Oracle® ILOM Feature Updates and Release Notes Firmware Release 3.2.x

Part No: E37450-26
April 2018

Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2.x

Part No: E37450-26

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E37450-26

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Describes firmware enhancements, known issues, and workarounds for Oracle Integrated Lights Out Manager (ILOM) 3.2.x firmware.
- **Audience** – Technicians, system administrators, and authorized Oracle service providers.
- **Required knowledge** – Users should have experience managing system hardware.

Product Documentation Library

Documentation and resources for this product and related products are available at http://docs.oracle.com/cd/E37444_01/index.html.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

Oracle ILOM Firmware Versions and Download Methods

Oracle ILOM Firmware Version Numbering Scheme

Oracle ILOM uses a firmware version numbering scheme that helps you to identify the firmware version you are running on your server or chassis monitoring module (CMM). This numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` - Represents the major version of Oracle ILOM.
- `b` - Represents a minor version of Oracle ILOM.
- `c` - Represents the update version of Oracle ILOM.
- `d` - Represents a micro version of Oracle ILOM. Micro versions are managed per platform or group of platforms. See your platform product notes for details.
- `e` - Represents a nano version of Oracle ILOM. Nano versions are incremental iterations of a micro version.

For example, Oracle ILOM 3.2.1.1.a would designate:

- Oracle ILOM 3 as the major version
- Oracle ILOM 3.2 as a minor version
- Oracle ILOM 3.2.1 as the first update version
- Oracle ILOM 3.2.1.1 as a micro version of 3.2.1
- Oracle ILOM 3.2.1.1.a as a nano version of 3.2.1.1

Tip - To identify the Oracle ILOM firmware version installed on your Oracle server or blade chassis, click System Information > Firmware in the web interface, or type `version` in the command-line interface.

System Firmware Downloads Using MOS

Updates to the Oracle ILOM firmware are available through standalone software updates that you can download from the My Oracle Support (MOS) web site for each Oracle server or blade chassis system. To download these software updates from the MOS web site, see the instructions that follow.

Note - For instructions on how to perform the firmware update, see "Updating Oracle ILOM Firmware" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* .

▼ Download Product Software and Firmware

1. **Go to `http://support.oracle.com`.**
2. **Sign in to My Oracle Support.**
3. **At the top of the page, click the Patches & Updates tab.**
4. **In the Patch Search panel, click Product or Family (Advanced).**
5. **In the Product Is list box, type a full or partial product name until a list of product matches appears in the list box, and then select the product name of interest.**
   Example Product Names: Oracle Server X5-2 or SPARC M6-32.
6. **In the Release Is list box:**
   a. **Click the Down arrow in the Release Is list box to display a list of matching product folders.**
      A list of one or more product software releases appears.
   b. **Select the check box next to the software release of interest.**
      For example: X4-2 SW 1.0.1 or SPARC M6-32 Sun Systems Firmware 9.2
7. **Click Search.**
   A Patch Search Results screen appears displaying a list of patch names and descriptions.
8. **In the Patch Search Results screen, select the Patch Name of interest.**
9. **In the Patch Name selection, click one of the following actions:**

- **Readme – Opens the selected patch Readme file.**
- **Add to Plan – Adds the selected patch to a new or existing plan.**
- **Download – Downloads the selected patch.**

Related Information

- Firmware Downloads and Release History for Oracle Systems (http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html)
- Firmware Resources (http://www.oracle.com/technetwork/systems/patches/firmware/firmware-resources-1429462.html)

SPARC System Firmware Downloads Using Solaris IPS

The latest versions of platform firmware for selected SPARC servers are now available in the Solaris 11.3 Image Packaging System (IPS) Support Repository. System administrators can use the `pkg install` command to access the latest server platform firmware versions. The IPS firmware server packages deliver the exact same files that are currently available for download from My Oracle Support (http://support.oracle.com). The installation of the firmware packages will only place the firmware files into the Solaris file system hierarchy. The administrator of the system must manually run the firmware update process, and then power-cycle the server to complete the firmware update process.

For more information about how to download SPARC platform firmware using the Oracle Solaris IPS method, see the following sections:

- "Before You Begin" on page 13
- "Download SPARC Firmware From the Solaris IPS Support Repository" on page 14

Before You Begin

- Oracle Solaris 11.3 or later must be installed on the SPARC server.
- Users must have an Oracle Solaris support contract to access the Support Package Repository.
- For more information about Solaris IPS, refer to the Solaris 11.3 IPS documentation (http://www.oracle.com/technetwork/server-storage/solaris11/technologies/lifecycle-management-2237945.html).

▼ Download SPARC Firmware From the Solaris IPS Support Repository

1. **Access the Oracle Solaris Support Package Repository.**

2. **Use the `pkg list` command to identify firmware update packages for server.**

   Command Example: `pkg list -af firmware/system/`*ServerType*

   Package names include the name of the server.

3. **Use the `pkg install` command to download the firmware package files.**

   Command Example: `pkg install firmware/system/T5-4`

   The `pkg install` command places the files in the Solaris file system under /`var/firmware/`*ServerType*.

   Tips:

   - For subsequent downloads to the same package name, use the `pkg update` command.
   - To query the package manifest, use the `pkg contents` command.

4. **Refer to the README file for instructions on how to apply the firmware update.**

   Path Example:

   `/var/firmware/system/T5-4/sysfw9-0/p21342653_942e/README.html`

Note - For further firmware update instructions, see "Updating Oracle ILOM Firmware" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

Related Information

- Firmware Downloads and Release History for Oracle Systems (`http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html`)
- Firmware Resources (`http://www.oracle.com/technetwork/systems/patches/firmware/firmware-resources-1429462.html`)

Updates to Oracle ILOM 3.2.1 Firmware

The section lists initial point releases for Oracle ILOM 3.2.1 firmware, as well as known issues and workarounds.

Initial 3.2.1 Point Releases for Servers and Sun Blade 6000 Chassis

The following table identifies the initial Oracle ILOM 3.2.1 firmware point releases that are available for Oracle server service processors (SPs) and chassis monitoring modules (CMMs).

Server SP or CMM	Initial Oracle ILOM 3.2.1 Firmware Point Release
x86 server service processor (SP)	3.2.1.*x* firmware release
Sun Blade 6000 CMM	3.2.1.*x* firmware release
SPARC SP	3.2.1.*x* firmware release

For additional information about server-specific Oracle ILOM features, refer to the administration guide available for your server.

New 3.2.1 Features and Enhancements Summary

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.1.

TABLE 1 New Features and Enhancements Summary as of Oracle ILOM 3.2.1

Feature	Enhancement Description	For More Details, See:
New embedded mini help system for the Oracle ILOM web browser interface	Page-level help content is now available for the Oracle ILOM web interface as of Oracle ILOM 3.2.1. To access the help content, click the "More details..." link on the web page.	
New remote KVMS interface for newly released Oracle servers	The Oracle ILOM Remote Console Plus supports properties for graphically redirecting your host server KVMS devices.	"Using the Oracle ILOM Remote System Console Plus" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
New property for enabling and disabling server components	On systems that support this feature, the Requested Component State (`requested_state`) property allows system administrators to enable and disable components from the Oracle ILOM interfaces.	■ "Manually Enable or Disable an ASR Component" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* ■ "Health State: Definitions" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
New system log	The System Log reports system- and subsystem-level events pertaining to system inventory actions and component health status.	■ "Log Properties" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x* ■ "Log Properties" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
New serial console logging mode property in CLI	The `logging` property allows system administrators to enable or disable host console logging.	"Establishing a Host Serial Console Session to the Server (CLI)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Updated properties for setting the SPARC power policy	Properties as of Oracle ILOM 3.2.1 include: Disabled, Elastic, and Performance.	"Setting SP Power Management Settings for Power Policy (SPARC)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Ability to delete active user sessions	When necessary, such as when a user is away on vacation, system administrators can delete active user sessions	"Manage User Authenticated Sessions per Managed Device" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
New Verified Boot Feature for SPARC	Verified Boot can be used to verify system boot blocks and Oracle Solaris kernel modules before they are loaded on the system.	"Configuring SPARC Verified Boot Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Oracle ILOM 3.2.1 Known Issues

