

# iDRAC9 Version 7.20.30.50 Release Notes

This release includes support for PLDM updates for PERC 12, enhanced thermal management with throttling and CoolIT features, improved security with support for SHA384, SHA512, and AES-256 privacy types and fixes that improve iDRAC stability on Dell PowerEdge 16<sup>th</sup> and 15<sup>th</sup> generation servers. This release does not include support for Dell PowerEdge 14<sup>th</sup> generation servers.

**Current Release Version:** 7.20.30.50

**Previous Release Version:** 7.20.10.50

**Release Type:** Major (MA)

Topics:

- [Revision History](#)
- [Product Description](#)
- [New and enhanced features](#)
- [Resolved issues](#)
- [Known issues](#)
- [Limitations](#)
- [Environmental and system requirements](#)
- [Installation and upgrade considerations](#)
- [Where to get help](#)

## Revision History

- 6.10.00.00
- 6.00.30.27
- 6.10.30.00
- 6.10.30.20
- 6.10.80.00
- 7.00.00.00
- 7.00.30.00
- 7.00.60.00
- 7.10.30.00
- 7.10.50.00
- 7.10.70.00
- 7.10.90.00
- 7.20.10.50

 **NOTE:** The list of previous iDRAC versions that are supported may vary depending on the server model. To see the supported previous versions for a specific server:

1. Go to [Dell Support](#) page.
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. From the list, locate and expand the iDRAC entry and click **Older versions**.

List of all previous versions supported is displayed along with the download link and the release date.

# 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


June 2025


## 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:** This release only supports Dell PowerEdge 15<sup>th</sup> and 16<sup>th</sup> generation servers. This release does not support Dell PowerEdge 14<sup>th</sup> (14G) generation servers. The last release that supported 14G servers is iDRAC9 version 7.00.00.181.

 **NOTE:** For details about the previous releases, if applicable, or to determine the most recent release for your platform, and for the latest documentation version, see KB article 00178115 available at [Integrated Dell Remote Access Controller 9 Versions and Release Notes](#).

# New and enhanced features

## iDRAC Firmware

- Enabled auto deletion of old core files after iDRAC firmware update.

## Security

- Support for authentication types SHA384 and SHA512, and privacy type AES-256.

## Hardware

- Added support for multirated 2800 W or 3000 W PSUs on PowerEdge XE8640, PowerEdge XE9640, and PowerEdge XE9680.

## Automation—API and CLI

- OriginOfCondition URI support for Physical Disk RAID (PDR) alerts category events PDR16, PDR113, and PDR114.
- Support for OpenSSH version 9.9p2.

- Included NIC card temperature gauge in iDRAC through Redfish API.

## Storage

- Support for PLDM (rebootless) updates for PERC 12 controllers (H965).
- Support for Kingston MLC EMMC16G.

## Monitoring and alerting

- Improved Design for Debug (D4D) and usability messages.
- Added throttling and CoolIT features for thermal management.

## 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 14 <sup>th</sup> -Generation PowerEdge Rx4xx/ Cx4xx	iDRAC9 for 15 <sup>th</sup> -Generation PowerEdge Rx5xx/ Cx5xx	iDRAC9 for 16 <sup>th</sup> -Generation PowerEdge Rx6xx/ Cx6xx
SM-CLP	Removed	Removed	Removed
VM CLI	Removed	Removed	Removed
vFlash	Deprecated	Removed	Removed
Backup and Restore	Removed	Removed	Removed
<b>i 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	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
<b>i NOTE:</b> Attaching virtual external device using Java client is supported.			
SupportAssist direct upload, scheduling, and register	Removed	Removed	Removed
Diffie-Hellman key exchange (DH KEX) algorithms	Removed	Removed	Removed
<b>i NOTE:</b> Alternatively, use <a href="#">Secure Connect Gateway</a> or <a href="#">OpenManage Enterprise Services</a> plug-in for automatic case creation.			
<b>i NOTE:</b> 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.

## Resolved issues

### iDRAC Firmware

- 320857: Fixed the issue where the components hash value in FirmwareInventory was incorrect.
- 321452: Fixed the issue where downgrade versions were not displaying during catalog updates.
- 326051: Fixed the issue causing intermittent iDRAC resets.
- 326284: Fixed the issue causing intermittent sluggishness in iDRAC.
- 333756: Fixed the issue where the iDRAC update caused the battery rollup status to be in an unknown state.

### Automation—API and CLI

- 328045: The Redfish virtual media disconnect URI does not function correctly when login and access virtual media permissions are used.
- 331661: When Dynamic Numeric Segment (DNS) is enabled, the chassis URI with a double digit fails with a 404 error.
- 334426: Fixed the issue where DPU sensor thresholds were incorrectly displayed in the Redfish interface.

### Storage

- 324933: During a cold reboot while the server is facing high load, the storage enters an unknown state.
- 324414: The HBA H965i successfully issues and processes the Blink or Unblink RACADM commands for NVMe-specific drives, even though these drives do not support the blink or unblink operations.
- 333597: Fixed the issue where NVMe drives failed to display in the iDRAC UI Storage Summary page.

### Monitoring and alerting

- 320301: For the 3000 W PSU, the NominalVoltageType displays as Null under the Redfish Powersupplies URI, and the “Input Line Type” shows as “No Input” on the iDRAC UI power page.
- 323821: Fixed the issue where the GPU firmware update displayed the Actual Completion Time before the update is started or while in progress.
- 333839: Fixed the issue where the MinPasswordLength parameter in the iDRAC UI incorrectly showed a default value of 0.
- 334099: Fixed the issue where the JobState was incorrectly marked as Completed for failed jobs in the Redfish JobServices output.
- 335384: Fixed the issue with the EventTimestamp format in telemetry events.

### Automation—API and CLI

- Fixed CVE-2025-27113.
- Fixed CVE-2025-0840.

### Miscellaneous

- 325508: Fixed the issue where BIOS updates failed when performed through RHEL operating system or iDRAC.
- 332051: Fixed the issue where the virtual console fails to launch.
- 334054/335074: Fixed the issue where ACME enrollment failed when the server did not supply a Replay-Nonce.

