




Dell Update Packages User's Guide



Notes, cautions, and warnings

-  **NOTE:** A NOTE indicates important information that helps you make better use of your product.
-  **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
-  **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2016 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2016 - 10

Rev. A00

Contents

1 Getting Started.....	5
What's new in this release.....	5
DUP event viewer.....	5
Zip pack elimination.....	5
Slot information for hard drive.....	6
Dependency.....	6
Supported Operating Systems.....	6
Prerequisites.....	6
Prerequisites And Features For Systems Running Linux.....	6
Dell-Qualified and Dell-Enabled Packages.....	6
Prerequisites and Features for Systems Running Windows.....	6
Downloading DUPs.....	7
Downloading DUPs through Repository Manager.....	7
Installing Device Drivers.....	8
Interactive Mode.....	8
Non-Interactive Mode.....	8
Installation Order of DUPs.....	8
Best practices for using DUPs.....	9
Other Documents You May Need.....	9
Contacting Dell.....	9
2 Using Dell Update Packages.....	10
Updating Packages Component and System Compatibility.....	10
Executing DUPs in Linux Environment.....	10
Interactive Mode.....	10
Non-Interactive Mode.....	10
Verifying the Digital Signature.....	11
Executing DUPs On Systems Running Windows.....	11
Verifying the Digital Signature On Systems Running Windows.....	12
Compatibility checking.....	12
Information while applying the Updates on a Running System.....	12
System Reboot Required.....	12
Saving Console Output for Linux.....	13
Delivering DUPs to the Systems.....	13
Updating Multiple Systems.....	13
Remote Terminal Sessions.....	13
Stand-Alone Systems and Firewalls.....	13
Confirming the Update.....	13
3 Update and Rollback in Lifecycle Controller Enabled Server.....	15
Update in Lifecycle Controller.....	15
Rollback in Lifecycle Controller.....	15



4 Command Line Interface Reference.....	17
Linux CLI Options.....	17
Windows CLI Options.....	18
Exit Codes for CLI.....	20
5 Linux Troubleshooting.....	22
Known Issues.....	22
Diagnostic Tasks Will Not Run While a DUP Reboot is Pending.....	22
Abnormal Termination of a DUP.....	22
Error While Loading Shared Libraries.....	22
Insufficient Free Physical Memory to Load the BIOS Image.....	22
Kernel Panic While Running Storage Controller Firmware Update Packages.....	22
Loss of Functionality While Renaming Linux DUPs.....	23
DUPs Fail on 64-bit Red Hat Enterprise Linux Operating System.....	23
DUP Update of Firmware Might Fail While Running in the UEFI Mode.....	23
Messages.....	23
DUP Message Logs.....	28
Message Location.....	29
Messages Log Files.....	29
6 Troubleshooting for Systems Running Windows.....	30
Known Issues.....	30
Inventory Failure.....	30
Messages.....	30
DUP Message Logs.....	32
Message Location.....	32
Messages Log Files.....	32
7 Trusted Platform Module and BitLocker Support.....	34
8 Microsoft Windows Server 2008 User Account Control.....	36
UAC Restrictions When Running DUPs Remotely.....	37
9 Frequently Asked Questions.....	38



Getting Started

A Dell Update Package (DUP) is a self-contained executable in a standard package format that updates a single software element on the system.

Using DUPs, you can update a wide range of system components and apply scripts to similar sets of Dell systems to bring the system components to the same version levels.

 **NOTE: On Dell's 12th and 13th generation of PowerEdge servers, iDRAC and Lifecycle Controller has common DUP update.**

 **NOTE: OS Collector inventory and update support available with Dell's 12th and 13th generation of PowerEdge servers.**

You can use DUPs to:

- Apply an individual update to a system by using an interactive command line interface (CLI).
- Install device drivers in interactive and non-interactive modes.
- Execute multiple updates on the system by using a script comprised of non-interactive commands that you write using the CLI feature.
- Leverage the scheduling of your operating system and software distribution utilities to apply updates remotely to any number of systems.

What's new in this release

This release of Dell Update Package (DUP) supports Microsoft Windows Server 2016 (64-bit) and Red Hat Enterprise Linux 6.8 Server (64-bit).

 **NOTE: For detailed information on various Dell systems and operating systems on which DUP is supported, see the *Dell Systems Software Support Matrix* at dell.com/openmanagemanuals.**

DUP event viewer

The event viewer log captures the DUP execution status along with the details of that particular component which updated.

For Windows operating systems DUP generates the event log in the event viewer <application logs> folder and the corresponding instances get generated.

For the Linux operating systems DUP generates the event log in the </var/log/messages> folder.

The log instance provides details of different performance parameters like Exit Code, DUP log location and name details.

Zip pack elimination

DUP facilitates you to extract the contents of the DUP payload and other contents in an existing folder or a defined location.



Slot information for hard drive

DUP provides specific information about the hard drive location detail with the slot number, storage controller, enclosures and other particulars. The details of the slot information are also captured in the DUP log files.

Dependency

DUP supports the following dependencies:

- Soft Dependency — Dependency(s) that needs to be applied in order to use certain new features coming with the update. For example, when the features of BIOS 1.7 are enabled only when iDRAC is at 2.3 then the dependency on iDRAC version is a soft dependency and the BIOS update would be applied but the specific features would not be available till iDRAC is at least 2.3.
- Hard Dependency — Dependency(s) that must be applied in order to apply the correct update. For example, the update for upgrading BIOS to 1.7 might require iDRAC version to be at least 2.0. Then user needs to update iDRAC version to 2.0 before updating BIOS 1.7.

 **NOTE: In certain scenarios, for a complete update or upgrade, you have to install two and more DUPs. In such scenarios, sometimes you have to restart the system to complete the update of previously installed DUPs.**

Supported Operating Systems

For detailed information on various Dell systems and operating systems on which DUP is supported, see the *Dell Systems Software Support Matrix* at dell.com/openmanagemanuals.

Prerequisites

Before you install and use DUPs, ensure that:

- The system and operating system is supported by DUPs. See [Supported Operating Systems](#) for more information.
- You have administrator privileges.

Prerequisites And Features For Systems Running Linux

This section lists all the prerequisites and features for systems running the Linux operating system.