This section describes known issues and workarounds as of Oracle ILOM 3.2.1. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Issue Description	Link
Oracle ILOM creates a directory in your home directory when you launch the Remote Console Plus	"Directory Created Upon Launching Oracle ILOM Remote Console Plus" on page 17
Web browser connection to Oracle ILOM hangs when using IE 9	"Internet Explorer (IE) 9 - Exhibiting Slow Response Time or Time-Out Behavior " on page 17
Web browser connection to Oracle ILOM hangs when using Firefox and an HTTPS connection	"Firefox Version 13 or Later: HTTPS Connection Exhibiting Slow Response Time or Time-Out Behavior" on page 18
WS-MAN configuration properties fail to back up in Oracle ILOM 3.2.1 or later	"Misleading Error Message When Backing Up WS-MAN Properties in Oracle ILOM 3.2.x" on page 19
Oracle ILOM clock on systems configured for Israel timezone transitions to standard time early	"Systems Configured for Israel Timezone: Use Europe/ Athens Timezone to Correct SP or CMM Clock Transition for New DST End Date" on page 19

Directory Created Upon Launching Oracle ILOM Remote Console Plus

Bug 15820344

Issue: When you launch the Oracle ILOM Remote Console Plus, the following directory is created in your home directory:

```
V3.00E10P2 Build Number_ Testing
```

Update: This is expected behavior. Ignore the directory.

Internet Explorer (IE) 9 - Exhibiting Slow Response Time or Time-Out Behavior

Issue: Experienced one or more of the following behaviors with the IE 9 browser: 1) Unable to establish a web connection to Oracle ILOM after logging in and providing a password; 2) Experienced a long delay after clicking on a tab in Oracle ILOM; 3) Received a browser timeout error message.

Workaround: Follow these steps to edit the system registry by adding an internet setting for background connections.

1. Open the Registry Editor (regedit.exe).

   For example, click Start, click Run, type `regedit`, and click OK.

2. Navigate to the following registry key:

   HKEY_CURRENT_CONFIG > Software > Microsoft > Windows > Current Version> Internet Settings
3. In the Edit menu, point to New, and then click DWORD Value.
4. Type `BackgroundConnections` and press Enter.
5. Perform the following to set a value for the new BackgroundConnection entry:

   a. Select the BackgroundConnections entry.
   b. Click Edit > Modify;
   c. Set value to `0`
   d. Click OK
6. Confirm that new registry entry for DWORD was created with a value of `0`.
7. Restart Internet Explorer.

Firefox Version 13 or Later: HTTPS Connection Exhibiting Slow Response Time or Time-Out Behavior

Issue: Experienced one or more of the following behaviors when using a Firefox browser and an HTTPS connection: 1) Unable to establish a web connection to Oracle ILOM after logging in and providing a password; 2) Long delay occurs after clicking on a tab in Oracle ILOM; 3) Received a browser time-out error message.

Workaround: Follow these steps to resolve Firefox HTTPS connections with Oracle ILOM.

1. In the Firefox URL text box, type: `about:config`
2. Accept the following message by clicking "`I'll be careful, I promise!`".

   This might void your warranty!
3. Search for `network.http.spdy.enabled`
4. If `network.http.spdy.enabled` is found, do the following:

   a. Double-click `network.http.spdy.enabled` and set the value to `false`.
   b. Close and restart Firefox.

Misleading Error Message When Backing Up WS-MAN Properties in Oracle ILOM 3.2.x

Issue: As of firmware release 3.1.2, the WS-MAN API has been deprecated in Oracle ILOM and it will no longer be supported in future Oracle ILOM firmware releases. Therefore, if you upgrade the Oracle ILOM firmware to 3.2.1 or later and attempt to back up the SP configuration containing WS-MAN properties, Oracle ILOM displays the following error message:

```
Config restore: Unable to restore property                                    '/
SP/services/wsman/https_port', permission denied.
```

Update: The above restore error message is misleading since it implies that the back up operation for the WS-MAN properties failed due to user permission levels. In this case, Oracle ILOM failed to back up the WS-MAN properties because the WS-MAN properties are no longer supported by Oracle ILOM as of firmware release 3.2.1 and later.

Systems Configured for Israel Timezone: Use Europe/Athens Timezone to Correct SP or CMM Clock Transition for New DST End Date

Issue: If the Oracle ILOM service processor (SP) or chassis monitoring module (CMM) clock is configured to use the Israel timezone, the clock will incorrectly transition from Daylight Saving Time (DST) to standard time on September 8th, 2013. As of 2013, the DST end date in Israel is the last Sunday in October.

Workaround: For systems configured to use the Israel timezone, change the value of the Oracle ILOM Timezone property for the SP or CMM clock to Europe/Athens. The Europe/Athens timezone shares the same offset from Coordinated Universal Time as the Israel timezone, and transitions from DST to standard time on the last Sunday in October.

You can change the Oracle ILOM Timezone property for the SP or CMM clock in the web interface or command-line interface (CLI).

- In the web interface, click ILOM Administration → Date and Time → Timezone → Europe/Athens.
- In the CLI, type **`set /SP|CMM/clock timezone=Europe/Athens`**.

Documentation Updates and Known Issues

This section describes updates or known issues in the Oracle ILOM Documentation Library as of Oracle ILOM 3.2.1. Specific Bug or Enhancement Request numbers and updates for the issues are provided, where available.

Issue Description	Link
Oracle ILOM guides renamed as of Oracle ILOM 3.2.1	"Oracle ILOM Documentation Library Guides Renamed" on page 20
Abbreviated ILOM titles used under Related Information sections	"Abbreviated Titles Used in Cross References" on page 21
References to remote console application changed	"Remote Console References Changed to Reflect Web Interface Nomenclature" on page 21
Windows Vista support removed	"Windows Vista Support Removed from Documentation" on page 22

Oracle ILOM Documentation Library Guides Renamed

The guides in the Oracle ILOM Documentation Library have been renamed as of Oracle ILOM 3.2.1. The former and current titles are listed below.

Former Title	Current Title
Oracle Integrated Lights Out Manager (ILOM) Quick Start Guide	*Oracle ILOM Getting Started Guide* *Firmware Release 3.2.1*
Oracle Integrated Lights Out Manager (ILOM) User's Guide	*Oracle ILOM User's Guide for System Monitoring and Diagnostics* *Firmware Release 3.2.1*
Oracle Integrated Lights Out Manager (ILOM) Configuration and Maintenance Guide	*Oracle ILOM Administrator's Guide for Configuration and Maintenance* *Firmware Release 3.2.1*
Oracle Integrated Lights Out Manager (ILOM) Basic CLI Command Reference	*Oracle ILOM Quick Reference for CLI Commands* *Firmware Release 3.2.1*
Oracle Integrated Lights Out Manager (ILOM) SNMP, IPMI, CIM, WS-MAN Protocol Management Reference Guide	*Oracle ILOM Protocol Management Reference for SNMP and IPMI* *Firmware Release 3.2.1*

Former Title	Current Title
Oracle Integrated Lights Out Manager (ILOM) Feature Updates and Release Notes	*Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2.1*

Abbreviated Titles Used in Cross References

In the Oracle ILOM guides, abbreviated titles are used to refer to other guides in the Oracle ILOM Documentation Library. The abbreviated titles are listed below.