# Known issues

## iDRAC firmware

**Table 2. SNMP operations failure after iDRAC firmware upgrade**

Details	
Description	SNMP-enabled user account created in previous releases encounters failure in receiving SNMP traps and other SNMP operations after upgrading to iDRAC9 version 7.20.30.00 or later, if the authentication protocols are changed to SHA384/512 and the SNMP passphrase is disabled. This is due to the failure in SNMP user creation.
Workaround	Perform the following steps: <ol style="list-style-type: none"><li>1. Enable the passphrase and provide both authentication and privacy passphrases.</li><li>2. Change the user password for existing users to regenerate hashes.</li><li>3. Create users in the new releases.</li></ol>
Systems Affected	All systems supported by this release.
Tracking number	344060

**Table 3. SNMP Walk/GET failure with disabled passphrase**

Details	
Description	SNMP walk or GET operations fail when the SHA512 authentication protocol is used in combination with any privacy protocol, if the passphrase is disabled.
Workaround	Enable the passphrase and provide both authentication and privacy protocols.
Systems Affected	All systems supported by this release.
Tracking number	344262

## Storage

**Table 4. Issue with M2 drives connected to M2 riser**

Details	
Description	M2 drives connected to M2 riser are not listed in iDRAC interfaces.
Workaround	Perform a system cold reboot.
Systems Affected	All systems supported by this release.
Tracking number	341332

**Table 5. Monitoring issues with external PERC and enclosure drives**

Details	
Description	External PERC and enclosure drives cannot be monitored in the iDRAC UI and other interfaces.
Workaround	Perform a system cold reboot.
Systems Affected	All systems supported by this release.
Tracking number	341408

**Table 6. Communication issue with SLED after firmware update**

Details	
Description	After performing a firmware update using the Validated Stack catalog (24.09.00) from the Lead chassis, one of the SLEDs stopped communicating with the Management Module (MM).
Workaround	Rebooting the iDRAC or reseating the sled will resolve this issue.
Systems Affected	All systems supported by this release
Tracking number	343464

**Table 7. BOSS firmware update SMART events issue**

Details	
Description	<p>During a BOSS firmware update, there is a possibility that the listed SMART events can be generated in the Lifecycle Controller (LC) for the drives behind BOSS, in addition to the BOSS firmware update successful event.</p> <ol style="list-style-type: none"> <li>1. PDR115: The Disk 1 on Integrated BOSS 1 is in read-only mode.</li> <li>2. SSD0002: The Available Spare of SSD Disk 1 on Integrated BOSS 1 is 0 which is less than the threshold value 10.</li> <li>3. PDR110: The (device name) reliability has degraded.</li> <li>4. PDR114: The (device name) is approaching read-only mode.</li> <li>5. PDR111: The volatile memory backup device on (device name) is no longer functional.</li> <li>6. SSD0001: The Write Endurance of SSD Disk 0 on Integrated BOSS 1 is less than the threshold value of Remaining Write Rated Endurance.</li> </ol>
Workaround	Ignore the warning.
Systems Affected	All systems supported by this release.
Tracking number	329998

**Table 8. Samsung SSDR update issue**

Details	
Description	When updating the Samsung SSDR, 1.9T M.2 from iDRAC, it may display the message "Unable to verify Update Package signature."
Workaround	Update the DUP from the operating system.
Systems Affected	All systems supported by this release.
Tracking number	323251

**Table 9. Drives not visible after enclosure firmware update**

Details	
Description	Following a firmware update for PowerVault MD 2412, MD 2424, or MD 2460, some drives that are configured with these enclosures may not appear in iDRAC under the storage physical disks page.
Systems Affected	All systems with Intel chipset and Windows operating system.
Workaround	Perform an iDRAC reset.
Tracking number	320555

## Automation—API and CLI

### Table 10. Issue with SetTraceSeverity action

Details	
Description	The SetTraceSeverity action completes successfully even though the UpdateType property is omitted from the request body.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	341336

## Monitoring and alerting

### Table 11. GPU firmware update job status issue

Details	
Description	Following a successful GPU firmware update, the job status changes to "Completed" instead of showing as pending for a virtual AC cycle. Although there is an LC message prompting to AC cycle the system, the job status is incorrectly marked as complete.
Workaround	N/A
Systems Affected	All systems supported by this release with NVIDIA HGX H100 8-GPUs.
Tracking number	342643

### Table 12. P2PBridge.SL.2 information missing in firmware inventory

Details	
Description	After upgrading the iDRAC firmware, the P2PBridge.SL.2 information may disappear from the Firmware Inventory.
Workaround	Performing a cold boot or rebooting the iDRAC resolves this issue.
Systems Affected	PowerEdge XE9680
Tracking number	314436, 303971

### Table 13. Critical system health alerts during PSU firmware updates

Details	
Description	The iDRAC UI shows a critical system health status while updating the PSU firmware.
Workaround	Allow the update process to finish.
Systems Affected	PowerEdge XE9680L
Tracking number	338825

## Miscellaneous

### Table 14. Non-Functional Keys in ESXi 9.0

Details	
Description	<p>Certain keys are not functioning within the ESXi 9.0 server operating system, both in the iDRAC virtual console and directly within the operating system, for various languages. The affected keys are:</p> <ul style="list-style-type: none"> <li>German: ß, ü, ö, ä, °, §, Ü, Ö, Ä, ², ³, {, €, μ</li> <li>Spanish: º, ¡, ñ, ´, ¢, ª, ,, ¿, Ñ, ¨, Ç, ¬, {, €</li> </ul>

**Table 14. Non-Functional Keys in ESXi 9.0 (continued)**

Details	
	<ul style="list-style-type: none"> <li>French: ², é, è, ç, à, ^, ù, °, ", £, µ, §, {, €, ¢</li> <li>Japanese: ¥, {, all Japanese characters</li> <li>Chinese: {, all Traditional Chinese characters</li> </ul>
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	340305

**Table 15. Import failure of SCP templates**

Details	
Description	SCP templates created without the new SNMPv3 keys (SHA384v3Key and SHA512v3Key) fail during import.
Workaround	To generate the new SNMPv3 keys, update the password. If the keys are presently unset, they are created automatically during this process.
Systems Affected	All systems supported by this release
Tracking number	343985/343557