Dell-Qualified and Dell-Enabled Packages

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

- Add executable privileges to the package filename. Type the following command: `chmod +x packagename.bin`.
- Verify that the package meets the prerequisites for performing an update. To perform the check, type: `./packagename.bin -c`.
- Utilize one of the following methodologies for performing the updates. The first method is called the Single update method. In this method, **Run** the DUP from the command line in interactive mode to perform the update. The other method is called the Script method. Use this method if you want to run one or more updates from a script in non-interactive mode.

Prerequisites and Features for Systems Running Windows

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

 **NOTE: Run the DUP Check option on the target system and ensure that the system meets the prerequisites for performing an update.**

To run the check from the CLI, type: `packagename.exe /c /s`.

To run the check from the GUI:

1. Double-click the **.exe** file for the DUP you downloaded.
2. 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 older version prior to DUP 7.2 framework is `%SystemDrive%\dell\updatepackage\log`.

The paths of the log files from 7.2 DUP framework are:

Windows Server 2008 and Windows Server 2012: `%SystemDrive%\Program Data\Dell\UpdatePackage\log`.

3. Determine that the target system meets compatibility requirements.
For more information, see the Dell OpenManage Legacy Compatibility Guide, the Dell Systems Software Support Matrix, and [Other Documents You May Need](#).
4. Create a directory structure for performing the updates.
5. Determine a methodology for performing the updates. The first method is Single update method. In this method, Run DUP from the command line in interactive mode to perform the update. The other method is Script method. Use this method if you want to run one or more updates from a script in non-interactive mode.

 **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.**


Downloading DUPs

You can download DUPs from www.dell.com/support.

 **NOTE: DUPs are also available in the repository folder in the Dell OpenManage Server Update Utility DVD, along with the `Catalog.xml` (that contains information about both Windows and Linux DUPs) and `DellSoftwareBundleReport.html` files.**

To download DUPs from www.dell.com/support:

1. Go to www.dell.com/support and select **Support for Work**.
2. Type the **Service Tag** and click **submit**.
3. Select **Drivers and Downloads**.
4. Select the operating system, category, and the update importance.
The list of applicable updates are displayed.
5. Click **Download**.
6. To complete downloading the file, follow the instructions on the screen.

 **NOTE: You can also download a different file format from the File Title column by selecting a file format for the DUP and clicking it. In case you want to download more than one file type, you must do it one at a time.**

 **NOTE: You can also download a DUP or group of DUPs using Dell Repository Manager. See the *Dell Repository Manager User's Guide* for more information.**

Downloading DUPs through Repository Manager

You can download DUPs from Dell Repository Manager.

1. In the **Dell Repository Manager** window, click **My Repositories** tab.
2. Click **New → Create New Repository**.
The **Create Repository** window is displayed.
3. Type the **Name** and **Description**.
4. Click **Next**.
The **Base Repository** window is displayed.



 **NOTE: Click Cancel at any time to exit without creating a new repository.**

5. Select a source for the repository.

 **NOTE: You can also click on Help menu and choose the option: Import Repository from Catalog file...**

6. Select and open from the repository list displayed.
7. Click on the **Components tab** to view the list of DUPs available.
8. Choose any or all of the DUPs displayed.
9. Click on **Download File**. Provide the path and click **OK**.
10. The selected DUPs appear in the **Job Queue**.
11. Once completed the DUPs are available in path provided.
12. You can update the components using DUPs.

 **NOTE: See the DRM user's guide for more information from openmanagemanuals.com.**

Installing Device Drivers

DUPs update BIOS, firmware, drivers, and applications. If a device driver is not present in the system, DUPs allow you to perform fresh installation of the driver. You can install the driver provided the supported hardware is present.

Interactive Mode

In an interactive mode, if a fresh installation 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 installation is applicable, executing DUPs with the **/s** switch installs the driver.

For example, `packagename.exe /s` and `packagename.exe /s /r` performs fresh installation of driver DUPs.


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

Installation Order of DUPs

If you are installing multiple DUPs, install the updates that require a reboot at the end. For recommended installation order see the following table.

Table 1. Update Packages: Recommended Installation Order

Installation Order	System Software Components
1	Device driver
2	Device firmware
3	ESM firmware
4	Lifecycle Controller
5	BIOS

 **NOTE: If you have updated the BIOS, power supply firmware, PERC firmware, PCIeSSD firmware, Mellanox, Emulex firmware and driver, chipset and video drivers, Intel, QLogic and Broadcom firmware the changes to the components take effect only after you reboot the system. On 13G systems, the SAS expander firmware does not require a reboot.**

 **NOTE: For a single reboot, install the ESM firmware update before the BIOS update.**

 **NOTE: On 13G systems, the iDRAC and Lifecycle Controller has common DUP update.**

Best practices 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 of any issues.
- Make sure that you have a backup of operating system files or system configuration files stored on a system other than the one you are updating.
- Make sure that the updates are 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.
- On a Microsoft Hyper-V virtual machine, while updating the host operating system components, ensure that the guest operating systems are not running.
- Do not shut down the system while an update is in progress.
- Make sure that the system reboots without power interruption after performing a BIOS update.
- Do not close any terminal console windows used for performing the DUP CLI execution, while DUP executions are in progress.

Other Documents You May Need

To access other documents go to dell.com/support/manuals and select the product or use the direct link on the *Dell Systems Management Tools and Documentation DVD*.

- *Dell OpenManage Legacy Compatibility Guide*

 **NOTE: You do not need to install Dell OpenManage Server Administrator on the system to run DUPs.**

- *Dell OpenManage Server Update Utility User's Guide*
- *Dell OpenManage Deployment Toolkit (DTK) User's Guide*
- *Dell OpenManage Essentials User's Guide*
- *Dell Systems Software Support Matrix*
- *Glossary*
- *Dell Repository Manager Users Guide*
- *Dell OpenManage Chassis Management Controller User's Guide*

Contacting Dell

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

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.



Using Dell Update Packages

Dell provides a number of aids to help you determine whether or not the system requires an update. You can download DUP from dell.com/support/manuals. For more information, see [Downloading DUPs](#).

