

# iDRAC9 with Lifecycle Controller Version 3.31.31.31

Release Notes

## Notes, cautions, and warnings

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

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

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

© 2018 - 2019 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

# Contents

<b>1 Release summary.....</b>	<b>5</b>
Priority and recommendations.....	5
<b>2 Compatibility.....</b>	<b>6</b>
License Requirements.....	6
Supported systems.....	6
Previous versions.....	6
Supported managed server operating systems and hypervisors.....	6
Supported web browsers.....	7
Supported software.....	7
<b>3 New and enhanced features.....</b>	<b>8</b>
Hardware.....	8
iDRAC and LC firmware.....	8
OS deployment.....	8
Automation—API and CLI.....	8
Security.....	8
Storage and storage controllers.....	8
<b>4 Fixes.....</b>	<b>9</b>
iDRAC and LC firmware.....	9
Security.....	9
<b>5 Important notes.....</b>	<b>10</b>
<b>6 Known issues — To be fixed in future releases.....</b>	<b>12</b>
Storage devices not found in iDRAC.....	12
NIC or FC device slot listed in hardware inventory even when disabled in BIOS.....	12
<Keyboard_Mouse_USB_reset_warning> button in Virtual Console with Java plug-in.....	12
Foreign Preview not found & not able to clear the foreign config on storage controller in iDRAC.....	12
Firmware Downgrade of Storage Controllers.....	13
Header Error while using Powershell for Redfish requests.....	13
Port 5353 blocked by iDRAC internal firewall and appears as Open Filtered .....	13
<b>7 Limitations.....</b>	<b>14</b>
Authentication.....	14
Automation — API and CLI.....	14
Hardware.....	14
iDRAC and LC firmware.....	14
Monitoring and alerting.....	15
Networking and IO.....	15
OS deployment.....	16
Security.....	16
Storage and storage controllers.....	16

SupportAssist and parts replacement.....	17
Firmware and driver update.....	17
Miscellaneous.....	17
<b>8 Updating iDRAC firmware.....</b>	<b>18</b>
Downloading iDRAC firmware installation file.....	18
Updating iDRAC firmware from host OS.....	18
Updating iDRAC remotely using iDRAC web interface.....	18
<b>9 Lifecycle Controller Remote Services — client tools.....</b>	<b>19</b>
<b>10 Resources and support.....</b>	<b>20</b>
<b>11 Contacting Dell EMC.....</b>	<b>21</b>

# Release summary

This release adds support for Secure Enterprise Key Manager (SEKM).

 **NOTE:** You cannot downgrade the iDRAC and storage controller firmware to a non-SEKM version if SEKM has been enabled on the storage controller.


## Version

iDRAC9 with LC 3.31.31.31

## Release date

June 2019

To download this version of iDRAC, see [Downloading iDRAC firmware installation file](#).

 **NOTE:** For details about the previous releases, if applicable, or to determine the most recent release for your platform, and for latest documentation version, see *KB article SLN308699* available at [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals).

### Topics:

- [Priority and recommendations](#)

## Priority and recommendations

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

# Compatibility

## License Requirements

iDRAC features are available based on the purchased license.

- iDRAC Enterprise — Available on all servers.
- iDRAC SEKM — Only available on systems mentioned in the *Supported Systems* section.

For more information about the features available for a license, see the iDRAC licenses section in the iDRAC 3.31.31.31 User's Guide available at [dell.com/idracmanuals](http://dell.com/idracmanuals).

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

## Supported systems

- PowerEdge R640
- PowerEdge R740
- PowerEdge R740xd
- PowerEdge R840
- Precision 7920 Rack

## Previous versions

- 3.21.21.21
- 3.21.21.22
- 3.21.24.22
- 3.21.25.22
- 3.23.23.23
- 3.24.24.24
- 3.30.30.30

## Supported managed server operating systems and hypervisors

- Microsoft Windows
  - Server 2012 R2 Foundation
  - Server 2012 R2 Essentials
  - Server 2012 R2 Standard
  - Server 2012 R2 Datacenter
  - Server 2016 Essentials
  - Server 2016 Standard
  - Server 2016 Datacenter
  - Server 2019 Datacenter
  - Server 2019 Standard
  - Server 2019 Essentials
  - Server 1809 aka, Redstone 5
  - WinPE 5.0 64-bit
  - WinPE 10
- Linux

