

Integrated Dell Remote
Access Controller 6 (iDRAC6)
Version 1.8

Release Notes



What's New

- Regular Maintenance
- Enabled iDRAC support for:
 - AMD CPU (Interlagos) for R815 and R715
 - AMD CPU (Valencia) for R415 and R515
 - Bromolow CPUs for R210 II
 - 1600 MHz SDIMM/RDIMM for R415 and R515
 - 1600 MHz UDIMM for R210 II
 - 2 GB DIMM for R815 and R715
- Added RACADM "getLED" command support

Hardware and Software Requirements

This section provides the list of supported systems, supported managed server operating systems, supported Web browsers, and supported BIOS firmware versions.

Supported Systems

iDRAC6 is supported on the following Dell PowerEdge systems:

- DELL PowerEdge R710
- DELL PowerEdge R815
- DELL PowerEdge T410
- DELL PowerEdge R715
- DELL PowerEdge R210
- DELL PowerEdge R510
- DELL PowerEdge T310
- DELL PowerEdge R910
- DELL PowerEdge R310
- DELL PowerEdge R415
- DELL PowerEdge R515
- DELL PowerEdge T610
- DELL PowerEdge R610
- DELL PowerEdge R410
- DELL PowerEdge R810
- DELL PowerEdge T710
- DELL PowerEdge R210 II
- DELL PowerVault DR6000
- DELL PowerVault NX3000
- DELL PowerVault NX3100
- DELL PowerVault NX200
- DELL PowerVault DL2100
- DELL PowerVault NX300
- DELL PowerVault DL2200
- DELL EqualLogic DX6004S
- DELL EqualLogic DX6000
- DELL EqualLogic FS7500
- DELL EqualLogic DX6012S
- DELL EqualLogic DX6000G
- DELL PowerEdge T710

Supported Managed Server Operating Systems

The iDRAC6 is supported on the following operating systems:

- Microsoft Windows Server 2003 family - Windows Server 2003 R2 (Standard, Enterprise, and DataCenter Editions) with SP2 (x86, x86_64) and Windows Server 2003 Compute Cluster Edition
- Microsoft Windows Server 2008 SP2 (Standard, Enterprise, and DataCenter Editions) (x86, x86_64)
- Microsoft Windows Server 2008 EBS x64 SP1 (Standard and Premium Editions)
- Microsoft Windows Server 2008 R2 SP1 (Standard, Enterprise, and DataCenter Editions) (x86_64)
- Microsoft Windows Server 2008 HPC Edition Server R1/R2 SP1
- SUSE Linux Enterprise Server (SLES) 10 SP3 (x86_64)
- SUSE Linux Enterprise Server (SLES) 11 SP1 (x86_64)
- Red Hat Enterprise Linux (RHEL) 6.0 (x86_64) SP1
- Red Hat Enterprise Linux (RHEL) 5.5 (x86, x86_64) SP7
- Hyper-V and Hyper-V R2
- VMware ESX 4.0 Update 3
- VMware ESX 4.1 Update 1
- VMware ESX 5.0

- ESXi 4.0 Update 3 Flash and HDD
- ESXi 4.1 Update 1 Flash and HDD
- XenServer 5.6 HDD
- XenServer 5.6 FP1 HDD

Note:

Use the Dell-customized ESXi 4.0 Update 1 Embedded edition. This image is available at support.dell.com and vmware.com. The remote deployment and local installation of ESXi through Virtual Media is not supported for standard ESXi Embedded version 4.0, as the installation may fail with the error message, "Installation failed as more than one USB device found."

Supported Web Browsers

- Microsoft Internet Explorer 7.0 for Windows Server 2003 SP2, Windows Server 2008 SP2, Windows XP 32-bit SP3, and Windows Vista SP2
- Microsoft Internet Explorer 8.0 for Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2 x64, Windows XP 32-bit SP3, Windows 7, and Windows Vista SP2.
- Internet Explorer 8 requires Java Runtime Environment (JRE) version 1.6.14 or later.
- Microsoft Internet Explorer 8.0 (64-bit) for Windows 7 (x86_64), Windows Vista (x86_64) and Windows Server 2008 R2 (x86_64), Windows Server 2008 SP2 (x86_64), Windows Server 2003 SP2 (x86_64)
- Microsoft Internet Explorer 9.0 for Windows Vista (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows 7 (32-bit) (64-bit) or higher, Windows Server 2008 (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows Server 2008 R2 64-bit
- Mozilla Firefox 3.05 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 x64 R2, Windows Vista SP2, Windows 7 x64
- Mozilla Firefox on SLES 10 x64 SP3, SLES 11 x64 SP1, RHEL 5.5 and RHEL 6.0 x64 Native version.
- Mozilla Firefox 4.0 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Vista SP2, Windows 7

Installation

Prerequisites

The recommended BIOS firmware versions are:

- | | |
|--------------------------|------------|
| • DELL PowerEdge R710 | 6.0.4 |
| • DELL PowerEdge R815 | 1.5.2 (Q2) |
| • DELL PowerEdge T410 | 1.8.1 |
| • DELL PowerEdge R715 | 1.5.2 (Q2) |
| • DELL PowerEdge R210 | 1.8.1 |
| • DELL PowerEdge R510 | 1.8.1 |
| • DELL PowerEdge T310 | 1.8.1 |
| • DELL PowerEdge R910 | 2.4.1 |
| • DELL PowerEdge R310 | 1.8.1 |
| • DELL PowerEdge R415 | 1.8.1 |
| • DELL PowerEdge R515 | 1.2.5 |
| • DELL PowerEdge T610 | 6.0.4 |
| • DELL PowerEdge R610 | 6.0.4 |
| • DELL PowerEdge R410 | 1.8.1 |
| • DELL PowerEdge R810 | 2.4.1 |
| • DELL PowerEdge T710 | 6.0.4 |
| • DELL PowerEdge R210 II | 1.2.2 |
| • DELL PowerVault DR6000 | 6.0.7 |
| • DELL PowerVault NX3000 | 6.0.7 |
| • DELL PowerVault NX3100 | 1.8.2 |
| • DELL PowerVault NX200 | 1.8.2 |
| • DELL PowerVault DL2100 | 6.0.7 |
| • DELL PowerVault NX300 | 1.8.2 |

- DELL PowerVault DL2200 1.8.2
- DELL EqualLogic DX6004S
- DELL EqualLogic DX6000
- DELL EqualLogic FS7500
- DELL EqualLogic DX6012S
- DELL EqualLogic DX6000G

Installation and Configuration Notes

For information about iDRAC6, including installation and configuration information, see the "Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise Version 1.70 User Guide" and the "Dell OpenManage Server Administrator User's Guide." These documents are located on the Dell Support website at "support.dell.com/manuals." On the "Manuals" page, click "Software" > "Systems Management". Click on the appropriate product link on the right-side to access the documents.

Upgrade

Upgrading from iDRAC versions 1.50 or 1.70 to 1.80.

Uninstallation

- Use the rollback feature to uninstall iDRAC6 1.80.
- For systems purchased with new eMMC cards and iDRAC6 1.80 firmware version, firmware downgrades are not allowed to lower version.
- On certain hardware configurations, based on the firmware release, firmware downgrades are not allowed.

Open Issues, Resolutions, and Limitations

- Sometimes the "Save As" and "Clear Log" buttons on the "Remote Access" > "Logs" > "iDRAC Log" page may disappear when you hover the mouse near these buttons. This is a known limitation with the GUI.

Resolution: To resolve this, click "Refresh".

- On some Windows operating systems, under certain conditions, executing vmcli.exe fails. This is due to the run-time components of Visual C++ Libraries (VC++ 2008 redistributable package) required to run applications that are not available.

Resolution: To resolve this, download and install Microsoft Visual C++ 2008 Redistributable Package (x86) from the following location:
microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en.

- The iDRAC6 Web interface may Log out when you try to upload any files other than the original SSL certificate files in the "Upload Certificate" page.

Resolution: Login to the Web interface again and upload the correct SSL certificate.

- If you add more than 800 work notes, the GUI page may take additional time to load the page. This is due to huge amount of data that needs to be transacted between the GUI and iDRAC6. The new work notes may not be displayed after the page is loaded.

Resolution: To resolve this click "Refresh".

- After adding or removing new hardware, system inventory page may not update the changes automatically. This is because inventory data collected during manufacturing process may not be updated with new changes.

Resolution: Select "Ctrl+E" during BIOS POST and enable "Collect System Inventory on reboot". Save and exit from "Ctrl+E" option, then reboot the system to collect the new system inventory. After the Inventory is collected, the "System Inventory" page in the iDRAC6 Web interface displays the correct Hardware and software inventory data.

- Virtual MAC under "System Details" page is not populated if system inventory was not run from iDRAC Web interface before entering system details page. This is because the inventory data may not be available for Virtual MAC to display.

Resolution: Click "System Inventory" on the iDRAC GUI homepage. Ensure that inventory data is displayed on the inventory page. After the data is loaded, click on the "System Details" tab for Virtual MAC to display the inventory data, if the system supports this feature.

- While accessing iDRAC6 Web-interface through IPv6 network using Mozilla Fire Fox 4.0 or later, accepting CSR certificate throws as error message "An error has occurred during a connection to <server certificate info>, Peer certificate issuer has been marked as not trusted by the user. (Error code: sec_error_untrusted_issuer)."

Resolution: Create a certificate request and issue to trusted domain. Register it to domain DNS server. Use trusted domain name, instead of the IPv6 address.

