



Hewlett Packard
Enterprise

HPE System Management Homepage 7.6.1 Release Notes HP-UX, Linux, and Windows Operating Systems

Abstract

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

- HPE Insight Diagnostics
- Array Configuration Utility, HPE Smart Storage Administrator
- HP Software Version Control Agents

This release notes is for system administrators and any level of user of HPE SMH.

Part Number: 872142-001a
Published: June 2017
Edition: 2

© Copyright 2004, 2017 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Acknowledgments

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Itanium® is a trademarks of Intel Corporation in the U.S. and other countries.

Microsoft ® and Windows® are registered trademarks of Microsoft group of companies.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

Java is registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Citrix® and XenDesktop® are trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware® ESX® and ESXi™ are registered trademarks or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

1 Features	4
Product features.....	4
Partition Manager.....	5
Available IP addresses.....	5
Integrated applications to HPE SMH.....	5
2 Known problems, issues, limitations, and workaround	8
HPE SMH for Windows and Linux.....	8
3 Support and other resources	15
Accessing Hewlett Packard Enterprise Support.....	15
Accessing updates.....	15
Registering for software technical support and update service.....	16
How to use your software technical support and update service.....	16
Warranty information.....	16
Hewlett Packard Enterprise authorized resellers.....	16
Websites.....	16
Customer self repair.....	17
Remote support.....	17
Documentation feedback.....	17
More on HPE Management Homepage (HPE SMH) documentation.....	17
4 Content updates, release updates, and new/changed information in this document edition	18
June 2017 release for Linux and Windows.....	18
November 2016 release for Linux and Windows.....	18
April 2016 release for Linux and Windows.....	19
August 2015 release for Linux and Windows.....	19
March 2015 release for Linux and Windows.....	20
December 2013 release for Linux and Windows.....	20
October 2013 release for Linux and Windows.....	20
January 2013 release for Linux and Windows.....	21
June 2012 release for Linux and Windows.....	21
February 2012 release for Linux and Windows.....	22
April 2011 release for Linux and Windows.....	23
September 2010 release for Linux and Windows.....	24
March 2010 release for Linux and Windows.....	24
November 2009 release for Linux and Windows.....	25
January 2009 release for Linux and Windows.....	25
5 Security bulletin and alert policy for non-Hewlett Packard Enterprise owned software components	27
Subscribing to security bulletins.....	27
6 Related information	28
SMH documentation.....	28
HP-UX documentation.....	30

1 Features

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

- HPE Insight Diagnostics
- Array Configuration Utility, HPE Smart Storage Administrator
- HP Software Version Control Agents

The HPE System Management Homepage (HPE SMH) for HP-UX, Linux, and Windows provides the features described in [Product features](#). They are applicable to all releases, except where noted.

Product features

Following is the list of features supported by HPE System Management Homepage (HPE SMH) as a product.

- Provides security for HPE 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 HPE Web-enabled System Management Software that provides information to HPE SMH.
- Common HTTP and HTTPS service for HPE Insight Management Agents and utilities, for reduced complexity and system resource requirements.
- Simplified architecture for implementing HTTP security and Hewlett Packard Enterprise 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 HPE SMH.
This feature is available only on HP-UX 11i v2 and HP-UX 11i v3 systems.
- Consolidated API logging for SMH and WebApps: Provides an option to log the critical and major events of both the SMH and its WebApps to the system log for viewing and auditing.
- Verbose logging: Provides an option to enable/disable this feature, by enabling this feature to check the complete log information.
- HPE SMH configuration parameters are listed in the `parameter` tag and the corresponding description is available in the `user_prompt` tag.

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 HPE SMH. To use this feature on HP-UX 11i v1, you must install `KRNG11i`, the Strong Random Number Generator software for HP-UX 11i v1, available from the Software Depot website at [Hewlett Packard Enterprise Software Depot](#).

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, HPE SMH would only be accessible using the IP addresses defined at system startup. If new IP addresses were defined then HPE SMH would have to be restarted to use them.

With this new HPE SMH feature, any configuration change in the list of available IP addresses, in clustered and non-clustered environments, would automatically reconfigure HPE 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></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.hpe.com/info/hpux-core-docs> and select HP-UX 11i v2 from the product list.

Integrated applications to HPE SMH

HPE SMH is a framework for a number of integrated applications. HPE SMH provides the following system management functionality (described in “[HPE SMH integrated applications](#)” (page 5)) through a single-user interface and the HPE SMH GUI (Graphical User Interface).

- ❗ **IMPORTANT:** In HPE 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 HPE 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 HPE 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.

