Hewlett Packard Enterprise

HPE BladeSystem Onboard Administrator 4.60

Release Notes

Abstract

This document provides Onboard Administrator release information for version 4.60. This document supersedes the information in the documentation released with the previous version. This document is intended for the person who installs, administers, and troubleshoots the Onboard Administrator.

Part Number: 778713-004
August 2016
Edition: 5

Contents

Description

The HPE BladeSystem Onboard Administrator is the intelligence of the HPE BladeSystem c-Class infrastructure (c3000 or c7000). It is the enclosure management processor, subsystem, and firmware base that supports the HPE BladeSystem c-Class enclosure and all the managed devices contained within the enclosure.

Onboard Administrator provides a single point where management tasks can be performed on server blades or switches within the enclosure. Management tasks can be performed using the Onboard Administrator GUI, command line interface, and the enclosure's display (HPE Insight Display).

Onboard Administrator provides:

- Wizards for simple, fast setup and configuration.
- Highly available and secure access to the HPE BladeSystem infrastructure.
- Security roles for server, network, and storage administrators.
- Agent-less health, status, and thermal logic power/cooling information and control.

Before proceeding with Onboard Administrator setup, Hewlett Packard Enterprise recommends referring to the HPE BladeSystem c3000 or c7000 Enclosure documentation at the Hewlett Packard Enterprise BladeSystem Information Library (**http://www.hpe.com/support/BladeSystem/docs**).

The Onboard Administrator version 4.60 release provides several functionality enhancements and important security enhancements. For more information, see "Enhancements (on page 6)."

Update recommendation

Optional - Update to this firmware version if any documented fixes or enhanced functionality provided by this version would be useful to your system.

Supersedes information

Replaces version 4.50.

Product models

This version of the Onboard Administrator is supported on the following BladeSystem c-Class enclosures:

- c3000 enclosure
- c7000 enclosure

Firmware dependency

For firmware compatibility information, see the HP Service Pack for ProLiant Information Library (**http://www.hpe.com/info/spp/documentation**).

Operating systems

The Onboard Administrator firmware operates in an embedded environment within each enclosure. No specific operating system installation dependency exists.

Languages

In addition to English, which is embedded in the firmware, the Onboard Administrator GUI supports the following language packs:

- Simplified Chinese
- Japanese

Important notes

- **Firmware upgrade**

  The OA 4.50 release introduces a standardized code signing and validation mechanism that enhances the firmware image authenticity.

  For customers using ROM image to upgrade OA:

  For OA with firmware version earlier than 3.50, first upgrade to OA 3.50 and then continue upgrading to OA 4.50 or later versions.

  For customers using Smart Component to upgrade OA:

  OA firmware update mechanisms that rely on HPE Smart Component (for example, EFM) are not be affected by this new code-signing mechanism. For OA firmware versions earlier than 3.50, the Smart Component automatically performs the intermediate upgrade to OA 3.50 before performing the upgrade to OA 4.50 or later.

- **Flash Disaster Recovery**

  Flash Disaster Recovery to OA 4.50 or later is not supported. The change is due to the implementation of a new firmware image signing mechanism in OA firmware version 4.50 and later, which causes the Flash Disaster Recovery mechanism to identify the firmware image as an invalid image.

  The workaround for this is to use the Flash Disaster Recovery procedure to recover to a firmware version prior to 4.50 and then perform a firmware upgrade to the intended version (4.50 or later).

- **EFM**

  The OA only supports SPP ISO images that are less than 4GB in size, whether hosted directly via the Enclosure DVD feature or an attached USB key, or mounted remotely via a specified URL. If an ISO image exceeds 4 GB, the CLI `SHOW FIRMWARE MANAGEMENT` command displays ISO URL Status as `Invalid URL`.

  For SPP ISO images that are greater than 4GB in size, you must create a custom ISO image that excludes components not required for the OA EFM blade firmware update process. At minimum, the custom ISO image must contain the firmware components for HPE ProLiant BL servers. (When using HP SUM to create the custom ISO image, select **Firmware** as Component Type, and select **HP ProLiant BL Series** as Server Type.) For information about creating a custom ISO image compatible for OA EFM functionality, see the *HPE BladeSystem Onboard Administrator User Guide*. For more information on HP SUM, see HP Smart Update Manager online help or the Hewlett Packard Enterprise Information Library (**http://www.hpe.com/info/hpsum/documentation**).

