HP System Management Homepage Release Notes

HP-UX, Linux, and Windows Operating Systems

Table of Contents

List of Tables

1 Features

HP System Management Homepage (HP SMH) is a web-based interface that consolidates and simplifies single system management for HP servers running the HP-UX, Linux, and Windows operating systems. HP SMH aggregates and displays data from Web Agents and other HP Web-enabled System Management Software that includes:

- HP Insight Diagnostics
- Array Configuration Utility
- HP Software Version Control Agents

The HP System Management Homepage (HP SMH) for HP-UX, Linux, and Windows provides the following features. They apply to all releases, except where noted.

Product features

- Provides security for HP Insight Management Agents using the Secure Sockets Layer (SSL) for Linux and Windows.
- Provides web-based applications and security using SSL.
- Enables you to configure the trust mode level.
- Manages the user system access through the user group account.
- Displays all HP Web-enabled System Management Software that provides information to HP SMH.
- Common HTTP and HTTPS service for HP Insight Management Agents and utilities, for reduced complexity and system resource requirements.
- Simplified architecture for implementing HTTP security and HP management updates.
- Access control through Network Interface Card (NIC) binding and advanced configuration features for individual and groups of users.
- Broad operating system and browser support.
- Automated log collection via `smhassist`.

  This feature is available only on HP-UX 11i v2 and HP-UX 11i v3 systems.

- Command Line Interface (CLI) - `smhconfig` - provides users with administrator rights access to set values through the command line.
- Facility to disable port 2301.
- Logging into `syslog` the activities related to login and logout performed on HP SMH.

  This feature is available only on HP-UX 11i v2 and HP-UX 11i v3 systems.

- Consolidated API logging for HP SMH and WebApps: Provides an option to log the critical and major events of both the HP SMH and its WebApps to the system log for viewing and auditing.

Partition Manager

To start Partition Manager, a user with Administrator (root) privileges can run the `parmgr` command with the `-b` option to bypass the authentication step under HP SMH. To use this feature on HP-UX 11i v1, you must install `KRNG11i`, the Strong Random Number Generator software for HPUX 11i v1, available from the Software Depot web site at **http://www.hp.com/go/softwaredepot**.

Available IP addresses

In HP-UX only, when autostart mode is enabled, any access made through port 2301 detects a change in the list of available IP addresses. In previous releases, SMH would only be accessible using the IP addresses defined at system startup. If new IP addresses were defined then SMH would have to be restarted to use them.

With this new SMH feature, any configuration change in the list of available IP addresses, in clustered and non-clustered environments, would automatically reconfigure SMH, restarting it when needed. Environment changes such as enabling a new network card, adding ifconfig aliases, or a cluster package failover would trigger this feature.

Alternatively, you can disable this feature by adding the following line to the `/opt/hpsmh/conf.common/smhpd.xml` file: `<monitor-ip-changes>0</monitor-ip-changes>`

For more information, go to the *Distributed Systems Administration Utilities V1.1 Release Notes for HP-UX 11i v2 March 2006* at **http://www.hp.com/go/hpux-core-docs** and select HP-UX 11i v2 from the product list.

Integrated applications to HP SMH

HP SMH is a framework for a number of integrated applications. HP SMH provides the following system management functionality (described in "HP SMH integrated applications" (page 8)) through a single-user interface and the HP SMH Graphical User Interface (GUI).

IMPORTANT: In HP SMH on HP-UX, there are some applications such as Authenticated Commands (PAM), Resource Management, and Network Services Configuration that are not web-based. To access such applications from SMH, an X-windows application must be running on the computer whose IP address you enter in the **DISPLAY** text box in the application's launch page.

