Dell™ Update Packages for Microsoft® Windows® Operating Systems

User's Guide

Notes and Cautions

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

△ **CAUTION:** A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Information in this document is subject to change without notice.

April 2009

Contents

1

Getting Started With Dell Update Packages

Overview

Dell™ Update Packages (DUPs) allow administrators to update a wide range of system components simultaneously and apply scripts to similar sets of Dell systems to bring system software components up to the same version levels.

By using DUPs, you can perform the following functions:

- Apply an individual update to a system by using an intuitive graphical user interface (GUI)
- Install device drivers in interactive and non-interactive modes
- Batch a number of updates for your system by using the command line interface (CLI) feature
- Leverage your company's software distribution tools to remotely apply updates to any number of servers

A DUP (Dell Update Package) is a self-contained executable in a standard package format and each Update Package is designed to update a single software component on your system. This product feature allows you to select and apply just the updates that you want for your system, thus minimizing the resources required to transport the Update Packages across your network.

DUPs improve your ability to update your systems effectively. For example, each DUP contains pertinent information about when Dell issued the package, which systems the package is designed to support, and what functional enhancements are contained in the update or which problems were fixed.

Many devices rely on more than one driver or application to operate correctly. For example, network interface cards (NICs) have base drivers, teaming drivers and teaming applications, while certain storage controllers have base drivers and miniport drivers. Updating only the base driver of a teaming-enabled NIC may break the teaming functionality.

Likewise, updating only the miniport driver of a storage controller may also create problems. The Update Packages will now support installation of a single driver for a device as well as multiple drivers, in a single package.

Each DUP contains the execution logic to verify that the update will work on your system. By using DUPs, you are not required to use any Dell OpenManage software applications, you do not need to create alternative media, and you do not have to reboot your system to MS–DOS® to apply the updates. Each DUP also carries a digital signature to ensure reliable and trusted authentication. See "Verifying the Digital Signature" for more information.

Administrators can apply DUPs on the Windows operating system by running the packages in the stand-alone mode. In this mode, the packages present an interactive GUI that provides administrators with certain choices, such as whether to reboot if the update requires a system reboot before taking effect. The GUI that is available through DUPs running in stand-alone mode presents dialog boxes to notify administrators of errors that may occur if the DUPs cannot be applied to the system or if the prerequisites are not met. The GUI also lists the purpose of the package, the devices it updates, the BIOS, driver, or firmware version to which it updates, supported operating systems, supported Dell platforms, and prerequisites (if any). DUP has a welcome display which lists information about the new features and any known issues with the package.

You can use DUPs interactively, which is ideal for applying a limited number of updates. You can also use DUPs in batch mode to accommodate large environments with multiple systems or to process multiple updates per system. In addition, you can use remote scripting with systems management software solutions.

This guide is designed to familiarize you with DUPs so that you can begin applying them to simplify the system software maintenance on your Dell systems. The "Using Dell Update Packages" section of this guide provides sample scenarios for using Update Packages.

Server Update Utility and DUPs

Dell OpenManage Server Update Utility (SUU) is a DVD–based application that is used to identify and apply the latest updates to your system. It is both a Graphical User Interface (GUI) and a Command Line Interface (CLI) based application. SUU compares the versions of components currently installed on your system with the update components packaged on the *Dell Server Updates* DVD and then displays a comparison report of the versions and provides the option of updating the components. You can use SUU to update your system or view the updates available for any system listed in the repository. The *Dell Server Updates* DVD is available as part of the Dell OpenManage subscription service kit. You can download SUU from the Dell Support website at **support.dell.com**.

Windows DUPs can be downloaded from the Dell Support website at **support.dell.com**. They are also available in the repository on the *Dell Server Updates* DVD. The **repository** folder in the *Dell Server Updates* DVD contains Windows and Linux DUPs, **Catalog.xml** (that contains information about both Windows and Linux DUPs), and the **DellSoftwareBundleReport.html**. SUU uses DUPs to update the system components.

NOTE: See the *Server Update Utility User's Guide* available on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Tools and Documentation* DVD for information on how SUU identifies and applies updates to your entire system.

Update Options

You can update your system components using any one of the two options listed below:

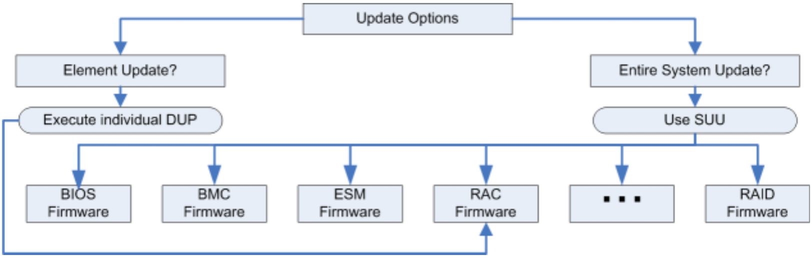
Element Update–To update an *individual* system software component (element) to a specific version. Use DUP to perform element updates.

System Update–To update all elements on your system. Dell recommends that you use SUU to automatically:

- inventory the Dell firmware and drivers on that system
- compare the installed configuration with the content on the *Dell Server Updates* DVD
- report on discrepancies and recommend updates, including any prerequisites that may impact the update sequence
- update and (if needed) reboot the system

Figure 1-1 helps you choose between SUU and DUPs when performing updates:

Figure 1-1. Choosing Between SUU and DUPs



Supported Operating Systems

For a complete list of supported systems and operating systems, see the *Dell Systems Software Support Matrix* located on the *Dell Systems Management Tools and Documentation* DVD or on the Dell Support website at **support.dell.com**. The *Dell Systems Software Support Matrix* has information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage™ components that can be installed on these systems.

Before You Begin

DUPs are available for applying updates to your system software components.

The following prerequisites apply for installing and using DUPs:

- DUPs support Dell systems running the operating systems listed in the "Overview" section.
- You must be able to log on to the system with an account that has Administrator privileges.

How to Obtain DUPs from the Dell Support Website

1. Log on to **support.dell.com**.
2. Select **Drivers and Downloads**.
3. Enter your service tag or choose your product model.

4 Select your product family and product line.

5 Select your operating system, language, category, and the update importance. A list of applicable updates are displayed.

6 Click **Download Now**.

7 You can also download a different file format from the column labeled **File Title**. Select a file format for your DUP and single-click its filename. If you want to download more than one file type, you must do so one at a time.

8 To complete the download of your file, follow the directions on the screen.

Before installing DUPs, read the information provided, both online and in the download package. Ensure that the updates you selected are both necessary and appropriate for your system. You may also need to complete some or all of the following steps:

1 Run the DUP **Check** option on the target system to ensure that the system meets the prerequisites for performing an update.

   To run the check from the CLI, type the following command at the command line prompt:

   ```
   packagename.exe /c /s
   ```

   To run the check from the GUI, perform the following steps:

   a Double-click the **.exe** file for the DUP you downloaded.

   b Read the information about the update in the GUI's scrolling text window.

   You can view the log results after running the check option from either the CLI or the GUI. The default path for the log file is **C:\dell\updatepackage\log**.

2 Determine that the target system meets compatibility requirements. See the *Dell OpenManage Server Administrator Compatibility Guide* and the *Dell Systems Software Support Matrix* for additional information. See "Other Documents You Might Need" for the location of the *Dell OpenManage Server Administrator Compatibility Guide* and the *Dell Systems Software Support Matrix*.

3 Create a directory structure for performing the updates (for example, create a directory for each system type).

4 Determine a methodology for performing the updates.

- Single update method: Run DUPs from the GUI in the interactive mode to perform the update.
- Script method: Use this method if you have a requirement for running one or more updates from a script on a single system.

  See the sample scripts in "Command Line Interface Reference."

NOTE: DUPs for Windows can also be found in the repository on the *Dell Server Updates* DVD that contains the updated BIOS, drivers and firmware components for Dell systems.

Installation Order of DUPs

If you are installing multiple Update Packages, install the updates that require a reboot last. Dell recommends the installation order as described in Table 1-1.

Table 1-1. Update Packages: Recommended Installation Order

Installation Order	System Software Components
1	Device drivers
2	Device firmware
3	ESM firmware
4	BIOS

NOTE: If you are installing both ESM and BIOS updates, install the ESM firmware update before the BIOS update.

NOTE: If you are planning to install Server Administrator as well as a BIOS update, install Server Administrator before the BIOS update. If you have updated the BIOS already and you are planning to install Server Administrator, reboot your system so that the changes to the BIOS will take effect.

