

# iDRAC9 Version 4.40.40.00

## Release Notes

## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

# Contents

<b>Chapter 1: Release summary.....</b>	<b>6</b>
Priority and recommendations.....	6
<b>Chapter 2: Compatibility.....</b>	<b>7</b>
License Requirements.....	7
Supported systems.....	7
Previous versions.....	9
Supported managed server operating systems and hypervisors.....	9
Supported web browsers.....	9
Supported software.....	10
<b>Chapter 3: New and enhanced features.....</b>	<b>11</b>
iDRAC and LC firmware.....	11
Hardware.....	11
Miscellaneous.....	11
<b>Chapter 4: Fixes.....</b>	<b>12</b>
iDRAC and LC firmware.....	12
Monitoring and alerting.....	12
Networking and I/O.....	12
OS deployment.....	12
Storage and storage controllers.....	12
<b>Chapter 5: Deprecated features.....</b>	<b>13</b>
<b>Chapter 6: Important notes.....</b>	<b>14</b>
<b>Chapter 7: Known issues — To be fixed in future releases.....</b>	<b>18</b>
LC logs display incorrect version change for disks .....	19
Blue screen while deploying OS through Lifecycle Controller .....	19
Server stops responding during POST with Config Error.....	19
OME-M Deployment and Configuration Job Fails with Error LC063.....	19
Unable to generate CSR through Redfish.....	20
vFlash detaching after iDRAC firmware update.....	20
MAC identities displayed in RESERVED state.....	20
SEL events may not be correctly displayed in the earlier versions of iDRAC.....	20
CMC firmware update fails.....	20
Telemetry data Disabled without confirmation.....	21
WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page.....	21
CPU information missing under Hardware Inventory.....	21
Storage Devices displayed in gray text.....	21
Backplane Rollback contents not populating in iDRAC.....	21
Test network connection fails.....	22
MetricReport output does not match the DMTF schema.....	22

Service Validator reporting errors for Redfish API services.....	22
Lifecycle Controller fails to resolve IPv6 DNS addresses.....	22
Performing GET with Top query parameter returns no error.....	23
Server Configuration Profile import job fails.....	23
Unable to add iDRAC Static IP.....	23
Creating virtual media image takes longer on safari browser.....	23
iDRAC displays warning message for different plug-in selection.....	23
Read-only user Virtual Console session disconnects.....	24
iDRAC Virtual Console entering Connecting Viewer state.....	24
PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation.....	24
CPU PPIN in Hardware inventory in iDRAC GUI shows as “Not Supported”.....	24
Performing GET method on chassis PCIe slots displays all PCIe slots.....	24
Virtual Media performance is degraded with QLogic 25G OCP.....	25
iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings.....	25
Virtual console display in iDRAC GUI is blurred.....	25
iDRAC unable to obtain the current time after reboot.....	25
Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs.....	26
Few Virtual Keyboard keys not working for other languages.....	26
DellCertificateCollection URI response not according to DMTF standards.....	26
Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525 .....	26
Field required displayed in Internet Explorer browser.....	26
Firmware update using pud method failing.....	27
Uploaded firmware link not available in the SoftwareImages property in Redfish.....	27
PCIe types and lanes information not getting populated using Redfish.....	27
iDRAC reboots while collecting SupportAssist logs.....	27
Webserver restarts after remote presence port number is updated.....	28
Getting an error SWC0018 during OS installation .....	28
WSMan query with space between attributes fails.....	28
Attributes for CNA cards not displayed through Redfish or RACADM interface.....	28
Unable to create a recurring job after same recurring job was completed.....	28
SCP Import Job completes with error due to HddSeq error.....	29
iDRAC LC Log shows reset cause as ‘Internal Error’.....	29
Access to serial interface fails.....	29
LC log created after going to Virtual media page in iDRAC GUI.....	29
Boot mode error during OS deployment.....	30
Repetitive PR7 messages related to PSU in LC logs after a system erase operation.....	30
After a warm reboot, LC logs display Disk Inserted.....	30
iDRAC DUP update fails in Linux operating systems when secure boot is enabled .....	30

<b>Chapter 8: Limitations.....</b>	<b>31</b>
Authentication.....	31
Automation — API and CLI.....	31
BIOS and UEFI.....	32
Hardware.....	32
iDRAC firmware.....	32
Monitoring and alerting.....	32
Networking and IO.....	33
OS deployment.....	33
Security.....	34
Storage and storage controllers.....	34

SupportAssist and parts replacement.....	34
Firmware and driver update.....	35
Miscellaneous.....	35
<b>Chapter 9: Updating iDRAC firmware.....</b>	<b>36</b>
Downloading iDRAC firmware installation file.....	36
Updating iDRAC firmware from host OS.....	36
Updating iDRAC remotely using iDRAC web interface.....	36
<b>Chapter 10: Lifecycle Controller Remote Services — client tools.....</b>	<b>38</b>
<b>Chapter 11: Resources and support.....</b>	<b>39</b>
<b>Chapter 12: Contacting Dell EMC.....</b>	<b>41</b>

# Release summary


The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell servers. This release adds multiple fixes and enhancements that improve iDRAC stability.

## Version

iDRAC9 4.40.40.00

## Release date

June 2021

 **NOTE:** For details about the previous releases, if applicable, or to determine the most recent release for your platform, and for latest documentation version, see *KB article SLN308699* available at <https://www.dell.com/support/article/sln308699>.

### Topics:

- [Priority and recommendations](#)

## Priority and recommendations

Recommended: Dell recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

# Compatibility


## Topics:

- [License Requirements](#)
- [Supported systems](#)
- [Previous versions](#)
- [Supported managed server operating systems and hypervisors](#)
- [Supported web browsers](#)
- [Supported software](#)


## License Requirements

iDRAC features are available based on the purchased license.

- iDRAC Express—Available by default on all blade servers, and rack or tower servers of 600 or higher series
- iDRAC Enterprise—Available on all servers as an upgrade
- iDRAC Datacenter—Available on all servers as an upgrade.
- iDRAC Secure Enterprise Key Manager(SEKM)—Only available on systems that are mentioned in the Supported Systems section
- BMC – Available on Dell PowerEdge C6420 only.

 **NOTE:** iDRAC Secure Enterprise Key Manager(SEKM) is not supported in this release on Dell PowerEdge MX740c and MX840c.

For more information about the features available for a license, see the iDRAC licenses section in the iDRAC User's Guide available at [dell.com/idracmanuals](http://dell.com/idracmanuals).

 **NOTE:** To manage new and existing licenses, go to the [Dell Digital Locker](#).

## Supported systems


- PowerEdge C4140
- PowerEdge C6420
- PowerEdge C6525
- PowerEdge FC640
- PowerEdge MX740c
- PowerEdge MX840c
- PowerEdge M640
- PowerEdge M640-VRTX
- PowerEdge R240
- PowerEdge R340
- PowerEdge R440
- PowerEdge R540
- PowerEdge R640
- PowerEdge R740
- PowerEdge R740xd
- PowerEdge R740xd2
- PowerEdge R840
- PowerEdge R940
- PowerEdge R940xa
- PowerEdge R6415

- PowerEdge R6515
- PowerEdge R6525
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge R7515
- PowerEdge R7525
- PowerEdge T140
- PowerEdge T340
- PowerEdge T440
- PowerEdge T640
- PowerEdge XE2420
- PowerEdge XE7420
- PowerEdge XE7440
- DCS9660
- DCS9670
- DCS9690
- DSS8440
- DSS9600
- DSS9620
- DSS9630
- Precision 7920 Rack
- 7920 XL Rack
- Dell EMC XC Core XC640 System
- Dell EMC XC Series XC640 Appliance
- Dell EMC XC Series XC6420 Appliance
- Dell EMC XC Core XC6515
- Dell EMC XC Core XC740xd2
- Dell EMC XC Core XC740xd System
- Dell EMC XC Series XC740xd Appliance
- Dell EMC XC Core XC940 System
- Dell EMC XC Series XC940 Appliance
- Dell EMC XC Core XCXR2
- PowerVault NX3200
- Dell Storage NX3330
- OEMR R7525
- OEMR R7515
- OEMR R7415
- OEMR R7425
- OEMR R6415
- OEMR R6515
- OEMR R6525
- OEMR R940
- OEMR R940XA
- OEMR R840
- OEMR R740
- OEMR R740xd
- OEMR R740xd2
- OEMR R640
- OEMR R540
- OEMR R440
- OEMR R340
- OEMR R240
- OEMR T440
- OEMR T640



## Previous versions

- 4.10.10.10
- 4.11.11.11
- 4.20.20.20
- 4.22.00.00
- 4.30.30.30
- 4.32.10.00
- 4.40.00.00
- 4.40.10.00

 **NOTE:** Updating iDRAC firmware from a previous version such as 3.2x, 3.1x, 3.0x to the latest version is not supported. Update the firmware to version 3.30.30.30 first, and then update to version 4.00.00.00 or later.