Table 1-1 HP SMH integrated applications

Application Name	Operating System	Application Description
Accounts for Users and Groups (ugweb)	HP-UX	The Accounts for Users and Groups (ugweb) tool is a web-based single-system management tool for managing user accounts and groups on a local system, a Network Information Service (NIS) system, and an LDAP (Lightweight Directory Access Protocol) server. For more information, see the product's online help.
Auditing and Security Attributes Configuration (secweb)	HP-UX	The HP-UX Auditing and Security Attributes Configuration tool is a tool for configuring and managing security attributes, and for configuring and managing the auditing subsystem without having to convert the system to Trusted mode. For more information, see the product's online help.
Authenticated Commands (PAM)	HP-UX	Using Pluggable Authentication Modules (PAM), configure account authentication, password authentication, session authentication, and user authentication.
Disks and File Systems (fsweb)	HP-UX	The Disks and File Systems (fsweb) tool supports system administration tasks, including management of logical groups and volume groups, disk management tasks, and file system tasks. The fsweb tool supports these file systems: Cache File System (CFS), Compact Disc File System (CDFS), Common Internet File System (CIFS), Hierarchical File System (HFS), Network File System (NFS), and Veritas File System (VxFS). For more information, see the product's online help.
Distributed System Authentication Utilities (DSAU)	HP-UX	Distributed Systems Administration Utilities provide several tools for simplifying the management of groups of systems and Serviceguard clusters. Configure configuration synchronization, consolidated logging, and view system logs.
Event Monitoring Service (web-based) (EMSweb)	HP-UX	The EMSWeb tool (bundle EventMonitorGUI) enables the user to manage requests to monitor resources on the system. Using the EMSWeb tool the user can create and manage requests to monitor resources.

Application Name	Operating System	Application Description
Error Management Technology (EMT)	HP-UX	Error Management Technology provides a quick, easy method of accessing error/cause/action information on all system errors. Use it to query or customize error data.
EVWEB	HP-UX	EVWEB is a user component of System Fault Management (SFM). Using evweb, you can view and administer various Web-Based Enterprise Management (WBEM) events that are generated on an HP-UX system. For more information, see the product's online help.
IPMI Event Viewer	HP-UX	View hardware events.
Kernel Configuration (kcweb)	HP-UX	The kcweb tool allows the user to configure an HP-UX kernel and to monitor consumption of kernel resources controlled by parameters. For more information, see the product's online help.
Network Interfaces Configuration	HP-UX	Network Interfaces Configuration is a web-based system management tool that enables you to configure network interfaces on HP-UX installed systems. For more information, see the product's online help.
Network Services Configuration (ncweb)	HP-UX	The ncweb tools allows the user to configure network services. For more information, see the product's online help.
Partition Manager (parmgr)	HP-UX, Linux, Windows	Partition Manager (parmgr) is a web-based application that allows system administrators to use a convenient graphical user interface (GUI) to configure and manage nPartitions on HP server systems. Partition Manager can also detect several types of configuration problems. For more information, see the product's online help.
Peripheral Devices Configuration (pdweb)	HP-UX	The pdweb tool lists and manages the OLRAD-capable PCI slots reported by the `olrad` command and Peripheral Devices reported by the `ioscan` command. On selecting a slot/device from the list, it displays details about the selected device/slot. It allows a user to Add / Replace / Delete an OLRAD-capable card online, to view the devices reported by `ioscan` command, and to re-install the Device Special Files where possible. For more information, see the product's online help.
Printer Management	HP-UX	Configure printers or plotters, manage print requests, and save or restore print spooler configuration.
Resource Management	HP-UX	Using the Event Monitoring Service, configure and view resource monitoring requests on the managed node.
Resource Monitors	HP-UX	Configure the display monitor, and configure the X server.
Role-based Access Control (RBAC)	HP-UX	Allows you to distribute administrative responsibilities by creating roles with appropriate authorizations and assigning them to non-root users and groups.
Security Attributes Configuration (secweb)	HP-UX	The secweb tool enables you to configure system-wide and per user values of security attributes of local and Network Information Service (NIS) users. For more information, see the product's online help.

Application Name	Operating System	Application Description
Serviceguard Cluster - Serviceguard Manager	HP-UX and Linux	Serviceguard allows you to create high availability clusters of HP 9000 and HP Integrity servers. In the event of a component failure, Serviceguard coordinates the failover process by transferring it to other highly available component(s) thereby preventing a network, hardware, or software issue from significantly disrupting service. Serviceguard Manager is the graphical user interface for Serviceguard. You can then do the following: Monitor, Administer, Configure Serviceguard clusters. For more information, see the product's online help.
Software Management	HP-UX	Copy depot software, install software, list depot software, list Installed software, remove depot software, and remove installed software.
Time	HP-UX	Set the system clock, list the NTP client networks, and display NTP network time sources.