Important Tips to Remember for Using DUPs

- Prepare repair disks before you perform any updates.
- Download the currently installed version of drivers, BIOS, and firmware so that you have a backup plan in case any issues arise.
- When you are upgrading any RAID controller software drivers, the enhanced Storage Management Service may need to be upgraded. Check the *Dell OpenManage Server Administrator Compatibility Guide* before proceeding. See "Other Documents You Might Need" for more information.
- Ensure that you have a backup of the Windows operating system registry files or system configuration files stored on a system other than the ones you are updating.
- The updates must be planned for and performed by the system administrator who knows which applications could be affected.
- Before updating all systems, perform the upgrade on one nonessential system to test the update.
- Do not run other applications while executing DUPs.
- Do not shut down the system while an update is in progress.
- Ensure that the system reboots without power interruption after performing a BIOS update.
- You cannot run a DUP in interactive mode from a Telnet session.

Fresh Install of Device Drivers

DUPs update BIOS, firmware, drivers, and applications. If a device driver is not already present in your system, DUPs allows you to do a fresh install of the driver. The driver is installed if the hardware that the driver supports is present.

Interactive Mode

In interactive mode, if a fresh install is applicable, DUP displays a message to install the driver along with the version of the package. Click `Yes` to install the package. Installation results are logged in the "DUP Message Logs".

Non–Interactive Mode

When a fresh install is applicable, executing DUPs with the /s switch installs the driver.

For example, `packagename.exe /s` and `packagename.exe /s /r` does a fresh install of driver DUPs. See "CLI Options" for more information on the command syntax.

NOTE: Not all driver DUPs support fresh install. See the *Dell Update Packages for Microsoft Windows operating systems* readme file for the list of drivers that do not support fresh install.

User Account Control In Windows Server 2008

User Account Control (UAC) is a new security feature in the Windows Server 2008 operating system. When enabled, it restricts access to critical system resources for all users except the built-in local Administrator. With UAC, users have to upgrade to an Administrator account before running DUPs. See "Microsoft Windows Server 2008 User Account Control" for more information.

Support For Trusted Platform Module (TPM) and BitLocker

A TPM is a secure microcontroller installed on the motherboard of your system which provides basic security-related functions. BitLocker™ is a data protection feature in the Windows Server 2008 operating system. TPM interacts with BitLocker to provide protection at system startup. A successful DUP execution depends on TPM Security, TPM Activation and BitLocker settings. See "Trusted Platform Module (TPM) and BitLocker Support" for more information.

Other Documents You Might Need

- The *Dell OpenManage Server Administrator Compatibility Guide* on the Dell Support website at **support.dell.com**, or on the *Dell Systems Management Tools and Documentation* DVD that came with your system. This document summarizes all Dell systems management releases that precede the current release date.

  NOTE: Dell Update Packages do not require Dell OpenManage Server Administrator to be installed on your system.

- The *Server Update Utility User's Guide* on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Tools and Documentation* DVD which provides information on how to identify and apply updates to your system. SUU is one of the applications used to update your Dell system or to view updates available for any supported system. SUU compares the versions of components currently installed on your system with update components packaged on the *Dell Server Updates* DVD. It then displays a comparison report of the versions and provides an option of updating the components.

  NOTE: Only users with administrative privileges can perform updates with SUU.

- The *Dell OpenManage Deployment Toolkit (DTK) User's Guide* on the Dell Support website at **support.dell.com.** The DTK includes a set of utilities for configuring and deploying Dell systems and is designed for customers who need to build scripted installations to deploy large numbers of servers in a reliable fashion without having to dramatically change their current deployment processes. The guide also provides information on how to execute Linux DUPs in the Dell-provided or in the customized embedded Linux environment including the required dependencies.

  NOTE: Currently, DUPs are supported only in the DTK embedded Linux environment. Running DUPs in the Windows Preinstallation (Windows PE) environment for pre-operating system hardware updates is not supported. See the *Dell Update Packages for Linux User's Guide* and the *Dell OpenManage Deployment Toolkit User's Guide* for more information.

- The *Dell OpenManage IT Assistant User's Guide* on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Tools and Documentation* DVD. Dell OpenManage IT Assistant allows you to load DUPs and System Update Sets into a central repository, then compare the packages to the versions of the software currently running on your enterprise systems. You can then decide whether to update systems that are not in compliance, either immediately or according to a schedule you define. You can use SUU with IT Assistant to update multiple systems in a single session.
- The *Dell Systems Software Support Matrix* on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Tools and Documentation* DVD. This document has information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.

Obtaining Technical Assistance

If at any time you do not understand a procedure described in this guide, or if your product does not perform as expected, different types of help are available. For more information see "Getting Help" in your system's *Installation and Troubleshooting Guide* or the *Hardware Owner's Manual*.

Additionally, Dell Enterprise Training and Certification is available; see **www.dell.com/training** for more information. This service might not be offered in all locations.

2

Using Dell Update Packages

Before You Begin

This section is to help you get the most out of Dell™ Update Packages (DUPs). Updating the system software on your Dell systems should be a key element of your company's overall change management policies and procedures. Maintaining the system software on your Dell systems helps ensure trouble-free operation.

Before you apply any update to your system, you may want to carefully plan your update strategy, based on the conditions that are necessitating the update. Many reasons may exist for making the decision to update your Dell system, such as:

- Correcting a security concern
- Correcting a problem on your system, based on a recommendation from Dell Support personnel
- Updating a system software component to a minimum level required by an application
- Gaining access to a new feature or improved performance
- Updating all of the system components as part of your company's periodic maintenance process

Each of the preceding update situations entails different levels of urgency, but all require a certain level of planning to ensure a successful update with minimal disruption to your applications and users. The following subsections help you develop the system update strategy that best fits your needs, your company's policies and procedures, and the tools available to you.

Develop Your System Update Plan

You may want or need to update your system for many reasons, as mentioned in the preceding section. This update requirement may be classified as either planned or unplanned.

Planned updates occur as a part of your regular cycle of maintaining your systems with up-to-date BIOS, firmware, and drivers. Many IT organizations establish a regular schedule for performing the updates, which are integrated with the planned maintenance functions. The frequency of these updates varies from company to company; however, it is not uncommon for companies to adopt quarterly or semiannual update schedules. Irregular but still planned updates may occur whenever a system is retasked with a new application or the operating system is either upgraded or changed. Any time that you have scheduled planned outage or downtime for your system may be a good time to consider upgrading the system software components.

Unplanned updates typically occur as a result of applying a critical upgrade to your system to avoid data loss, service interruption, or security threats. You may, for example, be advised to apply an update in response to a call you have placed to a Dell support professional. Although the urgency of applying such an update is greater than a planned update, you know that you must apply careful thought and consideration to ensure a successful update with minimal disruption to your users. The key to success is always having a well-planned strategy for all possible scenarios.

Acquiring DUPs

NOTE: DUPs currently do not support every device type. Dell will continue to make DUPs available on additional devices in future releases.

NOTE: Windows DUPs can be downloaded from the Dell Support website at **support.dell.com**. For instructions, see "How to Obtain DUPs from the Dell Support Website". DUPs are also available in the repository on the *Dell Server Updates* DVD.

Dell provides a number of aids to help you determine whether or not your system requires an update. The Dell File Watch notification service, available on **support.dell.com**, allows you to create an account and register to receive e-mail notifications when Dell publishes an update file for your system. You have the option of specifying which server models you would like to be notified about by entering either the server model type or the Dell hardware service tag. Each e-mail notification includes a short summary of the new file available for your system and a Web link to locate that update file on **support.dell.com**.

After you locate your Update Package, read the summary information to determine whether or not you should download the update and apply it to your system. You can run the Update Package on the target system and read the summary information displayed in the Update Package's interactive window. This information is provided to help you determine whether the update is appropriate for your system and your specific environment.

Executing DUPs

To run DUPs from the interactive graphical user interface (GUI), perform the following steps. This procedure applies to all Update Packages.

1. Execute the DUP by double-clicking the filename from within Windows Explorer.
2. Read the update information displayed in the DUP window.
3. Click **Install** to install the DUP.
4. Reboot the system, if necessary.

To execute DUPs from the command line interface (CLI), see "Command Line Interface Reference."

Verifying the Digital Signature

A digital signature is used to authenticate the identity of the signer of an Update Package and to certify that the original content is unchanged. Digital signature of DUPs gives you a more reliable and trustful method of authentication.

Verifying the digital signature ensures that the original Update Package was received correctly and that the content has not been modified since it was signed.

To verify the Update Package’s digital signature, perform the following steps:

1. Start Windows Explorer and locate the Update Package whose digital signature you want to verify.
2. Right-click the filename.
3. Click **Properties** in the pop-up menu.
4. In the **Properties** window, click the **Digital Signatures** tab.

