

Dell™ Lifecycle Controller

Version 1.3

User 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.

© 2009 Dell Inc. All rights reserved.

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

Trademarks used in this text: *Dell* and the *DELL* logo are trademarks of Dell Inc.; *Microsoft*, *Windows*, and *Windows Server* are registered trademarks of Microsoft Corporation in the United States and/or other countries; *Red Hat*, *Red Hat Linux*, and *Red Hat Enterprise Linux* are registered trademarks of Red Hat, Inc. in the United States and other countries; *SUSE* is a registered trademark of Novell, Inc. in the United States and other countries; *Intel* is a registered trademarks of Intel Corporation in the U.S. and other countries; *Broadcom* is a trademark of Broadcom corporation.

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

December 2009

Contents

1	Overview	9
	Remote Services	9
	Unified Server Configurator (USC)	10
2	Unified Server Configurator and Unified Server Configurator - Lifecycle Controller Enabled	13
	What's new in USC/USC-LCE 1.3	13
	USC-LCE	14
	USC and USC-LCE Support for:	14
	Common Features	14
	Launching the Product	14
	Using the Wizards	15
	Disabling USC or USC-LCE	17
	Canceling a Request to Enter System Services	17
	Using USC Settings Wizard.	18
	Deploying the Operating System Using the OS Deployment Wizard.	19
	Hardware Diagnostics	27
	Repairing USC	28
	Repairing USC - LCE	28
	How to Upgrade to an iDRAC6 Express Card	29
	Installing the iDRAC6 Express Card	29
	Transferring an iDRAC6 Express Card	30
	Removing the iDRAC6 Express Card	30

Unified Server Configurator - Lifecycle Controller	
Enabled Unique Features	30
Updating USC - LCE	30
Updating the Platform using the Platform Update Wizard	31
Rolling Back to Previous BIOS and Firmware Versions	34
Hardware Configuration	36
Part Replacement	58
Configuring a Local FTP Server	59
Requirements for a Local FTP Server	59
Creating the Local FTP Server Using Dell Server Updates DVD	60
Creating the Local FTP Server Using Dell Repository Update Manager	60
Accessing Updates on a Local FTP Server	60
Configuring a Local USB Device	60
Creating the Local USB Repository Using Dell Server Updates DVD	61
Creating the Local USB Repository Using Dell Repository Update Manager	61
3 Remote Service Features	63
Web Services for Management	63
What's New in Remote Services 1.3	67
Auto-Discovery	67
Configuring DHCP/DNS	67
Auto-Discovery Configuration	68
Auto-Discovery Workflow	69
Connecting Directly to Provisioning Server for Handshake	70

Remotely Reinitiating Auto-Discovery in New Environments	71
Using Custom Certificates	73
Remote Firmware Inventory	74
Instant Firmware Inventory	74
Supported Devices	75
Remote Update	77
Benefits of Remote Update	77
Supported Devices	78
Scheduling Remote Update	79
Remote Scheduling Types	80
Remote Operating System Deployment	81
Remote Operating System Deployment Main Features	81
Remote Operating System Deployment Interface	81
Operating System Deployment Typical Use Case Scenario	85
Staging and Booting to Operating System Image on vFlash	86
Part Replacement	87
A Troubleshooting and Frequently Asked Questions	91
Error Messages	91
Frequently Asked Questions.	105
Index	109

Overview

In order to provide new and robust server management capabilities, the Unified Server Configurator/Unified Server Configurator - Lifecycle Controller Enabled (USC/USC-LCE) software product has been enhanced to include additional remote services functionality. Since this addition allows for a comprehensive approach to server management, the entire set of software components is now called Dell™ Lifecycle Controller.

The Lifecycle Controller software components are built upon the integrated Dell Remote Access Controller 6 (iDRAC6) Express card and the Unified Extensible Firmware Infrastructure (UEFI) system firmware. The iDRAC6 works together with the UEFI firmware to access and manage every aspect of the hardware, including component and subsystem management that is beyond the traditional BMC (Baseboard Management Controller) capabilities.

Remote server management is accomplished using the network for programmatic web services, while command line (CLI) and graphical user interfaces (GUI) are provided by the iDRAC6 card in an operating system-and system-power-state independent manner. The UEFI environment provides the local console interface, and the infrastructure for locally and remotely managing system components.

The remote services functionality enables consoles, such as the Dell Management Console (DMC) and partner consoles, to access Lifecycle Controller features in a pre-operating system environment. USC/USC-LCE provides an embedded solution on the local server to assist with provisioning in a pre-operating system environment.

Remote Services

Remote services are accessible over the network using a secured web services interface and can be programmatically utilized by applications and scripts. Remote services enables existing consoles to perform one-to-many bare metal server provisioning. The combination of a new Auto-discovery feature to identify and authenticate the attached Dell system to the network and integration with one-to-many management consoles reduces the manual steps required for server provisioning. Additionally, remote services provides remotely accessible operating system deployment related features that

simplifies the tasks involved in operating system and driver installation. For more information on the features supported by the remote services provisioning solution, see "Remote Service Features."

Unified Server Configurator (USC)

Unified Server Configurator (USC): Base-level product that uses BMC and provides operating system deployment, hardware diagnostics, and USC settings capabilities.

Unified Server Configurator - Lifecycle Controller Enabled (USC - LCE): Full-featured product that uses iDRAC6 Express and Enterprise cards, and provides platform updates, hardware configuration, operating system deployment, hardware diagnostics, USC settings, dedicated NIC port, virtual KVM, and virtual media capabilities. Dell systems series 200-500 can be upgraded to USC-LCE. For more information, see your *Hardware Owner's Manual*.

For information on the supported systems and operating systems, see the *Dell Systems Software Support Matrix*.

See the *Glossary* at support.dell.com/manuals for terms used in this document.

USC or USC - LCE displays features that are supported by the system, depending on your system configuration. See "Table 1-1" for more details.

Table 1-1. Product Classification

Dell System Series	Options	Available Remote System Management Device	USC or USC-LCE	Available Features
100	No Options	Embedded BMC	USC	BMC - Operating System Deployment, Hardware Diagnostics, USC Settings
200 to 500	Standard	Embedded BMC	USC	BMC - Operating System Deployment, Hardware Diagnostics, USC Settings
	Optional	Embedded BMC + iDRAC6 Express Card	USC-LCE	BMC - Operating System Deployment, Hardware Diagnostics, USC Settings iDRAC6 Express - adds Platform Update, Hardware Configuration, Driver Repository
		Embedded BMC + iDRAC6 Express card + iDRAC6 Enterprise card	USC-LCE	BMC - Operating System Deployment, Hardware Diagnostics, USC Settings iDRAC6 Express - adds Platform Update, Hardware Configuration, Driver Repository iDRAC6 Enterprise - adds Full Remote Management, Dedicated NIC port, Virtual KVM, Virtual Media, Virtual Flash

Table 1-1. Product Classification (continued)

Dell System Series	Options	Available Remote System Management Device	USC or USC-LCE	Available Features
600 to 900	Standard	Embedded BMC with iDRAC6 Express card	USC-LCE	BMC with iDRAC6 Express - Operating System Deployment, Hardware Diagnostics, USC Settings, Platform Update, Hardware Configuration, Driver Repository
	Optional*	Embedded BMC with iDRAC6 Express card + iDRAC6 Enterprise card	USC-LCE	BMC with iDRAC6 Express - Operating System Deployment, Hardware Diagnostics, USC Settings, Platform Update, Hardware Configuration, Driver Repository iDRAC6 Enterprise - adds Full Remote Management, Dedicated NIC port, Virtual KVM, Virtual Media, Virtual Flash

* For Dell modular systems — BMC, iDRAC6 Express card, and iDRAC6 Enterprise card are included as standard configurations.

Unified Server Configurator and Unified Server Configurator - Lifecycle Controller Enabled

Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE) reside on an embedded flash memory card and are embedded configuration utilities that enable systems and storage management tasks from an embedded environment throughout your system's life cycle. USC and USC - LCE are similar to a BIOS utility in that they can be started during the boot sequence and can function in a pre-operating system environment. "Table 1-1" details the Dell™ system series, remote system management device options, USC or USC-LCE, and available features.

Using USC, you can download drivers for operating system installation from the Dell FTP website at ftp.dell.com or using local devices such as a USB device or the *Dell Systems Management Tools and Documentation* or the *Dell Server Updates* DVD. You can also deploy an operating system, or run Hardware Diagnostics to validate the system and attached hardware. Depending on your system, you can upgrade from a Baseboard Management Controller (BMC) to an iDRAC6 Express or an iDRAC6 Enterprise card; this hardware upgrade will also upgrade USC to USC - LCE. See "How to Upgrade to an iDRAC6 Express Card" and the *Hardware Owner's Manual* for your system for more information on how to upgrade. Using USC - LCE, you can quickly identify, download, and apply system updates without searching the Dell Support site at support.dell.com. You can also configure BIOS and system devices (such as NIC, RAID, and iDRAC), deploy an operating system, and run Hardware Diagnostics to validate the system and attached hardware.

What's new in USC/USC-LCE 1.3

These are the new features introduced in USC/USC-LCE 1.3:

USC-LCE

- Support for part replacement
- Support for configuring Provisioning Server and Auto-Discovery from iDRAC configuration utility
- Report vFlash health status and presence
- Support for BIOS boot order
- Version compatibility check for BIOS, iDRAC and USC

USC and USC-LCE Support for:

- Series 7 controllers
- SED (Self-encryption disk) drive
- Dell Repository Update Manager with option to specify sub-directory
- FTP authentication

Common Features

This section contains the features that are common to both USC and USC - LCE. Any additional steps or information required for USC - LCE tasks are noted and provided.

Launching the Product

To launch either USC or USC - LCE, boot the system and press the <F10> key within 10 seconds of the Dell logo being displayed during the system boot process to enter **System Services**.

If the system is in one of the following states, pressing <F10> will not allow you to enter **System Services**:

- **System Services disabled** — If you power on or restart your system while iDRAC is initializing, the message **System Services disabled** will display during the system boot process. This situation happens if you power on your system immediately after AC is applied to the system, or if you restart the system immediately after resetting iDRAC. To avoid this issue, wait about a minute after resetting iDRAC to restart your system, thus allowing enough time for iDRAC to complete initialization.

If the message `System Services disabled` still displays, then the product may have been manually disabled. See "Disabling USC or USC-LCE" for information on how to enable USC or USC - LCE.

- **System Services update required** — If the message `System Services update required` appears when you boot your system, the embedded device that stores the product may contain corrupted data. To resolve the issue, update the product by executing USC or USC - LCE Dell Update Package (DUP). See the *Dell Update Packages User's Guide* at support.dell.com/manuals for more information.

If an operating system is not installed on the system or if executing the DUP does not fix the problem, run USC or USC - LCE repair package. See "Repairing USC" or "Repairing USC - LCE" for more information.

- **System Services not available** — Another process is currently using iDRAC. It is recommended that you wait for 30 minutes for the current process to complete; then, reboot your system and try to enter USC or USC - LCE again.

If you believe the system is in an error condition or if you cannot wait the recommended 30-minute time period, see "Canceling a Request to Enter System Services." After rebooting, try to enter USC or USC - LCE again. The first time you launch USC or USC - LCE, it displays **USC Settings** wizard that allows you to configure your preferred language and network settings. See "Using USC Settings Wizard" for more information.

Using the Wizards

Wizard Description

USC and USC - LCE provide the following wizards based on your system's configuration:

- **OS Deployment** — Enables you to install an operating system. See "Deploying the Operating System Using the OS Deployment Wizard" for more information.
- **Hardware Diagnostics** — Enables you to perform diagnostics to validate the memory, I/O devices, CPU, physical disks, and other peripherals. See "Hardware Diagnostics" for more information.

- **USC Settings** — Enables you to specify the language, keyboard layout, and network settings to be used with USC or USC-LCE. See "Using USC Settings Wizard" for more information.

Along with the above mentioned wizards, USC and USC-LCE provide the following options:

- **Home** — Enables you to navigate back to **Home** screen.
- **About** — Enables you to view the version information of USC-LCE and UEFI. Click **View Readme** in the **About** wizard to view USC-LCE readme.

USC - LCE provides the following additional wizards based on your system's configuration:

- **Platform Update** — Enables you to download and apply updates for your system. You can access the updates from ftp.dell.com or a USB device attached to your system. See "Updating the Platform using the Platform Update Wizard" and "Configuring a Local USB Device" for more information.
- **Hardware Configuration** — Enables you to configure system devices. See "Hardware Configuration" for more information.

Launching a Wizard

USC and USC - LCE display the available wizards in the left pane. Click the wizard you want to launch, and then follow the instructions displayed in the right pane.

Wizard Task Flow USC

When using USC for the first time, It is recommended that you run the wizards in the order listed below:


- **USC Settings** — You do not need to run this wizard again unless you want to change the language, keyboard, or network settings.
- **OS Deployment** — Run this wizard to install operating system.
- **Hardware Diagnostics** — Ensure that you maintain your system by running diagnostics on a regular basis.

Wizard Task Flow USC - LCE

When using USC - LCE for the first time, it is recommended that you run the following wizards listed in order:

- **USC Settings** — You do not need to run this wizard again unless you want to change the language, keyboard, or network settings.
- **Platform Update** — Download and apply any updates. Ensure that you run the **Platform Update** wizard regularly so that your system is up to date.
- **Hardware Configuration** — Run this wizard to configure your system devices.
- **OS Deployment** — Run this wizard to install operating system.
- **Hardware Diagnostics** — Ensure that you maintain your system by running diagnostics on a regular basis.

Accessing Help

Each USC or USC - LCE screen has a **Help** button in the upper-right corner. Click **Help**  to display help for the current screen.

Viewing Readme

Click **About**→**View Readme** to display the *Readme* file.

Disabling USC or USC-LCE


You can disable USC or USC - LCE to prevent your system from entering it on start-up:

- 1 Press <Ctrl> <e> within 5 seconds when prompted during system start-up.
The **iDRAC6 Configuration Utility** page displays.
- 2 Navigate to **System Services**.
- 3 Select **Disable System Services**.
- 4 Save your changes and exit the **iDRAC6 Configuration Utility** page menu. The system reboots automatically.

To enable USC or USC-LCE, repeat "step 1" and "step 2", and then select **Enable System Services**.

Canceling a Request to Enter System Services

If USC or USC - LCE causes the system to repeatedly reboot, you can cancel a request to enter System Services.

 **CAUTION: This action cancels all tasks USC or USC - LCE is in the process of executing. Dell strongly recommends that you cancel the request to enter System Services only when absolutely necessary.**

- 1 Press <Ctrl><e> within 5 seconds when prompted during system start-up.

The iDRAC6 Configuration Utility page displays.

- 2 Navigate to System Services.
- 3 Select Cancel System Services.

Save your changes and exit the iDRAC6 Configuration Utility page.

The system reboots automatically.

Using USC Settings Wizard

USC Settings wizard enables you to specify the language, keyboard layout, and network settings for USC or USC - LCE. USC settings apply only to USC or USC - LCE and do not apply to the system or any other application running on the system.

- 1 Launch USC Settings Wizard:
 - a Boot your system and press the <F10> key within 10 seconds of the Dell logo being displayed.
 - b Wait until USC Home screen is displayed, then click USC Settings in the left pane.
- 2 Click Language and Keyboard in the right pane. Use the up-arrow and down-arrow keys to access all options on the Language and Keyboard Type drop-down menus.
 - a Select the language from the Language drop-down menu.
 - b Select the type of keyboard you are using from the Keyboard Type drop-down menu.
 - c Click Finish.
- 3 Click Network Settings in the right pane.
 - a Use the NIC Card drop-down menu to select the NIC card you want to configure on your system.
 - b Use the IP Address Source drop-down menu to select either No Configuration, DHCP, or Static IP. The IP Address Source function only supports IPv4.

- **No Configuration** - Select if you do not want to configure your NIC.
- **DHCP** - Select to obtain an IP address from a DHCP server.
- **Static IP** - Select to use a static IP address. Specify the following IP address properties. If you do not have this information, see your network administrator.
 - **IP Address**
 - **Subnet Mask**
 - **Default Gateway**
 - **DNS Address**

c Click **Finish**.

If USC settings are not configured correctly, an error message is displayed.

Deploying the Operating System Using the OS Deployment Wizard

The **OS Deployment** wizard assists you in installing an operating system on your system.

USC does not provide a local operating system drivers repository that may be required for operating system installation. You have to download the operating system drivers from the Dell FTP website at ftp.dell.com or use a local source that has drivers on it — for example, *Dell Systems Management Tools and Documentation DVD* or a local USB device.

USC - LCE provides a local repository for drivers that may be required for operating system installation, depending on which operating system you are installing. The **OS Deployment** wizard extracts these drivers and copies them to a staging directory. For supported Microsoft® Windows® operating systems, these extracted drivers are installed during the operating system installation. For supported Linux operating systems, such as Red Hat® Enterprise Linux® versions 4.7, 4.8, 5.2, and 5.3 and SUSE® Linux Enterprise Server version 10 SP2, you must manually install the extracted drivers after the operating system installation is completed. However, starting with Red Hat Enterprise Linux version 5.4, SUSE Linux Enterprise Server version 10 SP3, 11 and later installs, the extracted drivers are installed during the operating system installation. See "Deploy the Operating System" for more information.

Although USC - LCE comes with embedded drivers that are factory installed, there may be more current drivers available. You should run the **Platform Update** wizard to ensure that you have the most current drivers before installing the operating system.

Before installing the operating system, the **OS Deployment** wizard detects if a boot device is available. A boot device is a physical disk, virtual disk, or other storage device on which the operating system can be installed.

If your system has a RAID controller, you can configure a virtual disk and choose to use the virtual disk as the boot device.

If your system does not have a RAID controller or if you choose to bypass the optional RAID configuration, the **OS Deployment** wizard installs the operating system to a default location, which is typically the disk identified as Disk 0 in the BIOS utility.