- **FIPS**

  Onboard Administrator 3.71 has received FIPS 140-2 Certification. For more information, see the NIST CSRC Cryptographic Module Validation Program website (**http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140valall.htm#2587**).

Enhancements

Onboard Administrator 4.60 provides support for the following enhancements:

- **Hardware additions**

  None.

- **Features: additions and changes**

- **General**
  - GUI, CLI, Smart components, help files, URLs, and product names rebranded to align with HPE branding guidelines.
  - Enhanced information reporting of Gen9 servers booted in UEFI mode.
  - Support the configuration of SNMP trap agent address when non-default VLAN is enabled on OA.
  - Enhanced syslog to show the flooding information when VLAN configured nodes flood the management network.
- **Remote Support**
  - Modified to connect to the HPE remote support URL.
- **EFM**
  - Enhanced error handling mechanism in EFM for servers in UEFI boot mode.
  - Enhanced EFM to display a detailed name for smart array controllers.
  - EFM enhanced to identify more devices in the EFM report.
  - Enhanced the status reporting of EFM operations to align with HPSUM return codes.

Fixes

- **General**
  - Resolved EFM discovery/update failure when the server power policy in the EFM configuration is set to "must be off".
  - Resolved an issue of time synchronization between active and standby OA when date and time settings were changed from "Manual" to "NTP".
  - Resolved an issue where information on only the last server NIC port of a multiport adapter was shown on GUI and CLI. Now details of all the server NIC ports are displayed.
  - Corrected the type mismatch of ORD cpqRackCommonEnclosureManagerLocation, which could cause failures in the SNMP clients. The definition is changed from STRING to INTEGER.
  - Resolved an issue where iLOs became inaccessible after OA failover occurs with iLOs configured in EBIPA for IPv6. This occurs when an external router in the management network is configured to send Router Advertisements.
  - Fixed an issue where all iLOs were reset after making EBIPA changes to an empty bay. Now only the specific iLOs are reset.
  - Fixed an issue where OA lost its IP address after a OA firmware upgrade when ENCLOSURE_IP_MODE was enabled.
  - Addressed an issue where EFM was reporting success when the firmware update of iLO 4 failed.
  - Resolved an issue where connecting to Blade Servers with some specific versions of iLO firmware using the "CONNECT SERVER" CLI would result in successful connection but without displaying the "hpiLO" prompt.
- **Security**

  The following security vulnerabilities were fixed:
  - CVE-2015-5364 – Addressed a vulnerability in UDP stack that can be exploited in UDP flood scenario to cause Denial of Service (DoS) in the OA.
  - CVE-2015-5621 – Addressed a vulnerability in Net-SNMP that causes a DoS and possibly allows execution of arbitrary code via a crafted packet..

- CVE-2015-6563 – Addressed a vulnerability in OpenSSH that allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid.
- CVE-2015-6564 – Addressed a vulnerability in OpenSSH that might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpected early MONITOR_REQ_PAM_FREE_CTX request.
- CVE-2015-3195 – Addressed a vulnerability in OpenSSL that can be exploited to obtain sensitive information from process memory by triggering a decoding failure in a PKC#7 or CMS application.
- CVE-2015-3196 – Addressed a vulnerability in OpenSSL that results in a DoS by remote servers via a crafted ServerKeyExchange message.
- CVE-2015-8605 – Addressed a vulnerability in IPv4 stack that can be exploited to cause a DoS via an invalid length field in a UDP IPv4 packet.
- CVE-2015-0797 and CVE-2016-0799 – Addressed a vulnerability in OpenSSL that could enable security attacks by passing large amounts of untrusted data to certain functions in OpenSSL.
- CVE-2012-3954 – Fixed a memory leak issue in DHCPv6 daemon that could result in out of memory condition in OA.
- CVE-2015-8605 – UDP payload length not properly checked. Addressed a vulnerability where a badly formed packet with an invalid IPv4 UDP length field can cause a DHCP server, client, or relay program to terminate abnormally.
- CVE-2016-2108 – Addressed a vulnerability in ASN.1 implementation in OpenSSL that can cause a DoS via any field in crafted serialized data.