- RHEL 7.6
- RHEL 6.10
- SLES
  - SLES 15
- Ubuntu
  - Ubuntu 18.04
- VMware
  - ESXi 6.5 U2
  - ESXi 6.7 U1

## Supported web browsers

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari 11.1
- Mozilla Firefox 63
- Mozilla Firefox 64
- Google Chrome 69
- Google Chrome 70

## Supported software

### Java

- Java - Oracle version
- OpenJDK 8u202

### iDRAC tools

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

- Dell EMC iDRAC Tools for Microsoft Windows Server(R), v9.3.0
- Dell EMC iDRAC Tools for Linux, v9.3.0
- Dell EMC iDRAC Tools for VMware ESXi (R), v9.3.0

This version contains:

- Remote/Local RACADM on Windows or Linux or ESXi
- IPMI Tool on Windows or Linux
- VMCLI on Windows or Linux

Download the DRAC tools from the **Drivers & downloads** page for your system at [www.dell.com/support](http://www.dell.com/support).

Before installing iDRAC tools from OM 9.3.0, you must uninstall any older versions of DRAC tools. For more information about uninstalling applications, see the documentation for your operating system.

## New and enhanced features

### Hardware

- N/A

### iDRAC and LC firmware

- Added support for Dell EMC OpenManage Secure Enterprise Key Manager (SEKM) with key management functionality.
- Added the attribute IPVer for IP version in the list of I/O identity optimization attributes list.
- Added support for updating IDSDM firmware using out-of-band methods, to version 1.9 or later.

### OS deployment

- N/A

### Automation—API and CLI

- N/A

### Security

- Support for Secure Enterprise Key Manager in iDRAC.

### Storage and storage controllers

- Added feature to enable PERC to switch to SEKM security mode.



## iDRAC and LC firmware

- The SEKM feature is activated by purchasing an iDRAC upgrade license key and requires the presence of an iDRAC Enterprise license.
- The SEKM feature adheres to industry standards (KMIP) for enterprise key management systems and provides a robust solution for locking self-encrypting drives.

## Security

- This release adds Secure Enterprise Key Manager capabilities to PowerEdge servers by embedding code into iDRAC for secure key exchange with an external Key Manager Server (KMS).
- Storage Controllers use an external secure key store for key management.

## Important notes

1. It is required to install SEKM license before you update the iDRAC to SEKM supported version, 3.31.31.31. If you install the SEKM license after updating the iDRAC to SEKM supported version, you will then have to reapply SEKM supported iDRAC firmware.
2. If you are configuring a Gemalto based KeySecure SEKM Server with iDRAC, and to get the redundancy feature functional, you need to copy the Certificates manually from primary Gemalto KeySecure cluster to Secondary Gemalto SEKM KeySecure cluster. The redundancy feature will work only after that, if iDRAC is set up for SSL certificate-based authentication.
3. Key sharing between multiple iDRACs is supported and can be configured on the SEKM server. If all iDRACs are part of the same SEKM group, all keys must be assigned to the same group with the right permissions to share the keys.
4. The Server Configuration Profile (SCP) attribute RepositoryUpdate under the System.Embedded.1-1 component has been renamed to SCP.1#RepositoryUpdate in iDRAC versions 3.40.40.40 and above. However, templates containing the older naming of the attribute are still compatible with 3.40.40.40 and above.
5. 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>
6. 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 an AC power cycle (cold boot) is performed, the OEMDRV drive is automatically deleted.

7. CPLD firmware update has no impact on Trusted Platform Module enablement.
8. 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.
9. If the network is not configured and you try to perform a network operation in LC, a warning message is displayed. When you go to the network settings page from this message, the left navigation panel on network settings page may not be displayed.
10. If Test Network Connection fails for a valid address in LC, try configuring the network settings again. If the issue persists, restart the system and retry the operation.
11. Reboot an already launched instance of LC while you reset or update iDRAC. If you do not reboot, LC may show unexpected behavior.
12. Fibre channel NIC cards with dual or four ports are displayed as a single port card in LC. However, all ports are updated when a firmware update is performed.
13. 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.
14. Rollback is not supported for CPLD.
15. If an NVMe drive reports a 'Failed' status due to any of the controller SMART errors, it should be treated as a predictive failure. 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.

