DELLTechnologies

iDRAC9 Version 7.00.39.00 Release Notes

This release includes support for the PowerEdge XE9640.
Current Release Version: 7.00.39.00
Release Type: Minor (MI)

Topics:

Revision History

- N/A

Product Description

The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell servers. iDRAC alerts administrators to server issues, helps them perform remote server management, and reduces the need for physical access to the server. Additionally, iDRAC enables administrators to deploy, monitor, manage, configure, update, and troubleshoot Dell servers from any location without using any agents. It accomplishes this regardless of the operating system or hypervisor presence or state.

iDRAC also provides an out-of-band mechanism for configuring the platform, applying firmware updates, saving or restoring a system backup, or deploying an operating system, either by using a GUI or a remote scripting language, such as Redfish or RACADM.

Release date

September 2023

Priority and recommendations

Recommended: Dell Technologies 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).

Minimum version

N/A

ⓘ **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.

New and enhanced features

Hardware

- Support for PowerEdge XE9640.

Deprecated features

The following table displays the features that are listed as deprecated*, Removed**, and To be Removed***:

Table 1. Deprecated Features

Features	iDRAC9 for 14th-Generation PowerEdge Rx4xx/ Cx4xx	iDRAC9 for 15th-Generation PowerEdge Rx5xx/ Cx5xx	iDRAC9 for 16th-Generation PowerEdge Rx6xx/ Cx6xx
SM-CLP	Removed	Removed	Removed
VM CLI	Removed	Removed	Removed
vFlash	Deprecated	Removed	Removed
Backup and Restore	Removed	Removed	Removed
ⓘ **NOTE:** Alternatively, use the Server Configuration Profiles (SCP) feature to import or export server configuration settings and firmware updates.			
RBAP and Simple Identity profiles	Removed	Removed	Removed
WSMan	Deprecated	Deprecated	Deprecated
DCIM_account profile	Removed	Removed	Removed
Telnet and TLS 1.0	Removed	Removed	Removed
SHA1	Removed	Removed	Removed
Java, ActiveX, and HTML5 plugins for vConsole, vMedia, and RFS access	Removed	Removed	Removed
ⓘ **NOTE:** Attaching virtual external device using Java client is supported.			
SupportAssist direct upload, scheduling, and register	Removed	Removed	Removed
ⓘ **NOTE:** Alternatively, use Secure Connect Gateway or OpenManage Enterprise Services plug-in for automatic case creation.			
ⓘ **NOTE:** In iDRAC release version 7.00.00.00 and later versions, Dell Tech Support no longer accepts automatic uploads of SupportAssist Collections.			

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

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

To be Removed***- Expected to be removed from iDRAC code in an upcoming release.

Fixes

N/A

Known issues

Monitoring and alerting

Table 2. Delay in crash capture logs

Description	If the server experiences a CPU error such as RSOD, iDRAC may take longer to collect logs about the crash.
Workaround	N/A (Power cycle the system if it takes more than ten minutes to restart).
Systems Affected	All 15th and 16th generation of PowerEdge servers with Intel CPU.
Tracking number	262320

Table 3. Multiple Export SPDM Certificate jobs logged

Description	Multiple jobs displayed in the Job queue for Export SPDM Certificate: SPDMHWCert_download.der in Lifecycle (LC) Logs during a drive hot plug, Host reboot, iDRAC reboot, or while real time operations like controller property or configuration change, VD creation and deletion is performed.
Workaround	Ignore these events as they are internal jobs that are triggered during an inventory collection.
Systems Affected	All systems supported by this release configured with PERC 12.1.
Tracking number	264238

Table 4. SEL events may not be correctly displayed in the earlier versions of iDRAC

Description	New SEL events were introduced in iDRAC versions 4.4x. If iDRAC is rolled back to an earlier version, then new events logged in the version of iDRAC before it was rolled back may be displayed as an unknown event.
Workaround	N/A
Systems Affected	All PowerEdge Rx5x5 or Cx5x5 series servers supported by this release.
Tracking number	186384

Table 5. PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation

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

Table 6. After a warm reboot, LC logs display Disk Inserted

Description	After performing a server warm reboot, iDRAC may report Disk Inserted in LC logs for drives behind HBA.
Workaround	Ignore the log entry.
Systems Affected	All systems supported by this release.
Tracking number	144819 and 141414

Table 7. Repetitive PR7 messages related to PSU in LC logs after a system erase operation

