HP-UX Host Intrusion Detection System (HIDS) Version 4.8 Release Notes

HP-UX 11i v3

Abstract

This document describes about new features and defect fixes for Host Intrusion Detection System (HIDS).

HP Part Number: 766145-002
Published: March 2015
Edition: 1

Contents

HP secure development lifecycle

Starting with HP-UX 11i v3 March 2013 update release, HP secure development lifecycle provides the ability to authenticate HP-UX software. Software delivered through this release has been digitally signed using HP's private key. You can now verify the authenticity of the software before installing the products, delivered through this release.

To verify the software signatures in signed depot, the following products must be installed on your system:

- `B.11.31.1303` or later version of SD (Software Distributor)
- `A.01.02.00` or later version of HP-UX Whitelisting `(WhiteListInf)`

To verify the signatures, run: `/usr/sbin/swsign -v -s <depot_path>`

For more information, see *Software Distributor documentation* at: http://www.hp.com/go/sd-docs.

NOTE: Ignite-UX software delivered with HP-UX 11i v3 March 2014 release or later supports verification of the software signatures in signed depot or media, during cold installation. For more information, see *Ignite-UX* documentation at: http://www.hp.com/go/ignite-ux-docs.

1 Announcement

The *HP-UX Host Intrusion Detection System Version 4.8* is updated to provide the fix for POODLE vulnerability. For more information about POODLE, see POODLE.

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. Many types of attacks can bypass network-based detection systems. HP-UX HIDS monitors these bypassed attacks and complements the existing network-based security mechanisms, bolstering enterprise security.

HP-UX HIDS seeks patterns that might suggest security breaches or misuse by examining information about system activity from a variety of data sources. It detects illicit activities that include attempting to break into or disrupt the system, modifying system files and directories, or attempting to spread a virus. When HP-UX HIDS detects an intrusion attempt, it issues an alert to the administrative interface, where users can immediately investigate the situation, and take necessary action against the intrusion. In addition, users can customize a local response to an alert as described in Appendix B, Response Programs in the *Host Intrusion Detection System Administrator Guide*.

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

Compatibility with previous versions

HP-UX HIDS v4.8 software is backward compatible with HIDS versions 4.7, 4.4, 4.3, 4.2, 4.1, 4.0, and 3.1. However, surveillance schedules created with v3.1 or v4.0 must be migrated to HIDS v4.3 (see "Migrating schedules from older versions of HIDS" (page 10)). Schedules created with HIDS v4.1 or v4.2 do not need to be migrated. However, v4.1 schedule must be migrated in order to make use of the configuration properties introduced in v4.2 and supported in v4.3.

NOTE: HP-UX HIDS v4.8 is not backward compatible with HIDS v1.0 and HIDS v2.0, v2.1, and v2.2 (collectively referred to as HIDS 2.x). HIDS v1.0 and HIDS v2.x are obsolete. HIDS v4.8 schedules with the `Log File Monitoring` detection template feature enabled cannot be activated by HIDS agents running the HIDS v4.1 software.

The Schedules configured with Containers (SRPs) cannot be activated on agents running HIDS v4.3 and earlier.

Compatibility with other products

HP-UX HIDS is not compatible with all HP software products; see Table 1 for the list of products that are supported. Do not run HP-UX HIDS on systems that are running unsupported products (or vice versa).

Table 1 HP-UX HIDS Product Compatibility

Product	Support
HP-UX 11i v3	Yes
HP-UX 11i v2	No
HP-UX 11i v1.6	No
HP-UX 11i v1.5	No
HP-UX 11i v1	No

Table 1 HP-UX HIDS Product Compatibility *(continued)*

Product	Support
NIS, NIS+	Yes
OpenView	Yes
ServiceGuard	Not tested
Third-party Event Monitoring Service (EMS)	Not tested
Trusted Mode operation	Yes
Virtual Vault	No

Benefits

The HP-UX HIDS intrusion detection product offers the following benefits:

- Automatically monitors each configured host system within the network for possible signs of unwanted and potentially damaging intrusions.
- Provides continuous surveillance against inappropriate system usage that include attempting to break into or disrupt the system, modifying system files and directories, or attempting to spread a virus.
- Continuously examines ongoing activity on a system and seeks out patterns that might suggest security breaches or misuse due to the exploitation of certain vulnerabilities:

  Vulnerability: Unauthorized File Modification
  Monitors: Critical system and application programs and configuration files
  System and application log files
  File additions and deletion
  Critical files made world writable
  Privileged “setuid” programs created
  Files modified by non-owners
  Vulnerability: Poorly written privileged programs
  Monitors: Buffer overflows and Race conditions
  Vulnerability: Weak password or unauthorized access
  Monitors: Logins/Logouts
  Vulnerability: Password guessing
  Monitors: Failed logins and failed su attempts
  Monitors: Messages logged to text based log files

  NOTE: Logins/Logouts, Failed logins and failed su attempts are not supported in HP-UX Containers (HP-UX SRP).

- Complements network-based security solutions and bolsters the overall security of the computing infrastructure. HP-UX HIDS is designed to detect intrusions that network-based security products cannot identify, thereby strengthening the integrity of the host system as the last line of defense.
- Provides immediate notification when a suspicious activity is detected, and supports real-time response.

2 Installation requirements

This chapter provides information about HIDS installation.

IMPORTANT: Read this entire chapter before installing or updating to HIDS v4.8.

Introduction

HP-UX HIDS v4.8 bundle can be downloaded from the HP Software Depot Website. The following product versions are supported:

- HPUX-HIDS F.04.08 for HP-UX 11i v3

The HIDS software product bundle, `HPUX-HIDS`, contains the `IDS` and `IDS-KRN` products. The `IDS-KRN` product is used to reduce the likelihood of a system reboot for future HIDS software updates. The `IDS` product contains four filesets. Table 2 lists the filesets included in the `IDS` product.

Table 2 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 System Manager manages and monitors the HP-UX HIDS agents.
`IDS.IDS-ENG-A-MAN`	The manpages for HP-UX HIDS.

Table 3 describes which software is required on the administration and agent systems and on a dual or evaluation system running administration and agent software together. The "Installation summary" (page 8) describes how to package the software into software depots and install it on your administration and agent systems.

Table 3 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
JRE 6.0	YES	NO	YES
Java 6.0 patches	YES	NO	YES
`IDS-KRN`	YES	YES	NO
OpenSSL	YES	YES	YES

Installation summary

The following sections provide step-by-step instructions for updating to or cold-installing HIDS v4.8. This section provides a summary of the tasks.

In addition to these *Release Notes*, you will need the *Host Intrusion Detection System Administrator Guide Software Release 4.8,* for information on configuration and initial startup.

1. Ensure that your administration and agent systems meet the requirements as described in **"Hardware and software requirements" (page 9)**.
2. If you want to migrate your existing schedules to HIDS 4.2, complete the steps listed in **"Migrating schedules from older versions of HIDS" (page 10)**.
3. Perform the preinstallation tasks described in **"Preinstallation" (page 10)**.
4. Create software depots for the administration system and the agent systems, as described in **"Making depots" (page 10)**.
5. Install the software on your administration and agent systems, as described in **"Installing depots" (page 14)**.
6. Perform the post-installation tasks described in **"Postinstallation" (page 16)**.
7. Create secure communication certificates and perform other configuration tasks, as outlined in **"Configuration" (page 16)**.

Hardware and software requirements

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

Administration and agent systems

Each administration and agent system must meet the following requirements:

- The administration and agent system must be running HP-UX 11i v3. To check, enter the following command:

  ```
  # uname -r
  ```

  It should display `B.11.31`.
- The system must be running on HP-UX 11i v3.
- You must be a superuser to do the installation.

Administration system

The system on which you plan to install the administration software must meet the following requirements:

- 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 Runtime Environment 6.0 (JRE 6.0) and all the corresponding Java patches. Java installation is part of these installation instructions.

Agent systems

Each system on which you plan to install the agent software must meet the following requirements:

- You must have 8 MB of free disk space in `/opt/ids`.
- The memory mapped file (`/var/opt/ids/ids_*`) is 20 M in size. HP recommends that you have at least 50 M of free space in `/var` for the memory mapped files and log files.
- The `cron` daemon must be enabled. Refer to *cron*(1M) for more information.
- Virtual memory usage by the `idscor` process can be as high as 200 M. You may need to increase the `maxdsiz` tunable parameter for your system.