   NOTE: If this tab is not displayed, the Update Package is not signed.

5 Select the signature from the signature list, and click **Details**.

NOTE: The signature is not verified until you click **Details**.

The **Digital Signature Details** window appears.

6 Read the digital signature information to verify that the digital signature is OK.

7 Click **OK** to close the window.

Compatibility Concerns

Meeting System Prerequisites

DUPs are designed to confirm that all prerequisites are satisfied before applying the update to your system. Each DUP checks to ensure the following:

- The DUP applies to your target system.
- The DUP applies to the operating system running on your system.
- The device associated with the DUP is present on your system.
- Minimum required versions of related system software are running on your system.

DUPs are designed with built-in error handling capabilities to ensure that the preceding requirements are validated. If the conditions are not met, no update occurs. The design also allows you to create groups of DUPs and apply them to a wide range of systems. For example, if some of the Dell systems in your environment contain PERC 6/i RAID controllers and the others contain PERC 5/i controllers, you could include both the PERC 6/i and PERC 5/i storage controller DUPs in one script and run this script on every system in your environment. The RAID Update Packages would be installed on the systems as appropriate, while the RAID Update Packages that did not apply would not be installed.

Additionally, if you only want to verify that a given DUP can be applied to your system, you can invoke the package by using the following CLI command:

```
packagename.exe /c /s
```

This command executes the dependency rules within the DUP, issues any warnings, exits without applying the update to your system, and writes the results to a log file (located in the **C:\dell\updatepackage\log** default directory). You can also use the DUP to set an exit code to perform decisions within your scripts.

Updating Non-English Operating Systems

You can use DUPs on non-English operating systems; however, DUPs are not provided in other languages at this time. Therefore, the summary information and error messages appear in English only. Support for additional languages may be provided in a future release.

Effects of Applying the Updates on a Running System

System Reboot Required

Certain DUPs, such as those that update the system BIOS, require a reboot for the new software to take effect. After you apply an update that requires a reboot, you must restart the system to complete the update.

You have the option of choosing to defer the reboot until another time as long as you do not turn off the system. This feature is primarily intended to allow you to apply any number of updates together and perform the system reboot after the last update has been applied. If this process is interrupted, through a power interruption, for example, you must repeat the updates. Therefore, Dell recommends that you schedule updates for a time when the reboot can take place immediately after you apply the last update.

Impact on Users and Applications

Generally, you can apply the updates to a running system because they consume few system resources. Be sure to read the information contained in the DUP before applying the update to determine if applying the update may cause a service interruption to your users or applications. When in doubt, always apply updates at a time when no critical applications or users require the system.

Specifying the Order of Multiple Updates

When applying multiple updates at the same time, be sure to use the order indicated in the "Installation Order of DUPs" section. As previously noted in the "System Reboot Required" section, you may defer rebooting the system until after running the last of multiple Update Packages.

You may also want to use the /l option to specify that each of the Update Packages writes to the same log file. This option allows you to create a single log file to consolidate the execution results.

Delivering DUPs to Your Systems

Using Software Distribution Applications With Update Packages

Many IT organizations use internally developed or purchased software distribution applications to remotely install and update software. Update Packages have been designed to operate with any such tool, provided that the tool can remotely deliver and execute a Microsoft® Windows® application and supply that application with command line arguments. Consult the documentation for your tool or contact the tool's supplier to determine if these capabilities are available.

Updating Many Systems

For large environments that consist of hundreds or perhaps thousands of systems, remote software distribution applications provide the best solution. Many of these tools can effectively leverage the DUPs and provide the convenience of installing and updating a variety of software, such as operating systems and applications, in a heterogeneous environment.

Network file shares are also an effective method of making DUPs accessible in a distributed environment. When a DUP begins execution, it first copies the contents of the DUP to a temporary location on the system's local drive. This process ensures that the update can be completed even if the connection to the network share is lost for any reason.

Remote Terminal Sessions

In today's highly distributed environment, it is quite common for IT organizations to use remote access solutions, such as Microsoft Terminal Services, to gain access to their remote systems. You may use this type of solution to run DUPs.

NOTE: If your terminal session is disconnected during a NIC driver update, you will need to re-connect and verify that the update has completed successfully.

Stand-alone Systems and Firewalls

For systems that are not connected to the Internet, you need to download your DUPs from **support.dell.com** by using a system that does have access to the Internet, such as your desktop or portable computer. You can make DUPs available to your system by copying them onto removable media that your system supports (such as CD, USB devices, tape, and so on).

Confirming the Update

To ensure that DUPs were applied to your system, review the log files that were generated during execution. See "DUP Message Logs" for detailed information about the logging feature.

If you want to revert to an earlier (older) version of the software after updating to a newer version, you must download the appropriate Update Package from **support.dell.com** and install it. To install the earlier version from a script, use the **/s** (unattended) mode. In addition, you must use the CLI **/f** option, which forces the downgrade. To install the earlier version from the GUI, you are prompted to ensure that you want to do so.

If your system loses power during the update process, you must perform the updates again.

Update and Rollback in Unified Server Configurator Lifecycle Controller Enabled (USC LCE)

Dell Unified Server Configurator (USC) Lifecycle Controller Enabled (LCE) is an embedded configuration utility that enables systems and storage management tasks from an embedded environment throughout the system's life cycle.

Residing on an embedded flash memory card, USC LCE is similar to a BIOS utility in that it can be started during the boot sequence and can function independently of an installed operating system.

Using USC LCE, you can quickly identify, download, and apply system updates without searching the Dell Support website at **support.dell.com**. You can also configure your system BIOS and system devices (such as NIC, RAID, and iDRAC), deploy an operating system, and run diagnostics to validate your system and the attached hardware.

NOTE: Certain platforms or systems may not support the full set of features provided by USC LCE.

Update in USC LCE

You can update your system BIOS, iDRAC firmware, power supply firmware, and RAID and NIC firmware. Use the **Platform Update** wizard to display a list of available updates for your system.

You can define a location to search for available updates from the following options:

- the Dell File Transfer Protocol (FTP) server (**ftp.dell.com**). You can use a proxy server to access **ftp.dell.com**.
- a USB device. When accessing updates from a local USB device, the USB device must be plugged in before selecting the **Platform Update** option in USC LCE.

NOTE: See the *Dell Unified Server Configurator User Guide* available on the Dell Support website at **support.dell.com** for more information on updating the platform.

After you select the updates you want to apply, USC LCE downloads and applies the updates. If you decide to update any device in USC LCE, the update package of the corresponding device is downloaded. After successfully downloading, verifying, and extracting the DUPs, the corresponding devices are updated. If the update fails, error messages are displayed.

Rollback in USC LCE

You can update any component, for example BIOS, in both USC LCE and your operating system environment. After the update is successful in your operating system environment using DUPs, you can enter USC LCE and revert the component to the version that was previously installed before the update occurred.

USC LCE supports platform firmware rollback to the previous version. If your operating system has a non–functioning application because of a BIOS or firmware flash, reboot to USC LCE and roll back to the previous version.

NOTE: Only BIOS and firmware can be rolled back. The USC LCE application, the Dell Diagnostics application, and drivers needed for operating system installation cannot be rolled back to an earlier version.

If you have updated your system's BIOS or firmware only once, the rollback feature offers the option of reverting to the factory-installed BIOS or firmware images. If you have updated your BIOS or firmware to multiple versions, the factory-installed images are overwritten and you cannot revert to them.

NOTE: Rollback is not supported in your operating system environment. To enable rollback, ensure that you boot into USC LCE.

Typical Usage Scenarios

Scenario One — Firmware Update During a Hardware Upgrade

As the systems administrator, you are responsible for your company's Dell system, which runs the electronic mail services for 42 employees. You have scheduled a weekend hardware upgrade for the mail server to add additional SAS drives. You plan to use the enhanced Storage Management Service, RAID systems management software to stripe the new disk drives. The enhanced Storage Management Service is a part of the Server Administrator, which you have been using to manage your system's day-to-day functions. The **readme.txt** file that came with the installation instructions for your new disk drives requires that the PERC 6/E storage controller's firmware is of the latest version in order to configure the new disk drives. Consequently, you must upgrade the PERC 6/E firmware as part of your weekend hardware update.

To accomplish this update, you perform the following general steps:

1. Log on to your account on **support.dell.com** from your office desktop or portable system.

   Because you have an account on **support.dell.com**, the Dell hardware service tag of your server is automatically displayed.