Description	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)".
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	129440

Networking and IO

Table 8. LOM image recovery failing

Description	If the LOM image is corrupted, then performing LOM Root of Trust by an AC cycle may fail.
Workaround	Recover the LOM image manually by running the RACADM command "racadm recover <fqdd>" or perform a host cold boot.
Systems Affected	PowerEdge XE9640
Tracking number	268764

Table 9. Disabled (OS) network cards missing in iDRAC GUI

Description	Network cards that are disabled (OS) through BIOS settings, iDRAC may not display the disabled cards under System>Overview>Network Devices>Summary page.
Workaround	User other iDRAC interfaces like RACADM or Redfish.
Systems Affected	All systems supported by this release.
Tracking number	270000

Table 10. DPU offline after a VMware ESXi PSOD

Description	After a Purple Screen of Death (PSOD) in VMware ESXi, a warm reboot is triggered, causing the DPU to become unresponsive and preventing it from coming back online.
Workaround	Perform a cold reboot of the host system.
Systems Affected	All systems supported by this release.
Tracking number	272873

Table 11. Network firmware update job failing

Description	Unable to create a network firmware update job after running the "racadm systemerase reinstallfw" command immediately after performing "racadm systemerase lcdata" command.
Workaround	Update or rollback the network firmware and then try the "racadm systemerase reinstallfw" command.

Table 11. Network firmware update job failing (continued)

Systems Affected	All systems supported by this release.
Tracking number	263013

Table 12. DPU firmware (BMC) update failing

Description	DPU firmware update for BMC may fail, and iDRAC may intermittently report the current version as 0.0.0.0.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	257943

Table 13. Unable to add iDRAC Static IP

Description	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.
Workaround	Use the IPV4Static group (IPv4Static.1.Address, IPv4Static.1.Gateway,IPv4Static.1.Netmask) to set static IP address.
Systems Affected	All systems supported by this release.
Tracking number	185458

Table 14. Partial information displayed for Mellanox Cards

Description	iDRAC interfaces only display partial information for the Mellanox network cards, such as, in InfiniBand mode the card is displayed as a NIC device. Also, no board manufacturer and version is available.
Workaround	N/a
Systems Affected	All systems supported by this release.
Tracking number	179265

Table 15. NIC or FC device slot listed in hardware inventory even when disabled in BIOS

Description	For some NIC or FC cards, even if the device slot is disabled in BIOS, the slot may still get listed in the hardware inventory.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	104535

Automation — API and CLI

Table 16. Drive property not displayed

Description	In Redfish API, properties of some Samsung drives are displayed as unknown in the GET operation response.
Workaround	N/A
Systems Affected	All systems supported by this release
Tracking number	266130

Table 17. Expand query parameter issue

Description	Performing a GET method on ComponentIntegrity instance with Expand query parameter may fail to expand some of properties.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	263837

Table 18. System not powering on after Chassis reset action

Description	After a chassis reset that is performed through Redfish, if the ResetType is set to PowerCycle, then system may power off and fail to power on automatically.
Workaround	Power on the system using any iDRAC interface.
Systems Affected	All systems supported by this release
Tracking number	234900

Table 19. Server reboots while applying device firmware update

Description	While applying firmware update through Redfish interface for a device that does not require a reboot for the update, setting @Redfish.OperationApplyTime property to Immediate in the request body may cause the server to reboot.
Workaround	N/A
Systems Affected	All systems supported by this release
Tracking number	233764

Table 20. iDRAC firmware update failure

Description	iDRAC firmware update through Redfish may fail an error message is displayed "400 BadRequest-InstanceID for operation is Invalid" while the system is under performance stress.
Workaround	Retry the update operation.
Systems Affected	All systems supported by this release
Tracking number	263709

Table 21. GET method on Port collection returning incorrect information

Description	GET method on the Ports collection URI with a filter query parameter that includes "ne" operator returns incorrect details.
Workaround	N/A
Systems Affected	All systems supported by this release
Tracking number	261094

Table 22. Redfish Validator error

Description	Running schema validator to check schema conformance may display an error about NetworkAttributeRegistry instance that the JSON does not match the required URIs in Schema of AttributeRegistry.
Workaround	N/A
Systems Affected	All systems supported by this release

Table 22. Redfish Validator error (continued)