## Supported managed server operating systems and hypervisors

- Microsoft Windows
  - Server 2016 Essentials
  - Server 2016 Standard
  - Server 2016 Datacenter
  - Server 2019 Essentials
  - Server 2019 Datacenter
  - Server 2019 Standard
  - WinPE 5.0 64-bit
  - WinPE 10
- Linux
  - RHEL 8.4
  - RHEL 7.9
- SLES
  - SLES 15 SP3
- Ubuntu
  - Ubuntu 20.04.1
- VMware
  - ESXi 7.0 U2
  - ESXi 7.0 U1
  - ESXi 6.7 U3

## Supported web browsers

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari 12.x
- Mozilla Firefox 64
- Mozilla Firefox 65
- Google Chrome 75
- Google Chrome 76

# Supported software

## Java

- Java - Oracle version

## OpenSource tools

- OpenJDK 8u202
- Adopt Open JDK
- You may utilize an open source version of AdoptOpenJDK or OpenJDK ("Adopt Open JDK") subject to the terms and conditions of the Adopt Open JDK community at the link below.
- You use Adopt Open JDK at your own risk. Adopt Open JDK may not meet your requirements or expectations. It could include quality, technical or other mistakes, inaccuracies or typographical errors.
- Dell does not provide support or maintenance for Adopt Open JDK.
- Dell makes no express warranties, and disclaims all implied warranties, including merchantability, fitness for a particular purpose, title, and non-infringement as well as any warranty arising by statute, operation of law, course of dealing or performance or usage of trade regarding Adopt Open JDK.
- Dell has no liability to you for any damage that arise out of or relate to your use of Adopt Open JDK.

## iDRAC tools

This version of iDRAC requires the following tools based on the operating system:

- Dell EMC iDRAC Tools for Microsoft Windows Server(R), v10.0.1
- Dell EMC iDRAC Tools for Linux, v10.0.1
- Dell EMC iDRAC Tools for VMware ESXi (R), v10.0.1

This version contains:

- Remote/Local RACADM on Windows or Linux or ESXi
- IPMI Tool on Windows or Linux
- Secured Component Verification (SCV)

Download the DRAC tools from the **Drivers & downloads** page for your system at <https://www.dell.com/support>.

Before installing iDRAC tools from OM 9.5.0, you must uninstall any older versions of DRAC tools. For more information about uninstalling applications, see the documentation for your operating system.

# New and enhanced features

## Topics:

- [iDRAC and LC firmware](#)
- [Hardware](#)
- [Miscellaneous](#)

## iDRAC and LC firmware

- Added support for SEKM features in:
  - PowerEdge XE7420
  - PowerEdge XE7440
- Added support for System Erase with SEKM enabled.

## Hardware

- Added support for AMD EPYC 75F3, 7413, and 7313 CPUs.
- Added support for PM1733 and PM1735 v2 drives.
- Added support for 1100W Titanium power supply units.
- Added support for NVIDIA A100 GPU on PowerEdge R840 and PowerEdge R940xa.
- Added support for NVIDIA A10 GPU (24 GB, 150W, PCIe) on PowerEdge R7525 , PowerEdge R740xd, and PowerEdge XE2420.
- Added support for AEP and 256GB LRDIMMs on PowerEdge R840 and PowerEdge R940xa.
- Added support for Single Socket chassis configuration in PowerEdge R6525.
- Added support for Pre-Enablement of 700W PSU on PowerEdge R6515.
- Added support for 1100W -48V DC PSU on PowerEdge R6525 and PowerEdge R7525.

## Miscellaneous

- Added support for VMWare ESXi 7.0 U2 on PowerEdge XE7420 and PowerEdge XE7440.
- Added support for Ubuntu 20.04.2 on PowerEdge XE7420 and PowerEdge XE7440.

**Topics:**

- [iDRAC and LC firmware](#)
- [Monitoring and alerting](#)
- [Networking and I/O](#)
- [OS deployment](#)
- [Storage and storage controllers](#)

## iDRAC and LC firmware

- 173593: Fixed the issue that displayed the Storage OIDs to be unavailable.
- 191905: Fixed the issue that caused iDRAC Service Module failure in PowerEdge MX740c.

## Monitoring and alerting

- 195302: Fixed an issue that displayed a change in disk version after a BIOS update.
- 195449: Fixed an issue that reported incorrect PSU voltage.

## Networking and I/O

- 193142: Fixed the issue that caused a failure in VAM properties update.
- 185043: Fixed the issue that displayed incorrect VLAN values after IPv6 configuration.

## OS deployment


- 194191: Fixed the issue that caused a failure in RFS disconnection after the mounted drive is unavailable.
- 187731: Fixed an issue that caused failure in booting into ISO image that was attached through Redfish API.

## Storage and storage controllers

- 184393: Fixed the issue that created a pending operation when a VD was deleted.

## Deprecated features

The following table displays the features that are listed as Deprecated\* or Removal\*\*:

Features	iDRAC9	iDRAC9 for PowerEdge Rx5xx/ Cx5xx
SM-CLP	Removal	Removal
VM CLI	Removal	Removal
VFlash	Deprecated	Removal
Backup and Restore	Removal	Removal
 <b>NOTE:</b> Alternatively, use the Server Configuration Profiles (SCP) feature to import or export server configuration settings and firmware updates.		
RBAP and Simple Identity profiles	Removal	Removal
WSMan	Deprecated	Deprecated
DCIM_account profile	Removal	Removal
Telnet and TLS 1.0	Removal	Removal

Deprecated\*- No longer being updated or new features added.

Removal\*\*- Code has been removed, this feature is no longer functional.

## Important notes

1. OS collector application is now bundled with iDRAC Service Module version 4.0.1 and later versions. After iDRAC firmware is upgraded to version 4.40.40.00 or later versions, iDRAC inventory will no longer display OS Collector application separately in the firmware inventory page.
2. CPLD update may fail if DUP method is used while power cap policy is enabled.
3. While encrypting VD's through Lifecycle controller, ensure that the first VD in the list is selected. Selecting a VD that is already secured does not affect the existing encryption of the VD.
4. For partition enabled COMMs adapter, a PR6 Lifecycle Log message may be displayed as partition-1 even though the values are configured as other than first partition.
5. Before updating PSU firmware on PowerEdge C series systems, ensure that all the blades are powered off in the chassis first. If any of the blades are powered on, the PSU firmware update process may fail, and LC logs report the failure.
6. Before performing SecureErase on a vFlash, ensure that the partitions on the vFlash are detached.
7. When streaming alerts using Remote Syslog or Redfish event listener, not every message ID/message gets streamed. To confirm which message ID/messages can be streamed, see the [EEMI guide](#).
8. Ensure that you use digest authentication for HTTP/HTTPS share for all iDRAC and LC features, basic authentication is no longer supported and is blocked by iDRAC due to security risks.
9. Intel ColdStream NVMe devices do not support cryptographic erase. For more information, see Intel's documentation for the specific device.
10. Remote File Share (RFS) through HTTP is only supported without authentication.
11. If part replacement is performed on systems with two PSUs while upgrade option is enabled, then the firmware update for both the PSUs are repeated once.
12. While PERC inventory is in progress, Lifecycle controller logging may fail after a warm reboot by RTCM for HBA, BOSS, or NVME drives.
13. While accessing iDRAC GUI and Redfish through the same browser, if the webserver times out, then RedfishService may prompt you to enter the login credentials to create a session. Select Cancel to clear the Redfish login prompt and proceed to the iDRAC login page.
14. Creating RAID using the selected controller is not supported through Lifecycle Controller interface. Use iDRAC GUI to create the virtual disk, then relaunch Lifecycle Controller and retry the deployment operation.
15. A new storage GUI has been introduced with this release. The old storage GUI is still accessible but would be deprecated in a future iDRAC release.
16. For Telemetry reports through subscription, if there are more than two subscriptions, it is recommended to update the Metric Report Recurrence interval to above 60 seconds.
17. IPMItool interface does not report non-communicative PSU status for PowerEdge Rx4xx/Cx4xx servers.
18. In Redfish API, all BIOS certificate related operations are now supported using the new URI: /redfish/v1/Systems/{ComputerSystemId}/Boot/Certificates
19. Adding an iDRAC system with firmware version 4.40.00.00 to a group manager with systems having iDRAC versions earlier than 3.xx, 4.0x, 4.1x, 4.2x, or 4.3x is not supported, ensure all the systems have the latest iDRAC firmware version 4.4x or any later versions.
20. Arrow keys on virtual keyboard of the iDRAC Virtual Console with eHTML5 plug-in do not respond inside BIOS boot manager after the system reboots. Close and reopen the eHTML5 Virtual console session.
21. Before deleting a VD that hosts the OS, ensure uninstalling the iSM. If VD is deleted without uninstalling iSM, LC log may display the following error: "ISM0007 The iDRAC Service Module Communication has ended with iDRAC".
22. If an Active Directory user is configured for SSO with RSA token authentication, then the RSA token is bypassed and user can log in directly. This is because RSA is not applicable for AD-SSO, Active Directory smart card, and local user smart card logins.
23. While performing any method (GET/POST and so on) on an incorrect resource URI, a proper extended error message specifying that "Resource URI is incorrect" is not provided in the response body.
24. When auto negotiation is disabled while iDRAC in Shared LOM mode, the speed and duplex values shown in the GUI and racadm output may not accurately show the actual speed and duplex on the link.
25. While performing a firmware update or rollback through LifeCycle controller GUI, the component information displayed in the table listing the available updates may be truncated if it exceeds the table column or row width.
26. If SOL session is active for a long duration or if the system is rebooted multiple times, the SOL session gets terminated automatically.

