete the configuration with the required and optional steps that are described in “Chapter 2: Configuration” of *HP-UX Host Intrusion Detection System Administrator’s Guide Software Release 3.0*. The following is an annotated list of some of the sections in the chapter.

### Required

Before you can run HP-UX HIDS, you must complete the following configuration step.

- Section “Setting Up the HP-UX HIDS Secure Communications”

You may need to create keys and certificates to ensure secure communication between the Administration system and the Agent systems.

If you are updating from release 1.0, your old keys and certificates are invalid; they must be recreated.

If you are updating from release 2.0, your old keys and certificates are preserved.

### Optional

You may also need to complete one or more of the following steps.

- Section “Configuring a Multihomed Agent System”

If you have agent systems with more than one IP address, you may need to specify the correct address to the agent and administration software.

- Section “Configuring a Multihomed Administration System”

If you have an administration system with more than one IP address, you may need to specify the correct address to the agent and administration software.

- Section “Enabling Over 23 Agents (Thread Limits)”

With more than 23 agent systems active at one time, you will need to increase the thread limit.

- Section “Working with Firewalls”

If you have firewalls between the administration system and agents systems, you must configure the firewall systems.

- Section “Working with NIS”

If you use NIS, you must configure the NIS master system.



## Attention

USE OF THE HP-UX HOST INTRUSION DETECTION SYSTEM AND ASSOCIATED DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE") IS SUBJECT TO THE HP SOFTWARE LICENSE TERMS SET FORTH BELOW. USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE LICENSE TERMS. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND. IF THE SOFTWARE IS BUNDLED WITH ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE UNUSED PRODUCT FOR A FULL REFUND.

THIS PRODUCT MAKES USE OF THE OPENSOURCE PRODUCT:

## LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

## OpenSSL License

```
/* =====  
* Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.  
*  
* Redistribution and use in source and binary forms, with or without  
* modification, are permitted provided that the following conditions  
* are met:  
*  
* 1. Redistributions of source code must retain the above copyright  
*   notice, this list of conditions and the following disclaimer.  
*  
* 2. Redistributions in binary form must reproduce the above copyright  
*   notice, this list of conditions and the following disclaimer in  
*   the documentation and/or other materials provided with the  
*   distribution.  
*  
* 3. All advertising materials mentioning features or use of this  
*   software must display the following acknowledgment:  
*   "This product includes software developed by the OpenSSL Project  
*   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"  
*  
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to  
*   endorse or promote products derived from this software without  
*   prior written permission. For written permission, please contact  
*   openssl-core@openssl.org.  
*  
* 5. Products derived from this software may not be called "OpenSSL"  
*   nor may "OpenSSL" appear in their names without prior written  
*   permission of the OpenSSL Project.  
*  
* 6. Redistributions of any form whatsoever must retain the following  
*   acknowledgment:  
*   "This product includes software developed by the OpenSSL Project  
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
```

```
=====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

## Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given
* attribution as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
```

```
*   The word 'cryptographic' can be left out if the routines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson
*   (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

---

## HP Software License Terms

The following License Terms govern your use of the accompanying Software.

**License Grant.** HP grants you a license to Use one copy of the Software. "Use" means storing, loading, installing, executing or displaying the Software. You may not modify the Software or disable any licensing or control features of the Software. If the Software is licensed for "concurrent use", you may not allow more than the maximum number of authorized users to Use the Software concurrently.

**Ownership.** The Software is owned and copyrighted by HP or its third party suppliers. Your license confers no title or ownership and is not a sale of any rights in the Software, its documentation or the media on which they are recorded or printed. Third party suppliers may protect their rights in the Software in the event of any infringement.

With respect to Sun's implementation of the Java Secure Socket Extension (JSSE) and the Java Cryptography Extension (JCE) that are included in this software, Sun is a third party beneficiary of this license.

**Copies and Adaptations.** You may only make copies or adaptations of the Software for archival purposes or when copying or adaptation is an essential step in the authorized Use of the Software on a backup product, provided that copies and adaptations are used in no other manner and provided further that Use on the backup product is discontinued when the original or replacement product becomes operable. You must reproduce all copyright notices in the original Software on all copies or adaptations. You may not copy the Software onto any public or distributed network.

**No Disassembly or Decryption.** You may not disassemble or decompile the Software without HP's prior written consent. Where you have other rights under statute, you will provide HP with reasonably detailed information regarding any intended disassembly or decompilation. You may not decrypt the Software unless necessary for the legitimate use of the Software.

**Transfer.** You may transfer your rights under this Agreement to another party on a permanent basis. Your license will automatically terminate upon any transfer of the Software. Upon transfer, you must deliver the Software, including any copies and related documentation, to the transferee. The transferee must accept these License Terms as a condition to the transfer.

**Termination.** HP may terminate your license upon notice for failure to comply with any of these License Terms. Upon termination, you must immediately destroy the Software, together with all copies, adaptations and merged portions in any form.

**Export Requirements.** You may not export or re-export the Software or any copy or adaptation in violation of any applicable laws or regulations.

**U.S. Government Restricted Rights.** The Software and any accompanying documentation have been developed entirely at private expense. They are delivered and licensed as "commercial computer software" as defined in DFARS 252.227-7013 (Oct 1988), DFARS 252.211-7015 (May 1991) or DFARS 252.227-7014 (Jun 1995), as a "commercial item" as defined in FAR 2.101(a), or as "Restricted computer software" as defined in FAR 52.227-19 (Jun 1987) (or any equivalent agency regulation or contract clause), whichever is applicable. You have only those rights provided for such Software and any accompanying documentation by the applicable FAR or DFARS clause or the HP standard software agreement for the product involved.

**Disclaimer.** TO THE EXTENT ALLOWED BY LOCAL LAW, THE SOFTWARE IS PROVIDED TO YOU "AS IS" AND WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, WHETHER ORAL OR WRITTEN, EXPRESS OR IMPLIED. HP SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF A THIRD PARTY'S INTELLECTUAL PROPERTY.

Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you. You may have other rights that vary from country to country, state to state, or province to province.

**Limitation of Liability.** HP WILL NOT IN ANY EVENT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING LOST PROFITS, LOST DATA, OR BUSINESS INTERRUPTION) RELATED TO ANY USE, REPRODUCTION, MODIFICATION, OR DISTRIBUTION OF THE SOFTWARE, WHETHER BASED ON WARRANTY, CONTRACT, TORT OR ANY OTHER LEGAL THEORY. APPLICABLE LAW MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

**Entire Agreement.** These License Terms contains the entire understanding and agreement of the parties relating to the subject matter hereof. Any representation, promise, or condition not explicitly set forth in these License Terms shall not be binding on either party.