**Table 16. Installing OOB Drivers Issue**

Details	
Description	After installing the RHEL (RHEL 9.4, RHEL 8.10) operating system, the OOB drivers do not install due to a dependency issue caused by the irdma RPM. The irdma package depends on the InfiniBand stack, which is unavailable in the pre-boot environment.
Workaround	After installing the operating system, run the following commands: <ol style="list-style-type: none"> <li>1. Search for OEMDRV location: <code>blkid   grep "OEMDRV"</code></li> <li>2. Mount the location: <code>mount /dev/sda1 /mnt</code></li> <li>3. Run the RPMs manually: <code>rpm -vih /mnt/rpms/x86_64/*.rpm</code></li> </ol>
Systems Affected	PowerEdge XR4000r, PowerEdge XR4000z, PowerEdge XR4510c, PowerEdge XR4520c, PowerEdge XR4000w.
Tracking number	301742

**Table 17. Missing GPU component entries in iDRAC Firmware Inventory**

Details:	
Description	Following an AC cycle, entries pertaining to NVIDIA H100 component versions are missing from the iDRAC Firmware Inventory page. This prevents the accelerator firmware update from progressing, as H100 Baseboard Update Bundle registration is required.
Workaround	Resolve this issue by rebooting the iDRAC.
Systems Affected	PowerEdge XE9680
Tracking number	285593

## 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. The software inventory for Chassis Manager (CM) firmware is available on all SLEDs, allowing updates to be initiated from any SLED. However, if a CM update is started from one SLED, any attempt to initiate another CM update from a different SLED fails, indicating that an update is already in progress.
2. If attributes that need a staged job for modification are changed using a Server Configuration Profile (SCP) import while the host is in power off state, a manual server reboot is necessary to finalize the attribute update. Additionally, to perform a compliance check using the OpenManage Enterprise (OME) template, ensure that the system is powered on before initiating the check.
3. In iDRAC, attaching a folder that is in an NFS share hosted by a Linux-based operating system is not supported.
4. In Lifecycle (LC) interface, It is recommended to avoid performing any operations on media that is mounted as RFS through iDRAC GUI/RACADM/Redfish.
5. 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.
6. 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.
7. 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.
8. 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.
9. If Lifecycle controller logs display RED057 message during a component update, then run the command `systemerase ldata` through RACADM interface and then retry the operation.
10. While performing a PSU firmware update through the host OS in the 15<sup>th</sup> or later Generations of PowerEdge servers, ensure that you perform a cold reboot to apply the update.
11. 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.
12. During OS deployment from LCUI, unmounting OEMDRV through the LC UI or Host OS is not supported. To unmount OEMDRV, either exit LCUI (F10) or wait for automatic unmounting after 18 hours.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. After updating the iDRAC license to Data Center license, ensure that you reboot the iDRAC for Idle server detection feature related attributes to function.
19. In LifeCycle Controller GUI, use the mouse to browse files or folders. Browsing files using keyboard is not supported.

20. 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.
21. 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.
22. 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.
23. 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`
24. 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>
25. 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.
26. 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.
27. Firmware rollback is not supported for CPLD, NVDIMM, SAS/SATA drives, and PSU (on modular systems).
28. 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.
29. 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.
30. 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.
31. 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).
32. 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.
33. Lifecycle Controller supports ISO images with ISO-9660 format only. Other formats including combination with ISO-9660 are not recommended.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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. iDRAC may not always report SWC5015 errors when updating chassis manager (CM) firmware on multiple sleds concurrently. This is an intermittent error reporting issue and does not affect the firmware update functionality.
2. For Log SEL1514, the inlet temperature sensor is erroneously referred to as "Intlet temperature." This issue will be corrected in the upcoming release.
3. The log PWR2402 typically indicates a communication failure. However, on some systems, this log may also appear when a co-processor is restarted and communication with the power firmware is reestablished.