16. This note is applicable only to PowerEdge C6420, DCS9650, DCS9670, and DCS9690 systems. If you update iDRAC to this version from version 3.02.x.x or earlier, you must perform a power cycle of the system before performing any power-related operations. The power cycle is required to tune the memory parameters without affecting the host. iDRAC tunes the memory parameters at the first power cycle after a firmware update.

To complete the memory tuning:

- a. Update to this version of iDRAC.
  - b. At the next possible maintenance cycle, or before any power operations are performed, turn off the host.
  - c. Wait for 2 minutes for iDRAC to reset and tune the memory parameters.
  - d. Power on the host.
17. This note is applicable only to PowerEdge M640 and FC640. If you update iDRAC to this version, you must perform a virtual reset of the system from CMC. Reseat is required to tune the memory parameters and to resolve issues that may lead to the watchdog timer causing iDRAC to be reset.

To complete the memory tuning:

- a. Update to this version of iDRAC.
  - b. At the next possible maintenance cycle, perform a virtual reset.
18. The first inventory collection after system reboot may display both PR7 (New Device Detected) and PR8 (Device not detected) messages. This happens after updating iDRAC Firmware to 3.31.31.31 from a previous version. A change in the slot number display format causes this behavior, which is expected.
19. 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
20. This note is applicable only to PowerEdge M640 and FC640. The host may not power on When performing a BIOS Recovery operation. To recover from this condition, perform a virtual/physical reset operation of the blade server.
21. LC logs may display Message ID PR36 ("Version change that is detected for PCIe SSD firmware. Previous version:X.X.X, Current version:X.X.X") after updating the iDRAC firmware to version 3.31.31.31 or later. Ignore the log entry as it is due to a change in the naming convention.
22. After downgrading the iDRAC firmware from version 3.31.31.31 to any previous versions, storage page and drives may display warnings. To resolve the issue, reset iDRAC using the 'racreset' command.
23. Use the following commands If you get an error while performing SupportAssist collection through RACADM using HTTPS share:
  - a. Racadm supportassist collect
 

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

```
racadm supportassist exportlastcollection -l <https> -u <username> -p <password>
```
24. If SMBv2 share fails in Lifecycle GUI, ensure that:
  - the **Digitally sign communications** option is disabled
  - permissions to access the folder/file are granted
  - folder/file name does not have a space
  - share contains fewer files and folders

## Known issues — To be fixed in future releases

### Storage devices not found in iDRAC

<b>Description</b>	If you disable the external slot that is connected to PERC, iDRAC will not detect the PERC card or storage devices present in the server.
<b>Workaround</b>	Remove the PERC card from the external slot that needs to be disabled and powercycle the system.
<b>Systems affected</b>	All system supported by this release.
<b>Tracking number</b>	113901

### NIC or FC device slot listed in hardware inventory even when disabled in BIOS

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

### <Keyboard\_Mouse\_USB\_reset\_warning> button in Virtual Console with Java plug-in

<b>Description</b>	Button does not display the localized name, you may see the button's English variable name with no online help support. The intent of this button is to reset keyboard mouse functionality without having user to restart the Virtual Console
<b>Workaround</b>	Keyboard and Mouse reset functionality works. Does not disrupt the end user experience, only impairs the aesthetic.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	119759

### Foreign Preview not found & not able to clear the foreign config on storage controller in iDRAC

<b>Description</b>	iDRAC not detecting foreign configuration present on drives with unsupported RAID level while the controller is in eHBA mode. Clearing foreign configuration will not available through iDRAC web interface
<b>Workaround</b>	Use Racadm to clear the foreign config
<b>Systems affected</b>	All systems supported by this release
<b>Tracking number</b>	116804