Issues and workarounds

- **Browsers**
  - OA GUI is not accessible in Chrome versions 43.0.2357.10 to 44.0.2383.

    The issue was caused by a “regression” in Chrome (or WebKit). Customers should use an alternative browser like Firefox or Internet Explorer or try a different version of Chrome.
  - SSO-to-iLO connection from the OA using an iLO host name fails with Microsoft Internet Explorer 11 on Windows 8.

    On a Windows 8 system with Internet Explorer 10 or Internet Explorer 11, if the OA web GUI session is loaded using a host name instead of an IP address, an attempt to open an iLO window using SSO from the OA web GUI might result in the iLO page loading in the OA web GUI window instead of the intended new window.

    This issue was determined to be a bug in Internet Explorer and is expected to be fixed in a future release or update for Internet Explorer. To work around this issue, either use an IP address to load the OA Web GUI, or turn off Protected Mode for the appropriate zone in Internet Explorer’s settings. This issue occurs only on Internet Explorer browsers.
- **FIPS**
  - Certificates smaller than 2048 bits in size are not compliant with FIPS requirements as enforced by the OA firmware starting with OA 4.20. When the OA running OA firmware version 4.40 or greater is operating in FIPS Mode ON/DEBUG and is configured with a 1024-bit LDAP certificate that was installed when running a previous version of OA firmware, FIPS Mode ON/DEBUG is considered to be operating in a degraded state due to the presence of the non-compliant certificate. While operating in this FIPS-Degraded Mode operational state, attempts to set FIPS Mode OFF from the OA GUI **Network Access>FIPS tab** will fail and show the error message `The selected FIPS mode is already enabled`. When the non-compliant certificate is

removed, the FIPS-Degraded operational status is cleared, FIPS Mode can then be successfully set to OFF from the GUI interface. Note that the OA CLI command SET FIPS MODE OFF can be successfully used to set FIPS Mode OFF even with non-compliant 1024-bit LDAP certificates installed in the OA.

Prerequisites

To access the OA web interface, you must have the OA IP address and a compatible web browser. You must access the application through HTTPS (HTTP packets exchanged over an SSL/TLS-encrypted session).

The OA web interface requires an XSLT-enabled browser with support for JavaScript 1.3 or the equivalent.

Supported browsers include:

- Microsoft Internet Explorer 8, 9, 10, 11
- Mozilla Firefox ESR 17 and ESR 24
- Google Chrome

Before running the web browser to access the OA GUI, you must enable the following browser settings:

- ActiveX (for Microsoft® Internet Explorer)
- Cookies
- JavaScript

If you use an installed language pack with the OA GUI, and the browser does not display all characters correctly, make sure the operating system has the corresponding language support installed.

Installation instructions

For installation instructions, see the *HPE BladeSystem Onboard Administrator User Guide*.

Acronyms and abbreviations

CMVP

Cryptographic Module Validation Program

EFM

Enclosure Firmware Management

FIPS

Federal Information Processing Standard

HP SUM

HP Smart Update Manager

HPE SIM

HPE Systems Insight Manager

HTTPS

hypertext transfer protocol secure sockets

iLO

Integrated Lights-Out

IPv6

Internet Protocol version 6

ISO

International Organization for Standardization

LDAP

Lightweight Directory Access Protocol

NIST

National Institute of Standards and Technology

OA

Onboard Administrator

PSU

power supply unit

RSA

Rivest, Shamir, and Adelman public encryption key

RTC

real-time clock

SSL

Secure Sockets Layer

SSO

single sign-on

SSP

Selective Storage Presentation

UEFI

Unified Extensible Firmware Interface

USB

universal serial bus

Related information

The latest documentation for the Onboard Administrator is available at the Information Library (**http://www.hpe.com/info/docs**) (select the **HP BladeSystem** radio button under **Products and Solutions**, then select the **HP Onboard Administrator** check box under **HP BladeSystem**).

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 (**mailto: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.