4. For Technical Support Reports (TSR) larger than 5 MB, it is recommended to use remote export instead of local export due to device limitations.
5. Since the CMOS battery sensor is no longer available, the Lifecycle Controller logs display BAT0022 when the CMOS battery voltage drops below 2.2 V while the server is on AC power. Also, if the server has a PERC battery, the Battery view 'Attribute' tab appears on the system overview page, showing the PERC-attached battery. For direct-attached configurations without a battery, this tab is not available.
6. SCV reports generated through the iDRAC UI, and the CLI application may display different SCV application version suffixes. This is a known behavior and has no functional impact.
7. Optimizing fan control algorithms to reduce system power consumption may increase GPU temperatures. This change maintains GPU performance across both maximum performance and minimum power thermal profiles.
8. When an older version of iDRAC firmware (older than version 7.10.30.00) is installed on the PowerEdge 16G XR series servers, then an error message is observed in the iDRAC Lifecycle Controller (LC) log stating "HWC8010 - The System Configuration Check operation resulted in the following issue: Config Error: Sig Pwr Cable 0".
9. SCV validation is not supported when accessing the iDRAC UI over HTTP. Ensure that the HTTPS protocol is used for logging into the iDRAC UI to enable SCV validation.
10. During continuous reboot cycles, SYS336 may occasionally appear in the LC logs. This is merely an informational entry and does not affect functionality.
11. The reporting format in SCV application version 1.92 has undergone a redesign. The iDRAC UI reporting format is in alignment with SCV application version 1.91. Therefore, there may be variations in comparisons between SCV application reporting and iDRAC UI.
12. When servers with SPDM-enabled components undergo an AC power cycle stress or a host reboot stress (cold or warm boot), the LC logs may show errors that are related to SPDM export issues. To address this, it is recommended to incorporate appropriate time intervals between consecutive power cycles. The time that is required for iDRAC readiness may differ based on the server configuration. The objective of these necessary time gaps is to ensure the full functionality of iDRAC and the completion of the Secured Component Verification (SCV) inventory before commencing the next stress cycle.
13. 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.
```

14. 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 then firmware partition. To free up space in the partition, perform System erase by selecting the Lifecycle controller data option in then System category and retry the update.
15. iDRAC displays an 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.
16. The operating system 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 operating system Collector application separately in the firmware inventory page.
17. Redfish Life Cycle Events (RLCE) do not support event generation for collection resources.
18. For staged operations that require a system reboot, after the system reboot is complete RLCE events for the operation may take up to 20 s depending on the system configuration.
19. A Redfish request to update or post with a JSON format payload supports only the first valid JSON in the request. If additional text is passed in the payload, the text gets discarded.
20. During the firmware update process for enclosures like PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460, there are observations of PDR8 and PDR5 disk removal and insertion logs.
21. There is a possibility that the operation for collecting Management Module logs may not successfully complete when gathering iDRAC TSR logs in modular servers. In such cases, directly collect EC Logs from OMEM.
22. In Dell PowerEdge 15<sup>th</sup> Generation servers, the JCP042 error message may be displayed multiple times in the LC logs due to a job failure while retrying the same job. This failure could be caused by memory corruption. To resolve this, run the RACADM command `systemerase lcddata` and then retry the operation.
23. In Dell PowerEdge 15<sup>th</sup> Generation servers with AMD chipset, PR1 & PR10 logs are displayed in LC logs for PSUs when Retire and Repurpose operation is performed. This does not impact server functionality.
24. In Dell PowerEdge 15<sup>th</sup> Generation servers with AMD chipset, SEL events were introduced in iDRAC versions 4.4x. If iDRAC is rolled back to an earlier version, then new events that are logged in the version of iDRAC before it was rolled back may be displayed as an unknown event.
25. After a warm reboot of the server, iDRAC may report "Disk Inserted" in the LC logs for drives behind HBA or PERC12 controllers. This log entry can be safely ignored.
26. After manually powering on the server following a system erase on LC data, several messages stating "PR7 New device detected: POWER SUPPLY (PSU.Slot.X)" may be displayed in the LC logs.
27. While PERC inventory is in progress, Lifecycle controller logging may fail after a warm reboot by RTCM for HBA, BOSS, or NVMe drives.

28. AD/LDAP diagnostic results display Not Run or Not Applicable for Ping Directory Server Tests. ICMP ping tests are no longer performed while running AD/LDAP diagnostics.
29. 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 a 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 a ready state before performing iDRAC reset. To check the status of the services, run the command `getremoteservicesstatus`.
30. 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.
31. After any iDRAC reset event, including the iDRAC firmware update, the LC Log event time is incorrectly reported for a few events. This condition is momentary, and iDRAC time catches up to the correct time.
32. 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 I/O

1. The Intel IPU adapter does not support HII or X-UEFI, and is a channel card with no Dell OEM support. As a result, iDRAC cannot populate a significant amount of data, and some data may not be updated or display default values.
2. Performing PLDM-based channel firmware updates for cards other than Mellanox and NVIDIA ConnectX-7 using the Redfish interface is not supported.
3. On the LC UI Network Settings page, the IPV4 settings are not being saved through DHCP, causing IP addresses to not be assigned. If DHCP fails in the LC UI, opt for a static IP or configure the settings through the iDRAC UI or RACADM interface.
4. When bifurcation is disabled (set to platform default) for a NIC devices in the PCI slot, the PCI lanes that are allocated to the device display as x16 instead of x4.
5. In the iDRAC UI, NVIDIA NIC adapters or NVIDIA BlueField-3 DPUs that are configured in InfiniBand (IB) mode, are classified under the NIC Devices and InfiniBand Devices.