Updating Packages Component and System Compatibility

You can run the DUP and read the summary information. This information is provided to help you determine whether the update is appropriate for the system and specific environment.

Executing DUPs in Linux Environment

You can run DUPs from the console in two modes:

- interactive
- non-interactive

Interactive Mode

In the interactive mode, you issue a command, and the interface prompts you for permission to continue executing the command. When you execute a package in this mode, it first displays a scrollable view of the release notes for the package. You may view these notes before continuing with the execution of the package.

DUP may be executed from a local console attached to the target system or from an administrator's workstation by using a remote shell, such as *ssh*. Once a package has been delivered to the target system, administrators can execute the package by performing the following:

- Type `./packagename.bin` from the working directory.



NOTE: Where packagename is the model and component-specific name of the package

- Ensure that the `.bin` file has the appropriate permissions set and that a user account with **root** privileges to executes the update.
- The progress and status is displayed to the console (**stdout**) and log its activity to `/var/log/messages`.

Non-Interactive Mode

Non-interactive mode is essential when executing a script for applying DUPs to multiple systems. When applying DUPs to multiple systems, you cannot answer yes or no during script execution.

- Type `-q` for non-interactive mode.
- `-f` for force.
- `-r` for reboot if a reboot is required for the type of update being performed.

In the following command example, the command applies a BIOS DUP without any user confirmation, forces the execution in the case of a downgrade from a more recent BIOS version, and reboots the system after the DUP is applied. This command is executed provided the DUP satisfies all the system and version requirements.

```
BIOS_XR23Y_LN_1.2.8.BIN -q -f -r
```

For more information on 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 provide a 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.

 **NOTE: Verifying the digital signature is applicable for systems running Windows and Linux.**


Verifying the Digital Signature on Systems Running Linux

If you do not already have it installed on your system, you must install the Gnu Privacy Guard (GPG) to verify a Linux DUP digital signature. To use the standard verification procedure, perform the following steps:

1. Get the Dell Linux public GnuPG key, if you do not already have it. You can download it by navigating to lists.us.dell.com and clicking the **Dell Public GPG key** link.
2. Import the public key to the **gpg** trust database by running the following command: `gpg --import <Public Key Filename>`

 **NOTE: You must have a private key to complete the process.**

3. To avoid a distrusted-key warning, validate the public key by its fingerprint before you use it.
 - a. Type the following command: `gpg --edit-key 23B66A9D`
 - b. In the GPG key editor, type **fpr**. The following message appears: `pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group) <linux-security@dell.com> Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D`. If the fingerprint of the imported key is the same as the key owner's, you have a correct copy of the key. You can verify the key's owner in person, over the phone, or by any other means that guarantees that you are communicating with the key's true owner.
 - c. While still in the key editor, type **sign**.
 - d. Answer the list of trust-validation questions that appear and create a passphrase to use as the secret key. You must import and validate the public key only once.
4. Obtain the Linux DUP and its associated signature file from dell.com/support/manuals/downloads.

 **NOTE: Each Linux DUP has a separate signature file, which is displayed along with the DUP. You need both the DUP and its associated signature file for verification. By default, the signature file is named the same as the DUP filename with a `sign` extension.**

5. Verify the DUP using the following command: `gpg --verify <Linux Update Package signature filename> <Linux Update Package filename>`.

Executing DUPs On Systems Running Windows

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. Check the DUP inventory report for Package version and installed versions of component.
4. Click **Install** to install the DUP.
5. Reboot the system, if necessary.

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



Verifying the Digital Signature On Systems Running Windows

To verify the Update Package's digital signature:

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. If this tab is not displayed, the Update Package is not signed.
5. Select the signature from the signature list, and click **Details**.
The **Digital Signature Details** window appears.

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

6. Read the digital signature information to verify that the digital signature is **OK**.
7. Click **OK** to close the window.

Compatibility checking

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

- The logged-on user has root privileges.
- DUP to be applied in the command is compatible with the target system and the operating system running on a system.
- The device associated with the DUP is present on the system.
- The minimum required versions of related system software are running on the 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. DUPs also check for dependencies between BIOS and certain ESM packages. The application design allows you to create groups of DUPs and apply them to a wide range of systems. Additionally, if you only want to verify that a given package can be applied to the system, you can invoke the package by using the following CLI command:

```
./Packagename.bin -c for Linux
```

```
packagename.exe /c /s for Windows
```

This command executes the dependency rules within the DUP, issues any warnings, exits without applying the update to the system, and writes the results to the console. You can also use the DUP to set an exit code to perform decisions within the scripts.

Information while applying the Updates on a Running System

This section describes all the effects of applying the updates on a running system.

System Reboot Required

Certain packages, 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, for example, through a power interruption, you must repeat the updates. Therefore, it is recommended that you schedule updates for a time when the reboot can take place immediately after you apply the last update.

Saving Console Output for Linux

As the DUPs are executed, messages are printed to the console. To redirect console output, use the following syntax with interactive commands:

```
./packagename.bin|tee -a logname.lo
```

The **|tee** specifies the output from the DUP to be sent to both the console and to a log file. The **-a** switch ensures that the output is appended to a file, protecting any previous log file output from being overwritten.

Delivering DUPs to the Systems

The DUP application does not provide scheduling and delivery of the packages to multiple systems. You must rely on third-party or native operating system applications to accomplish script execution and distribution on multiple systems.

Updating Multiple Systems

For large environments that consists of multiple systems, remote software distribution applications provide the best solution. Many of these tools can effectively leverage the DUP 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 also are an effective method of making DUP accessible in a distributed environment. When a DUP begins execution, it first copies the contents of the package to a temporary location on the local drive of the system. 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 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 the 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 or that have firewall which block user downloads, you need to download DUP from dell.com/support by using a system that has Internet access, such as desktop or portable computer. You can make DUP available to the system by copying them onto removable media that the system supports.

Confirming the Update

To ensure that the DUPs were applied to the system, review the console output that was generated during execution. For detailed information about the messages, see [Linux Troubleshooting](#).

If you want to revert to a previous (older) version of the software after updating to a newer version, you must download the appropriate DUP from dell.com/support/manuals and install it.

