

Oracle Hardware Management Pack 2.4 Security Guide



E72069-08
May 2023



Oracle Hardware Management Pack 2.4 Security Guide,

E72069-08

Copyright © 2017, 2023, Oracle and/or its affiliates.

Primary Author: Ralph Woodley

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Copyright © 2017, 2023, Oracle et/ou ses affiliés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, la documentation du logiciel, les données (telles que définies dans la réglementation "Federal Acquisition Regulation") ou la documentation qui l'accompagne sont livrés sous licence au Gouvernement des États-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des États-Unis, la notice suivante s'applique :

UTILISATEURS DE FIN DU GOUVERNEMENT É.-U. : programmes Oracle (y compris tout système d'exploitation, logiciel intégré, tout programme intégré, installé ou activé sur le matériel livré et les modifications de tels programmes) et documentation sur l'ordinateur d'Oracle ou autres logiciels Oracle. Les données fournies aux utilisateurs finaux du gouvernement des États-Unis ou auxquelles ils ont accès sont des "logiciels informatiques commerciaux", des "documents sur les logiciels informatiques commerciaux" ou des "données relatives aux droits limités" conformément au règlement fédéral sur l'acquisition applicable et aux règlements supplémentaires propres à l'organisme. À ce titre, l'utilisation, la reproduction, la duplication, la publication, l'affichage, la divulgation, la modification, la préparation des œuvres dérivées et/ou l'adaptation des i) programmes Oracle (y compris tout système d'exploitation, logiciel intégré, tout programme intégré, installé, ou activé sur le matériel livré et les modifications de ces programmes), ii) la documentation informatique d'Oracle et/ou iii) d'autres données d'Oracle, sont assujetties aux droits et aux limitations spécifiés dans la licence contenue dans le contrat applicable. Les conditions régissant l'utilisation par le gouvernement des États-Unis des services en nuage d'Oracle sont définies par le contrat applicable à ces services. Aucun autre droit n'est accordé au gouvernement américain.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle®, Java, et MySQL sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut être une marque appartenant à un autre propriétaire qu'Oracle.

Intel et Intel Inside sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Epyc, et le logo AMD sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité et excluent toute garantie expresse ou implicite quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Contents

1	Product and Application Security Overview	
	About Oracle Hardware Management Pack	1-1
	Basic Security Principles	1-1
	Oracle Hardware Management Pack Security Summary	1-2
2	Securing Oracle Hardware Management Pack	
	Keep Your Operating System Up to Date	2-1
	The Host-to-ILOM Interconnect Interface	2-1
	Support for Transport Layer Security (TLS) Encryption	2-2
	Support for Using TLS Encryption with IPMI Over an Ethernet Network Connection	2-2
	Support for Using TLS Encryption With Oracle Hardware Management Pack Commands Over an Ethernet Network Connection	2-2
	Choosing SNMP Security Settings	2-3
	Secure Login Passwords When Using ipmitool	2-4
3	Installing or Uninstalling Oracle Hardware Management Pack Components	
	Running the Oracle Hardware Management Pack Installer	3-1
	Uninstall of Oracle Hardware Management Pack	3-1

1

Product and Application Security Overview

This section provides an overview of the Oracle Hardware Management Pack product, including security guide information, and explains the general principles of application security.

The following topics are covered:

- [About Oracle Hardware Management Pack](#)
- [Basic Security Principles](#)
- [Oracle Hardware Management Pack Security Summary](#)

About Oracle Hardware Management Pack

Oracle Hardware Management Pack is available for many x86- based servers and some SPARC-based servers. Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of cross-operating system command-line interface tools (CLI Tools) for managing your servers. These tools are installed on your host operating system so you can perform system management tasks directly from the host. While the Oracle Hardware Management Pack provides useful features for managing an Oracle server, it is completely optional.

With the Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle servers and server modules in your data center with the advantage of not having to connect to two management points, the host and Oracle ILOM. This functionality enables you to use a single IP address (the host's IP) to monitor multiple servers and server modules.