27. Critical event PDR1016 will not be generated when M.2 drives from the BOSS-S2 controller are removed since M.2 drives are directly attached to BOSS controller and not connected to the backplane.
28. While performing BIOS Recovery operation all iDRAC resets are blocked and if a iDRAC reset to default operation is performed, it causes iDRAC to be set to factory defaults and iDRAC will not reset. The condition is expected and a manual iDRAC reset is recommended.
29. After an iDRAC reboot, the iDRAC GUI may take some time to initialize causing some information to be unavailable or some options to be disabled.
30. AD/LDAP diagnostic results will display Not Run or Not Applicable for Ping Directory Server Tests. ICMP ping tests are no longer performed while running AD/LDAP diagnostics.
31. While generating Server Configuration Profile templates using the Clone or Replace option, ensure that the template is updated using a password that complies with the restrictions set on the target iDRAC, or use the 'Include Password Hash' option.
32. While clearing the Job queue using RACADM, WSMAN, or Redfish interface, it is recommended to use JID\_CLEARALL instead of JID\_CLEARALL\_FORCE. Use JID\_CLEARALL\_FORCE only to recover iDRAC Lifecycle controller from either a failed state or job that is stuck in running. It is also recommended that after you use "JID\_CLEARALL\_FORCE", iDRAC reset is needed to ensure iDRAC is back in a good working state.
33. For Dell online catalog update, downloads.dell.com only supports https protocol.
34. After updating the iDRAC license to Data Center license, ensure that you reboot the iDRAC for Idle server detection feature related attributes to function.
35. Updating firmware from version 3.30.30.30/3.34.34.34/3.36.36.36 to 4.00.00.00 or later using http/https/ftp share may fail if you use default file name. Ensure to rename the file name before you proceed with the firmware update.
36. In LifeCycle Controller GUI, use mouse to browse files or folders. Keyboard navigation does not work while browsing files.
37. If the BIOS date and time are set incorrectly while resetting iDRAC to default settings, the iDRAC's IP address may be lost. Reset iDRAC or AC power cycling the server to recover iDRAC IP.
38. iDRAC GUI search output points to a GUI page where the search keywords are missing within the page. These are typical false positives like any other search engine that may be ignored.
39. While performing any method (GET/POST and so on) on an incorrect Dell-specific URI, a proper extended error message specifying that "Resource URI is incorrect" is not provided in the response body.
40. PSU Part Replacement Firmware Update will not initiate if the secondary string of the new firmware is the same as the secondary string of replaced PSU's existing firmware. Firmware version string format is denoted as xx.yy.zz, where zz is the secondary string.
41. You may get an irrelevant response message while performing operating system method to Insert media with incorrect media for firmware upgradation or OS deployment.
42. While streaming telemetry reports for an older version of Rsyslog servers, the system may intermittently miss a few reported data. Upgrade the Rsyslog server to the latest version.
43. If a single DUP is used to update firmware for multiple devices, and if any update fails then the firmware for the subsequent cards may display an incorrect version. Update the firmware for all the failed devices again.
44. iDRAC RESTful API with Redfish displays an error stating unacceptable header specified in request for commands that are run on PowerShell. You need to explicitly include a header while using Powershell for any type of Redfish request.
45. When node initiated discovery or Group Manager is enabled, iDRAC uses mDNS to communicate through port 5353. Turn off Group Manager and node initiated discovery to disable mDNS.
46. SMART monitoring is disabled for a hard drive while it is set to Non-Raid mode.
47. In systems with network adapters without internal temperature sensors, for some adapters the NIC temperature sensors metric value is reported as 0.
48. After any iDRAC reset event, including the iDRAC firmware update, the LC Log event time is incorrectly reported for few events. This condition is momentary, and iDRAC time catches up to correct time.
49. Performing GET method on Steps only shows the next scheduled jobs and not the completed jobs.
50. If you install OMSA while iSM is already installed and connected, iSM may restart after the OMSA installation is complete.
51. After iDRAC is upgraded to version 4.00.00.00 or later for the first time, there may be a change in network settings option including IPv4 and IPv6. Reconfigure the network settings to resolve this.
52. After iDRAC is upgraded to version 4.00.00.00 or later, you may stop receiving encrypted email alerts from iDRAC, if the external email server does not support encryption. iDRAC firmware version 4.00.00.00 or later introduces a user-selectable encryption option and the default protocol is StartTLS. To start receiving email messages again, disable the email encryption by using the following RACADM command: `racadm set idrac.RemoteHosts.ConnectionEncryption None`
53. Windows Server 2012, Windows Server 2008 R2, and Windows 7 do not support TLS 1.2 and TLS 1.1. Install the following update to enable TLS 1.2 and TLS 1.1 as a default secure protocols in WinHTTP in Windows: <http://support.microsoft.com/kb/3140245/EN-US>
54. The drivers that LC exposes are present in a read-only drive that is labeled OEMDRV and the drive is active for 18 hours. During this period:
  - a. You cannot update any DUP.
  - b. LC cannot involve CSIOR.

However, if a server AC power cycle or iDRAC reboot is performed, the OEMDRV drive is automatically detached.

55. CPLD firmware update has no impact on Trusted Platform Module enablement.
56. Depending on the virtual storage device attached through iDRAC, that is, USB drive or CD/DVD .ISO file, LC displays Virtual Floppy or Virtual CD respectively.
57. If the network is not configured and you try to perform a network operation in LC, a warning message is displayed. When you go to the network settings page from this message, the left navigation panel on network settings page may not be displayed.
58. If a network operation fails for a valid address, try configuring the network settings again. If the issue persists, restart the system and retry the operation.
59. When you reset or update the iDRAC, you must reboot LC if it is launched already. If you do not reboot, LC may show unexpected behavior.
60. Fibre-channel NIC cards with dual or four ports are displayed as a single port card in LC. However, all ports are updated when a firmware update is performed.
61. The option to enable or disable the disk cache policy for SWRAID controllers are supported only on SWRAID controller driver version 4.1.0-0025 or later.
62. Rollback is not supported for CPLD and HBA controllers.
63. When CMCs are daisy chained, only the first CMC (CMC which is connected to Top of Rack switch) receives LLDP packets. Other CMCs do not receive LLDP packets. So, the iDRAC network port (dedicated mode) LLDP information is not available in the blades whose corresponding CMC is not the first CMC in the daisy chain. The LLDP information is also not available for every CMC in the daisy chain that is not connected to TOR switch directly.
64. If any of the NVMe drives report a 'Failed' status (Red LED) due to any of NVMe controller SMART errors (critical warning bits set), it should be treated as a predictive failure (Blinking amber LED). These errors include SMART errors such as:
  - a. Available spare threshold
  - b. Reliability degraded
  - c. Read-only mode
  - d. Virtual memory backup failed, and so on.
65. Ensure that the SSH client is updated to the latest version. Following SSH configurations are no longer available on iDRAC:

KEX algorithms:

  - a. diffie-hellman-group14-sha1

MAC:

  - a. umac-64
  - b. umac-64-etm@openssh.com
66. This note is applicable only to PowerEdge M640 and FC640. After the BIOS recovery operation, host may not turn on. To recover from this condition, do a virtual/physical reset operation of the blade server.
67. After updating the iDRAC firmware, LC logs may display Message ID PR36 that "Version change detected for PCIe SSD firmware. Previous version:X.X.X, Current version:X.X.X." This is due to a change in the naming convention. Ignore the log entry.
68. After downgrading the iDRAC firmware to any previous versions, storage page and drives may display warnings. To resolve the issue, reset iDRAC using the 'racreset' command.
69. This note is applicable only to PowerEdge R540. While updating the BIOS firmware through local RACADM with local share, you may get an error "ERROR: RAC989: Unable to apply the BIOS\_3P4XY\_WN64\_1.6.11.EXE firmware update." Use the direct DUP installation or installation through CIFS/NFS share to update the BIOS firmware.
70. If you get an error while performing SupportAssist collection through RACADM using HTTPS share, use the following commands to perform the collection:
  - a. Racadm SupportAssist collect.

```
racadm supportassist collect -t Sysinfo
```
  - b. Racadm SupportAssist exportlastcollection

```
racadm supportassist exportlastcollection -l <https> -u <username> -p <password>
```
71. The Lifecycle Controller GUI features available on your system depends on the iDRAC license installed. The GUI help pages may display information about features that are not available with the license installed. For licensed feature list, see the Licensed Feature section in iDRAC User's guide available at [Dell.com/iDRACmanuals](http://Dell.com/iDRACmanuals).
72. For improved support on drives and operating system deployment, it is recommended to use the UEFI BIOS boot mode.
73. To create a virtual disk or deploy an operating system, ensure that you use the Dell supported SATA, SAS, or NVMe drives. For more information, see the documentation for BIOS, controller, and drive.
74. In the software inventory, the hash value for iDRAC firmware is displayed as NA instead of hash.
75. If SMBv2 share fails in Lifecycle GUI, ensure that:



- The **Digitally sign communications** option is disabled.
  - Permissions to access the folder or file is granted.
  - folder/file name does not have a space.
  - Share contains fewer files and folders.
76. While iDRAC is initializing, all communications with iDRAC may fail. For any service requests, wait until the initialization process is complete.
  77. Performing Redfish Patch method on Read-Only property for PowerControl resource returns a status code 200.
  78. In iDRAC, if there is no link that is detected in the selected iDRAC port then the iDRAC IP is displayed as 0.0.0.0.
  79. While performing a firmware update on a system where the operating system is installed with GNOME GUI enabled, system may get into Suspend mode. To avoid the system from going into suspend mode, ensure that you change the power settings in the operating system. To change the power settings:
    - a. Go to Settings, and select Power.
    - b. For the option, "When the Power Button is pressed" select Power Off.
  80. Firmware update on drives and backplanes through Windows DUP will reflect in iDRAC after a cold boot. In Lifecycle logs, version change may be displayed repeatedly if cold reboot is not done.
  81. FRU objects or properties for Network adapters that are embedded on the motherboard are not available through any of the iDRAC interfaces.
  82. Lifecycle Controller supports ISO images with ISO-9660 format only. Other formats including combination with ISO-9660 are not recommended.
  83. UserDefined delay AC Recovery Power Delay is slow with lower limit of 60, but some conditions might cause BMC ready to be later than this and hence may not work. So, it is advised that the UserDefined delay be set to 80 s or higher. Any values less than this may cause the operation to fail.
  84. The iDRAC feature "Topology LLDP" is not supported on 1 GbE controllers and on selected 10 GbE controllers (Intel X520, QLogic 578xx).
  85. Mellanox network adapters that are used in PowerEdge MX740c and MX840c servers must be updated to version 14.23.10.20 or later, before updating the iDRAC firmware to version 4.00.00.00 or later.
  86. Install SEKM license before you update the iDRAC to SEKM supported version 4.00.00.00 or later. If you install the SEKM license after updating the iDRAC to SEKM supported version, you have to reapply SEKM supported iDRAC firmware.
  87. If you are configuring a Gemalto based KeySecure SEKM Server with iDRAC, and to get the redundancy feature functional, copy the certificates manually from primary Gemalto KeySecure cluster to secondary Gemalto SEKM KeySecure cluster. The redundancy feature works after the iDRAC is set up for SSL certificate-based authentication.
  88. Key sharing between multiple iDRACs is supported and can be configured on the SEKM server. Key sharing can be done if all the iDRACs are part of the same SEKM group and all keys are assigned to the same group with the right permissions.
  89. When FCP is enabled, 'Default Password Warning' setting is disabled after the default user password is changed.
  90. Firmware update from iDRAC versions earlier than version 3.30.30.30 is not supported (For example, updating iDRAC firmware from version 3.21.21.21 to version 4.00.00.00 or later is not supported). First update to version 3.30.30.30 or higher, and then initiate update to 4.00.00.00 or later.
  91. If system lockdown mode is enabled while a user is logged into LifeCycle Controller GUI, then lockdown mode will not be applicable on LifeCycle Controller.
  92. Due to a DMTF tool limitation, the URIs for some OEM actions that are extensions to the DMTF schemas may not appear in the OpenAPI.YAML file.
  93. The iDRAC Virtual Keyboard labeling is changed to upper case to align it with the physical keyboard layout.
  94. For enhanced security, keyboard interactive authentication is enabled on the iDRAC SSH Server. SSH clients now require keyboard interactive authentication before logging in a user in to iDRAC.
  95. If you see iSM0050 event in LC log, then ensure that you update the iDRAC Service Module (iSM) to version 3.4 or to a TLS-capable iSM. iSM without TLS capability is not supported on iDRAC firmware version 3.30.30.30 or later.

# Known issues — To be fixed in future releases

## Topics:

- LC logs display incorrect version change for disks
- Blue screen while deploying OS through Lifecycle Controller
- Server stops responding during POST with Config Error
- OME-M Deployment and Configuration Job Fails with Error LC063
- Unable to generate CSR through Redfish
- vFlash detaching after iDRAC firmware update
- MAC identities displayed in RESERVED state
- SEL events may not be correctly displayed in the earlier versions of iDRAC
- CMC firmware update fails
- Telemetry data Disabled without confirmation
- WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page
- CPU information missing under Hardware Inventory
- Storage Devices displayed in gray text
- Backplane Rollback contents not populating in iDRAC
- Test network connection fails
- MetricReport output does not match the DMTF schema
- Service Validator reporting errors for Redfish API services
- Lifecycle Controller fails to resolve IPv6 DNS addresses
- Performing GET with Top query parameter returns no error
- Server Configuration Profile import job fails
- Unable to add iDRAC Static IP
- Creating virtual media image takes longer on safari browser
- iDRAC displays warning message for different plug-in selection.
- Read-only user Virtual Console session disconnects
- iDRAC Virtual Console entering Connecting Viewer state
- PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation
- CPU PPIN in Hardware inventory in iDRAC GUI shows as “Not Supported”
- Performing GET method on chassis PCIe slots displays all PCIe slots
- Virtual Media performance is degraded with QLogic 25G OCP
- iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings
- Virtual console display in iDRAC GUI is blurred
- iDRAC unable to obtain the current time after reboot
- Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs
- Few Virtual Keyboard keys not working for other languages
- DellCertificateCollection URI response not according to DMTF standards
- Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525
- Field required displayed in Internet Explorer browser
- Firmware update using pud method failing
- Uploaded firmware link not available in the SoftwareImages property in Redfish
- PCIe types and lanes information not getting populated using Redfish
- iDRAC reboots while collecting SupportAssist logs
- Webserver restarts after remote presence port number is updated
- Getting an error SWC0018 during OS installation
- WSMAN query with space between attributes fails
- Attributes for CNA cards not displayed through Redfish or RACADM interface

- Unable to create a recurring job after same recurring job was completed
- SCP Import Job completes with error due to HddSeq error
- iDRAC LC Log shows reset cause as 'Internal Error'
- Access to serial interface fails.
- LC log created after going to Virtual media page in iDRAC GUI
- Boot mode error during OS deployment
- Repetitive PR7 messages related to PSU in LC logs after a system erase operation
- After a warm reboot, LC logs display Disk Inserted
- iDRAC DUP update fails in Linux operating systems when secure boot is enabled

## LC logs display incorrect version change for disks

<b>Description</b>	After a disk firmware upgrade, LC logs may report it as a firmware downgrade with PR36 message.
<b>Workaround</b>	Restart the host system.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	197049

## Blue screen while deploying OS through Lifecycle Controller

<b>Description</b>	You may experience a blue screen while deploying an OS with software RAID controller S150 using Lifecycle Controller.
<b>Workaround</b>	Reboot the system manually to complete the OS installation. Ensure that S150 firmware is updated to the latest version.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	199714

## Server stops responding during POST with Config Error

<b>Description</b>	Server may stop responding during POST after a Lifecycle Controller System Erase job with the message- The System Configuration Check operation resulted in the following issue: Config Error: CPU 1 and CPU ID.
<b>Workaround</b>	iDRAC reset.
<b>Systems affected</b>	PowerEdge R7525 with EPYC 7003-generation processors and x24 Expander or x4 Rear backplanes.
<b>Tracking number</b>	196985

## OME-M Deployment and Configuration Job Fails with Error LC063

<b>Description</b>	OME-M deployment jobs fail when iDRAC NTP and Host NTP settings are out of sync.
<b>Workaround</b>	Ensure that the Host OS and iDRAC NTP settings are set accurately.
<b>Systems affected</b>	All PowerEdge MX series systems supported by this release.