For Systems Running Linux:

To install the previous version from a script, use **-q** (unattended) mode. In addition, you must use the CLI **-f** option, which forces the downgrade.

 **NOTE: If the system loses power during the update process, you must perform the updates again.**



 **NOTE:** DUPs for Linux can also be found in the repository on the *Dell OpenManage Server Update Utility DVD* that contains the updated BIOS, and firmware components for Dell systems. For more information, see the *Dell OpenManage Server Update Utility User's Guide* available at dell.com/support/manuals.

For Systems Running Windows:

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. You are prompted to ensure that you want to install an earlier version.

Update and Rollback in Lifecycle Controller Enabled Server

Dell Lifecycle Controller Enabled Server is an embedded configuration utility that enables systems and storage management tasks from an embedded environment throughout the life cycle of a system.

Residing on an embedded flash memory card, Lifecycle Controller 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 Lifecycle Controller, you can quickly identify, download, and apply system updates without searching the Dell Support website. You can also configure the system BIOS and system devices (such as NIC, RAID, and iDRAC), deploy an operating system, and run diagnostics to validate the system and the attached hardware.

 **NOTE: For information on update and rollback for iDRAC, see Integrated Dell Remote Access Controller 8 (iDRAC8) Version 2.00.00.00 Users Guide available at dell.com/esmmanuals.**

 **NOTE: Certain platforms or systems may not support the full set of features provided by Lifecycle Controller.**

Update in Lifecycle Controller

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

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

- The Dell File Transfer Protocol (FTP) system (**ftp.dell.com**). You can use a proxy system 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 Lifecycle Controller. For more information on updating the platform, see the *Dell Lifecycle controller User Guide* available at **dell.com/support/manuals**.

After you select the updates you want to apply, Lifecycle Controller downloads and applies the updates. If you decide to update any device in Lifecycle Controller, 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 Lifecycle Controller

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

Lifecycle Controller supports platform firmware rollback to the previous version. If the operating system has a non-functioning application because of a BIOS or firmware flash, reboot to Lifecycle Controller and roll back to the previous version.

 **NOTE: The BIOS and firmware can be only rolled back. The Lifecycle Controller application, the Dell Diagnostics application, and drivers required for operating system installation cannot be rolled back to an earlier version.**

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





NOTE: Rollback is not supported in the operating system environment. To enable rollback, ensure that you boot into Lifecycle Controller.

Command Line Interface Reference




You can display information about the CLI options by typing the DUP name and either **-h** or **--help** at a command line prompt.




The console displays all of the command line options and provides help for each choice.

Linux CLI Options

For a list of CLI options for systems running Linux, a description of each option, and the command syntax see the following table:

Table 2. Linux CLI Options: Usage

CLI Option	CLI Task Description	Command Syntax
(no option; run command without options) Run commands in an interactive mode.	Apply the DUP in an interactive mode; the DUP interacts with the user if it is valid.	<code>./packagename.bin</code>
-h or --help Help option	Display command line options and help information. The --help option executes before all other -- options.	<code>./packagename.bin -h</code> <code>./packagename.bin --help</code>
	 NOTE: This option exits after displaying the requested information; no DUP verification or updates occur.	
-c Check option	Determine if the update can be applied to the target system.	<code>./packagename.bin -c</code>
-f Force option	Force a downgrade or update to an older version. The -q option is required when using the -f option.	<code>./packagename.bin -q -f</code>
	 NOTE: Before downgrading the software to a previous version, refer to the documentation of the previous version.	
--list List package contents option	Display all files that are contained in the DUP.	<code>./packagename.bin --list</code>
	 NOTE: This option exits after displaying the requested information; no DUP verification or updates occur.	
-q Run command in non-interactive mode	Execute the DUP silently without user intervention.	<code>./packagename.bin -q</code>

CLI Option	CLI Task Description	Command Syntax
-r Reboot option	Reboot the system, if required, after performing the update. The reboot does not occur: <ul style="list-style-type: none"> If the DUP fails or is not applicable to the target system. If the DUP does not require the target system to be rebooted. <p> NOTE: The -q option is required with this option.</p>	<code>./packagename.bin -r -q</code>
-v, --version Display version option	Display the version, fixes, enhancements, and release date; lists systems to which the DUP can be applied. <p> NOTE: This option exits after displaying the requested information; no DUP verification or updates occur.</p>	<code>./packagename.bin -v</code> <code>./packagename.bin --version</code>
--extract <path>	Extract all files contained in the DUP to the path you specify. If the directory specified in the path does not exist, it is created. <p>If the path contains spaces, use quotation marks around the <path> value.</p> <p> NOTE: This option exits after extracting the requested files; no DUP verification or updates occur.</p>	<code>./packagename.bin --extract /update</code> <code>./packagename.bin --extract "/update files"</code>

Windows CLI Options

For a list of the CLI options for systems running Windows, a description of each option, and the command syntax see the following table.





 **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. For information on log files, see [DUP Message Logs](#).**

Table 3. Windows CLI Options: Usage

CLI Option	CLI Task Description	Command Syntax
/? or /h Help option	Displays command line options and help information.	<code>packagename.exe /?</code> <code>packagename.exe /h</code>
/c Check option	Determines if the update can be applied to the target system. <p>The /s option is required with this option.</p> <p>Options /f, /e, and /r are not valid with this option.</p>	<code>packagename.exe /s /c /l=c:\pkg.log</code>

CLI Option	CLI Task Description	Command Syntax
	When you click Install in the graphical user interface (GUI) mode, the same checking process is performed.	
/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.	<code>packagename.exe /s /e=c:\update</code> <code>packagename.exe /s /e="c:\update files"</code>
/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.	<code>packagename.exe /s /f /l=c:\pkg.log</code>
/l=<filename> Log option	Appends logged messages to a specified ASCII file; creates a new file if one does not exist.  NOTE: If the file name contains spaces, use quotation marks around the <filename> value.	<code>packagename.exe /s /l=c:\pkg.log</code> <code>packagename.exe /s /l="c:\Update Log \pkg.log"</code>
/r Reboot option	Reboots the system, if required, after performing the update. The reboot does not occur: <ul style="list-style-type: none"> • 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.	<code>packagename.exe /s /r /l=c:\pkg.log</code>
/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.	<code>packagename.exe /s /l=c:\pkg.log</code>



CLI Option	CLI Task Description	Command Syntax
	 NOTE: Using the /s option causes all output to be written to log files.	
<u>/u=<filename></u> 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.	<pre>packagename.exe /s /u=c:\pkg.log</pre> <pre>packagename.exe /s /u="c:\Update Log \pkg.log"</pre>

Exit Codes for CLI

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

After running DUPs, see the exit codes described in the following table.

