Dell Lifecycle Controller
USC/USC-LCE
Version 1.4

User's Guide

Notes and Cautions

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

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

Contents

1

Overview

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 with the UEFI firmware to access and manage every aspect of the hardware, including component and subsystem management that is beyond the traditional Baseboard Management Controller (BMC) capabilities.

The UEFI environment provides the local console interface and the infrastructure for locally managed system components.

Unified Server Configurator (USC) or Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE) provides an embedded solution on the local server to assist with provisioning in a pre-operating system environment. It simplifies the end-to-end server lifecycle management as described below:

- Provisioning — Entire pre-operating system configuration from a unified interface.

- Deployment — Simplifies operating system installation with drivers resident on the Lifecycle Controller.

- Patching/Updates (USC-LCE only) — Operating system agnostic and minimizes the maintenance downtime with direct access to updates on the Dell support site. It simplifies BIOS and firmware updates by maintaining a working version for rollback purpose.

- Servicing (USC-LCE only) — Continuous availability of diagnostics without hard drive dependency. Provides capability to flash firmware automatically when replacing field replaceable components such as a Dell PowerEdge RAID controller, NIC or power supply.

Why Use USC/USC-LCE?

Systems management is typically a key part of an administrator's role. Being able to install an operating system, updating firmware for function and policies requirements, configuring devices and getting the most out of an IT network are integral aspects of this role. In the past, many tools have been used to help the administrator, starting with tools such as DSA, Systems Build

and Update Utility, and DTK that shipped on multiple CDs, Dell then developed a single software tool DVD, Systems Build and Update Utility. Storing, retrieving, and using these multiple disks in their many versions is a time consuming experience for the administrator.

As a clear response to these problems, Dell now provides the Lifecycle Controller, a flash chip embedded on the system itself with the Dell Unified Server Configurator application (USC). The Lifecycle Controller allows the IT administrator to do away with media altogether, allowing operating system deployment with locally embedded driver repositories, firmware updates, hardware configuration, and platform specific diagnostic routines. Since the USC is available even when the operating system is not functional or even installed, it allows added flexibility in provisioning the system and customizing to suit the customer's requirements. As the tool is integrated and embedded, formatting or reinstalling the operating system does not remove the tool, thus saving significant time and money.

USC and USC-LCE Features and Support Information

Table 1-1. USC and USC-LCE Features

Product Name	Features
USC	Base-level product that uses BMC and provides the following capabilities: • Operating System Deployment • Hardware Diagnostics • USC Settings

Table 1-1.   USC and USC-LCE Features

Product Name	Features
USC-LCE	Fully-featured product that uses iDRAC6 Express and Enterprise cards, and provides the following capabilities: • Operating System Deployment • Hardware Diagnostics • USC Settings • Platform Update • Hardware Configuration • View and Export Hardware Inventory • View and Export Lifecycle Log

NOTE: You can upgrade Dell systems series *y21x-y51x* to USC-LCE. See the *Hardware Owner's Manual* for more information.

USC or USC-LCE displays features that are supported by the system, depending on the system configuration. Table 1-2 shows the product classifications for Remote Services. For example, for a Dell system *y11x* series, y denotes alphabets like M, R, or T; and x denotes numbers.

Table 1-2.   Product Classification

Dell System Series	Options	Available System Management Device	USC or USC-LCE	Available Features
y11x	No Options	Embedded BMC	USC	**BMC** - Operating System Deployment, Hardware Diagnostics, USC Settings

Table 1-2. Product Classification *(continued)*

Dell System Series	Options	Available System Management Device	USC or USC-LCE	Available Features
y21x to *y51x*	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, Lifecycle Log, Hardware Inventory
		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, Lifecycle Log, Hardware Inventory **iDRAC6 Enterprise** - adds Full Remote Management, Dedicated NIC port, Virtual Console, Virtual Media, part replacement, vFlash SD card management

Table 1-2. Product Classification *(continued)*

Dell System Series	Options	Available System Management Device	USC or USC-LCE	Available Features
y61x to y91x	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, Lifecycle Log, Hardware Inventory
	Optional[1]	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, Lifecycle Log, Hardware Inventory
				iDRAC6 Enterprise - adds Full Remote Management, Dedicated NIC port, Virtual Console, Virtual Media, part replacement, vFlash SD card management

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

For information on the supported systems and operating systems, see the *Dell Systems Software Support Matrix* at **support.dell.com/manuals**.