Dual system

If a system is both an administration system and an agent system, it must meet the requirements for both system types.

Migrating schedules from older versions of HIDS

Surveillance schedules created using HIDS v3.1 and v4.0 must be migrated before they can be run by HIDS v4.8 agents. Schedules created using HIDS v4.1 do not need to be migrated unless the features introduced in v4.2 and supported in v4.8 are needed. Schedules created using HIDS v4.2, 4.3, and v4.4 do not need to be migrated.

NOTE: If you are migrating schedules created using HIDS v3.1, you must first upgrade to HIDS v4.0 and convert them to HIDS v4.1 schedules by running `guiSchedConvert` before converting them to v4.4 schedules using the process described below.

Complete the following process to migrate HIDS v4.0 schedules to HIDS v4.4 schedules:

1. Use the v4.0 `idsgui` to convert all the Java schedules that you want to migrate into text files. Use the **Details** tab in the GUI Schedule Manager to save the schedules. The text schedules are saved in `/var/opt/ids/gui/logs/<schedulename.txt>`
2. Use `/opt/ids/bin/migrator` to migrate each schedule to HIDS v4.8. Use this command with the following options:

   `-i` *`input schedule`*

   `-o` *`<output directory>`*

   If this option is not specified, the tool creates the schedules and group files in `/etc/opt/ids/schedules` and `/etc/opt/ids/schedules/groups`, respectively. If this option is specified, the schedule files are created in the specified *`<output directory>`*, and the corresponding group files are created in *`<output directory>`*`/groups`

The migrated schedules will contain `monitor_failed_attempts` and `log_severity_def` properties in the `GLOBALS` section.

Preinstallation

Before installing v4.8 on a system that has a previous version of HP-UX HIDS installed and running, HP recommends that you stop `agent` and `admin` processes.

IMPORTANT: For systems that do not currently have any version of HP-UX HIDS installed, HP recommends 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 least two* of them: one administration depot and one or two agent depots. Table 4 lists and describes these depots.

After you select the two or three that you need, HP recommends that you go through the rest of this section and "Installing depots" (page 14) and mark the substeps that you will need to complete.

Table 4 Software depots

Depot	Contents
11i Admin+Agent Depot `/var/depot/ids_11i_admin+agent`	• Required system patches • Required Java patches

Table 4 Software depots *(continued)*

Depot	Contents
For an HP-UX 11i system supporting the HIDS administration *and* agent software	• JRE 6.0 • `IDS.IDS-ADM-RUN` and `IDS.IDS-ADM-SHLIB` subproduct • `IDS.IDS-AGT-RUN` subproduct • `IDS.IDS-ENG-A-MAN` subproduct • `IDS-KRN` subproduct • OpenSSL product
11i Admin Depot `/var/depot/ids_11i_admin` For an HP-UX 11i system supporting the HIDS administration software	• Required Java patches • JRE 6.0 • `IDS.IDS-ADM-RUN` and `IDS.IDS-ADM-SHLIB` subproduct • `IDS.IDS-ENG-A-MAN` subproduct • OpenSSL product
11i Agent Depot `/var/depot/ids_11i_agent` For an HP-UX 11i system supporting the HIDS agent software	• Required system patches • `IDS.IDS-AGT-RUN` subproduct • `IDS.IDS-ENG-A-MAN` subproduct • `IDS-KRN` subproduct • OpenSSL product

Creating the depot directory

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.
2. If it does not exist, create the base directory for the depots as follows:

   ```
   # mkdir /var/depot
   ```

Get the HP-UX HIDS product

HP-UX HIDS v4.8 for HP-UX 11i v3 is available from the HP Software Depot (http://software.hp.com)

From the HP-UX 11i v3 system versions

Refer to the *HP-UX 11i Version 3 Installation and Update Guide* for information on installing HIDS with a system installation or upgrade. If the system is already installed, you can use the method described in "From an Application Release CD " (page 12) to complete the installation.