Table 1 HPE SMH integrated applications (continued)

Application Name	Operating System	Application Description
Disks and File Systems (fsweb)	HP-UX	<p>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.</p> <p>The fsweb tool supports these file systems: Cache File System (CFS), Compact Disc File System (CDFFS), Common Internet File System (CIFS), Hierarchical File System (HFS), Network File System (NFS), and Veritas File System (VxFS).</p> <p>For more information, see the product's online help.</p>
Distributed System Authentication Utilities (DSAU)	HP-UX	<p>Distributed Systems Administration Utilities provide several tools for simplifying the management of groups of systems and Serviceguard clusters.</p> <p>Configure configuration synchronization, consolidated logging, and view system logs.</p>
Event Monitoring Service (web-based) (EMSweb)	HP-UX	<p>The EMSWeb tool (bundle EventMonitorGUI) enables the user to manage requests to monitor resources on the system.</p> <p>Using the EMSWeb tool the user can create and manage requests to monitor resources.</p>
Error Management Technology (EMT)	HP-UX	<p>Error Management Technology provides a quick, easy method of accessing error/cause/action information on all system errors.</p> <p>Use it to query or customize error data.</p>
EVWEB	HP-UX	<p>EVWEB is a user component of System Fault Management (SFM).</p> <p>Using evweb, you can view and administer various Web-Based Enterprise Management (WBEM) events that are generated on an HP-UX system.</p> <p>For more information, see the product's online help.</p>
IPMI Event Viewer	HP-UX	View hardware events.
Kernel Configuration (kcweb)	HP-UX	<p>The kcweb tool allows the user to configure an HP-UX kernel and to monitor consumption of kernel resources controlled by parameters.</p> <p>For more information, see the product's online help.</p>
Network Interfaces Configuration	HP-UX	<p>Network Interfaces Configuration is a web-based system management tool that enables you to configure network interfaces on HP-UX installed systems.</p> <p>For more information, see the product's online help.</p>
Network Services Configuration (ncweb)	HP-UX	<p>The ncweb tools allows the user to configure network services.</p> <p>For more information, see the product's online help.</p>
Partition Manager (parmgr)	HP-UX Linux Windows	<p>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 server systems.</p> <p>Partition Manager can also detect several types of configuration problems.</p>

Table 1 HPE SMH integrated applications (continued)

Application Name	Operating System	Application Description
		For more information, see the product's online help.
Peripheral Devices Configuration (pdweb)	HP-UX	<p>The pdweb tool lists and manages the OLRAD-capable PCI slots reported by the <code>olrad</code> command and Peripheral Devices reported by the <code>ioscan</code> command.</p> <p>On selecting a slot/device from the list, it displays details about the selected device/slot.</p> <p>It allows a user to Add/Replace/Delete an OLRAD-capable card online, to view the devices reported by <code>ioscan</code> command, and to re-install the Device Special Files where possible.</p> <p>For more information, see the product's online help.</p>
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	<p>The secweb tool enables you to configure system-wide and per user values of security attributes of local and Network Information Service (NIS) users.</p> <p>For more information, see the product's online help.</p>
Serviceguard Cluster - Serviceguard Manager	HP-UX Linux	<p>Serviceguard allows you to create high availability clusters of HPE 9000 and HPE Integrity servers.</p> <p>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.</p> <p>Serviceguard Manager is the graphical user interface for Serviceguard.</p> <p>You can then do the following: Monitor, Administer, Configure Serviceguard clusters.</p> <p>For more information, see the product's online help.</p>
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 Known problems, issues, limitations, and workaround

This chapter explains in detail, various problems, issues, limitations, and their workaround for HPE System Management Homepage (HPE SMH) across many releases.

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

HPE SMH for Windows and Linux

- **Issue:** The NIC tab is not shown in HPE SMH 7.6.1 UI after setting the data source as SNMP on Linux 64 bit, Windows 32 bit and Linux 32 bit operating systems.

Workaround: Edit the file `C:\hp\hpsmh\data\htdocs\hmanics\hmanics.js.php.en` on Windows 32 bit operating system and `\opt\hp\hpsmh\data\htdocs\hmanics\hmanics.js.php.en` on Linux operating system to include `<?php virtual('/hmanics/nc-cmmn.js'); ?>` at the end of the file, and saving it will resolve the issue.

- **Issue:** HPE SMH for Linux could be vulnerable to privilege elevation.

