iDRAC9 with Lifecycle Controller Version 3.16.16.16

Release Notes

DELLEMC

Notes, cautions, and warnings

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

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

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

Contents

Overview

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 EMC 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.

Topics:

*   Version

Version

iDRAC9 with LC 3.16.16.16

Release Date

December 2017

Previous version

N/A

Importance

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).

2

Platforms affected

- PowerEdge C4140

What is supported

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.

For information on the features available for a license, see the Managing Licenses section in the iDRAC 3.15.15.15 User's Guide available at http://www.dell.com/idracmanuals

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
- WinPE 5.0 64-bit
- WinPE 10

RedHat

- RHEL 7.4
- RHEL 6.9

SLES

- SLES 12 SP3

Ubuntu

- Ubuntu 16.04.03

VMware

- ESXi 6.0 U3
- vSphere 2016 U1

Citrix

- XenServer 7.1 CU1

Supported web browsers

- Microsoft Internet Explorer 10 (Windows 2008 R2 only)
- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari version 8.0.8
- Safari version 9.0.3
- Mozilla Firefox version 52

- Mozilla Firefox version 54
- Google Chrome version 57
- Google Chrome version 58

Java support

- Java - Oracle version

New in this release

Hardware — Server or storage platform specific

- Significant enhancement and optimizations in PCIe adapter card cooling algorithms.
- Further optimized and fine-tuned fan responses to provide additional airflow and power optimizations on most supported platforms.
- Added support for Boot Optimized Storage Solution (BOSS) controllers. You can perform tasks such as inventorying, monitoring, staged configuration, and update of BOSS controllers using iDRAC.

iDRAC and LC firmware

- Asset Tag is restored as part of the Easy Restore operation after a system board replacement.

Monitoring and alerting

- SupportAssist Collections can be uploaded to Dell EMC without registering with SupportAssist.

Security

- Removed TLS 1.0 for Port 5900.
- Added option to enable or disable virtual media using the iDRAC web interface.
- Added option to configure IP blocking using the iDRAC web interface. This feature helps in blocking IPs if incorrect login credentials are used.

Updates

- Improved keyboard pass-through support and added more keystrokes to the exception list.

Fixes

- Fixed issue with OpenIPMI improperly resolving the channel to the I2C bus.

Topics:

Hardware — Server or storage platform specific

- Fixed issues that could result in the fan3 or all the fans running unexpectedly at full speed on some platforms.

Important notes

1. 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

2. The drivers exposed by LC are present in a read-only drive labeled OEMDRV and the drive is active for 18 hours. During this period:

   - You cannot update any DUP.
   - LC cannot involve CSIOR.

   However, if an AC power cycle (cold boot) is performed, the OEMDRV drive is automatically deleted.

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

4. 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.

5. If the network is not configured and you try to perform a network operation in LC, a warning message is displayed. When you navigate to the network settings page from this message, the left navigation panel on network settings page may not be displayed.

6. 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.

7. 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.

8. 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.

9. 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.

10. Rollback is not supported for CPLD.

11. 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 (only in the case of 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.

12. 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). This includes SMART errors such as:

    - Available spare threshold
    - Reliability degraded
    - Read-only mode
    - Virtual memory backup failed, and so on

Limitations

- 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.
- Sometimes, when using WSMan, an Internal SSL Error is reported and the WSMan command fails. If this happens, retry the command.
- Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
- If the LCD display is blank, press any one of the 3 LCD buttons to turn on the LCD before inserting a USB storage device.
- 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.
- 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.
- Some of the supported components may not be displayed on the **Firmware Update** > **View Current Versions** page. To update this list, restart the system.
- 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.
- You may be unable to scroll using the keyboard. Use the mouse to scroll.
- 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**.
- 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**).
- When Virtualization Mode is set to NPAR for Network Adapter 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**.
- 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.
- Deployment of Windows Server operating systems (OS) using LC may fail with one of the following message:
  - Windows installation cannot continue because a required driver could not be installed.
  - Product key required.
  - Windows cannot find the software license terms.