2. Select **Drivers and Downloads**.

3. Select your model, product family, and product line.

4. Locate **PERC 6/E**, which matches the controller type for your system.
5. Click the firmware name and then click the filename for the **Update Package for Microsoft Windows** in the **File Formats** section.
6. Click **Download Now** to download the Update Package to your hard drive.
7. After the Update Package has finished downloading to your system, copy the file to your system's **C:\temp** directory.
8. Verify the digital signature for the Update Package.

   You arrive on Saturday to begin the upgrade process.

9. Notify the users on your system and shut down the electronic mail services.
10. Verify that all users have disconnected, and then execute the firmware Update Package by double-clicking the filename from within Windows Explorer.
11. Read the information displayed in the Update Package window and confirm that this is the correct firmware for your PERC controller.
12. Click **Install** to load the PERC 6/E firmware.
13. Reboot the system to confirm that the new firmware has been loaded and that the system is fully operational.

You have successfully updated your RAID controller's firmware and you are ready to finish the hardware upgrade by adding the new drives, configuring the disk stripe set, and resuming mail services.

Scenario Two — Retasking a System

You are the systems administrator for a large company. Your group requires an additional system to support a new financial analysis package, and you have access to a Dell system that is no longer in use from another department within the company. Because the Dell system has an older operating system installed on it, you plan to upgrade the operating system before installing the new financial application. You also plan to install the most current BIOS, firmware, and drivers offered by Dell, as well as install the Dell OpenManage™ Server Administrator systems management software.

To prepare the system to run the company's new financial software, you perform the following general steps:

1. Use the *Dell Systems Management Tools and Documentation* DVD that came with the Dell system to install the most current version of the Windows Server 2003 operating system.

   NOTE: The Dell OpenManage systems management software kit is now available on a single DVD titled *Dell Systems Management Tools and Documentation*.

2. Log on to **support.dell.com**.
3. Select **Drivers & Downloads** and choose a model or enter the service tag for the Dell system.
4. Select the product family, product line, and the product model.
5. Locate the BIOS, ESM firmware, and PERC 6/E Update Packages for the Dell system and download them.

   Additionally, download the Server Administrator application.

   NOTE: To install the current version of drivers for your operating system, download the current version of the *Dell Systems Management Tools and Documentation* DVD from the Dell Support website at **support.dell.com**. Drivers are located in the SERVICE directory in the DVD.

6. Copy the files that you downloaded to the system's **C:\temp** directory.
7. Verify the digital signature for each Update Package.
8. Create a simple batch file that executes the following packages one-by-one in this order:

   - PERC 6/E driver
   - PERC 6/E firmware
   - ESM system firmware
   - BIOS

   Use the CLI /s option on each line in the batch file for these packages so that you can schedule the process by using the task manager. On each line of the file, you also include the following line to check the results of the execution:

   ```
   /l=c:\temp\6950_upgrade.log
   ```

9. Analyze the log file, verify that the packages installed successfully, and note that the system has rebooted.
10. Install Server Administrator.

At this point, the Dell system is running the most current operating system and the system BIOS, system firmware, RAID controller's firmware, and drivers are up–to–date. You are now ready to install the financial application for your division.

Scenario Three — BIOS Update for 200 Systems

You are the systems administrator for a large business with over 500 stores. Every store location has a Dell system that is used to manage the company’s inventory and billing systems. About 200 of these stores are running on Dell systems. You have entered all your system model types into Dell's File Watch service on **support.dell.com**. File Watch notifies you when Dell posts any new software updates on **support.dell.com** for the system types that you registered. Recently, you received an e-mail message from the File Watch system advising you of a new BIOS update that is available for your systems.
This BIOS update is designed to dynamically regulate the system's cooling fan speeds, which allows the systems to run quieter and consume less energy. Because you remotely manage these systems, you have invested in a software distribution tool that allows you to schedule remote software installation and updates. You also have a planned 4-hour service window each weekend when you can perform any maintenance functions necessary on the company’s systems.

To roll out the BIOS update to the company’s servers, you perform the following general steps:

1. Log on to **support.dell.com**.
2. Select **Drivers and Downloads**, and select your product.
3. Download the new BIOS DUP for the system.
4. Verify the digital signature for the Update Package.

5. Use the software distribution tool to create an update task that delivers the BIOS DUP to all the systems in the network.

   The update task is simply a batch command that invokes the BIOS DUP and uses the CLI **/r /s** options to ensure that the system is rebooted when it is necessary.

   This BIOS DUP runs only on the specified Dell systems; therefore, you can distribute it to all the systems regardless of the system model type.
   The DUP does not affect other systems.

   NOTE: Some of the BIOS versions available in DUPs support more than one Dell system.

6. Use the software distribution tool to schedule the BIOS update task to run on all systems at 2:00 A.M. this coming Saturday, which falls within the allotted 4-hour maintenance window.
7. On Sunday morning, you log in to your system and check the execution results report within the software distribution tool and determine that the BIOS DUP was successfully applied to 180 of your 200 systems.
8. The attempted BIOS update on the remaining 20 systems returned the message that the update was not required.
9. Log on to any one of the 20 systems and check the BIOS DUP log file.

   You confirm that on these 20 systems, the BIOS version was already up to date, as these systems were those most recently purchased from Dell.

You have successfully completed the BIOS update process for the company.

3

Command Line Interface Reference

Using the CLI

This section provides information for using the command line interface (CLI) for Dell™ Update Packages (DUPs).

CLI Options

You can display information about CLI options by typing the DUP name and either `/?` or `/h` at a command line prompt. For example, type the following command to get a help screen about the CLI options:

```
PE2850-BIOS-WIN-A02.exe /?
```

Table 3-1 provides a list of the CLI options, a description of each option, and the command syntax.

NOTE: DUPs for Microsoft® Windows® operating systems cannot display output at the command line because they are Windows GUI applications. All output information is written to a log file. See "DUP Message Logs" for information on log files.

Table 3-1. CLI Options: Usage

CLI Option	CLI Task Description	Command Syntax
`/?` or `/h` Help option	Displays command line options and help information.	*packagename*`.exe /?` *packagename*`.exe /h`
`/c` Check option	Determines if the update can be applied to the target system. The /**s** option is required with this option. Options /**f**, /**e**, and /**r** are not valid with this option. When you click **Install** in the graphical user interface (GUI) mode, the same checking process is performed.	*packagename*`.exe /s /c /l=c:\pkg.log`

Table 3-1. CLI Options: Usage *(continued)*

CLI Option	CLI Task Description	Command Syntax

`/e=<path>`
Extract option
	Extracts all files contained in the DUP to the path you specify. If the directory specified in the path does not exist, it is created.
	If the path contains spaces, use quotation marks around the <*path*> value.
	The /**s** option is required with this option.
	Options /**f**, /**c**, and /**r** are not valid with this option.
		`packagename``.exe /s /e=c:\update`
		`packagename``.exe /s /e="c:\update files"`

`/f` Force option	Allows downgrade of the software to a previous (older) version. The /**s** option is required with this option. Options /**e** and /**c** are not valid with this option. **NOTE:** Before downgrading the software to a previous version, see the documentation for the previous version.	*`packagename`*`.exe /s /f /l=c:\pkg.log`

`/l=<filename>`
Log option
	Appends logged messages to a specified ASCII file; creates a new file if one does not exist. If the file name contains spaces, use quotation marks around the <*filename*> value.
	The /s option is required with this option.
		`packagename``.exe /s /l=c:\pkg.log`
		`packagename``.exe /s /l="c:\Update Log\pkg.log"`

`/r` Reboot option	Reboots the system, if required, after performing the update. The reboot does not occur: • If the DUP fails or is not applicable to the target system • If the DUP does not require a reboot The /**s** option is required with this option. Options /**e** and /**c** are not valid with this option.	*`packagename`*`.exe /s /r /l=c:\pkg.log`

Table 3-1. CLI Options: Usage *(continued)*

CLI Option	CLI Task Description	Command Syntax
`/s` Silent option	Executes the update silently without user intervention. When /s is not specified, the DUP is launched in GUI (interactive) mode. The /**s** option is required when using the /**e**, /**f**, /**c**, /**l**, and /**u** options. **NOTE:** Using the /s option causes all output to be written to log files.	`*packagename*.exe /s /l=c:\pkg.log`

`/u=<filename>`
Unicode Log option
	Appends logged messages to a specified Unicode file; creates a new file if one does not exist. If the file name contains spaces, use quotation marks around the <*filename*> value.
	The /**s** option is required with this option.
		`*packagename*.exe /s /u=c:\pkg.log`
		`*packagename*.exe /s /u="c:\Update Log\pkg.log"`

Exit Codes for CLI

After running DUPs, the exit codes described in Table 3-2 are set.