**Tracking number** 195935

## Unable to generate CSR through Redfish

**Description** Generating CSR through Redfish action CertificateService.GenerateCSR fails while passing in dash for email string value.

**Workaround** Use iDRAC GUI or RACADM to generate the CSR.

**Systems affected** All systems supported by this release.

**Tracking number** 196084

## vFlash detaching after iDRAC firmware update

**Description** Updating iDRAC firmware to version 4.40.00.00 or later may cause the vFlash partitions to detach on first boot after the update.

**Workaround** Reattach the detached vFlash partitions through any iDRAC interfaces after the first boot.

**Systems affected** All systems supported by this release.

**Tracking number** 194849

## MAC identities displayed in RESERVED state

**Description** MAC identities displayed in RESERVED state for some of the partitions after Slot Deployment is performed using Attach and Apply Immediately operation.

**Workaround** Redeploy OMEM.

**Systems affected** All PowerEdge MX series systems supported by this release

**Tracking number** 194347

## SEL events may not be correctly displayed in the earlier versions of iDRAC

**Description** New SEL events were introduced in this version of iDRAC. If iDRAC is rolled back to an earlier version, then new events logged in this version of iDRAC may be displayed as an unknown event in the earlier version of iDRAC.

**Workaround** N/a

**Systems affected** All PowerEdge Rx5x5 or Cx5x5 series servers supported by this release.

**Tracking number** 186384

## CMC firmware update fails

**Description** Updating CMC firmware through Dell Update Package from iDRAC or RACADM interfaces, fails with RED084 and RED085 error.

**Workaround** Use the CMC GUI to update the CMC firmware. Reset iDRAC and retry uploading the DUP to iDRAC.

**Systems affected** PowerEdge M640

**Tracking number** 190600

## Telemetry data Disabled without confirmation

**Description** Disabling Telemetry data stream through iDRAC GUI, is applied immediately after Apply is selected instead of displaying a warning message for confirmation is not seen after selecting apply. The warning or confirmation message is only visible after the success window is closed and canceling the warning fails to cancel the task.

**Workaround** Enable the Telemetry data stream using either iDRAC GUI or RACADM interface.

**Systems affected** All systems supported by this release.

**Tracking number** 194248

## WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page

**Description** In certain configurations, if the NIC partitions are enabled, WWM/MAC page may display the MAC/WWN details for the Mezz cards that are installed in the system in random order. The display order may vary from the port or partition ordering.

**Workaround** Go to the Network device page for specific device details that are associated with port and partitions.

**Systems affected** PowerEdge MX series

**Tracking number** 194452

## CPU information missing under Hardware Inventory

**Description** iDRAC inventory fails to populate CPU information after a system reboot.

**Workaround** Reset iDRAC.

**Systems affected** All systems supported by this release.

**Tracking number** 189573/158951

## Storage Devices displayed in gray text

**Description** After a reboot stress followed by BIOS update, storage devices may appear as not ready or in gray text.

**Workaround** Reset iDRAC.

**Systems affected** All PowerEdge Rx5xx/Cx5xx series supported by this release.

**Tracking number** 194537

## Backplane Rollback contents not populating in iDRAC

**Description** After updating backplane firmware to a newer version and then updating it back to a previous version from host OS, the backplane information is not displayed while trying to apply the firmware Rollback.

**Workaround**

- Perform the following:
  - Reboot the iDRAC when an update is performed from host OS.
  - Use any iDRAC interfaces (RACADM/GUI/Redfish) for backplane update operation.

**Systems affected** All systems supported by this release.

**Tracking number** 184368

## Test network connection fails

**Description** Testing the network connection may fail when IPv6 address is used for operations in LC GUI.

**Workaround** Ping and test the network IP through iDRAC GUI.

**Systems affected** All systems supported by this release.

**Tracking number** 180776

## MetricReport output does not match the DMTF schema

**Description** LastDayMaxPowerTime, LastDayMinPowerTime, LastHourMaxPowerTime, LastHourMinPowerTime, LastMinuteMaxPowerTime, LastMinuteMinPowerTime, LastWeekMaxPowerTime, and LastWeekMinPowerTime may have an invalid MetricType in MetricDefinitions.

**Workaround** N/a. The MetricReport output is further modified to match DMTF schema, and will be fixed in subsequent releases.

**Systems affected** All systems supported by this release.

**Tracking number** 180398

## Service Validator reporting errors for Redfish API services

**Description** To continue support firmware backward compatible, you may get errors for Redfish API services in the Service Validator. They do not have any functional impact on the system and may be ignored.

**Workaround** N/a

**Systems affected** All systems supported by this release.

**Tracking number** 183321

## Lifecycle Controller fails to resolve IPv6 DNS addresses

**Description** Connection issues may occur if Lifecycle Controller network interface set to use IPv6 protocol, and FQDN is defined for share/repository address.

**Workaround** For local shares and repositories, enter the IPv6 address for the Share Name value as the issue is limited to DNS resolution. This will bypass requirement for DNS resolving.

**Systems affected** All systems supported by this release.

**Tracking number** 165692

## Performing GET with Top query parameter returns no error

<b>Description</b>	Top query on a Parity URI instance returns complete response instead of an error code.
<b>Workaround</b>	N/a
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	175801

## Server Configuration Profile import job fails

<b>Description</b>	Importing SCP fails with error "Not one of the Possible Values for Attribute" when VNC password is not set or set lower than eight characters in length.
<b>Workaround</b>	Set eight character length VNC password.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	185635

## Unable to add iDRAC Static IP

<b>Description</b>	After setting iDrac static IP using IPV4 group (IPv4.1.Address, IPv4.1.Gateway,IPv4.1.Netmask) using Redfish or RACADM interface, a new IP address may not apply and system may become inaccessible.
<b>Workaround</b>	Use the IPV4Static group (IPv4Static.1.Address, IPv4Static.1.Gateway,IPv4Static.1.Netmask) to set static IP address.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	185458

## Creating virtual media image takes longer on safari browser

<b>Description</b>	Creating a virtual media image takes longer when the target folder contains many files.
<b>Workaround</b>	N/a
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	185657

## iDRAC displays warning message for different plug-in selection.

<b>Description</b>	iDRAC GUI displays a warning "Virtual console session of a different plug-in type is currently running. Please close existing session and try again".
<b>Workaround</b>	Close the existing session and change the plug-in to eHTML5.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	184648

## Read-only user Virtual Console session disconnects

<b>Description</b>	Read-only Virtual Console session with eHTML5 plug-in disconnects while server is rebooting or due to a network disruption or when the primary session is in reconnecting state.
<b>Workaround</b>	Close and reopen the eHTML5 Virtual console session.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	184596

## iDRAC Virtual Console entering Connecting Viewer state

<b>Description</b>	iDRAC Virtual Console with eHTML5 plug-in enters connecting viewer state when iDRAC is left idle for around 30 minutes.
<b>Workaround</b>	Close and reopen the eHTML5 Virtual console session.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	180173

## PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation

<b>Description</b>	PR1 & PR10 logs are displayed in Lifecycle logs for PSUs when Retire and Repurpose operation is executed. This doesn't impact server functionality.
<b>Workaround</b>	N/a
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	186119

## CPU PPIN in Hardware inventory in iDRAC GUI shows as “Not Supported”

<b>Description</b>	CPU PPIN in Hardware inventory in iDRAC GUI shows as "Not Supported" after iDRAC firmware update from previous version to 4.40.00.00.
<b>Workaround</b>	Reboot the host so the CSIOR runs and populates supported CPU PPINs in Hardware inventory.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	185523

## Performing GET method on chassis PCIe slots displays all PCIe slots

<b>Description</b>	iDRAC displays all the empty and populated slots as part of PCIe empty slot feature. All the 8 slots entries are seen under one sled even though only few are associated with that particular sled.
<b>Workaround</b>	N/a



**Systems affected** PowerEdge FC640, PowerEdge R740XD

**Tracking number** 172943

## Virtual Media performance is degraded with QLogic 25G OCP

**Description** Virtual Media performance is degraded when iDRAC is configured on the QLogic 25G OCP for shared LOM.

**Workaround** Configure iDRAC on dedicated port or integrated port or embedded shared LOM.

**Systems affected** PowerEdge Rx5xx/ Cx5xx with QLogic 25G OCP.

**Tracking number** 183014

## iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings

**Description** iDRAC time will not synchronize when Server Configuration Profile was exported with SNTP settings and then imported with SNTP settings.

**Workaround** Configure NTP settings and export the Server configuration Profile. Import the Server configuration profile with NTP and manually configure SNTP settings.

**Systems affected** All systems supported by this release

**Tracking number** 181069

## Virtual console display in iDRAC GUI is blurred

**Description** Virtual console display from iDRAC GUI is blurred for a fraction of second and gets corrected automatically when opened in Google chrome.