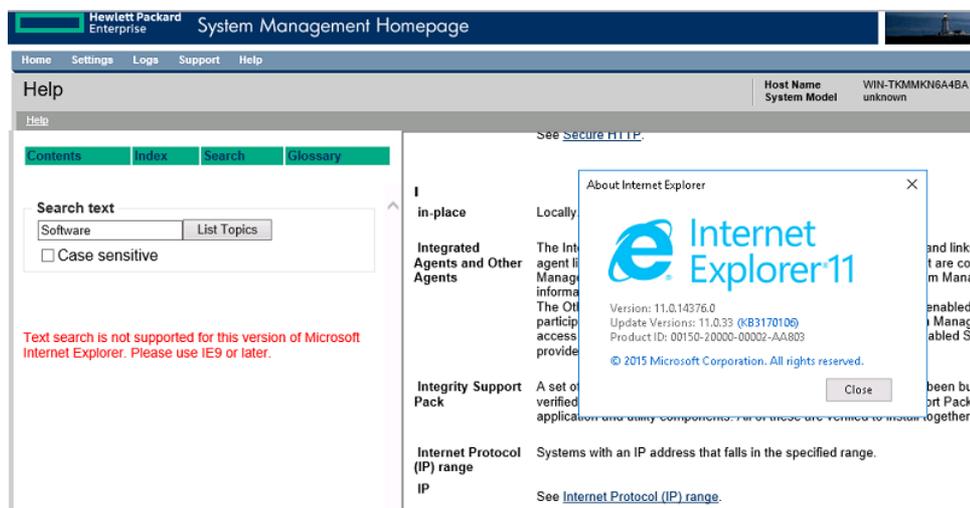
Description: Any binary/script placed under `cgi-bin` can be made to execute, by setting certain environmental variables and using `smhrun`. Insecure file and folder permissions on `/opt/hp/hpsmh/` can also lead to root privilege escalation.

Workaround: The following precautions must be taken on Linux OS:

- Do not provide login access to the “hpsmh” user (created during installation) by editing the `/etc/passwd` file or any other means.
- Do not add any user to the “hpsmh” group (created during installation).

- **Issue:** Search functionality is not working in HPE SMH Help page when opened in IE browser.

Description: When you log in to HPE System Management Homepage and using online help, try to search for information, using the Search option, you may get the following error:



Workaround: This issue may occur if the IE browser is not set to the default version. To set the IE browser to the default version:

1. In the browser window, press **F12**.

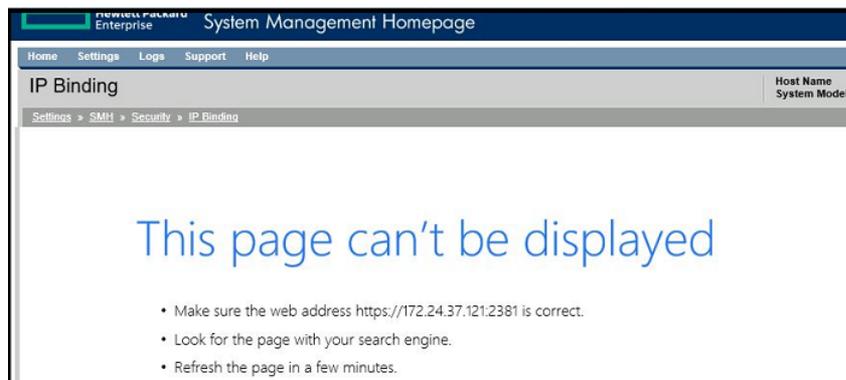
The version setting details are displayed in the lower right window. If the version is set to “8”, then error message about using IE 9 or later pops up.

2. Change the version to IE 11 from the drop-down menu.

You should be able to perform the search now.

- **Issue:** This page can't displayed error is seen after applying and removing the values in IE 11 for IP binding feature..

Description: In IP binding feature, after adding or removing values, when we click **Apply**, the following error is displayed:



Workaround: Refresh the page. After refreshing the page, the functionality works as expected.

- **Issue:** Warning messages displayed while uninstalling HPE SMH in RHEL 6.8 and SLES 12 SP1 OS.

Description: When you uninstall the HPE SMH in RHEL 6.8 (x64, x86), the following warning messages are displayed:

In RHEL 6.8 (x86), the warning messages displayed are:

- warning: erase unlink of /var/spool/opt/hp/hpsmh/logs failed: No such file or directory
- warning: erase unlink of /var/spool/opt/hp/hpsmh failed: No such file or directory
- warning: erase unlink of /opt/hp/hpsmh/lbin/smhstarted_ipv4 failed: No such file or directory

In RHEL 6.8(x64), the warning message displayed is:

- warning: erase unlink of /opt/hp/hpsmh/lbin/smhstarted_ipv4 failed: No such file or directory

In SLES 12 SP1 OS, the warning message displayed is:

- warning: file /opt/hp/hpsmh/lbin/smhstartd_ipv4: remove failed: No such file or directory

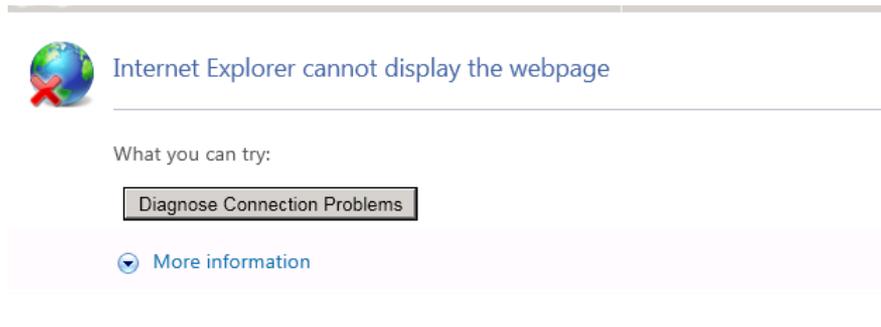
Workaround: There is no workaround required for this issue as this has no impact on the functionality of HPE SMH.