The exit codes help you determine and analyze the execution results after you run DUPs.

Table 3-2. Exit Codes

Value	Message Name	Description
0	SUCCESSFUL	The update was successful.
1	UNSUCCESSFUL (FAILURE)	An error occurred during the update process; the update was not successful.
2	REBOOT_REQUIRED	You must restart the system to apply the updates.

Table 3-2. Exit Codes *(continued)*

Value	Message Name	Description
3	DEP_SOFT_ERROR	Some possible explanations are: • You attempted to update to the same version of the software. • You tried to downgrade to a previous version of the software. To avoid receiving this error, provide the /f option.
4	DEP_HARD_ERROR	The required prerequisite software was not found on your system. The update was unsuccessful because the server did not meet BIOS, driver, or firmware prerequisites for the update to be applied, or because no supported device was found on the target system. DUP enforces this check and blocks an update from being applied if the prerequisite is not met, preventing the server from reaching an invalid configuration state. The prerequisite can be met by applying another DUP, if available. In this case, the other package should be applied before the current one so that both updates can succeed. A DEP_HARD_ERROR cannot be suppressed by using the /f switch.
5	QUAL_HARD_ERROR	The DUP is not applicable. Some possible explanations are: • The operating system is not supported by the DUP. • The system is not supported by the DUP. • The DUP is not compatible with the devices found in your system. A QUAL_HARD_ERROR cannot be suppressed by using the /f switch.
6	REBOOTING_SYSTEM	The system is being rebooted.

Sample Script

The following example shows how you can use scripts to run DUPs.

The **Update.bat** script is an example of updating the BIOS and ESM firmware on a Dell system. The execution results are placed in a log file named **PE2600.log**. Text that represents the exit codes from the execution of each package is also placed in the file. You may want to handle some of the exit codes differently in the scripts you write.

This script assumes that DUPs have already been downloaded to a folder on the target system.

Update.bat script

```
@echo off
set LOG=C:\Updates\PE2600.log
set PKG=C:\Updates\ESM\ESM-WIN-A18.exe
echo Executing %PKG% >>%LOG%
%PKG% /s /l=%LOG%
set ExitCode=%ErrorLevel%
if %ExitCode% EQU 0 echo Result: SUCCESSFUL >>%LOG%
if %ExitCode% EQU 1 echo Result: UNSUCCESSFUL >>%LOG%
if %ExitCode% EQU 2 echo Result: REBOOT_REQUIRED
>>%LOG%
if %ExitCode% EQU 3 echo Result: DEP_SOFT_ERROR
>>%LOG%
if %ExitCode% EQU 4 echo Result: DEP_HARD_ERROR
>>%LOG%
if %ExitCode% EQU 5 echo Result: QUAL_HARD_ERROR
>>%LOG%
if %ExitCode% EQU 6 echo Result: REBOOTING_SYSTEM
>>%LOG%
set PKG=C:\Updates\BIOS\PE2600-BIOS-WIN-A04.exe
echo Executing %PKG% >>%LOG%
%PKG% /s /l=%LOG%
Set ExitCode=%ErrorLevel%
if %ExitCode% EQU 0 echo Result: SUCCESSFUL >>%LOG%
if %ExitCode% EQU 1 echo Result: UNSUCCESSFUL >>%LOG%
if %ExitCode% EQU 2 echo Result: REBOOT_REQUIRED
>>%LOG%
```

```
if %ExitCode% EQU 3 echo Result: DEP_SOFT_ERROR
>>%LOG%
if %ExitCode% EQU 4 echo Result: DEP_HARD_ERROR
>>%LOG%
if %ExitCode% EQU 5 echo Result: QUAL_HARD_ERROR
>>%LOG%
if %ExitCode% EQU 6 echo Result: REBOOTING_SYSTEM
>>%LOG%
```

4

Troubleshooting

Messages

Table 4-1 provides descriptions and solutions to messages that you may receive when running Dell™ Update Packages (DUPs).

NOTE: The **Readme.txt** file, which is available on the Dell Support website at **support.dell.com**, provides the latest information regarding known issues.

Table 4-1. Update Packages: Message Information

Message	Description/Solution
`This Update Package is not compatible with your system. Your system: <system model name>`	Select a compatible DUP, and try the update again.
`This Update Package is not compatible with your system. Your system: <system model name> Systems(s) supported by this package: <system model name>...: <system model name>`	Select a compatible DUP, and try the update again.
`This Update Package cannot be executed under the current operating system.`	DUPs support Microsoft® Windows® 2000 Server, Windows Server® 2003 and the Windows Server 2008 operating systems. Latest information on various Dell systems and operating systems that DUPs are supported on are available in the *Dell Systems Software Support Matrix*. This document is available on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Tools and Documentation* DVD.

Table 4-1. Update Packages: Message Information *(continued)*

Message	Description/Solution
`Your system does not have the minimum operating system version or service pack required for this Update Package.`	The DUP you selected cannot be installed because the minimum operating system version or service pack requirements were not met. Install the appropriate version, and try the update again. Or, use an alternate update method on **support.dell.com**.
`Your system exceeds the maximum operating system version supported by this Update Package.`	The DUP you selected cannot be installed because your system exceeded the maximum operating system version supported by the DUP. Install the appropriate version or select another DUP, and try the update again.
`This Update Package is not compatible with any of the devices detected in your system.`	Select a compatible DUP for the device(s) you want to update, and try again.
`The prerequisite software version for this update was not found: Software application name: <name> Current version: <version> Required version: <version>`	The DUP you selected cannot be installed because a prerequisite requirement was not met. Install the appropriate prerequisite software version, and try the update again.
`The software to be updated was not found. Install the following software, and then retry the update. Software name: <name> Required version: <version>`	Your system does not contain the software that matches the DUP.

Table 4-1. Update Packages: Message Information *(continued)*

Message	Description/Solution
`The version of this Update Package is newer than the currently installed version. Software application name: <name> Package version: <version> Installed version: <version>`	This message confirms the version of the currently installed software before the update is performed.
`The version of this Update Package is older than the currently installed version. Software application name: <name> Package version: <version> Installed version: <version>`	The DUP you selected cannot be installed because a newer version of the software already exists on the system. To install the older version: (Using the Interactive mode) Click **Yes** when prompted to continue with the installation. (Using the CLI) Specify the **/f** option.
`The version of this Update Package is the same as the currently installed version. Software application name: <name> Package version: <version> Installed version: <version>`	The DUP you selected cannot be installed because the same version of the software already exists on the system. (Using the Interactive mode) Click **Yes** when prompted to continue with the installation.
`This package is not compatible with the version of Server Agent on your system. You must upgrade to Server Administrator before running this package.`	Use an alternative update method from **support.dell.com**.

Table 4-1. Update Packages: Message Information *(continued)*

Message	Description/Solution
`Administrator privileges are required to perform this update.`	Log in with Administrator privileges, and try the update again.
`You must reboot the system for the update to take effect.`	If you shut down or power off the system after performing an update, you will lose the update.
`An Update Package is already running. Wait until it is complete before proceeding with another update.`	You can run only one DUP at a time.

`This Update Package is not installed. Software application name: <name> Package version: <version>`
`Would you like to install?`
	In interactive mode, if a fresh install is applicable, you are presented with a choice to install or not. The package version is also displayed.

DUP Message Logs

Logging occurs when you install a DUP. The logs maintain information about all update activity. Update Packages write messages to the following logs:

- Package log
- Support log
- Windows operating system event log

Package Log

Use the Package log to view and analyze various events and errors that may have occurred during the package installation. The Package log file resides in the following default location:

C:\dell\updatepackage\log\*packagename*.txt

where **C:** is your system drive and ***packagename*** is the name of the DUP that you installed.

This log is encoded in Unicode, which supports localized systems.

Package Log File Example

```
====> Dell Update Package application started <====

Command:C:\WINNT\TEMP\DUPBIOS\PE2650_BIOS_WIN_A21.EXE
/f /s /l=C:\WINNT\TEMP\5000021.dup

Date:2006-11-09 10:22:56

=====================================================

All files extracted OK

Release ID: R136685

Update Package version: 5.3.0 (BLD_31)

User: SYSTEM

Collecting inventory...

Running validation...

The version of this Update Package is newer than the
currently installed version.

   Software application name: BIOS

   Package version: A21

   Installed version: A19

Executing update...

Execution complete
```

```
The system should be restarted for the update to take
effect.

=================> Update Result <==================

Update ready to be applied at reboot

Application: BIOS

Previous version: A19

New version: A21

====================================================

Exit code = 2 (Reboot required)

2006-11-09 10:23:11
```

Support Log

Use the Support log to view and analyze execution details that have occurred during the package installation. Contents of this log are useful when communicating with Dell™ support representatives during issue diagnosis. This log includes package XML details for the specific device updated.
The Support log file resides in the following default location:

C:\dell\updatepackage\log\support\*packagename*.log

where C: is your system drive and ***packagename*** is the name of the DUP that you installed. If you install the same package more than once on the same system, the package appends the output to this log. This log is encoded in Unicode, which supports localized systems.