6. During a DPU (Smart NIC) firmware update, SUP0516 message about the 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.
7. The firmware version for DPU cards on the 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.
8. iDRAC may display some unsupported attributes such as PCleOfflineOnlineFQDDList, 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.
9. In PowerEdge R650 and PowerEdge R750 servers, the error 'HWC8010: Configuration error: Add-in card in slot x' may appear after installing a DPU card and restarting the server. To prevent this error, install the DPU card in PCIe Slot 1 for the PowerEdge R650 and in Slot 2 for the PowerEdge R750.
10. iDRAC IPv6 autogenerated 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.
11. Setting the iDRAC static IP using the IPv4 group (IPv4.1.Address, IPv4.1.Gateway, IPv4.1.Netmask) using Redfish or RACADM interface may result in the new IP address not applying, causing the system to become inaccessible. To set a static IP address, use the IPv4Static group (IPv4Static.1.Address, IPv4Static.1.Gateway, IPv4Static.1.Netmask).
12. The iDRAC interfaces show limited details for Mellanox network cards. For instance, when in InfiniBand mode, the card appears as a NIC device. Also, the board manufacturer and version information are not displayed.
13. 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.
14. In an 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.
15. 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.
16. When auto negotiation is disabled while iDRAC is in Shared LOM mode, the speed and duplex values shown in the UI and RACADM output may not accurately show the actual speed and duplex on the link.
17. In systems with network adapters without internal temperature sensors, for some adapters the NIC temperature sensors metric value is reported as 0.

18. 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.
19. 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 the network settings page may not be displayed.
20. 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.
21. 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.
22. If SMBv2 share fails in Lifecycle UI, 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.
23. While iDRAC is initializing, all communications with iDRAC may fail. For any service requests, wait until the initialization process is complete.
24. 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.
25. FRU objects or properties for Network adapters that are embedded on the motherboard are not available through any of the iDRAC interfaces.
26. The iDRAC feature "Topology LLDP" is not supported on 1 GbE controllers and on selected 10 GbE controllers (Intel X520, QLogic 578xx).

## Storage

1. Drive erase operation fails when using server configuration profile (SCP). To overcome this issue, perform the operation using any other supported interfaces.
2. When a PowerVault MD 2412, PowerVault MD 2424, or PowerVault MD 2460 enclosure is connected to an HBA465e and a primary Enclosure Management Module (EMM) is removed, an LC log message PDR5 is generated, indicating that the associated drives that are connected to the enclosure are removed. As a result, the associated drives are not displayed in the iDRAC UI or other interfaces. To resolve this issue, perform an iDRAC reset.
3. ControllerDrivesDecommission operation may take over an hour to complete on a fully populated system.
4. The purge operation of KMS keys may not complete if the PurgeKeyPolicy is set to Keep N, N-1 Keys and the rekey operation is performed, but some drives do not finish rekeying within 180 s. The purge operation will be completed during the next rekey operation.
5. Some storage operations may cause the SystemConfigHash to change, as these operations internally depend on BIOS or iDRAC HII attributes that are essential for the feature or hash generation.
6. For PowerVault MD 2412, MD 2424, or MD 2460 enclosures, the overall status may show as degraded or failed in iDRAC, even if all monitored components are healthy. This may occur because some unmonitored components are possibly reporting errors. Contact Dell support for assistance.
7. On systems with many Virtual disks (VD), the hardware inventory may display a blank Physical Disk ID for some of the VDs. To get more accurate information, see the storage page in iDRAC UI.
8. If the drive backplane of a server is faulty, then the slots that are located behind that backplane may provide inaccurate reports.
9. If a faulty drive is hot-plugged into a BOSS-N1 controller, it might generate a duplicate PDR110 Lifecycle (LC) log entry without a drive PPID.
10. The standard erase process for non-Instant Secure Erase (ISE) drives can be time-consuming and may increase the risk of multiple job failures. For larger drives, this process could potentially take hours or even days.
11. If a faulty drive is hot-inserted into the BOSS controller, its Part Number does not appear in the PDR3 Lifecycle logs. To find the part number, check the Storage overview page.
12. Following a disk firmware upgrade, LC logs might incorrectly indicate a firmware downgrade with a PR36 message. Restarting the host system resolves this issue.
13. Reports about the drives that are not certified by Dell may not be in the Telemetry reports.
14. The 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.
15. 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.
16. Before performing SecureErase on a vFlash, ensure that the partitions on the vFlash are detached.
17. Intel ColdStream NVMe devices do not support cryptographic erase. For more information, see Intel's documentation for the specific device.

18. Creating RAID using the selected controller is not supported through Lifecycle Controller interface. Use the iDRAC UI to create the virtual disk, then relaunch the Lifecycle Controller and retry the deployment operation.
19. Before deleting a VD that hosts the operating system, ensure that you uninstall iSM. If a VD is deleted without uninstalling iSM, the LC log may display the error: "ISM0007 The iDRAC Service Module Communication has ended with iDRAC."
20. 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 the BOSS controller and not connected to the backplane.
21. SMART monitoring is disabled for a hard drive while it is set to Non-RAID mode.
22. 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.
23. 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.
24. 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.
25. For improved support on drives and operating system deployment, it is recommended to use the UEFI BIOS boot mode.
26. 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.
27. 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 a cold reboot is not done.
28. The iDRAC Virtual Keyboard labeling is changed to the upper case to align it with the physical keyboard layout.

## Automation—API and CLI

1. Performing a GET method on URIs listed in the GET response for