From the HP Software depot

1. Log in as superuser (`root`) on the depot system; see "Creating the depot directory" (page 11).
2. Open the HP Software Depot Website:

   http://software.hp.com. Choose the "Security and Manageability" section, and under this section, select the "HP-UX Host Intrusion Detection System (HP-UX HIDS)" product.
3. Using the instructions on the Website, download the 11i product depot into `/var/tmp/HP-UX HIDS_11i.depot`.

4. Copy the HP-UX HIDS product to your administration and agent depots, as appropriate.
   a. • 11i Agent Depot

      Copy the `11i IDS-KRN` product and `IDS` agent subproducts into the `ids_11i_agent` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS-KRN 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, copy the 11i administration subproducts into the `ids_11i_admin` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/idsprod/HPUX-HIDS_11i.depot IDS.IDS-ADM-RUN
      IDS.IDS-ENG-A-MAN IDS.IDS-ADM-SHLIB @ /var/depot/ids_11i_admin
      ```

   c. • 11i Admin+Agent Depot

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

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/idsprod/HPUX-HIDS_11i.depot * @
      /var/depot/ids_11i_admin+agent
      ```

From an Application Release CD

1. Log in as superuser (`root`) on the depot system. See "Creating the depot directory" (page 11).
2. Do the following:

   Locate the HP-UX 11i Application Release CD that contains the HP-UX HIDS product bundle and load it into your CD reader. In this procedure it is mounted on `/SD_CDROM`.

   a. • 11i Agent Depot

      Copy the `11i IDS-KRN` product and `IDS` agent subproducts into the `ids_11i_agent` depot:

      ```
      # # swcopy -x enforce_dependencies=false -s
      /SD_CDROM HPUX-HIDS.IDS-KRN HPUX-HIDS.IDS.IDS-AGT-RUN
      HPUX-HIDS.IDS.IDS-ENG-A-MAN @ /var/depot/ids_11i_agent
      ```

   b. • 11i Admin Depot

      If your administration system is not running an agent, copy the 11i administration subproducts into the `ids_11i_admin` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /SD_CDROM HPUX-HIDS.IDS.IDS-ADM-RUN HPUX-HIDS.IDS.IDS-ENG-A-MAN
      HPUX-HIDS.IDS.IDS-ADM-SHLIB @ /var/depot/ids_11i_admin
      ```

   c. • 11i Admin + Agent Depot

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

      ```
      # swcopy -x enforce_dependencies=false -s
      /SD_CDROM HPUX-HIDS.IDS-KRN HPUX-HIDS.IDS @
      /var/depot/ids_11i_agent
      ```

Get patches for Java

1. Log in as superuser (`root`) on the depot system. See "Creating the depot directory" (page 11).
2. Create a directory in which you can save the patches and make a depot. This procedure uses `/var/tmp/javapatch`.

3. Open the HP Java Website:
   http://www.hp.com/go/java,
4. Click the patches link.
5. Take note of the patches that you need, based on your administration system.
6. Open the HP Support Website: http://www.hp.com/go/hpsc
7. Click on individual patches.
   You must be registered before you can download patches.
8. Using the instructions on the Website, download the 11i Java patches into /var/tmp/javapatch.
   Some patches might have dependency patches (patches that must be installed first). Click the dependency links and download the dependency patches as well.
9. Unpack the patch file sets:
   ```
   # sh -c 'for i in /var/tmp/javapatch/PH*; do sh $i; done'
   ```
10. Copy the patch file sets into your administration depot using *one* of the following steps:
    a. • 11i Admin Depot
       If your administration system 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 -x enforce_dependencies=false -s $i  *  @
       /var/depot/ids_11i_admin; done'
       ```
    b. • 11i Admin + Agent Depot
       If your administration system *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 -x enforce_dependencies=false
       -s $i  * @ /var/depot/ids_11i_admin+agent; done'
       ```

Get Java software

1. Log in as superuser (root) on the depot system. See "Creating the depot directory" (page 11).
2. Open the HP Java Website:
   http://www.hp.com/go/java.
3. Select JDK and JRE 6.0(latest release 6.0.xx) link for the appropriate platform (Itanium or PA-RISC).
4. Click downloads.
5. Download JDK or JRE. JRE is sufficient and is a smaller depot.
6. Using the instructions on the Website, download the software, for example, to /var/tmp/jre6_16006_ia.depot for 11i v3.