- **Issue:** HPE SMH is vulnerable to weak authentication vulnerability.

Workaround: All users must follow the best practice of signing out of HPE SMH before closing the browser.

- **Issue:** Logging into HPE SMH using Internet Explorer 9 or 10 throws the error “Page can't be displayed”

Description: When using Internet Explorer 9 or 10 to launch HPE SMH, the following error is displayed:



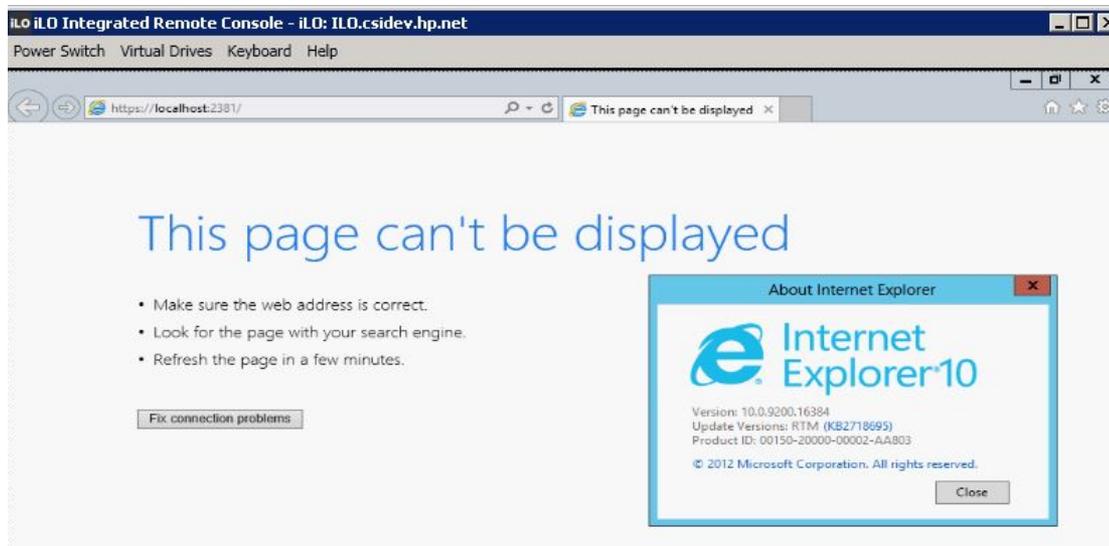
NOTE: This issue is not found in other browsers such as Firefox or Google Chrome.

Workaround: Update the IE browser with the following setting:

1. Click **ToolsInternet OptionsAdvanced**.
2. Select the check box next to TLS 1.2 to enable it.

- **Issue:** HPE System Management Homepage for Windows (x64) and HPE Insight Diagnostics Online Edition for Windows x64 Editions fails to open on W2K12 OS with supported IE browser.

Description: The HPE SMH and HPE Insight Diagnostics fail to launch in the IE browser. When the user clicks on the shortcuts, the IE browser is launched with the following error message:



NOTE: This issue is not found in Windows 2012 R2 and Windows 2016 OS. This issue is also not observed with Firefox or Google Chrome.

Workaround: Enable the TLS 1.2 for your IE browser. To enable TLS 1.2:

1. Open Internet Explorer.

NOTE: Ensure that you are using IE 9 or later.

2. Click **ToolsInternet OptionsAdvanced**.
3. Select the check box next to TLS 1.2 to enable it.

- **Issue:** Old icons are displayed even after upgrading to the latest version of HPE System Management Homepage

Description: Even after upgrading from the older HPE SMH versions to the latest HPE SMH version (7.6), the product icons remain the same and not change to the new icon.

Workaround: After upgrading to HPE SMH 7.6 from any older version:

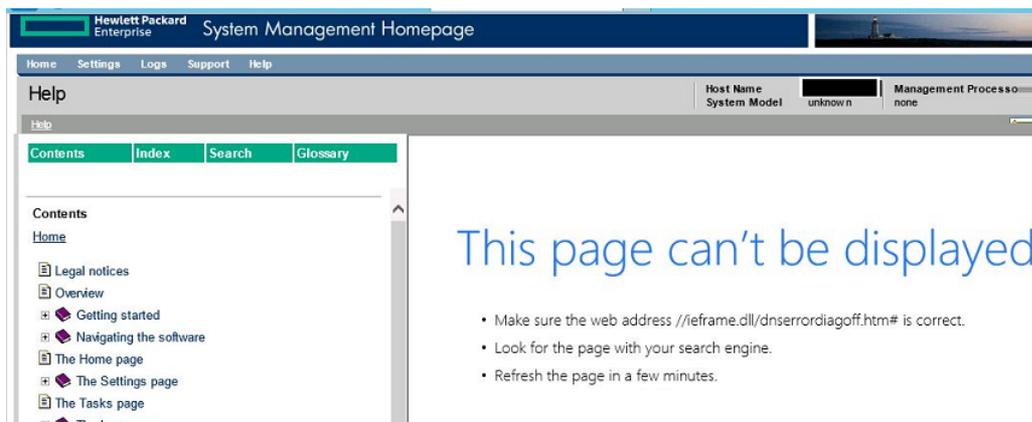
1. From the command prompt, run the following command:

```
ie4uinit.exe -ClearIconCache
ie4uinit.exe -show
```