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

What's new in USC/USC-LCE 1.4

The new features introduced in USC/USC-LCE 1.4:

- vFlash SD Card
  - Configuration Wizard
  - Determine different vFlash SD card properties:
    - vFlash present or absent
    - Health status
    - vFlash size
  - Enable and disable vFlash SD card
  - Initialize vFlash SD card
- Operating System
  - Install custom operating systems[1]
  - Install the following UEFI capable operating systems:

    ![NOTE icon] **NOTE:** The Unified Extensible Firmware Interface (UEFI) is an industry standard interface between an operating system and the platform firmware. Some benefits of using an UEFI capable operating system: boot from storage devices of capacity 2.2 TB and above, operating system boots faster, supports IPv6 network protocol and enhanced network security.

    - Microsoft Windows Server 2008 (64-bit)
    - Microsoft Windows Server 2008 R2 (64-bit)
    - Microsoft Windows Server 2008 SP2 (64-bit)
    - SUSE Linux Enterprise Server (SLES) version 11 SP1 (64-bit)
- Dell Update Packages (DUPs) — Single component updates using only Windows based DUPs for USC-LCE version 1.4 and above.
- Network
  - Test network connectivity[1]
  - Support network share for platform update, hardware inventory export, and lifecycle log.
- View and export Hardware Inventory
- View and export Lifecycle log

- Apply configuration for the replaced part
- Delete configuration details on the Lifecycle Controller.

1. Indicates the newly introduced feature for USC.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **support.dell.com/manuals**. On the **Manuals** page, click **Software → Systems Management**. Click on the appropriate product link on the right-side to access the documents.

- The *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* provides information about configuring and using an iDRAC6 for blade servers to remotely manage and monitor your system and its shared resources through a network.

- The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides complete information about configuring and using an iDRAC6 for rack and tower servers to remotely manage and monitor your system and its shared resources through a network.

- The *Dell Repository Manager Version User Guide* provides information about creating customized bundles and repositories comprised of Dell Update Packages (DUPs), for systems running supported Microsoft Windows operating systems.

- The *Glossary* provides information about the terms used in this document.

2

Getting Started With USC or USC-LCE

Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE) reside on an embedded flash memory card. It is an embedded configuration utility that enables 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 and can be started during the boot sequence, and can function in a pre-operating system environment. "Table 1-2" details the Dell system series, system management device options, USC or USC-LCE, and available features.

Using USC, you can:

- Download drivers for operating system installation from one of the following sources:
  - Dell FTP website at **ftp.dell.com**
  - USB mass storage device, or the *Dell Server Updates* DVD, or the *Dell Systems Build and Update Utility* DVD
  - Network share
- 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 Integrated Dell Remote Access Controller 6 (iDRAC6) Express or an iDRAC6 Enterprise card; this hardware upgrade will upgrade USC to USC-LCE.
- Quickly identify, download, and apply system updates without searching **support.dell.com**. You can 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.

Pre-requisites for Using USC or USC-LCE

Before using USC/USC-LCE you should ensure that the following pre-requisites are met:

- Ensure that your network is configured.
- Ensure that your system has the latest versions of iDRAC and BIOS installed.

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>** does not allow you to enter **System Services**:

- **System Services disabled** — If you turn on or restart your system while iDRAC is initializing, the message System Services disabled is displayed during the system boot process. This occurs if you turn 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" on page 19 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 the USC or USC-LCE repair package. See "Repairing USC" on page 91 or "Repairing USC-LCE" on page 91 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 Request to Enter System Services" on page 19. 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" on page 19 for more information.

Using the Wizards

Wizard Description

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

- **OS Deployment** — Enables you to install an operating system. See "Operating System Deployment" on page 21 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" on page 23 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" on page 19 for more information.

Along with the above mentioned wizards, USC and USC-LCE provides 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 apply updates for your system. You can download the updates from **ftp.dell.com**, access from an USB device attached to your system, or from a network share. See "Updating the

Platform using the Platform Update Wizard" on page 37, "Configuring a Local USB Device" on page 79, and "Network Share" on page 39 for more information.

- **Hardware Configuration** — Enables you to configure system devices. See "Hardware Configuration" on page 25 for more information.

- **Lifecycle Log** — Enables you to view and export lifecycle log and add comments to lifecycle log. See to "Viewing Lifecycle Log History" on page 72, "Exporting Lifecycle Log" on page 73, and "Adding a Comment to Lifecycle Log" on page 75 for more information.