Support Log File Example

```
====<< PACKAGE LOG (SEZ) >>====> Dell Update Package
application started <==============================

Command:
C:\WINDOWS\TEMP\DUPBIOS\PE2850_BIOS_WIN_A06.EXE /f /s
/l=C:\WINDOWS\TEMP\5000012.dup

Date:2006-11-13 16:59:11

====================================================
<< SEZ >>Creating temp folder:
C:\Temp\PE2850_BIOS_WIN_A06

<< PACKAGE LOG (SEZ) >>All files extracted OK

<< PACKAGE LOG >>Release ID: R136644

<< PACKAGE LOG >>Update Package version: 5.3.0
(BLD_31)

Command Line: /f /s /l=C:\WINDOWS\TEMP\5000012.dup
/packagename="PE2850_BIOS_WIN_A06.EXE"
/supportlogdir="C:\Dell\UpdatePackage\log"
/currentpath="C:\WINDOWS\system32"

<< PACKAGE LOG >>User: SYSTEM

Package source:
C:\Temp\PE2850_BIOS_WIN_A06\SPSETUP.exe

<< PACKAGE LOG >>Collecting inventory...

Inventory command: biosie.exe -i inv.xml

Inventory Execution: returnCode=0, exitCode=0

<SVMInventory lang="en"><Device componentID= "159"
display="BIOS"><Application componentType= "BIOS"
version="A04" display = "BIOS" /></Device><System
systemID="016D"></System><OperatingSystem osVendor=
"Microsoft"  osArch="x64"  majorVersion="5"
minorVersion="2"  spMajorVersion="1"  spMinorVersion=
"0" ></OperatingSystem></SVMInventory>

<< PACKAGE LOG >>Running validation...

No custom validation configuration file found
(CVConfig.xml)

<SVMValidation lang="en" ><System systemID="016D"
></System><OperatingSystem osVendor="Microsoft"
osArch="x64"  majorVersion="5"  minorVersion="2"
spMajorVersion="1"  spMinorVersion="0"
></OperatingSystem><Device componentID="159"
display="BIOS" ><Application componentType="BIOS"
```

```
version="A04"  display="BIOS" ><Package version="A06"
></Package></Application><Validation type="info"
result="true" ><Message>The version of this Update
Package is newer than the currently installed version.

   Software application name: BIOS

   Package version: A06

   Installed version:
A04</Message></Validation></Device><TargetCompareStat
e>1</TargetCompareState></SVMValidation>

<< PACKAGE LOG >>The version of this Update Package is
newer than the currently installed version.

   Software application name: BIOS

   Package version: A06

   Installed version: A04

<< PACKAGE LOG >>Executing update...

Execution command: biosie.exe -u update.xml

Update Execution: returnCode=0, exitCode=0

<SVMExecution lang="en"><Device componentID= "159"
display="BIOS"><Application componentType= "BIOS"
version="A04" display = "BIOS" ><Package version=
"A06"/><SPStatus result="true"><Message id="0">The
update was successful. Reboot the system to complete
the BIOS
update.</Message></SPStatus></Application></Device><R
ebootRequired>0</RebootRequired></SVMExecution>

Device: BIOS, Application: BIOS

The update was successful. Reboot the system to
complete the BIOS update.

<< PACKAGE LOG >>Execution complete

<< PACKAGE LOG >>The system should be restarted for
the update to take effect.
```

```
=====<< PACKAGE LOG >>======> Update Result <=======

Update ready to be applied at reboot

<< PACKAGE LOG >>Application: BIOS

Previous version: A04

New version: A06

================<< PACKAGE LOG >>=====================

Error code before being mapped: 0002

<< PACKAGE LOG >>Exit code = 2 (Reboot required)

?<?xml version="1.0" encoding="UTF-16"?>

<SoftwareComponent schemaVersion="1.0" packageID=
"R136644" releaseID="R136644" dateTime="2006-10-
05T14:59:57-05:00" releaseDate="October 05, 2006"
vendorVersion="A06" dellVersion="A06" packageType=
"LWXP" xmlGenVersion="1.0.2378">

  <Name>

    <Display lang="en"><![CDATA[Dell Server System
BIOS,A06]]></Display>

  </Name>

  <ComponentType value="BIOS">

    <Display lang="en"><![CDATA[BIOS]]></Display>

  </ComponentType>

  <Description>

    <Display lang="en"><![CDATA[PowerEdge 2850, BIOS,
A06   ]]></Display>

  </Description>

  <LUCategory value="BIOS">

    <Display lang="en"><![CDATA[Server
BIOS]]></Display>
```

```
  </LUCategory>

  <Category value="BI">

    <Display lang="en"><![CDATA[FlashBIOS
Updates]]></Display>

  </Category>

  <SupportedDevices>

    <Device componentID="159" embedded="1">

      <Display lang="en"><![CDATA[Server System
BIOS]]></Display>

    </Device>

  </SupportedDevices>

  <SupportedSystems display="1">

    <Brand key="3" prefix="PE">

      <Display lang=
"en"><![CDATA[PowerEdge]]></Display>

      <Model systemID="16D">

        <Display lang="en"><![CDATA[2850]]></Display>

      </Model>

    </Brand>

  </SupportedSystems>

  <InstallInstruction fileName=
"PE2850_BIOS_WIN_A06.EXE" typeCode="LWXP">

    <Display lang="en"><![CDATA[Dell Update Package
Instructions for PE2850_BIOS_WIN_A06.EXE:

Installation:

    Browse to the location where you downloaded the
    file and double-click PE2850_BIOS_WIN_A06.EXE.
    Read over the release information presented in the
    dialog window.

    Download and install any prerequisites identified
    in the dialog window before proceeding.

    If this is a BIOS update package, install any
    necessary Embedded Systems Management firmware
    prior to this BIOS update. Otherwise, go next step.

    Click the Install button.

    Follow the remaining prompts to perform the update.

]]></Display>

  </InstallInstruction>

  <RevisionHistory>

    <Display lang="en"><![CDATA[* Updated Intel(R)
Xeon(TM) Dual-Core Processor with 2x2MB L2 Cache A0
Stepping Microcode (Patch ID=0C).

    Added code to support Dell SAS5/e adapter card.

    Added code to increase the fan speeds if there are
    RAID Cards in the system.

]]></Display>

  </RevisionHistory>

  <ImportantInfo URL=
"http://support.dell.com/support/downloads/format.asp
x?releaseid=R136644&amp;c=us&amp;l=en&amp;s=
gen&amp;cs">

    <Display lang="en"><![CDATA[When a RAID card is
present in the system, the fan speeds will not
increase unless the BMC firmware has been also updated
to version 1.68 or later.

]]></Display>

  </ImportantInfo>
  <Criticality value="1">

    <Display lang="en"><![CDATA[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).]]></Display>

  </Criticality>

</SoftwareComponent>

Registered system log event source

<< PACKAGE LOG >>2006-11-13 16:59:12

<< SEZ >>Deleting temp folder
```

Windows Operating System Event Log

Messages are logged to the Windows System Event Log (SEL) if the update is attempted. You can use the Windows Event Viewer to view and manage Windows events.

The log file includes the following information:

- Date and time that the DUP was launched
- User that launched the update
- DUP type
- DUP version
- Framework version of the DUP
- Version that was already installed on the system

The log file is created even when invalid options are provided to the package, execution is aborted by the administrator, or an error condition is encountered. In addition, administrators can create their own log files by providing the /l option on the command line. The syntax is as follows:

```
packagename.exe /s /l=mylogfile.log
```

Windows SEL Entry Example

The following is an example of an informational message in the SEL that you may view after a successful DUP execution.

```
=====================================================
Update successful
Package:  PE1850-BIOS-WIN-A01.exe
Description:  Dell Server System BIOS, A01
Previous version:  A00, New version:  A01
Log file:  C:\Dell\UpdatePackage\log\PE1850-BIOS-WIN-
A01.txt
Exit code = 6 (Rebooting System)
=====================================================
```

5

Frequently Asked Questions

Question: Must I reboot my system after applying every Dell™ Update Package (DUP)?