Complete Title	Abbreviated Title
Oracle ILOM Getting Started Guide Firmware Release 3.2.1	*Oracle ILOM Getting Started Guide (3.2.1)*
Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.1	*Oracle ILOM User's Guide (3.2.1)*
Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.1	*Oracle ILOM Administrator's Guide (3.2.1)*
Oracle ILOM Quick Reference for CLI Commands Firmware Release 3.2.1	*Oracle ILOM Quick Reference for CLI Commands (3.2.1)*
Oracle ILOM Protocol Management Reference for SNMP, IPMI, CIM, WS-MAN Firmware Release 3.2.1	*Oracle ILOM Protocol Management Reference (3.2.1)*
Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2.1	*Oracle ILOM Feature Updates and Release Notes (3.2.1)*

Remote Console References Changed to Reflect Web Interface Nomenclature

In previous iterations of the Oracle ILOM documentation, the remote console applications were referred to as the *Remote Console* and *Remote Console Plus*. To reflect the nomenclature in the Oracle ILOM web interface, these references have been changed to *Remote System Console* and *Remote System Console Plus*, respectively.

Windows Vista Support Removed from Documentation

In previous iterations of the Oracle ILOM documentation, Windows Vista was incorrectly listed as a supported operating system for the remote console feature. Windows Vista has been removed as a supported operating system in the Oracle ILOM documentation library and web interface help pages.

Updates to Oracle ILOM 3.2.2 Firmware

This section includes the following information about the Oracle ILOM 3.2.2 firmware release

New Features and Enhancements for Oracle ILOM 3.2.2

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.2.

TABLE 2 New Features and Enhancements Summary as of Oracle ILOM 3.2.2

Feature	Enhancement Description	For More Details, See:
VLAN Tagging	Enable VLAN tagging to enable the system to generate and process VLAN-tagged Ethernet frames.	"Modifying Default Connectivity Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Virtual Remote Storage Device Feature	Use the Oracle ILOM Virtual Remote Storage Device feature to redirect a remote image file from the SP to the host.	"Redirecting an Image File From a Storage Device to the Host Server" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
BIOS Boot Mode Property (x86 only)	View whether the system is configured to boot in UEFI or Legacy BIOS Boot Mode.	"Web and CLI: BIOS Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
UEFI Diagnostics (x86 only)	For servers shipping with the Unified Extensible Firmware Interface (UEFI) and Oracle ILOM 3.2.2 or later, UEFI Diagnostics replaces PC-Check as the diagnostic test suite.	"Enabling x86 Diagnostics to Run at Boot" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
More Details Provided for On-Board IO Devices	On servers running Oracle ILOM 3.2.2 and Oracle Hardware Management Pack, you can view additional information about on-board IO devices, such as PCIe host bus adapters. This extended information	"Getting Started With Oracle ILOM 3.2.x" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

Feature	Enhancement Description	For More Details, See:
	is available in the command-line interface under the following hierarchies: ■ `/System/Storage` ■ `/System/PCI_Devices` ■ `/System/Networking/Ethernet_NICs` Additionally, a new target has been added to the CLI to provide information about Infiniband devices: `/System/Networking/Infiniband` In the web interface, information about IO devices is provided in the following System Information pages: ■ System Information > Storage ■ System Information > Networking ■ System Information > PCI Devices	

Known Issues as of Oracle ILOM 3.2.2

This section describes known issues that have been reported since the Oracle ILOM 3.2.2 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
There are limitations on the ability to view detailed information about on-board IO devices.	“More Details Limitations on On-Board IO Devices ” on page 24
Special keys become locked after you use key combinations with special keys.	“Special Keys in the Oracle ILOM Remote System Console Plus Become Locked” on page 25
HTTPS Protocol Not Supported for Certain File Transfers	“HTTPS Protocol Not Supported for Certain File Transfers ” on page 29

More Details Limitations on On-Board IO Devices

Issue: As described in “New Features and Enhancements for Oracle ILOM 3.2.2” on page 23, Oracle ILOM provides details about on-board IO devices, such as PCIe host bus adapters. However, there are limitations on this capability:

- Only IPv4 address information is provided for IO devices.
- On x86 systems, this capability is only available on systems running BIOS firmware version 24002100, at minimum.

- On SPARC platforms, enhanced information is not available for the following host bus adapters (HBA):
  - Sun Storage 6 Gb SAS PCIe RAID HBA, Internal
  - Sun Storage 6 Gb SAS REM RAID HBA

Special Keys in the Oracle ILOM Remote System Console Plus Become Locked

Issue: If you use a key sequence that includes a special key in the Oracle Integrated Lights Out Manager (ILOM) Remote Console Plus application, the special key remains engaged for subsequent keystrokes or mouse clicks. For example, if you use the **`Ctrl+Print Screen`** key sequence, the **`Ctrl`** key is locked. Subsequent keystrokes or mouse clicks sent by the remote console application to the host are a combination of the special key and the desired keystroke or mouse click.

Workaround: To unlock the special key, click the button corresponding to the locked key at the top of the Oracle ILOM Remote System Console Plus window.

Resolved Issues as of Oracle ILOM 3.2.2

This section describes the issues that have been resolved as of Oracle ILOM 3.2.2. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Resolved Issue	Link
Audit log object references missing session numbers	"Session Numbers Added to Audit Log Object References" on page 25

Session Numbers Added to Audit Log Object References

Issue: The Oracle ILOM audit log tracks user actions such as logins, logouts, configuration changes, and password changes. Prior to the 3.2.2 firmware release, audit log entries for user logins and logouts included the following generic object reference:

```
object = "/SP/session/type"
```

Administrators were unable to match login and logout events for each user session.

Update: As of firmware release 3.2.2, session numbers have been added to audit log object references to enable you to match login and logout events for each session:

```
Audit
ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
476    Mon Nov 18 18:27:17 2013  Audit     UI        minor
root : Close Session : object = "/SP/sessions/16/type" : value =
"console" : success
475    Mon Nov 18 15:29:46 2013  Audit     UI        minor
root : Open Session : object = "/SP/sessions/16/type" : value =
"console" : success
```

Updates to Oracle ILOM 3.2.4 Firmware

This section includes the following information about the Oracle ILOM 3.2.4 firmware release.

New Features and Enhancements for Oracle ILOM 3.2.4

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.4.

TABLE 3 New Features and Enhancements Summary as of Oracle ILOM 3.2.4

Feature	Enhancement Description	For More Details, See:
Enhanced IP Connectivity Settings available in Oracle ILOM on selected systems.	Oracle ILOM, as of firmware 3.2.4, supports the ability to independently enable or disable the property States for IPv4 and IPv6 network connectivity. In addition, a new static IPv6 gateway property is available for configuration. These enhanced IP settings are available on most new server models and a select number of legacy servers that are running a later software release. **Note -** If the IP connectivity enhancements described in this section are not available for configuration, refer to the server administrator guide or product notes to determine if a later software release is available that supports these IP enhancements.	"Modifying Default Connectivity Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
FIPS Mode	The Oracle ILOM web and command-line interfaces enable you to configure a Federal Information Processing Standards (FIPS) compliant mode. When this mode is enabled, Oracle ILOM uses cryptographic algorithms in compliance with the FIPS 140-2 security standards to protect sensitive or valuable data on the system.	"Operating Oracle ILOM in FIPS Compliance Mode" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
IPMI 2.0	For high security, Intelligent Platform Management Interface (IPMI) v2.0 sessions are enabled by default.	"Modifying Default Management Access Configuration Properties" in *Oracle ILOM*