- The RACADM Command Line Reference Guide for iDRAC6 1.7, iDRAC6 3.2, and CMC 3.2 defines RACADM command "arp" displays interface as "Device". However, for Rack and Tower servers, the interface is displayed as "iFace".
- iDRAC browse a page that uses JavaScript functions to retrieve page data, the progress bar in Internet Explorer may not always be accurate.
- The iDRAC6 1.70 User Guide mentions that disabling Smart Card Logon sets the CLI out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM to their default state. This should be read as "On disabling Smart Card Logon, CLI out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM retain their state".
- To successfully launch Virtual Media, ensure that you have installed a 64-bit JRE version on a 64-bit operating system with 64-bit browser or a 32-bit JRE version on a 32-bit operating system with 32-bit browser. iDRAC6 does not support 64-bit ActiveX versions. Also, ensure that for Linux, the "compat-libstdc++-33-3.2.3-61" related package is installed for launching Virtual Media. On Windows, the package may be included in the .NET framework package.
- The RACADM Command Line Reference Guide for iDRAC6 1.7, iDRAC6 3.2, and CMC 3.2 defines, RACADM command "racdump" displays Trace log information gettracelog, RAC event log getraclog, System event log getsel. There is a separate command available to display Trace logs, RAC logs, and SEL logs.
- You must disable the Internet Explorer "Enhanced Security Mode" for the Java-based virtual console and virtual media plug-in to function properly. Else, specify the ActiveX plug-in in the iDRAC6 configuration instead of Java. In addition, you must add the iDRAC6 web URL to the Intranet security zone only. Also, this zone settings must be "Medium-Low" or lesser, for the control to function properly.
- Integrated Dell Remote Access Controller 6 (iDRAC6) Version 1.7 User Guide specifies "iDRAC Settings" instead of "Remote Access" in the navigation paths mentioned in the procedural steps.
- The expiry date of the iDRAC default certificate is changed to 2023. To get this updated certificate, clear the "Preserve Configuration" option while updating iDRAC6 firmware using the Web interface. Make sure to delete the cache from the Web interface (Internet Explorer and Firefox).

While using the Firefox Web browser, an error may be seen if the certificate contains the same serial number as another certificate. Use the following link or procedure to resolve the same. (support.mozilla.com/en-US/kb/Certificate%20contains%20the%20same%20serial%20number%20as%20another%20certificate)

Resolution: Delete your old exception and use temporary exceptions for subsequent visits to the iDRAC page.

To delete your old exception:

1. On the Firefox window, click "Firefox", and then click "Options."
For Windows XP, click Tools and then "Options."
For Linux OS, click "Edit" and then "Preferences."
The "Options" window is displayed.
2. Click "Advanced", and then click on the "Encryption" tab.
3. Click "View Certificates". The "Certificate Manager" window is displayed.
4. Click on the "Servers" tab.
5. Identify the item that corresponds to the site that generates the error.
Note: For the Certificate Authority (CA) for that server, the CA name appears above the site name.
6. Click on the server certificate that corresponds to the site that generates the error, click "Delete", and then click OK. The exception is deleted.
7. Click on the "Authorities" tab and select the item that corresponds to the CA that you noted earlier, click "Delete", and then click OK. The exception is deleted.

To add a temporary exception to allow access to the page:

1. When you access the iDRAC Web interface, an Untrusted error message appears.
2. Click "I Understand the Risks".
3. Click "Add Exception...". The "Add Security Exception" window is displayed.
4. Click "Get Certificate". The "Certificate Status" section displays.
5. Select the "Permanently store this exception" option.
6. Click "Confirm Security Exception". The "Add Security Exception" window closes and the iDRAC Web interface page is displayed.

- Using WSMAN and running up to 256 jobs through the job schedules may lead to reduced iDRAC performance.
- Collect System Inventory on Restart (CSIOR) feature enables auto-refresh of firmware and hardware inventory during system startup. By default, CSIOR is enabled in a system. Before using features such as part replacement or setting attributes, ensure that CSIOR is enabled.
- If any iSCSI attributes are set on partition 1 on Qlogic, IscsiOffloadMode on partition 3 remains pending with the same current value. However, CreateTargetedConfigJob or DeletePendingConfiguration on partition 3 will not work unless an explicit SetAttribute command is invoked on partition 3. Similar behavior applies to FCoE attributes on partition 1 and FCoEOffloadMode on partition 4.

Resolution: To commit or delete pending on IscsiOffloadMode on partition 3 or FCoEOffloadMode on partition 4, invoke the SetAttribute method on the partitions. This allows CreateTargetedConfigJob or DeletePendingConfiguration to work.

- Import System Profile Operation Behavior: All the attributes that you can enumerate or set through device profiles (RAID, Simple NIC, BIOS, LC Management, iDRAC Card) are part of the Import System Profile operation. The attributes that you cannot enumerate through these profiles are excluded. Settings that are not covered by these profiles but may be settable through other interfaces are also excluded.
Note: For the WSMAN interface, the RestoreImage() method in the Lifecycle Controller (LC) Management profile accomplishes the Import System Profile behavior.

Global Support

For information on technical support, visit www.dell.com/contactus.

For information on documentation support, visit support.dell.com/manuals. On the **Manuals** page, click **Software** -> **Systems Management**. Click on the specific product on the right-side to access the documents.

Information in this document is subject to change without notice.

© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™, and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, and Celeron® are registered trademarks and Core™ is a trademark of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® , and XenMotion® are registered trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.