Launch the Operating System Deployment Wizard

- 1** To launch USC, boot your system and press the <F10> key within 10 seconds of the Dell logo being displayed.
- 2** Click **OS Deployment** in the left pane.
- 3** Click **Deploy OS** in the right pane.
- 4** For USC, continue with the "Select the Operating System Driver Source Location (for USC only)" procedure that follows.
- 5** For USC - LCE, if your system has a RAID controller, continue with "Optional RAID Configuration." If your system does not have a RAID controller, continue with "Select an Operating System."

Select the Operating System Driver Source Location (for USC only)

Use this screen to select the driver required for operating system installation. You can download operating system drivers from an online repository or from a local drive.

- 1** Select either **Online Repository** or **Local Drive**.

FTP Repository

Select **FTP Repository** to download drivers from an FTP server. Enter the appropriate information according to the method you are using to access the FTP server.

If you use a firewall, you should configure it to allow outgoing FTP traffic on port 21. The firewall must also be configured to accept incoming FTP response traffic.

- To download drivers from the online repository (Dell FTP server), you must enter **ftp.dell.com** in the **Address** field.

or

To download drivers from a locally-configured online repository, in the **Address** field you must specify the server host name or the IP address of the server on which the drivers reside. For information on setting up local FTP server, see "Configuring a Local FTP Server."

- To download drivers by using a proxy server to access an FTP server, you must specify:
 - **Address** — The IP address of the local FTP server or **ftp.dell.com**.
 - **User Name** — The user name to access the FTP location.
 - **Password** — The password to access this FTP location.
 - **Proxy Server** — The server host name or the IP address of the proxy server
 - **Proxy Port** — The port number of the proxy server
 - **Proxy Type** — The type of proxy server. HTTP and SOCKS 4 proxy types are supported by USC.
 - **Proxy User Name** — The user name required for authentication on the proxy server
 - **Proxy Password** — The password required for authentication on the proxy server
- 2** Select **Save Locally** to save the drivers locally from the online repository. From the **Save Locally** drop-down menu, select the USB drive to save the system drivers.

Local Drive

Select **Local Drive** if the drivers are available from a USB device or *Dell Systems Management Tools and Documentation DVD*. For information on setting up a USB device for updates see "Configuring a Local USB Device."

3 Click Next.

If your system has a RAID controller, continue with "Optional RAID Configuration." If your system does not have a RAID controller, continue with "Select an Operating System."

Optional RAID Configuration

If your system has a RAID controller, you have the option of launching the **RAID Configuration** wizard and configuring a virtual disk as the boot device.

To configure RAID:

- Select **Configure RAID Now** and click **Next**. This option launches the **RAID Configuration** wizard. After RAID configuration is complete, you will return to the **OS Deployment** wizard. See "Configuring RAID."

To bypass RAID configuration:

- Select **Go Directly to OS Deployment** and click **Next**. This option launches the **OS Deployment** wizard. If you select this option, the operating system will be installed on the default boot device identified in the BIOS utility. Continue with "Select an Operating System."

Deploy the Operating System

The drivers required by the operating system, or recommended for updating your system after installation, are extracted to a temporary location.

These files are deleted after an 18-hour period or when you press the <F10> key to either cancel operating system installation or re-enter USC after rebooting.



NOTE: During the 18-hour period when drivers are extracted to a temporary location after the operating system is installed, you cannot update USC or USC-LCE, drivers, or hardware diagnostics using a DUP. If you attempt an update using a DUP during this time period, the DUP will display a message that another session is open.

Select an Operating System

Use the following steps to select an operating system:

- 1 Select the operating system you want to install and click **Next**.

- 2 USC or USC - LCE extracts the drivers required by the operating system you selected. The drivers are extracted to an internal USB drive named OEMDRV.
- 3 After the drivers are extracted, USC or USC - LCE prompts you to insert the operating system installation media.

Important

- For Red Hat Enterprise Linux 4.x server and Red Hat Enterprise Linux 5.x, the drivers are extracted to OEMDRV under /oemdrv/*.rpm. For SUSE Linux Enterprise Server 10 SP2, the drivers are extracted under /linux/suse/x86_64-sles10/install/*.rpm.
- When installing the Microsoft Windows operating system, the extracted drivers are automatically installed during the operating system installation. When installing the Red Hat Enterprise Linux 4.x operating system, the operating system installation uses native drivers. After the Linux installation is complete, you need to manually install the drivers extracted by USC or USC-LCE. See "Update Drivers for Linux Systems Only" for more information.

Kickstart Installation for the Linux Operating System

If you are using a kickstart installation for the Linux operating system, provide the following information in the post-installation script:

- Command to mount the USB device containing the operating system drivers labeled OEMDRV. For example:

```
mkdir OEMDRV
```

```
mount /dev/sdc1 /mnt/OEMDRV
```

- Path to the operating system drivers on the OEMDRV drive:

For Red Hat Enterprise Linux: /oemdrv/*.rpm

For SUSE Linux Enterprise Server:

```
/linux/suse/x86_64-sles10/install/*.rpm
```

- Command to install the drivers: rpm -Uvh *.rpm

Insert the Operating System Media

Insert the operating system installation media when prompted and click **Next**.

USC supports internal SATA optical drives and USB optical drives and USC - LCE supports internal SATA optical drives, USB optical drives, and virtual media devices. If the installation media is corrupt or not readable, then USC and USC-LCE may be unable to detect the presence of a supported optical drive. In this case, you may receive an error message stating that no optical drive is available. If the media is not valid (if it is the incorrect CD or DVD, for example), a message displays requesting that you insert the correct installation media.

For USC - LCE only: Virtual media is supported through iDRAC. See the User Guide for your system's iDRAC device for more information on setting up virtual media through iDRAC.


Reboot the System

Prerequisite

Microsoft Windows Server 2008 UEFI operating system installations are not currently supported.

Use the following step to reboot the system:

- 1 Click **Finish** to reboot the system and continue with the operating system installation. Upon reboot, the system boots to the operating system installation media.

 **CAUTION: During the beginning of Windows Server® 2003 installation, the installer will automatically detect and possibly assign the default drive letter C to USC and USC-LCE temporary storage device OEMDRV. Creating a new Windows-bootable system partition on the hard-disk will assign the partition to a drive letter other than C; this is standard Windows installer behavior. To assign the new partition to C, see "Assign a Windows-Bootable System Partition to the C: Drive" for more information.**

Post-requisites

- When the system reboots after you click **Finish**, you may be prompted to press a key before booting to the operating system installation media. If you do not press a key, the system boots to the hard-disk and not the operating system installation media.

- In the event that the operating system installation is interrupted and the system reboots before installation completes, you may be prompted to press a key in order to boot from the operating system installation media.
- You can cancel the operating system installation by pressing the <F10> key. Pressing the <F10> key at any point during the installation process or while rebooting causes any drivers provided by the **OS Deployment** wizard to be removed.
- After the operating system is installed, you cannot update USC or USC-LCE by running a DUP in the operating system environment for the next 18 hours.

Red Hat Enterprise Linux version 5.x Installation Warning

During Red Hat 5.x installation, you will receive a warning that a read-only file system was detected; Linux has detected the temporary storage area of USC and USC-LCE that stores updates for your system. When you click **OK**, a second warning will appear indicating that the read-only file system has a loop partition layout and that it needs to be formatted. Click the **Ignore drive** button. You may see both warnings several times during the course of Red Hat 5.x installation.

Update Drivers for Linux Systems Only

On the following operating systems, it is recommended that you update your system with the extracted drivers after installation. The drivers are extracted to a drive (or device) named `OEMDRV`.

- Red Hat Enterprise Linux server — The location of the drivers on the `OEMDRV` drive after installation is:
`/oemdrv/*.rpm`
- Red Hat Enterprise Linux server — The location of the drivers on the `OEMDRV` drive after installation is:
`/oemdrv/*.rpm`
- SUSE Linux Enterprise Server 10 with Service Pack 2 — The location of the drivers on the `OEMDRV` drive after installation is:
`/linux/suse/x86_64-sles10/install/*.rpm`


Use the following command to install the drivers:

```
rpm -Uvh *.rpm
```

Assign a Windows-Bootable System Partition to the C: Drive

After you have completed USC or USC - LCE portion of Windows Server 2003 installation, your server will reboot and begin the text-mode portion of the installation. During this phase, you may need to perform the following steps to ensure Windows installs to your C: drive.

Following these instructions after Windows Server 2003 setup presents you with a list of existing drive partitions and/or unpartitioned space available on your computer.

- 1 Select the unpartitioned space, and then press <c> to create a hard-disk partition. Follow the on-screen instructions to create a partition.
 **NOTE:** The partition may not be enumerated as a C: drive.
- 2 Select the newly-created partition, and then press <d> to delete the partition. Follow the on-screen instructions to delete the partition.
- 3 Select the unpartitioned space again, and then press <c> to create a primary hard-disk partition. The partition will now be enumerated as C: drive.
- 4 Follow the on-screen instructions to create a partition. Windows will now install on the C: drive.

See <http://support.microsoft.com/kb/896536> for more information on assigning the Windows-bootable system partition to the C: drive.

Installing Red Hat Enterprise Linux 5.3 or Red Hat Enterprise Linux 4.8 on a system with SAS7 (H200) controller

Perform the following steps to install Red Hat Enterprise Linux 4.8 / Red Hat Enterprise Linux 5.3:

- 1 Copy the driver image file (*.img or *.dd) into a USB key. Specify the driver image file location when prompted for a driver diskette.
- 2 Select Red Hat Enterprise Linux 4.8/Red Hat Enterprise Linux 5.3 on the **OS Deployment** screen of USC.
- 3 After USC reboots to the OS installer CD/DVD, enter the following command: > linux dd

- 4 Insert the driver update disk (DUD) when prompted, and specify the location of the USB drive and press <Enter>.
- 5 Complete the installation as directed by the installation program.

Hardware Diagnostics

Utilizing the **Hardware Diagnostics** utility, it is recommended that you run diagnostics as part of a regular maintenance regimen to validate that the system and attached hardware are functioning properly. Because the diagnostics utility has a physical (as opposed to logical) view of attached hardware, this utility may be able to identify hardware problems that the operating system and other online tools cannot. You can use the hardware diagnostics utility to validate the memory, I/O devices, CPU, physical disks, and other peripherals.

Performing Hardware Diagnostics

To start the hardware diagnostics utility, click **Hardware Diagnostics** in the left pane and click **Run Hardware Diagnostics** in the right pane. When the diagnostics utility launches, follow the instructions on the screen.

You must reboot your system to exit the Hardware Diagnostics utility and press <F10> to re-enter USC or USC-LCE.

The results of the diagnostics tests are displayed on the screen when the tests complete. The test results describe the problems found. You can use this information to search the Dell Support website at support.dell.com for details on resolving the problem.

If you want to exit the **Hardware Diagnostics** utility, press the <Esc> key; this will cause the system to reboot.

Updating the Hardware Diagnostics Utility

For Systems Supporting USC

Download the required Dell Update Package (DUP) from Dell Support site at support.dell.com. Run the DUP as an executable in the installed operating system.

For Systems Supporting USC - LCE

Use the **Platform Update** wizard to update the hardware diagnostics utility. See "Updating the Platform using the Platform Update Wizard" for more information. Alternatively, you can also download the required Dell Update Package (DUP) from Dell Support site at support.dell.com and run the DUP as an executable in the installed operating system.

Repairing USC

If the message `System Services update required` appears when you boot up, the embedded device that stores USC may contain corrupted data. To resolve the issue, you must first attempt to update USC by executing USC Dell Update Package (DUP). See the *Dell Update Packages User's Guide* available at support.dell.com/manuals for more information.


Repairing USC - LCE

If the message `System Services update required` appears when you boot up, the embedded device that stores USC - LCE may contain corrupted data. To resolve the issue, you must first attempt to update USC - LCE by executing USC - LCE Dell Update Package (DUP). See the *Dell Update Packages User's Guide* available at support.dell.com/manuals for more information. If running the DUP does not solve the problem, use USC - LCE repair package:

- 1 Go to ftp.dell.com → `LifecycleController` and download the file named `USC_1.3.0_Rep_Pack_A00.usc` (or newer version) to a temporary location.
- 2 Connect to iDRAC on your system using the iDRAC Web interface. For more information on iDRAC, see the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide*.
- 3 From the iDRAC Web interface, click **Remote Access**.
- 4 Select the **Update** tab, and then browse to USC - LCE Repair Package you downloaded from ftp.dell.com.
- 5 Click **Next**, and then click **OK** to confirm the upload. Allow the process to complete before you continue to "step 6."
- 6 Reboot your system, and then press the `<F10>` key to enter USC - LCE.
- 7 Complete the installation of all recommended updates. See "Updating the Platform using the Platform Update Wizard" for more information. When updates are complete, your system automatically reboots.


- 8 While the system reboots, press the <F10> key again to enter USC - LCE.

If a warning message appears on the initial USC - LCE screen, you must repeat "step 7" until the server is in a fully-recovered state.

 **NOTE:** Updates that are required for a complete system recovery are pre-selected by USC - LCE. Dell highly recommends running all selected updates on your system.


How to Upgrade to an iDRAC6 Express Card

This section provides information about installing an iDRAC6 Express card, transferring the iDRAC6 Express card from one system to another system, and Uninstalling iDRAC6 Express card. This hardware upgrade will also upgrade USC to USC-LCE.

 **NOTE:** This is applicable only to Dell System Series 200-500.

Installing the iDRAC6 Express Card

- 1 Turn off the system, including any attached peripherals, and disconnect the system from the electrical outlet.

 **NOTE:** To discharge the residual power in the system, press the power button once.

- 2 Insert the iDRAC6 Express card into the iDRAC6 Express slot. See the *Hardware Owner's Manual* for your system for more information on Installing iDRAC6 Express Card.
- 3 Reconnect the system and peripherals to their power sources. iDRAC automatically starts. Wait one minute, before switching on the system, to allow the iDRAC to fully start.
- 4 Switch on the system, and then press <F10> to enter USC. USC automatically detects the iDRAC6 Express card installed on the system and completes the upgrade process.

If the installation is successful, you are able to boot to Unified Server Configurator — Lifecycle Controller Enabled.

If the installation fails, you must upgrade iDRAC. See the *Integrated Dell Remote Access Controller User Guide* for more information. After you have upgraded iDRAC, repeat the above instructions.

Transferring an iDRAC6 Express Card

If the iDRAC6 Express card is transferred from one system to another:

- The rollback feature is unavailable on the new system. See "Rolling Back to Previous BIOS and Firmware Versions" for more information.
- All pending USC-LCE tasks that are in the process of execution are deleted on the new system.
- Run **Platform Update** wizard to download the appropriate driver pack for the new system.

The driver pack is deleted if the iDRAC6 Express card is transferred to a different Dell system. For example, if you move the iDRAC6 Express card from Dell R410 system to Dell T410 system, the driver pack is deleted.

Removing the iDRAC6 Express Card

- 1 Turn off the system, including any attached peripherals, and disconnect the system from the electrical outlet. To discharge the residual power in the system, press the power button once.
- 2 Remove the iDRAC6 Express card from the iDRAC6 Express slot. See the *Hardware Owner's Manual* for your system for more information on Installing iDRAC6 Express Card.
- 3 Reconnect the system and peripherals to their power sources.
- 4 Switch on the system, and then press <F10> to enter USC.

Unified Server Configurator - Lifecycle Controller Enabled Unique Features

This section contains the features that are only available in USC - LCE. For information on features common to USC and USC - LCE see "Common Features."

Updating USC - LCE

You can update to the latest version of USC - LCE using the **Platform Update** wizard. It is recommended that you run the **Platform Update** wizard on a regular basis to access updates as they become available. See "Updating the Platform using the Platform Update Wizard" for more information.

Updating the Platform using the Platform Update Wizard

Use the **Platform Update** wizard to view the current versions of the installed applications and firmware information. You can use the **Platform Update Wizard** to display a list of available updates for your system. After you select the updates you want to apply, USC - LCE downloads and applies the updates.

To ensure optimal system performance and avoid system problems, Dell recommends that you download and apply updates on a regular basis.

To run the **Platform Update** wizard, you need access to the Dell File Transfer Protocol (FTP) server at <ftp.dell.com>. Alternatively, your system administrator may provide the updates on a local USB device or on a *Dell Server Update Utility* DVD. Contact your system administrator to find out the preferred method for accessing updates in your organization. See "Configuring a Local FTP Server" for more information.

If you are using FTP as your update method, you must configure the network card using USC - LCE **USC Settings** wizard before accessing the updates. See "Using USC Settings Wizard" for more information.

Version Compatibility

The version compatibility features ensures that only the Lifecycle Controller, BIOS and iDRAC versions that are compatible with system components are installed. The console will display upgrade or downgrade error messages to warn you about compatibility issues for various components; these messages will be displayed for ten seconds only.

View Current Version Information

- 1 Boot your system and press the <F10> key within 10 seconds of the Dell logo being displayed.
- 2 Click **Platform Update** in the left pane.
- 3 Click **View Current Versions** in the right pane.

Launch the Platform Update Wizard

- 1 Boot your system and press the <F10> key within 10 seconds of the Dell logo being displayed.
- 2 Click **Platform Update** in the left pane.
- 3 Click **Launch Platform Update** in the right pane.

Select Download Method

You can download updates from Dell's FTP server at ftp.dell.com using the **Platform Update** wizard or from a local FTP server or from a local USB device or *Dell Server Updates* DVD.

To enable the text boxes and drop-down menus under local **FTP server** or **Dell FTP Server** and **USB Device**, select the corresponding **FTP Server** or **Local Drive** check box.

- 1 Select either **FTP Server** or **Local Drive**.

FTP Server

Select **FTP Server** to download updates from the configured FTP server using the **Platform Update** wizard. Enter the appropriate information according to the method you are using to access the FTP server.