Feature	Enhancement Description	For More Details, See:
	As an alternative to IPMI v1.5, IPMI v2.0 provides enhanced authentication and IPMI packet encryption.	*Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Oracle ILOM Remote System Console Plus Session Count	By default, Oracle ILOM enables you to launch up to four video redirections of the host console. As of Oracle ILOM 3.2.4, you can optionally limit the number of redirection sessions.	"Modify KVMS Maximum Client Session Count (Optional)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
UEFI Diagnostics (x86 only)	The UEFI Diagnostics configuration paradigm has been simplified to enable you to start and stop the diagnostics tests from the configuration page. In addition, you can view the status of the diagnostic tests in the Oracle ILOM web interface.	"Enabling x86 Diagnostics to Run at Boot" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
Transport Layer Security Protocol Support	Transport Layer Security (TLS) v1.1 and v1.2 have been added as supported protocols for the HTTPS service in Oracle ILOM. TLS provides higher security than Secure Socket Layer (SSL) implementations.	"Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Deprecated SSL and Weak Cipher Properties for HTTPS Management Access Deprecated Weak Ciphers property for SSH Management Access	For greater communication security over the Internet, TLS properties are enabled by default in newer Oracle ILOM firmware releases (3.2.4.x and later). If a managed device is running an older Oracle ILOM firmware release, you should disable the SSL and Weak Ciphers properties and enable the TSL properties.	"Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
IP Address Restriction	Prior to the 3.2.4 firmware release, Oracle ILOM enabled you to assign IP addresses in the following subnetworks to the NET MGT port: ■ 169.254.10.*n* ■ 169.254.11.*n* ■ 169.254.12.*n* However, these IP addresses are reserved for special use. As of the 3.2.4 firmware release, Oracle ILOM issues an error message when you attempt to assign the listed addresses to the NET MGT port.	"Modifying Default Connectivity Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Web Interface Accessibility	The Oracle ILOM web interface has been updated for compliance with Oracle's Accessibility Guidelines.	`http://www.oracle.com/us/corporate/accessibility/index.html`

Known Issues as of Oracle ILOM 3.2.4

This section describes known issues that have been reported since the Oracle ILOM 3.2.4 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
An error appears when you attempt to launch the Oracle ILOM Remote System Console Plus.	“Cannot Launch Oracle ILOM Remote Console Application After Updating Server to 3.2.4 Firmware Release ” on page 29
Special characters in user password causes Snapshot downloads from web interface to fail.	“Snapshot Download Hangs With Use of Special Characters in User Password” on page 30
HTTPS Protocol Not Supported for Certain File Transfers	“HTTPS Protocol Not Supported for Certain File Transfers ” on page 29

HTTPS Protocol Not Supported for Certain File Transfers

Issue: File transfer using the HTTPS protocol is not supported in Oracle ILOM firmware version 3.2.4 and earlier. This limitation, in Oracle ILOM firmware releases 3.2.4 and earlier, affect all file transfers using `dump_uri` or `load_uri` CLI properties, as well as selecting the HTTPS option from the Transfer Method list box in the Web interface.

Workaround: Use a different file transfer protocol.

Cannot Launch Oracle ILOM Remote Console Application After Updating Server to 3.2.4 Firmware Release

Issue: Unable to launch a video redirection of the host console after updating the server firmware to Oracle ILOM 3.2.4. When you attempt to start a redirection session, the following error message appears:

```
Bad Device Capabilities Response Status: 2
```

Workaround: The error message indicates that the remote console version in which you are using is incompatible with the server you are trying to access. If you attempt to access a server running Oracle ILOM 3.2.4 with a version of the remote console application from a prior Oracle ILOM release, the redirection will fail.

In general, it is advisable to access the host using the remote console application on the same server. If you prefer to download the remote console application, ensure that you download the same version of the application that is on the server you want to access.

Snapshot Download Hangs With Use of Special Characters in User Password

Issue: Snapshot will silently fail to run from the Oracle ILOM web interface when using a URL transfer method (FTP/FTP/FTPS/HTTP/HTTPS) that requires a password and the password provided contains one of the following characters: less than sign (<); greater than sign (>); left or right parenthesis (()); single quote ('); double quote ("); backslash (\); semicolon (;); period (.); ampersand (&); dollar sign ($); pipe (|); or apostrophe (').

Workarounds:

- Use the Oracle ILOM CLI to generate the snapshot.
- Download the snapshot file rather than sending the to a URL.
- Change the user account on the remote server to not use a password with non-supported special characters (noted above).

Updates to Oracle ILOM 3.2.5 Firmware

This section includes the following information about the Oracle ILOM 3.2.5 firmware release.

New Features and Enhancements for Oracle ILOM 3.2.5

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.5.

TABLE 4 New Features and Enhancements Summary as of Oracle ILOM 3.2.5

Feature	Enhancement Description	For More Details, See:
Password Policy for All Local Users	Administrators can set password policy restrictions for all local users using the Oracle ILOM CLI or web interface.	"Managing Password Policy Restrictions for Local Users" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Configuration for SSH State and Weak Ciphers	Oracle ILOM provides CLI and web configuration properties for SSH State (enabled by default) and Weak Ciphers (disabled by default). **Note -** For greater security, TLS properties are enabled in Oracle ILOM in newer firmware releases (3.2.4.x and later). If a managed device is running an older Oracle firmware release, you should disable the properties for SSL and Weak Ciphers andenable the properties for TSLv1, 2 and 3.	"Management of SSH Server State and Weak Ciphers" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Enhancements to Banner Message Management	Configuration enhancements for pre-login and post-login banner messages are available in the Oracle ILOM CLI and web interface.	"Management of Banner Messages at Log-In" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Configuration for Automatic Service Requests	Oracle ILOM provides CLI and web configuration properties for Automatic Service Requests.	"Managing Automatic Service Requests" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Configuration for CLI Custom Prompt on	Oracle ILOM provides CLI and web configuration properties for specifying a CLI custom prompt.	"CLI Session Timeout and Custom Prompt Configuration Properties" in *Oracle ILOM*

Feature	Enhancement Description	For More Details, See:
Oracle Network OPUS Switches	**Note -** This feature is initially available on Oracle ILOM OPUS switches.	*Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Enhanced Host History Log for SPARC Domain Servers	The Oracle ILOM web interface provides the ability to view the status history log for domains. **Note -** This enhanced browser-based feature is equivalent to viewing the domain-specific status history logs from the CLI.	"Establishing a Host Serial Console Session to the Server (CLI)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Prepare to Remove and Return Service Actions for SPARC M Series servers.	Oracle ILOM provides CLI and web configuration properties for removing or returning SPARC M series removable components for service.	"Administering Removable Devices on SPARC M-Series Servers" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
Configuration to View Time Stamp in x86 Host Console Log	New Oracle ILOM CLI `timestamp` property for x86 servers under: /HOST/console.	"Establishing a Host Serial Console Session to the Server (CLI)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Known Issues as of Oracle ILOM 3.2.5

This section describes known issues that have been reported since the Oracle ILOM 3.2.5 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
Verified Boot Configuration Limitation on SPARC Servers.	"Verified Boot Policy and Non-Volatile RAM Configuration Might Cause Boot to Fail on SPARC Servers" on page 33
Error message after updating to a later Oracle ILOM firmware release.	"Unable to Power On Host From Web Interface Error Message " on page 33
Firmware update process takes longer than expected on x86 systems.	"x86 Delay BIOS Firmware Option Can Cause a Longer Reset and Multiple Reboots " on page 33
Modifying alert management rules 1 and 2 causes errors to occur on Oracle Netra Modular Systems.	"Restricted Use of Alert Management Rules on Oracle Netra Modular Systems" on page 34
Oracle Solaris remote storage devices do not appear in the Oracle ILOM Remote System Console Plus application.	"Solaris OBP Storage Devices Do Not Appear On Remote System Console Plus" on page 34
Oracle ILOM Java-based remote system console applications not working when Java 7 is present and TLS 1.1 or 1.2 is enabled.	"TLS Limitations On Remote System Consoles When Running Java 7 or Earlier" on page 35
M Series Servers do not support an IPv4 DHCP connection on SP.	"M-Series Servers Do Not Support DHCP Connection on SP" on page 35
Incorrect health state reported for Netra FMM hardware resources.	"Incorrect Fault Management Health State Reported for NMS FMM Hardware Resources" on page 36

Verified Boot Policy and Non-Volatile RAM Configuration Might Cause Boot to Fail on SPARC Servers

Server Platforms: SPARC T and M Series Servers

Server Software: SPARC software release 9.1.0 or later.

