

HP-UX Bastille Version B.3.2 Release Notes



HP Part Number: 5992-5039A
Published: October 2009
Edition: 1

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Confidential 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. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Table of Contents

1	About this product.....	5
1.1	Features and benefits.....	5
1.2	Support.....	6
2	New features in this release.....	7
2.1	Greater coverage of the CIS HP-UX security benchmark.....	7
2.2	Reporting enhancements.....	7
2.3	Bug fixes in this release.....	7
3	Installing HP-UX Bastille.....	9
4	Known issues and workarounds.....	11
4.1	Changes made by HP-UX Bastille might cause other software to stop working.....	11
4.2	Cannot use X because \$DISPLAY is not set.....	11
4.3	System is in original state.....	11
4.4	HP-UX Bastille must be run as root.....	11
4.5	Problems opening, copying, or reading files.....	11
4.6	Errors related to individual configuration files.....	11
4.7	HP Secure Shell locks you out of your system immediately when passwords expire.....	11
4.8	HP-UX Bastille configures a firewall using IPFilter.....	11
4.9	Security Patch Check.....	11
4.10	Rerun HP-UX Bastille after installing new software or applying new patches.....	12
4.11	Diagnostic tips.....	12
5	Support and other resources.....	13
5.1	Contacting HP.....	13
5.1.1	Before you contact HP.....	13
5.1.2	HP contact information.....	13
5.1.3	Subscription service.....	13
5.1.4	Documentation feedback.....	13
5.2	Related information.....	13
5.3	Typographic conventions.....	14

1 About this product

HP-UX Bastille is a system hardening and reporting program that enhances the security of the HP-UX operating system by consolidating essential hardening and lock-down checklists from industry and government security organizations, and making them accessible to administrators in an easy to use package. The HP-UX Bastille GUI interface guides users through creating a custom security configuration profile. The policy configuration engine hardens HP-UX to specification by locking down each selected security item. Security items include:

- Configuring daemons, services, firewalls, and client software to use more secure settings
- Disabling unused or unneeded `inetd` services
- Creating `chroot` jails for commonly used server programs
- Assessing the current HP-UX system against all relevant lock-down items with the reporting feature
- Applying saved configuration profiles to multiple similar machines with a command-line batch mode

These HP-UX Bastille features ease compliance with regulatory requirements and industry-consensus security benchmarks like the Center for Internet Security (CIS) benchmark. HP-UX Bastille also facilitates internal and external security audits.



NOTE: HP-UX Bastille is built from the open-source, cross-platform software program Bastille. HP made significant contributions to the open-source Bastille software over many years. The original Linux version is now named Bastille-Linux to avoid confusion with other cross-platform implementations, and is not covered by this document.

1.1 Features and benefits

HP-UX Bastille provides the following features and benefits:

- Locks down the system
 - Increases security by configuring daemons and system settings
 - Turns off unnecessary services such as `pwgrd`
 - Assists with creation of `chroot` jails to partially limit the vulnerability of common internet services such as web servers and DNS
 - Configures automatic runs of Software Assistant (SWA) or Security Patch Check
 - Configures an IPFilter-based firewall
- Provides an interactive, wizard-style GUI interface
 - Guides users to optimize the trade off between security, usability, and functionality
 - Explanatory text helps less experienced administrators make appropriate security decisions
- Reports security configuration state
 - Generates reports in HTML, text, and `config` file format
 - Establishes a baseline for comparison to later configuration differences with the `bastille_drift` command
- Returns the security configuration to the state before HP-UX Bastille was run with the `revert -r` feature.
 - Provides a safety net in case of unexpected incompatible changes when hardening running systems
- Integrates with HP Systems Insight Manager (SIM)
 - Locks down and reporting available from SIM menus
 - `SIM.config` pretested configuration for SIM server lock down

- Install-time Security (ITS) for Ignite-UX and Update-UX
 - Applies predefined HP-UX Bastille security configuration profile during first system boot
 - Enables out-of-the-box security by avoiding any vulnerability window after initial install

1.2 Support

For customers with an HP-UX support agreement, technical support is available through the HP World Wide Response Centers at www.hp.com/support. Support is also offered through the IT Resource Center at www.itrc.hp.com.

For the HP-UX discussion forum, from the ITRC home page click **Forums**→**HP-UX**→**Security**. Or, the direct link is [ITRC Forums Security](#).