Launching a Wizard

USC and USC-LCE display the wizards in the left pane. Click the wizard that you want to launch and 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:

1 **USC Settings** — You do not need to run this wizard again unless you want to change the language, keyboard, or network settings.

2 **OS Deployment** — Run this wizard to install operating system.

3 **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:

1 **USC Settings** — You do not need to run this wizard again unless you want to change the language, keyboard, or network settings.

2 **Platform Update** — Apply any updates. Ensure that you run the **Platform Update** wizard regularly so that your system is up to date.

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 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. It is strongly recommended 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**.

4 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.

3

USC and USC-LCE Features

This section gives a brief description of the Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE) features.

USC and USC-LCE Enabled Common Features

Operating System Deployment

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 is required for operating system installation. Since USC does not support single Dell Update Package (DUP) update, use one the following methods to access the driver packages:

- Provide the path to the catalog file that is located at **ftp.dell.com**, or the local FTP with all the DUPs.
- Provide the path to the catalog file that is located on the USB mass storage device or the *Dell Server Updates DVD* with all the DUPs.

USC-LCE provides a local repository for drivers that is required for operating system installation, depending on the 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 Red Hat Linux Enterprise Linux version 4.8, manually install the extracted drivers after the operating system installation is complete. However, for Red Hat Enterprise Linux version 5.5, SUSE Linux Enterprise Server version 10 SP3, SUSE Linux Enterprise Server version 11 SP1 and later installs, the extracted drivers are installed during the operating system installation.

Although, USC-LCE comes with embedded drivers that are factory installed, there may be more current drivers available. You must 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.

See the following sections for more information:

1 "Launching the Operating System Deployment Wizard" on page 29.

2 "Selecting the Operating System Driver Source Location (for USC only)" on page 29.

3 "Deploying the Operating System" on page 31.

4 "Selecting an Operating System" on page 31.

5 "Inserting the Operating System Media" on page 33.

6 "Rebooting the System" on page 34.

See the following sections for more information on installation of specific operating systems:

• "Installing the Drivers for RHEL 4.8 Operating System" on page 32

• "Assigning a Windows-Bootable System Partition to Drive C" on page 35

• "Red Hat Enterprise Linux 4.8 on a System with SAS7 (H200) Controller" on page 35

Hardware Diagnostics

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 using the **Hardware Diagnostics** utility. Since the diagnostics utility has a physical (as opposed to logical) view of attached hardware, this utility is 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.

See the following sections, for more information:

- "Performing Hardware Diagnostics" on page 36
- "Updating the Hardware Diagnostics Utility" on page 36

USC or USC-LCE Repair

When you boot the managed node, and if you see the message `System Services update required` during the power on self test (POST) sequence, the embedded device that stores USC might contain corrupted data. To resolve this issue, see the following sections:

- "Repairing USC" on page 91
- "Repairing USC-LCE" on page 91

USC-LCE Unique Features

USC-LCE Platform Update

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, It is recommended that you download and apply updates on a regular basis.

The system administrator provides the updates on any of the following locations or media:

- FTP Server
- Local USB Device
- *Dell Server Updates* DVD
- Network Share

Contact your system administrator to find out the preferred method for accessing updates in your organization.

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 "Configuring a Local FTP Server" on page 77 for more information.

See "Updating the Platform using the Platform Update Wizard" on page 37 for more information.

Platform Rollback

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 current 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 operating system driver pack 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.

See "Rolling Back to Previous BIOS and Firmware Versions" on page 42 for more information.

Hardware Configuration

USC-LCE provides different wizards for configuring the hardware.

- **Configuration Wizards** guide you through setting up system devices. The Configuration Wizards include: Physical Security Configuration, System Date/Time Configuration, iDRAC Configuration, RAID Configuration, RAID Security Key Configuration, and vFlash Media Configuration.

  See the following sections for more information:

  – "Physical Security Configuration" on page 43
  – "System Date/Time Configuration" on page 44
  – "iDRAC Configuration" on page 45
  – "RAID Configuration" on page 54 - You can configure RAID through the **OS Deployment** wizard. See "Configuring RAID Through the Operating System Deployment Wizard" on page 61 for more information.
  – "Viewing Secure Capability Status and Virtual Disks of the Series 7 Controller" on page 62 and "Creating a Secure Virtual Disk on Series 7 Controller" on page 62 - To view and create secure virtual disks.
  – "vFlash SD Card Configuration" on page 64.