Issue: The boot operation on SPARC T and M series servers might fail when the following configuration parameters are set:

- Boot Policy for Verified Boot in Oracle ILOM is set to `Enforce`.
- Non-volatile RAM configuration variable for `use-nvramrc?` is set to `True`.

Note - If a Device Alias is created using the `nvalias` command, the `use-nvramrc?` variable is automatically set to `True`. The `use-nvramrc?` variable can be manually set to `False` by using the `setenv` OpenBoot command. For further details about using OpenBoot commands, see the OpenBoot Command Reference Manual in the Oracle Solaris documentation collection.

Workaround: When the Oracle ILOM Boot Policy for Verified Boot is set to `Enforce`, set the Non-Volatile configuration for `use-nvramrc?` to `False`; or, set the Oracle ILOM Boot Policy for Verified Boot to `None` or `Warning`.

Unable to Power On Host From Web Interface Error Message

Issue: The following error message might appear after updating Oracle ILOM:

```
Internal Error - DCC : Fini : Stack not restored : Page processing terminated
```

Workaround: Clear the cache in the web browser.

x86 Delay BIOS Firmware Option Can Cause a Longer Reset and Multiple Reboots

Server Platform: Oracle x86 server platforms

Issue: If the server has a pending BIOS upgrade, a routine reset will take longer to complete. The pending BIOS upgrade will cause the server to power cycle and reboot several times. This is expected behavior. If the upgrade includes an FPGA update, the process can take as long as 26 minutes to complete.

Note that a pending BIOS upgrade exists when both of theses conditions are true:

- You updated the BIOS and SP firmware using Oracle ILOM.
- During the Oracle ILOM firmware update process, you selected `Delay BIOS Upgrade`.

Workaround: No workaround is necessary. The Issue described in this release note is considered expected behavior.

Restricted Use of Alert Management Rules on Oracle Netra Modular Systems

Server Platform: Oracle Netra Modular Systems

Issue: Errors occur after modifying the Oracle ILOM alert management configuration properties for rules 1 and rule 2.

The alert management properties for rule 1 and rule 2 are reserved for internal system-related functions. If the alert properties for rule 1 or rule 2 are edited on an Oracle Netra Modular System, errors will occur on the system and the management functionality will be adversely affected.

Workaround: Do not edit the alert management properties for rule 1 and rule 2. When needed, configure only the alert management rule properties from 3 to 15.

Solaris OBP Storage Devices Do Not Appear On Remote System Console Plus

Server Platforms: SPARC T and M Series Servers

Software: Oracle Solaris 11.3

Issue: Solaris OBP storage devices do not appear in the Oracle ILOM Remote System Console Plus application.

Workaround: Refresh the Solaris OBP device tree.

TLS Limitations On Remote System Consoles When Running Java 7 or Earlier

Server Platforms: All Oracle server SPs.

Software:

- Oracle ILOM Remote System Console *or* Oracle ILOM Remote System Console Plus
- Java SE Development Kit (JDK) 7 and earlier *or* Java SE Runtime Environment (JRE) 7 and earlier

Issue: The Oracle ILOM Java-based remote system consoles do not support TLSv1.1 or TLSv1.2 when Java 7 (or earlier) is running on the server.

Workaround: Perform one of the following:

- If the server SP is required to operate with TLSv_1.1 enabled or TLSv_1.2 enabled, install Java 8 and then launch and use the Oracle ILOM Java-based remote system console application.

  or
- Enable TLSv_1.0 only and then launch and use the Oracle ILOM Java-based remote system console application.

M-Series Servers Do Not Support DHCP Connection on SP

Server Platforms: M5/M6/M7 server SPs

Software: System Firmware 9.4.3 and earlier

Issue: The Oracle ILOM CLI and web interface provides IPv4 connectivity properties for both DHCP and Static. If the connectivity property for DHCP is enabled, the network connection to Oracle ILOM (server SP) might not work properly.

Workaround: Perform any of the following:

- Enable a Static IPv4 network connection.
- Update to a later system firmware release that is available for your server from My Oracle Support.

Incorrect Fault Management Health State Reported for NMS FMM Hardware Resources

Hardware Platform: Netra Modular System (NMS) Frame Monitoring Module (FMM)

Software: System Software 1.0; System Firmware 3.2.5.14

Issue: At the time of the Netra FMM release, Oracle Solaris Fault Management Architecture (FMA) was not supported. FMM alert notifications were incorrectly generated with a faulted health state. An OK health state should have been reported for the following Netra FMM hardware resources that were incorrectly reported as Faulted:

- Fault fault.frame.computenode.deactivation.policy.mismatch Resource: `/FRAME/FBN/ComputeNode`
- Fault fault.frame.computenode.activation.policy.mismatch Resource: `/FRAME/FBN/ComputeNode`
- Fault: fault.frame.computenode.not-installed Resource: `/FRAME/FBN/ComputeNode`
- Fault fault.frame.computenode.inactive Resource: `/FRAME/FBN/ComputeNode`
- Fault fault.frame.computenode.activation.failed Resource: `/FRAME/FBN/ComputeNode`
- Fault fault.frame.computenode.deactivation.failed Resource: `/FRAME/FBN/ComputeNode`
- Fault fault.frame.computenode.communication-lost Resource: `/FRAME/FBN/computenode`
- Fault fault.frame.computenode.link.fail Resource: /FRAME/FBN/computenode

---

Note - An **OK** health state indicates that the hardware resource is present in the chassis and in use. No known problems have been detect. A **Faulted** health state indicates that the hardware resource is present in the chassis but is unusable because one or more problems have been detected. The hardware resource is disabled (offline) to prevent further damage to the system.

Workaround: Disregard the Faulted alert notifications for the Netra FMM hardware resources listed above. These faulted alert notifications should be treated as an OK alert notification. For more information about fault management behavior in Oracle ILOM, refer to these sections:

- "Administering Open Problems" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*
- "Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

Updates to Oracle ILOM 3.2.6 Firmware

This section includes the following information about the Oracle ILOM 3.2.6 firmware release.

New Features and Enhancements for Oracle ILOM 3.2.6

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.6.