2 Issues and workarounds

HP SMH undergoes rigorous testing before releasing any given version of the product. From HP test activities to date, the following items have been uncovered that you should keep in mind. Also, refer to the *HP System Management Homepage Installation Guide* and *HP System Management Homepage Online Help* for known issues.

HP SMH 6.3 release for Windows and Linux

- **Issue**: HP SMH 32-bit service does not get started on systems running on 64-bit operating systems, for example: SUSE Linux Enterprise Server 11 SP1, 64-bit and Red Hat Linux Enterprise Server 6, 64-bit.

  Description: HP SMH installs successfully, with default configurations. However, after verifying the status running the command `/etc/init.d/hpsmhd status`, the HP SMH status displays as unused and HP SMH service cannot be started.

  Workaround: To resolve the issue, verify whether the system has all the required 32-bit library packages installed, if not, install the missing packages.

- **Issue**: HP SMH becomes inaccessible after installing Windows XP Service Pack 2.

  Description: In addition to HP SMH becoming inaccessible, HP Systems Insight Manager and the HP Version Control Repository Manager also become inaccessible. The Windows XP Service Pack 2 implements a software firewall that prevents browsers or other clients from accessing the ports required for access to the Version Control Repository Manager.

  Workaround: To resolve the issue, you must configure the firewall with exceptions to allow access through the ports used by HP Systems Insight Manager, HP Version Control Agent, and other HP Version Control Repository Managers.

  HP recommends the following actions:
  1. Select **Start** ⇒ **Settings** ⇒ **Control Panel**.
  2. Double-click **Windows Firewall** to configure the firewall settings.
  3. Select **Exceptions**.
  4. Click **Add Port**, and then enter the product name and the port number.

     Add the following exceptions to the firewall protection:

     Table 2-1 Firewall protection

Product	Port Number
HP SMH Insecure	Port 2301, optional port
HP SMH Secure	Port 2381

  5. Click **OK** to save your settings, and close the **Add a Port** dialog box.
  6. Click **OK** to save your settings, and close the **Windows Firewall** dialog box.

  This configuration leaves the default SP2 security enhancements intact, but will allow traffic over the ports indicated above. The secure and insecure ports must be added to enable proper communication from your browser and other clients that access the Version Control Repository Manager.

- **Issue**: Using an ampersand character in the group name during HP SMH installation on a Windows XP system prevents you from logging into HP SMH after installation.

  Workaround: HP recommends that you avoid using the ampersand character in group names.

- **Issue**: HP Systems Insight Manager features do not support the use of Extended ASCII characters when specifying the HP Systems Insight Manager system.

  Description: The use of Extended ASCII characters does not allow the trust relationship to establish.

  Workaround: HP recommends that you avoid using Extended ASCII characters when specifying the HP Systems Insight Manager system.

- **Issue**: Forceful downgrading to SMH 6.0 from 6.1 or later fails on x86_64 Windows platform.

  Description: When SMH is downgraded forcefully from 6.1 or later to 6.0 using the command `cp010944.exe /f` the following error message appears:

  NOTE: This error is applicable for Windows x86_64 platform for SMH 6.0 only.

  Workaround: HP recommends that you use the following procedure to manually downgrade SMH to 6.0:

  1. Extract the SMH 6.0 component `cp010944.exe` to a folder say **C:\abc**.
  2. Navigate to the folder **C:\abc** in the command prompt. Execute the following command: `setup.exe /s /removeonly /f1 C:\abc`. This removes the currently installed version of HP SMH.
  3. Proceed normally to install the SMH 6.0 using the following exe file: `cp010944.exe`.

- **Issue**: The search in SMH Help page does not work for Japanese characters on Internet Explorer if the language is set to Japanese.