  This happens 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.
- LC supports the following characters for username and password:

Alphabets	a-z, A-Z
Numbers	0-9
Special characters	`- _ .`

- If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.
- 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 3.15.15.15 User's Guide available at **www.dell.com/idracmanuals**.
- 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.
- 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

- While viewing the current hardware inventory, some properties related to devices installed in PowerEdge VRTX system are not displayed.
- LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC GUI.
- The ISCSI offload attribute can be enabled only on two of the four available ports. If a card, which has this attribute enabled on two of its ports, is replaced with another card that has the attribute 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.
- In LC, not all the vendor FC cards are supported for VLAN configuration.
- LC displays two drive names for some CDs or DVDs, such as the ones containing operating systems.
- 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.
- 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 appears 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.
- LC does not support OS deployment on Dell Precision Workstation R7920.
- LC does not support SOCK4 proxy with credentials.
- 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.
- 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.
- The inventory displayed in LC GUI 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.
- 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 Re-purpose and Retire operation is performed.
    - Network is configured with the network cable connected but the network card is replaced later.
- If you set a user with only SHA256 password, for example, through SCP, you cannot delete the user using the GUI. To delete such a user, edit the user explicitly setting a password and then try to delete the user.
- 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`.
- RACADM supports the underscore character (_) for `iDRAC.SerialRedirection.QuitKey` along with the existing symbols shown in the integrated help.
- 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 the iDRAC and then retry the operation after the iDRAC has finished restarting.`
- If iDRAC is in lock-down mode, and you run the `racadm rollback` command followed by the `racadm resetcfg` command, 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.
- 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`.
- 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 GUI (**Maintenance** > **Lifecycle Log**) or by using the RACADM command `racadm lclog view`.
- 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 GUI (**iDRAC Settings** > **Users**) to verify the number of iDRAC local users.
- 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 GUI (**iDRAC Settings** > **Users**) to verify that the user exists.
- 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.

    1. Open Group Manager on one of the member iDRACs.
    2. In the search box, type the controlling system's Service Tag.
    3. Double click the iDRAC that matches the search results and navigate to **iDRAC Settings** > **Diagnostics**.
    4. Select **Reset iDRAC**.

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

- When setting the iDRAC Service Module (ISM) monitoring attributes from the GUI, 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.
- 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 till the new values take effect. Any DHCP settings may take more time (>30 seconds) depending on the network environment.
- If the system ID/Health LED turns from blue to off while running host stress test, press the ID button for one second and then press it again to turn on the LED.
- 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 unrelated error message.
- Due to a limitation of Google Chrome browser, HTML5 vConsole intermittently displays the following error message: **Chrome ran out of memory while trying to display the webpage.**
- If an H730P adapter is installed in slot 9 (internal PERC slot) of PowerEdge T640, iDRAC displays it as H730P Integrated RAID Controller (Embedded).
- 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.
- iDRAC features cannot access CIFS or Samba shares when only SMBv1 protocol is enabled. All iDRAC features work with SMBv2/SMBv3 protocol. For information on enabling SMBv2/SMBv3 protocol, see the documentation for your operating system.
- When accessing the iDRAC web interface for the first time using Google Chrome version 59.0, the mouse pointer may not be visible. Refresh the page to display the mouse pointer or use Google Chrome version 61.0 or later.
- Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
- Part-replacement of BOSS-S1 controller will not be detected by Lifecycle Controller. Follow the controller's user guide after replacement.
- 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.
- After downgrading iDRAC from this version to either version 3.00.00.00 or 3.11.11.11, the jobs created in the job queue are deleted. Recreate the jobs after the downgrade is complete.
- By default, iDRAC uses SMB1 protocol and all iDRAC features that use CIFS share will fail if SMB1 is disallowed on Windows/Samba mounts. To use CIFS shares, enable SMB 1 on the system where the share is located. This, however, may lower your system's security. To retain security and compatibility, it is recommended to upgrade your Samba server to version 4.0 or later, which supports SMB 2.0 protocol.
- 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.