7. Transfer the software to the administration depot using one of the following steps:
   a. • 11i Admin Depot

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

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/jre6_16006_ia.depot  * @
      /var/depot/ids_11i_admin
      ```

   b. • 11i Admin + Agent Depot

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

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/jre6_16006_ia.depot  * @
      /var/depot/ids_11i_admin+agent
      ```

Get OpenSSL software

In addition to Java, you must also download OpenSSL on your system. OpenSSL A.00.09.07l/A.00.09.08d is the latest version of the software.

Following are the steps to download the OpenSSL software:

1. Log in as superuser (`root`).
2. Insert the software CD into the appropriate drive, if you are downloading OpenSSL from the Application Software CD.
3. Download the software to the `/var/tmp/openssl.depot` directory.
4. Transfer the software to the depot using one of the following steps:
   a. • 11i Agent Depot

      Copy the OpenSSL software into the `ids_11i_agent` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/openssl.depot  * @  /var/depot/ids_11i_agent
      ```

      • 11i Admin Depot

      If your administration system is not running an agent, copy the OpenSSL software into the `ids_11i_admin` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/openssl.depot  * @  /var/depot/ids_11i_admin
      ```

   b. • 11i Admin + Agent Depot

      If your administration system is running an agent, copy the OpenSSL software into the `ids_11i_admin+agent` depot:

      ```
      # swcopy -x enforce_dependencies=false -s
      /var/tmp/openssl.depot  * @  /var/depot/ids_11i_admin+agent
      ```

IMPORTANT: If you have an Internet Express OpenSSL 0.9.7c software installed on your system, you cannot upgrade to OpenSSL A.00.09.07l. You must remove the Internet Express OpenSSL 0.9.7c software before installing OpenSSL A.00.09.07l/A.00.09.08d.

Installing depots

This section describes the procedure to install the depot.

NOTE: In the following procedure, `swinstall` does not reinstall any patches or applications that are already installed. You can ignore messages to that regard. The software you need will be installed properly. *Do not reinstall any patches without consulting HP Support first.*

The `swinstall` option `-x autoreboot=true` in the following procedure 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 v4.8 reboot my agent system?" (page 15).

1. Log in as superuser (`root`) on the HP-UX HIDS administration system.
2. Make sure you are the only user on the system, since the installation might require a reboot.
3. On your administration system, install one of the admin software depots described in "Making depots" (page 10), as follows:
   a. • 11i Admin Depot

      Install the `ids_11i_admin` depot (a reboot *may* occur):

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

   b. • 11i Admin and Agent Depot

      Install the `ids_11i_admin+agent` depot (a reboot *may* occur):

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

   IMPORTANT: Make sure to run `swinstall` with dependencies enforced (i.e., do NOT invoke `swinstall` with "`-x enforce_dependencies=FALSE`) to prevent unusable software from being installed on the system.

4. On each of your agent systems, install one of the agent software depots described in "Making depots" (page 10), as follows:
   a. Log in as superuser (`root`) on each HP-UX HIDS agent system.
   b. Install the `ids_11i_agent` agent depot (a reboot may occur):

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

Will installing HP-UX HIDS v4.8 reboot my agent system?

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

1. If you choose the Reinstall Filesets option in the graphical interface to `swinstall`, all HIDS filesets will be installed, and a system reboot *will* occur.
2. If you pass the `-x reinstall=true` option to the command-line invocation of `swinstall`, all HIDS filesets will be installed, and a system reboot *will* occur.
3. If you are installing HP-UX HIDS v4.8 on a system for the first time (a fresh install), a reboot *will* occur.

Table 5 Reboot matrix

Update from:	Update to Version 4.8
Not installed	Reboot
Version 4.7	No Reboot
Version 4.4	No Reboot
Version 4.3	No Reboot

Table 5 Reboot matrix *(continued)*

Update from:	Update to Version 4.8
Version 4.2	No Reboot
Version 4.1	No Reboot
Version 4.0	No reboot
Version 3.1	No Reboot

Postinstallation

- The HP-UX startup in progress list should display OK for the Starting 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 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" (page 16).
- 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. It also checks that all the *necessary* and superseding patches (or patches that supersede them) have been installed although it does not verify if a patch has a superseding patch.