  Description: When Japanese characters are entered in the **Search** form in SMH Help page and the a Search button is clicked, no results are displayed. This is applicable only on Internet Explorer browser when the language is set to Japanese [ja-JP].

  Workaround: Enter the same Japanese characters in the search box on the results page and click on "Search" again. The documents matching your query is displayed.

- **Issue:** HP SMH 6.0 supports the following:

  - SSLv2

    Note: SSLv2 is disabled by default.

  - SSLv3

  - TLSv1

  Workaround: To enable the use of SSLv2 in the HP SMH:

  1. As a precautionary measure, copy the existing smhpd.xml file into a different directory.
  2. Manually add the tag:

     Note: To set this configuration on a group of servers, this setting is included in those affected by the Replicate Agent Settings feature in HP SIM. The source server must be configured manually using the following steps and then the setting can be installed simultaneously to other systems using HP SIM.

     a. Open the smhpd.xml in the \hp\hpsmh\conf directory on the boot drive with a text editor.
     b. Add the following line between the <system-management-homepage> and </system-management-homepage> tags:

        `<disable-sslv2>False</disable-sslv2>`

     c. Save the file.
  3. Restart the HP SMH service.

- **For Windows systems only:**

  Issue: When a system is running near the limit of the number of threads or processes its resources can support, HP SMH may not be able to start.

  Description: HP SMH 6.0 provides a way for users to reduce the number of threads required to avoid this issue. Modifying this setting might affect HP SMH response time and throughput.

Workaround: To modify this setting, use `smhconfig` command to set the maximum threads value:

1. Execute the following command to set the maximum thread value on the HP SMH. `smhconfig max-threads=value` where, max-threads value range is 64-512.
2. Execute the following command to restart the HP SMH service `smhconfig -r`
1. As a precautionary measure, copy the existing smhpd.xml file into a different directory.
2. Manually add the tag:
    a. Open the smhpd.xml in the \hp\hpsmh\conf directory on the boot drive with a text editor.
    b. Add the following line between the <system-management-homepage> and </system-management-homepage> tags:

    `<max-threads>value</max-threads>`

    Note: The value can be 64-512 on Windows systems. The default value for Windows systems is 250.

    c. Save the file.
3. Restart the HP SMH service.

Support and other resources

Information to collect before contacting HP

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

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:

  http://welcome.hp.com/country/us/en/contact_us.html

- In the United States, call 1-800-HP-INVENT (1-800-474-6836) to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.

- In other locations, see the Contact HP Worldwide website for contact options:

  http://welcome.hp.com/country/us/en/wwcontact.html

Registering for software technical support and update service

HP Insight software includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP. Customers who purchase an electronic license are eligible for electronic updates.

With this service, Insight software customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

http://www.hp.com/services/insight

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

After you have registered, you will receive a service contract in the mail containing the Customer Service phone number and your Service Agreement Identifier (SAID). You need your SAID when you contact technical support. Using your SAID, you can also go to the Software Update Manager (SUM) web page at **http://www.itrc.hp.com** to view your contract online.

Warranty information

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight software products.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator web site:

  http://www.hp.com/service_locator

- In other locations, see the Contact HP worldwide web site:

  http://welcome.hp.com/country/us/en/wwcontact.html

Documentation feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to:

docsfeedback@hp.com

Include the document title and manufacturing part number in your message. All submissions become the property of HP.

New and changed information in this edition

The following sections list what is new for the HP SMH releases.

April 2011 release for Linux and Windows

HP SMH 6.3 for Linux and Windows includes the following product enhancements:

- Command Line Interface option to list the current settings in HP SMH.
- Enhanced management of HP SMH self-signed certificate.
- Consolidated API logging for HP SMH Webapps.
- Platform-specific setup files for Windows x86 and x64 versions, available on Windows OS only.
- Enhanced installer log handling, available on Windows OS only.
- Enhanced Apache startup issue handling, available on Windows OS only.
- Support for enabling Tomcat integration on Integrity systems with IPv6-enabled support, available on Windows OS only.
- Enhanced default UI Timeout support for 120 seconds and enhanced UI Timeout warning message.
- Support for the new operating systems:
  - Microsoft Windows Server 2011 Small Business
  - Red Hat Enterprise Linux 6

The following open source products are revved:

- Updated PHP version to 5.3.3
- Updated libxml2 version to 2.7.8

NOTE: Corrected possible information disclosure may be used to obtain the version information of the web server used by HP System Management Homepage.