- **HII Advanced Configuration** allows you to configure certain devices, such as Network Interface Controllers (NICs) and the BIOS, using Human Interface Infrastructure (HII).

  See "HII Advanced Configuration" on page 65 for more information.

- **Part Replacement Configuration** allows you to automatically update a new part to either the firmware version or the configuration of the replaced part or both.

  See "Part Replacement Configuration" on page 67 for more information.

- **Export Hardware Inventory** allows you to export information about the hardware installed in the managed node.

  See "Exporting Hardware Inventory" on page 69 for more information.

- **View Hardware Inventory** allows you to see information related to the hardware installed in the managed node.

  See "Deleting Configuration and Resetting Defaults" on page 72 for more information.

- **Delete Configuration and Reset Defaults** allows you to delete the current iDRAC settings and reset the iDRAC to factory defaults. It also deletes lifecycle logs on the managed node.

  See "Deleting Configuration and Resetting Defaults" on page 72 for more information.

Lifecycle Log

Lifecycle Controller provides the history of firmware changes of the related components installed on a managed node. The log shows the following:

- Firmware update history based on device, version and date
- Events based on severity, category, and date
- Customer comments based on date

NOTE: Lifecycle log is available even if the operating system is not installed on the system and is independent of the power state of the system.

Use this feature to:

- View Lifecycle Log history. See "Viewing Lifecycle Log History" on page 72 for more information.
- Export Lifecycle Log. See "Exporting Lifecycle Log" on page 73 for more information.
- Add a comment to Lifecycle Log. See "Adding a Comment to Lifecycle Log" on page 75 for more information.

4

USC and USC-LCE Operations

This section provides the tasks required to perform different operations on the Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE).

USC and USC - LCE Common Features

Launching 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 "Selecting the Operating System Driver Source Location (for USC only)" on page 29 procedure that follows.

5 For **USC-LCE**, if your system has a RAID controller, continue with "Optional RAID Configuration" on page 31. If your system does not have a RAID controller, continue with "Selecting an Operating System" on page 31.

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

Use this screen to select the driver required for operating system installation. Download operating system drivers from an online repository or from a local device (USB, network share, or DVD).

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" on page 77.

- 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 Server Updates* DVD. For information on setting up a USB device for updates see "Configuring a Local USB Device" on page 79.

3 Click **Next**.

If your system has a RAID controller, continue with "Optional RAID Configuration" on page 31. If your system does not have a RAID controller, continue with "Selecting an Operating System" on page 31.

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 Through the Operating System Deployment Wizard" on page 61 for more information.

  NOTE: For USC, the **Raid Configuration** wizard is available only through the **OS Deployment** wizard.

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 is installed on the default boot device identified in the BIOS utility. Continue with "Selecting an Operating System" on page 31.

Deploying 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.

Selecting an Operating System

To select the operating system, do any of the following:

- For installing an operating system that is available in the list, select one of them and click **Next**. If a UEFI capable operating system is selected, USC-LCE displays two installation modes — **UEFI** or **BIOS**. Select one of options and click **Next**.

- For installing a custom operating system, select the required operating system from the list and click **Next**.

  The drivers are extracted and USC or USC-LCE prompts you to insert the operating system installation media.

- For installing an operating system that is not available in the list, select the option **Any Other Operating System** and click **Next**.

  The drivers are not extracted, so prepare the drivers for the required operating system.

Driver Extraction

- For Microsoft Windows operating system, the drivers are extracted to an internal USB drive named OEMDRV.
- For Red Hat Enterprise Linux 4.8 operating system, the drivers are extracted to OEMDRV under /oemdrv/*.rpm. Manually install the extracted drivers after the installation is complete. See "Installing the Drivers for RHEL 4.8 Operating System" on page 32 for more information on driver installation.

Installing the Drivers for RHEL 4.8 Operating System

To install the drivers after the RHEL 4.8 operating system installation:

1 Use the following command to mount the USB device containing the operating system drivers labeled OEMDRV.

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

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

   /oemdrv/*.rpm

2 Use the command rpm -Uvh *.rpm to install the drivers.

Inserting the Operating System Media

1 Depending on the operating system or option selected, do one of the following:

- If the operating system from the list is selected, insert the standard operating system installation media when prompted and click **Next**. USC or USC-LCE validates the media.