FTP Authentication

USC supports anonymous login by authenticating the blank username, a password of your choice, and the FTP server address with the FTP servers in order to download the catalog information. If you use a firewall, you should configure it to allow outgoing FTP traffic on port 21. The firewall must also be configured to accept incoming FTP response traffic.

To download updates by using a proxy server to access the FTP server, you must specify:

- **Address** — The IP address of the local FTP server or ftp.dell.com.
- **User Name** — The user name to access the FTP location.
- **Password** — The password to access this FTP location.
- **Catalog Location** — The specific location/sub-directory where the catalog resides.
- **Proxy Server** — The server host name of the proxy server.
- **Proxy Port** — The port number of the proxy server.
- **Proxy Type** — The type of proxy server. HTTP and SOCKS 4 proxy types are supported by USC - LCE.
- **Proxy User Name** — The user name required for authentication on the proxy server.

- **Proxy Password** — The password required for authentication on the proxy server.

Local Drive

Select **Local Drive** if you are accessing the updates from a local USB device or *Dell Server Updates* DVD. Select the appropriate volume label from the **Local Drive** drop-down menu.

See "Configuring a Local USB Device" for more information.

- 2 Click Next.

Select and Apply Updates

The **Select Updates** screen displays a list of available updates.

- 1 Select the check box for each update that you want to apply to your system. The components for which a more current update is available are selected by default.

If you want to compare the version of the update with the version currently installed on the system, compare the versions in the **Current** and **Available** fields.

- **Component** — Displays the available updates. Select the check box for each update you want to apply.
- **Current** — Displays the component version currently installed on the system.
- **Available** — Displays the version of the available update.

- 2 Click Apply.

Post-requisites

- The system reboots after the update process is complete. When applying more than one update, the system may need to reboot between updates. In this case, the system boots directly into USC - LCE and continues the update process. No action on your part is required when the system reboots to complete the update process.
- If the iDRAC firmware update is interrupted for any reason, you may need to wait for up to 30 minutes before attempting another firmware update.

Important

- USC-LCE does not support the update or rollback of PERC 5/E Adapter for external storage, SAS 5i/R Adapter for tape, PERC S100 and PERC S300 Adapters, and Intel™ NIC Adapters.
- A NIC wrapper.efi error may be displayed if you try updating the NIC using platform update in USC without the latest versions of iDRAC and BIOS. Upgrade to the latest BIOS and iDRAC versions to ensure this error does not occur.



CAUTION: While using USC to update the power supply unit firmware, the system will shut down after the first task. It will take a couple of minutes to update the PSU firmware and then automatically power on.

Rolling Back to Previous BIOS and Firmware Versions

USC - LCE enables you to roll back to a previously-installed version of BIOS or firmware. It is recommended that you use this feature if you have a problem with the currently-installed version and want to revert to the previously-installed version.

Only BIOS and firmware can be rolled back. USC - LCE, the hardware diagnostics application, and drivers needed for operating system (OS) installation cannot be rolled back to earlier versions.

This feature is available only if you have used the USC - LCE update feature to update BIOS and firmware, or if you have updated the system BIOS or firmware using a post-operating system Dell Update Package. If you have used other update methods, this feature is not available.

Important

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 more than once, the factory-installed images are overwritten and you cannot revert to them.

Launch the Rollback Wizard

- 1** Boot your system to launch USC - LCE. When the Dell logo displays, press the <F10> key within 10 seconds.
- 2** Click **Platform Update** in the left pane.
- 3** Click **Launch Platform Rollback** in the right pane.

Select and Apply Rollbacks

The **Platform Rollback** screen displays a list of available rollback components.

- 1 Select the check box of each rollback image that you want to apply to the system.

To compare the version of the rollback image with the version currently installed on the system, compare the versions in the **Current** and **Previous** fields.

- **Component** — Displays the available updates; select the check box of each update you want to apply.
- **Current** — Displays the component version currently installed on the system.
- **Previous** — Displays the version of the rollback image.

- 2 Click **Apply**.

Post-requisite

The system reboots after the update process is complete. When applying more than one update, the system may need to reboot between updates. In this case, the system boots directly into USC - LCE and continues the update process. This is an unattended update process.

Updating Devices That Affect Trusted Platform Module Settings

If BitLocker protection is enabled on your system, updating certain components requires you to enter a recovery password or insert a USB flash drive containing a recovery key during the next system boot. This situation occurs only if the Trusted Platform Module (TPM) security setting is set to **On with Pre-boot Measurements**. For information on how to set TPM settings, see the *BIOS User Guide* available at support.dell.com/manuals.

When USC - LCE detects that TPM security is set to **On with Pre-boot Measurements**, a warning message displays indicating that certain updates require the recovery password or USB flash drive with the recovery key. The warning message also indicates which components affect the BitLocker. You can choose either not to update or to roll back those components by navigating to the **Select Updates** screen and deselecting the check boxes for the components.

Hardware Configuration

USC - LCE provides two different methods for configuring your hardware, both of which are available from the main **Hardware Configuration** screen:

- **Configuration Wizards** guide you through setting up system devices. The Configuration Wizards include: Physical Security Configuration, System Date/Time Configuration, iDRAC Configuration, and RAID Configuration.
- **Advanced Configuration** allows you to configure certain devices, such as Network Interface Controllers (NICs) and the BIOS, using Human Interface Infrastructure (HII).
- **Part Replacement Configuration** allows you to automatically update a new part to the previous part's firmware level.

Important

- If your system does not have a RAID controller, the **OS Deployment** wizard bypasses the RAID configuration option and goes directly to "Select an Operating System."
- Using USC-LCE, you can navigate to the RAID configuration page from the **Hardware Configuration Tab-> Configuration Wizards->RAID Configuration**.
- For S100 /S300 controllers, virtual disks cannot be created using the **RAID Configuration** Wizard in USC - LCE. To create RAID, use the controller utilities by pressing <Ctrl><R> when prompted during system start-up.
- ESX 3.5 and Citrix operating systems do not support series 7 controllers.
- USC has the capacity to display only three storage controllers for RAID configuration on the console.
- If there are any internal storage controller cards on the system, all other external cards cannot be configured. If there are no internal cards present, then external cards can be configured.

Configuring RAID

To configure RAID, follow these steps:

- 1 Click **OS Deployment** on the left pane.

- 2 Select **Configure RAID Now**. The system will display all the storage controllers available for configuration, including the series 6 and 7 controllers.
- 3 Select a storage controller.
The RAID Configuration options are displayed.
- 4 Complete RAID settings and click **Finish**.
The RAID configuration is applied on the disks.

Viewing Secure Capability Status and Virtual Disks of the Series 7 Controller

You can create, change or delete the security key on security-capable controllers. Setting a security key allows you to create secured virtual disks using Self Encryption Disks (SED).

To view the secure capability status and virtual disks of the series 7 controller, follow these steps:

- 1 Click **OS Deployment** on the left pane. The **Configure RAID wizard** and **Install operating system** options are displayed.
- 2 Select **Configure RAID Now**. The number of virtual disks present on every controller is displayed, along with information on whether the virtual disk is secure. The controllers with security capability are displayed suffixed with the phrase **Security Capable**.

Creating a Secure Virtual Disk on Series 7 Controller

To create a secure virtual disk on series 7 controller, follow these steps:

- 1 Click **OS Deployment** on the left pane.
The **Configure RAID Now** and **Go Directly to OS deployment** options are displayed.
- 2 Select **Configure RAID Now**. The number of virtual disks present on every controller is displayed, along with information on whether the virtual disk is secure.
- 3 Select **Secure Capable Controllers** and click **Next**. Two options are displayed:
 - **Configure Security Key Now**
 - **Continue Virtual Disk Configuration**

- 4 Select **Configure Security Key Now** and click **Next**. The security key configuration screen is displayed.
- 5 The following options are displayed:
 - **Create Security Key**
 - **Change Security Key**
 - **Delete Security Key**
- 6 Choose **Create Security Key**, if it is not configured and enter the details in the relevant fields on this page.
- 7 Click **Finish**. The security key will be created on the controller and the **Configuration Options** page is displayed with two options - **Express Wizard** and **Advanced wizard**.
- 8 Select **Advanced Wizard** and click **Next**.
- 9 Select the required RAID level and click **Next**. The user interface displays three filters. Here a new filter is displayed for encryption capability.
- 10 Select **Self-encryption** from the Encryption Capability dropdown. The self-encryption disks (SEDs) are displayed.
- 11 Select the required physical disks and click **Next**.
- 12 In the **Additional Settings** page, check the **Secure Virtual Disk** box and click **Next**.
- 13 The Summary Page is displayed with details of the virtual disk attributes.
- 14 Click **Finish**.

Updating RAID Controller Firmware

To update RAID controller firmware, follow these steps:

- 1 Click **Platform update** on the left pane.
The platform update options are displayed.
- 2 Select the repository option and click **Next**.
The components are displayed with current and available firmware updates.
- 3 Select the storage card and click **Apply**.
The update process is initiated and the firmware update is completed.

Physical Security Configuration

Use the **Physical Security Configuration Wizard** to control access to the system control panel.

To launch the **Physical Security Configuration Wizard**:

- 1 Click **Hardware Configuration** in the left pane.
- 2 Click **Configuration Wizards** in the right pane.
- 3 Click **Physical Security Configuration** to launch the wizard.
- 4 Set **System Control Panel Access** to one of the following options:
 - **Disabled** — You do not have access to information or control, other than the information displayed by the management controller, and you cannot specify actions.
 - **View Only** — You can move through the data screens to obtain information using the system control panel interface.
 - **View and Modify** — You can obtain information and make changes using the system control panel interface.
- 5 Click **Finish** to apply the changes.

To return to the **Configuration Wizards** screen, click **Back**. To exit the wizard, click **Cancel**.

System Date/Time Configuration

Use the **System Date/Time Configuration Wizard** to set the date and time for the system.

To launch the **System Date/Time Configuration Wizard**:

- 1 Click **Hardware Configuration** in the left pane.
- 2 Click **Configuration Wizards** in the right pane.
- 3 Click **System Date/Time Configuration** to launch the wizard.

The default system date and system time shown in USC - LCE is the date and time reported by the system BIOS.
- 4 Modify the **System Date** and **Time** (HH:MM:SS AM/PM) values, as required.
- 5 Click **Finish** to apply the changes.

To return to the **Configuration Wizards** screen, click **Back**. To exit the wizard, click **Cancel**.

iDRAC Configuration

Use the **iDRAC Configuration Wizard** to configure and manage iDRAC parameters.

This wizard is similar to the iDRAC Configuration Utility in the legacy BIOS operation. You can use the wizard to configure iDRAC parameters applicable to the system, such as LAN, common IP settings, IPv4, IPv6, virtual media, and LAN user configuration.

To launch the **iDRAC Configuration Wizard**:

- 1** Click **Hardware Configuration** in the left pane.
- 2** Click **Configuration Wizards** in the right pane.
- 3** Click **iDRAC Configuration** to launch the wizard.

The following steps will walk you through the **iDRAC Configuration Wizard**:

- a** "LAN Configuration"
- b** "Advanced LAN Configuration"
- c** "Common IP Configuration"
- d** "IPv4 Configuration"
- e** "IPv6 Configuration"
- f** "Virtual Media Configuration"
- g** "LAN User Configuration"
- h** "Confirmation"

LAN Configuration

View or configure iDRAC LAN, IPMI over LAN, MAC address, and NIC selection.

- **iDRAC LAN** — Enables or disables the iDRAC NIC. Disabling iDRAC LAN deactivates the remaining controls.
- **IPMI Over LAN** — Enables or disables Intelligent Platform Management Interface (IPMI) commands on the iDRAC Local Area Network (LAN) channel.

- **MAC Address** — Enables you to view the Media Access Control (MAC) address that uniquely identifies each node in a network (read-only).
- **NIC Selection** — Enables you to view or edit the NIC mode using the following mode options:
 - **Dedicated** — This option enables remote access to utilize the dedicated network interface available on the Dell Remote Access Controller (DRAC). Because the DRAC interface is not shared with the host operating system and routes management traffic to a separate physical network, it can be separated from the application traffic.



NOTE: This option is available only if an iDRAC6 Enterprise controller is present in the system.

- **Shared with failover** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through the LAN on motherboard LOM 1 and LOM 2, but it transmits data only through LOM 1. If LOM 1 fails, the remote access device fails over to LOM 2 for all data transmission. The remote access device continues to use LOM 2 for data transmission. If LOM 2 fails, the remote access device fails over all data transmission back to LOM 1.
- **Shared with failover - LOM 2** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through the LAN on Motherboard LOM 1 and LOM 2, but transmits data only through LOM 2. If LOM 2 fails, the remote access device fails over to LOM 1 for all data transmission. The remote access device continues to use LOM 1 for data transmission. If LOM 1 fails, the remote access device fails over all data transmission back to LOM 2. If one LOM fails but is later restored, you can manually revert back to the original LOM settings by editing the NIC selection through the **iDRAC Hardware Configuration** wizard.
- **Shared with failover - All LOMS** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating

system is configured for NIC teaming. The remote access device receives data through NIC 1, NIC 2, NIC 3, and NIC 4; but it transmits data only through NIC 1. If NIC 1 fails, the remote access device will transmit data on NIC 2. If NIC 2 fails, the remote access device will transmit data on NIC 3. If NIC 3 fails, the remote access device will transmit data on NIC 4. If NIC 4 fails the remote access device fails over all data transmission back to NIC 1, but only if the original NIC 1 failure has been corrected.



NOTE: Shared with failover - All LOMS option may not be available on iDRAC6 Enterprise controller.

Advanced LAN Configuration

- 1** Set additional attributes for VLAN, VLAN ID, VLAN priority, Auto Negotiate, LAN speed, and LAN duplex.
 - **VLAN** — Enables or disables the VLAN mode of operation and parameters. When VLAN is enabled, only matched VLAN ID traffic is accepted. When disabled, VLAN ID and VLAN Priority are not available, and any values present for those parameters are ignored.
 - **VLAN ID** — Sets the VLAN ID value. Legal values fall in the range of 1 to 4094, as defined by IEEE 801.1g specification.
 - **VLAN Priority** — Sets the VLAN ID priority value. Legal values fall in the range of 0 to 7, as defined by IEEE 801.1g specification.
 - **Auto Negotiate** — Turns the auto-negotiate feature on or off. When auto-negotiate is on, it determines whether iDRAC automatically sets the **Duplex Mode** and **Network Speed** values by communicating with the nearest router or hub. When auto-negotiate is off, you must set the **Duplex Mode** and **Network Speed** values manually.
 - **LAN Speed** — Configures the network speed to 100 Mb or 10 Mb to match the user's network environment. This option is not available if **Auto-Negotiate** is set to **On**.
 - **LAN Duplex** — Configures the duplex mode to **Full** or **Half** to match the user's network environment. This option is not available if **Auto-Negotiate** is set to **On**.
- 2** Click **OK** to save your settings and return to the **LAN Configuration** menu.
- 3** Click **Next** to proceed to "Common IP Configuration."

Common IP Configuration

Register the iDRAC name, set the domain name from DHCP, and specify the domain name and host name string.

- **Register iDRAC Name** — If set to **Yes**, the iDRAC name is registered with the Domain Name System (DNS). If set to **No**, no registration takes place.
- **iDRAC Name** — Enables you to view or edit the iDRAC name to be used when registering with DNS. The **iDRAC Name** string can contain up to 63 printable ASCII characters. You can edit the **iDRAC Name** string when **Register iDRAC Name** is **No**. The information in this field is erased after updating the iDRAC firmware.
- **Domain Name from DHCP** — If set to **Yes**, iDRAC acquires the domain name from the Dynamic Host Configuration Protocol (DHCP) server. If set to **No**, you must enter the domain name manually.
- **Domain Name** — Enables you to view or edit the iDRAC domain name to be used if it is not acquired from DHCP. You can specify a domain name when **Domain Name from DHCP** is set to **No**. The information in this field is erased after updating the iDRAC firmware.
- **Host Name String** — Enables you to specify or edit the host name associated with iDRAC. The information in this field is erased if iDRAC is reset to the original defaults or if the iDRAC firmware is updated. The **Host Name** string can contain up to 62 ASCII printable characters.

Click **Next** to proceed to "IPv4 Configuration."

IPv4 Configuration

Enable or disable IPv4, and set the RMCP+ encryption key, IP address source, subnet mask, default gateway, and DNS server values.

- **IPv4** — Enables or disables iDRAC NIC IPv4 protocol support. Disabling IPv4 deactivates the remaining controls.
- **RMCP+Encryption Key** — Configures the RMCP+ encryption key using 0 to 40 hexadecimal digits (no blanks allowed). The default setting is all zeros (0).
- **IP Address Source** — Enables or disables the ability of the iDRAC NIC to acquire an IPv4 address from the DHCP server; deactivate or activate the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** controls.

- **Ethernet IP Address** — Enables you to specify or edit a static IPv4 address for the iDRAC NIC. The IP address you enter in the **Ethernet IP Address** field is reserved, and used only when DHCP fails to resolve and assign an available IP address. The **Ethernet IP Address** field is limited to a maximum value of 255.255.255.255.
- **Subnet Mask** — Enables you to specify or edit the static subnet mask for the iDRAC NIC. The subnet mask defines the significant bit positions in the IPv4 address. The **Subnet Mask** string should be in the form of a netmask, where the more significant bits are all ones (1) with a single transition to all zeros (0) in the lower-order bits. For example: 255.255.255.0. The **Subnet Mask** field is limited to a maximum value of 255.255.255.255.
- **Default Gateway** — Enables you to specify or edit the static IPv4 default gateway for the iDRAC NIC. Requests that cannot be resolved locally are routed to this address. The **Default Gateway** field is limited to a maximum value of 255.255.255.255.
- **Get DNS Servers from DHCP** — If set to **Yes**, the iDRAC NIC acquires the Domain Name System (DNS) server information from the DHCP server, and deactivates the **DNS Server 1** and **DNS Server 2** controls. If set to **No**, the iDRAC NIC does not acquire the DNS Server information from the DHCP server, and you must manually define the **DNS Server 1** and **DNS Server 2** fields.
- **DNS Server 1** — Enables you to specify or edit the static IPv4 address for a primary DNS server. This IPv4 address is that of a DNS server utilized for name-to-IPv4 address resolution. The **DNS Server 1** field is limited to a maximum value of 255.255.255.255.
- **DNS Server 2** — Enables you to specify or edit the static IPv4 address for a secondary DNS server. In the event that DNS Server 1 does not produce results, the **DNS Server 2** IPv4 address serves as a backup utilized for name-to-IPv4 address resolution. This field is limited to a maximum value of 255.255.255.255.