March 2011 release for HP-UX

HP SMH 3.2.2 for HP-UX 11i v3 includes product enhancements and fixes for internally found defects. Following are the product enhancements:

▲ A CLI-based option to configure the SSL Cipher Suite.

December 2010 release for HP-UX

HP SMH 3.2.0 for HP-UX 11i v2 includes product enhancements and fixes for internally found defects. Following are the product enhancements:

- HP SMH on 11i v2 supports both Apache 2.0 and Apache 2.2. SMH can be configured to use either Apache 2.0 or Apache 2.2.

NOTE: The minimum version of Apache required to be installed for facilitating Apache 2.2 support with HP SMH is `hpuxws22Apache` **B.2.2.8.10**.

NOTE: If HP SMH is configured for Apache 2.2 version, install Tomcat 2.2 version to facilitate the Java application functioning.

- A CLI-based option to configure the SSL Cipher Suite.
- Port 1188 is the default port used by Tomcat instance within SMH. This port can be configured to a different value.
- A new configuration parameter `TOMCAT_PORT` is added in HP-UX 11i v2 to configure the port used for Apache and Tomcat communication.

September 2010 release for Linux and Windows

HP SMH 6.2 for Linux and Windows includes the following product enhancements:

- A CLI-based configurable logging option where log severity for `smh_enc.log` can be configured. Only log messages equal to or higher than the severity set in `smh_enc.log` will be logged.
- An option to enable/disable **Port 2301** on the HP SMH installer (Windows only).
- Support for the Autostart mode (Linux only).
- A CLI-based option to configure the SSL Cipher Suite.
- The **System Status** and **Overall System Summary** tabs on the SMH Home page have been changed to **Overall System Health Status** and **Component Status Summary** respectively.
- Better UI timeout handling and detailed webapp timeout logging in `smh_enc.log`.
- Support for logging the security settings changes through the GUI and CLI.

The following open source products were revved:

- Updated OpenSSL version to 0.9.8n
- Updated Apache version to 2.2.15
- Updated PHP version to 5.2.13

NOTE: Corrected possible information disclosure may be used to obtain the version information of the web server used by HP System Management Homepage.

September 2010 release for HP-UX

HP SMH 3.2.1 for HP-UX 11i v3 includes product enhancements and fixes for internally found defects. Following are the product enhancements:

- HP SMH on 11i v3 supports both Apache 2.0 and Apache 2.2. SMH can be configured to use either Apache 2.0 or Apache 2.2.
- Port 1188 is the default port used by Tomcat instance within SMH. This port can be configured to a different value.
- A new configuration parameter TOMCAT_PORT is added in HP-UX 11i v3 to configure the port used for Apache and Tomcat communication.
- **System Status** and **Overall System Summary** tabs on the SMH Home page have been changed to **Overall System Health Status** and **Component Status Summary** respectively.

HP SMH 3.1.2 for HP-UX 11i v2 includes fixes for the internally found defects.

March 2010 release for Linux and Windows

HP SMH 6.1.0 provides the provides the following functionalities over previous HP SMH Windows and Linux releases:

- Added operating system support to include:
    - Microsoft Windows 7 for x86 and x64
    - Microsoft Windows 2008 R2 Server core
    - Microsoft Windows Vista SP2
    - SUSE Linux Enterprise Server (SLES) 11 for x86 and AMD64/EMT64T
    - SUSE Linux Enterprise Server (SLES) 10 SP2 or later for x86 and AMD64/EMT64T
    - SUSE Linux Enterprise Server (SLES) 9 SP4 for x86 and AMD64/EMT64T
    - XEN 5.5 update 2
- The following open source products were revved:
    - Updated OpenSSL version to 0.9.81
    - Updated Namazu (Windows only) version to 2.0.20

NOTE: Corrected possible information disclosure may be used to obtain the version information of the web server used by HP System Management Homepage.