    NOTE: USC or USC-LCE renders the drivers through the `OEMDRV` directory to the operating system.

- If the operating system from the list is selected and you want to install a custom operating system, insert the custom operating system media with all the operating system components that are specific to your requirements and click **Next**.

    NOTE: USC or USC-LCE renders the drivers through the `OEMDRV` directory to the custom operating system.

- If **Any other Operating System** option is selected, insert the operating system installation media with all the operating system components that are specific to your requirements and click **Next.**

    NOTE: USC or USC-LCE does not render the extracted drivers in the `OEMDRV` directory to the operating system.

2 Based on the media inserted, do one of the following:

- If the standard operating system installation media is validated, continue the installation. Else, insert the correct media and click **Next**.

- If the custom operating system installation media is inserted and if the validation check fails, the message — `The selected media doesn't match the standard media certification of the OS <name of the selected operating system>` appears. Click **Yes** to continue, else **No** to insert a different media and retry.

- If **Any other Operating System** option is selected and the custom media is inserted. Click **Next** to continue as the USC or USC-LCE does not validate the media.

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 media. In this case, an error message is displayed stating that no media is available.

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.

Rebooting the System

Prerequisite

Use the following step to reboot the system:

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 Microsoft 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 "Assigning a Windows-Bootable System Partition to Drive C" on page 35 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.

- 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.

Assigning a Windows-Bootable System Partition to Drive C

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

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

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 icon] **NOTE:** The partition may not be enumerated as drive **C**.

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 drive **C**.

4 Follow the on-screen instructions to create a partition. Windows now installs on drive **C**.

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

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:

1 Copy the driver image file(*.**img** or *.**dd**) into a USB drive. Specify the driver image file location when prompted for a driver diskette.

2 Select Red Hat Enterprise Linux 4.8 on the **OS Deployment** screen of USC.

3 After USC reboots to the operating system 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

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. Use this information to search from **support.dell.com** for details on resolving the problem.

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

Updating the Hardware Diagnostics Utility

For Systems Supporting USC

Download the required Dell Update Package (DUP) from **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" on page 37 for more information. Alternatively, you can also download the required DUP from **support.dell.com** and run the DUP as an executable in the installed operating system.

USC and USC-LCE Unique Features

Updating the Platform using the Platform Update Wizard

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.

NOTE: When using a local repository to upgrade from USC-LCE version 1.3 to version 1.4, ensure to create a catalog with Linux-based DUPs. For USC-LCE 1.4 feature enhancements, only Windows-based DUPs are available. See the *Dell Repository Manager User's Guide* at **support.dell.com/manuals** for information on creating a local repository using Dell Repository Update Manager.

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.

Single Component DUP Update

For USC-LCE, you can update the firmware, BIOS using individual DUPs.

Viewing 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.

Launching 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.

Selecting the Download Method

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.

📝 **NOTE:** Make sure that the catalog file and DUPs that are downloaded from ftp.dell.com, are copied into the root folder of the source.

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

1 Select either of the following:

- **FTP Server**
- **Local Drive**
- **Network Share**

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 or Update package path** — The specific location/sub-directory where the catalog resides.

  📝 **NOTE:** If the catalog file and DUP are downloaded from ftp.dell.com, do not copy them into a sub-directory.

- **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.
- **Test Network Connection** — To verify if USC-LCE is able to connect to the IP address that you provided. By default, it pings the Gateway and DNS server IP, and also pings any host and proxy IP.

Local Drive (CD/DVD/USB)

Select **Local Drive** if you are accessing the updates from a local USB mass storage device or the *Dell Server Updates* DVD. To provide the path to the updates:

a Select the volume label from the drop-down menu.

b In the **Catalog Location or Update package path** field, type the name of the DUP (for example, **APP_WIN_RYYYZZZ.EXE**) along with the sub-directory if required. Or, if you have the **catalog.gz** file, you need not enter the file name, instead type the sub-directory if any.

> **NOTE:** If the catalog file and DUP are downloaded from **ftp.dell.com**, do not copy them into a sub-directory.

See "Configuring a Local USB Device" on page 79 for more information.

Network Share

Select **Network Share** if you are accessing the updates from a shared folder on a network.