Click **Next** to proceed to "IPv6 Configuration."

IPv6 Configuration

Set IPv6, IP address source, ethernet IP address, IPv6 address, prefix length, default gateway, and DNS server values.

- **IPv6** — Enables or disables the iDRAC NIC IPv6 protocol support. Disabling IPv6 deactivates the remaining controls.
- **IP Address Source** — Enables or disables the ability of the iDRAC NIC to acquire an IPv6 address from the DHCP server. Disabling **IP Address Source** deactivates the **Ethernet IP Address**, **Prefix Length**, and **Default Gateway** controls.
- **Ethernet IP Address** — Enables you to specify or edit the static IPv6 address for the iDRAC NIC when not provided by DHCP. This field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The multi-cast (ff00/8) and loopback (::1/128) values are not valid addresses for the Ethernet IP address and/or the other address related fields described in this section. IPv6 Address forms supported:
 - **X:X:X:X:X:X:X** — In this preferred form, **X** represents the hexadecimal values of the eight 16-bit pieces of the address. You can omit leading zeros in individual fields, but you must include at least one numeral in every field.
 - **::** (two colons) — Using this form, you can represent a string of contiguous zero fields in the preferred form. The **::** can only appear once in the address. You can also use this form to represent unspecified addresses (0:0:0:0:0:0:0:0).
 - **x:x:x:x:d.d.d.d** — This form is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes. In this form, **x** represents the hexadecimal values of the six high-order 16-bit pieces of the address, and **d** represents the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).
- **Prefix Length** — Enables you to specify or edit the number of significant bits in the IPv6 address to be used as a prefix, up to a maximum of 128. The prefix length number of bits in the Ethernet IP address is the netmask for the IPv6 network to which the iDRAC NIC belongs. The more significant bits that are defined, the fewer IPv6 addresses will be available on the network with the specified prefix.

- **Default Gateway** — Enables you to specify or edit the static IPv6 default gateway for the iDRAC NIC when not provided by DHCP. This is the address that will be used to route requests when they cannot be resolved locally. The **Default Gateway** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
- **Get DNS Servers from DHCP** — If set to **Yes**, the iDRAC NIC acquires the Domain Name System (DNS) server information from the DHCP server and deactivates the DNS Server 1 and DNS Server 2 controls. If set to **No**, the iDRAC NIC does not acquire the DNS server information from the DHCP server, and you must manually specify the DNS Server 1 and DNS Server 2 fields.
- **DNS Server 1** — Enables you to specify or edit the static IPv6 address for a primary DNS server when not provided by DHCP. The **DNS Server 1** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The IPv6 address is that of a DNS server utilized for name-to-IPv6 address resolution.
- **DNS Server 2** — Enables you to specify or edit the static IPv6 address for a secondary DNS server when not provided by DHCP. In the event that DNS Server 1 does not produce results, the DNS Server 2 IPv6 address serves as a backup DNS server utilized for name-to-IPv6 address resolution. The **DNS Server 2** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Click **Next** to proceed to "Virtual Media Configuration."

Virtual Media Configuration

Set Virtual Media and Virtual Flash parameters.

The Virtual Media and Virtual Flash features are available only if the system includes iDRAC 6 Enterprise. The Virtual Flash feature is only available if an SD card is installed and enabled in the iDRAC.

- **Virtual Media** — Select attached, auto-attached, or detached mode. If set to **Attach**, the virtual media devices are available for use in the current operating environment. Virtual Media enables a floppy image, floppy drive, or CD/DVD drive from your system to be available on the managed systems console, as if the floppy image or drive were present (attached or connected) on the local system. If set to **Detach**, you cannot access virtual

media devices. If set to **Auto-Attach**, the virtual media device is automatically mapped to the server every time the user physically connects a media.

- **vFlash Status** — Displays the status as either:
 - Formatted
 - Not formatted
 - Not present
 - Not licensed (the vFlash is not Dell-licensed)

For more information on supported virtual media devices, see the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* available at support.dell.com/manuals.

- **vFlash** — Enable or disable the use of flash memory that resides in the iDRAC file system. This memory can be used for persistent storage and accessed by the system. If set to **Enabled**, the virtual flash card is configured as a virtual drive; it appears in the boot order, allowing you to boot from the virtual flash card. If set to **Disabled**, virtual flash is not accessible.

Prerequisites to Enable or Disable vFlash

- To boot from the virtual flash, the virtual flash image must be bootable. The virtual flash feature of iDRAC requires a formatted secure digital (SD) card that is 256 MB or greater. This feature can be enabled only if a valid image is present on the SD card. See the *User Guide* for your system's iDRAC device for more information.
- Dell-branded vFlash media is required for the virtual flash partition.

Click **Next** to proceed to "LAN User Configuration."

LAN User Configuration

Set account access, account-related attributes, and smart card authentication using one of the following methods:

- **Auto-Discovery** - Enables or disables auto-discovery.
- **Provisioning Server Address** - Enables you to enter the Provisioning Server address; valid address formats are IPv4, IPv6, or the provisioning server hostname.

Provisioning Server address criteria are:

- A list of IP addresses and/or hostnames and ports separated by comma.
- Hostname can be fully qualified.
- IPv4 address – starts with ‘(‘ and ends with ‘)’ when specified at the same time with a hostname.
- Each IP address or hostname can be optionally followed by a ‘:’ and a port number.
- Example of valid strings are - hostname, hostname.domain.com
- **Account Access** — Enables or disables account access. Disabling account access deactivates all other fields on the **LAN User Configuration** screen.
- **Account Username** — Enables the modification of an iDRAC username. The **Account Username** field accepts a maximum of 16 printable ASCII characters.
- **Password** — Enables an administrator to specify or edit the iDRAC user's password. The **Password** string is encrypted and cannot be seen or displayed after this property is set. The **Password** field accepts a maximum of 20 characters.
- **Confirm Password** — Re-enter the iDRAC user's password to confirm.
- **Account Privilege** — Assigns the user's maximum privilege on the IPMI LAN channel to one of the following user groups: Admin, Operator, User, or No Access.
 - **Admin** — Privileges: Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands
 - **Operator** — Privileges: Login to iDRAC, Configure iDRAC, Configure Users, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands
 - **User** — Privileges: Login to iDRAC
 - **No Access** — No assigned privileges
- **Smart Card Authentication** — Enables or disables Smart Card Authentication for iDRAC log in. If enabled, a Smart Card must be installed to access the iDRAC.

- **Enabled** — Enabling Smart Card login disables all command-line out-of-band interfaces including SSM, Telnet, Serial, remote RACADM, and IPMI over LAN.
- **Disabled** — On subsequent logins from the graphical user interface (GUI), the regular login page displays. All command-line out-of-band interfaces—including Secure Shell (SSH), Telnet, Serial, and RACADM—are set to their default states.
- **Enabled with RACADM** — Enabling smart card login with RACADM disables all command-line out-of-band interfaces—including SSM, Telnet, Serial, remote RACADM, and IPMI over LAN—while still allowing RACADM access.

Click **Next** to proceed to "Summary."

Summary

Displays the summary of the iDRAC configuration changes.

Click **Apply** to proceed to "Confirmation."

Confirmation

Confirm the changes you made by viewing the **Summary** screen. You can apply the changes, or cancel all changes and exit the **iDRAC Configuration Wizard**. If you apply the changes, a **Please Wait** message displays while your changes are saved. When the operation is complete, a final **Confirmation** screen displays indicating whether the changes were applied successfully, left unchanged, or failed.

Click **Finish** to save your settings and return to the main wizards screen.

RAID Configuration

If your system has one or more supported PERC RAID controller(s) with PERC 6.1 firmware or greater or SAS RAID controller(s), you have the option of using the **RAID Configuration** wizard to configure a virtual disk as the boot device.

To launch the **RAID Configuration Wizard**:

- 1** Click **Hardware Configuration** in the left pane.
- 2** Click **Configuration Wizards** in the right pane.
- 3** Click **RAID Configuration** to launch the wizard.

The following steps will walk you through the **RAID Configuration** wizard:

- a "View Current Configuration"
- b "Select RAID Controller"
- c "Foreign Configuration Found"
- d "Select the Express or Advanced Wizard"
- e "Select Basic Settings"
- f "Express Wizard Only - Assign a Hot Spare"
- g "Express Wizard Only - Review Summary"
- h "Advanced Wizard Only - Select Physical Disks"
- i "Advanced Wizard Only - Additional Settings"
- j "Advanced Wizard Only - Review Summary"

View Current Configuration

The **View Current Configuration** screen displays the attributes of any virtual disks already configured on the supported RAID controllers attached to the system. You have two options:

- Accept the existing virtual disks without making changes. To select this option, click **Back**. If you intend to install the operating system on an existing virtual disk, ensure that the virtual disk size and RAID level are appropriate.
- Delete all existing virtual disks and use the **RAID configuration** wizard to create a single, new virtual disk to be used as the new boot device. To select this option, click **Next**.



NOTE: RAID 0 does not provide data redundancy. Other RAID levels provide data redundancy and may enable you to reconstruct data in the event of a disk failure.

Select RAID Controller

The **Select RAID Controller** screen displays all supported RAID controllers attached to the system. Select the RAID controller on which you want to create the virtual disk, and then click **Next**.

Foreign Configuration Found

The **Foreign Configuration Found** screen displays only if a foreign configuration resides on the selected RAID controller.

A foreign configuration is a set of physical disks containing a RAID configuration that has been introduced to the system but is not yet managed by the RAID controller to which it is attached. You may have a foreign configuration if physical disks have been moved from a RAID controller on another system to a RAID controller on the current system.

You have two options: **Ignore Foreign Configuration** and **Clear Foreign Configuration**.

- If the foreign configuration contains data that you want to keep, select **Ignore Foreign Configuration**. If you select this option, the disk space containing the foreign configuration is not available for use in a new virtual disk.
- To delete all data on the physical disks containing the foreign configuration, select **Clear Foreign Configuration**. This option frees the disk space containing the foreign configuration and makes it available for use in a new virtual disk.

Click **Next** after making your selection.

Select the Express or Advanced Wizard

- Create a virtual disk using either the **Express Wizard** or the **Advanced Wizard**.
- The **Express Wizard** enables you to select the RAID level only. The **Express Wizard** then selects a virtual disk configuration for the user which implements the selected RAID level and optionally enables you to assign a hot spare. Select **Express Wizard** to quickly create a virtual disk using recommended settings. This wizard is not available on all controllers.



NOTE: If the available physical disks are using both Serial Attached SCSI (SAS) and Serial ATA (SATA) protocols, it is recommended that you use the **Advanced Wizard**.

- The **Advanced Wizard** enables you to specify which protocol is used when creating the disk pool for the virtual disks. A disk pool is a logical grouping of disks attached to a RAID controller on which one or more virtual disks can be created. In addition to the RAID level, the **Advanced Wizard** allows

more flexibility with physical disk selection, span configuration, cache policy, and other virtual disk attributes. Select **Advanced Wizard** to specify all virtual disk settings.



NOTE: It is recommended that you have a good knowledge of RAID and your hardware configuration to use the **Advanced Wizard**.

Click **Next** after making your selection.

Select Basic Settings

Select the RAID type for the virtual disk from the **RAID Level** drop-down menu:

- **RAID 0** — Stripes data across the physical disks. RAID 0 does not maintain redundant data. When a physical disk fails in a RAID 0 virtual disk, there is no method for rebuilding the data. RAID 0 offers good read and write performance with 0 data redundancy.
- **RAID 1** — Mirrors or duplicates data from one physical disk to another. If a physical disk fails, data can be rebuilt using the data from the other side of the mirror. RAID 1 offers good read performance and average write performance with good data redundancy.
- **RAID 5** — Stripes data across the physical disks, and uses parity information to maintain redundant data. If a physical disk fails, the data can be rebuilt using the parity information. RAID 5 offers good read performance and slower write performance with good data redundancy.
- **RAID 6** — Stripes data across the physical disks, and uses two sets of parity information for additional data redundancy. If one or two physical disks fail, the data can be rebuilt using the parity information. RAID 6 offers better data redundancy and read performance but slower write performance with very good data redundancy.
- **RAID 10** — Combines mirrored physical disks with data striping. If a physical disk fails, data can be rebuilt using the mirrored data. RAID 10 offers good read and write performance with good data redundancy.
- **RAID 50** — A dual-level array that uses multiple RAID 5 sets in a single array. A single physical disk failure can occur in each of the RAID 5 without any loss of data on the entire array. Although the RAID 50 has increased write performance, when a physical disk fails and reconstruction takes place, performance decreases, data/program access is slower, and transfer speeds on the array are affected.

- **RAID 60** — Combines the straight block level striping of RAID 0 with the distributed double parity of RAID 6. Your system must have at least eight physical disk to use RAID 60. Because RAID 60 is based on RAID 6, two physical disk from each of the RAID 6 sets could fail without loss of data. Failures while a single physical disk is rebuilding in one RAID 6 set do not lead to data loss. RAID 60 has improved fault tolerance because more than half the number of total physical disk must fail for data loss to occur.



NOTE: The virtual disk size is automatically calculated and displayed in the **Size** field. You cannot change the virtual disk size. The disk size may be displayed inaccurately after you complete RAID configuration for a SAS 6/iR controller.

If you are using the **Express Wizard**, proceed to "Express Wizard Only - Assign a Hot Spare."

If you are using the **Advanced Wizard**, click **Next** and proceed to "Advanced Wizard Only - Select Physical Disks."

Express Wizard Only - Assign a Hot Spare

A hot spare is an unused backup physical disk that can be used to rebuild data from a redundant virtual disk. A hot spare can be used only with a redundant RAID level. Hot spares also have requirements for physical disk size. The hot spare must be as big as or bigger than the smallest physical disk included in the virtual disk. If the RAID level and physical disk availability do not meet these requirements, a hot spare will not be assigned.

To assign a hot spare to the virtual disk:

- 1 Select the **Assign a Hot Spare Disk** check box or leave the check box clear.
- 2 Click **Next** to continue with "Express Wizard Only - Review Summary."

Express Wizard Only - Review Summary

Review the virtual disk attributes you selected before creating a virtual disk.



CAUTION: Clicking the **Finish** button deletes all existing virtual disks except for any foreign configurations that you specified should be kept. All data residing on the deleted virtual disks will be lost.

Click **Finish** to create a virtual disk with the displayed attributes.

OR

To return to a previous screen to review or change selections, click **Back**. To exit the Wizard without making changes, click **Cancel**. For more control over the virtual disk attributes, click **Cancel** and use the **Advanced Wizard** to create the virtual disk.

Advanced Wizard Only - Select Physical Disks

Use the **Select Physical Disks** screen to select the physical disks to be used for the virtual disk. The number of physical disks required for the virtual disk varies depending on the RAID level. The minimum and maximum numbers of physical disks required for the RAID level are displayed on the screen.

- Select the protocol for the disk pool from the **Protocol** drop-down menu: **Serial Attached SCSI (SAS)** or **Serial ATA (SATA)**. SAS drives are used for high performance, and SATA drives provide a more cost-effective solution. A disk pool is a logical grouping of physical disks on which one or more virtual disks can be created. The protocol is the type of technology used to implement RAID.
- Select the media type for the disk pool from the **Media Type** drop-down menu: **Hard Disk Drives (HDD)** or **Solid State Disks (SSD)**. HDDs use traditional rotational magnetic media for data storage, and SSDs implement flash memory for data storage.
- Select the span length from the **Select Span Length** drop-down menu. The span length value refers to the number of physical disks included in each span. Span length applies only to RAID 10, RAID 50, and RAID 60. The **Select Span Length** drop-down menu is active only if the user has selected RAID-10, RAID-50, or RAID 60.
- Select the physical disks using the check boxes at the bottom of the screen. Your physical disk selection must meet the requirements of the RAID level and span length. To select all of the physical disks, click **Select All**.

Click **Next** after making your selections.

Advanced Wizard Only - Additional Settings

Use the **Additional Settings** screen to specify cache policies and stripe element size. You can also assign a hot spare to the virtual disk.


- Select the stripe element size from the **Stripe Element Size** drop-down menu. The stripe element size is the amount of disk space a stripe consumes on each physical disk in the stripe. The **Stripe Element Size** drop-down menu may contain more options than initially displayed on the screen. Use the up-arrow and down-arrow keys to display all options.
- Select the read policy from the **Read Policy** drop-down menu.
 - **Read Ahead** — The controller reads sequential sectors of the virtual disk when seeking data. The Read Ahead policy may improve system performance if the data is written to sequential sectors of the virtual disk.
 - **No Read Ahead** — The controller does not use the Read Ahead policy. The No Read Ahead policy may improve system performance if the data is random and not written to sequential sectors.
 - **Adaptive Read Ahead** — The controller initiates the Read Ahead policy only if the most recent read requests accessed sequential sectors of the disk. If the recent read requests accessed random sectors of the disk, then the controller uses the No Read Ahead policy.
- Select the write policy from the **Write Policy** drop-down menu.
 - **Write Through** — The controller sends a write-request completion signal only after the data is written to the disk. The Write Through policy provides better data security than the Write Back policy since the system assumes the data is available only after it has been written to the disk.
 - **Write Back** — The controller sends a write-request completion signal as soon as the data is in the controller cache but has not yet been written to disk. The Write Back policy may provide faster write performance, but it also provides less data security since a system failure could prevent the data from being written to disk.
 - **Force Write Back** — The write cache is enabled regardless of whether the controller has an operational battery. If the controller does not have an operational battery, data loss may occur in the event of a power failure.
- To assign a hot spare to the virtual disk, select the **Assign a Hot Spare Disk** check box. A hot spare is an unused backup physical disk that can be used to rebuild data from a redundant virtual disk.