- Support for Firefox web browser version 3 and 3.5.

March 2010 release for HP-UX

HP SMH 3.1.0 for HP-UX 11i v2 and HP-UX 11i v3 includes product enhancements and fixes for internally found defects. Following are the product enhancements:

- Automated log collection via smhassist.
- Command Line Interface (CLI) - smhconfig - that provides users with administrator rights access to set values through the command line.
- Facility to disable port 2301.
- Logging into syslog the activities related to login and logout performed on HP SMH.
- Help page and help icon for custom menu.

There are no changes in HP SMH 2.2.9.3 for HP-UX 11i v1.

November 2009 release for Linux and Windows

Following are the product enhancements for the HP SMH November 2009 Linux and Windows release:

- Support for the new operating systems:
  - Microsoft Windows Server 7 for x86 and x64
  - Microsoft Windows Server 2008 R2 for x64
  - Microsoft Windows Server 2008 R2 for 64-bit Itanium-based systems
  - Red Hat Enterprise Linux 5 update 3 for x86 and AMD64/EMT64T
  - Red Hat Enterprise Linux 5 update 4 for x86 and AMD64/EMT64T
  - VMware ESX 4.0
- Support for Internet Explorer web browser version 8.
- SMHlogreader tool support.
- Native x64 support.

October 2009 release for HP-UX

Defects are fixed in HP SMH 3.0.2.1 for HP-UX 11i v2 and HP-UX 11i v3, and HP SMH 2.2.9.3.1 for HP-UX 11i v1. Following are the details:

- Changes are made in the Namazu search engine to fix a security vulnerability. This defect fix was earlier (July web release) available only on HP-UX 11i v3. This release includes the fix in all three HP-UX versions (HP-UX 11i v1, v2, and v3).
- The following defects are resolved:
  - CR QXCR1000961776. On HP-UX 11i v1 systems, HP SMH now correctly displays the Description and other data in the System Summary page.
  - CR QXCR1000939573. On HP-UX 11i v1, 11i v2, and 11i v3 systems, you can now access HP SMH using IPv6 address in the URL when SMH is in both 'autostart URL' mode and 'Start on Boot' mode. This is possible on both ports, 2301 and 2381.
  - CR QXCR1000940148. Unnecessary awk errors are no longer logged on HP-UX 11i v1 and v2. The issue is not applicable to HP-UX 11i v1.

> **IMPORTANT:** The support for long length passwords of up to 255 characters in the shadow password mode is not available yet. HP SMH is pre-enabled to support maintaining long passwords ahead of this feature actually being available in HP-UX.

September 2009 release for HP-UX

HP SMH 3.0.2 for HP-UX 11i v2 and HP-UX 11i v3 includes product enhancements and defect fixes. Following are the product enhancements:

- Support for IPv6 addresses.
- Support for Internet Explorer web browser version 8.
- Support for long length passwords of up to 255 characters in the shadow password mode.
- Support for Java 6. This enables you to open the Java-based HP SMH plug-in applications such as HP Serviceguard and Partition Manager, where Java 6 is installed. On HP-UX 11i v1 HP SMH continues to support Java 1.5.

HP SMH 2.2.9.3 for HP-UX 11i v1 contains defect fixes.

March 2009 release for HP-UX

HP SMH 3.0.0 for HP-UX 11i v2 and HP-UX 11i v3 provides the following product enhancements:

- Improved feature-rich user interface
- User configurable user interface properties

- User control of session and user interface timeouts
- Capability to verify HP SMH software dependency information using the new `smhassist` command

HP SMH 2.2.9.2 for HP-UX 11i v1 contains defect fixes.