Tracking number	268459

Table 23. RLCE reports Incorrect value for fan sensor

Description	Redfish Life Cycle Events may report incorrect data for fan sensor URI after a hot pluggable fan is removed.
Workaround	Restart the host system.
Systems Affected	All systems supported by this release.
Tracking number	193777

Table 24. 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

Table 25. Performing GET with Top query parameter returns no error

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

Table 26. Uploaded firmware link not available in SoftwareImages property

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

Table 27. Attributes for CNA cards not displayed through Redfish or RACADM interface

Description	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.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	151560

Table 28. Unable to create a recurring job after same job was completed

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

Table 28. Unable to create a recurring job after same job was completed (continued)

Systems Affected	All systems supported by this release.
Tracking number	147501

Table 29. Get operation not displaying model or serial number for PCIe devices

Description	If you perform a Get operation for a PCIe device using Redfish API, the response may not display the model and serial number of the device.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	111564

Storage

Table 30. Duplicate enclosure entries and missing path

Description	While performing the firmware update for a storage enclosure, the iDRAC storage enclosures page may display duplicate enclosure entries and the redundant path as Not Present.
Workaround	Perform an iDRAC reset.
Systems Affected	All systems supported by this release configured with PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 enclosures.
Tracking number	269048

Table 31. PERC H965i missing from iDRAC

Description	PERC H965i controller not listed in iDRAC after flashing iDRAC firmware is updated.
Workaround	Perform a cold boot or warm boot or AC power cycle or an iDRAC reset.
Systems Affected	All systems supporting by this release.
Tracking number	273349

Table 32. PSID revert failing

Description	PSID revert operations on a locked VOSS drive fails with a STOR013 event log.
Workaround	Cold reboot the host and then retry the operation.
Systems Affected	All systems supporting by this release.
Tracking number	270241

Table 33. Backplane firmware rollback failing

Description	Backplane firmware rollback operation may fail though iDRAC interfaces.
Workaround	Obtain the DUP for the version that is required and perform a manual update.
Systems Affected	All 16th Generation of PowerEdge servers with SEP and E3 backplane configurations.
Tracking number	266122

Table 34. Backplane Storage Enclosure firmware update failing

Description	The backplane Storage Enclosure firmware update through Lifecycle Controller GUI may fail.

Table 34. Backplane Storage Enclosure firmware update failing (continued)

Workaround	Try the update operation through iDRAC GUI or the host OS.
Systems Affected	All systems supporting by this release with backplane enclosure configurations.
Tracking number	262593

Table 35. Storage Enclosure in failed or degraded state

Description	iDRAC may display the enclosure in failed state or degraded after the enclosure was removed and reinstalled.
Workaround	Perform an iDRAC reboot.
Systems Affected	All systems that are supported by this release with PERC H965e connected to SAS4 JBODs on PowerVault MD 2412, or PowerVault MD 2424, or PowerVault MD 2460 enclosures.
Tracking number	267129

Table 36. Unblink operation not working

Description	Unblink operation on drives that are installed in the enclosures including PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 fails.
Workaround	Try the unblink operation using the PERC CLI tool.
Systems Affected	All systems supported by this release.
Tracking number	264210

Table 37. Delay in storage inventory

Description	A delay in storage components inventory in iDRAC GUI page may occur in server configurations that are connected to PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 through the PERC H965e adapter.
Workaround	N/A.
Systems Affected	All systems supported by this release.
Tracking number	265429

Table 38. Cryptographic Erase on VOSS drive failing

Description	Cryptographic Erase on VOSS M.2 drive fails intermittently when multiple erase operations are performed on VOSS M.2 drives.
Workaround	Retry the drive erase operation.
Systems Affected	All systems supported by this release.
Tracking number	265203

Table 39. VOSS drives not secured

Description	When SDPM is enabled from iDRAC GUI or BIOS setup menu on an SEKM supported system, VOSS drives may not get Secured after a system reboot.
Workaround	Perform an additional cold reboot to secure the SED VOSS drives.
Systems Affected	All systems supported by this release.
Tracking number	264297

Table 40. Unable to update external enclosures

Description	Changing external enclosure element (EMM/PSU/Fan/TempProbes) inventory/monitoring and Enclosure AssetTag and AssetName may fail for PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 that is connected to the server through PERC H840.
Workaround	N/A
Systems Affected	All systems that supported by this release with PERC H840 connected to SAS4 JBODs on PowerVault MD 2412 or PowerVault MD 2424, or PowerVault MD 2460.
Tracking number	260963, 260401, 257318