TABLE 5 New Features and Enhancements Summary as of Oracle ILOM 3.2.6

Feature	Enhancement Description	For More Details, See:
Revised Minimum Length Requirement for Local User Account Password Policy	The User Management Password Policy Minimum Length text box accepts values from 1 to 16. **Note -** A password value set to less than 8 characters is considered weak. To ensure greater password security, the password minimum length in the Password Policy should be set to a value of 8 to 16 characters. The Minimum Password Policy Length, by default, is set to 8 characters.	"Managing Password Policy Restrictions for Local Users" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Removed SSL and Weak Cipher Properties for HTTPS Management Access Removed Weak Ciphers Property for SSH Management Access	The SSL and Weak Ciphers properties for management access have been removed.	"Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* "Enable the Strongest TLS Encryption Properties" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
Collection of Fault Data for Oracle ILOM Back Up and Restore Operations	Oracle ILOM supports a new property to optionally include fault data when backing up or restoring the Oracle ILOM configuration.	"Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
New Allowed Services property for the Local	The Oracle ILOM Local Host Interconnect feature supports a new Allowed Services property. This new property enables you to specify one or more allowed	"Dedicated Local Management Connection" in *Oracle ILOM Administrator's Guide for*

Feature	Enhancement Description	For More Details, See:
Host Interconnect Management Connections	communication services for a local host interconnect management configuration.	*Configuration and Maintenance Firmware Release 3.2.x*
Increased SSH RAS Maximum Key Size for Local User Authentication	The maximum RAS key file size for SSH local user authentication was increased to 8192 bits.	"CLI Authentication Using Local User SSH Key" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Support for User Management RADIUS Alternate Server Configurations	Oracle ILOM supports up to five alternate RADIUS server configurations for remote user authentication.	"Configuring RADIUS" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Revised List of Supported Web Browsers	Updates were made to the supported web browser list.	"Supported Web Browsers for Oracle ILOM" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Revised Minimum User Role Requirement for Backing up or Restoring the Oracle ILOM Configuration	As of later releases of Oracle ILOM firmware 3.2.6.x, the Admin (a) role is required at a minimum to initiate a back up or restore operation of the Oracle ILOM configuration. Note that only the configuration properties in which you have privileges to change are backed up or restored to the SP or CMM.	"Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
The Verbosity Debug option for SPARC `/host/diag` is no longer supported on newer SPARC servers (T7, M7, and so on).	The Verbosity Debug setting for newer SPARC servers (T7, M7) is no longer supported as of Oracle ILOM firmware version 3.2.6.x or SPARC SW 9.7.x.	"Setting Diagnostic Tests to Run" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
New Oracle ILOM Remote System VNC Console	The Oracle ILOM Remote System VNC Console is supported for use on newer SPARC server hardware releases (S7-2 and later series servers (SW 9.7.2 or later)).	"Connecting to the Oracle ILOM Remote System VNC Console" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Host management support for configuring NEBS Mode on new Netra SPARC servers.	The Network Equipment-Building System (NEBs) mode is available for configuration on new Netra SPARC servers (such as Netra SPARC S7-2, running SW 9.7.2 or later).	"Setting Host Control and Boot Properties on SPARC Host Server" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Removed SNMP Support for Performing Backup and Restore Operations of the SP	The ability to use SNMP to backup or restore the Oracle LOM configuration has been removed in Oracle ILOM firmware version 3.2.6.x and will not be supported in future releases. **Note -** Oracle ILOM continues to support backup and restore functionality of the SP or CMM configuration files using the Oracle ILOM CLI or web interface. .	"Manage Oracle ILOM Backup and Restore Configurations (SNMP)" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x* "Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Known Issues as of Oracle ILOM 3.2.6

This section describes known issues that have been reported since the Oracle ILOM 3.2.6 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
Boot Device Error Received on x86 Servers.	"Error Received After Setting x86 Boot_Device to CDROM " on page 39
Firefox Certificate Warning Page in CMM Web Interface Is Missing the Add Exception Button To Bypass the Certificate Error	"Firefox Fails to Load Oracle ILOM Web Pages From CMM Due to Certificate Error" on page 40
Table Numbering Issue Seen in *Oracle ILOM 3.2 Administrator's Guide*	"Table Numbering Off in HTML Version of Oracle ILOM Administrator Guide for Configuration and Maintenance" on page 40
Web browser help topics not updated.	"Help Topics (More Info) Not Updated in Oracle ILOM Web Interface " on page 41

Error Received After Setting x86 Boot_Device to CDROM

Oracle ILOM Firmware Release: 3.2.6 and later

Oracle Servers: x86 Oracle Servers

Issue: After issuing the following command the following error appeared.

```
set boot_device=cdrom

Reboot and Select proper Boot device or Insert Boot Media in selected Boot
device and press a key
```

Update: The boot list target names have changed as of Oracle ILOM 3.2.6 firmware release. Use the `show` command to view the device boot targets and the `set` command to configure the device boot target. For example:

```
show /SP/bootlist

set /SP/bootlist bootdev=<n>
```

Firefox Fails to Load Oracle ILOM Web Pages From CMM Due to Certificate Error

Mozilla FireFox Version: 5.0.1 and later

Oracle ILOM Firmware Release: 3.x.x and later

Oracle Hardware: Chassis Monitoring Module (CMM) and Blade Servers

Issue: After successfully logging in to the CMM and selecting a blade server, a certificate error (`Your connection is not secure. Go Back or Advanced`) appears. After clicking Advanced, the UI control (Add Exception) that enables you to bypass the certificate error and correctly load the web page is not present.

Workaround: To bypass the certificate error and correctly load the web page, follow these steps:

1. In the CMM web interface, right-click the content frame (*frame displaying certificate error*) and select "This Frame" > "Open Frame in New Tab".

   Firefox reloads the certificate error in a single-frame display.
2. In the single-frame display, click Advanced.

   The certificate error message redisplays with the Add Exception button.
3. Click the Add Exception button.

   A dialog to Add a Security Exception appears.
4. In the dialog, click Confirm Security Exception to bypass the certificate warning and to continue loading the web page.
5. Return to the frame that you opened in Step1, then right click and select "This Frame" > "Reload Frame".

   The frame set successfully reloads.
6. Repeat Steps 1 through 5 as needed for chassis component frames that appear without the UI control (Add Exception) to bypass the certificate error.

Update: A fix for this issue is available in later Firefox versions such as version 45.

Table Numbering Off in HTML Version of Oracle ILOM Administrator Guide for Configuration and Maintenance

Topic: Setting Diagnostic Tests to Run

HTML Link: https://docs.oracle.com/cd/E37444_01/html/E37446/z40000061594801.html#scrolltoc

Issue: The table numbering in the list does not match the table numbering in the tables that follow. This issue appears only in the HTML version of the *Oracle ILOM Administrator's Guide for Configuration and Maintenance*.

Workaround: Refer to the "Setting Diagnostic Tests to Run" topic in the PDF version of administrator guide: `https://docs.oracle.com/cd/E37444_01/pdf/E37446.pdf`

Update: The table numbering issue reported in the HTML version of the administrator's guide was fixed per the updated Oracle ILOM 3.2 library publication on April 5, 2016.

Help Topics (More Info) Not Updated in Oracle ILOM Web Interface

Oracle ILOM Firmware Release: 3.2.6.x

Issue: The help topics associated with the following Oracle ILOM web browser pages were not updated to reflect the latest 3.2.8 features.

- Management Access > SSH page
- User Management > Password Policy
- Configuration > Back up and Restore
- User Management > User Accounts

Workaround: For information about using the latest 3.2.8 features, refer to the appropriate online documentation:

Web Page	3.2.6 Feature Change	For details, see
Management Access > SSH	The weak ciphers check box has been removed from the Administration > Management Access > SSH Server page.	"Management Services and Network Default Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
User Management > Password Policy	New support for a one character password policy was added to the ILOM Administration > User Management > Password Policy page.	"Managing Password Policy Restrictions for Local Users" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Configuration > Back up and Restore	A check box to include fault data was added to the ILOM Administration > Configuration > Back up and Restore page.	"Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Web Page	3.2.6 Feature Change	For details, see
User Management > User Accounts	The web help page for User Management. User Accounts incorrectly claims that the Admin (a) User Role is required to modify the Single Sign-On property. The User Management role (u) is required to modify the Single Sign-On property.	"Single Sign-On Service (Enabled by Default)" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Updates to Oracle ILOM 3.2.7 Firmware

This section includes the following information about the Oracle ILOM 3.2.7 firmware release.