- Select the physical disk to be used as the hot spare from the **Hot Spare Disk** drop-down menu. A hot spare can be used only with a redundant RAID level. Hot spares also have requirements for physical disk size. The hot spare cannot be smaller than the smallest physical disk included in the virtual disk. If the RAID level and physical disk availability do not meet these requirements, the **Assign a Hot Spare Disk** check box is disabled.

Click **Next** after making your selection.

Advanced Wizard Only - Review Summary

The **Summary** screen displays the virtual disk attributes based on your selections.

 **CAUTION: Clicking the **Finish** button deletes all existing virtual disks except for any foreign configurations that you specified should be kept. All data residing on the deleted virtual disks will be lost.**

Click **Finish** to create a virtual disk with the displayed attributes.

OR

To return to a previous screen to review or change selections, click **Back**. To exit the Wizard without making changes, click **Cancel**.

Advanced Configuration

Use **Advanced Configuration** to modify advanced settings.

- 1 Select **Hardware Configuration** from the left menu
- 2 Click **Advanced Configuration** in the right panel.
- 3 Select the device you want to configure.

Depending on the configuration setting changes, the following message may be displayed: **One or more of the settings requires a reboot to be saved and activated. Do you want to reboot now?** You can select **No** and continue making additional configuration changes or perform other tasks such as operating system deployment. All changes will be applied during the next system boot.

USC - LCE Hardware Configuration allows you to configure other devices through Human Interface Infrastructure (HII). HII is a UEFI-standard method for viewing and setting a device's configuration. You can utilize a single utility to configure multiple devices that had different pre-boot

configuration utilities in the past. HII also provides localization, meaning that utilities that were previously English-only, such as the BIOS <F2> setup, may now have a localized HII equivalent.

As of the current release of USC - LCE, your server's default configuration contains setups for two device types that are supported in the Hardware Configuration Advanced Configuration: the system **BIOS** and **NIC**.

- The **BIOS** setup is very similar to the current setup utility (press the <F2> key during system startup); however, HII can access only a subset of the utilities available in system startup.
- The **NIC** setup reflects various NIC attributes, some of which were visible in the controller option read-only memory (ROM). However, many of these attributes were previously only modifiable in Operating System utilities.

Depending on your system configuration, other device types may also appear in Advanced Configuration, if they support the HII configuration standard.

Advanced Configuration wizard allows you to configure the following:

- System BIOS Settings
- Intel Pro/1000 PT Server Adapter
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Gigabit VT Quad Port Server Adapter
- Intel 10 Gigabit AF DA Dual Port Server Adapter
- Intel 10 Gigabit AT Port Server Adapter
- Intel 10 Gigabit XF SR Port Server Adapter
- Broadcom (Dual Port) 10G KX4
- Broadcom (Quad Port) GBE
- Intel (Quad Port) GBE
- Intel (Dual Port) 10G KX4
- Broadcom (Dual Port) 10G SFP+
- Broadcom (Quad Port) 10/100/1000 BASET
- Intel (Quad Port) 10/100/1000 BASET
- Intel (Dual Port) 10/100/1000 BASET
- Broadcom NetXtreme Gigabit Ethernet
- Broadcom 5709C NetXtreme II GigE
- Broadcom 5709C NetXtreme II GigE

- Broadcom 57710 NetXtreme II 10GigE

Important

- You can configure only one NIC at a time.
- Integrated Broadcom NICs are controlled both by the BIOS and by settings stored on the device itself. As a result, the **Boot Protocol** field in the HII of integrated NICs has no effect; this setting is instead controlled by the BIOS on the **Integrated Devices** screen. To set integrated NICs to an iSCSI or PXE boot mode, select **System BIOS Settings**, then select **Integrated Devices**. On this screen, you will see a list of each embedded NIC—select the appropriate value: **Enabled** for no boot capability, **Enabled with PXE** to use the NIC for PXE boot, or **Enabled with iSCSI** to use the NIC to boot from an iSCSI target.

Part Replacement

Part replacement configuration is an automatic update of the firmware for a new part to the level of the previous part if enabled; the update occurs automatically when you reboot your system after replacing the part. It is activated by a license, and can be disabled remotely, as well as through the USC interface.

Prerequisites

- Part replacement configuration is a licensed feature. Your system should be equipped with a Dell-licensed vFlash card for this functionality.
- When **Collect System Inventory On Restart** is disabled, the cache of system inventory information may become stale if new components are added without manually entering USC after power on.
- The replaced card should belong to the same family as the previous component.

Supported Devices

The following devices can have part replacement firmware updates:

- NICs (Broadcom)
- PERC, SAS and CERC series 6 and 7
- Power Supply Units

Collect System Inventory on Restart

When you enable the **Collect System Inventory On Restart** property, hardware inventory and part configuration information is discovered and compared with previous system inventory information on every system restart.

- 1 Click **Hardware Configuration** on the left pane.
- 2 Click on **Part Replacement Configuration**.
- 3 Click either **Enabled** or **Disabled** from the **Collect System Inventory on Restart** dropdown.

Part Firmware Update

This setting allows you to configure the action to be taken when part replacement is detected.

From the part firmware update drop down, select one of the following:

- **Disabled** - Firmware update on replaced parts will not be performed.
- **Allow version upgrade only** - Firmware update on replaced parts will only be performed if the firmware version of the new part is lower than the existing part.
- **Match firmware of replaced part** - Firmware on the new part will be updated to the version of the original part.

Configuring a Local FTP Server

If your organization's users are on a private network that does not have access to external sites, specifically **ftp.dell.com**, you can provide platform updates from a locally-configured FTP server. The users in your organization can access updates or drivers for their Dell server from the local FTP server instead of **ftp.dell.com**. A local FTP server is not required for users who have access to **ftp.dell.com** through a proxy server. Check **ftp.dell.com** frequently to make sure your local FTP server has the most recent updates.

Requirements for a Local FTP Server

The following requirements apply when configuring a local FTP server.

- The local FTP server must use the default port (21).

- You must use **USC Settings** wizard to configure the network card on your system before accessing updates from the local FTP server. See "Using USC Settings Wizard" for more information.

Creating the Local FTP Server Using Dell Server Updates DVD

- 1 Download the *Dell Server Updates* ISO to your system from Dell Support site at support.dell.com, and burn it to a DVD.
- 2 Copy the repository folder of the DVD you just created to the root directory of the local FTP server.
- 3 Use this local FTP server for Platform Update.

Creating the Local FTP Server Using Dell Repository Update Manager

See the *Dell Repository Manager User Guide* on the Dell Support site at support.dell.com/manuals for information on creating a local FTP server using Dell Repository Update Manager.

Accessing Updates on a Local FTP Server

The users in your organization need to know the IP address of the local FTP server in order to specify the online repository when using the **OS Deployment** wizard.

If your users are accessing the local FTP server through a proxy server, then they need to know the following information for the proxy server:

- The proxy server host name or IP address
- The port number of the proxy server
- The user name required for authentication on the proxy server
- The password required for authentication on the proxy server
- The type of proxy server

Configuring a Local USB Device

If your organization's users are on a private network that does not have access to external sites like ftp.dell.com, you can provide updates from a locally-configured USB device.

The USB device you use as a repository must be able to hold at least 3 GB of content.

A USB device is not required for users that have access to <ftp.dell.com> through a proxy server.

For the latest updates, download the most recent *Dell Server Updates* ISO for your system from the Dell Support website at <support.dell.com>.

Creating the Local USB Repository Using Dell Server Updates DVD

To create a repository on a local USB device using *Dell Server Updates* DVD:

- 1** Download the *Dell Server Updates* ISO to your system from the Dell Support site at <support.dell.com>, and burn it to a DVD.
- 2** Copy the repository folder of the DVD you just created to the root directory of the USB device.
- 3** Use this USB device for Platform Update with the catalog location as `\repository`.

Creating the Local USB Repository Using Dell Repository Update Manager

See the Dell Repository Manager User Guide on the Dell Support site at <support.dell.com/manuals> for information on creating a local USB device using Dell Repository Update Manager.

Remote Service Features

The Dell™ Lifecycle Controller Remote Services are a set of features that allow systems management in a one-to-many mode. Remote Services capabilities use the web services based hardware management interface provided by the Lifecycle Controller firmware. They are aimed at simplifying tasks like operating system deployment, remote update and inventory, and automating the setup and configuration of new Dell systems remotely.

Web Services for Management

Web Services for Management (WS-MAN) is a Simple Object Access Protocol (SOAP)-based protocol designed for systems management. WS-MAN is published by the Distributed Management Task Force (DMTF) and provides an interoperable protocol for devices to share and exchange data across networks. The WS-MAN implementation complies with the DMTF WS-MAN specification version 1.0.0.

Dell Lifecycle Controller - Remote Services uses WS-MAN to convey DMTF Common Information Model (CIM)-based management information; the CIM information defines the semantics and information types that can be manipulated in a managed system. The Dell-embedded server platform management interfaces are organized into profiles, where each profile defines the specific interfaces for a particular management domain or area of functionality. Additionally, Dell has defined a number of model and profile extensions that provide interfaces for additional capabilities. The data and methods available through WS-MAN are provided by the Lifecycle Controller - Remote Services' instrumentation interface mapped to the following DMTF profiles and Dell extension profiles:

Standard DMTF

- Base Server — defines CIM classes for representing the host server.
- Base Metrics — defines CIM classes for providing the ability to model and control metrics captured for managed elements.

- Host LAN Network Port — defines CIM classes for representing a network port that provides a LAN interface to a host system, its associated controller, and network interfaces.
- Service Processor — defines CIM classes for modeling service processors.
- USB Redirection — defines CIM classes for describing information about USB redirections. For keyboard, video, and mouse devices, this profile should be used if the devices are to be managed as USB devices.
- Physical Asset — defines CIM classes for representing the physical aspect of the managed elements.
- SM CLP Admin Domain — defines CIM classes for representing CLP's configuration.
- Power State Management — defines CIM classes for power control operations.
- Command Line Protocol Service — defines CIM classes for representing CLP's configuration.
- IP Interface — defines CIM classes for representing an IP interface of a managed system.
- DHCP Client — defines CIM classes for representing a DHCP client and its associated capabilities and configuration.
- DNS Client — defines CIM classes for representing a DNS client in a managed system.
- Record Log — defines CIM classes for representing different type of logs.
- Role Based Authorization — defines CIM classes for representing roles.
- SMASH Collections — defines CIM classes for representing CLP's configuration.
- Profile Registration — defines CIM classes for advertising the profile implementations.
- Simple Identity Management — defines CIM classes for representing identities.
- SSH Service — defines CIM classes for extending the management capability of referencing profiles by adding the capability to represent an SSH service and its associated sessions in a managed system.

- Battery — defines CIM classes for describing and setting the logical properties of the battery. Such properties include the description of the battery's charge status and the time it takes for the battery charge to be depleted. The profile also describes operations such as recharging the battery.

Dell Extensions

- Dell Active Directory Client Version 2.0.0 — defines CIM and Dell extension classes for configuring the Active Directory client and the local privileges for Active Directory groups.
- Dell Virtual Media — defines CIM and Dell extension classes for configuring Virtual Media. Extends the USB Redirection Profile.
- Dell Ethernet Port — defines CIM and Dell extension classes for configuring NIC Side-Band interface for the NIC. Extends the Ethernet Port Profile.
- Dell Power Utilization Management — defines CIM and Dell extension classes for representing the host server's power budget and for configuring/monitoring the host server's power budget.
- Dell OS Deployment — defines CIM and Dell extension classes for representing the configuration of operating system deployment features. It extends the management capability of referencing profiles by adding the capability to support operating system deployment activities by manipulating operating system deployment features provided by the service processor. For more information on Dell OS Deployment functions, see "Remote Operating System Deployment Interface."
- Dell Software Update Profile — defines CIM and Dell extensions for representing the service class and methods for updating BIOS, component firmware, Lifecycle Controller firmware, Diagnostics, and Driver Pack. Update methods support update from CIFS, NFS, FTP, and HTTP network share locations and from update images located in the Lifecycle Controller. Update requests are formulated as jobs and can be scheduled immediately or at a later time with a choice of types of reboot action to apply the updates.

- Dell Software Inventory Profile — Defines CIM and Dell Extensions for representing currently installed BIOS, component firmware, Diagnostics, Unified Server Configurator, and Driver Pack versions. Also provides representation of versions of BIOS and firmware update images available in Lifecycle Controller for rollback and re-installation.
- Dell Job Control Profile — Defines CIM and Dell extensions for managing jobs generated by update requests. Jobs can be created, deleted, modified and aggregated into job queues to sequence and perform multiple updates in a single reboot.
- Lifecycle Controller Management Profile — Defines CIM and Dell extensions for getting and setting attributes for managing Auto-Discovery and Part Replacement Lifecycle Controller features.

The Lifecycle Controller - Remote Services WS-MAN implementation uses SSL on port 443 for transport security, and supports basic and digest authentication. Web services interfaces can be utilized by leveraging client infrastructure such as Windows® WinRM and Powershell CLI, open source utilities like WS-MANCLI, and application programming environments like Microsoft® .NET®.

There are additional implementation guides, white papers, profile specifications, class definition (.mof) files, and code samples available in the Dell Tech Center at www.delltechcenter.com. See:

- Lifecycle Controller area -
<http://www.delltechcenter.com/page/Lifecycle+Controller>
- Dell CIM Extension Specifications
<http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions>
- Lifecycle Controller WS-MAN Script Center
<http://www.delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller>

For more information, also see the following:

- DTMF Web site: www.dmtf.org/standards/profiles/
- WS-MAN release notes or Readme file.

What's New in Remote Services 1.3

These are the new features introduced in 1.3:

- Auto-Discovery enhancements
- Remote firmware inventory and update
- Operating system deployment using Dell-licensed vFlash
- Part replacement

Auto-Discovery

The Auto-Discovery feature allows newly installed servers to automatically discover the remote management console that hosts the Provisioning Server. The Provisioning Server provides custom administrative user credentials to the iDRAC so that the unprovisioned server can be discovered and managed by the management console.

When Auto-Discovery is enabled, the iDRAC6 requests an IP address from DHCP and either acquires the name of the Provisioning Server host and/or subsequently resolves the address through DNS. After acquiring the Provisioning Server host address, the iDRAC6 securely handshakes before acquiring custom administrative account credentials. The iDRAC can now be managed through its newly acquired credentials to perform operations, such as remote operating system deployment.

If you ordered a Dell system with the Auto-Discovery feature **Enabled** (factory default setting is **Disabled**), then the iDRAC will be delivered with DHCP-enabled and no enabled user accounts. If the auto-discovery feature is set to **Disabled**, you can manually enable this feature and disable the default administrative account from the **iDRAC6 Configuration Utility** when booting your system. For more information on Enabling and Disabling Auto-Discovery feature, see "Auto-Discovery Configuration."

Configuring DHCP/DNS

Before adding your Dell system to the network and utilizing the Auto-Discovery feature, ensure that Dynamic Host Configuration Protocol (DHCP) server/Domain Name System (DNS) are configured with added

support for Auto-Discovery. There are several options for enabling the network environment to support discovery of the Provisioning Server host by unprovisioned servers.

One of the following prerequisites must be met for the Auto-Discovery feature to work properly:

- The DHCP server provides a comma separated list of Provisioning Server locations using a vendor scope option of class LifecycleController option 1. These locations can be a hostname or IP address and optionally include a port. The iDRAC will resolve the hostname of the management console to an IP address with a DNS lookup.
- The DNS server specifies a service option `_dcimprovsrv._tcp` that will resolve to an IP address.
- The DNS server specifies an IP address for a server with the known name `DCIMCredentialServer`.

For more information on configuring DHCP and DNS, see *Lifecycle Controller Auto Discovery Network Setup Specification* on the Dell Enterprise Technology Center at www.delltechcenter.com/page/Lifecycle+Controller.

Auto-Discovery Configuration

Before enabling the Auto-Discovery feature, do the following:

- 1 Press <Ctrl><e> when prompted within 5 seconds during system start-up.

The iDRAC6 Configuration Utility page displays.

- 2 Enable NIC (for modular system only)
- 3 Enable DHCP.
- 4 Navigate to LAN Parameters.
- 5 Select Domain Name from DHCP.
- 6 Select On.
- 7 Select DNS Server from DHCP.
- 8 Select On.
- 9 Navigate to LAN user configuration.
- 10 Select Account Access.

- 11 Select **Disabled**. This disables the default administrative account.
- 12 Save and exit iDRAC6 Configuration Utility.
- 13 Restart your system.

Enabling/Disabling Auto-Discovery

- 1 Press <Ctrl><e> when prompted within 5 seconds during system start-up.

The **iDRAC6 Configuration Utility** page displays.

- 2 Navigate to **LAN User Configuration**.
- 3 Select **Auto-Discovery**.
- 4 Select **Enable** to enable the Auto-Discovery feature. Select **Disable** to disable the Auto-Discovery feature



NOTE: Auto-Discovery feature will not run if any administrator accounts are enabled.

Auto-Discovery Workflow

This is the Auto-Discovery workflow once it is configured and enabled:

- 1 Plug in your new Dell system to your network
- 2 Plug-in the power cables to turn on the system.
- 3 iDRAC starts, acquires the Provisioning Server IP addresses/hostnames from DHCP/DNS and announces itself to the Provisioning Server.
- 4 The Provisioning Server validates and accepts the secure handshake session from the iDRAC.
- 5 The Provisioning Server provides custom user credentials with administrator privileges to iDRAC.
- 6 iDRAC receives and completes the secure handshake.