# Firmware Downgrade of Storage Controllers

<b>Description</b>	You cannot downgrade the PERC firmware from SEKM supported controller firmware to a previous version if SEKM is enabled on the controller. Downgrading of other PERC controller firmware in the same system which is not in SEKM mode may also fail.
<b>Workaround</b>	To downgrade firmware for the PERC controllers that are not in SEKM mode, you can use the OS DUP update method or disable SEKM on the controllers and then retry the downgrade from iDRAC.
<b>Systems affected</b>	All system supported by this release.
<b>Tracking number</b>	130745

# Header Error while using Powershell for Redfish requests

<b>Description</b>	iDRAC RESTful API with Redfish displays an error stating unacceptable header specified in request for commands run on PowerShell. Unlike other REST API tools such as Python, CURL and Postman, the PowerShell Invoke-WebRequest command does NOT automatically add a header to REST requests; the header must be explicitly included by the programmer.
<b>Workaround</b>	You need to explicitly include a header while using Powershell for any type of Redfish request.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	N/A

# Port 5353 blocked by iDRAC internal firewall and appears as Open|Filtered

<b>Description</b>	When node initiated discovery or Group Manager is enabled, iDRAC uses mDNS to communicate through port 5353. However, when both are disabled, port 5353 is blocked by iDRAC's internal firewall and appears as Open Filtered port in the port scans.
<b>Workaround</b>	Group Manager and node initiated discovery need to be turned off in order to disable mDNS.
<b>Systems affected</b>	All systems supported by this release.
<b>Tracking number</b>	N/A

# Limitations

## Authentication

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

## Automation — API and CLI

1. Sometimes, when using WSMAN, an Internal SSL Error is reported and the WSMAN command fails. If this issue occurs, retry the command.
2. 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`.
3. RACADM supports the underscore character (`_`) for `iDRAC.SerialRedirection.QuitKey` along with the existing symbols shown in the integrated help.
4. Using remote RACADM, if you use the `racadm hwinventory export` command to export the hardware inventory using an incorrect CIFS share, an incorrect message is displayed: `RAC930 : Unable to export the hwinventory`. If the issue persists, restart iDRAC and retry the operation after iDRAC has finished restarting.
5. If iDRAC is in lockdown mode and you run the command 'racadm rollback', followed by the command 'racadm resetcfg', an incorrect message is displayed: `ERROR: A firmware update is currently in progress. Unable to reset the RAC at this time`. Reboot iDRAC to display the correct error message.
6. While using a `Top` or `Skip` command, if you enter a value greater than the unsigned long type (4,294,967,295), you may get an incorrect error message.
7. You cannot use the FQDD of iDRAC (`iDRAC.Embedded.1`) when changing iDRAC mode from Shared LOM to Dedicated.

## Hardware

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

## iDRAC and LC firmware

1. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
2. LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC web interface.
3. 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.
4. 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.

5. After downgrading iDRAC from version 3.30.30.30 to version 3.00.00.00, 3.11.11.11, or 3.15.15.15, the jobs created in the job queue are deleted. Recreate the jobs after the downgrade is complete.
6. On PowerEdge R6415, R7415, R7425, if you downgrade iDRAC firmware from version 3.30.30.30 to an earlier version, some certificate-related operations may not function properly and certain hardware information may not be displayed correctly. To resolve the issue, reset iDRAC using the 'racresetcfg' command.
7. Remote syslog settings may not be retained after iDRAC firmware is downgraded from version 3.30.30.30 to an older version. Ensure that you reconfigure the remote syslog settings after downgrading the iDRAC firmware.
8. During import server profile operation, if the image filename is "Backup.img", operation may fail. To avoid this failure, change the filename.

