

**DELL UPDATE
PACKAGES FOR
MICROSOFT
WINDOWS Version
7.4**

Release Notes



Release Type and Definition

This Readme contains updated information for your "Dell Update Packages for Microsoft Windows Operating Systems User's Guide" and any other technical documentation included with the Dell Update Packages for Windows operating systems.

Version

7.4

Release Date:

December 2013

Previous Version

7.3

Importance

Dell Update Packages offer ease and flexibility for updating the system software on Dell PowerEdge systems. Update Packages are available for the following software components:

- System BIOS
- System firmware, also known as the Embedded Systems Management (ESM) firmware
- Dell Remote Access Controller (DRAC)/Integrated Dell Remote Access Controller(IDRAC) firmware, which also includes Embedded Remote Access (ERA) firmware
- Integrated Dell Remote Access Controller(IDRAC) firmware
- PowerEdge Expandable RAID Controller (PERC) firmware and driver
- Cost-Effective RAID Controller (CERC) firmware and driver
- Software RAID Controller firmware and driver
- SEP firmware
- IDE Controller drivers
- Baseboard Management Controller (BMC) firmware
- SCSI Backplane (BP) firmware
- SAS BP firmware
- SAS Expander firmware
- SSD firmware
- SED firmware
- OpenManage Server Administrator updates
- Onboard Video Drivers
- SAS HDD Firmware
- SAS Controller firmware
- PowerVault 100T firmware
- PowerVault 110T firmware
- PowerVault MD1120 firmware
- PowerVault MD1200 firmware
- PowerVault RD1000 firmware
- Broadcom Network Adapter driver
- Intel Network Adapter driver
- QLogic Network Adapter driver
- Emulex Network Adapter driver
- Power Supply firmware
- Broadcom Network Adapter Firmware
- Intel Network Adapter Firmware

- QLogic Network Adapter Firmware
- Emulex Network Adapter Firmware
- Mellanox Network Adapter Firmware
- iSM

CONTENTS

- CRITICALITY
- MINIMUM REQUIREMENTS
- UPDATE PACKAGES: SUPPORTED COMPONENTS
- KNOWN ISSUES

CRITICALITY

2 – Recommended

It is recommended that you apply this update during your next scheduled update cycle. The update contains feature enhancements or changes that will keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

MINIMUM REQUIREMENTS

The Update Packages support Dell systems running the following Windows operating systems:

- Microsoft Hyper-V Server 2012 R2
- Microsoft Windows Server 2012 R2 x86 Editions
- Microsoft Windows Server 2012 Standard, Enterprise, Datacenter and Foundation x64 Editions
- Microsoft Windows Server 2008 SP2 Standard, Enterprise, and Datacenter x86 Editions
- Microsoft Windows Server 2008 SP2 Standard, Enterprise, and Datacenter x64 Editions
- Microsoft Windows Server 2008 R2 Standard, Enterprise, and Datacenter x64 Editions with SP1
- Microsoft Windows Server 2008 R2 SP1 HPC Edition
- Microsoft Windows Server 2008 R2 Standard, Enterprise, and Datacenter x64 Editions with SP2
- Microsoft Windows Server 2008 Core Standard, Enterprise, and Datacenter Editions (x64) with SP2
- Microsoft Windows Essential Business Server 2008 Standard and Premium Editions (x64) with SP1
- Microsoft Windows Small Business Server 2011 Standard and Premium Editions
- Microsoft Windows Storage Server 2008 R2 Express, Workgroup, Standard, and Enterprise Editions
- Microsoft Windows Small Business Server 2011 Essentials
- Microsoft Windows Storage Server 2008 Basic, Workgroup, Standard, and Enterprise Editions
- Microsoft Hyper-V R2 and Windows Server 2008 with Hyper-V role R2

NOTE: For the latest information about the various Dell systems and operating systems that Dell Update Packages are supported on, see the "Dell Systems Software Support Matrix" on the Dell Support website at ["dell.com/support/manuals"](http://dell.com/support/manuals).

NOTE: Update Packages may also be applied in a pre-operating system environment that uses the Embedded Linux (ELI) through the Dell OpenManage Deployment Toolkit (DTK).