Table 4. Exit Codes

Value	Message Name	Display Name	Description
0	SUCCESSFUL	Success	The update was successful.
1	UNSUCCESSFUL (FAILURE)	Unsuccessful	An error occurred during the update process; the update was not successful.
2	REBOOT_REQUIRED	Reboot required	You must restart the system to apply the updates.
3	DEP_SOFT_ERROR	Soft dependency error	Some possible explanations are: <ul style="list-style-type: none"> You attempted to update to the installed 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	Hard dependency error	The required prerequisite software was not found on the system. The update was unsuccessful because the system 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.
5	QUAL_HARD_ERROR	Qualification error	The DUP is not applicable to the system. Some possible explanations are: <ul style="list-style-type: none"> 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	Rebooting system	The system is being rebooted.
9	RPM_VERIFY_FAILED	RPM verification has failed	The Linux DUP framework uses RPM verification to ensure the security of all DUP dependent Linux utilities. If security is compromised, the framework displays a

Value	Message Name	Display Name	Description
			<p>message and an RPM Verify Legend, and then exits with exit code 9.</p> <p>RPM produces output <i>only</i> if there is a verification failure. The format of the output is:</p> <pre>.SM5DLUGT 'utility name'</pre> <p>For example, if the <i>fmt</i> command is compromised, the framework displays the message:</p> <pre>rpm verify failed: .M..... /usr/bin/fmt</pre> <p>RPM Verify Output Legend:</p> <ul style="list-style-type: none"> .- Verification test passed S- File Size differs M- Mode differs (includes permissions and file type) 5- MD5 sum differs D- Device major/minor number mismatch L- ReadLink(2) path mismatch U- User ownership differs G- Group ownership differs T- mTime differs
13	UPDATE_SUCCESSFUL_SOFT_DEPENDENCY_NOT_MET	Update is successful. Soft Dependencies are not met.	The applied update is successful. The soft dependencies, which enable all the features of the updated software are not met. Apply the dependent updates for getting the full features.
14	REBOOT_REQUIRED_SOFT_DEPENDENCY_NOT_MET	Update is successful. Reboot is required. Soft Dependencies are not met.	The update is successful. Reboot is required to complete the update. The soft dependencies, which enable all the features of the updated software are not met. Apply the dependent updates after reboot for getting the full features.
15	CONTAINER_POWER_CYCLE_REQUIRED	Update is successful. Container power cycle is required for update to be applied.	To enable the update the container power cycle operation is required to be applied.
16	CONTAINER_POWER_CYCLE_REQUIRED_SOFT_DEPENDENCY_NOT_MET	Update is successful. Container power cycle is required for update to be applied. Soft dependencies are not met.	Container power cycle is required for the update to be applied.



Linux Troubleshooting

This section describes possible troubleshooting steps related to Linux Operating System.

Known Issues

The issues listed below are known issues and corrective actions for Dell Update Packages (DUPs) for Linux operating systems. Also see the corresponding *Readme for Linux* at dell.com/support/manuals.

 **NOTE: The Readme file, which is available at dell.com/support/manuals, provides the latest information regarding known issues.**

Diagnostic Tasks Will Not Run While a DUP Reboot is Pending

If you try to run a diagnostic task and there are pending updates, the diagnostic task fails.

To resolve this, complete all pending updates, reboot the system and then run a diagnostic task.

Abnormal Termination of a DUP

A DUP may stop abruptly due to a power outage or abnormal termination.

To resolve this:

1. Remove the lock file from the lock folder.
2. Type the command: `rm -f /var/lock/.spsetup`.
3. Run the DUP again to reapply the update.

Error While Loading Shared Libraries

The following error may be displayed when you load shared libraries. **Error while loading shared libraries: libstdc++.so.5: Cannot open shared object file: No such file or directory.**

To install the compatibility libraries, using the following command: `RPM -ih compat-libstdc++-33-3.2.3-47.3.i386.rpm`.

Insufficient Free Physical Memory to Load the BIOS Image

BIOS updates require 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 DUP for the BIOS may fail. To resolve, the BIOS can be updated using UEFI-based update utility or Lifecycle Controller Platform Update option, run the DUP after adding more memory or immediately after a reboot.

Kernel Panic While Running Storage Controller Firmware Update Packages

Linux systems running one or more applications that interact with SCSI devices in certain ways are known to cause a kernel panic situation.

To resolve this, stop the Dell OpenManage Server Administrator and Dell OpenManage Server Administrator Storage Management Service before running the storage controller firmware DUPs.

Loss of Functionality While Renaming Linux DUPs

Linux DUPs can be executed even if they are renamed, but some functionality is lost. Renamed Linux DUPs with extensions that are in the Linux MIME (Multimedia Internet Message Extensions) database could fail to execute from various X-Windows desktops, for example GNOME. In this case the desktop issues a file open error message indicating that the DUP cannot be opened. This occurs if a DUP with an uppercase **.BIN** extension is renamed to a lowercase **.bin** extension. The **.bin** extension has an entry in the Linux MIME database which leads to the file open error.

DUPs Fail on 64-bit Red Hat Enterprise Linux Operating System

If DUPs fail to run on a 64-bit Red Hat Enterprise Linux operating system, manually install the following RPMs:

- `compat-libstdc++-33.i686`
- `libstdc++-4.4.4-5.el6.i686`
- `libxml2.i686`

 **NOTE: The RPMs are available on the Red Hat Enterprise Linux 6.3 x64 media.**

DUP Update of Firmware Might Fail While Running in the UEFI Mode

When Red Hat Enterprise Linux 6 or SLES 11 is installed and booted in a UEFI environment, flashing firmware using DUP might fail after DUP reboots the system.