January 2009 release for Linux and Windows

HP SMH 3.0 provides the following functionality over previous HP SMH releases:

- New user interface
- Support for Kerberos on Windows
- Support for Command Line Interface
- The ability to disable port 2301
- User configurable user interface properties
- User control of session and user interface timeouts
- Log localization
- IPv6 support

Added operating system support to include:

- **HP ProLiant servers**
  - Microsoft Windows Server 2008 Essential Business
  - Microsoft Windows Server HPC 2008
  - Microsoft Windows Server 2003 Standard Edition SP2 for x86 and x64
  - Microsoft Windows Server 2003 R2 Standard Edition SP2 for x86 and x64
  - Microsoft Windows Server 2003, Web Edition SP2
  - Microsoft Windows Server 2003 Enterprise Edition SP2 x86 and x64
  - Microsoft Windows Server 2003 R2 Enterprise Edition SP2 x86 and x64
  - Microsoft Windows Server 2003 Small Business Standard and Premium R2
  - Microsoft Windows Vista Business Edition
  - Microsoft Windows Vista Enterprise Edition
  - Microsoft Windows Vista Ultimate Edition
  - Microsoft Windows XP SP2
  - Red Hat Enterprise Linux 4 update 8 or later for x86 and AMD64/EMT64T
  - Oracle Enterprise Linux
  - SUSE Linux Enterprise Server (SLES) 11 for x86 and AMD64/EMT64T
  - SUSE Linux Enterprise Server (SLES) 10 SP2 or later for x86 and AMD64/EMT64T
  - VMware ESX 3.5 update 5
  - Citrix XEN 5.6
- **HP Integrity servers**
  - Microsoft Windows Server 2008 for Itanium-based systems, 64-bit

Security bulletin and alert policy for non-HP owned software components

Open source software (such as OpenSSL) or third-party software (such as Java) are sometimes included in HP products. HP discloses that the non-HP owned software components listed in the HP System Management Homepage end user license agreement (EULA) are included with HP System Management Homepage.

To view the EULA, use a text editor to open the `eula_license.xml` file, and search for third-party software.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

HP has a well-defined process when a security defect is found that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Subscribing to security bulletins

To receive security information (bulletins and alerts) from HP:

1. Open a browser and go to the HP home page at **http://www.hp.com**.
2. Click the **Support and Drivers** tab.
3. Click **Sign up: driver, support, and security alerts,** which appears under **Additional Resources** in the right navigation pane.
4. Select **Business and IT Professionals** to open the Subscriber's Choice web page.
5. Do one of the following:

   - Sign in if you are a registered customer.

   - Enter your email address to sign-up now. Then, select the box next to **Driver and Support alerts** and click **Continue**.

Related information

HP SMH documentation

For more information about HP SMH, see the following sources:

- *HP System Management Homepage Release Notes*   The release notes provide documentation for what's new with the release, features and change notifications, system requirements, and known issues. The release notes are available on the HP Technical Documentation website at **http://www.hp.com/go/hpux-core-docs**, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the release notes is available at the HP SMH web page at **http://h18013.www1.hp.com/products/servers/management/agents/documentation.html**.

- **HP System Management Homepage Help System**   The help system provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. In HP SMH, go to the **Help** menu.

- *HP System Management Homepage Installation Guide*   The installation guide provides information about installing and getting started using HP SMH. It includes an introduction to basic concepts, definitions, and functionality associated with HP SMH. The installation guide is available on the HP Technical Documentation website at **http://www.hp.com/go/hpux-core-docs**, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the installation guide is available on the Management CD and at the HP SMH web page at **http://h18013.www1.hp.com/products/servers/management/agents/documentation.html**.

- *HP System Management Homepage User Guide*   The user guide provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. The user guide is available on the HP Technical Documentation website at **http://www.hp.com/go/hpux-core-docs**, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the user guide is available at the HP SMH web page at **http://h18013.www1.hp.com/products/servers/management/agents/documentation.html**.

- **Simplifying single-system management on HP-UX 11i – HP System Management Homepage (HP SMH)**   This white paper introduces HP SMH and its various plug-ins. The use cases involving HP SMH plug-ins highlight the features provided by HP SMH. The white paper is available on the HP Technical Documentation website at **http://www.hp.com/go/hpux-core-docs**, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2,

and search with the document title "Simplifying single-system management on HP-UX 11i - HP System Management Homepage (HP SMH)."