**Workaround** Use any other browser.

**Systems affected** All systems supported by this release.

**Tracking number** 182595

## iDRAC unable to obtain the current time after reboot

**Description** While the system is in power off state, iDRAC fails to obtain the current time after it is reset. Older logs are displayed until iDRAC synchronizes with current time.

**Workaround** N/a.

**Systems affected** All PowerEdge Rxx5x/Rx5x/Cxx5x (15th Generation) systems supported by this release.

**Tracking number** 183347

## Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs

<b>Description</b>	Firmware version change may be displayed multiple times in Lifecycle log for PCIe SSDs after performing the update through Lifecycle controller. The firmware is updated only once.
<b>Workaround</b>	N/a
<b>Systems affected</b>	PowerEdge R7525.
<b>Tracking number</b>	181254

## Few Virtual Keyboard keys not working for other languages

<b>Description</b>	Some keys or key combination may not provide the correct output for languages other than english.
<b>Workaround</b>	Use the physical keyboard or Windows On-Screen Keyboard.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	181505

## DellCertificateCollection URI response not according to DMTF standards

<b>Description</b>	An array of members are missing in Dellcertificatecollection resource collection. Without the members this resource collection is not compliant to DMTF standards.
<b>Workaround</b>	N/a
<b>Systems affected</b>	All systems supported by this release
<b>Tracking number</b>	164791

## Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525

<b>Description</b>	Local video does not turn off and remains on regardless of the local video server setting in iDRAC virtual console on PowerEdge C6525 and PowerEdge C6400.
<b>Workaround</b>	N/a
<b>Systems affected</b>	PowerEdge C6525, PowerEdge C6400.
<b>Tracking number</b>	171650

## Field required displayed in Internet Explorer browser

<b>Description</b>	If any invalid value(s) including alphabets or special characters are entered in a numeric field, Internet explorer browser displays "Field Required" instead of displaying an error "Invalid Value".
<b>Workaround</b>	Use other browsers such as Chrome/Firefox/Edge.

**Systems affected** All systems supported by this release.

**Tracking number** 163829

## Firmware update using pud method failing

**Description** Updating firmware through RACADM fwupdate -p -u -d fails with remote RACADM.

**Workaround** Use the RACADM update command to update the firmware.

**Systems affected** All systems supported by this release.

**Tracking number** 166686

## Uploaded firmware link not available in the SoftwareImages property in Redfish

**Description** While performing GET method on BIOS or Manager Schema through Redfish, the SoftwareImages property may not display the uploaded firmware link.

**Workaround** N/A

**Systems affected** All systems supported by this release.

**Tracking number** 156737

## PCIe types and lanes information not getting populated using Redfish

**Description** When Get method is performed for PCIe slots schema, slots that do not have a PCIe card populated the PCIe types and lanes are displayed empty.

**Workaround** N/A

**Systems affected** All systems supported by this release.

**Tracking number** 157364

## iDRAC reboots while collecting SupportAssist logs

**Description** iDRAC may reboot with an "Internal Error" during SupportAssist logs collection when it experiences lower runtime resources.

**Workaround** N/A

**Systems affected** All systems supported by this release.

**Tracking number** 161623

## Webserver restarts after remote presence port number is updated

<b>Description</b>	Changing the Remote Presence Port number through virtual console settings page may cause a system restart, further causing a session timeout for iDRAC GUI.
<b>Workaround</b>	N/a
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	144597

## Getting an error SWC0018 during OS installation

<b>Description</b>	Modifying BIOS Boot Mode while installing operating system thorough Lifecycle Controller GUI, an error "SWC0018" is displayed.
<b>Workaround</b>	This message does not impact the installation, click OK to proceed.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	143561

## WSMan query with space between attributes fails

<b>Description</b>	Query parsing error is observed while parsing the SQL query with a space in some properties.
<b>Workaround</b>	Scripts may be edited to remove the space between properties to be selected in the WSMAN Query parameter.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	153493

## Attributes for CNA cards not displayed through Redfish or RACADM interface

<b>Description</b>	If the partitions are disabled on FCoE capable CNA cards, few HII attributes values for WWN, VirtWWN, WWPN, VirtWWPN are displayed in the iDRAC GUI's Network page. However, the same data is not displayed when Get commands are performed in Redfish and RACADM interfaces.
<b>Workaround</b>	N/A
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	151560

## Unable to create a recurring job after same recurring job was completed

<b>Description</b>	Creating a recurring job will fail if the same job was completed recently and its Task ID still exists.
<b>Workaround</b>	Wait for ten minutes for the Task ID to be deleted

**Systems affected** All systems supported by this release.

**Tracking number** 147501

## SCP Import Job completes with error due to HddSeq error

**Description** In a system with BOSS card containing two M.2 SATA SSDs, if you export an SCP XML file and make some changes to the BIOS and NIC attributes before importing it, the import may fail with an error "HddSeq".

**Workaround** Configure the attribute using BIOS (F2) Page and set BIOS Boot-mode to UEFI mode before importing the file.

**Systems affected** All systems supported by this release.

**Tracking number** 151725

## iDRAC LC Log shows reset cause as 'Internal Error'

**Description** Some of the log events in LC Log shows 'The iDRAC firmware was rebooted with the following reason: Internal Error'. This happens when iDRAC recovers from an error that was captured error handler. This is part of iDRAC recovery mechanism.

**Workaround** N/A

**Systems affected** All systems supported by this release.

**Tracking number** 154238

## Access to serial interface fails.

**Description** The serial interface cannot be accessed with a user account that has Easy 2FA enabled. It is because the serial interface is an exempted interface which is not supported on Easy 2FA feature.

**Workaround** Disable 2FA on user account, and retry the operation.

**Systems affected** All systems supported by this release.

**Tracking number** 152106

## LC log created after going to Virtual media page in iDRAC GUI

**Description** After navigating to the virtual media page, an LC log is created stating "The operation GetAttachStatus of the DCIM\_OSDeploymentService was performed".

**Workaround** No such operation is performed, ignore this log.

**Systems affected** All systems supported by this release.

**Tracking number** 142442

## Boot mode error during OS deployment

<b>Description</b>	While deploying OS using LC UI, if the current boot mode is set to UEFI and you change the boot mode to BIOS and click Finish on the last LC UI page, an error is displayed stating that the boot mode could not be set. The system reboots after you click OK. However, on next boot to LC UI, the boot mode is changed to BIOS and the boot device selected during OS deployment is discarded.
<b>Workaround</b>	Before deploying OS using LC UI, change the boot mode to BIOS from BIOS setup (F2 at POST).
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	98665

## Repetitive PR7 messages related to PSU in LC logs after a system erase operation

<b>Description</b>	When the system is powered on manually after performing a system erase on LC data, several messages are displayed in LC logs for PSU stating "PR7 New device detected: POWER SUPPLY (PSU.Slot.X)".
<b>Workaround</b>	N/A
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	129440

## After a warm reboot, LC logs display Disk Inserted

<b>Description</b>	After performing a server warm reboot, iDRAC may report Disk Inserted in LC logs for drives behind HBA. Please ignore the log entry.
<b>Workaround</b>	N/A
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	144819 and 141414

## iDRAC DUP update fails in Linux operating systems when secure boot is enabled

<b>Description</b>	On all Linux Operating Distributions, while secure boot is enabled, if you perform iDRAC DUP update, it fails with an error "This Update Package is not compatible with your system."
<b>Workaround</b>	For iDRAC DUP updates, use other interfaces such as iDRAC GUI, RACADM, or WSMAN.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	113574

# Limitations

## Topics:

- [Authentication](#)
- [Automation — API and CLI](#)
- [BIOS and UEFI](#)
- [Hardware](#)
- [iDRAC firmware](#)
- [Monitoring and alerting](#)
- [Networking and IO](#)
- [OS deployment](#)
- [Security](#)
- [Storage and storage controllers](#)
- [SupportAssist and parts replacement](#)
- [Firmware and driver update](#)
- [Miscellaneous](#)

## Authentication

1. LC supports the following characters for username and password:
  - Alphabets (a-z, A-Z)
  - Numbers (0-9)
  - Special characters (-, \_, .)
2. If there are no slots available to add a new user in iDRAC, the Group Manager Job for Add New User shows a failure with error GMGR0047. Use the web interface (**iDRAC Settings > Users**) to verify the number of iDRAC local users.
3. If the user does not exist on a specific iDRAC, Group Manager Jobs for Change User Password and Delete User show a failure with error GMGR0047. Use the web interface (**iDRAC Settings > Users**) to verify that the user exists.