Configuration

After 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 of *Host Intrusion Detection System Administrator Guide, Software Release 4.8*. The following is an annotated list of some of the sections in chapter 2 of that guide.

Required

Before you can run HP-UX HIDS, you must complete the configuration step described in the section "Setting Up the HP-UX HIDS Secure Communications" in the Host Intrusion Detection System Administrator Guide.

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

If you are upgrading from HIDS v 2.x or v3.x, your old keys and certificates are preserved.

Optional

You might also need to complete one or more of the following steps:

- Configuring a multihomed agent system

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

- Configuring a multihomed administration system

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

- Enabling over 23 agents (Thread Limits)

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

- Working with firewalls

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

- Working with NIS

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

3 New and changed features

HP-UX HIDS v4.8 is updated to provide the fix for POODLE vulnerability.

4 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

Perform updates instead of cold reinstalls

HP-UX HIDS is designed to support updates. If users cold reinstall the newer version by first removing the older version (`swremove`), two reboots (instead of just one or possibly none) will occur and there is the possibility of losing some 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 or readable causes the agent to fail security checks and to exit. Changing file permissions also results in `swverify` errors.

Known problems and limitations

The following problems and limitations are applicable for HIDS v4.8 release.

The GUI schedule manager does not validate modifications to pathnames_X/programs_X template properties

The GUI Schedule Manager saves modifications made to the template properties in Surveillance Groups without validating that the Surveillance Schedules and Groups can be successfully parsed. Incorrect modifications to the Surveillance Schedules and Groups, including incorrect modifications to template property values, are only detected when the GUI System Manager attempts to activate the schedule or when the GUI System Manager is restarted and attempts to load the schedules.

If a Surveillance Group is not successfully parsed when the GUI System Manager is started, the group is removed from the schedule and the group will not appear in the Schedule Manager window. If a schedule contains only the group that was removed, then the GUI System Manager displays an error dialog stating that it was unable to parse the schedule and the schedule will not appear in the System Manager and Schedule Manager windows.

The following scenarios illustrate instances where the GUI Schedule Manager allows administrators to make and save invalid modifications to pathname_X/program_X filter template properties:

Example 1 Invalid modification - Scenario 1

In this example, the GUI Schedule Manager allows the administrator to enter an unequal number of `pathnames_X` and `programs_X` pathname groups:

```
pathnames_1 | file1 & file 2 | file3 | file4
programs_1 | prog1 | prog2
```

However, the administrator will not be able to activate the schedule as there is no corresponding program for `file4`.

Example 2 Invalid modification - Scenario 2

In this example, the GUI Schedule Manager allows the administrator to enter an empty pathname or program when editing a `pathnames_X` or a `programs_X` template property:

```
pathnames_1 | file1 |   | file2
programs_1 | prog1 | prog2
```

As there is no valid pathname value between the two pipe delimiters , the GUI Schedule Manager fails to parse the schedule when the administrator tries to activate it.

Diagnosing the problem

Run the `idsadmin --activate <schedule name>` command to print useful diagnostic information, including the line number of the schedule file entry that caused a parsing error. The `idsadmin` command provides detailed error messages that can help administrators diagnose and resolve the problem.

IMPORTANT: The GUI System Manager must be closed before directly editing a Surveillance Schedule or Group in a text editor. Otherwise, changes made using an editor will be overwritten by the GUI System Manager when it exits.

TIP: HP recommends that administrators backup copies of Surveillance Schedules and Groups files periodically in case they need to be restored.

Incorrectly formatted raw reports sent as an Email

Reports in `raw` format that are generated in `/var/opt/ids/reports` are formatted correctly. However, if the `raw` report is sent to an email address using the `--email-to` option, then the report may not be formatted correctly. For example, long entries in a `raw` report can be broken up across multiple lines, and reports generated when specifying the `:` character as a delimiter (using the `--report-delimiter` option) may not include the first few entries.