UPDATE PACKAGES: SUPPORTED COMPONENTS

Update Packages currently do not support every system component type.

Dell will continue to make Update Packages available on additional devices in future releases.

This release of Update Packages supports updates to the devices listed in the following table.

Component Type	Supported Components
BIOS	BIOS
DRAC firmware	DRAC 5, iDRAC6, iDRAC7
BMC firmware	BMC
SCSI BP firmware	BP
SAS BP, SEP firmware	BP
Storage enclosure	PowerVault MD1000, PowerVault MD1120, PowerVault MD1200, PowerVault MD1220, PowerVault MD3000
RAID Firmware and drivers	PERC H200, PERC S300 Adapter, PERC 5/E, PERC 5/i, SAS 5/i, SAS 5/iR Adapter, SAS 5/E, SAS 5/iR, SAS 6/iR, SAS 6/iR Adapter, PERC 6/E, PERC 6/i, PERC 6/i Adapter, CERC6/i PERC H310 Adapter, PERC H310 Mini Blade, PERC H710P Mini Blade, PERC H810 Adapter, PERC H710P Adapter, PERC H710 Mini Monolithic, PERC H310 Mini Monolithic, PERC H710 Adapter H710P Mini Monolithic, PERC H710 Mini Blade PERC H700 Adapter, PERC H700 Modular, PERC H800 Adapter, PERC H700 Integrated
Tape drives firmware	PowerVault 100T DDS4, PowerVault 110T DAT72, PowerVault 110T LTO1, PowerVault 110T LTO2, PowerVault 110T LTO2-L, PowerVault 110T LTO3, PowerVault 110T LTO3-HH, PowerVault 110T LTO4, PowerVault 110T SDLT320, PowerVault 110T DLT VS80, PowerVault 110T DLT VS160, PowerVault 110T SDLT
Removable disk drive	PowerVault RD1000 backup firmware
Network adapter driver	Broadcom NetXtreme family of adapters Broadcom NetXtreme II family of adapters Intel PRO PCI-E Gigabit family of adapters QLogic Network family of adapters Emulex Network family of adapters Mellanox Network Adapter Mellanox ConnectX-3 Dual Port 10 GbE DA/SFP + Ethernet

Adapter.

Network adapter firmware	Broadcom NetXtreme family of adapters Broadcom NetXtreme II family of adapters Intel PRO PCI-E Gigabit family of adapters QLogic Network family of adapters Emulex Network family of adapters Mellanox Network Adapter Firmware Mellanox ConnectX-3 Dual Port 10 GbE DA/SFP + Ethernet Adapter.
--------------------------	---

KNOWN ISSUES

For all Dell Update Packages

- On a Hyper-V virtual machine setup, while updating the Host OS components, ensure that the Guest OS's is not running.
- On systems with a FAT32 partition as the boot drive, you cannot execute DUPs and the inventory collector used by SUU as FAT32 does not support access control lists.
- Do not run other applications while executing Dell Update Packages.
- For firmware Dell Update Packages, an update package will not inventory the device if only a native non-Dell driver is installed. Thus the firmware update packages will not upgrade a device with a native driver.
- For driver Dell Update Packages, an update package can inventory the device, but will not upgrade the driver if the native driver is at a higher version than the Dell driver being installed.
- On some servers running Windows 2000 Server, the digital signature information of signed Dell Update Packages displays the message "The certificate is not valid for requested usage."

Root Cause:

The message is caused by an out-of-date root certificate on the server.

Solution:

To update the root certificate:

- i. Enable Windows Update.
- ii. Go to "www.update.microsoft.com".
- iii. Select "Custom" to perform a scan of your machine for updates.
After the scan completes, it will list all available updates.
Select the "Software, Optional" category.
- iv. Look for "Root Certificates Update", and select it. Your root certificates will be updated.
- v. After your root certificates are updated, check the digital signature information of your Dell Update Packages again. The information should now indicate that the digital signature is valid.