Known Issues — To be fixed in future releases

1. **Description**

   Actual Output Wattage is displayed as 0 in Power Supplies page of iDRAC web interface.

   Resolution

   Actual Output Wattage and Input Line Type are not applicable for PowerEdge FX2 and PowerEdge C6420 platforms.

   Version/Systems affected: PowerEdge FX2 and PowerEdge C6420.

   Dell tracking: 81069

2. **Description**

   RAC Serial and IPMI Serial attributes are displayed on iDRAC GUI of PowerEdge C6420 systems even though they are not applicable for this system.

   Resolution

   N/A

   Version/Systems affected: PowerEdge C6420

   Dell tracking: 81639

3. **Description**

   Incorrect slot names are displayed in LC logs when NVMe Disks are installed in the system.

   Resolution

   When an NVMe disk is replaced in a system that has multiple slots in a bay, PR7 message is displayed with Bay <number>, where the <number> is actually the slot number. For example, in the following message, Slot number is 3 and Bay number is 2:

   ```
   [Date]   PR7   Dell NVMe PCIe SSD Configuration Data(Bay 3:Enclosure Internal 0-2)
   ```

   Version/Systems affected: All systems supported by this release.

   Dell tracking: 79270

4. **Description**

   Although the ProcAts attribute is not supported in BIOS, you may be able to create a configuration job using WSMan. However, the job fails and returns an error message. This attribute is not visible in any of the interfaces or WSMan enumeration.

   Resolution

   Do not use the ProcAts attribute because it is not supported in BIOS.

   Version/Systems affected: All systems supported by this release.

   Dell tracking: 78968

5. **Description**

   The online help of iDRAC web interface does not list the **eSwitch Mode** on the **Overview** > **Network Devices** page.

   Resolution

   The eSwitch Mode field displays the eSwitch mode of the network controller.

   Version/Systems affected: All systems supported by this release.

   Dell tracking: 80729

6. **Description**

   If the system has a direct-attached NVMe SSD configuration, a dummy storage NVMe controller named PCIe SSD in Slot 1 in Bay 1 (PC) is listed in SNMP Walk/Get.

   Resolution

   N/A

Version/Systems affected: All systems supported by this release.

Dell tracking: 80884

7. **Description**

If you access the iDRAC web interface using Safari version older than 10, you cannot download any files from iDRAC.

Resolution

Use Safari version 10 or later, or use any other browser supported by this release.

Version/Systems affected: All systems supported by this release.

Dell tracking: 82456

8. **Description**

In a system with two Power Supply Units (PSU), when AC is removed from one of the PSUs, **Input Line Type/Line Status** shows as **Low Line** on the Power Supplies page (**System** > **Overview**) and Hardware Inventory page (**System** > **Inventory**) of the iDRAC GUI.

Resolution

When **PSU Status/Detailed State** is **Input Lost**, Input Line Type/Line Status is inapplicable.

Version/Systems affected: PowerEdge C4140, R440, R540, R640, R740, R740XD, R940, R7920, T440 and T640.

Dell tracking: 82931

9. **Description**

Success event is logged in Lifecycle log when user tries to update NVDIMM with a firmware that has a corrupted header.

Resolution

N/A

Version/Systems affected: All systems supported by this release.

Dell tracking: 83367

10. **Description**

On a H830 controller, after you use auto-configuration to create more than 64 VDs and then try a reset-config operation, the pending delete action is applied only for the first 64 VDs.

Resolution

N/A

Version/Systems affected: All system supported by this release.

Dell tracking: 82424

11. **Description**

When you perform a power cycle operation on the host after a firmware update, the host may remain in powered-off state.

Resolution

Power on host using any of iDRAC interfaces.

Version/Systems affected: PowerEdge C6420, DCS9650, DCS9670, DCS9690

Dell tracking: 85056

12. **Description**

If you upgrade to this version of iDRAC and then update the SEP backplane firmware to 4.23 on a system that has a SAS expander with an HBA330 controller, then the SEP update may fail.