Hardware Management Agent SNMP Plugins run on the host operating system of Oracle servers. The SNMP Plugins use the Oracle Hardware Storage Access Libraries to communicate with the service processor. Information about the current state of the server is fetched automatically by the Hardware Management Agent. For more information on the Hardware Management Agent, refer to the .

You can use the Oracle Server CLI Tools to configure Oracle servers. The CLI Tools work with Oracle Solaris, Oracle Linux, Oracle VM and other variants of the Linux operating systems. For a list of tools, refer to the .

See the Oracle Hardware Management Pack documentation for more information about capabilities and usage.

- Oracle Hardware Management Pack 2.4 Documentation Library at: <https://www.oracle.com/goto/ohmp/docs>
- For general Oracle ILOM information refer to: <https://www.oracle.com/goto/ilom/docs>

Basic Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- Access

Use physical and software controls to protect your hardware or data from intrusion.

 - For hardware, access limits usually mean physical access limits.
 - For software, access limits usually mean both physical and virtual means.
 - Firmware cannot be changed except through the Oracle update process.
- Authentication

Authentication provides a means to identify a person or entity. Set up all authentication features such as a password system in your platform operating systems to verify that users are who they say they are.

Authentication provides varying degrees of security through measures such as badges and passwords. For example, ensure that personnel use employee badges properly to enter a computer room.
- Authorization

Authorization defines what an authenticated user or entity can do. Use authorization to ensure company personnel can only work with hardware and software that they are trained and qualified to use.

For example, set up a system of read/write/execute permissions to control user access to commands, disk space, devices, and applications.
- Accounting

Customer IT personnel can use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

 - Use system logs to monitor user logins. In particular, track system administrator and service accounts through system logs because these accounts can access powerful commands.
 - Periodically retire or archive log files when they exceed a reasonable size, in accordance with the customer company policy. Log files can become very large over time, so it is essential to maintain them.
 - Use component serial numbers to track system assets for inventory purposes. Oracle part numbers are electronically recorded on all cards, modules, and motherboards.

Oracle Hardware Management Pack Security Summary

Important security items to remember when configuring all system management tools are:

- *System management products can be used to obtain a bootable root environment.*

With a bootable root environment, you can obtain Oracle ILOM access, Oracle System Assistant access, and hard disk access.
- *System management products include powerful tools that require root access to run.*

With this level of access, it is possible to change hardware configuration and erase data.

2

Securing Oracle Hardware Management Pack

To help ensure security, refer to the following sections on using Oracle Hardware Management Pack components.

- [Keep Your Operating System Up to Date](#)
- [The Host-to-ILOM Interconnect Interface](#)
- [Support for Transport Layer Security \(TLS\) Encryption](#)
- [Choosing SNMP Security Settings](#)
- [Secure Login Passwords When Using ipmitool](#)

Keep Your Operating System Up to Date

It's very important to keep your system up-to-date with the latest security patches.

For more information on Linux, refer to the administration and security guides of your Linux documentation. You can find Oracle Linux documentation here:

<https://docs.oracle.com/en/operating-systems/linux.html>

For Oracle Solaris 10, 11 or 11.1 operating systems, you can find documentation on updating and securing your operating system here:

<https://docs.oracle.com/en/operating-systems/solaris.html>

The Host-to-ILOM Interconnect Interface

The Host-to-ILOM interconnect is an alternative to the standard, slower Keyboard Controller Style (KCS) internal interface for service processor communication. The Host-to-ILOM interconnect allows clients on the host operating system to communicate with the Oracle ILOM service processor over an internal high-speed interconnect. This interconnect is implemented by an internal Ethernet-over-USB connection, running an IP stack. Oracle ILOM and the host are given internal non-routable IP addresses for communication over this channel.