Table 41. PERC Rekey failing

Description	If iDRAC and PERC have the same Key Ids then PERC Rekey command fails.
Workaround	Use the iDRAC Rekey command instead of PERC Rekey.
Systems Affected	All systems supported by this release.
Tracking number	230629/189445

Table 42. Backplane firmware update job failing

Description	Unable to create a backplane firmware update job after running the "racadm systemerase reinstallfw" command immediately after performing "racadm systemerase lcdata".
Workaround	Restart the iDRAC and then try "racadm systemerase reinstallfw" command.
Systems Affected	All systems supported by this release.
Tracking number	265093

Table 43. BOSS configuration job failing

Description	A device configuration job to enable or disable security on BOSS devices may fail with JCP042 message. A PR19 configuration update success message is also logged as the configuration of attributes succeeds.
Workaround	Retry the configuration job.
Systems Affected	All systems supported by this release.
Tracking number	263709

Table 44. LC logs display incorrect version change for disks

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

Miscellaneous

Table 45. No Input for Input Line Type

Description	iDRAC GUI displaying No Input or Low line value for PSU Input Line Type after PSU input operation is changed to DC mode.
Workaround	N/A

Table 45. No Input for Input Line Type (continued)

Systems Affected	All systems supported by this release with DC PSUs.
Tracking number	265024

Table 46. PSUs missing

Description	PSUs missing from the iDRAC GUI Power Supplies section when a single or multiple PSUs are removed from the system.
Workaround	Perform an iDRAC reboot or run the racadm getsensorinfo command.
Systems Affected	PowerEdge XE9640
Tracking number	267245

Table 47. iDRAC not displaying Intel GPU retimer

Description	iDRAC may fail to display the Intel Data Center GPU Max Subsystem Retimer devices on the inventory page after a cold boot.
Workaround	Perform an iDRAC reset or reboot the host system.
Systems Affected	PowerEdge XE9640
Tracking number	269065

Table 48. Virtual console flickering

Description	Virtual Console screen flickering and sluggish after changing performance to Maximum Video Quality with Windows Server 2022 DC installed along with video driver.
Workaround	Set the Performance in the Console Control page to default settings.
Systems Affected	All Dell PowerEdge 16th generation servers supported by this release.
Tracking number	255108

Table 49. Customer SSL certificate deleted

Description	After an iDRAC firmware update, the web-server certificate gets replaced with a self-signed certificate if a custom certificate is deployed after enabling the USB-NIC.
Workaround	Redeploy the custom web-server certificate after enabling the USB-NIC.
Systems Affected	All systems supported by this release.
Tracking number	273127

Table 50. iSM in Limited Mode

Description	iDRAC may display iSM status as limited mode or not running after an iDRAC reboot.
Workaround	Switch the USB NIC to off and then on and then check the updated state after 2 minutes.
Systems Affected	All systems that are supported by this release.
Tracking number	273077

Table 51. PSU details unavailable

Description	PSU1 details are missing from iDRAC GUI under Power Supply section.
Workaround	Perform an iDRAC Reboot or use the racadm getsensorinfo command.

Table 51. PSU details unavailable (continued)

Systems Affected	All systems supported by this release.
Tracking number	270961

Table 52. No event log for PSU removal

Description	After removing a PSU from the external enclosure, iDRAC fails to log a PSU1000 event.
Workaround	N/A.
Systems Affected	All systems that are supported by this release configured with PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 enclosure.
Tracking number	270136

Table 53. Part number and firmware version not displaying

Description	Part number for PSU and enclosures, and enclosure firmware version not displaying in iDRAC.
Workaround	N/A.
Systems Affected	All systems supported by this release with PERC H965e controller and external JBODs.
Tracking number	264622

Table 54. Power supply absent

Description	Power supply unit displayed as Absent in the Hardware Inventory page after iDRAC firmware is upgraded to version 7.00.00.00.
Workaround	Perform an iDRAC reboot or run the racadm getsensorinfo command to see the information.
Systems Affected	All systems supported by this release.
Tracking number	267183

Table 55. Few Virtual Keyboard keys not working for other languages

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

Important notes

Authentication

1. 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.
2. 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.