2. Restart the system. The new icons will be displayed now.

- **Issue:** HPE SMH help page shows “page can’t be displayed error” in IE

Description: When HPE SMH is opened in IE browser and Help is clicked, the following error message is displayed:



Workaround: When you select any of the other links in the Help page, and the page works fine.

- **Issue:** Port 2301 in Internet Explorer 8 Windows (32 bit) gives the following error:

Unable to complete your request due to added security features

Workaround: Add HPE SMH IP in the trusted sites, then the port 2301 works fine.

- **Issue:** Java plug-ins are required and must be enabled for displaying some Help pages in HPE SMH.

Description: All Linux distributions do not have Java plug-ins available or enabled by default, even after a full OS installation, except for RHEL6. This results in missing contents of some help pages in HPE SMH on all Linux flavors except RHEL6. Firefox does not pop-up any error messages to notify the users that HPE SMH requires Java plug-ins to run properly, and the help pages display only empty contents. However, Microsoft Internet Explorer throws up JAVA error message in such a scenario, which is missing in the case of FireFox browsers.

Also, the issue of Java plug-ins must be enabled for displaying some Help pages occurs when HPE SMH server IP is added in trusted sites list and then java scripting is disable on the trusted sites. This is only seen on SLES10 SP4 on both IE and FF browsers.

Workaround: As a workaround for this issue, Install java plug-ins on FireFox browser and enable java scripting on the browsers. The fix for this issue will be available in a future release of HPE SMH.

- **Issue:** Passwords may be stored in web browsers and retrieved.

Workaround: Clear the browser cache so that the old passwords are removed and cannot be retrieved.

- **Issue:** HPE SMH 6.x and 7.x versions generate and display exceptions on Windows operating systems.

Description: Under certain conditions, for example, during vulnerability scanning by the HPE Web Inspect tool, HPE SMH 6.x and 7.x versions generate and display exceptions on some latest Windows operating systems on which the dump file creation feature is enabled. Such exceptions create a dump in the system default directory. These files may contain sensitive information. Dump files may be created in system default directory like `C:\ProgramData\Microsoft\Windows\WER\ReportQueue` on Windows operating systems. Whenever you use an application to perform any of the restricted operations, the dump files are created in the system default directory. This typically occurs on Apache-based systems. HPE SMH, which is built around Apache web server creates such dump files with sensitive information, whenever unhandled exceptions are encountered because of any restricted operations.

Workaround: The resolution to this issue is to be provided by Apache Software Foundation. However, there are a few of the commands and options available on Windows operating systems to disable or redirect the dump file creation (to a safer location).

Using Command Line Interface:

- To disable dump file creation, run the following command `wmic recoveros set DebugInfoType = 0`
- To redirect dump file location, run the following command `wmic recoveros set DebugFilePath = <file_path>` where, <file_path> refers to the new location for the dump file creation.

For more information, see the Microsoft knowledge base <http://support.microsoft.com/kb/307973>.

Using Control Panel:

Two different approaches are available on some versions of Windows 2008 to achieve the same functionality.

Approach 1:

1. From **Start**, go to **Control Panel** ⇒ **Action Center** (under System and Security category).
2. Click **Maintenance**.
3. Click **Settings**.
4. Click **Change report settings for all users**, and then select **Never check for solutions**.

Approach 2:

1. From **Start**, go to **Control Panel** ⇒ **System and Maintenance**.
2. Click **Problem Reports and Solutions**.
3. Click **Change Settings**.
4. On the **Change Settings** page, click **Advanced Settings**.
5. On the **Advanced Settings** page, select **Change Settings** option for the menu item **For all users and programs problem reporting is set to:**
6. Select **Off**, and then click **OK**.
7. On the **Advanced Settings** page, click **OK**.
8. On **Change Settings** page, click **OK**.

Using Registry:

On some Windows operating systems, you can edit either of the following Registry keys to disable Windows Error Reporting, by modifying the **Disabled** settings. Type `REG_DWORD` with the following possible value: `Disabled`

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting`

For more information, see <http://msdn.microsoft.com/en-us/library/bb513638%28v=vs.85%29.aspx>.