## Automation — API and CLI

1. Creating RAID 10 configuration is not supported through Redfish interface. Use the other iDRAC interfaces to create a RAID 10 configuration.
2. Sometimes, when using WSMAN, an Internal SSL Error is reported and the WSMAN command fails. If this issue occurs, retry the command.
3. Using WSMAN, the attribute *LCD.ChassisIdentifyDuration* cannot be set to **-1 (indefinite blink)**. To make the LED blink indefinitely, use the *IdentifyChassis* command with **IdentifyState=1**.
4. RACADM supports the underscore character (\_) for *iDRAC.SerialRedirection.QuitKey* along with the existing symbols shown in the integrated help.
5. If iDRAC is in lockdown mode and you run the command 'racadm rollback', followed by the command 'racadm resetcfg', an incorrect message is displayed: **ERROR: A firmware update is currently in progress. Unable to reset the RAC at this time.** Reboot iDRAC to display the correct error message.
6. While using a Top or Skip command, if you enter a value greater than the unsigned long type (4,294,967,295), you may get an incorrect error message.

# BIOS and UEFI

1. When setting the iDRAC Service Module (iSM) monitoring attributes from the web interface, if the BIOS watchdog timer is enabled, an error may be displayed but the attributes are set. To avoid the error, disable the BIOS watchdog timer or disable the iSM Auto System Recovery and then apply the attributes.

## Hardware

1. In LC, not all the vendor FC cards are supported for VLAN configuration.
2. If an H730P adapter is installed in slot 9 (internal PERC slot) of PowerEdge T640, iDRAC displays it as H730P Integrated RAID Controller (Embedded).
3. Blinking operations are not supported on the Virtual disk created on BOSS-S2 cards.

## iDRAC firmware

1. PowerEdge servers that shipped with iDRAC9 4.40.40.00 or later versions require stepped downgrades before rolling back to version 4.40.00.00 or older firmware. The iDRAC9 must be downgraded to 4.40.10.00 and then to the older firmware.
2. In Firmware Rollback page, the component names may vary in iDRAC GUI and Lifecycle Controller(LC) GUI.
3. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
4. LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC web interface.
5. The iSCSI offload attribute can be enabled only on two of the four available ports. If a card, which has this attribute that is enabled on two of its ports, is replaced with another card that has the attribute that is enabled on the other two ports, an error occurs. The firmware does not allow the attribute to be set because it is already set on the other two ports.
6. The "Discovered Servers" view of Group Manager may not show available iDRACs as available to onboard. Verify that the iDRACs are on the same link local network and not separated by a router. If they are still not visible, reset the Group Manager's controlling iDRAC.
  - a. Open Group Manager on one of the member iDRACs.
  - b. In the search box, type the controlling system's Service Tag.
  - c. Double-click the iDRAC that matches the search results and go to iDRAC Settings -> Diagnostics.
  - d. Select Reset iDRAC.

When iDRAC fully restarts, Group Manager should see the new iDRAC.

7. If Emulex LightPulse LPe31002-M6-D and Emulex LightPulse LPe35002-M2 FC adapters are configured to boot from FC storage arrays using VAM method in iDRAC, then a maximum of two boot target arrays can be configured instead of eight.
8. During import server profile operation, if the image filename is "Backup.img", operation may fail. To avoid this failure, change the filename.

## Monitoring and alerting

1. In certain cases, Group Manager Jobs view may not show a detailed error message for a member iDRAC job. For more information about the failure, review the job execution details in the Lifecycle Logs of the member iDRAC by using the web interface (**Maintenance > Lifecycle Log**) or by using the RACADM command `racadm lcllog view`.
2. PCIe SSDs in NVMe RAID mode may not display the updated state due to predicted failure. To update RAID-related information, ensure that a CSIOR is performed.
3. If the LCD display is blank, press any one of the three LCD buttons to turn on the LCD before inserting a USB storage device.
4. If Flex Address is enabled on Chassis Management Controllers (CMC), iDRAC and LC do not display the same MAC addresses. To view the chassis-assigned MAC address, use the iDRAC web interface or the CMC web interface.
5. The inventory displayed in LC UI may not be the same as that of any iDRAC interfaces. To get the updated inventory, run the CSIOR, wait for 2 minutes, reboot the host, and then check the inventory in LC UI.
6. In certain cases, in Group Manager Jobs view, the completion percentage for a job may be displayed incorrectly (>100%) for a job in progress. This is a temporary condition and does not affect how Group Manager jobs are performed. When the job is completed, Group Manager Jobs view displays **Completed successfully** or **Completed with errors**.



7. While running host stress test, if the system ID/Health LED turns off from blue, then press the ID button for a second and press it again to turn on the LED.
8. When setting the iDRAC Service Module (iSM) monitoring attributes from the web interface, if the BIOS watchdog timer is enabled, an error may be displayed but the attributes are set. To avoid the error, disable the BIOS watchdog timer or disable the iSM Auto System Recovery and then apply the attributes.
9. iDRAC supports iSM version 3.4.1 and above.
10. Redfish or other iDRAC interfaces only display the FQDD of a faulty part, use the LCLogs for detailed information.

## Networking and IO

1. While performing any network operation, LC may go into an infinite loop if there are network glitches, leaks, or packet loss. Restart LC and retry the operation with the correct NFS share name details.
2. If NPAR is enabled, LC might show unexpected behavior when configuring network settings. Disable NPAR and execute the network setting configurations. To disable the NPAR option, go to **System Setup > Device Setting**.
3. When NPAR is enabled, the port numbers displayed on the LC **Network Settings** page (**Settings > Network Settings**) do not match the port numbers displayed on the **Device Settings** page (**System Setup > Advanced Hardware Configuration > Device Settings**).
4. When Virtualization Mode is set to NPAR for network adapters that support the partitioning feature, *PartitionState* attribute can only be used for checking the state of partitions created for base partition in WSMAN enumeration. You can see the states of all the partitions by pressing F2 during POST and going to **Device Setting**.
5. The process of retrieving IPv6 address from the DHCP server with VLAN connection takes a few minutes. Wait for a few minutes and check the **Network Settings** page to view the assigned IPv6 address.
6. Network operations such as Update, Export, or Import may take more time than expected. The delay may occur because the source or destination share is not reachable or does not exist, or due to other network issues.
7. LC does not support SOCK4 proxy with credentials.
8. LC UI supports share names and file paths that are up to 256 characters long. However, the protocol you use may only allow shorter values for these fields.
9. Because of internal UEFI network stack protocol implementation, there may be a delay while opening the LC UI **Network Settings** page or while applying the network setting.
10. Before performing any network operations, verify that the network is configured with the network cable connected. In some scenarios, a warning message may not be displayed but the operation may fail. Following are some examples that may lead to failure:
  - Static IP is configured without the network cable being connected.
  - Network cable is disconnected.
  - After a Repurpose and Retire operation is performed.
  - Network is configured with the network cable connected but the network card is replaced later.
11. Any changes to the network settings in iDRAC take effect after 30 seconds. Any automation or user verification needs to wait for 30 seconds before verifying the new settings. iDRAC returns the old active value until the new values take effect. Any DHCP settings may take more time (>30 seconds) depending on the network environment.
12. When trying to save network details using the Network Configuration page of LC UI, the following error message may be displayed: *Unable to save the IPvX network settings, where x is the version of IP (IPv4 or IPv6).* The following could be one reason for this error:

On the Network Settings page of Lifecycle Controller GUI, the IP Address Source for both IPv4 and IPv6 is either DHCP or Static and DHCP is selected by default. So, even if you want to use only one version of IP address, LC tries to validate both versions, and displays an error if the network details for the unintended version cannot be validated.

If the error does not apply to the IP version you are using, click OK to close the error message. All the other settings that you configured are saved. You can either click Cancel or Back to navigate away from the Network Settings page.

13. If the Gateway IP is not configured in a network, the network settings and operations in LC UI may show some unexpected behavior.

## OS deployment

1. Operating system installation fails when the OS media volume name (label) is blank. Recommendation is to add a valid volume name for OS media (USB drive, DVD and so on) before starting the OS installation.
2. While installing SUSE Linux Enterprise Server (SLES) operating system, a media verification warning message may be displayed. This has no impact on the installation, to proceed, click **Yes**.

3. Windows operating system deployment may intermittently fail with the following error message:

```
A required CD/DVD drive device driver is missing. If you have a driver floppy disk, CD, DVD, or USB drive, please insert it now.
```

Reboot to LC and retry until the operating system is successfully deployed.