DUP relies on a warm reset to enable firmware flashing. In the UEFI mode, the kernel by default performs a cold reset.

Boot the system with the `reboot=k` kernel command line option to enable the firmware flashing procedure to complete successfully. You could add this to `/etc/grub.conf` to be persistent across reboots.

 **NOTE: Using the `reboot=w` option as documented in the Linux Kernel documentation might cause a Kernel Panic to occur on Red Hat Enterprise Linux 6 while the system shuts down.**

Messages

For descriptions and solutions to messages that you may receive when running DUPs, see the following table:

Table 5. Update Packages Message Information

Message	Description/Solution
This Update Package is not compatible with your system Your system: <Model Name> System(s) supported by this package: <Model Name>	Select a compatible DUP, and try the update again.
This Update Package cannot be executed under the current operating system.	DUPs supports Linux operating systems and kernels supported by the <code>--rebuild</code> option.
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>	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.



Message	Description/Solution
<pre>Current version:<version> Required version: <version></pre>	
<pre>You must use the -f option to continue with the update in the non-interactive mode.</pre>	<p>The version of this DUP is either older than or the same as the version installed. To apply the DUP, you must force execution.</p>
<pre>The software to be updated was not found. Install the following software, and then retry the update. Software name: <name> Required version: <version></pre>	<p>The system does not contain the software that matches the DUP.</p>
<pre>The version of this Update Package is newer than the currently installed version. Software application name: <name> Package version: <version> Installed version: <version></pre>	<p>This message confirms the version of the currently installed software before the update is performed.</p> <p>(Using the interactive mode) Type Y or N when prompted to continue.</p> <p>(Using the CLI) Specify the -f option.</p>
<pre>The version of this Update Package is older than the currently installed version. Software application name: <name> Package version: <version> Installed version: <version></pre>	<p>The DUP you selected cannot be installed because a newer version of the software already exists on the system. To install the older version:</p> <p>(Using the interactive mode) Type Y or N when prompted to continue.</p> <p>(Using the CLI) Specify the -f option.</p>
<pre>The version of this Update Package is the same as the currently installed version. <version> Software application name: <name> Package version: <version> Installed version: <version></pre>	<p>The DUP you selected cannot be installed because the same version of the software already exists on the system.</p> <p>(Using the interactive mode) Type Y or N when prompted to continue.</p> <p>(Using the CLI) Specify the -f option.</p>
<pre>This package is not compatible with the version of Server Agent on your system. You must upgrade to Server Administrator before running this package.</pre>	<p>Use an alternative update method from dell.com/support/manuals.</p>
<pre>This update package requires an OpenIPMI driver. Currently no OpenIPMI driver is installed on the system.</pre>	<p>The DUP you selected cannot be installed because you do not have the OpenIPMI driver installed on the system.</p>
<pre>In order to assist in the <update install>, you can download and install a version of the OpenIPMI driver that meets the minimum version requirement from dell.com/support/manuals. The minimum version required is <version>.</pre>	<p>Download and install the minimum required OpenIPMI driver from dell.com/support/manuals.</p>
<pre>This Update Package requires a newer version of the OpenIPMI driver than is currently installed on the system, which is version <version>.</pre>	<p>The OpenIPMI driver that is currently installed on the system does not meet the minimum version requirements of the selected DUP.</p>

Message	Description/Solution
Kernel source for the running kernel is not installed, and the currently installed OpenIPMI driver RPM was installed without the kernel source for the running kernel. In order to install OpenIPMI driver modules for the running kernel that meet the minimum version requirement, you must install kernel source for the running kernel, and then use DKMS (see man page for dkms) to install and build OpenIPMI driver modules for the running kernel. To install kernel source for the running kernel, install the <filename> RPM that is applicable to the running kernel.	Install the kernel source for the running kernel, and then use the Dynamic Kernel Module Support (DKMS) framework to install and build the OpenIPMI driver modules for the running kernel. You must install the kernel source by installing the .rpm file required by the kernel. For information on using DKMS, see the man page for DKMS from linux.dell.com/dkms/manpage.html .
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. After performing a BIOS update, do not power off the system. Reboot the system for the update to take effect.
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.
WARNING: DO NOT STOP THIS PROCESS OR INSTALL OTHER DELL PRODUCTS WHILE <BIOS FRMW> UPDATE IS IN PROGRESS. THESE ACTIONS MAY CAUSE YOUR SYSTEM TO BECOME UNSTABLE.	Do not interrupt DUP execution.
Cannot find utilities on the system to execute package.	The package must have certain utilities to execute.
Make sure the following utilities are in the path:<path>	The utilities named must be in the path mentioned in the message.
File already exists.	The package is attempting to overwrite an existing file.
Rebuilding package <package_name> to support kernel version "kernel.x". This process may take several minutes to complete...	The DUP application is rebuilding the package to support a different kernel version.
No specific kernel version specified! Building support for current kernel...	Unable to determine current system kernel. The DUP application attempts to rebuild the package.
Cannot create directory /extract directory. Please ensure that there is enough space.	Extracting the package to this path requires more disk space than available.
Cannot create temporary file "filename"	The package cannot create the temporary file for a technical reason, such as lack of disk space, permissions, or an existing file.
Unable to create Temp Files. Please ensure that there is enough space in the tmp folder.	The package cannot create temporary files due to lack of space in the tmp folder.
Archive cannot be extracted. Please ensure that there is enough space in the tmp folder.	Insufficient space for extracting the archive.