- **Issue:** HPE 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: HPE SMH installs successfully, with default configurations. However, after verifying the status running the command `/etc/init.d/hpsmhd status`, the HPE SMH status displays as unused and 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:** Using an ampersand character in the group name during HPE SMH installation on a Windows operating system prevents you from logging into HPE SMH after installation.

Workaround: Hewlett Packard Enterprise recommends that you avoid using the ampersand character in group names.

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

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

Workaround: Hewlett Packard Enterprise recommends that you avoid using Extended ASCII characters when specifying the HPE 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 only.

Workaround: Hewlett Packard Enterprise 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 SMH.

3. Proceed normally to install the SMH using the following exe file: `cp010944.exe`.

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

- SSLv2

NOTE: SSLv2 is disabled by default and it cannot be enabled in 7.2 onwards.

- SSLv3

- TLSv1

Workaround: To enable the use of SSLv2 in the 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 HPE SIM. The source server must be configured manually using the following steps and then the setting can be installed simultaneously to other systems using HPE 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-ssl2>False</disable-ssl2>
```

- c. Save the file.

3. Restart the 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, SMH may not be able to start.

Description: SMH 6.0 provides a way for users to reduce the number of threads required to avoid this issue. Modifying this setting might affect 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 SMH.
`smhconfig max-threads=value` where, `max-threads` value range is 64-512.
2. Execute the following command to restart the SMH service `smhconfig -r`
3. As a precautionary measure, copy the existing `smhpd.xml` file into a different directory.
4. 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.

5. Restart the HPE SMH service.

3 Support and other resources

This section explains about support, contact information, and customer related useful information regarding HPE System Management Homepage (HPE SMH).

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
Contact HPE Support Worldwide
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
Hewlett Packard Enterprise Support Center

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
 - To download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - Software Depot website:
Hewlett Packard Enterprise Software Depot
 - To view and update your entitlements and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
Hewlett Packard Enterprise Support Center
-
- ① **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.
-

Registering for software technical support and update service

HPE Insight software includes one year of 24 x 7 HPE Software Technical Support and Update Service. This service provides access to Hewlett Packard Enterprise 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 Hewlett Packard Enterprise. Customers who purchase an electronic license are eligible for electronic updates.

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

<http://www.hpe.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 [Hewlett Packard Enterprise Support Center](#) to view your contract online.

Warranty information

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

Hewlett Packard Enterprise authorized resellers

For the name of the nearest Hewlett Packard Enterprise authorized reseller, see the following sources:

- In the United States, see the Hewlett Packard Enterprise U.S. service locator website:
[Find a Partner](#)
- In other locations, see the Contact Hewlett Packard Enterprise worldwide website:
[Contact HPE Support Worldwide](#)

Websites

Website	Link
Hewlett Packard Enterprise Information Library	<u>www.hpe.com/info/enterprise/docs</u>
Hewlett Packard Enterprise Support Center	<u>www.hpe.com/support/hpesc</u>
Contact Hewlett Packard Enterprise Support Worldwide	<u>www.hpe.com/assistance</u>
Subscription Service/Support Alerts	<u>www.hpe.com/support/e-updates</u>
Software Depot	<u>www.hpe.com/support/softwaredepot</u>
Customer Self Repair	<u>www.hpe.com/support/selfrepair</u>
Insight Remote Support	<u>www.hpe.com/info/insightremotesupport/docs</u>
Serviceguard Solutions for HP-UX	<u>www.hpe.com/info/hpux-serviceguard-docs</u>

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

[Customer Self Repair](#)

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

[Hewlett Packard Enterprise Information Library](#)

Documentation feedback

Hewlett Packard Enterprise 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@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

More on HPE Management Homepage (HPE SMH) documentation

For more information on documentation and other manuals of HPE System Management Homepage (SMH), see **[System Management Homepage \(SMH\) Software](#)**.

4 Content updates, release updates, and new/changed information in this document edition

The following sections list content updates, release updates, and new/changed information in this document edition for HPE System Management Homepage (HPE SMH) releases.

June 2017 release for Linux and Windows

As per SMH EOL terms, future patch releases will continue to provide fixes for security vulnerabilities and might not provide support to any new OS or Browser. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

Supports for the following operating system:

- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 6.9 for x86 and AMD64/EM64T
- SUSE Linux Enterprise Server 12.2

Supports for the following browser:

- Firefox 52 ESR

Updated the following components:

- PHP to version 5.6.27