## Monitoring and alerting

1. In certain cases, Group Manager Jobs view may not show a detailed error message for a member iDRAC job. For more information about the failure, review the job execution details in the Lifecycle Logs of the member iDRAC by using the web interface (**Maintenance > Lifecycle Log**) or by using the RACADM command `racadm lclog view`.
2. PCIe SSDs in NVMe RAID mode may not display the updated state due to predicted failure. To update RAID-related information, ensure that a CSIOR is performed.
3. If the LCD display is blank, press any one of the three LCD buttons to turn on the LCD before inserting a USB storage device.
4. If Flex Address is enabled on Chassis Management Controllers (CMC), iDRAC and LC do not display the same MAC addresses. To view the chassis-assigned MAC address, use the iDRAC web interface or the CMC web interface.
5. The inventory displayed in LC UI may not be the same as that of any iDRAC interfaces. To get the updated inventory, run the CSIOR, wait for 2 minutes, reboot the host, and then check the inventory in LC UI.
6. In certain cases, in Group Manager Jobs view, the completion percentage for a job may be displayed incorrectly (>100%) for a job in progress. This is a temporary condition and does not affect how Group Manager jobs are performed. When the job is completed, Group Manager Jobs view displays **Completed successfully** or **Completed with errors**.
7. While running host stress test, if the system ID/Health LED turns off from blue, then press the ID button for a second and press it again to turn on the LED.
8. When setting the iDRAC Service Module (iSM) monitoring attributes from the web interface, if the BIOS watchdog timer is enabled, an error may be displayed but the attributes are set. To avoid the error, disable the BIOS watchdog timer or disable the iSM Auto System Recovery and then apply the attributes.
9. iDRAC version 3.30.30.30 supports iSM version 3.4.0 and above.

## Networking and IO

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

- Network cable is disconnected.
  - After a Repurpose and Retire operation is performed.
  - Network is configured with the network cable connected but the network card is replaced later.
11. Any changes to the network settings in iDRAC take effect after 30 seconds. Any automation or user verification needs to wait for 30 seconds before verifying the new settings. iDRAC returns the old active value until the new values take effect. Any DHCP settings may take more time (>30 seconds) depending on the network environment.
  12. When trying to save network details using the Network Configuration page of LC UI, the following error message may be displayed:  
Unable to save the IPvX network settings, where X is the version of IP (IPv4 or IPv6). The following could be one reason for this error:  
  
On the Network Settings page of Lifecycle Controller GUI, the IP Address Source for both IPv4 and IPv6 is either DHCP or Static and DHCP is selected by default. So, even if you want to use only one version of IP address, LC tries to validate both versions, and displays an error if the network details for the unintended version cannot be validated.  
  
If the error does not apply to the IP version you are using, click OK to close the error message. All the other settings that you configured are saved. You can either click Cancel or Back to navigate away from the Network Settings page.
  13. If the Gateway IP is not configured in a network, the network settings and operations in LC UI may show some unexpected behavior.

## OS deployment

1. 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.

2. Deployment of Windows Server operating systems (OS) using LC may fail with one of the following messages:

- Windows installation cannot continue because a required driver could not be installed
- Product key required
- Windows cannot find the software license terms

This issue occurs when the Windows setup copies the driver to the scratch space (X: drive) and the scratch space becomes full. To resolve this issue, do any of the following:

- Remove all the installed add-on devices before starting the OS installation. After the OS installation is complete, connect the add-on devices and manually install the remaining drivers using Dell Update Packages (DUPs).
- To avoid physically removing the hardware, disable the PCIe slots in the BIOS.
- Increase scratch space size beyond 32 MB using `DISM set-scratchspace` command when creating customized deployment. For more details, see Microsoft's documentation.

3. LC displays two or more drive names for some CDs or DVDs, such as the ones containing operating systems.
4. If the operating system (OS) selected for installation and the OS on the media used are different, LC displays a warning message. However, while installing Windows OS, the warning message is displayed only when the bit count (x86 or x64) of the OS does not match. For example, if Windows Server 2008 x64 is selected for installation and Windows Server 2008 x86 media is used, the warning is displayed.
5. LC does not support OS deployment on Dell Precision Workstation R7920.
6. In Windows10, HTML5 plug-in does not support Virtual media connection on the following versions of Edge browsers:
  - a. Microsoft Edge 44.17763.1.0
  - b. Microsoft EdgeHTML 18.17763

## Security

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

## Storage and storage controllers

1. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
2. 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`