BIOS and UEFI

1. 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.
2. 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.

iDRAC firmware

1. In iDRAC, attaching a folder that is in an NFS share hosted by a Linux-based operating system is not supported.
2. In Lifecycle (LC) interface, It is recommended to avoid performing any operations on media that is mounted as RFS through iDRAC GUI/RACADM/Redfish.
3. Updating iDRAC firmware to version 6.xx or later changes the static IPv4 or IPv6 DNS settings. Ensure that you reconfigure the network settings after the upgrade is complete.
4. Firmware update using an FTP fails if the HTTP proxy is used without any authentication. Ensure that you change the proxy configuration to allow the CONNECT method to use non-SSL ports. For example, while using a squid proxy, remove the line "http_access deny CONNECT !SSL_ports" that restricts from using the CONNECT method on non-SSL ports.
5. To apply a firmware update that is scheduled and awaiting a host reboot, ensure that you perform a cold reboot instead of a warm reboot.
6. For catalog updates through downloads.dell.com, adding catalog location or name is not required. Adding downloads.dell.com as HTTPS Address enables iDRAC to find the appropriate catalog file.
7. If Lifecycle controller logs display RED057 message during a component update, then run the command systemerase lcdata through RACADM interface and then retry the operation.
8. While performing a PSU firmware update through the host OS in the 15 th or later Generations of PowerEdge servers, ensure that you perform a cold reboot to apply the update.
9. During OS deployment through SCP, if the SCP configuration file includes the attribute "OSD.1#AnswerFileName" then a virtual USB device OEMDRV is attached to the server that contains the file with responses for an unattended OS installation. This device will be available for the duration as specified in the optional attribute "OSD.1#ExposeDuration" in the template and if the attribute is not specified, it remains attached for about 18 hours. After the OS installation is complete, detaching the ISO and the driver pack also unmounts the OEMDRV device.
10. 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 Lifecycle Controller (LC) logs report the failure.
11. Adding an iDRAC system with firmware version 4.4x or later to a group manager of systems with iDRAC versions earlier than 3.xx, 4.0x, 4.1x, 4.2x, or 4.3x is not supported. Ensure that all the systems have the latest iDRAC firmware version 4.4x or any later versions.
12. While performing a firmware update or rollback through LifeCycle controller(LC) GUI, the component information displayed in the table listing the available updates may be truncated if it exceeds the table column or row width.
13. 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.
14. 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.
15. After updating the iDRAC license to Data Center license, ensure that you reboot the iDRAC for Idle server detection feature related attributes to function.
16. In LifeCycle Controller GUI, use the mouse to browse files or folders. Browsing files using keyboard is not supported.
17. 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.
18. 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.
19. When node initiated discovery or Group Manager is enabled, iDRAC uses mDNS to communicate through port 5353. Turn off the Group Manager and node initiated discovery to disable mDNS.
20. After iDRAC is upgraded to version 4.xx or later, you may stop receiving encrypted email alerts from iDRAC, if the external email server does not support encryption. iDRAC firmware version 4.xx or later includes 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`
21. 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

22. 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.

23. 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.
24. Firmware rollback is not supported for CPLD, NVDIMM, SAS/SATA drives, and PSU (on modular systems).
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. Lifecycle Controller supports ISO images with ISO-9660 format only. Other formats including combination with ISO-9660 are not recommended.
31. 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.
32. 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.
33. 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.
34. 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.
35. Product Name for GPU may be displayed as Not Applicable if the product area data is not available on the GPU FRU chip.

Monitoring and alerting

1. In iDRAC firmware version 6.00.30.00, Crash Video Capture is set to disabled state by default. To enable it, perform the RACADM set command on the attribute

   ```
   idrac.virtualconsole.CrashVideoCaptureEnable.
   ```

2. While updating a device firmware through LC interface, Lifecycle logs may display RED032, RED096, and RED008 messages if the size of the image payload exceeds the available space in firmware partition. To free up space in the partition, perform LCWipe or Systemerase by selecting the Lifecycle controller data option in System category and retry the update.
3. iDRAC displays additional fan sensor for each installed dual-rotor fan. System fan slots that are blank or if a single rotor fan is removed from the system, iDRAC displays two sensors.
4. 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.
5. Redfish Life Cycle Events (RLCE) do not support event generation for collection resources.
6. For staged operations that require system reboot, after the system reboot is complete RLCE events for the operation may take up to 20 s depending on the system configuration.
7. A Redfish request to update or post with JSON format payload supports only the first valid JSON in the request. If additional text is passed in the payload, the text gets discarded.
8. While PERC inventory is in progress, Lifecycle controller logging may fail after a warm reboot by RTCEM for HBA, BOSS, or NVME drives.