Special characters not supported when specifying filters using the `tune` command

The pound (#) and pipe (|) characters are currently not supported for specifying filters when using the `tune` command. Use of these characters can cause parsing errors.

The `idsadmin` command does not parse schedules whose property lines exceed 65535 characters

If a schedule has a property line exceeding 65535 characters, `idsadmin` or `idsagent` does not parse the schedule but logs an error message. In older versions of HIDS, running these commands on schedules with property lines exceeding 65535 characters can cause HIDS to dump core.

Limitation when using `idsadmin` in interactive mode

After an `idsadmin tune` or `report` command is executed, and if `idsadmin` had established a connection with an agent before the `tune` or `report` command was invoked, `idsadmin` no longer has a connection to that agent. A status command will reestablish a connection to that agent.

The idsadmin tool cannot monitor more than one agent at a time

The `idsadmin` tool does not monitor or display alerts in near real-time from multiple agents at the same time. The `idsadmin` tool can only monitor and display alerts from one agent at any given time. To view alerts for multiple agents at the same time, you must use the GUI System Manager or use the `idsadmin --report` command to generate a consolidated alert report across multiple agents.

Display of schedules created using earlier versions of HIDS

The GUI System Manager does not display v4.0 or v3.x text schedules that were placed in `/etc/opt/ids/schedules` unless these schedules are migrated to HIDS v4.1 or HIDS v4.2 or HIDS v4.3 or HIDS v4.4. For more information on migrating schedules, see "Migrating schedules from older versions of HIDS" (page 10)

The migrator tool does not update `suppression_targets_to_ignore` properly

When migrating schedules from 4.0, the migrator tool does not escape the `.` character present in the pathname of the default files (for example, `.rhosts`) for which alerts are not suppressed. After migration, you must manually insert the `\` character if you do not want to suppress the alerts for these files.

Limitation while using the `ids.cf` file for configuring duplicate alert suppression

In the `/etc/opt/ids/ids.cf` file, non-commented lines in a `[ENVIRONMENT] ... [END]` section cannot be preceded by commented lines. For example, if you want to configure duplicate alert suppression through the `ids.cf` file, you must place the `SUPPRESSION` line before any commented lines as shown in the following example:

```
[ENVIRONMENT]
IDS_USER ids
ALLOW_DUMPS 1
#AGGREGATION 0 # 0(1) to turn alert aggregation off(on).
#SUPPRESSION 0 # 0(1) to turn duplicate alert suppression off(on).
#SUPPRESSION_REPORT 0 # 0(1) to turn reporting of suppressed alerts off(on).
# # these flags overrides flags in schedule file
[END]
```

To enable duplicate alert suppression, move it to the line before the first commented line of the section and uncomment it as shown below:

```
[ENVIRONMENT]
IDS_USER ids
ALLOW_DUMPS 1
SUPPRESSION 0 # 0(1) to turn duplicate alert suppression off(on).
#AGGREGATION 0 # 0(1) to turn alert aggregation off(on).
#SUPPRESSION_REPORT 0 # 0(1) to turn reporting of suppressed alerts off(on).
# # these flags overrides flags in schedule file
[END]
```

Unexpected behavior by `idsagent` when `report`, `resync`, or `tune` command is executed

If the `/var/opt/ids/gui/logs/{agent}_alert.log` file is corrupted, the `report`, `resync`, or `tune` commands may behave unexpectedly.

SSH does not perform a clean exit after `idsagent` is started

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

```
ssh -l root <machine> /usr/dt/bin/dtterm
```

Then, run the `/sbin/init.d/idsagent start` commands interactively.

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, “Configuring HP-UX HIDS,” in the *Host Intrusion Detection System Administrator Guide*.

Dropped kernel audit records

Depending on the system profile and product configuration, and under heavy loads, 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 the frequency that reminder notices are sent and the point at which a notice is sent when audit records are no longer being dropped, respectively. For more information see Appendix E, “The Agent Configuration File,” in the *Host Intrusion Detection System Administrator Guide*.