To update using Network Share, select either **CIFS** or **NFS** and type the following details:

For CIFS

- **Share Name** — Type the path to the shared folder where the respository is located. For example, for a catalog file, type **xxx.xxx.xx.xx****Catalog**, and for a share folder, type **xxx.xxx.xx.xx****Share**.

- **Domain and User Name** — Type the correct domain and user name required to log on to the network share. For example, **myDomain\\login-name**, and if there is no domain, type the login-name.

- **Password** — Type the correct password.

- **Catalog Location or Update Package Path** — If you have the DUP, type **firmware\\APP_WIN_RYYYZZZ.EXE**, or if you have the **catalog.gz** file, you need not enter the file name, instead type the sub-directory if any.

  NOTE: If the catalog file and DUP are downloaded from **ftp.dell.com**, do not copy them into a sub-directory.

For NFS

- **Share Name** — Type the path to the shared folder where the respository is located. For example, for a catalog file, type **xxx.xxx.xx.xx****Catalog**, and for a shared folder, type **xxx.xxx.xx.xx****Share**.

- **Catalog Location or Update Package Path —** If you have the DUP, type **firmware\\APP_WIN_RYYYZZZ.EXE**, or if you have the **catalog.gz** file, you need not enter the file name, instead type the sub-directory if any.

  NOTE: If the catalog file and DUP are downloaded from **ftp.dell.com**, do not copy them into a sub-directory.

2 Click **Test Network Connection** to verify if USC-LCE is able to connect to the IP address that you provided. By default, it pings the Gateway and DNS server IP.

3 Click **Next**.

Selecting and Applying the 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 turn on.**

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.

Rolling Back to Previous BIOS and Firmware Versions

You can roll back to previous BIOS and Firmware versions using the **Rollback** wizard.

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.

Launching 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.

Selecting and Applying 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.

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 walks you through the **iDRAC Configuration** Wizard:

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 transmits data on NIC 2. If NIC 2 fails, the remote access device transmits data on NIC 3. If NIC 3 fails, the remote access device transmits 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 801.11g 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 the following section.

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 the following section.

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 the following section.

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: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: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 the following section.

Virtual Media Configuration

Use this feature to set control modes for the available Virtual Media devices. The Virtual Media is available only if the system includes iDRAC 6 Enterprise.

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

Set the following control modes using the Virtual Media configuration:

- **Attached** - 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 system's console, as if the floppy image or drive were present (attached or connected) on the local system.

- **Detached** - The virtual media devices are not accessible.

- **Auto-attached** - The virtual media devices are automatically mapped to the server every time the user physically connects a media.

Click **Next** to proceed to the following section.

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 the following section.

Summary

Displays the summary of the iDRAC configuration changes.

Click **Apply** to proceed to the following section.

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.

Important

- 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.
- USC can 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.

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" on page 55

b "Select RAID Controller" on page 55

c "Foreign Configuration Found" on page 55

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.

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" on page 58.

If you are using the **Advanced Wizard**, click **Next** and proceed to "Advanced Wizard Only - Select Physical Disks" on page 59.

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 the following section.

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.c

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**.

Configuring RAID Through the Operating System Deployment Wizard

Important

- If your system does not have a RAID controller, the **OS Deployment** wizard bypasses the RAID configuration option and goes directly to "Selecting an Operating System" on page 31.

- ESX 3.5 and Citrix operating systems do not support series 7 controllers.

- Using USC-LCE, you must navigate to the RAID configuration page from the **Hardware Configuration** Tab→ **Configuration Wizards**→ **RAID Configuration**.

To configure RAID:

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

NOTE: To create secure virtual disks using USC-LCE, navigate to **Hardware Configuration** Tab→ **Configuration Wizards**→ **RAID Security Key Configuration**.

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 is 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 drop-down. 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**.

vFlash SD Card Configuration

Use this feature to enable or disable the vFlash SD card, check the health and properties, and initialize the vFlash SD card. The Dell vFlash SD card enables the part replacement feature. USC-LCE support vFlash SD cards of sizes 1 GB, 2 GB, or 8 GB.

NOTE: The options under vFlash SD card are grayed-out if there is no SD card inserted in the slot.

See the *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* available at **support.dell.com/manuals** for more information on vFlash SD card and the installation procedure.