Answer: DUPs that are running in the interactive mode determine if it is necessary to reboot your system. If so, you are prompted to reboot. In the silent unattended mode, the exit code is set to 2, which indicates that a system restart is required.

Question: Which operating systems are supported by DUPs?

Answer: For a complete list of supported systems and operating systems, see the *Dell Systems Software Support Matrix* located on the *Dell Systems Management Tools and Documentation* DVD or on the Dell Support website at **support.dell.com**. The *Dell Systems Software Support Matrix* has information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage™ components that can be installed on these systems.

Question: How do I perform updates if my operating system is not supported by DUPs?

Answer: For those operating systems that are not currently supported, you can perform updates by using the existing update formats from the Dell Support website at **support.dell.com**.

Question: I cannot locate a DUP on support.dell.com for my device. Where is it?

Answer: Ensure that you have provided all the required information for downloading DUPs, such as product category, product line, product model, download category, and operating system.

DUPs are not available for all devices. Dell will continue to make additional DUPs available for more devices in future releases. See the **readme.txt** file for a list of devices currently supported by DUPs.

Question: I'm using a software distribution tool to deploy my applications or operating system updates to my remote servers. Can I use DUPs with this tool to remotely update my servers?

Answer: DUPs are designed to work with most software distribution tools. See the documentation for your tool for more information.

Question: Where can I find the error messages generated by a DUP that is running in unattended mode?

Answer: The execution messages are stored in the Package log file and in the Windows System Event Log (SEL), which are described in "DUP Message Logs" section of this guide.

The Package log file resides in the following default directory:
C:\dell\updatepackage\log\*packagename*.txt

The Windows SEL is available through the Windows Event Viewer.

Question: When I execute a DUP from the command line prompt, I continue to see Windows dialog boxes and pop-up messages. Can I direct the output to the command line prompt console?

Answer: Use the **/s** and **/l** options to direct the output to the log files.

Question: How can I gain access to the DUP dependency information and other information?

Answer: This information is displayed on the initial graphical user interface (GUI) screen when you run the DUP.

Some information is also available by using the CLI **/c /s** options. (You must use the **/c /s** options together.) However, this method provides limited information, such as the version of the update and whether it is applicable for the target system.

Question: Can I use DUPs on other vendors' systems?

Answer: No. DUPs are designed for use on Dell systems only.

Question: I recently updated the BIOS on my system and now I would like to go back to the previous version. Can I do this with DUP?

Answer: Yes. Download the DUP for the previous version of your system BIOS from **support.dell.com** and install it. If a DUP is not available, use one of the other formats on **support.dell.com**.

Question: Why does the DUP for the system BIOS require a reboot?

Answer: The BIOS update is applied only after you reboot your system.

Question: I'd like to apply several updates to my system at once. Can I do this with DUPs? Do I need to be concerned about the order in which I apply the updates?

Answer: Yes, you can apply multiple updates to your system at the same time. See the "Scenario Two — Retasking a System" section for more information. The installation order is very important. See Table 1-1 for information about the update order.

Question: If I rename Windows DUPs, will they still function correctly?

Answer: Yes.

Question: Can I modify DUPs?

Answer: No. DUPs contain logic to guard against potential corruption of their contents. Because of this design, DUPs cannot be modified.

NOTE: If you modify the contents of DUPs, Dell will not support them.

Question: Can I use any other program to inspect or extract the contents of DUPs?

Answer: Yes, you can use WinZip or an equivalent software application.

NOTE: DUPs contain logic to guard against potential corruption of their contents. Because of this design, DUPs cannot be modified. If you modify the contents of DUPs, Dell will not support them.

Question: I am running a non-English version of Windows 2000. Can I use DUPs?

Answer: Yes. You can use DUPs on non-English versions of Windows 2000 Server and Windows Server 2003 operating systems. Currently, DUPs are available only in English.

Question: How will I know when there are new DUPs available for my systems?

Answer: You can check **support.dell.com** for updates or register for the File Watch Service at **www.dell.com** to receive automatic notification for upgrades to your system.

Question: Why do BIOS and firmware updates fail to re-apply (update to the same version), even when using the force (/f) option in CLI mode?

Answer: Re-installation of BIOS or firmware DUPs wastes valuable company time and resources. It accomplishes nothing. If you still wish to apply such an update, run DUPs in the GUI mode and confirm the re-application.

Question: Why does my system only execute one of the CLI options that I entered in a command string?

Answer: Only certain CLI options can be used simultaneously. When invalid combinations of CLI options are entered in a single command string, only the option with the highest priority is executed. See Table 3-1 for details on which commands can be used together.

Question: How do I verify that the DUPs that I have downloaded has a digital signature?

Answer: In Windows Explorer, locate the DUP that you want to verify and right-click the filename. Click **Properties** in the pop-up window. If you see the **Digital Signatures** tab in the **Properties** window, the DUP has a digital signature. If that tab is not displayed, the DUP is not signed. See " Verifying the Digital Signature" for additional information.

Question: Why can't I use a signed DUP with my current release of DUP?

Answer: DUPs released on September 6, 2005 and later are digitally signed.

A

Microsoft Windows Server 2008 User Account Control

In previous versions of Windows®, user accounts were often members of the local Administrators group and had access to administrator privileges. Members of the local Administrators group could install, update, and run software since an Administrator account has system-wide access. When a user was added to the local Administrators group, that user was automatically granted every Windows privilege. These privileges provided access to all operating system resources. Hence, user accounts with Administrator privileges posed a security risk by providing access to operating system resources that could be exploited by malicious software (or malware).

User Account Control (UAC) is a new security feature in the Windows Server® 2008 operating system. When enabled, it restricts access to critical system resources for all users except the built-in local Administrator.

The three types of user accounts in the Windows Server 2008 operating system are:

- Domain Administrator Account which is a user account with administrator privileges.
- Standard User Account which allows the user to install software and change system settings that do not affect other users or the security of the computer.
- Local Administrator Account which is the default super user of the operating system.

The user experience for a Domain Administrator Account differs from a Local Administrator Account when UAC is enabled. When a Domain Administrator Account requires access to critical system resources, the Windows Server 2008 operating system prompts for one of the below before launching a program or task that requires full administrator access:

- Permission to elevate privileges (in the case of a user in the Domain Administrators group)
- Domain administrator credentials to elevate privileges (in the case of standard users)

UAC prompts users in the Domain Administrators group (except the Administrator account) to click **Continue**, if they need to elevate privileges, or to click **Cancel** when performing functions that may entail a security risk. With UAC, users have to upgrade to an Administrator account before running DUPs.

NOTE: Since the user experience is configurable with the Security Policy Manager snap-in (**secpol.msc**) and with Group Policy, there are multiple UAC user experiences. The configuration choices made in your environment will affect the prompts and dialogs seen by standard users, administrators, or both. UAC can be disabled by disabling the **User Account Control: Run Administrators in Admin Approval Mode** setting and requires a system reboot.

If a DUP is run in the GUI mode, the Windows Server 2008 operating system needs the user to permit the operation. But if a DUP is run in unattended mode, the user can bypass the popup window for permission by performing any of the below actions:

- Change the group security policy, `User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode`, to **No Prompt** to disable the popup or elevate privileges without prompting for the Administrators group.
- Disable UAC.
- Use scripts to run the DUP and impersonate yourself as a local administrator at runtime.

UAC Restrictions When Running DUPs remotely

By default, after UAC starts up, all Administrator Account users login as Standard Users. Thus, rights to access critical system resources are not available until the user confirms the privilege elevation request. This restriction disables the option to remotely deploy DUPs. UAC returns an **Access Denied** error if the management node agent runs on these login credentials.

You can bypass the UAC restrictions by:

- Enabling remote agent use of the Local System Account to perform a DUP update. The Local System Account is not protected by UAC (recommended option).
- Using the Local Administrator Account on each remote machine where the DUP is running.

- Disabling UAC for all users on remote machines (not a recommended option).
- Not upgrading to Administrator account on remote machines.

NOTE: Only two accounts (the Local Administrator Account and the Local System Account) are not protected by UAC. All other users including accounts with local administrator rights or domain administrator rights have UAC enabled by default. Even though UAC can be disabled by updating the local or domain security policy, it is not recommended. Remote users have to login as a built-in Local Administrator Account or obtain the Local System Account privilege in order to launch a DUP remotely.