- OpenSSL to version 1.0.2k
- Apache to version 2.4.25

November 2016 release for Linux and Windows

HPE SMH 7.6 for Linux and Windows is the last release for this product and after this release the product will move into maintenance phase. The HPE SMH includes the following product enhancements. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated. The product has also been rebranded to carry Hewlett Packard Enterprises brand.

Support for the following new browser:

- Google Chrome 50 or higher

Support for the following operating systems:

- Windows Server 2016 managed node support – Standard and Datacenter and Essentials editions
- Windows Server 2016 CMS support
- RHEL 7.2 CMS support
- SLES 12.1 support
- RHEL 6.7 CMS support
- RHEL 6.8 managed node support

April 2016 release for Linux and Windows

SMH 7.5 Update 5 for Linux and Windows includes the following product enhancements. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

- Support for the following new browsers:
 - Google Chrome 47.0
 - Internet Explorer 11
- Support for the following operating systems:
 - Supports Red Hat Enterprise Linux 7.2
 - Support SUSE Linux Enterprise Server 12.1
- Updated the following components:
 - PHP to version 5.5.31
 - Curl to version 7.47.0
 - OpenSSL to version 1.0.2g
- SSL Protocol – user can enable or disable SSL protocols by listing all the protocols with '+' to enable and '-' to disable, separated by semicolon.

For example: `smhconfig -H -SSLv2;-SSLv3;+TLSv1;+TLSv1.1;+TLSv1.2`

Where, SSLv2 and SSLv3 are disabled and TLSv1, TLSv1.1, TLSv1.2 are enabled.

NOTE: To enable all the protocols, use `All` command.

August 2015 release for Linux and Windows

SMH 7.5 Update 1 for Linux and Windows includes the following product enhancements. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

- Support for the following new browsers:
 - Google Chrome 43.0
 - Firefox 38 ESR
- Support for the new operating systems:
 - Supports Red Hat Kernel-based Virtual Machine
 - Supports Red Hat Enterprise Linux 7 update 1 for x86 and AMD64/EMT64
 - Supports Red Hat Enterprise Linux 7 for x86 and AMD64/EMT64

March 2015 release for Linux and Windows

SMH 7.4 Update 2 for Linux and Windows includes the following product enhancements. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

- Support for the following new browsers:
 - Google Chrome 40.0
 - Firefox 31 ESR
- Support for the new operating systems:
 - Supports Red Hat Enterprise Linux 5.11 for x64 and AMD64/EM64T.
 - Supports Red Hat Enterprise Linux 6.6 for x64 and AMD64/EM64T.
 - Supports SUSE Linux Enterprise Server 12

December 2013 release for Linux and Windows

SMH 7.3 for Linux and Windows includes the following product enhancements. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

- Enhancements:
 - Enabled Simplified Chinese localization
 - Updated English OLH files
 - Updated the following components:
 - Apache to version 2.4.6
 - Libxml2 to version 2.9.1
 - OpenSSL to version 1.0.1e
 - Curl to version 7.32.0
 - PHP to version 5.5.2
 - zlib to version 1.2.8

October 2013 release for Linux and Windows

SMH 7.2.2 for Linux and Windows includes the following product enhancements and defect fixes. The following list of changes are applicable to both Windows and Linux versions, unless specifically stated.

- Enhancements:
 - Enabled support for SUSE Linux Enterprise Server 11 SP3
 - Updated PHP to version 5.4.11
 - Updated libxml2 to version 2.9.0 for Windows

- Updated cURL to version 7.28.1
- Updated libxslt to version 1.1.28
- Defect fixes:
 - Fixed a security issue that could allow escalation of non-administrator privileges to local administrative privileges.

January 2013 release for Linux and Windows

SMH 7.2 for Linux and Windows includes product enhancements and defect fixes. The following list of changes is applicable to both Windows and Linux versions, unless specifically stated.

- Enhancements:
 - Improved certificate management
 - Added support for the following browsers:
 - Firefox ESR 17.0
 - Internet Explorer 10.0
 - Upgraded Apache to version 2.4.3
 - Enabled support for Transport Layer Security (TLS) protocol 1.1 / 1.2
 - Improved User Interface for Online Help
 - Improved CLI options for easier management of SMH configurations
 - Secured HTTP communication
- Defect fixes:
 - Improved login features for the Operating Systems

June 2012 release for Linux and Windows

SMH 7.1 for Linux and Windows includes product enhancements and defect fixes. The following list of changes is applicable to both Windows and Linux versions, unless specifically stated.

- Enhanced to provide information on the webapp availability and loading statistics on the WebApps page.
- Support for the following new browsers:
 - Firefox 9.0
 - Firefox 10.0
- Support for the new operating systems:
 - Windows Multipoint Server 2011 for x64
 - Windows 2008 R2 SP1 - Server Core
 - Red Hat Enterprise Linux 6.2

- Red Hat Kernel-based Virtual Machine
- SUSE Linux Enterprise Server (SLES) 11 SP2
- Inclusion of the revved open source products:
 - Updated PHP version from 5.3.8 to 5.3.10
 - Updated libxml2 to version 2.7.8
 - Updated OpenSSL version from 1.0.0e to 1.0.0h
 - Updated cURL version from 7.21.7 to 7.24.0

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

- Secured handling of the HTTP response

February 2012 release for Linux and Windows

SMH 7.0 for Linux and Windows includes product enhancements and fixes for internally found defects. The following list of changes is applicable to both Windows and Linux versions unless specifically stated.

- Improved CLI options, for easier management of SMH configurations
- Improved CLI options, for Kerberos group validation (Windows only)
- Clarified log messages
- Updated HTTP links
- Improved handling of the following components:
 - SMH configuration file and settings
 - IP fields
 - CLI options
 - Memory resources
 - Revoked trusted certificate
- Support for the following new features:
 - Secured handling of HTTP request and responses
 - A command line option to modify the locality and state information in the SMH PKCS (Public-Key Cryptography Standards) data
- Support for the following new browsers:
 - Microsoft Internet Explorer 9.0
 - Firefox 6.0

- Firefox 7.0
- Firefox 8.0
- Inclusion of the revved open source products:
 - Updated PHP version from 5.3.3 to 5.3.8
 - Updated OpenSSL version from 0.9.8n to 1.0.0e
 - Updated cURL version from 7.21.3 to 7.21.7
 - Apache to version from 2.2.15 to 2.2.21

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

April 2011 release for Linux and Windows

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

- Command Line Interface option to list the current settings in SMH.
- Enhanced management of SMH self-signed certificate.
- Consolidated API logging for 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
 - Microsoft Windows Server 2008 R2 SP1
 - Red Hat Enterprise Linux 6
 - Red Hat Enterprise Linux 5 update 6 for x86 and AMD64/EMT64

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 System Management Homepage.

September 2010 release for Linux and Windows

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 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 System Management Homepage.

March 2010 release for Linux and Windows

SMH 6.1.0 provides the provides the following functionalities over previous 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 System Management Homepage.

- Support for Firefox web browser version 3 and 3.5.

November 2009 release for Linux and Windows

Following are the product enhancements for the 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.

January 2009 release for Linux and Windows

SMH 3.0 provides the following functionality over previous 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:

- **HPE 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
- **HPE Integrity servers**
 - Microsoft Windows Server 2008 for Itanium-based systems, 64-bit

5 Security bulletin and alert policy for non-Hewlett Packard Enterprise owned software components

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

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

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

Hewlett Packard Enterprise 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 Hewlett Packard Enterprise:

1. Open a browser and go to the Hewlett Packard Enterprise home page at <http://www.hpe.com>.
2. Click the **Download Drivers** under **Support**.
3. Click **Sign up: driver, support, & security alerts**, which appears under **Other support resources**.
4. Do one of the following:
 - Under **Subscribe today** enter your Email address, First and Last name, product information, and click **Subscribe**.
 - Under **Already subscribed?** sign in to customize your preferences and update your profile.

6 Related information

This chapter gives more insight about related information about SMH

SMH documentation

For more information about SMH, see the following sources:

- ***Hewlett Packard Enterprise 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 Hewlett Packard Enterprise Technical Documentation website at **HP-UX Product Manuals**, select HP-UX System Administration 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 SMH web page at **System Management Homepage documentation**.
- ***Hewlett Packard Enterprise System Management Homepage Help System***
The help system provides a complete set of documentation for using, maintaining, and troubleshooting SMH. In SMH, go to the **Help** menu.
- ***Hewlett Packard Enterprise System Management Homepage Installation Guide***
The installation guide provides information about installing and getting started using SMH. It includes an introduction to basic concepts, definitions, and functionality associated with SMH. The installation guide is available on the Hewlett Packard Enterprise Technical Documentation website at **HP-UX Product Manuals**, select HP-UX System Administration 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 SMH web page at **System Management Homepage documentation**.
- ***Hewlett Packard Enterprise System Management Homepage User Guide***
The user guide provides a complete set of documentation for using, maintaining, and troubleshooting SMH. The user guide is available on the Technical Documentation website at **HP-UX Product Manuals**, select HP-UX System Administration 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 SMH web page at **System Management Homepage documentation**.
- ***Simplifying single-system management on HP-UX 11i System Management Homepage (SMH)***
This white paper introduces SMH and its various plug-ins. The use cases involving SMH plug-ins highlight the features provided by SMH. The white paper is available on the Technical Documentation website at **HP-UX Product Manuals**, select HP-UX System Administration 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 - System Management Homepage (SMH)."
- ***Safe and Powerful: Security in HP-UX System Management Homepage (SMH)***
This white paper provides an overview of the security aspects in 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 Technical Documentation website at **HP-UX Product Manuals**, select HP-UX System Administration 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.
- **System Management Homepage website**
The website provides SMH information and product links. Go to the SMH website at [HPE System Management Homepage Software](#).
- **Insight Essentials software page**
This web page is at [Server Management](#).

HP-UX documentation

For more information about using SMH in an HP-UX environment, see the following sources. They are available on the Instant Information DVD and on the Technical Documentation website at **HP-UX Product Manuals**.

- **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 SMH.
- For HP-UX operating system release documentation, check for the latest version on **HP-UX Product Manuals**.