4. Deployment of Windows Server operating systems (OS) using LC may fail with one of the following messages:
  - Windows installation cannot continue because a required driver could not be installed
  - Product key required
  - Windows cannot find the software license termsThis issue occurs when the Windows setup copies the driver to the scratch space (X: drive) and the scratch space becomes full. To resolve this issue, do any of the following:
  - Remove all the installed add-on devices before starting the OS installation. After the OS installation is complete, connect the add-on devices and manually install the remaining drivers using Dell Update Packages (DUPs).
  - To avoid physically removing the hardware, disable the PCIe slots in the BIOS.
  - Increase scratch space size beyond 32 MB using `DISM set-scratchspace` command when creating customized deployment. For more details, see Microsoft's documentation.
5. LC may display multiple drive names for some CDs or DVDs, such as the ones containing operating systems.
6. If the operating system (OS) selected for installation and the OS on the media used are different, LC displays a warning message. However, while installing Windows OS, the warning message is displayed only when the bit count (x86 or x64) of the OS does not match. For example, if Windows Server 2008 x64 is selected for installation and Windows Server 2008 x86 media is used, the warning is displayed.
7. In Windows10, HTML5 plug-in does not support Virtual media connection on the following versions of Edge browsers:
  - a. Microsoft Edge 44.17763.1.0
  - b. Microsoft EdgeHTML 18.17763

## Security

1. Cryptographic Erase operation is not supported for hot-plugged NVMe disks. Reboot the server before starting the operation. If the operation continues to fail, ensure that CSIOR is enabled and that the NVMe disk is qualified by Dell EMC.

## Storage and storage controllers

1. Part number for Predictive failure message "PDR16" for NVMe drive may appear as "Not Available" immediately after the cold reboot. Allow some time after the cold reboot for iDRAC to initialize the inventory.
2. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
3. If your system has a PERC card configured in Enhanced HBA mode and you downgrade iDRAC to an older version, the SET commands for storage configuration may fail. To resolve the issue, ensure that a Collect System Inventory On Reboot (CSIOR) is performed after the downgrade. To perform a CSIOR, use the following methods:
  - a. Completely turn off the system and then turn it on again.
  - b. Ensure that CSIOR is enabled before turning off the system.
  - c. Use the following RACADM command: `racadm serveraction powercycle`
4. Few legacy drives do not support the SMART ID #245 "Remaining Rated Write Endurance". In such cases, iDRAC interfaces may display the "Remaining Rated Write Endurance" attribute as unavailable.
5. If a M.2 SATA drive attached to BOSS-S2 controller is removed, performing a blink operation may not fail for the removed drive.

## SupportAssist and parts replacement

1. Part-replacement of BOSS-S1 controller is not detected by Lifecycle Controller. After replacing the controller, follow the instructions in the controller's documentation.

## Firmware and driver update

1. After an iDRAC reset or firmware update operation, the *ServerPoweredOnTime*—a property in RACADM and WSMAN—may not be populated until the host server is restarted.
2. Some of the supported components may not be displayed on the **Firmware Update > View Current Versions** page. To update this list, restart the system.
3. If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.
4. Firmware update is supported only for LAN on Motherboards (LoM), Network Daughter Cards (NDC), and network adapters from Broadcom, QLogic, and Intel, and some of the QLogic and Emulex fiber channel cards. For the list of supported fiber channel cards, see the *Lifecycle Controller User's Guide* available at <https://www.dell.com/idracmanuals..>
5. After the CPLD firmware is updated on modular systems, the firmware update date is displayed as 2000-01-01 on the View Current Versions page. The update date and time is displayed according to the time zone configured on the server.
6. On some modular systems, after a firmware update, the Lifecycle Log displays the time-stamp as 1999-12-31 instead of the date on which the firmware update was performed.
7. It is not recommended to perform CPLD update along with other updates. If a CPLD update is uploaded and updated along with other updates using iDRAC web interface, CPLD update completes successfully but the other updates do not take effect. To complete the iDRAC updates, reinitiate the updates.

## Miscellaneous

1. You may be unable to scroll using the keyboard. Use the mouse to scroll.
2. Due to a limitation of Google Chrome browser, HTML5 virtual console intermittently displays the following error message:

```
Chrome ran out of memory while trying to display the webpage.
```

3. When accessing the iDRAC web interface for the first time using Google Chrome version 59.0, the mouse pointer may not be visible. To display the mouse pointer, refresh the page or use Google Chrome version 61.0 or later.
4. If you use the HTML5 plug-in on Chrome version 61.0 to access Virtual Console, you cannot connect to Virtual Media. To connect to Virtual Media using the HTML5 plug-in, use Chrome version 63 or later.
5. Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
6. A Serial-On-Lan (SOL) session that has been active for more than five days or multiple reboots may get terminated automatically. If the session terminates, you must reinitiate the session.
7. Due to an issue with Safari, if an ipv6 literal address is used to log into the Web GUI, Safari is not able to launch the HTML5 based vConsole. Alternative options are to use Java based vConsole, or HTML5 vConsole by using the corresponding DNS name or by using an alternate browser in Mac OS.
8. iDRAC login page does not allow password entry using Firefox browser in Ubuntu management OS.
9. iDRAC and LC features cannot access CIFS or Samba shares when only SMBv1 protocol is enabled. All iDRAC features work with SMBv2 protocol. For information on enabling SMBv2 protocol, see the documentation for your operating system.
10. In Lifecycle Controller GUI, using keyboard to browse folders and files is not supported. Use the mouse to navigate through files and folders.


# Updating iDRAC firmware

## Topics:

- [Downloading iDRAC firmware installation file](#)
- [Updating iDRAC firmware from host OS](#)
- [Updating iDRAC remotely using iDRAC web interface](#)

## Downloading iDRAC firmware installation file

### About this task

 **NOTE:** For information about updating iDRAC firmware using various interfaces, see the *iDRAC User's Guide* available at <https://www.dell.com/idracmanuals..>

### Steps

1. Go to <https://www.dell.com/support>.
2. In the **Enter a Service Tag, Serial Number...** field, type the Service Tag or the model number of your server, and press Enter or click the search icon.
3. On the product support page, click **Drivers & downloads**.
4. Select the appropriate operating system.
5. From the list, locate the iDRAC entry and click the download icon.

## Updating iDRAC firmware from host OS

From the host operating system, execute the installation package that you downloaded and follow the instructions of the update wizard.

For more information about opening executable files on your system, see the operating system's documentation.

## Updating iDRAC remotely using iDRAC web interface

### About this task

You can remotely update the firmware from the management stations using the iDRAC web interface.

### Steps

1. Extract the self-extracting installation package to the management station.
2. Access the iDRAC web interface using a supported web browser.
3. Log in as an administrator.
4. Click **Maintenance > System Update**.  
The **Manual Update** page is displayed.
5. Select **Local** to upload the firmware image from the local system.
6. Click **Browse**, select the .d9 file that you extracted or the Dell Update Package for Windows, and click **Upload**.
7. Wait for the upload to complete. After the upload is complete, the **Update Details** section displays the uploaded file and the status.
8. Select the firmware file and click **Install**.  
The message **RAC0603: Updating Job Queue** is displayed.

9. To view the status of the firmware update, click **Job Queue**.

### **Results**

After the update is complete, iDRAC restarts automatically.

# Lifecycle Controller Remote Services — client tools

## Redfish API

For information about Redfish, see the DMTF website <https://www.dmtf.org/standards/redfish>. This website provides access to schema files, white papers, technical notes, and so on.

For iDRAC Redfish API guide, go to <https://developer.dell.com>

## Resources and support

For more information about the features of this release, see the documentation for iDRAC 4.xx.

### Latest Release Notes

To access the latest Release Notes for this version of iDRAC:

1. Go to [www.dell.com/idracmanuals](https://www.dell.com/idracmanuals).
2. Click the link for the generation and then click the firmware series of iDRAC.
3. Click **DOCUMENTATION**.
4. Click **MANUALS AND DOCUMENTS**.

### Accessing documents using direct links

You can directly access the documents using the following links:

**Table 1. Direct links for documents**


URL	Product
<a href="https://www.dell.com/idracmanuals">https://www.dell.com/idracmanuals</a>	iDRAC and Lifecycle Controller
<a href="https://www.dell.com/cmcmanuals">https://www.dell.com/cmcmanuals</a>	Chassis Management Controller (CMC)
<a href="https://www.dell.com/esmmanuals">https://www.dell.com/esmmanuals</a>	Enterprise System Management
<a href="https://www.dell.com/serviceabilitytools">https://www.dell.com/serviceabilitytools</a>	Serviceability Tools
<a href="https://www.dell.com/omconnectionsclient">https://www.dell.com/omconnectionsclient</a>	Client System Management

### Accessing documents using the product search

1. Go to <https://www.dell.com/support>.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, **PowerEdge** or **iDRAC**.  
A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **DOCUMENTATION**.
5. Click **MANUALS AND DOCUMENTS**.

### Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to <https://www.dell.com/support>.
2. Click **Browse all products**.
3. Click the desired product category, such as Servers, Software, Storage, and so on.
4. Click the desired product and then click the desired version if applicable.  
 **NOTE:** For some products, you may need to navigate through the subcategories.
5. Click **DOCUMENTATION**.

6. Click **MANUALS AND DOCUMENTS**.



## Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues, see <https://www.dell.com/contactdell>.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.