Message	Description/Solution
Please provide a directory name to extract to.	Provide a directory name for the extracted files.
ROOT directory cannot be used for extraction.	Create a directory for the extracted files.
Successfully extracted to "/extractdir"	The package contents were extracted to the directory you designated.
Cannot find utilities on the system to extract package. Make sure the following utilities are on the path: <path>	Locate the listed utilities and add their directory to the specified path.
Rebuilding Package Failed - Error creating driver support directory.	The package could not be rebuilt because the support directory could not be created.
Rebuilding Package Failed - Error copying kernel modules.	The package could not be rebuilt because the kernel modules could not be copied.
Rebuilding Package Failed - Error re-creating archive.	The package could not be rebuilt because the archive could not be recreated.
Rebuilding Package Failed - Uninstallation of driver was unsuccessful.	The package could not be rebuilt because the driver could not be uninstalled.
Package has been rebuilt successfully.	The package rebuild was successful.
Rebuilding Package Failed - Error creating output package.	Make sure that the directory from which the package rebuild option is being executed is writable.
Rebuilding Package Failed - Error creating wrapper files.	The required wrapper files could not be created.
Output package:	Specifies the name of the output package.
Package execution requires 'root' user privileges.	Log in with root privileges, and try the update again.
Successfully extracted to <target_directory>.	The package is being extracted to the target directory.
Rebuilding package packagename.bin to support 'uname -r'.	DUP is rebuilding the packages to support the running kernel.
This process may take several minutes to complete.	Wait for the process to complete.
Rebuilding Package Failed - Unable to extract package contents.	Unable to extract the contents of the package.
Rebuilding Package Failed - Server Administrator device driver (HAPI) is already installed on the system. Package can be rebuilt only on a system that does not have Server Administrator device driver (HAPI) installed.	Packages cannot be rebuilt on a system that has the HAPI device driver installed.
Unable to Install Dell Instrumentation Driver (HAPI).	The package cannot install the HAPI driver.

Message	Description/Solution
Rebuilding Package Failed - RPM Installation failed with error code=<RPM Install Error Return code>	Provides the RPM error code that prevented the package from being rebuilt.
packagename.bin: Rebuilding Package failed - Unable to extract package contents.	Make sure that there is enough space in the /tmp directory.
packagename.bin: Rebuilding Package - Kernel <kernel-version> is already supported by this package.	You do not have to rebuild this package because you have already customized the package for the kernel. You will only receive this message if you have previously used the --rebuild option and then ran the rebuilt package.
packagename.bin: Rebuilding Package Failed - RPM Installation failed with error code=<LSB_Compliant RPM Install Error Return code>	Check the LSB Compliant RPM error return codes to determine the exact reason for failure.
packagename.bin: Rebuilding Package Failed - Error creating driver support directory.	Make sure that enough space is available in the /tmp directory.
packagename.bin: Rebuilding Package Failed - Error copying kernel modules.	Make sure that enough space is available in the /tmp directory.
packagename.bin: Rebuilding Package Failed - Error recreating archive.	Make sure that enough space is available in the /tmp directory.
packagename.bin: Rebuilding Package Failed - Uninstall of driver was unsuccessful.	The driver could not be uninstalled.
packagename.bin: Rebuilding Package Failed - Error creating files.	Make sure that enough space is available in the /tmp directory.
Package has been rebuilt successfully. Output package: packagename.bin:--CUSTOM.	Package is ready for distribution and execution on production systems with the same running kernel as the system on which it was rebuilt.
Package has been rebuilt successfully.	Package is ready for distribution and execution on production systems with the same running kernel as the system on which it was rebuilt.
packagename.bin: Rebuilding Package failed - Unable to extract package contents.	Make sure that enough space is available in the /tmp directory.
packagename.bin: Rebuilding Package failed - Server Administrator is installed on the system.	Packages cannot be rebuilt on a system that has Server Administrator installed. Uninstall Server Administrator from the system before using the --rebuild option.
The installed operating system version is not supported by this Update Package. To customize this package, see "Rebuilding Packages" in the Update Package User's Guide. In no event shall Dell Inc. be held liable for any direct, indirect, incidental, special, or consequential damages suffered during or after package customization and execution.	The prerequisites for rebuilding the package are present on the system, Dell is not responsible for any problems that may occur if you apply customized packages to the system.
In no event shall Dell Inc. be held liable for any direct, indirect, incidental,	Fully consider this statement before executing a customized package that was enabled by the --rebuild option.



Message	Description/Solution
special, or consequential damages suffered during or after package customization and execution.	
Attempt to update BIOS or firmware to the same version. Update was unnecessary and not applied.	Re-application of BIOS or firmware DUP serves no purpose.
Inventory operation exceeded specified timeout.	Inventory operations have time-out limits as defined in the package's PIEConfig.xml file. Time-out durations are in seconds. If an operation times out, the remainder of the package update is cancelled.
Execution operation exceeded specified timeout.	Execution update operations have time-out limits as defined in the package. Time-out durations are in seconds. If an operation times out, the remainder of the package update is cancelled.
/var/lock directory must exist.	Create this system directory to make sure that package updates do not execute concurrently.
Unable to build a device driver for the running kernel because it is not supported on your system.	Select a compatible DUP and try again.
The Intel IMB driver is currently loaded. Please unload the driver before executing.	Unload the Intel IMB driver before installing the selected DUP.
Warning: The shell less command is not available. When viewing Release Notes, press space to continue viewing notes, q to continue DUP processing.	Continue to view the release notes, or install the less command from operating system media, and re-execute the package interactively.
Press 'q' to exit DUP (--version). Press 'q' to continue with DUP execution (dup dup execution).	The Linux DUP framework uses the Linux utility, <i>less</i> , to display the release notes relevant to the specific firmware or driver release managed by the DUP. When viewing release notes, DUP prompts when executed with the below options: --version: Press 'q' to exit DUP (--version) All other DUP execution: Press 'q' to continue with DUP execution.
Warning: Screen widths of less than <numeric value> can distort the information view.	To optionally correct this, answer < No > to stop package execution. Increase the width of the terminal window to the required size and then re-execute the package interactively.

DUP Message Logs

Logging occurs when you run a command for a DUP. The logs maintain information about all update activities. DUPs write to the Messages log. If you install the same package more than once on the same system, the log is appended. The messages files directory contain messages about a wide range of events on the system. Therefore, you must scan through the log file to find the messages that are relevant to DUPs.

Message Location

The default location of the message log files is **`/var/log/dell/updatepackage/log`**.

Messages Log Files

The messages log file includes the following information

- Date and time the DUP was launched
- Package release ID number
- The full path and filename of the support log generated by the command
- DUP type
- DUP version
- Framework version of the DUP
- Software application name of the DUP
- Version of the currently installed DUP
- Version that the command is trying to apply to the system
- Exit code that results from execution of the command
- Whether a reboot was performed

 **NOTE: The support log files are intended for use by Dell support personnel. Dell encourages you to redirect the DUP output to a file of your choice.**

Troubleshooting for Systems Running Windows

This section describes possible troubleshooting steps related to systems running Microsoft Windows.