Time units cannot be specified for template properties in schedule manager

In the Schedule Manager’s template property editing windows, you can not specify time unit (For example, s = seconds, m = minutes, d = days, w = weeks) for template property time values. Some time-related template properties are interpreted as being in seconds (example, the `fail_interval` and `warning_interval` properties for the Repeated Failed Logins template), while other properties are interpreted as being in minutes (for example, the `fail_interval` property for the Repeated Failed su commands template).

Schedules that contain username template values cannot be run by Version 3.x agents

Starting with HIDS 4.0, user names and user IDs can be specified for user template properties such as `users_to_monitor` and `priv_user_list`. HIDS v3.x supports only user IDs values for these user template properties, therefore schedules that contain user names instead of user IDs cannot be run by v3.x agents. The schedules should only specify user IDs values for these user template properties if they are to be run by both v3.x and v4.0 (or later) agents.

Error log file rotation

When you rotate an agent’s error log file (default location is `/var/opt/ids/error.log`), the idsagent process must be restarted by sending it a HUP signal in order for all new errors to appear in a newly created error log file.

The `swverify` command reports error after removing the IDS Agent or the IDS Admin Sub-product from a server that has HIDS bundle installed

After installing HP-UX HIDS v4.3 on a server, and if IDS Agent™ (IDS-AGT-RUN fileset) or `IDS Admin` (IDS-ADM-RUN and IDS-ADM-SHLIB filesets) sub product is removed from the installation, the `swverify IDS` command report displays the following error message:

ERROR: File "/opt/ids/lbin/ssl-tool" missing. ERROR: Fileset "IDS.IDS-AGT-RUN,l=/opt/ids,r=F.04.03.01" had file errors.

NOTE: Similar error will be displayed if `IDS Agent` sub product is removed from the server.

5 Related documentation

Documentation

HP-UX HIDS documentation includes manuals, manpages, information on HP OpenView SMART Plug-In, and HP Support Center.

Manuals

The following document is available at the HP technical documentation Website HIDS documents and on the Instant Information CD in the Internet and Security Solutions collection.

HP Part No.	Title
766144-002	*HP-UX Host Intrusion Detection System Version 4.8 Administrator Guide.*

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
`/opt/ids/share/man/man1m`	• *IDS_checkAdminCert*(1M) • *IDS_checkAgentCert*(1M) • *IDS_checkInstall*(1M) • *IDS_genAdminKeys*(1M) • *IDS_genAgentCerts*(1M) • *IDS_importAgentKeys*(1M) • *idsadmin*(1M) • *idsagent*(1M) • *idsgui*(1M)
`/opt/ids/share/man/man4m`	• *ids.cf*(4) • *idsschedule*(4)

HP OpenView SMART Plug-In

The OVO HPUX_HIDS-SPI has been certified by HP for OVO V5.x as well as V6.x, and is known to work with OVO V7.1. A future HPUX_HIDS-SPI version is being planned for certification with OVO V8.

HP Support Center

Get help from your peers in the HP Support Center (HPSC). It is available at:

http://www.hp.com/go/hpsc

Support Model

In the future, HP-UX HIDS customers will receive maintenance versions and minor versions of the product, instead of individual patches for various defect fixes. HP recommends that customers adopt the latest version to take advantage of defect fixes and new functionalities.

The support model, in light of this approach (product versions instead of individual patches) is:

- The latest maintenance or minor version is the actively supported version.

- Customers using a prior major version (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 the problem they are experiencing has been corrected in the latest version. Specifically, this means that v4.8 is now the actively supported version on HP-UX 11i v3 and all previous versions are supported on a best-effort basis.

NOTE: Support for version 2.x of HP-UX HIDS was discontinued on March 31, 2007. HP recommends that all customers using HP-UX HIDS v2.x upgrade to v4.8. For more information about discontinuance, see http://www.hp.com/softwarereleases/releases-media2/discon/index.htm.

Localization

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

6 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Support policy for HP-UX

For more information about support policy for HP-UX, see HP-UX support policy.

A HP Software license

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 OPENSSL 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.

OpenSSL license

```
  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.

OpenSSL License
---------------

/* ====================================================
==========
* Copyright (c) 1998-2006 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

```
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 rouines 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 many 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.