Enhancements for Firmware Version 3.2.7

The Oracle ILOM 3.2.7 firmware release is a security and bug fix release.

Deprecation Notices and Important Operating Notes

Deprecation Notice for IPMI 2.0 Management Service

Present Behavior: IPMI 2.0 Management Sessions - Enabled (default). Support for IPMI 2.0 client interfaces.

Future Behavior: The following IPMI Management Service changes will occur in future Oracle ILOM firmware releases after firmware version 3.2.7.

- First feature change: Oracle ILOM will add a new client interface as an alternative to the IPMI 2.0 Client interface.
- Second feature change: The default configuration property for IPMI 2.0 Sessions will change from Enabled to Disabled in a future release. Clients relying on IPMI 2.0 will be

unable to communicate with Oracle ILOM unless the configuration property for IPMI 2.0 Sessions is manually enabled.

- Third feature change: Removal of IPMI 2.0 client support. IPMI 2.0 clients will no longer be able to communicate with Oracle ILOM.

For future updates about IPMI Management Service support in Oracle ILOM, refer to the latest firmware release information published in this guide.

Deprecation Notice for Default Self-Signed Certificate

Present Behavior: An earlier version of the default SSL self-signed certificate is provided by Oracle ILOM.

Future Behavior: A newer version of the default SSL self-signed certificate will be provided in a future Oracle ILOM firmware release.

Impact to Customer Configuration:

After updating to a future firmware release, users connecting to Oracle ILOM through the web interface will need to accept a newer version of the default SSL self-signed certificate that is provided by Oracle ILOM. Customer provided SSL certificates will not be impacted by this change.

For future updates about the default SSL self-signed certificate that is provided by Oracle ILOM, refer to the latest firmware release information published in this guide.

Update for Supported Web Browsers

As of firmware release 3.2.7, the listing of web browsers supported by Oracle ILOM was updated in the Oracle ILOM documentation. For details, see either:

- "Supported Web Browsers for Oracle ILOM" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

  - or -

- "Supported Operating System Web Browsers" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

.

Updates to Oracle ILOM 3.2.8 Firmware

This section includes the following information about the Oracle ILOM 3.2.8 firmware release.

New Features and Enhancements for Oracle ILOM 3.2.8

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.8.

TABLE 6 New Features and Enhancements Summary as of Oracle ILOM 3.2.8

Feature	Enhancement Description	For More Details, See:
New IPMI Over TLS Service	To increase IPMI management security, a new TLS service and interface are supported in Oracle ILOM.	"Server Management Using IPMI" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x* "Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
New SSL Certificate Behavior for Web Interface and Remote Console Users	Unique self-signed Default SSL Certificate and fingerprint ships with each Oracle ILOM instance (SP, FMM, CMM). Additional certificate checks performed by Oracle ILOM for when the self-signed certificate is in use.	"Improve Security by Using a Trusted SSL Certificate and Private Key" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x* "Regenerate Self-Signed Default SSL Certificate Issued By Oracle" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x* "Resolving Warning Messages for Self-Signed SSL Certificate" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
New directory path for X86 Diagnostic output	Diagnostic test output path changed as of Oracle ILOM 3.2.8.	"Enabling and Running Oracle ILOM Diagnostic Tools" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

Feature	Enhancement Description	For More Details, See:
Required Java and TLS versions for Oracle ILOM remote KVMS consoles.	The Java-based Oracle ILOM remote KVMS console applications support the following versions of Java and TLS. ■ Java 8 and 9, or Java 7u131 and later. ■ TLS v1.1 and v1.2	"Requirements for Using the Oracle ILOM Remote System Console" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* "Requirements for Using the Oracle ILOM Remote System Console Plus" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Update for supported web browser versions.	The list of web browsers supported by Oracle ILOM was updated in the Oracle ILOM documentation.	"Supported Web Browsers for Oracle ILOM" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x* "Supported Operating System Web Browsers" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

Known Issues as of Oracle ILOM 3.2.8

This section describes known issues that have been reported since the Oracle ILOM 3.2.8 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
Updated known issue for Oracle ILOM Remote System Console Storage Redirection feature.	"Storage Redirection Feature in Oracle Remote System Console Not Supported With 64-bit Java" on page 46
Web browser help topics not updated.	"Help Topics (More Info) Not Updated in Oracle ILOM Web Interface " on page 47
Incorrect reference to change requests in Feature Updates and Release Notes for Oracle ILOM 3.0.	"Incorrect Change Request Number in Oracle ILOM 3.0 Feature Updates and Release Notes" on page 48

Storage Redirection Feature in Oracle Remote System Console Not Supported With 64-bit Java

Oracle ILOM Firmware Release: 3.0.8.x and later

Bug Number: 15539270

Issue: An attempt to start Storage Redirection might fail when using a 64-bit Java runtime environment (JRE). The 64-bit JRE is the default on a 64-bit system. When using a 64-bit JRE to start Storage Redirection, the following error message appears:

"Redirection is not supported on this platform"

Previously Published Workaround: Install a 32-bit JRE on the 64-bit system. JREs can be downloaded from this site: `http://java.com/en/download/index.jsp`

Updates To This Issue: Java will no longer be offering a 32-bit JVM. The Storage Redirection feature in the Oracle ILOM Remote System Console will no longer work. This issue is being addressed and an update will be published at a later time.

Help Topics (More Info) Not Updated in Oracle ILOM Web Interface

Oracle ILOM Firmware Release: 3.2.8.x

Issue: The help topics associated with the following Oracle ILOM web browser pages were not updated to reflect the latest 3.2.8 features.

- Management Access > IPMI page
- Management Access > SSL page
- Remote Control > Redirection page

Workaround: For information about using the latest 3.2.8 features, refer to the appropriate online documentation:

Web Page	3.2.8 Feature Description	For details, see
Management Access > IPMI	New Oracle TLS IPMI Session Support	"IPMI TLS Service and Interface" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x* "Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
Management Access > SSL	New self-signed Default SSL Certificate Behavior	"Regenerate Self-Signed Default SSL Certificate Issued By Oracle" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
Remote Control > Redirection	Additional SSL certificate checks when the Default SSL Certificate is in use.	"Resolving Warning Messages for Self-Signed SSL Certificate" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Update: The help topics for the Oracle ILOM web interfaces are now available in later Oracle ILOM firmware releases.

Incorrect Change Request Number in Oracle ILOM 3.0 Feature Updates and Release Notes

Known Problem: Incorrect Change Request (CR) Number Assoicated with Known Issue for Storage Redirection Not Supported With 64-bit JRE

Publication: *Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes*

Content : Storage Redirection Not Supported With 64-bit JRE

CR Number Correction: CR 6800702 instead of CR 680070

Updated CR Numbers: CR 7800702 is now known as Bug 15539270 and CR 6805732 is now known as Bug 15542242

Note - This documentation error will not be fixed in the *Oracle ILOM 3.0 Feature Updates and Release Notes*. An updated version of the Storage Redirection limitation appears in the "Storage Redirection Feature in Oracle Remote System Console Not Supported With 64-bit Java" on page 46 .

Updates to Oracle ILOM 3.2.9 Firmware

This section includes the following information about the Oracle ILOM 3.2.9 firmware release.

New Features and Enhancements for Oracle ILOM 3.2.9

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.9.