With enhancements to the Auto-Discovery process you can:

- Configure the provisioning server host address through the iDRAC Configuration utility, USC, or using WinRM commands instead of using DHCP or DNS.
- Remotely reinitiate Auto-Discovery in new environments.
- Upload custom client and server certificates using WS-MAN.

Connecting Directly to Provisioning Server for Handshake

This feature allows you to directly connect to a specified Provisioning Server host for handshake and registration of the new server on the network. The provisioning server IP address or host name can be configured through the USC console, iDRAC6 configuration utility or preset at the factory.

Set Provisioning Server IP addresses/resolvable names

There are multiple options for setting the Provisioning Server IP address/hostname used for Auto-Discovery. You can set it through a Web services request using WS-MAN, through the USC console or through the iDRAC6 configuration utility.

Set Provisioning Server Using a WS-MAN Request

The Provisioning Server IP address property string is set by invoking the `SetAttribute()` method on the `DCIM_LCService` class by issuing a Web services request using WS-MAN network management protocol. Command line examples of Microsoft WinRM and WSMANCLI `SetAttribute()` invocations are provided in the *Lifecycle Controller 1.3 Interface Guide* on the Dell TechCenter wiki at www.delltechcenter/page/Lifecycle+Controller.

The following conditions apply to using a command to set the provisioning server IP address/hostname:

- Make sure to enable the **Preserve Configuration** option while resetting the iDRAC6 to defaults, issuing the `racadm racresetcfg` or updating the iDRAC6 firmware. If it is disabled, the provisioning server IP/hostname will be erased.
- The information will be used only during the next handshake process and will not be used for any handshakes in progress.
- The string can contain multiple IP addresses and/or hostnames with the following format:
 - The string is a list of IP addresses and/or hostnames and ports separated by comma.
 - Hostname can be fully qualified.
 - IPv4 address – starts with ‘(‘ and ends with ‘)’ when specified at the same time with a hostname.

- Each IP address or hostname can be optionally followed by a ':' and a port number.
- Examples of valid strings are - hostname, hostname.domain.com

Setting Provisioning Server using the USC Console

- 1** Press <F10> **System Services** when prompted within 5 seconds during system start-up.
The **Unified Server Configurator Lifecycle Controller Enabled** page displays.
- 2** Navigate to **Hardware Configuration -> Configuration Wizard -> iDRAC6 Configuration**.
- 3** Use the **Next** button to navigate to **LAN User Configuration**.
- 4** Navigate to **Provisioning Server Addresses**.
- 5** Enter the IP/hostname string of the Provisioning Server host.
- 6** Click **Next** and then click **Apply**.
- 7** Click **Finish**.
- 8** Click **Exit and Reboot**. Confirm exit.

Set Provisioning Server using iDRAC6 Configuration Utility

- 1** Press <Ctrl+e> when prompted within 5 seconds during system start-up.
- 2** The **iDRAC6 Configuration Utility** page displays.
- 3** Navigate to **LAN User Configuration**.
- 4** Select **Provisioning Server**.
- 5** Enter the IP/hostname string of the Provisioning Server host.
- 6** Click **Enter**.
- 7** Save and Exit the **iDRAC6 Configuration Utility**.

Remotely Reinitiating Auto-Discovery in New Environments

This feature allows you to reinitiate Auto-Discovery through WS-MAN, even though Auto-Discovery has taken place earlier. It can be used when you need to move a server from one data center to another. The Auto-Discovery settings will be persisted using the existing user credentials.

When the server is powered on in the new data center, Auto-Discovery will run according to the settings, and will download the new user credentials for the new data center. This interface is supported using WS-MAN only, and the WS-MAN requests require iDRAC administrator username password credentials or credentials for an iDRAC user with Execute Server Command privilege.

The supported WS-MAN interface to reinitiate Auto-Discovery includes these options:

- Whether the iDRAC will be reset to the factory default configuration equivalent to a server with being ordered with the Auto-Discover option. Only **true** will be accepted as a value. This is a required input.
- Whether Auto-Discovery will run immediately or at the next iDRAC powercycle. This is a required input.
- Provisioning Server IP address/hostname. This is optional.

Regardless of the options you specify, the operations below will be performed by iDRAC as part of the next Auto-Discovery cycle:

- Enable NIC (modular servers)
- Enable IPv4
- DHCP enable
- Disable all administrator accounts
- Disable Active Directory
- Get DNS server address from DHCP
- Get DNS domain name from DHCP

The reinitiate interface and related interfaces are specified in the Dell Lifecycle Controller Management Profile available at www.delltechcenter.com/page/DCIM+Extensions+Library. Managed Object Format (MOF) files for related class and method definitions are also available in the Dell TechCenter DCIM Extensions Library area. The interfaces are:

ReinitiateDHS(ProvisioningServer, ResetToFactoryDefaults, PerformAutoDiscovery)

- **ProvisioningServer**: optional parameter to indicate the Provisioning Server information. This could be an IP address or a hostname.

- **ResetToFactoryDefaults:** required parameter (**TRUE** or **FALSE**) to indicate whether the current configuration data needs to be deleted prior to the next cycle of Auto-Discovery. Only **TRUE** will be accepted; specifying **FALSE** will cause an error message indicating the parameter value is not supported. **TRUE** will reset iDRAC to the default values and then set iDRAC for Auto-Discovery. iDRAC will not be available until the Auto-Discovery provisioning process is complete and the iDRAC receives the new credentials.
- **PerformAutoDiscovery:** required parameter to indicate when the next Auto-Discovery cycle should be performed: immediately or at the next boot. Select **Now** to run the Auto-Discovery cycle immediately; select **Next** to run it the next time you boot your system.

SetAttribute(ProvisioningServer)

- **ProvisioningServer:** parameter to indicate the Provisioning Server IP address/host name.
- **ClearProvisioningServer():** Method to clear the Provisioning Server property. No input parameters are required.

Using Custom Certificates

You can now transfer custom-defined certificates to the iDRAC6, and create a unique certificate based on the service tag of your system to ensure enhanced security. You can also have the factory preset the system with the certificate of your choice using the Custom Factory Install (CFI) process available from Dell.

Creating Custom Client Certificates through WS-MAN

The `DownloadClientCerts()` method on the `DCIM_LCService` class can be called to cause a custom signed Auto-Discovery client encryption certificate to be generated. The method takes as input a Certificate Authority generated key certificate and related hash and password parameters. The key certificate provided is used to sign a certificate containing the system service tag as the Certificate Name(CN). The method returns a job ID that can be used to check the success of the download, generation, and installation of the Auto-Discovery client private certificate. For examples of command line invocations using WinRM and WSMANCLI see the *Lifecycle Controller 1.3 Web Services Interface Guide*.

Providing Custom Server Certificates using WS-MAN

The `DownloadServerPublicKey()` method on the `DCIM_LCService` class can be called to transfer a Provisioning Server public key certificate. The Provisioning Server public key can be used as part of strict mutual authentication between the Auto-Discovery client and the provisioning server. The method takes as input a Provisioning Server public key certificate and related hash and hash type parameters. The method returns a job ID that can be used to check the success of the processing and installation of the Provisioning Server public key. For examples of command line invocations using WinRM and WSMANCLI see the *Lifecycle Controller 1.3 Web Services Interface Guide*. DCIM Profile specification and related MOF files are available at Dell TechCenter wiki in the DCIM Extension Library area (www.DellTechCenter.com).

Remote Firmware Inventory

Remote firmware inventory enables a WS-MAN client to use the Web services interface provided by iDRAC to instantly retrieve the firmware and embedded software inventory of the system. The inventory, however, does not retrieve hardware-related information, such as slot number or hardware settings.

The firmware inventory feature will return an inventory of the installed firmware on devices on the system and the inventory of available BIOS/firmware on the iDRAC6 express card Lifecycle Controller. It also returns the inventory of both the currently installed version of BIOS /Firmware on the iDRAC6 Express card and the versions available for rollback (N and N-1 versions) that can be installed using the remote update Web services interface.

Instant Firmware Inventory

Instant firmware inventory allows you to run an inventory independent of whether the system is turned on or off. Traditionally, the system firmware inventory was performed by downloading an inventory collector onto the operating system, executing it locally, and then gathering the results. Instant firmware inventory allows you to inventory the host platform remotely from a WS-MAN client, even if the host is not running an operating system. iDRAC user credentials used for the WS-MAN request authentication requires Execute Server Command privileges to request firmware and embedded

software inventory; it is not restricted to administrators. You can get a list of firmware for devices that are installed, and also the firmware that is available for rollback and reinstallation.

Supported Devices

Remote instant firmware inventory is supported on these devices:

- iDRAC6
- Storage controllers (RAID Series 6 and 7)
- NICs and LOMs (Broadcom)
- Power supplies
- BIOS
- Driver Pack
- USC
- Diagnostics

The instant firmware inventory class provides firmware inventory information on:

- The firmware installed in the supported devices
- The firmware versions available for installation for each device

Workflow

The `DCIM_SoftwareInventory` profile defines the Dell CIM data model extensions that represent installed and available to be installed versions of firmware and embedded software on the server. The firmware inventory can be accessed using the WS-MAN web services protocol.

This is the typical workflow for a request for firmware inventory using Windows WinRM:

- 1 Request inventory of the system using the WinRM enumeration command for class `DCIM_SoftwareIdentity`.
- 2 Inventory instances are pulled up from the system in both system-off and system-on conditions.
- 3 Users that have administrator or Execute Server Command privileges can retrieve the firmware and embedded software inventory of the system.

- 4 The enumeration request will generate a WinRM error when the UEFI system services are set to **Disabled**.
- 5 Requested inventories are collected as "Installed" and "Available" CIM instances.
- 6 The software currently installed on the component is listed as the "Installed Software Instance". The key property value of this instance, InstanceID represented as DCIM: INSTALLED :< COMPONENTTYPE> :< COMPONENTID> :< Version> and the status value of this instance is represented as "Installed"
- 7 The available software in the persistent storage is listed as the Available Software Instance. The key property value of the instance, InstanceID represented as DCIM: AVAILABLE :< COMPONENTTYPE> :< COMPONENTID> :< Version> and the status value of this instance is represented as "Available". Current installed software instances are also represented as available software instances.
- 8 Inventory instances provide input values for the update and rollback operations. To perform the update operation, pick the InstanceID value from the Installed Instance, DCIM: INSTALLED :< comptype> :< compid> :< version>. For the rollback operation pick the InstanceID Value from the Available instance, DCIM:AVAILABLE:<comptype>:<compid>:<version>. You will not be able to edit InstanceID values.
- 9 If the "version string" property value of "Available Software Instance" is equal to the "Installed Software Instance," then the InstanceID value of that Available Software Instance should not be used for the rollback operation.
- 10 If Unified Server Configurator (USC) is being run on the system during the inventory operation, only "Installed Instances" will be returned.

Important

- There may be DCIM_SoftwareIdentity instances for hardware that was previously installed and then removed still listed in the inventory as "available."
- When you perform an inventory of updates using remote enablement while the system is booted to USC, the inventory may not be complete. Some components could be missing from the list.

Remote Update

Remote update, also known as out-of-band update or operating system-independent platform update, allows you to update the system independent of the state of the operating system or the power on/off state.

Benefits of Remote Update

With Operating System independent platform update, an operating system need not be running on the system. Multiple updates can be scheduled together along with a graceful or power-cycle reboot into USC to perform the updates. Although the updates may involve intermediate BIOS restarts, Lifecycle Controller will automatically handle them until the updates are complete.

This feature supports two methods to perform updates:

- **Install from Uniform Resource Identifier (URI):** This method allows a WS-MAN request to install or update software on a host platform using a URI. The URI consists of a string of characters used to identify or name a resource on the network. The URI is used to specify the location of the Dell Update Package image on the network that can be downloaded to the Lifecycle Controller and then installed.
- **Install from Software Identity:** This method allows update or rollback to a version that is already available on the Lifecycle Controller.

You can use a WS-MAN capable application, script or command line utility to perform a remote update. The application or script performs WS-MAN invoke method request using one of the remote update interface methods. The iDRAC then downloads the firmware from the network share (local network share, CIFS, NFS, FTP, TFTP, http, https) URI and stages the updates to be performed at the specified time and utilizing the specified graceful, power cycle or none system reboot types.

Important

- When you perform a remote update on the Driver Pack for the system it will replace the current driver pack. The replaced driver pack will no longer be available.

- If you have NIC cards of different families on your system, different tasks will be displayed for each NIC card family. For example, if the LOMS and the add-in NIC card are both 5709, you will see two tasks. If you have 5709 LOMS and 5710 add-in NIC card, four tasks will be displayed.

Supported Devices

Remote Update is supported on the following devices:

- iDRAC6
- RAID Series 6 and 7
- NICs and LOMs (Broadcom)
- Power supplies
- BIOS
- Driver Pack
- USC
- Diagnostics

Workflow for Remote Update from URI

- 1 Use the appropriate WS-MAN client to send a method invocation request to the iDRAC IP address. The WS-MAN command includes the **UpdateFromURI()** method on the `DCIM_SoftwareInstallationService`, and the location from where iDRAC should download the Dell Update Package (DUP). The download protocols that are supported are FTP, HTTP, CIFS, NFS and TFTP.
- 2 When the WS-MAN command is invoked successfully, a Job ID will be returned back.
- 3 Additional **UpdateFromURI()** method invocation requests can be sent using WS-MAN to create other update jobs.
- 4 A reboot job can be created by invoking the **CreateRebootJob()** method on the `DCIM_SoftwareInstallationService` and specifying the desired reboot type. The reboot type can be graceful, power cycle or graceful with power cycle after 10 minutes.

- 5 Using the update and reboot Job IDs, you can use the `DCIM_JobService` profile to schedule these jobs to run immediately or at future date and time. You can also use the Job ID to query the status of a job or to cancel a job.
- 6 All jobs will be marked successful or, if an error occurred during downloading or updating, failed. For failed jobs, the error message and error message ID for the failure are available in the job information.

Important

- After successfully downloading the DUP and extracting it, the downloader will update the status of the job as "Downloaded" and the job can then be scheduled. If the signature is invalid or if download/extraction fails then the Job status is set to "Failed" with an appropriate error code.
- Updated firmware can be viewed by requesting firmware inventory after firmware update jobs have completed.

Scheduling Remote Update

The remote update scheduling capability provides the ability to schedule or stage firmware updates now or in the future. Updates for Diagnostics and USC can be performed directly and do not require any staging. These updates will be applied as soon as they are downloaded and do not need the Job Scheduler. All other remote updates are staged updates, and require scheduling, using different scheduling options. The DUPs are downloaded to the Lifecycle Controller and staged, and the actual update is performed by rebooting the system into UEFI System Services.

There are multiple options for scheduling updates:

- Run updates on the desired components at a desired time.
- Run the reboot command to get a reboot job ID.
- Check on the status of any of the jobs by enumerating `DCIM_SoftUpdateConcreteJob` instances and checking the `JobStatus` property value.
- Schedule the job using the `SetupJobQueue()` method on the `DCIM_JobService`.
- Delete existing jobs using the `DeleteJobQueue()` method on the `DCIM_JobService`.

Important

USC, Diagnostics and Driver Pack updates cannot be rolled back.

Rolling Back to Previous Versions

Use the `InstallFromSoftwareIdentity()` method to reinstall from previous versions of firmware for a component that are stored in the Lifecycle Controller. Instead of downloading the DUP, the `InstallFromSoftwareIdentity()` creates a job and returns the job ID.

Remote Scheduling Types

Immediate Update

To immediately update component firmware, schedule the update and reboot jobs with start time as `TIME_NOW`. Scheduling a reboot or update is not required for updates to the Lifecycle controller partitions (USC, Diagnostics). The updates are immediate for these partitions.

Scheduled Update

Specifying a scheduled start time for one or more jobs using the `SetupJobQueue()` method involves specifying a datetime value for the `StartTimeInterval` parameter. Optionally, a datetime value can be also be specified for the `UntilTime` parameter.

Specifying an `UntilTime` defines a maintenance window to run the updates within a time-bound slot. If the time window expires and the updates have not completed, any update jobs that are currently running will complete, but any unprocessed jobs whose scheduled start time has begun will be failed.

Setting the Scheduling Reboot Behavior

The `DCIM_SoftwareInstallationService.CreateRebootJob()` method takes one of the following reboot types as an input parameter and a reboot job ID is returned as an output parameter. The reboot Job ID is used as the first Job ID in the `JobArray` parameter of the `DCIM_JobService.SetupJobQueue()` method along with other update Job IDs.

- **Reboot 1 - Power cycle** - Performs the iDRAC PowerCycle that will power down the system and power it back up. This is not a graceful reboot. The system will power off the system without sending a shutdown request to an operating system running on the system. Only reboot type 1 will power on the system if the system is in an **Off** state, but A/C power is still applied.
- **Reboot 2 - Graceful reboot without forced shutdown** - Performs the iDRAC Graceful Shutdown command and if the system is powered off within the PowerCycle Wait Time, it powers the system back up and marks the reboot job as **Reboot Completed**. If the system is not powered off within the PowerCycle WaitTime, the reboot job is marked as failed.
- **Reboot 3 - Graceful reboot with forced shutdown** - Performs the iDRAC Graceful Shutdown command and if the system is powered off within the PowerCycle Wait Time, it powers the system back up and marks the reboot job as **Reboot Completed**. If the system is not powered off within the PowerCycle WaitTime, the system is Power Cycled.

Remote Operating System Deployment

The remote operating system deployment capabilities enable deployment of an operating system remotely using WS-MAN web services protocols and CIFS and NFS network file sharing protocols.