9. 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.
10. 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", an iDRAC reset is needed to ensure iDRAC is back in a good working state. Ensure that all the services are in ready state before performing iDRAC reset. To check the status of the services, run the command getremoteservicesstatus.
11. 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.
12. 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.
13. 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>
    ```

Networking and IO

1. During a DPU (Smart NIC) firmware update, SUP0516 message about firmware update is logged in Lifecycle (LC) Logs before the system restart log (SYS1000). The actual firmware update is applied at Post while the host system is powering on.
2. Firmware version for DPU cards on iDRAC Overview page (Network Devices section) may vary with the version that is displayed on the Firmware Inventory page. Use the version that is displayed on the Firmware Inventory page.
3. iDRAC may display some unsupported attributes such as PCIeOfflineOnlineFQDDList, SerialNumber, PermanentMACAddress, CSP Mode and DPUOSDeploymentTaskState for DPUs when GET is performed on the iDRAC attribute registry. These attributes are expected to be removed from the iDRAC code in an upcoming release.
4. iDRAC IPv6 auto-generated addresses change to stable-privacy assigned addressing when iDRAC is upgraded to firmware version 5.10.00.00 (or later) from any previous iDRAC versions.
5. In a SCP import job for enabling NPAR on a network port, if all partitions are not required then ensure that you apply the SCP import twice. Once to enable the NPAR on the port and the second time to disable the partitions that are not required.
6. 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.
7. When auto negotiation is disabled while iDRAC is 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.
8. In systems with network adapters without internal temperature sensors, for some adapters the NIC temperature sensors metric value is reported as 0.
9. After iDRAC is upgraded to versions 4.xx 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. While iDRAC is initializing, all communications with iDRAC may fail. For any service requests, wait until the initialization process is complete.
15. 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.
16. FRU objects or properties for Network adapters that are embedded on the motherboard are not available through any of the iDRAC interfaces.

17. The iDRAC feature "Topology LLDP" is not supported on 1 GbE controllers and on selected 10 GbE controllers (Intel X520, QLogic 578xx).

Automation — API and CLI

1. For Redfish OEM actions ExportLCLog and ExportHWInventory, the final job status message is not consistent across all supported network share protocols. When using NFS or CIFS share, final job status message is "<operation name> was successful" and while using HTTP or HTTPS, final job status message is "The command was successful". To view what operation was performed, see the JobType property in the job ID JSON output results.
2. For Telemetry reports, if the RecurrenceInterval is set to a value lower than the metric SensingInterval a few extra reports may be generated when no data is available at the source. Ensure that RecurrenceInterval is greater than and a multiple of SensingInterval.
3. During an iDRAC stress test, if the number of user sessions exceed eight, then iDRAC may display unexpected failures for Redfish operations.
4. Values for some properties may not reflect the same across different iDRAC interfaces, as there can be a delay in data refresh.
5. If you get 400 status code while performing Redfish MultipartUpload for firmware updates, wait for five minutes and retry the operation again.
6. 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.
7. 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.
8. 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.
9. In Redfish API, all BIOS certificate related operations are now supported using the new URI: /redfish/v1/Systems/ {ComputerSystemId}/Boot/Certificates.
10. 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.
11. You may get an irrelevant response message while performing operating system method to Insert media with incorrect media for firmware upgradation or OS deployment.
12. 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.
13. iDRAC RESTful API with Redfish displays an error stating unacceptable header specified in request for commands that are run on PowerShell. Ensure that you include a header while using Powershell for any type of Redfish request.
14. Performing GET method on steps only shows the next scheduled jobs and not the completed jobs.
15. Performing Redfish Patch method on Read-Only property for PowerControl resource returns a 200 status code.
16. 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.
17. In RACADM interface, using XML escape symbols such as `<` or `>` or `&` as AssetTag or as a substring in the AssetTag will be configured as regular characters that they represent.

Security

1. iDRAC v5.10.00.00 adds an enhanced security check for accessing iDRAC using a hostname. To access iDRAC using a hostname, ensure that you configure the hostname through the attribute `idrac.webserver.ManualDNSEntry` (`racadm set idrac.webserver.ManualDNSEntry kos2-204-i.datadomain.com`).
2. Setting Custom Cypher String with TLS version 1.3 is not supported.
3. Accessing iDRAC through OpenManage Enterprise Modular SSO may fail if iDRAC is configured with a short FQDN. Ensure that you configure iDRAC with full FQDN that includes a Hostname with Domain name.
4. 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.