See the following Website for reference:

"<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/rootcertprog.asp>"

- If you encounter the message, "This Update Package is not compatible with any of the devices detected on your system", for a supported device, ensure that you have the latest Dell drivers for your system from the Dell Support website at "www.support.dell.com."
- If you are using Windows BitLocker on Windows Server 2008, wait for BitLocker to finish encrypting the drive before executing Dell Update Packages.
- The DUP update process involves several resets to the USB bus which cause all USB devices to be enumerated again by the Operating System. If you insert the USB device for the first time and if you are prompted with the "Scan and Fix" process, select it to avoid multiple "Scan and Fix" messages each time the USB bus reset happens.

- Dell Update Packages do not require new refreshes of existing DUPs to be reinstalled since the firmware or driver payload does not change when the DUP is refreshed. A new DUP is available if changes have been made to the firmware or driver payload.
- If you login to a system running on Microsoft Windows Small Business Server 2008 operating system, by default you are logged in as a regular user even though you may have Administrator privileges. This is due to an in-built feature called User Account Control (UAC) that automatically reduces the potential of security breaches. Before you run DUPs on your system, elevate the privileges for administrators using Windows security options in Group Policy Editor. For more information, see the DUPs User Guide.
- Sometimes a pop up with dialog message saying "You need to format the disk in Drive A: before you can use it" if any USB Device is attached through iDRAC virtual media. If you get this pop up message then ignore it during DUP execution and close the pop up by clicking close button after DUP execution is completed (BITS041566).
"The Update Package is running on an unsupported new operating system, do you want to continue?" message will pop-up in Microsoft Windows Server 2012 operating system, because all DUPs are not recreated based on new DUP framework.
Note: Ensure that a drive is available for DUPs to mount a partition to complete an update successfully.

Power Supply Unit (PSU) Dell Update Packages (DUPs)

After a Successful Power Supply firmware update, the system turns off, for up to 5 to 10 minutes, and reboots automatically. If you perform a cold boot (AC Power cycle) during the firmware update, the system does not boot.

Unified Server Configurator (USC) Dell Update Packages (DUPs)

- Lifecycle controller updates require system services to be enabled.
- For the first time, before you attempt to run Driver Package Diagnostics DUPs, execute the USC DUP.
- If the operating system is installed from "Operating System Deployment", select "Reboot and Exit" in the USC environment before booting to the operating system. This closes the USC session which is held for 18 hours. If you do not want to enter the USC and select "Reboot and Exit", but want to execute the DUPs within 18 hours, unplug the power supply of the system, wait for 10 seconds, and then power on the system.

12 G BIOS

- BIOS updates require system services/Lifecycle controller to be enabled.
- If the operating system is installed from "Operating System Deployment", select "Reboot and Exit" in the USC environment before booting to the operating system. This closes the USC session which is held for 18 hours. If you do not want to enter the USC and select "Reboot and Exit", but want to execute the DUPs within 18 hours, unplug the power supply of the system, wait for 10 seconds, and then power on the system.
- BIOS DUP will use LC to update BIOS. BIOS DUP will stage the BIOS firmware to maser partition and create a SSIB update task, which is executed by the SSM manager on reboot. The update task in the SSIB is a call to update wrapper in LC which has BIOS update logic.

BIOS

- A BIOS update requires enough free physical memory to load the entire BIOS image into the physical memory. If there is insufficient free physical memory available on the system to load the BIOS image, the Dell Update Package for BIOS may fail. In this instance, the BIOS can be updated using the Diskette method, by running the Dell Update Package after adding more memory, or by running the Dell Update Package immediately after a reboot.
- BIOS update is not supported on PowerEdge R210 with BIOS version 1.0.33, 1.2.1, or 1.1.4 installed. BIOS versions earlier than 1.3.4 do not support the online update method used by the DUP process on the PowerEdge R210 under Window Server 2008R2. To update BIOS from one of the versions listed, use the offline BIOS update. Once version 1.3.4 of BIOS is installed, all future BIOS will be supported.

- BIOS update is not supported on PowerEdge T310 with BIOS version 1.0.2, 1.1.6, or 1.2.1 installed. BIOS versions earlier than 1.3.6 do not support the online update method used by the DUP process on the PowerEdge T310 under Window Server 2008R2. To update BIOS from one of the versions listed, use the offline BIOS update. Once version 1.3.6 of BIOS is installed, all future BIOS will be supported.
- BIOS update is not supported on PowerEdge R310 with BIOS version 1.0.0 installed. BIOS versions earlier than 1.1.5 do not support the online update method used by the DUP process on the PowerEdge R310 under Window Server 2008R2. To update BIOS from one of the versions listed, use the offline BIOS update. Once version 1.1.5 of BIOS is installed, all future BIOS will be supported.