Use the **vFlash SD Card Configuration** to:

- Enable/disable vFlash SD card.
- Determine the vFlash SD card properties:
    - Name
    - Health

Table 4-1.   Health Status and Response Action

Health State	Response Action
OK	None
Warning	Initialize and try again
Critical	Remove, reset, and try again
	Initialize and try again

- Size - Indicates the total size of the vFlash SD card.
- Available Space - Indicates the available size on the vFlash SD card to create a new partition.
- Type - Indicates the type of card, SD (Secure Digital) or MMC (MultiMediaCard).
- Write Protected - Indicates if the write-protect latch on the vFlash SD card is set to on or off position.

- Initialize vFlash - This deletes all the existing partitions on vFlash SD card.

NOTE: You can only use 256 MB of memory space in non-Dell SD cards.

Enable or Disable vFlash

If set to **Enabled**, the vFlash SD card is configured as a virtual drive; it appears in the BIOS boot order, allowing you to boot from the vFlash SD card. If set to **Disabled**, virtual flash is not accessible.

To enable or disable vFlash SD card:

⊘ **NOTE:** Ensure to set the write-protect latch on the vFlash SD card to **Off** position.

1 From the **vFlash Media** drop-down menu, select **Enable** or **Disable**.

2 Click **Finish** to apply the changes.

Initialize vFlash

⊘ The **Initialize vFlash** option is not available after you disable the vFlash SD card.

Click **Initialize vFlash** to erase all the data present on the vFlash SD card.

HII Advanced Configuration

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

1 Select **Hardware Configuration** from the left menu

2 Click **HII 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 are 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. **HII 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
- Intel Ethernet X520 10 GBE Dual Port KX4-KR Mezz

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 Configuration

Part replacement configuration is an automatic update of the firmware, or configuration, or both 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

- The part replacement configuration functionality is available only if the system has a Dell vFlash SD card.

- Enable the **Collect System Inventory On Restart** so that USC-LCE invokes **Part Firmware Update** and **Part Configuration Update** automatically on system startup.

  📝 **NOTE:** Ensure that **Part Firmware Update** and **Part Configuration Update** are not disabled.

- 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 turning the system on. In the manual mode, you must press <F10> after part replacement during reboot.

- The replaced card/part should belong to the same family as the previous component.

Supported Devices

You can update the part firmware and configuration for the following devices:

📝 **NOTE:** Only part firmware updates are supported on SAS cards and power supply units.

- NICs (Broadcom and Intel)
- 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** drop-down.

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 is not performed.
- **Allow version upgrade only** — Firmware update on replaced parts is only 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 is updated to the version of the original part.

Part Configuration Update

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

- **Disabled** — The feature is disabled and the current configuration is not applied if a part is replaced.

- **Apply always** — The feature is enabled and the current configuration is applied if a part is replaced.

- **Apply only if firmware match** — The feature is enabled and the current configuration is applied only if the current firmware matches with the firmware of a replaced part.

Viewing Hardware Inventory

Use this feature to view the hardware-related information for hardware components that are internal to the system chassis and the configuration for each component. This feature is independent of the operating system that may or may not be installed on the managed node. See Table C-1 for more information on the easy-to-use names of the hardware components listed on the **View Hardware Inventory** page.

> **NOTE:** Incorrect inventory data is displayed after performing **Delete Configuration and Reset Defaults**. See "Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller" on page 71 for displaying correct inventory data.

1 Click **Hardware Configuration** on the left pane.

2 Click on **View Hardware Inventory** on the right pane.

Exporting Hardware Inventory

Use this feature to export the hardware related information to an XML file. Store the XML file on an **USB Device,** or **Network Share,** or both the locations. See Table C-1 for more information on the easy-to-use names of the hardware components that are exported into the XML file.

> **NOTE:** Incorrect inventory data is exported into the XML file after performing **Delete Configuration and Reset Defaults**. See "Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller" on page 71 for exporting correct inventory data into the XML file.

> **NOTE:** The XML file is saved in this format - *HardwareInventory_<servicetag>_<timestamp>.xml*

Prerequisites

- If you use the network share, set the correct **Network Settings**. See "Using USC Settings Wizard" on page 19 for more information.
- If you are storing the exported file in an USB device, ensure that an USB device is connected to the managed node.
- If you are storing the exported file in network share, ensure that you have shared folder with the correct login credentials.

To export the hardware inventory:

1. Click **Hardware Configuration** on the left pane.
2. Click **Export Hardware Inventory** on the right pane**.**
3. Select **USB Device,** or **Network Share**, or both.