5. CPLD firmware update has no impact on Trusted Platform Module enablement.
6. 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

7. In the software inventory, the hash value for iDRAC firmware is displayed as NA instead of hash.
8. 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.
9. 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 redundance feature works after the iDRAC is set up for SSL certificate-based authentication.
10. When FCP is enabled, 'Default Password Warning' setting is disabled after the default user password is changed.
11. 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.
12. After upgrading or downgrading the iDRAC firmware, ensure that you review the version of the TLS protocol that is selected in the Web Server Settings page.

Storage

1. Servers with NVMe drives with different firmware versions and configured through a PERC may display PR36 messages in Lifecycle logs during the boot process.
2. Reports about the drives that are not certified by Dell may not be included in the Telemetry reports.
3. PatrolReadRate property is deprecated and not supported from iDRAC firmware version 5.10.25.00 and the later releases. Setting PatrolReadRate using SCP is not supported.
4. While encrypting VDs 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.
5. Before performing SecureErase on a vFlash, ensure that the partitions on the vFlash are detached.
6. Intel ColdStream NVMe devices do not support cryptographic erase. For more information, see Intel's documentation for the specific device.
7. 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.
8. Before deleting a VD that hosts the OS, ensure that you uninstall iSM. If a VD is deleted without uninstalling iSM, LC log may display the error: "ISM0007 The iDRAC Service Module Communication has ended with iDRAC".
9. 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.
10. SMART monitoring is disabled for a hard drive while it is set to Non-Raid mode.
11. 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.
12. 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.
13. 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.
14. For improved support on drives and operating system deployment, it is recommended to use the UEFI BIOS boot mode.
15. 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.
16. 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.
17. The iDRAC Virtual Keyboard labeling is changed to upper case to align it with the physical keyboard layout.

Miscellaneous

1. iDRAC may take about 15 to 20 minutes to display information about GPUs, network cards, DIMMs, or other components depending on the system configuration. It may display stale data for these components if a system reboot is performed multiple times in a span of 5 to 10 minutes. Perform an iDRAC reboot to clear out the stale data.
2. The host OS may display an incorrect folder size of the folder that is attached through remote file sharing.
3. Virtual Console and Virtual media may not function on Safari browser while iDRAC is set to use TLS version 1.3. Ensure that browser settings are updated to TLS 1.2 or below.
4. Configuring Power Factor Correction (PFC) for power supplies in all 15 th generation of PowerEdge systems is not supported.
5. While BIOS is set to Boot mode, boot capture video file size is limited to 2 MB. During the video capture, if the size of video file exceeds the limit, then only partial operation is captured.
6. CPLD update may fail if DUP method is used while power cap policy is enabled.
7. Remote File Share (RFS) through HTTP is only supported without authentication.
8. 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.
9. 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.
10. If SOL session is active for a long duration or if the system is rebooted multiple times, the SOL session gets terminated automatically.
11. For Dell online catalog update, downloads.dell.com only supports https protocol.
12. If you install OMSA while iSM is already installed and connected, iSM may restart after the OMSA installation is complete.
13. In SLES and RHEL, the native video players do not support the MPEG-1 video formats. To play the captured videos, install an MPEG decoder or a video player that supports this format.
14. You may experience frame loss or drift in frame rate in the boot or crash capture videos due to iDRAC memory constraints.

Limitations

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. For a newly created job, Redfish may display 404 error if you perform a Get method to see the details for the job. Wait for about ten seconds and try performing the Get method again.
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.

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. After a system cold reboot, the corresponding Unlock event for Boss Drives getting unlocked are not generated in iDRAC Lifecycle (LC) Logs. To verify if the BOSS drives are successfully unlocked and secured, see the BOSS Drive Secure State in the iDRAC GUI or run the RACADM command `racadm storage get pdisks -o`.
2. Operating system crash capture and last crash screen are not supported for all Linux based operating systems such as RHEL, SLES, Ubuntu, ESXI, and Cent operating systems.
3. 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 lclog view`.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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**.

9. 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.
10. 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.
11. iDRAC supports iSM version 3.4.1 and above.
12. 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. When multiple NICs are configured for the first time, and the first configured NIC port stops responding or shuts down, then any operation over network from Lifecycle Controller GUI using FQDN may fail from all configured NICs. Before trying any operation over network in LC GUI, ensure that you reboot the host when the first configured NIC goes down.
3. 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**.
4. 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**).
5. 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**.
6. 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.
7. 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.
8. LC does not support SOCK4 proxy with credentials.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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 an 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 terms

   This 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. Cold reboot (power cycle) 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.