Remote Operating System Deployment Main Features

These are the main capabilities of remote operating system deployment:

- Remote activation of local exposure of embedded drivers as a USB device
- Remote acquisition of embedded drivers per selected operating system.
- Boot to an ISO image located on a network share.
- Download an boot to ISO image to vFlash.

Remote Operating System Deployment Interface

Dell Operating System Deployment web services interface provides the capability to support operating system deployment activities by manipulating operating system deployment features provided by the iDRAC service processor. Detailed interface specifications and class definition (.mof) files can be found at the Lifecycle Controller area on the Dell Enterprise Technology Center at

www.delltechcenter.com. Using CIM and Dell extension classes using the web services protocols WS-MAN, Dell Operating System Deployment feature provides the following capabilities:

- Get the embedded driver pack (a package of all supported operating system drivers for all supported operating systems for the platform) version:

Remote management consoles, applications, and scripts request driver pack version and list of supported operating systems from iDRAC through WS-MAN.

The `GetDriverPackInfo()` method on the `DCIM_OSDeploymentService` class returns the embedded driver pack version and the list of operating systems supported by the driver pack.

- After determining which operating system the drivers are needed for, one of the following methods can be invoked through WS-MAN to unpack the appropriate drivers and expose them locally or acquire them remotely.
 - a The `UnpackAndAttach()` method on the `DCIM_OSDeploymentService` class extracts the drivers for the requested operating system and places them on an internal USB device labeled `OEMDRV`. The `OEMDRV` appears as a locally attached USB device to the system. The method takes the operating system name and an expose duration time as input parameters and returns a job identification that can be subsequently checked for the status of the unpack and attach activity.
 - b The `UnpackAndShare()` method on the `DCIM_OSDeploymentService` class extracts the drivers for the requested operating system and copies them to a network share. The method takes the operating system name and network share information as input parameters and returns a job identification that can be subsequently checked for the status of the unpack and share activity. Network share information includes the IP address of the share, the share name, share type, and username, password and workgroup data for secure shares.

Important

- The drivers unpacked and attached are removed after the time specified in **ExposeDuration** parameter or if no time is specified in the method invocation then by default the OEMDRV USB device will be removed after 18 hours.
- Ensure that ISO images attached during the process are detached before you use system services.
- When installing Red Hat Linux 5.3 using remote enablement commands, the installation will fail whenever there is an OEM drive (for driver source) attached. To avoid failure, do not attach the OEM drive when using remote enablement commands to install Red Hat Enterprise Linux 5.3.
- The following methods can be used to boot the system from an ISO image on a network share or to initiate PXE boot mechanisms:
 - a The **BootToNetworkISO()** method on the **DCIM_OSDeploymentService** class will boot the system using an ISO image that has been made available on a CIFS or NFS network share. The method takes the ISO image name, network share information, and exposure duration as input parameters and returns a job identification that can be subsequently checked for the status of the unpack and share activity. Network share information includes the IP address of the share, the share name, share type, and username, password and workgroup data for secure shares. For additional security a hash value can be calculated using well known hash algorithms and this value along with the type of the hash used can be provided as input parameters.
 - b The **BootToPXE()** method on the **DCIM_OSDeploymentService** class initiates a Pre-Boot Execution Environment (PXE) boot of the system. The method requires no input parameters.

Important

- The drivers unpacked and attached are removed after the time specified in **ExposeDuration** parameter. If no time is specified in the method invocation, then by default the OEMDRV USB device will be removed after 18 hours.
- Ensure that ISO images attached during the process are detached before you use system services.

- The following methods are used to directly detach the local OEMDRV device or the network ISO image. These can be used before the previously set exposure durations time out:
 - a** The **DetachDrivers()** method on the **DCIM_OSDeploymentService** class detaches and removes the **OEMDRV** device that had been previously attached by an invocation of the **UnpackAndAttach()** method.
 - b** The **DetachISOImage()** method on the **DCIM_OSDeploymentService** class detaches and removes the network share based ISO image that had been previously attached by an invocation of the **BootToNetworkISO()** method.
- Several methods described in this document return job identifiers as output parameters. The jobs provide a means of keeping track of a requested action that cannot be performed immediately and, because of underlying technology constraints, will take longer than standard web service request response timeouts. The returned job identifier can subsequently be used in WS-MAN Enumerate or Get requests to retrieve job object instances. Job object instances contain a job status property that can be checked to see what state the job is in and whether it completed successfully or encountered a problem and failed. If a job failure occurs, the job instance also contains an error message property that provides detailed information on the nature of the failure. Other properties contain other error identification information that can be used to localize the error message to the supported languages and get more detailed error descriptions and recommended response action descriptions.
- The **GetHostMACInfo()** method on the **DCIM_OSDeploymentService** class returns an array of physical network port MAC addresses representing all the LAN on Motherboard (LOM) ports in the system. The method requires no input parameters.
- All the **DCIM_OSDeploymentService** methods described in this document return error codes indicating whether the method successfully executed, an error occurred, or a job was created. Job creation occurs if the action being performed in the method cannot be completed immediately. Additionally, if an error occurs, the methods will also return output parameters that include an error message (in English) and other error identifiers that can be used to localize the error to languages supported by the USC. The other error identifiers can be used to index into and process

Dell Message Registry XML files. The Dell Message Registry files are available in the six supported languages, one file per language. In addition to translated error messages, the Message Registry files contain additional detailed error descriptions and recommended response actions for each error returned by the Lifecycle Controller Remote Services web service interface.

Operating System Deployment Typical Use Case Scenario

This section contains a typical scenario for deploying an operating system remotely.

Prerequisites and Dependencies

The following are the prerequisites and dependencies for deploying the operating system remotely:

- Boot disk is available to install operating system, or the operating system ISO image on the network share.
- It is recommended that the latest driver pack is installed and available in USC-LCE.
- Provisioning console, application or appropriate scripts that are capable of sending WS-MAN Web services requests and method invocations.

Workflow

The following is a typical workflow for remote operating system deployment:

- Create the custom pre-operating system/operating system image and share it on the network, or create the required operating system media ISO image.
- Get the list of supported operating system and driver pack version information.
- Stage the operating system drivers by unpacking and attaching drivers for operating system deployment. These drivers will be installed during the operating system deployment process.
- Remotely boot to the custom pre-operating system/operating system image to initiate the operating system deployment process.
- Run detach commands to detach the ISO media and driver device.

For more information on the Lifecycle Controller Remote Operating Systems Deployment feature including the Lifecycle Controller 1.3 Web Services Interface Guideline, white papers, the Dell OS Deployment Profile data model specification, class definition (.mof) files, sample code and scripts, see the Lifecycle Controller area on the Dell Enterprise Technology Center at www.delltechcenter.com.

Staging and Booting to Operating System Image on vFlash

This feature allows you to download an ISO image to the vFlash SD Card on the target system and booting the system to this ISO image.

Prerequisite

This feature is available only if you have Dell-licensed vFlash present on your system.

WS-MAN Methods

Important

- If the supported SD card is installed and not formatted, executing the download ISO command will first format the SD card and then download to ISO image.
- If you try to download an ISO image larger than the available space on the vFlash of your system using the TFTP protocol, the task will fail, but will not be reported through an error message. Subsequent commands that try to access this ISO will fail.

The new WS-MAN methods added to the operating system deployment profile for vFlash are:

- **DownloadISOToVFlash** - Downloads the image to the vFlash. Support is available for CIFS, TFTP and NFS.
- **BootToISOFromVFlash** - Boots to the ISO image that has been staged on the vFlash. You cannot perform this action if you are using the iDRAC GUI or RACADM commands to communicate with the vFlash. This command will also reboot or power on your system if it is in an **Off** state once executed.
- **DetachISOFromVFlash** - Detaches the partition so that the console cannot access it anymore.

- **DeleteISOFromVFlash** - Deletes the ISO image from the vFlash partition. It provides the capability to download an ISO image to the vFlash and then boot from it, allowing you to download custom install images to run from. This command will execute only if the ISO is detached.

You will need to perform the following steps to complete the process:

- 1 Download the ISO image to the vFlash.
- 2 Get the concrete job ID and poll for the completion of this job.
- 3 Run the `BootToISOFromVFlash` command. This will attach the image as a CD ROM, boot to the attached image and then continue with the operating system installation.
- 4 Detach the partition on the vFlash.
- 5 Delete the ISO image from the partition.

Part Replacement

Part Replacement provides the automated change of firmware of a newly replaced component, such as a PowerEdge™ RAID controller, NIC or power supply, to match that of the original part. This feature is disabled by default and may be enabled if required. It is a licensed feature and requires the Dell vFlash SD card. When a component is replaced and the Part Replacement feature is enabled, the actions taken by the Lifecycle Controller are displayed locally on the system monitor.

The presence of the vFlash SD Card and configuration of Part Replacement related properties can be accomplished remotely through the Web services interface using the WS-MAN protocol. For examples of command line invocations using WinRM and WSMANCLI see the *Lifecycle Controller 1.3 Web Services Interface Guide*. DCIM Profile specification and related MOF files are available at Dell TechCenter wiki in the DCIM Extension Library area (www.DellTechCenter.com).

Important

Part replacement is supported on modular systems with the following Broadcom devices:

- Broadcom NetXExtreme II 5709 Quad Port Ethernet Mezzanine Card for M-Series

- Broadcom NetXtreme II 57711 Dual Port 10 Gb Ethernet Mezzanine Card with TOE and iSCSI Offload for M-Series
- Broadcom 57710 10 Gb Ethernet card

Validating vFlash presence Using WS-MAN

To ensure that the system is equipped with a Dell-licensed vFlash card follow these steps:

- 1 Using an application, script or command line shell that can process WS-MAN based web services requests, send a get instance request for the DCIM_LCEnumeration class instance with the InstanceID of "DCIM_LCEnumeration:CCR1".
- 2 If the vFlash is present, the output will have the following attribute values:
 - `AttributeName = Licensed`
 - `CurrentValue = Yes`
- 3 If the vFlash is not present on the system, or if it is not Dell-licensed, the output will have the following attribute values:
 - `AttributeName = Licensed`
 - `CurrentValue = No`

Using WS-MAN to get/set Part Firmware Update Attributes

To get the current **Part Firmware Update** and **Collect System Inventory On Restart** property values using WS-MAN, an enumerate command request may be sent to get instances of the class DCIM_LCEnumeration. An instance object representing each attribute is returned per attribute where the `AttributeName` string property on the object will contain the name of the Part Replacement related property, such as **Part Firmware Update**. The `CurrentValue` property will contain the current setting of the property. See the Dell Lifecycle Controller Management Profile specification for specific attribute names and values.

To configure a Part Replacement related property value, set and apply actions are requested using the WS-MAN Web services protocol.

The set action is performed by invoking the `SetAttribute()` method on the DCIM_LCService class. The `SetAttribute()` method takes as input parameters the property names and values. The possible values of the Part Firmware Update are:

- **Allow version upgrade only** - If the input for the CurrentValue is **Allow version upgrade only**, firmware update on replaced parts will be performed if the firmware version of the new part is lower than the original part.
- **Match firmware of replaced part** - If the input for the CurrentValue is **Match firmware of replaced part**, firmware on the new part will be updated to the version of the original part.
- **Disable** - If the input is **Disable**, the firmware upgrade actions will not occur.

The apply action is performed by invoking the **CreateConfigJob()** method on the `DCIM_LCService` class. The **CreateConfigJob()** method takes as parameters the scheduled start time (which can be `TIME_NOW`) and a reboot if required flag. A job ID is returned as a parameter and can be used to check on the job completion status.

To check job completion status, enumerate instances of the `DCIM_LifecycleJob` class and check for the instance where the `InstanceID` = job ID returned by the **CreateConfigJob()** method. The `JobStatus` property on the job instance will indicate the job is completed when the part replacement properties have been set.

Troubleshooting and Frequently Asked Questions

This section describes the error messages commonly generated by USC and USC - LCE, and provides suggestions for resolving the errors. It also answers questions that are frequently asked by USC and USC - LCE users.

Also see <ftp://ftp.dell.com/LifecycleController/> to locate the file matching LC_*1.3.0*_MSG_REG.zip for the 1.3 Message Registry XML files for Remote Enablement web services.

Error Messages

"Table A-1" describes the error messages commonly generated by USC and USC - LCE, and provides suggestions for resolving the errors. "Table A-2" describes the error messages commonly generated by USC, and provides suggestions for resolving the errors. "Table A-3" describes the error messages commonly generated by USC - LCE, and provides suggestions for resolving the errors. "Table A-4" describes the error messages commonly generated by Lifecycle Controller, and provides suggestions for resolving the errors

Table A-1. USC and USC - LCE Error Messages and Resolutions

Error Message	Resolution
Unable to find a boot device on which to install the operating system	<p>USC or USC - LCE does not detect a device on which an operating system can be installed. One of the following situations is probably causing the error:</p> <ul style="list-style-type: none"> • The drives are not properly connected. • There are no recognized storage controllers on the system. • The on-board SATA controller is disabled in the BIOS. <p>To resolve this issue, click Exit and Reboot and shut down the system. Then, make sure you have at least one device on which to install an operating system before launching USC or USC - LCE again.</p>

Table A-1. USC and USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
Unable to copy driver files	The drivers required to install the operating system are corrupted. To resolve this issue, perform a platform update (see "Updating the Platform using the Platform Update Wizard.")

Table A-1. USC and USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
The inserted OS media is invalid	The operating system media is damaged or corrupted, or the optical device used to read the media is not functioning correctly.
The updates you are trying to apply are not Dell-authorized updates	USC or USC - LCE has detected that one or more of the DUPs used to update your system are not Dell authorized. If you are using a local USB device for your update repository and this problem persists, create it again using DUPs from the <i>Server Update Utility</i> DVD (see "Configuring a Local USB Device") or provide an alternate repository.
Fatal error launching USC has occurred. The system will reboot.	A fatal error occurred when launching USC or USC - LCE. The system will automatically reboot and attempt to enter USC or USC - LCE again. If the problem persists after rebooting, see "Repairing USC" or "Repairing USC - LCE."
Network is not configured	Network settings must be configured for USC or USC - LCE to work correctly. See "Using USC Settings Wizard" for information on configuring USC or USC - LCE network settings from the Network Settings page.
Unable to set new date and time	USC or USC - LCE was unable to change the system date and time. To resolve this issue: 1 Reboot the system. 2 Re-enter USC or USC - LCE by pressing the <F10> key. 3 Change the date and time settings again.
Invalid Proxy Server	The proxy server specified to access the FTP server is invalid. See "Select Download Method" for more information.
Please enter a valid Encryption Key of up to 40 Hex digits	Enter a valid encryption key that contains not more than 40 hex digits. Valid characters are within the ranges of 0–9, a–f, and A–F.
Please enter a valid IPv4 Address for this iDRAC	Enter a valid IPv4 protocol address for iDRAC that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid Subnet Mask	Enter a valid Subnet Mask that is between 0.0.0.0 and 255.255.255.255.

Table A-1. USC and USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
Please enter a valid Default Gateway Address	Enter a valid default gateway address that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid IPv4 DNS Server 1 Address	Enter a valid IPv4 DNS Server1 address that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid IPv4 DNS Server 2 Address	Enter a valid IPv4 DNS Server2 address that is between 0.0.0.0 and 255.255.255.255.
Account access change failed. Multiple user accounts required. See help for details.	You must create another user account. Click the Help button in the upper-right corner of the screen for more information.
Please enter a valid Username	You must enter a valid user name. To maintain compatibility with other iDRAC configuration tools, Dell recommends using only digits (0–9), alphanumeric characters (a–z, A–Z), and hyphens (–) in the user name string.
Please enter a valid Password	You must enter a valid password. To maintain compatibility with other iDRAC configuration tools, Dell recommends using only digits (0–9), alphanumeric characters (a–z, A–Z), and hyphens (–) in the password string.
Please enter a valid Confirmation password	You must re-enter the new password and the confirmation password. Be certain that both passwords are exactly the same.

Table A-2. USC Error Messages and Resolutions

Error Message	Resolution
Unable to find a device capable of reading the OS install media	<p>USC cannot detect a device to read the operating system media. One of the following situations is probably causing the error:</p> <ul style="list-style-type: none">• No optical device is available on the system. Shut down the system and add a SATA optical device or USB optical device.• If an optical device is present, it may not be properly connected. Check to ensure the device cables are adequately seated.• If an optical device is present, it is disabled in the BIOS. Reboot the system, enter the BIOS setup utility, and enable the SATA ports for the optical device.
The repository you selected as a source for the updates has failed an integrity check	<p>This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local FTP server for your update repository and this problem persists, create the repository again (see "Configuring a Local FTP Server") or provide an alternate repository.</p>

Table A-3. USC - LCE Error Messages and Resolutions

Error Message	Resolution
Drivers pack not found OR Error populating OS list	USC - LCE cannot find the drivers required to install the operating system. To resolve this issue, perform a platform update (see "Updating the Platform using the Platform Update Wizard.")
Unable to find a device capable of reading the OS install media	USC - LCE cannot detect a device to read the operating system media. One of the following situations is probably causing the error: <ul style="list-style-type: none">• No optical device is available on the system. Shut down the system and add a SATA optical device or USB optical device.• If an optical device is present, it may not be properly connected. Check to ensure the device cables are adequately seated.• If an optical device is present, it is disabled in the BIOS. Reboot the system, enter the BIOS setup utility, and enable the SATA ports for the optical device.• iDRAC virtual media is disabled. See the <i>Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide</i> for your system available at support.dell.com/manuals.
The repository you selected as a source for the updates has failed an integrity check	This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device") or provide an alternate repository.
Decompression of the catalog file failed	The catalog downloaded to compare currently installed versions with the latest available versions cannot be decompressed. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device") or provide an alternate repository.