From the host, you can connect and log in to Oracle ILOM over the Host-to-ILOM interconnect just as if the connection were coming over the network to the system's network management (NET MGT) port. All services or protocols exposed on the management network are made available over the Host-to-ILOM interconnect. As long as valid Oracle ILOM credentials are provided, the Host-to-ILOM interconnect can be used for both browser-based web access or CLI-based Secure Shell client access to Oracle ILOM.

The Oracle Hardware Management Pack installer presents the option of enabling the Host-to-ILOM interconnect on systems that support it. The interface can be left unconfigured during install but is enabled by default. Oracle recommends that the Host-to-ILOM interconnect be enabled only if the networking instruction supports RFC 3927 and the ability to have link-local IPv4 addresses. Also, care should be taken to ensure that the operating system is not acting

as a bridge or router. This ensures that management traffic between the host and Oracle ILOM remains private.

Oracle recommends unique passwords be created for each user on each Oracle ILOM service processor so that a compromised password could not be used against other systems with Oracle ILOM.

For more information, see the *Oracle Hardware Management Pack 2.4 Installation Guide*.

Support for Transport Layer Security (TLS) Encryption

Oracle Hardware Management Pack includes support for TLS encryption for command execution over the network.

- [Support for Using TLS Encryption with IPMI Over an Ethernet Network Connection](#)
- [Support for Using TLS Encryption With Oracle Hardware Management Pack Commands Over an Ethernet Network Connection](#)

Support for Using TLS Encryption with IPMI Over an Ethernet Network Connection

In previous versions of Oracle Hardware Management Pack prior to release 2.4.0.0, network IPMI encryption was handled using the LANPLUS interface. Support has been added to use IPMI with TLS using the custom ORCLTLS interface if it is supported by the target Oracle ILOM service processor (SP). To use IPMI over TLS, the target Oracle ILOM must be version 3.2.8.1 or later. You can verify support by logging into the target Oracle ILOM using the web interface and checking the TLS Sessions setting under Administration > Management Access > IPMI.

If IPMI over TLS support is not available in the target Oracle ILOM SP, the connection will fall back to the LANPLUS interface (if enabled).

Support for Using TLS Encryption With Oracle Hardware Management Pack Commands Over an Ethernet Network Connection

When using Oracle Hardware Management Pack CLI commands that access the Oracle ILOM SP, two methods of access are supported: a local Host-to-ILOM interconnect connection or a remote Ethernet network connection.

- Command execution using local access over the Host-to-ILOM connection is the fastest local interface available. If a Host-to-ILOM connection is not available, the slower local KCS interface is used. Security for local access is built-in and self-contained.

 **Note:**

For systems with an Oracle ILOM version earlier than 3.2.4, you must manually include credentials using the `-H` and `-U` options for any commands that access a service processor. If credentials are not provided the commands will default to the slower local KCS interface to access the local service processor.

- Command execution using remote Ethernet network access is encrypted using TLS by default starting with Oracle Hardware Management Pack 2.4.4. This means that commands that access an Oracle ILOM SP must present login credentials and also a trusted SSL client-side certificate for the target Oracle ILOM SP in order to validate the connection. This certificate checking feature is the default for a remote network connection when using the `fwupdate`, `ilomconfig` and `ubiosconfig` commands.

 **Note:**

Oracle recommends using SSL public key infrastructure on your network. Note that a `--no-cert-check` option is available to use with the `fwupdate`, `ilomconfig` and `ubiosconfig` commands in a safe network environment. However, use of this option makes the TLS connections vulnerable to man-in-the-middle attacks.

For more information on certificate checking, obtaining certificates and service processor access, refer to the "Service Processor Access" section in the for the `fwupdate`, `ilomconfig` and `ubiosconfig` commands.

Choosing SNMP Security Settings

Oracle Hardware Management Pack contains an SNMP Plugin module that extends the native SNMP agent in the host operating system to provide additional Oracle MIB capabilities. It is particularly important to note that the Oracle Hardware Management Pack does not itself contain an SNMP agent. For Linux, a module is added to the `net-snmp` agent, which must be previously installed. For Solaris, a module is added to the Solaris Management Agent.