Resolution

Perform a complete power cycle of the system and then retry the update. You can perform the power cycle either by completely turning off the system and turning it back on, or by using the `racadm serveraction powercycle` command. To avoid the power cycle, update the SEP backplane firmware before updating the iDRAC to this version.

Version/Systems affected: All systems supported by this release.

Dell tracking: 87700

13. **Description**

If you have a network card with some 10G ports or faster and some 1G ports, **Family Driver Version** may not display the correct version or may display **Unavailable**.

Resolution

Use operating system tools or OMSA to view the driver version.

Version/Systems affected: All systems supported by this release.

Dell tracking: 87441

14. **Description**

Using SCP import, you may be unable to configure user attributes when *UserName* attribute is at the end of the import file. The following error message is displayed in LCLog:

```
RAC022: Unable to set values for User Password, IPMILan, IPMISerial or User Admin
Privilege because the UserName is not configured.
```

Resolution

Retry the SCP import operation to configure user attributes. Alternatively, ensure that the *UserName* attribute appears first in **User attributes** list in the import file.

Version/Systems affected: All systems supported by this release.

Dell tracking: 86360

Installation

Installation instructions

- From the Windows host operating system (managed node), run the Dell Update Package for Windows and follow the instructions on the update wizard.
- From the Linux host operating system (managed node), run the Dell Update Package for Linux from the shell prompt. Follow the instructions displayed on the console.
- From the management station, remotely update the firmware using the iDRAC web interface:

  1. Extract the firmware image self-extracting file to the management station.
  2. Open the iDRAC web interface using a supported web browser.
  3. Log in as an administrator.
  4. Go to **Maintenance** > **System Update**. The Manual Update page is displayed.
  5. Select **Local** to upload the firmware image file from the local system (Local is selected by default). Click **Browse**, select the .d9 firmware image file that you extracted (step 1), or the Dell Update Package (DUP) for Windows, and click **Upload**.
  6. Wait for the upload to complete. After the upload is completed, the Update Details section displays the uploaded file and the status.
  7. Select the firmware file and click **Install**. The message `RAC0603: Updating Job Queue` is displayed.
  8. Click **Job Queue**. The Job Queue page is displayed, where you can view the firmware update job status. After the update is completed, iDRAC restarts automatically.

For more information, see the iDRAC 3.15.15.15 User's Guide available at http://www.dell.com/idracmanuals.

Upgrade

N/A

Uninstallation

N/A

Lifecycle Controller Remote Services — client tools

Use the OpenWSMAN CLI client tool to send WS-MAN commands to Lifecycle Controller.

OpenWSMAN CLI

OpenWSMAN CLI is an open source Linux WS-MAN client. OpenWSMAN CLI source code and installation details are available at **http://sourceforge.net/projects/openwsman/files/wsmancli**.

Sample OpenWSMAN CLI Command (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 WS-MAN commands do not work without these options: -c, -v, and -V. See the OpenWSMAN CLI Readme for details on these options.

Accessing documents from Dell Support site

Using direct links

You can directly access the documents using the following links:

Table 1. Direct links for documents

URL	Product
dell.com/idracmanuals	iDRAC and Lifecycle Controller
dell.com/cmcmanuals	Chassis Management Controller (CMC)
dell.com/openmanagemanuals	Enterprise System Management
dell.com/serviceabilitytools	Serviceability Tools
dell.com/OMConnectionsClient	Client System Management
dell.com/OMConnectionsEnterpriseSystemsManagement	OpenManage Connections Enterprise Systems Management

Using the product selector

You can also access documents by selecting your product.

1. Go to **https://www.dell.com/manuals**.
2. In the **Choose from all products** section, click **View products**.
3. Click **Software and Security** and then click the required link.
4. To view the document, click the required product version.

Contacting Dell

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

Dell 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 for sales, technical support, or customer service issues, go to https://www.dell.com/ contactdell.