The Bastille discussion list is available to the open source and user communities at:

<https://lists.sourceforge.net/lists/listinfo/bastille-linux-discuss>.

If you find a security vulnerability associated with HP-UX Bastille, report it at: http://welcome.hp.com/country/us/en/sftware_security.html.

HP-UX Bastille can potentially make changes that affect the functionality of other software. If you experience problems after applying Bastille changes to your system, be sure your support contact knows that you run Bastille on your system.

2 New features in this release

2.1 Greater coverage of the CIS HP-UX security benchmark

Expanded security hardening choices allow you to lock down your systems in alignment with the latest Center for Internet Security (CIS) Benchmark for HP-UX or other similar security hardening standards.

2.2 Reporting enhancements

To report on the overall security configuration state of a system, HP-UX Bastille offers an assessment-only mode that evaluates the security status for each hardening question, and generates a summary report for all questions.

Scored assessment reports provide a concise summary of compliance against a desired standard. For example, a weights file that selects the lock-down items used with a particular industry standard can be used for comparison against the system status.

2.3 Bug fixes in this release

- QXCR1000965106 – Module question `AccountSecurity.gui_login` reported as unanswered during lock down.
- QXCR1000965123 – Invalid parameter in shutdown script for TPS service, `XPRINTSERVERS`.
- QXCR1000965135 – Configuration item `MiscellaneousDaemons.nfs_core` not recognized by GUI or in lock down.
- QXCR1000965178 – Configuration items: `nisplus_server` and `nisplus_client` not reported correctly.
- QXCR1000965179 – Configuration item `screensaver_timeout` does not set timeout value properly.

3 Installing HP-UX Bastille

HP-UX Bastille is included as recommended software on the Operating Environment media and can be installed and run with Ignite-UX or Update-UX. HP-UX Bastille is installed by default, and a manual installation is only necessary to obtain the latest version from the web. For more information on installing HP-UX Bastille, see the *HP-UX Bastille Version B.3.2 User Guide* at <http://docs.hp.com/en/internet.html>.

The following prerequisites are required to install HP-UX Bastille:

- Root access
- HP-UX 11i v3 or HP-UX 11i v2
- HP compiled version of Perl D.5.8.0.D or later

Perl is available for download at:

<http://www.hp.com/go/perl>

- 1 MB disk space
1. To download the latest version of HP-UX Bastille, see the following website:

<http://www.hp.com/go/bastille>

2. Run the installation command:

```
# swinstall -s <path to depot> HPUXBastille
```

4 Known issues and workarounds

4.1 Changes made by HP-UX Bastille might cause other software to stop working

To revert the system to the state it was in before you ran HP-UX Bastille:

```
# bastille -r
```

This command confirms that the problem has been eliminated.

4.2 Cannot use X because `$DISPLAY` is not set

The user requests the X interface, but the `$DISPLAY` environment variable is not set. Set the environment variable to the desired display to correct the problem.

4.3 System is in original state

The user attempts to revert changes with the `-r` option, but there are no changes to revert.

4.4 HP-UX Bastille must be run as root

HP-UX Bastille must be run as the root user because the changes it makes affect system files.

4.5 Problems opening, copying, or reading files

Error messages citing problems performing these operations are usually related to NFS file systems that do not trust the root user on the local machine. Consult the options section in the *fstab* manpage for details.

4.6 Errors related to individual configuration files

Errors about individual configuration files indicate:

- That a system is too heavily modified for HP-UX Bastille to make effective changes.
- That the files, locations, or permissions of the HP-UX Bastille installation directories have been changed.

4.7 HP Secure Shell locks you out of your system immediately when passwords expire

You might need PAM patch: PHCO_24839 (HP-UX 11.11) available at the HP IT Resource Center:

<https://www2.itrc.hp.com/service/patch/mainPage.do>

4.8 HP-UX Bastille configures a firewall using IPFilter

The most common conflicts are with firewalls. When a network service that HP-UX Bastille did not turn off explicitly is not working, verify the firewall rules pass the ports needed. For more information, see *ipfstat(8)* and *ipmon(8)*.

4.9 Security Patch Check

Security Patch Check is being deprecated in favor of SWA.

4.10 Rerun HP-UX Bastille after installing new software or applying new patches

Installing new software or applying new patches might change the system state. On HP-UX, if vendor-specific fix scripts are run with `swverify` using either the `-x fix=true` option or the `-F` option, then HP-UX Bastille should be rerun.