B

Trusted Platform Module (TPM) and BitLocker Support

A TPM is a secure microcontroller with cryptographic capabilities designed to provide basic security-related functions involving encryption keys. It is installed on the motherboard of your system, and communicates with the rest of the system using a hardware bus. You can establish ownership of your system and its TPM through BIOS setup commands.

TPM stores the platform configuration as a set of values in a set of Platform Configuration Registers (PCRs). Thus one such register may store, for example, the motherboard manufacturer; another, the processor manufacturer; a third, the firmware version for the platform, and so on. Systems that incorporate a TPM create a key that is tied to platform measurements. The key can only be unwrapped when those platform measurements have the same values that they had when the key was created. This process is called "sealing" the key to the TPM. Decrypting it is called "unsealing". When a sealed key is first created, the TPM records a snapshot of configuration values and file hashes. A sealed key is only "unsealed" or released when those current system values match the ones in the snapshot. BitLocker™ uses sealed keys to detect attacks against the integrity of your system. Data is locked until specific hardware or software conditions are met.

BitLocker mitigates unauthorized data access by combining two major data-protection procedures:

- **Encrypting the entire Windows® operating system volume on the hard disk:** BitLocker encrypts all user files and system files in the operating system volume.
- **Checking the integrity of early boot components and the boot configuration data:** On systems that have a TPM version 1.2, BitLocker leverages the enhanced security capabilities of the TPM and ensures that your data is accessible only if the system’s boot components are unaltered and the encrypted disk is located in the original system.

BitLocker is designed for systems that have a compatible TPM microchip and BIOS. A compatible TPM is defined as a version 1.2 TPM. A compatible BIOS supports the TPM and the Static Root of Trust Measurement. BitLocker seals the master encryption key in the TPM and only allows the key to be released when code measurements have not changed from a previous secure boot. It forces you to provide a recovery key to continue boot if any measurements have changed. A one-to-many BIOS update scenario results in BitLocker halting the update and requesting a recovery key before completing boot.

BitLocker protects the data stored on a system through "full volume encryption" and "secure startup". It ensures that data stored on a system remains encrypted even if the system is tampered with when the operating system is not running and prevents the operating system from booting and decrypting the drive until you present the BitLocker key.

TPM interacts with BitLocker to provide protection at system startup. TPM must be enabled and activated before it can be used by BitLocker. If the startup information has changed, BitLocker enters recovery mode, and you need a recovery password to regain access to the data.

NOTE: See the Microsoft® TechNet website for information on how to turn on BitLocker. See the documentation included with your system for instructions on how to activate TPM. A TPM is not required for BitLocker; however, only a system with a TPM can provide the additional security of startup system integrity verification. Without TPM, BitLocker can be used to encrypt volumes but not a secure startup.

NOTE: The most secure way to configure BitLocker is on a system with a TPM version 1.2 and a Trusted Computing Group (TCG) compliant BIOS implementation, with either a startup key or a PIN. These methods provide additional authentication by requiring either an additional physical key (a USB flash drive with a system-readable key written to it) or a PIN set by the user.

NOTE: For mass BIOS updates, create a script that disables BitLocker, installs the update, reboots the system and then re-enables BitLocker. For one-to-one Dell™ Update Package (DUP) deployments, manually disable BitLocker and then re-enable it after rebooting your system.

NOTE: In addition to BIOS DUP, execution of firmware DUP for U320, Serial Attached SCSI (SAS) 5, SAS 6, Expandable RAID Controller (PERC) 5, PERC 6, and Cost Effective RAID Controller (CERC) 6 controllers is blocked on a system having a TPM version 1.2 chip, **TPM Security** set at *ON with pre-boot measurement,* and **TPM Activation** set at *Enabled* if you enable BitLocker (TPM or TPM with USB or TPM with PIN).

Glossary

The following list defines or identifies technical terms, abbreviations, and acronyms used in this guide.

ASCII

Acronym for American Standard Code for Information Interchange. A text file containing only characters from the ASCII character set (usually created with a text editor, such as Notepad in Microsoft® Windows®), is called an ASCII file.

BIOS

Acronym for basic input/output system. Your system's BIOS contains programs stored on a flash memory chip. The BIOS controls the following:

- Communications between the microprocessor and peripheral devices, such as the keyboard and the video adapter
- Miscellaneous functions, such as system messages

CLI

Abbreviation for command line interface. A CLI displays a prompt, the user types a command on the keyboard and terminates the command (usually with the Enter key), and the computer executes the command, providing textual output.

CLI mode

The method by which you can install Dell™ Update Packages (DUPs) from a script in silent/unattended mode.

Dell OpenManage Server Administrator

Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services. It resides solely on the system being managed and is accessible both locally and remotely from the Server Administrator home page. Remotely monitored systems may be accessed by dial-in, LAN, or wireless connections. Server Administrator ensures the security of its management connections through role-based access control (RBAC), authentication, and industry-standard secure socket layer (SSL) encryption.

device driver

A program that allows the operating system or some other program to interface correctly with a peripheral device, such as a printer. Some device drivers—such as network drivers—must be loaded from the **config.sys** file (with a device= statement) or as memory-resident programs (usually from the **autoexec.bat** file). Others—such as video drivers—must load when you start the program for which they were designed.

digital signature

A digital signature is used to authenticate the identity of the signer of a document and to certify that the original content is unchanged. It is an encryption scheme for authenticating digital information and is implemented using techniques from the field of public-key cryptography.

DOS

Acronym for Disk Operating System.

DRAC

Acronym for Dell Remote Access Controller.

DTK

Acronym for Dell OpenManage™ Deployment Toolkit. DTK includes a set of utilities for configuring and deploying Dell systems and is designed for users who need to build scripted installations to deploy large numbers of servers in a reliable fashion without having to dramatically change their current deployment processes. In addition to the command line utilities used to configure various system features, DTK also provides sample scripts and configuration files to perform common deployment tasks and documentation. These files and scripts describe the use of DTK in Microsoft Windows Preinstallation Environment (Windows PE) and embedded Linux environments.

ESM

Abbreviation for Embedded Systems Management.

firmware

Software (programs or data) that has been written onto read-only memory (ROM). Firmware can boot and operate a device. Each controller contains firmware that helps provide the controller's functionality.

GUI

Acronym for graphical user interface.

Interactive mode

The method by which you can install DUPs interactively through a GUI.

IPMI

Acronym for Intelligent Platform Management Interface. The Intelligent Platform Management Interface (IPMI) specification defines a set of common interfaces to computer hardware and firmware, which system administrators can utilize to monitor the system health and manage the system.

ITA

Acronym for Dell OpenManage IT Assistant. ITA provides a central point of access to monitor and manage systems on a local area network (LAN) or wide area network (WAN). It helps you to identify the groups of systems that you want to manage remotely and provides a consolidated view of all systems, giving you a central launch point for managing these systems.

PERC

Expandable RAID controller. A RAID controller is a device which manages the physical storage units in a RAID system, and presents them to the computer as logical units.

pre-operating system environment

A shell environment used to configure system hardware before a major operating system, such as Microsoft Windows or Linux, is installed.

RAID

Acronym for redundant array of independent disks.

repository

Repository is a database on the *Dell Server Updates* DVD that contains the updated BIOS, firmware, and driver components for Dell systems. The repository organizes these components into sets of updates for each supported system that, when applied, updates at one time all system components that require updates. Alternately, you can browse the repository for updatable systems and components without running the update application. You can access the repository for both Windows and Linux systems on the *Dell Server Updates* DVD.

SEL

Acronym for Microsoft Windows System Event Log.

SUU

Acronym for Dell OpenManage Server Update Utility. SUU is one of the applications used for identifying and applying updates to your system. You can use SUU to update your Dell system or to view the updates available for any system supported by SUU. SUU compares the versions of components currently installed on your system with update components packaged on the *Dell Server Updates* DVD. It then displays a comparison report of the versions and provides the option of updating the components.

System Software Component

Software elements requiring update to a desired software version for efficient patch management. The following list includes components which are updated:

- System BIOS
- System firmware, also known as Embedded Server Management (ESM) firmware
- Dell Remote Access Controller (DRAC) firmware
- PowerEdge™ Expandable RAID Controller (PERC) firmware and device drivers
- Network interface card (NIC) drivers

For the current list, see the Dell Support website at **support.dell.com**.

Trusted Platform Module (TPM)

A security hardware that provides hardware–based root of trust and can be leveraged to provide a variety of cryptographic services, such as early–boot component checking. BitLocker™ uses a TPM v1.2 with a TCG–compatible BIOS to check and validate the integrity of critical early boot components.

Unicode

A fixed width, 16-bit worldwide character encoding, developed and maintained by the Unicode Consortium.

Index