Dell Embedded Open Manage Server Administrator

The Dell Update Package for Dell Embedded Open Manage Server Administrator can only be applied in a pre-operating system environment that uses the Embedded Linux (ELI) through the Dell OpenManage Deployment Toolkit (DTK).

BMC firmware and BP firmware

When upgrading the BMC/ESM firmware or the BP firmware on PowerEdge 8G or 9G servers with the Windows Server 2003 R2 IPMI driver installed, the update may take up to 20 minutes to complete. To expedite such updates on PowerEdge 8G or 9G servers, you can uninstall the R2 IPMI driver before performing the firmware upgrade operation using the command "rundll32 ipmissetp.dll, RemoveTheDevice" from a command prompt. After the firmware flash is complete, you can install the driver again by executing the command "rundll32 ipmissetp.dll, AddTheDevice". On PowerEdge 9G servers, the driver can be re-installed by performing a "Scan for hardware changes" in the Device Manager.

11G iDRAC

When upgrading the iDRAC firmware for the first time on a server with Windows operating system, the following message might be displayed: "Windows has finished installing new devices.

The software that supports your device requires that you restart your computer. You must restart your computer before the new settings will take effect. Do you want to restart your computer now?" Select "No" to ignore this message. This message is due to the creation of a temporary USB device used for storing the firmware image. If you select "Yes", the firmware update process stops.

DRAC 5 firmware

Before updating the DRAC firmware, ensure that the following conditions are met:

- USB is enabled
- IPMI is working properly
- DRAC Virtual Flash is not in use by the operating system or another application
- WMI service is running

Power Supply Unit firmware

Power Supply Unit firmware updates can be performed only on Life Cycle Controller enabled systems.

All PERC firmware and all SAS firmware (All storage controller firmware)

- Only devices connected to a PERC SAS controller can be updated at this time. This includes PERC5, PERC6, H200, H310, H710P, H810, H710, H700, H800, SAS5 and SAS6 controllers.
- Do not run storage controller update packages if the controller is in use by other applications. The firmware upgrade may fail if any of the RAID controllers in the system are performing an I/O background task (consistency check, background initialization, rebuild, or reconstruction). Allow the background task to complete before attempting to upgrade the firmware. "Patrol Read" tasks will not affect a firmware upgrade.

PowerVault MD1000 firmware

The PowerVault update procedure requires the RAID controller to be in a known good state. If a problem occurs with the RAID controller during the update procedure, the Update Packages cannot communicate with the PowerVault system, inventory its firmware version, or perform the update. (138462)

PowerVault MD1000 firmware

- Stop all input/output to the PowerVault MD1000 before running the PowerVault MD1000 firmware update package.

WARNING: THE SERVER MUST BE REBOOTED AFTER UPDATING THE FIRMWARE ON MD1000 ENCLOSURES IN ORDER TO MAINTAIN ENCLOSURE MANAGEMENT. ACCESS TO THE ENCLOSURES WILL BE LOST IF THE SERVER IS NOT REBOOTED.

- When prompted for reboot after the update, select "Yes".

PowerVault 100T DDS4 firmware and all PowerVault 110T firmware (110T DDS4, 110T DAT72, 110T LTO1, 110T LTO2, 110T LTO2-L, 110T LTO3-HH, 110T LTO4, 110T SDLT320, 110T LTO3, 110T DLT VS80, 110T DLT VS160, and 110T SDLT)

- Before executing the firmware update, stop all tape backup activity and put all scheduled jobs on hold.
- After the firmware update is completed, restart your system for the updates to take effect.
Note: Tape automation devices are not supported by Dell Update Packages. Please disconnect or power off such devices before executing Dell Update Packages.

The tape automation devices are as follows:

1. PowerVault 120T
2. PowerVault 122T
3. PowerVault 124T
4. PowerVault 128T
5. PowerVault 130T
6. PowerVault 132T
7. PowerVault 136T
8. PowerVault 160T
9. PowerVault ML6000