Likewise, any security settings related to SNMP for the Oracle Hardware Management Pack SNMP Plugin are determined by the settings of the native SNMP agent or service, and not by the plugin. SNMP settings might include:

- **SNMPv1/v2c.** This version provides no encryption and uses community strings as a form of authentication. Community strings are sent in cleartext over the network and are usually shared across a group of individuals, rather than being private to an individual user.
- **SNMPv3.** This version uses encryption to provide a secure channel and has individual user names and passwords. SNMPv3 user passwords are localized so that they can be stored securely on management stations.

Oracle recommends that SNMPv3 be used if supported by the native SNMP agent. See the documentation for `net-snmp` service for instructions on how to configure SNMP securely.

Additionally, Oracle recommends that all SNMP traffic be isolated to a separate, secure management network.



Note:

SNMP functionality is disabled by default and must be enable and configured by the user as described in the *Oracle Hardware Management Pack 2.4 Server Management Agents User's Guide*.

Secure Login Passwords When Using ipmitool

The `ipmitool` command utility provides a broad range of management capabilities. When using `ipmitool` from the Oracle Solaris operating system to access a remote service processor, do not include the login password using the `-P` option in the command line or script as other Oracle Solaris users might be able to see it.

Instead, create a separate text file that contains only the password and use one of the following options when issuing a command or script that requires a login password:

Option	Description
<code>-f password_file</code>	<p>Specifies a file containing the remote Oracle ILOM service processor user account password. For example:</p> <pre># ipmitool -U root -f password.txt -H hostname bmc info</pre> <p>Where <i>hostname</i> is the host name or common name (when using a certificate) of the target service processor and <code>password.txt</code> is the text file containing the user account password.</p> <p>If the <i>password_file</i> argument for this option is absent or the file is empty, the password will default to NULL.</p>
<code>-f -</code>	<p>If a single hyphen character ("-") is used in place of <i>password_file</i>, the password can be read from either piped or redirected standard input. Example:</p> <pre># ipmitool -U root -f - -H hostname bmc info < password.txt</pre> <p>Where <i>hostname</i> is the host name or common name (when using a certificate) of the target service processor and <code>password.txt</code> is the text file containing the remote Oracle ILOM service processor user account password.</p>

For additional information on using `ipmitool`, refer to the man page.

3

Installing or Uninstalling Oracle Hardware Management Pack Components

The following topics are covered:

- [Running the Oracle Hardware Management Pack Installer](#)
- [Uninstall of Oracle Hardware Management Pack](#)

Running the Oracle Hardware Management Pack Installer

The Oracle Hardware Management Pack consists of a set of native install packages that can be installed using the native install tools for an operating system, such as RPM in Linux. In addition, a wizard-based installer can be used to assist with the installation. In addition to adding the native packages, the installer also helps configure the Oracle Hardware Management Pack for use.

Because the Oracle Hardware Management Pack installer must install native packages, it must be run as root or administrator. For more information, see the *Oracle Hardware Management Pack 2.4 Installation Guide*.

Uninstall of Oracle Hardware Management Pack

The Oracle Hardware Management Pack packages can be uninstalled using native package tools, such as Linux RPMs, or using the wizard-based uninstaller that comes with the Oracle Hardware Management Pack. When the native package method is used to remove packages, if you have previously saved a host credentials cache file using Oracle Hardware Management Pack to facilitate accessing Oracle ILOM using the Host-to-ILOM interconnect, the file will not be deleted. In this case, before uninstalling Oracle Hardware Management Pack packages, run the `ilomconfig delete credential` command to delete this file. This file is not used by Hardware Management Pack version 2.4.0.0 and later. If it exists due to a previous version of Hardware Management Pack it should be deleted before doing an uninstall.

Oracle recommends that the wizard-based installer be used to uninstall Oracle Hardware Management Pack. For more information, see the *Oracle Hardware Management Pack 2.4 Installation Guide*.