```
baseboardservice/<baseboardservice
ID>/redfish/v1/TelemetryService/MetricReportDefinitions/All
```

results in a 404 for AMD GPU. This occurs because the vendor does not support reading index URIs. Example of the URI:

```
https://<IP>baseboardservice/SMC.Embedded.1/redfish/v1/Chassis/UBB/Sensors/
IBC_CURRENT/Reading
```

2. Providing an incorrect port number for the `ltssmSetupTrigger` and `ltssmTriggerState` commands results in a generic error message stating "Unable to perform requested operation" instead of an invalid parameter error.
3. Performing the POST or GET method on the `ResetToDefaults` URI may fail with a 404-response code. Ensure that the `FactoryresetEnable` attribute is set to disabled while performing these methods.
4. After a PSU firmware update using Redfish, the system might face issues to power on, with no VGA console signal detected. Despite the CPLD showing power is good and all OMNI LEDs being lit, the system may stay unresponsive. To resolve this, perform an iDRAC reset.
5. The GET method on the Ports collection URI, when using a filter query parameter with the 'ne' operator, returns incorrect details.
6. Enabling or disabling the Hardware Management Console (HMC) Redfish URI requires an iDRAC reboot on the PowerEdge XE9680.
7. During the hot insertion or removal of an external Enclosure Management Module (EMM), critical logs are expected to be absent from the Fault List URI.
8. The PCIe Switch Board (PSB) firmware inventory might display an incorrect "installation date = 1970-01-01T00:00:00Z" when performing the "swinventory" command using RACADM. This issue does not affect functionality.
9. When upgrading iDRAC firmware from a version earlier than 7.10.70.00, ensure to delete the old PowerMetric MetricReportDefinition (MRD) using DELETE method on the URI (`/redfish/v1/TelemetryService/MetricReportDefinitions/PowerMetrics`) or perform a `racadm racresetcfg` to update the PowerMetrics MRD.
10. Telemetry service may experience a brief disruption (up to 60 s) during a server host reboot, whether initiated manually or as part of a device firmware update.
11. In LC UI, the checkbox for Telemetry Reports in SupportAssist remains active and is not disabled even when the Telemetry Data Stream is turned off.
12. Updating "Tpm2Algorithm" and "inteltxt" attributes through a single job is not supported using RACADM interface. Either update the Tpm2Algorithm and then update inteltxt through separate jobs or use the Server Configuration Profile (SCP) to update both the attributes in a single job.



13. The display of Intel IPU card's PartNumber and SerialNumber in the PCIeDevice instance URI may vary with Redfish, as Redfish interface does not support this card.
14. A compliance error in the Bios AttributeRegistry is marked due to a deviation from the schema to accommodate Value Level dependencies of BIOS attributes in the implementation. This can be disregarded as there is no impact on functionality.
15. 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.
16. 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.
17. During an iDRAC stress test, if the number of user sessions exceed eight, then iDRAC may display unexpected failures for Redfish operations.
18. Values for some properties may not reflect the same across different iDRAC interfaces, as there can be a delay in data refresh.
19. If you get 400 status code while performing Redfish MultipartUpload for firmware updates, wait for five minutes and retry the operation again.
20. 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 PowerEdge Servers Error and Event Messages Reference Guide at [dell.com/idracmanuals](http://dell.com/idracmanuals).
21. 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 go to the iDRAC login page.
22. 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.
23. In Redfish API, all BIOS certificate-related operations are now supported using the new URI: /redfish/v1/Systems/{ComputerSystemId}/Boot/Certificates.
24. PSU Part Replacement Firmware Update will not initiate if the secondary string of the new firmware is the same as the secondary string of the replaced PSU's existing firmware. The firmware version string format is denoted as xx.yy.zz, where zz is the secondary string.
25. You may get an irrelevant response message while performing operating system method to Insert media with incorrect media for firmware upgradation or operating system deployment.
26. 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.
27. 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.
28. Performing the GET method on steps only shows the next scheduled jobs and not the completed jobs.
29. Performing the Redfish Patch method on the Read-Only property for PowerControl resource returns a 200 status code.
30. 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.
31. In the RACADM interface, using XML escape symbols such as &lt; or &gt; or &amp; as AssetTag or as a substring in the AssetTag will be configured as regular characters that they represent.
32. The iDRAC attribute information can be accessed through the RACADM interface by running the Help command, or using Redfish interface by performing a GET on `redfish/v1/Registries`.

## 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 Cipher 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. When FCP is enabled, 'Default Password Warning' setting is disabled after the default user password is changed.
10. 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.
11. 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.

## Miscellaneous

1. If a system shuts down due to a thermal trip (not a standard thermal shutdown), it may remain in a critical state. Perform an AC power cycle to restore operation, then check system logs for the cause.
2. When PCI is disabled, the BIOS inventory information is not accessible to PLDM. As a result, iDRAC may incorrectly identify GPUs as Processing Accelerators. To resolve this issue, ensure that the PCI slots are enabled.
3. Issues may arise when uploading iDRAC firmware through the iDRAC GUI. To resolve this issue, power off the system and then proceed with the iDRAC DUP upload method.
4. Following an SDPM Sanitize job, a Job ID may be created but remain incomplete. To resolve this, delete the incomplete job from the iDRAC GUI and initiate a new job.
5. An iDRAC reset or upgrade causes the reinitialization of the Octal Small Form Factor Pluggable (OSFP) ports, which may result in the ports going down. It is recommended to plan any iDRAC resets or upgrades during maintenance windows.
6. During the server's pre-boot mode, only a limited number of sensors are inventoried. Once the server transitions to full-boot mode, all sensors are inventoried. A server remains in pre-boot mode if the GPU drivers are not installed.
7. iDRAC shows the GPU Board Part Number as N/A, which is expected and does not affect functionality.
8. In the middle of booting or when accessing the LC UI, the server may shut down immediately if the iDRAC detects a GPU leak. This also applies to other pre-boot environments.
9. 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.
10. The host operating system may display an incorrect folder size of the folder that is attached through remote file sharing.
11. The iDRAC GUI may indicate "High Line" instead of "Extended High Line" for all PSUs, even if three are of the extended type and one is "High Line." To ensure accurate configuration information, maintain consistency in the PSU types connected. If two different power supply types are installed, remove the undesired PSU and perform an iDRAC reset.
12. Servers equipped with 1400 W power supply units (PSUs) of different hardware revisions, such as A01 and A02, show a discrepancy in the iDRAC GUI. The A02 PSU is displayed as AC Type, while the A01 is shown as DC Type. To avoid this issue, use PSUs of the same A02 version.
13. The iDRAC firmware update for servers with an Identity Module installed fails from iDRAC Group Manager with the error "Firmware is invalid for this platform." To resolve this, use other iDRAC interfaces to update the firmware.
14. Some Virtual Keyboard keys or key combinations may not produce the correct output for languages other than English. To resolve this, use the physical keyboard or the Windows On-Screen Keyboard.
15. Virtual Console and Virtual media may not function on the Safari browser while iDRAC is set to use TLS version 1.3. Ensure that browser settings are updated to TLS 1.2 or below.
16. Configuring Power Factor Correction (PFC) for power supplies in all Dell 15<sup>th</sup> generation of PowerEdge servers is not supported.
17. While the BIOS is set to Boot mode, boot capture video file size is limited to 2 MB. During the video capture, if the size of the video file exceeds the limit, then only partial operation is captured.
18. CPLD update may fail if DUP method is used while power cap policy is enabled.
19. Remote File Share (RFS) through HTTP is only supported without authentication.
20. 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.
21. Arrow keys on the 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.



22. If the SOL session is active for a long duration or if the system is rebooted multiple times, the SOL session gets terminated automatically.
23. For Dell online catalog update, downloads.dell.com only supports the https protocol.
24. If you install OMSA while iSM is already installed and connected, iSM may restart after the OMSA installation is complete.
25. 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.
26. 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.
4. LDAP bind password does not accommodate password hashes; it solely supports clear text. Consequently, no password hash is supported for any SCP export. Additionally, there is no mechanism to retrieve the password in clear text through SCP, or any retrieval method through Redfish or RACADM. Users are responsible for managing their passwords.

### Automation — API and CLI

1. According to the DMTF specification, certain properties should support ReadWrite permissions. However, on the AMD GPU baseboard service, these properties are read-only. For example, the SpeedLimitMHz property is marked as ReadWrite in the schema, but cannot be modified in the AMD GPU baseboard implementation. URI:

```
URI: https://<ip>/baseboardservice/SMC.Embedded.1/redfish/v1/Systems/UBB/Processors/GPU0
```

2. Redfish continues to report the Operating System as running even if the server fails to boot the OS. This may not accurately reflect the actual state of the server.
3. When configuring streaming Telemetry reports, you can set up to 20 reports with a maximum interval of 30 minutes and 3 streaming destinations, or up to 15 reports with a minimum interval of 10 seconds and 2 streaming destinations; exceeding these limits may result in some report sequences being dropped.
4. During server reboot, it is recommended to wait a few seconds before initiating Redfish requests. Immediate sending of Redfish requests may result in failures.
5. The Expand Level feature in the Redfish API should be avoided, as it is likely to result in a timeout due to the management console's extended processing time.
6. When voltage warnings and critical events are logged in the LC logs, the Redfish `originalOfCondition` property will not display the absolute path URI of the failing sensor. Instead, it shows the URI as `redfish/v1/Chassis/System.Embedded.1/Sensors`.
7. After completing the Collecting Inventory process using POST, attempting to run Redfish GET requests immediately may result in a 503-status code (resource not available). Wait a few minutes before retrying the GET request.
8. When setting a value for the BIOS attribute EmbSata, the BIOS attributes SecurityFreezeLock and BootMode may also be reported as pending due to their dependency on other attributes.
9. The configuration result, such as the result for SCP configuration operation, has a limit of 32 KB. If the result surpasses this limit, certain configuration details may not be visible in the output of the Configuration result.
10. Attempting to enable SEKM for PERC 12 through a staged configuration job using the Redfish interface results in failure. Try SEKM activation for PERC 12 through the Redfish interface by using a real-time configuration job.
11. 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.
12. Sometimes, when using WSMAN, an Internal SSL Error is reported and the WSMAN command fails. If this issue occurs, retry the command.

13. 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`**.
14. RACADM supports the underscore character (`_`) for `iDRAC.SerialRedirection.QuitKey` along with the existing symbols shown in the integrated help.
15. 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.
16. 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. The error "RED027 - Insufficient space to upload the requested firmware image" may be displayed while uploading a firmware image. To resolve this issue, check for any existing core files in iDRAC by running the command `racadm coredump`. Then, run the command `racadm coredumpdelete -all` to clear all core files. After clearing the core files, retry the firmware upload process.
2. Launching the iDRAC UI using the Fully Qualified Domain Name (FQDN) on the Chrome browser with http default and custom port is not supported. To access the iDRAC UI, it is recommended to use other browsers such as Edge or Firefox.
3. In Dell 15G PowerEdge servers with iDRAC firmware version 7.10.50.00 or later, downgrading or rollback of iDRAC firmware to versions 4.40.00.00 or older is not supported. When attempted, the downgrade or rollback process appears successful, however, no firmware version changes are applied. In iDRAC Lifecycle Logs RAC0181 events are logged as "The iDRAC recovered from a firmware boot loader error with the following reason: Boot-time failover."
4. 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.
5. In the Firmware Rollback page, the component names may vary in iDRAC UI and Lifecycle Controller(LC) UI.
6. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
7. LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from the iDRAC web interface.
8. 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.
9. 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.
10. 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.
11. During import server profile operation, if the image filename is "Backup.img," the operation may fail. To avoid this failure, change the filename.

## Monitoring and alerting

1. In PowerEdge XE9680 servers configured with AMD GPUs, UEFI0060 event logs are not generated for Power Budgeting issues.
2. iDRAC9 intermittently displays a 0-Volt reading for CPU VCCD Voltage Regulator sensors when alternate supplier Voltage Regulators that do not support the I2C protocol are used.
3. Dell Connectivity Client requires accurate time settings in iDRAC or time synchronization with Network Time Protocol (NTP) to ensure robust verification of digital certificates, maintaining connectivity, and integrity of the logs.
4. NVIDIA GPU PerformanceState data is not available on iDRAC.
5. If the iDRAC time and the BIOS time are not synchronized, the CPLD update task ID is automatically deleted during a virtual power cycle.
6. When multiple server reboots or rapid reboots are performed in quick succession, some sensors may stop reporting. To recover from this state, reboot the iDRAC.
7. PR7 log entries may be recorded in the Lifecycle Controller (LC) logs during warm reboots, cold reboots, and AC power cycles.
8. 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 UI or run the RACADM command `racadm storage get pdisks -o`.
9. 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.
10. In certain cases, the 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`.
11. 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.
12. 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.
13. 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.
14. The inventory that is 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 the LC UI.
15. In certain cases, in the 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**.
16. While the server is under high utilization, 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.
17. 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.
18. iDRAC supports iSM version 3.4.1 and above.
19. 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 perform 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.

## Operating system deployment

1. Using iDRAC interfaces to perform operating system installation, depending on the operating system type, no LC log events get logged reporting that an operating system operation is being performed. This is a limitation of the operating system type itself, not an iDRAC limitation.
2. Once the operating system installation is complete, depending on the operating system type, the operating system hostname may not be populated in iDRAC interfaces. This is a limitation of the operating system type itself, not an iDRAC limitation. For operating system types that do not automatically populate this data, install iSM in the operating system and reboot the server to populate this data in iDRAC.
3. Operating system installation fails when the operating system media volume name (label) is blank. Recommendation is to add a valid volume name for operating system media (USB drive, DVD, and so on) before starting the operating system installation.
4. While installing an operating system, a media verification warning message may be displayed. This has no impact on the installation, to proceed, click **Yes**.
5. 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.

6. Deployment of Windows Server operating systems 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 operating system installation. After the operating system 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 a customized deployment. For more details, see Microsoft's documentation.

7. LC may display multiple drive names for some CDs or DVDs, such as the ones containing operating systems.
8. If the operating system selected for installation and the operating system on the media used are different, LC displays a warning message. However, while installing the Windows operating system, the warning message is displayed only when the bit count (x86 or x64) of the operating system 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.
9. In Windows10, the 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. SCP export and import only supports LDAP bind password as clear text, hash values are not supported
2. 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.
3. iDRAC9 does not support Personal Identity Verification (PIV) or Common Access Card (CAC) smart card users on a child or subdomain in a forest or collection of domains. To overcome this limitation, it is recommended to deploy all smart card users on the root domain instead of the child domains within the forest.

## Storage

1. When upgrading or downgrading firmware for channel devices or hard drives, refer to the vendor product documentation for brand-specific limitations, including flash limits.
2. iDRAC interfaces do not support slicing RAID volumes through software RAID controllers. To configure sliced RAID volumes, use F2 Device settings.
3. 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.
4. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
5. 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`
6. 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.
7. If a M.2 SATA drive attached to BOSS-S2 controller is removed, performing a blink operation may not fail for the removed drive.
8. The standard erase procedure for non-ISE drives is notably time-consuming, particularly for larger drives, potentially spanning hours or days, with the added risk of job failure. A workaround is to conduct the erase on each disk individually while other drives are uninstalled.

## 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 [iDRAC Manuals](#).
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. Replacing an existing Hardware Platform Management (HPM) or Secure Control Module (SCM) board with a used board is not recommended, as it may result in configuration settings not being applied to the replaced board.
2. When the attribute USBMux0Hmc0Lock is enabled, the iDRAC displays only limited information for GPU inventory data. Specifically, the Name, Product Name, Status, State, and Slot Number are displayed.
3. You may be unable to scroll using the keyboard. Use the mouse to scroll.
4. 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.
```


5. 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.
6. 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.
7. Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
8. 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.
9. 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.
10. iDRAC login page does not allow password entry using Firefox browser in Ubuntu management OS.
11. 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.
12. In Lifecycle Controller GUI, using keyboard to browse folders and files is not supported. Use the mouse to navigate through files and folders.