Table A-3. USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
File seek of catalog archive failed	The catalog downloaded to compare currently installed versions with the latest available versions is corrupt. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device") or provide an alternate repository.
FTP download of catalog sign file failed	The catalog downloaded to compare currently installed versions with the latest available versions has failed the digital signature verification check. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device") or provide an alternate repository.
Unable to resolve host name	This error is probably caused by one of the following: <ul style="list-style-type: none">• You have specified an invalid name for the platform update FTP server. See "Select Download Method."• The Domain Name Server (DNS) specified in the Network Settings page is invalid. See "Using USC Settings Wizard."
DUP corrupted	USC - LCE has detected that one or more of the DUPs used to update your system is corrupted. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device") or provide an alternate repository.
Please enter a valid IPv6 Address for this iDRAC	Enter a valid IPv6 network address for iDRAC. See "IPv6 Configuration."
Please specify the IPv6 network address prefix length in the range of 1 to 128	Enter the number of significant bits in the IPv6 address prefix for your network. The prefix length should be between 1 and 128. See "IPv6 Configuration."

Table A-3. USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
Please enter the IPv6 Default Gateway address	Enter the IPv6 default gateway address. See "IPv6 Configuration."
Please enter a valid IPv6 DNS Server 1 Address	Enter a valid IPv6 DNS Server1 address. See "IPv6 Configuration."
Please enter a valid IPv6 DNS Server 2 Address	Enter a valid IPv6 DNS Server2 address. See "IPv6 Configuration."
Please enter a valid iDRAC Name of up to 63 characters	Enter a valid iDRAC name that is less than or equal to 63 characters.
Please enter a valid Domain Name of up to 64 characters	Enter a valid domain name that is less than or equal to 64 characters.
Please enter a valid Host Name of up to 62 characters	Enter a valid host name that is less than or equal to 62 characters.
Please enter a value in the range of 1 to 4094	Enter a VLAN ID between 1 and 4094. See "Advanced LAN Configuration."
Please enter a value in the range of 0 to 7	Enter a VLAN ID priority value between 0 and 7. See "Advanced LAN Configuration."
iDRAC communication failure. Please power down, unplug the system, wait 5 seconds, apply power and power on	Communication with iDRAC has failed. To resolve this issue: 1 Turn off the system, and then unplug it. 2 Wait 5 seconds. 3 Plug the system back in, and then turn it on.
iDRAC hard failure. Please power down, unplug the system, wait 5 seconds, apply power and power on	Connection with iDRAC has failed. To resolve this issue: 1 Turn off the system, and then unplug it. 2 Wait 5 seconds. 3 Plug the system back in, and then turn it on.

Table A-3. USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
RAID configuration failed	USC - LCE failed when creating the RAID configuration. To resolve this issue: <ol style="list-style-type: none">1 Reboot the system.2 Re-enter USC - LCE by pressing the <F10> key.3 Try again to create the RAID configuration.
Generic Failure	USC - LCE experienced an unidentified error when creating the RAID configuration. To resolve this issue: <ol style="list-style-type: none">1 Reboot the system.2 Re-enter USC - LCE by pressing the <F10> key.3 Try again to create the RAID configuration.
Sufficient physical disks not available on any supported RAID controller. The wizard will exit.	You do not have a sufficient number of disks to support RAID configuration—you must attach more physical disks and start the RAID Configuration wizard again.
Please select required number of physical disk(s) for current span	The number of physical disks you selected for the current RAID span is incorrect. Review your span selections, and enter the correct number.
No physical disk has been selected for this virtual disk	The number of physical disks you selected for the virtual disk is insufficient. Review the minimum number of physical disks required for the current RAID level, and select at least that number of physical disks.
No controller is present in the system	No RAID controller is present in your system. To resolve this issue: <ol style="list-style-type: none">1 Add a supported RAID controller that includes two or more physical disks.2 Re-enter USC - LCE by pressing the <F10> key.3 Restart the RAID Configuration wizard.
No valid RAID level found	The number of physical disks attached to your system is insufficient for the RAID level you selected. Attach more physical disks and try again.

Table A-3. USC - LCE Error Messages and Resolutions (continued)

Error Message	Resolution
An error occurred. One or more settings may not be saved.	An error occurred when changing Hardware Advanced Configuration settings. To resolve this issue: 1 Reboot the system. 2 Re-enter USC - LCE by pressing the <F10> key. 3 Change the settings again.
An error occurred. One or more settings may not be restored.	An error occurred when restoring Hardware Advanced Configuration settings. To resolve this issue: 1 Reboot the system. 2 Re-enter USC - LCE by pressing the <F10> key. 3 Re-open the Advanced Configuration screen.
This feature is not supported in this configuration	Your modular system does not support the feature you selected.

Table A-4. Lifecycle Controller Error Messages and Resolutions

Error Message	Resolution
General failure	An error has occurred. No other details are available at this time. 1 Run the command again. 2 Reset iDRAC and run the command.
Lifecycle Controller is being used by another process	Lifecycle Controller is currently locked by another process. Ensure that the process is completed before attempting to run another command. 1 Run the command again after sometime. 2 Ensure that USC or DUP is not running. 3 Reset iDRAC and run the command

Table A-4. Lifecycle Controller Error Messages and Resolutions (continued)

Error Message	Resolution
Cannot access Driver Pack partition in Lifecycle Controller.	Driver Pack partition in Lifecycle Controller is not accessible. The Lifecycle Controller might be corrupted. 1 Reset iDRAC and run the command.
Driver Pack not found in Lifecycle Controller	No Driver Pack in Lifecycle Controller. 1 Update the Driver Pack using USC or DUP and then run the command again.
Cannot allocate memory	Unable to dynamically allocate memory to perform the task. 1 Reset iDRAC and run the command.
Driver Pack does not have drivers for the selected operating system.	Lifecycle Controller does not have any drivers for the selected operating system. The installation will have to use the native drivers present on the operating system media.
Cannot create USB device to copy drivers for the selected operating system.	Unable to create USB device to copy drivers for selected operating system. iDRAC may not be operating normally 1 Reset iDRAC and run the command again.
Cannot mount USB device to copy drivers for the selected operating system.	Unable to access the newly created USB device to copy drivers for selected operating system. iDRAC may not be operating normally 1 Reset iDRAC and run the command again
Unable to expose USB device containing operating system drivers to host system.	Unable to expose the newly created USB device (with drivers for selected operating system) to the host server. iDRAC may not be operating normally. 1 Reset iDRAC and run the command again.
Mount network share failed - incorrect username or password.	Unable to mount the network share using the credentials specified in the command. Either username or password is incorrect. 1 Run the command again with correct username and password.

Table A-4. Lifecycle Controller Error Messages and Resolutions (continued)

Error Message	Resolution
Mount network share failed - incorrect IP address or share name.	Unable to mount the network share using the credentials specified in the command. Either IP address or share name is incorrect. 1 Run the command again with correct IP address and share name.
Exposing ISO image as internal device to the host system failed.	Unable to expose the ISO image as internal CD device to the host system. The ISO file is no longer present, network errors are preventing access to the ISO file, or iDRAC may not be operating normally. 1 Reset iDRAC and run the command again.
Unable to locate the ISO image on the network share point.	Unable to find the ISO file specified in the network share. Ensure that you have specified the correct path to the ISO file in the command and all other user credentials are correct. 1 Run the command again with correct path to ISO file.
The fork() command for a child process to do the task failed	Failed to execute fork() system call to perform the task in a child process. iDRAC may not be operating normally. 1 Reset iDRAC and run the command
Unable to get size or label from Driver Pack for selected operating system.	Unable to get the size or label for selected operating system from the Driver Pack present in Lifecycle Controller. The driver pack may be corrupt. 1 Update the driver pack using USC or DUP and run the command again
Unable to boot to ISO image	Bootting to ISO has failed. Either BIOS was unable to boot to the ISO image or provider did not get a response in 5 minutes from BIOS on successful boot to ISO image. 1 Ensure there is no POST error that resulted in user interaction (Press F1 to continue or F2 to run setup). 2 Reset iDRAC and run the command
Unable to detach ISO image from the host	Unable to detach ISO image from the host. Either the image may have already detached or iDRAC may not be operating normally. 1 Reset iDRAC to automatically detach the ISO image.

Table A-4. Lifecycle Controller Error Messages and Resolutions (continued)

Error Message	Resolution
Unable to continue with DetachISOImage - another command is in the process of exposing ISO Image and booting to it.	Cannot continue with DetachISOImage because another command is in the process of exposing ISO image and booting to it. 1 See ConcreteJob status to ensure that the current running process is complete and then run DetachISOImage.
Unable to continue with DetachDrivers - UnPackAndAttach is in progress	1 Wait until UnpackAndAttach finishes and then run DetachDrivers.
Unable to detach USB device containing operating system drivers.	Detaching the USB device (that contains drivers for the operating system installation) from the host has failed. The device may have been detached already or iDRAC may not be operating normally. 1 Reset iDRAC to detach this device automatically.
Unable to continue with BootToPXE - another command is running.	Unable to continue with BootToPXE command because another process is using Lifecycle Controller. 1 See ConcreteJob status to ensure that the current running process is complete and then run BootToPXE.
Copying drivers for selected operating system failed.	Copying drivers for selected operating system failed. The Driver Pack may be corrupt. 1 Update the Driver Pack using USC or DUP and then run the command again.
Hash verification on the ISO image failed.	Hash verification on the ISO image has failed. The hash value specified in the command is either not correct or the ISO image has been changed. 1 Verify that the hash value specified in the command is correct. 2 Ensure that the ISO has not been changed - replace the ISO image on the share and run the command again.
Driver Pack config file not found in Lifecycle Controller. Driver Pack might be corrupt.	Driver Pack config file not found in Lifecycle Controller. Driver Pack may be corrupt. 1 Update the Driver Pack using USC or DUP and then run the command again.

Table A-4. Lifecycle Controller Error Messages and Resolutions (continued)

Error Message	Resolution
Invalid value for ExposeDuration - must be 60-65535 seconds	The value specified for ExposeDuration is out of range. It must be 60-65535 seconds 1 Run the command again with ExposeDuration value 60 to 65535 seconds.
Copying operating system drivers to network share failed	Copying drivers for selected operating system to network share failed. The share may be read-only or the driver pack present in Lifecycle Controller may be corrupt. 1 Ensure that the network share has write permission. 2 Update the Driver Pack using USC or DUP and then run the command again.
Unable to detach ISO image from the system	Cannot continue with DetachISOImage because system does not have attached ISO image. 1 Do not run DetachISOImage command.
Installed BIOS version does not support this method.	The system has an older version of BIOS that does not support this method. Install the latest version of BIOS to use this method. 1 Update the BIOS to version 1.2 or later and then run the command again.
Unable to continue with BootToPXE - ISO image is attached to the system.	Unable to continue with BootToPXE command because system has an ISO image attached. Detach the ISO image before continuing with BootToPXE. 1 Run DetachISOImage command and then run BootToPXE.
Lifecycle Controller is disabled	Lifecycle Controller is disabled on the system, so none of the remote enablement OSD commands will work. Ensure Lifecycle Controller is enabled before running any command 1 Reboot the system and enable System Services using CTRL+E option in the POST
Boot to ISO Image has been cancelled by user using CTRL+E option on the server	User has cancelled system services by using CTRL+E option during POST. This has effectively cancelled the WSMAN request to boot to ISO 1 Do not cancel system services using CTRL+E during POST when system is rebooting to the ISO

Frequently Asked Questions

When USC - LCE downloads updates, where are the files stored?

The files are stored in non-volatile memory, located on the main system board. This memory is not removable and is not accessible through the operating system.

Is a virtual media device or vFlash card required to store data for updates?

No. The files are stored in memory on the main system board.

What is virtual media?

Virtual media is remote media—like CDs, DVDs, and USB keys—that a server identifies as local media.

What should I do if an update fails?

If an update fails, USC-LCE will reboot and then attempt all the remaining pending updates selected. After the final reboot, the system returns to the USC-LCE Home page. Launch **Platform Updates** again and then re-select the update that had failed and click **Apply**.

What is vFlash or virtual flash?

vFlash is a formatted SD (Secure Digital) card that plugs into iDRAC6 Enterprise. vFlash can be formatted and enabled via iDRAC to make it accessible as a USB key for data storage. Virtual flash is a partition on vFlash to which you can remotely write an ISO. See the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* available at support.dell.com/manuals for more information.

Can I add my own drivers to use for operating system installation?

No. You cannot add your own drivers for operating system installation. See "Updating the Platform using the Platform Update Wizard" for more information on updating the drivers that are used for operating system installation.

Can I update the drivers used by an installed operating system through USC or USC - LCE?

No. USC or USC - LCE only provides drivers that are required for operating system installation. To update the drivers used by an installed operating system, see your operating system's help documentation.

Can I add my own drivers and firmware for updating USC or USC - LCE to a local USB device?

No. Only drivers and firmware downloaded from the *Server Update Utility* DVD's are supported. See "Configuring a Local USB Device" for more information.

Can I delete USC or USC - LCE?

No.

Can I use virtual media for the operating system media source during installation?

Yes. See the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* for your system's iDRAC device for more information (available at support.dell.com/manuals).

Can I use a virtual USB for my update repository?

Yes. See the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* for your system's iDRAC device for more information (available at support.dell.com/manuals).

What is UEFI? With which version does USC or USC - LCE comply?

UEFI (Unified Extensible Firmware Interface) is a specification that details an interface for transitioning control from the pre-boot environment to the operating system. USC or USC - LCE complies with UEFI version 2.1. See www.uefi.org for more information.

Within Hardware Configuration, what is the difference between the Configuration Wizards and Advanced Configuration?

USC - LCE offers two ways to configure hardware: *Configuration Wizards* and *Advanced Configuration*.

Configuration Wizards guide you through a sequence of steps to configure your system devices. The Configuration Wizards include iDRAC, RAID, System Date/Time, and Physical Security. See "Hardware Configuration" for more information.

Advanced Configuration allows you to configure Human Interface Infrastructure (HII) enabled devices (for example, NICs and BIOS). See "Advanced Configuration" for more information.

Does USC or USC - LCE support configuration of all RAID levels and all RAID cards for *xx1.x* systems?

USC or USC - LCE supports RAID levels 0, 1, 5, 6, 10, 50, and 60 on PERC 6 cards running PERC 6.1 firmware. RAID 0 and 1 are supported on the SAS 6/iR.

These are the latest generation of series 7 RAID controllers:

PERC - H700 (Internal) and H800 (External)

SAS - H200 (Internal) and SAS 6 GBPS (External)

Does USC - LCE support rollback of BIOS and firmware?

Yes. See "Rolling Back to Previous BIOS and Firmware Versions" for more information.

Which devices support system updates?

USC - LCE currently supports updates to the BIOS, iDRAC firmware, power supply firmware, and certain RAID and NIC controller firmware. See "Updating the Platform using the Platform Update Wizard" for more information.

Which devices are supported in Advanced Configuration within Hardware Configuration?

Advanced Configuration is available for the BIOS and NIC. Depending on your system configuration, other devices may also appear in Advanced Configuration if they support the HII configuration standard. See "Hardware Configuration" for more information.

What should I do if my system crashes while using USC or USC - LCE?

If your system crashes while using USC or USC - LCE, a black screen with red text will appear. To resolve this problem, first try rebooting your system and re-entering USC or USC - LCE. If that does not resolve the problem, perform the steps in "Repairing USC" of "Repairing USC - LCE." If that does not resolve the problem, contact Dell for technical assistance.

How do I find out the current installed version details of the USC-LCE product?

Click **About** on the left navigation pane.

What should I do if I have an issue with mouse synchronization when I access USC LCE over the iDRAC KVM?

Ensure that the **Single Cursor** option under **Tools** in the iDRAC KVM menu is selected on the iDRAC KVM client. See the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* available on the Dell Support site at support.dell.com/manuals for more information.

Index

A

auto-discovery, 67
 enable, 68

B

BIOS
 configuring with HII, 57
 rolling back, 34

BitLocker, 35

C

CLI, 9

D

deployment interfaces, 66

DHCP/DNS
 configure, 67

DUP, 15, 28

E

error messages, 91

F

FAQs, 105

firmware
 adding custom, 106
 interrupting install, 33
 rolling back, 34

FTP

 configuring a local server for
 updates, 59-60

H

hardware
 advanced configuration, 56
 configuration wizards, 36
 configuring, 36

hardware diagnostics
 updating the utility, 27

HII, 56

I

iDRAC

 configuring, 40
 Enterprise, 41, 46, 105

L

LAN

- advanced configuration, 42

Linux

- driver location, 23, 25
- updating drivers, 25

O

operating system

- adding custom drivers, 105
- deploying, 19-20
- launching the wizard, 20
- using virtual media for installation, 106

P

Part Replacement, 58, 87

physical security
configuring, 39

platform

- updating from local FTP server, 59-60

R

RAID

- configuration wizard, 22
- configuring, 49

Remote Firmware Inventory, 74

Remote Operating System
Deployment, 81

remote operating system
deployment, 81
deployment interface, 81
main features, 81
prerequisites and
dependencies, 85
use case, 85
workflow, 85

remote services, 9, 63

Remote Update, 77

Remotely reinitiating discovery
and handshake, 71

S

Scheduling Remote Update, 79

Staging and Booting to OS image
on vFlash, 86

SUSE

- driver location, 23

system crashes, 108

system date/time, 39

system services

- canceling request to enter, 17
- disabled, 14
- not available, 15

systems services

- update required, 15

T

TPM, 35

troubleshooting, 91

Types of remote scheduling, 80

U

UEFI, 56, 106

Uploading Custom
Certificates, 73

USC

deleting, 106

disabling, 17

repair package, 28

storing update files, 105

updating, 17

wizards, 15

installing to C drive, 26

wizards

Diagnostics, 15

Hardware Configuration, 16

OS Deployment, 15

Platform Update, 16

Settings, 16

WS-MAN, 63

V

vFlash, 105

virtual disk

configuring as a boot device, 22

virtual media

using for operating system

installation, 106

W

web services for management, 63

Windows

drivers, 23