Storage

1. iDRAC interfaces do not support slicing RAID volumes through software RAID controllers. To configure sliced RAID volumes, use F2 Device settings.
2. 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.
3. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
4. 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
5. 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.
6. 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. In PowerEdge systems with AMD configuration, if a PSU firmware update is initiated from LCUI, host goes into powered-off state and Job is Completed with status 0%. Ensure that you power on the system using any iDRAC interface to start the PSU firmware update.
2. CMC server component update does not support the iDRAC9 firmware packages. Use iDRAC GUI, RACADM interface, or OpenManage Enterprise Modular to perform any out-of-band updates of iDRAC9 firmware.
3. 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.
4. Some of the supported components may not be displayed on the **Firmware Update** > **View Current Versions** page. To update this list, restart the system.
5. If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.
6. 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..
7. 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.
8. On some modular systems, after a firmware update, the Lifecycle Log displays the timestamp as 1999-12-31 instead of the date on which the firmware update was performed.
9. 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.
11. When accessing iDRAC through a Safari web browser version 14.0.3 and later versions, if a page refresh is attempted using the browser refresh option, then the iDRAC session may get cleared and you may get redirected to the iDRAC dashboard page. To refresh the page, use the Refresh option available on the iDRAC console.

Environmental and system requirements

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)—Available on all servers as an upgrade.

  (i) **NOTE:** iDRAC Secure Enterprise Key Manager(SEKM) with PERC is not supported on MX series blade servers.
- BMC – Available only on Dell PowerEdge C series servers.

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.

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

Supported systems

16th Generation of PowerEdge Servers
PowerEdge XE9640

Supported managed server operating systems and hypervisors

- Microsoft Windows
  - Server 2022 Standard
  - Server 2022 Datacenter
  - Server 2019 Standard (Downgrade only)
  - Server 2019 Datacenter (Downgrade only)
  - WinPE 5.0 64-bit
  - WinPE 10
- Microsoft Azure Stack HCI v2 and v3
- Linux
  - RHEL 9.1
  - RHEL 8.7
- SLES
  - SLES 15 SP4
- Ubuntu
  - Ubuntu 22.04.1
- VMware
  - ESXi 8.0
  - ESXi 7.0 U3

Supported web browsers

- Microsoft EDGE
- Safari 15
- Mozilla Firefox 100
- Mozilla Firefox 99
- Google Chrome 102
- Google Chrome 101

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 Service Module (iSM)

iSM version 5.1.0.0 or later

iDRAC tools

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

- Dell iDRAC Tools for Microsoft Windows Server(R), v11.0.0.0
- Dell iDRAC Tools for Linux, v11.0.0.0
- Dell iDRAC Tools for VMware ESXi (R), v11.0.0.0

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.

Supported Key Management Server (KMS) for Secured Enterprise Key Manager (SEKM)

- CipherTrust Manager version 2.10.2
- IBM Security Guardium Key Lifecycle Manager version 4.1.1.0
- Utimaco Enterprise Secure Key Manager version 8.4.0
- KeySecure Classic version 8.12.5
- Thales Data Security Maanager (DSM) version 6.4.8

Installation and upgrade considerations

Downloading iDRAC firmware installation file

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

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

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

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**.

After the update is complete, iDRAC restarts automatically.

Resources and support

For more information about the features of this release, see the documentation for iDRAC 7.xx.

Latest Release Notes

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

1. Go to 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 56. Direct links for documents

URL	Product
https://www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
https://www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
https://www.dell.com/esmmanuals	Enterprise System Management
https://www.dell.com/serviceabilitytools	Serviceability Tools

Table 56. Direct links for documents (continued)

URL	Product
https://www.dell.com/omconnectionsclient	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.

   (i) **NOTE:** For some products, you may need to navigate through the subcategories.

5. Click **DOCUMENTATION**.
6. Click **MANUALS AND DOCUMENTS**.

Lifecycle Controller (LC) 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.

Where to get help

The Dell Technologies Support site contains important information about products and services including drivers, installation packages, product documentation, knowledge base articles, and advisories.

A valid support contract and account might be required to access all the available information about a specific Dell Technologies product or service.

Notes, cautions, and warnings

(i) **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.**