## 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.

 **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](http://dell.com/idracmanuals).

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

## Supported systems

**Table 18. Supported systems**

15 <sup>th</sup> Generation of PowerEdge Servers	16 <sup>th</sup> Generation of PowerEdge Servers
PowerEdge C6520	PowerEdge C6615
PowerEdge C6525	PowerEdge C6620
PowerEdge MX750c	PowerEdge HS5610
PowerEdge R250	PowerEdge HS5620
PowerEdge R350	PowerEdge MX760c
PowerEdge R450	PowerEdge R260
PowerEdge R550	PowerEdge R360
PowerEdge R650	PowerEdge R660
PowerEdge R650XS	PowerEdge R660XS
PowerEdge R750	PowerEdge R6615
PowerEdge R750XA	PowerEdge R6625
PowerEdge R750XS	PowerEdge R760
PowerEdge R6515	PowerEdge R760XA
PowerEdge R6525	PowerEdge R760XD2
PowerEdge R7515	PowerEdge R760XS
PowerEdge R7525	PowerEdge R7615
PowerEdge T150	PowerEdge R7625
PowerEdge T350	PowerEdge R860
PowerEdge T550	PowerEdge R960
PowerEdge XE8545	PowerEdge T160
PowerEdge XR11	PowerEdge T360
PowerEdge XR12	PowerEdge T560
PowerEdge XR4510c	PowerEdge XE8640
PowerEdge XR4520c	PowerEdge XE9680
Dell vSANR 6515 Ready Node	PowerEdge XR5610
Dell vSANR 7515 Ready Node	PowerEdge XR7620
Dell XC Core XC450	PowerEdge XR8610T
Dell XC Core XC650	PowerEdge XR8620T
Dell XC Core XC6520	PowerEdge OEMR T560
Dell XC Core XC7525	Dell XC Core XC660
Dell XC Core XC750	Dell XC Core XC760
Dell XC Core XC750xa	Precision 7960 Rack

**Table 18. Supported systems (continued)**

15 <sup>th</sup> Generation of PowerEdge Servers	16 <sup>th</sup> Generation of PowerEdge Servers
OEMR R250	Precision 7960 XL Rack
OEMR R350	
OEMR R450	
OEMR R550	
OEMR R650	
OEMR R650xs	
OEMR R6515	
OEMR R6525	
OEMR R750	
OEMR R750xa	
OEMR R750xs	
OEMR R7515	
OEMR R7525	
OEMR T150	
OEMR T550	
OEMR XE R250	
OEMR XE R350	
OEMR XR12	

## Supported managed server operating systems and hypervisors

 **NOTE:** AMD MI300X GPUs do not support any Windows operating system in this release of iDRAC.

- Microsoft Windows
  - Server 2025
  - Server 2022 Standard
  - Server 2022 Datacenter
- Linux
  - RHEL 9.5
  - RHEL 8.10
- SLES
  - SLES 15 SP6
- Ubuntu
  - Ubuntu 24.04.2

## Supported web browsers

- Microsoft EDGE
- Safari 16.6
- Safari 17.x
- Mozilla Firefox 128
- Mozilla Firefox 129
- Mozilla Firefox 130
- Google Chrome 137



- Google Chrome 138

## 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), v11.1.0.0
- Dell iDRAC Tools for Linux, v11.1.0.0
- Dell iDRAC Tools for VMware ESXi (R), v11.1.0.0

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 [Dell Support](#) page.

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 2.16
- IBM Security Guardium Key Lifecycle Manager version 4.1.1.0
- Utimaco Enterprise Secure Key Manager version 8.5.3
- Fortanix Data Security Manager version 4.23.2324
- Entrust KeyControl 10.3.1

 **NOTE:** Thales ended support and reached end-of-life for the Gemalto SafeNet KeySecure key management server (k150v) on December 31, 2023. Also, Thales discontinued the support for the Data Security Manager (DSM).

## Chassis Manager and iDRAC firmware alignment

Ensuring alignment between the Chassis Manager (CM) firmware version and the iDRAC firmware version is important for optimal performance and compatibility within Dell PowerEdge C-series servers.


Mismatched firmware versions can lead to functionality issues, security vulnerabilities, and potential system instability. The following table provides a general guideline for ensuring compatibility between CMC and iDRAC firmware versions.

**Table 19. CM and iDRAC firmware versions**

Chassis Model	CM Firmware Version	iDRAC Firmware Version
PowerEdge C6600 with PowerEdge C6615 sleds	2.20	7.20.30.50
PowerEdge C6400 with PowerEdge C6520 sleds	3.71	7.20.30.50
PowerEdge C6400 with PowerEdge C6525 sleds	3.71	7.20.30.50
PowerEdge C6400 with PowerEdge C6420 sleds	3.71	7.00.00.181

## Installation and upgrade considerations

### Downloading iDRAC firmware installation file

 **NOTE:** For information about updating iDRAC firmware using various interfaces, see the *iDRAC User's Guide* available at [iDRAC Manuals](#).

1. Go to [Dell Support](#) page.
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 operating system

From the host operating system, install the 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 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 [iDRAC manuals page](#).
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 20. Direct links for documents**

URL	Product
<a href="#">iDRAC Manuals</a>	iDRAC and Lifecycle Controller
<a href="#">CMC Manuals</a>	Chassis Management Controller (CMC)
<a href="#">ESM Manuals</a>	Enterprise System Management
<a href="#">Software Serviceability Tools</a>	Serviceability Tools
<a href="#">Client System Management Manuals</a>	Client System Management


### Accessing documents using the product search

1. Go to [Dell Technologies Support site](#).
2. In the **Identify your product or search support** search box, type the product name. For example, **PowerEdge** or **iDRAC**. A list of matching products are 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 [Dell Technologies Support site](#).
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**.

## Lifecycle Controller (LC) Remote Services — client tools

### Redfish API

For information about Redfish, see the DMTF website [DMTF Redfish](#). This website provides access to schema files, white papers, technical notes, and so on.

For iDRAC Redfish API guide, go to [Dell Developer Portal](#).

### iDRAC SNMP MIB Files

The iDRAC SNMP MIB files are now available for download along with the iDRAC firmware and can be accessed on the Dell Support page. To download the files:


1. Go to [Dell Support](#) page.
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. From the list, locate the iDRAC entry and click the iDRAC firmware version to expand for more information.
5. Click **View full driver details**.
6. Locate the iDRAC MIB file and click **Download**.

## 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

 **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.