TABLE 7 New Features and Enhancements Summary as of Oracle ILOM 3.2.9

Feature	Enhancement Description	For More Details, See:
TLS v1.0 is disabled by default.	For greater communication security, the configuration property for TLS v1.0 is disabled by default. TLS v1.1 and 1.2 are enabled by default.	"Web Server Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
Deprecation Notice for IPMI LAN and LANPLUS Services	The IPMI services for LAN and LANPLUS will not be supported in a future Oracle ILOM firmware release. Users will need to use the IPMI TLS service and the provided Oracle interface.	"Server Management Using IPMI" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x*

Known Issues as of Oracle ILOM 3.2.9

This section describes known issues that have been reported since the Oracle ILOM 3.2.9 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
Load and Dump Oracle ILOM CLI operations fail after entering password.	"Load and Dump CLI Commands Fail When Password Contains Non-URL Special Characters" on page 50

Known Issue	Link
Oracle ILOM Remote Console Plus is unable to connect remote storage to Microsoft Windows 7 host.	"Windows 7 Clients Do Not Support Host Storage Device Redirection When TLS v1.0 is Disabled" on page 51
Web browser help topics not updated.	"Help Topics (More Info) Not Updated in Oracle ILOM Web Interface " on page 51

Load and Dump CLI Commands Fail When Password Contains Non-URL Special Characters

Oracle ILOM Firmware Release: 3.2.9.x

Applies to: Load and dump CLI prompt: "Enter remote user password".

Issue: The `load` and `dump` commands fail for the following Oracle ILOM CLI targets upon passing a password containing non-URL special characters.

- `/SP/config`
- `/System/bios/config`
- `/SP/services/ssh/keys`
- `/SP/services/https`

Workaround: Choose one of the following workarounds to resolve this issue:

- Perform these actions using the equivalent functionality in the Oracle ILOM web interface.

  -or-

- In the Oracle ILOM CLI, encode the remote user password when specifying the destination URL.

  For example, if your password is *my_pwd*, the encoded password in a *dump* command URL would look like this:

  `dump -destination http://`*`username`*`:`*`my%3fpwd`*`@`*`hostname`*`:/`*`path`*`/`*`file`*

  where: *username* is the user name for the target host; *my%3fpwd* is an example encoded password for the target host; *hostname* is the name of the target host, *path* is the location to store the file on the target host; and *file* is the name of the file being transferred.

  -or-

- Change the user password on the remote host to an acceptable URL password.

Windows 7 Clients Do Not Support Host Storage Device Redirection When TLS v1.0 is Disabled

Oracle ILOM Firmware Release: 3.2.9.x and later

Client Operating System: Microsoft Windows 7 release

Issue: Host storage device redirections are not seen by Oracle ILOM Remote System Console Plus due to the following disabled TLS protocol settings:

- TLS v1.1 and v1.2 are disabled by default in Windows 7 operating system.

  Note - TLS v1.1 and v1.2 are enabled by default post Microsoft Windows 8.1 releases.

- TLS v1.0 is disabled by default in Oracle ILOM as of firmware version 3.2.9 to increase management security.

Workaround: Windows 7 system administrators need to enable the protocol settings for TLS v1.1 and v1.2 manually. Refer to this Oracle support article (Document ID 2239460.1) for instructions: `https://mosemp.us.oracle.com/epmos/faces/SearchDocDisplay?_adf.ctrl-state=1t2tyqxjx_280&_afrLoop=558018304338317`

Help Topics (More Info) Not Updated in Oracle ILOM Web Interface

Oracle ILOM Firmware Releases: 3.2.8.x , 3.2.9.x

Issue: The help topics associated with the following Oracle ILOM web browser pages were not updated to reflect the latest 3.2.8 features.

- Management Access > IPMI page
- Management Access > SSL page
- Remote Control > Redirection page

Workaround: For information about using the latest 3.2.8 features, refer to the appropriate online documentation:

Web Page	3.2.8 Feature Description	For details, see
Management Access > IPMI	New Oracle TLS IPMI Session Support	"IPMI TLS Service and Interface" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x*

Web Page	3.2.8 Feature Description	For details, see
		"Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
Management Access > SSL	New self-signed Default SSL Certificate Behavior	"Regenerate Self-Signed Default SSL Certificate Issued By Oracle" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*
Remote Control > Redirection	Additional SSL certificate checks when the Default SSL Certificate is in use.	"Resolving Warning Messages for Self-Signed SSL Certificate" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Updates to Oracle ILOM 3.2.10 Firmware

This section includes the following information about the Oracle ILOM 3.2.9 firmware release.

Oracle ILOM Documentation Updates

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.10.

TABLE 8 Updated Documentation

Content	Enhancement Description	For More Details, See:
Updated third-party software licenses.	License Guide updated.	*Licensing Information User Manual Oracle ILOM Firmware Release 3.2.x Last Updated: October 2017*

Updates to Oracle ILOM 3.2.11 Firmware

This section includes the following information about the Oracle ILOM 3.2.9 firmware release.

Oracle ILOM Documentation Updates

The following table identifies some of the firmware feature enhancements for Oracle ILOM 3.2.11.

TABLE 9 Updated Documentation

Feature	Enhancement Description	For More Details, See:
Updated third-party software licenses.	License Guide updated.	*Licensing Information User Manual Oracle ILOM Firmware Release 3.2.x Last Updated: October 2017*

Known Issues as of Oracle ILOM 3.2.11

This section describes known issues that have been reported since the Oracle ILOM 3.2.11 release. Specific Bug or Enhancement Request (ER) numbers and workarounds or updates for the issues are provided, where available.

Known Issue	Link
Oracle ILOM Remote System Console fails if custom authority SSL certificate is not recognized by Java Keystore.	"Oracle ILOM Remote System Console Failure After Uploading a Custom CertificationAuthority (CA) SSL Certificate Chain" on page 56

Oracle ILOM Remote System Console Failure After Uploading a Custom CertificationAuthority (CA) SSL Certificate Chain

Oracle ILOM Firmware Release: 3.2.11 and later

Server Platform: Sun Server X3-2 series models.

Issue: After uploading a CA SSL certificate chain to Oracle ILOM, the Oracle ILOM Remote System Console fails to start and the following message appears:

```
Warning: Certificate validation failed. Could not validate the Remote Host Certificate.
Either a man-in-the middle attack could be occuring or it is possible that the remote
host certificate has been changed.
```

Note - Additional SSL certificate validation checks have been introduced in Oracle ILOM as of firmware version 3.2.11.x.

When an SSL certificate chain is uploaded as a custom certificate to Oracle ILOM, the Oracle ILOM services only transmit the first certificate in the chain, which is known as the server certificate, to the Remote System Console. On the client side, if the intermediate certificate or certificates in the chain are not available in the Java keystore, then the certificate validation will fail.

Workaround: On the client side using the Java `keytool` command, import the intermediate certificate used to sign the server certificate (uploaded to Oracle ILOM) to the Java keystore, for instance:

- On Windows systems, at the command prompt, type:

  `keytool -importcert -alias <`*certalias***`> -file <`***intermediate-cert***`> -keystore "c:\Program Files (x86)\Java\jre[`***version***`]\lib\security\cacerts"`**

  Note - On Windows, the `keytool` command needs to be run as administrator. To start a command prompt as an administrator on Windows: Click Start, click All Programs, and then click Accessories. Right-click Command prompt, and then click Run as administrator.

- On Linux systems, at the command prompt, type:

  `keytool -importcert -alias <`*certalias***`> -file <`***intermediate-cert***`> -keystore [`***Java_home***`]/jre/lib/security/cacerts`**

Reference information:

- Oracle Java Keytool Documentation for Windows
- Oracle Java Keytool Documentation for Linux
- "Improve Security by Using a Trusted SSL Certificate and Private Key" in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*