Known Issues

The issues listed below are known issues and corrective actions for Dell Update Packages (DUPs) on systems running Windows operating systems. Also see the corresponding *Readme for Windows* at dell.com/support/manuals.

 **NOTE: The Readme file, which is available at dell.com/support/manuals, provides the latest information regarding known issues.**

Inventory Failure

 **NOTE: This issue is applicable to systems running Windows Server 2008 and higher.**

 **NOTE: An in-built feature called User Account Control (UAC) automatically reduces the potential of security breaches for a system running Windows operating system.**

Before you run SUU or DUPs on the system, change the security options in **Group Policy Editor**.

1. Open **Group Policy Editor** using one of the following methods:
 - For Local Group Policy, click **Start** → **Run** → **gpedit.msc**.
 - For Active Directory -based Group Policy Object (GPO), click **Start** → **Run** → **gpedit.msc** and browse to the required GPO.

 **NOTE: Ensure that the system is a member of the domain.**

The **Group Policy Editor** window is displayed.

2. Browse to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
3. Navigate to **User Account Control** → **Behavior of the elevation prompt for administrators in Admin Approval Mode**.
4. Right-click and select **Elevate without prompt**.

Messages

For descriptions and solutions to messages that you may receive when running DUPs, see the following table. Also see the corresponding *Readme for Microsoft Windows* at dell.com/support/manuals.

Table 6. Messages

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>	Select a compatible DUP, and try the update again.

Message	Description/Solution
Systems(s) supported by this package: <system model name>...: <system model name>	
This Update Package cannot be executed under the current operating system.	The operating system is not supported by DUP. For a list of supported operating system check the <i>Dell Systems Software Support Matrix</i> . This document is available at dell.com/support/manuals .
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 dell.com/support/manuals .
Your system exceeds the maximum operating system version supported by this Update Package.	The DUP you selected cannot be installed because the 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>	The system does not contain the software that matches the DUP.
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: In the interactive mode , Click Yes when prompted to continue with the installation. In the CLI mode 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. In 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	Use an alternative update method from dell.com/support/manuals .



Message	Description/Solution
upgrade to Server Administrator before running this package.	
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 an 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 run a command for a DUP. The logs maintain information about all update activities. DUPs write to the Messages log. If you install the same package more than once on the same system, the log is appended. The messages files directory contain messages about a wide range of events on the system. Therefore, you must scan through the log file to find the messages that are relevant to DUPs.

Message Location

The default path for the older version prior to DUP 7.2 framework log file is `%SystemDrive%\dell\updatepackage\log`.

The path of the log files from 7.2 DUP framework are:

Windows Server 2008 and Windows Server 2012: `%SystemDrive%\Program Data\Dell\UpdatePackage\log`.

 **NOTE: User needs to have administrative privilege to see the log files.**

Messages Log Files

The messages log file includes the following information

- Date and time the DUP was launched
- Package release ID number
- The full path and filename of the support log generated by the command
- DUP type
- DUP version
- Framework version of the DUP
- Software application name of the DUP
- Version of the currently installed DUP
- Version that the command is trying to apply to the system
- Exit code that results from execution of the command
- Whether a reboot was performed



NOTE: The support log files are intended for use by Dell support personnel. Dell encourages you to redirect the DUP output to a file of your choice.

Trusted Platform Module and BitLocker Support

A Trusted Platform Module (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 the system, and communicates with the rest of the system using a hardware bus. You can establish ownership of the system and its TPM using the 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 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 the 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 the data is accessible only if the boot components of the system 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: For information on how to turn on BitLocker, see the Microsoft TechNet website. For instructions on how to activate TPM, see the documentation included with the system. 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 the 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).

Microsoft Windows Server 2008 User Account Control

In Microsoft Windows Server 2008 and earlier, user accounts were often members of the local Administrators group and had access to administrator privileges. Members of the local Administrators group install, update, and run software since an Administrator account has system-wide access. When a user is added to the local Administrators group, that user is automatically granted Windows privileges. These privileges provides access to all operating system resources. Hence, user accounts with Administrator privileges posses a security risk by providing access to operating system resources that would 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, user account with administrator privileges.
- Standard User Account, 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, 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 following 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 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 pop-up window for permission by performing any of the following 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 pop-up window 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.
- Dell DUP HDD firmware update utility related to system memory utilization requires minimum of 8 GB to 16 GB RAM in the server.

UAC Restrictions When Running DUPs Remotely

By default, after UAC starts, 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 to launch a DUP remotely.**

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 the 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: The *Dell Systems Software Support Matrix* available at dell.com/support/manuals 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: If your operating system is not supported by the DUP, then the update must be applied Out-of-band using either iDRAC , LC or a Bootable ISO created using Dell Repository manager.

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

Answer: Make sure 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. For more information, see the documentation for the tool.

Question: Where can I find the error messages generated by a DUP that is running in an 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 [Messages Log Files](#).

The Package log file resides in the following default directory: %SystemDrive%\Program Data\Dell\UpdatePackage\log

Windows Server 2008 and Windows Server 2012: %SystemDrive%\Program Data\Dell\UpdatePackage\log.

The Windows SEL is available through the Windows Event Viewer.

Question: If you are updating the Power Supply, it may take some time to apply. What do I need to do?

Answer: While updating for the Power Supply from DUP, it may take sometime for the updates to apply. It is critical that the system is not unplugged, restarted or turned on, as the system switches to sleep mode for sometime to complete the update. Wait until the process is completed.

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 the system BIOS from **dell.com/support** and install it. If a DUP is not available, use one of the other formats on **dell.com/support**.

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

Answer: The BIOS update is applied only after you restart the 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 the system at the same time. For information about the update order, see [Installation Order of DUPs](#).

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

Answer: You can check **dell.com/support** for updates or register for the File Watch Service at **dell.com** to receive automatic notification for upgrades to the 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: In case you are facing issues with the CLI mode, 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. For details on which commands can be used together for different operating system, see [Command Line Interface Reference](#) .

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 Signature** 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 on Windows](#) for additional information.