## SupportAssist and parts replacement

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

## Firmware and driver update

1. After an iDRAC reset or firmware update operation, the *ServerPoweredOnTime*—a property in RACADM and WSMAN—may not be populated until the host server is restarted.
2. Some of the supported components may not be displayed on the **Firmware Update > View Current Versions** page. To update this list, restart the system.
3. If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.
4. Firmware update is supported only for LAN on Motherboards (LoM), Network Daughter Cards (NDC), and network adapters from Broadcom, QLogic, and Intel, and some of the QLogic and Emulex fiber channel cards. For the list of supported fiber channel cards, see version 3.31.31.31 *Lifecycle Controller User's Guide* available at [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals).
5. After the CPLD firmware is updated on modular systems, the firmware update date is displayed as 2000-01-01 on the View Current Versions page. The update date and time is displayed according to the time zone configured on the server.
6. On some modular systems, after a firmware update, the Lifecycle Log displays the time-stamp as 1999-12-31 instead of the date on which the firmware update was performed.
7. It is not recommended to perform CPLD update along with other updates. If a CPLD update is uploaded and processed along with other updates, CPLD update completes successfully but the other updates do not take effect. Reinitiate the other updates to complete them successfully.

## Miscellaneous

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

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

3. When accessing the iDRAC web interface for the first time using Google Chrome version 59.0, the mouse pointer may not be visible. To display the mouse pointer, refresh the page or use Google Chrome version 61.0 or later.
4. If you use the HTML5 plug-in on Chrome version 61.0 to access Virtual Console, you cannot connect to Virtual Media. To connect to Virtual Media using the HTML5 plug-in, use Chrome version 63 or later.
5. Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
6. A Serial-On-Lan (SOL) session that has been active for more than five days or multiple reboots may get terminated automatically. If the session terminates, you must reinitiate the session.
7. Due to an issue with Safari, if an ipv6 literal address is used to log into the Web GUI, Safari is not able to launch the HTML5 based vConsole. Alternative options are to use Java based vConsole, or HTML5 vConsole by using the corresponding DNS name or by using an alternate browser in Mac OS.
8. iDRAC 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.

# Updating iDRAC firmware

## Downloading iDRAC firmware installation file

**NOTE:** For information about updating iDRAC firmware using various interfaces, see version 3.31.31.31 *iDRAC User's Guide* available at [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals).

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

## Updating iDRAC firmware from host OS

From the host operating system, execute the installation package that you downloaded and follow the instructions of the update wizard. For more information about opening executable files on your system, see the operating system's documentation.

## Updating iDRAC remotely using iDRAC web interface

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

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

After the update is complete, iDRAC restarts automatically.

# Lifecycle Controller Remote Services — client tools

## OpenWSMAN CLI

OpenWSMAN CLI is an open source Linux WSMAN client. You can use OpenWSMAN CLI to send WSMAN commands to Lifecycle Controller.

OpenWSMAN CLI source code and installation details are available at [sourceforge.net/projects/openwsman/files/wsmancli](https://sourceforge.net/projects/openwsman/files/wsmancli).

Sample OpenWSMAN CLI Command for an enumeration operation:

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_SystemView  
-h (idrac ip address) -P 443 -u (idrac user) -p (idrac password) -v -j utf-8  
-y basic -R -o -m 256 -N root/dcim -c cert_name.cer -V
```

 **NOTE:** Lifecycle Controller uses a self-signed certificate for HTTPS (SSL) communication.

Self-signed certificates are not accepted by the OpenWSMAN CLI client and WSMAN commands do not work without these options: -c, -v, and -V. See the OpenWSMAN CLI Readme for details about these options.

## Resources and support

For more information about the features of this release, see the documentation for iDRAC 3.31.31.31.

### Latest Release Notes

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

1. Go to [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals).
2. Click the link for the generation and then click the version of iDRAC.
3. Click **Manuals & documents**.

### Accessing documents using direct links

You can directly access the documents using the following links:

**Table 1. Direct links for documents**


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

### Accessing documents using the product search

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, PowerEdge or iDRAC.  
A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **Manuals & documents**.

### Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. Click **Browse all products**.
3. Click the desired product category, such as Servers, Software, Storage, and so on.
4. Click the desired product and then click the desired version if applicable.  
 **NOTE:** For some products, you may need to navigate through the subcategories.
5. Click **Manuals & documents**.

## Contacting Dell EMC

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

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