- **Safe and Powerful: Security in HP-UX System Management Homepage (SMH)**   This white paper provides an overview of the security aspects in HP SMH. The white paper describes the various security features that the application provides, and includes security related tips for system administrators. The white paper is available on the HP Technical Documentation website at **http://www.hp.com/go/hpux-core-docs**, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2, and search with the document title "Safe and Powerful: Security in HP-UX System Management Homepage (SMH)."

- *hpsmh* **(1m) manpage**   For HP-UX releases, the manpage is available from the command line using the `man hpsmh` command. This information is not available for Linux and Windows operating systems.

- *smhstartconfig* **(1M) manpage**   For HP-UX operating system releases, the manpage is available from the CLI using the `man smhstartconfig` command. This information is not available for Linux and Windows operating systems.

- *sam* **(1M) manpage**   For HP-UX operating system releases, the manpage is available from the CLI using the `man sam` command. This information is not available for Linux and Windows operating systems.

- *smh* **(1m) manpage**   This command is available in HP-UX 11i v3 (B.11.31) only. This is an enhanced version of the *sam* (1m) command. For HP-UX operating system releases, the manpage is available from the CLI using the `man smh` command. This information is not available for Linux and Windows operating systems.

- *smhassist* **(1m) manpage**   You can use the `smhassist` command to verify the configurations of SMH and see if there are any dependent software, patches or configuration errors. For HP-UX 11i v3 (B.11.31) and HP-UX 11i v2 (B.11.23) operating system releases, the manpage is available from the CLI using the `man smhassist` command. This information is not available for HP-UX 11i v1 (B.11.11), Linux, and Windows operating systems.

- *smhconfig* **(1m) manpage**   You can use the `smhconfig` CLI to set configuration values through the command line. The CLI provides users having administrative rights access to modify configuration options, including the required security checks that allow the configuration options to be changed. For HP-UX 11i v3 (B.11.31) and HP-UX 11i v2 (B.11.23) operating system releases, the manpage is available using the `man smhconfig` command. This information is not available for HP-UX 11i v1 (B.11.11), Linux, and Windows operating systems.

- **HP System Management Homepage website**   The website provides HP SMH information and product links. Go to the HP SMH website at **http://hp.com/go/smh**.

- **HP Insight Essentials software page**   This web page is at **http://www.hp.com/servers/manage**.

HP-UX documentation

For more information about using HP SMH in an HP-UX environment, see the following sources. They are available on the Instant Information DVD and on the HP Technical Documentation web site at **http://www.hp.com/go/hpux-core-docs**.

- **HP-UX 11i Installation and Update Guides (v1, B.11.11; v2, B.11.23; v3 B.11.31)**   Provide instructions on how to install or update to HP-UX.

- **HP-UX 11i Release Notes (v1, B.11.11; v2, B.11.23; v3 B.11.31)**   Describe new features and functionality changes for HP-UX 11i, including information on HP SMH.

- For HP-UX operating system release documentation, check for the latest version on **http://www.hp.com/go/hpux-core-docs**.

Typographic conventions

find(1)	HP-UX manpage. In this example, "find" is the manpage name and "1" is the manpage section.
Book Title	Title of a book or other document.
Linked Title	Title that is a hyperlink to a book or other document.
http://www.hp.com	A Web site address that is a hyperlink to the site.
`Command`	Command name or qualified command phrase.
user input	Commands and other text that you type.
`computer output`	Text displayed by the computer.
Enter	The name of a keyboard key. Note that **Return** and **Enter** both refer to the same key. A sequence such as **Ctrl+A** indicates that you must hold down the key labeled **Ctrl** while pressing the **A** key.
term	Defined use of an important word or phrase.
`variable`	The name of an environment variable, for example `PATH` or `errno`.
value	A value that you may replace in a command or function, or information in a display that represents several possible values.
`<element>`	An element used in a markup language.
`attrib=`	An attribute used in a markup language.

Index

D
documentation, 21

F
features, 7
   new, 16

K
known issues, 11

M
manpages, 21

N
new functionality, 16

R
resources, 21

T
troubleshooting, 11
typographic conventions, 23