4.11 Diagnostic tips

When troubleshooting issues with HP-UX, remember these tips:

- To revert changes:
`# bastille -r`
- To list the current config file:
`# bastille -l`
- Locate the list of all actions performed by HP-UX Bastille at `/var/opt/sec_mgmt/bastille/log/action-log`
- Use the following files to help diagnose problems:
 - `/var/opt/sec_mgmt/bastille/log/action-log`
 - `/var/opt/sec_mgmt/bastille/log/error-log`
 - `/etc/opt/sec_mgmt/bastille/config`

5 Support and other resources

5.1 Contacting HP

5.1.1 Before you contact HP

Be sure to have the following information available before you contact HP:

- Technical support registration number (if applicable)
- Product serial number
- Product identification number
- Applicable error message
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

5.1.2 HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (<http://welcome.hp.com/country/us/en/wwcontact.html>).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
 - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
 - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (<http://www.hp.com/hps>).
- In other locations, see the Contact HP worldwide (in English) webpage (<http://welcome.hp.com/country/us/en/wwcontact.html>).

5.1.3 Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website: http://www.hp.com/country/us/en/contact_us.html

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

5.1.4 Documentation feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to feedback@fc.hp.com. Include the document title and manufacturing part number. All submissions become the property of HP.

5.2 Related information

The HP-UX Bastille website:

<http://www.hp.com/go/bastille>

At <http://docs.hp.com>:

- *HP-UX Bastille Version B.3.2 User Guide*:
<http://docs.hp.com/en/internet.html>

- *HP-UX 11i v3 Installation and Update Guide: HP Integrity Servers and HP 9000 Servers* (Chapter 3 – Security Considerations):
<http://docs.hp.com/en/oshpux11iv3.html>
- *HP-UX System Administrator's Guide: Security Management: HP-UX 11i Version 3* (Chapter 3 – HP-UX Bastille):
<http://docs.hp.com/en/oshpux11iv3.html>
- *HP-UX 11i Version 3 March 2009 Release Notes: Operating Environments Update Release* (Chapter 8 – HP-UX Bastille and Install Time Security):
<http://docs.hp.com/en/oshpux11iv3.html>

HP-UX Bastille manpages:

- *bastille(1M)* in *HP-UX 11i v3 Reference 1M System* at:
http://docs.hp.com/en/hpuxman_pages.html
- *bastille_drift(1M)* in *HP-UX 11i v3 Reference 1M System* at:
http://docs.hp.com/en/hpuxman_pages.html

The HP-UX Security Forum is offered through the HP IT Resource Center (ITRC) at:
[ITRC Forums Security](#)

Product specifications and download:

<http://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6849AA>.

For more information about HP-UX Bastille compatibility with Serviceguard, see the Serviceguard documentation available at:

<http://docs.hp.com/en/netsys.html>.

The IPFilter-SG rules are documented in the *HP-UX IPFilter Version 17 Administrator's Guide*. IPFilter documentation is available at:

<http://docs.hp.com/en/internet.html>

5.3 Typographic conventions

This document uses the following typographical conventions:

<code>%</code> , <code>\$</code> , or <code>#</code>	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells. A number sign represents the superuser prompt.
<code>audit(5)</code>	A manpage. The manpage name is <i>audit</i> , and it is located in Section 5.
Command	A command name or qualified command phrase.
Computer output	Text displayed by the computer.
Ctrl+x	A key sequence. A sequence such as Ctrl+x indicates that you must hold down the key labeled Ctrl while you press another key or mouse button.
ENVIRONMENT VARIABLE	The name of an environment variable, for example, <code>PATH</code> .
[ERROR NAME]	The name of an error, usually returned in the <code>errno</code> variable.
Key	The name of a keyboard key. Return and Enter both refer to the same key.
Term	The defined use of an important word or phrase.
User input	Commands and other text that you type.

<i>Variable</i>	The name of a placeholder in a command, function, or other syntax display that you replace with an actual value.
[]	The contents are optional in syntax. If the contents are a list separated by , you must choose one of the items.
{}	The contents are required in syntax. If the contents are a list separated by , you must choose one of the items.
...	The preceding element can be repeated an arbitrary number of times.
Ⓢ	Indicates the continuation of a code example.
	Separates items in a list of choices.
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task.
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