   USB Device

   Select **USB Device** if you are exporting the inventory log to a local USB device.

   a. Select the correct device from the **Choose Device** drop-down menu and enter the path to the folder.

      If the path is not provided, the file is stored in the root location of the device.

   b. Click **Finish**.

   Network Share

   Select **Network Share** if you want to store the file in a shared folder on a network.

   To update using Network Share, select either **CIFS** or **NFS** and type the following details:

   For CIFS

   - **Share Name** — Type the path to the shared folder where you must store the file. For example, type **xxx.xxx.xx.xx\HrdInvLog**.
   - **Domain and User Name** — Type the correct domain and user name required to log on to the network share. For example, **myDomain\login-name**, and if there is no domain, type the login-name.

- **Password** — Type the correct password.
- **File Location — Type the sub-directories if any. For example, 2010\Apr.**

For NFS

- **Share Name —** Type the path to the shared folder where you must store the file. For example, type \\xxx.xxx.xx.xx\HrdInvLog.
- **File Location —** Type the sub-directories if any. For example, 2010\Apr.

4   Click **Test Network Connection** to verify if USC-LCE is able to connect to the IP address that you provided. By default, it pings the Gateway and DNS server IP.

5   Click **Next**.

Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller

To view or export the correct hardware inventory data after resetting the Lifecycle Controller:

NOTE: After performing **Delete Configuration and Reset Defaults**, the system shuts down.

1   Power on the system and wait for a couple of minutes for iDRAC to start functioning.

2   Since Collect System Inventory on Restart (CSIOR) is not enabled upon reset, press <F10> to launch USC so that the system inventory is collected. After USC launches, exit the wizard and wait for the system to reboot.

3   Disconnect the power cord and wait for 30 seconds. Reconnect the power cord and boot the system to USC.

Deleting Configuration and Resetting Defaults

Use this feature to delete any sensitive data and configuration related information when you need to retire a managed node, reuse a managed node for a different application, or move a managed node to a non-secure location.

⚠ **CAUTION: This feature resets the iDRAC to factory defaults, and deletes all iDRAC user credentials and IP address configuration settings. It also deletes lifecycle logs that contain the history of all the change events, firmware upgrades, and user comments. It is recommended that you export the Lifecycle Log in a safe location before using this feature. After the operation, the system shuts down and you must manually turn on the system.**

To delete configuration and reset to factory defaults:

1 Click **Delete Configuration and Reset Defaults**.

2 Select **Reset Lifecycle Controller**.

3 Click **Finish**.

4 An error message is displayed, click **Yes** to continue or **No** to cancel the operation.

Viewing Lifecycle Log History

Use this feature to view:

- Firmware inventory

- History of firmware updates

- Update and configuration events only

  📝 **NOTE:** The details of the configuration changes are not shown.

- User comments

While viewing the lifecycle log, use different filtering and sorting options.

To view the Lifecycle Log History and to use the filtering options:

1 Click **Lifecycle Log** on the left pane.

2 Click **View Lifecycle Log History** on the right pane.

   The page displays a table with the following event information:

   - No — The serial number of the event.

   - Category — The category under which the events belong.

- Description — A brief description of the event. For example, Dell OS Drivers Pack, v.6.4.0.14, X14 was detected.
- TimeStamp — When the event occurred.

3 Use the following options in **Filter by Category** to see the required information:

- **All** — Displays all the data in the Lifecycle Log
- **Any Other Event** — Displays the data based on the event selected. For example, iDRAC, Inventory, Configuration Service, Job Control, Remote Update, OS Deployment, USC, and Others.

Use up/down arrows in the table to sort the data.

Exporting Lifecycle Log

Use this feature to export the Lifecycle Log information to an XML file. Store the XML file on an **USB Device,** or **Network Share,** or both the locations. See "Schema" on page 97 for more information on the schema.

Prerequisites

- If you use a network share, set the correct Network Settings. See "Using USC Settings Wizard" on page 19 for more information.
- If you need to store the exported file in an USB device, ensure that an USB device is connected to the managed node.
- If you need to store the exported file in network share, ensure that you have shared folder with the correct login credentials.

To export the Lifecycle Log:

1 Click **Lifecycle Log** on the left pane.

2 Click on **Export Lifecycle Log** on the right pane.

3 Select either **USB Device**, or **Network Share, or both**.

USB Device

Select **USB Device** if you are exporting the inventory log to a local USB device.

a Select the correct device from the **Choose Device** drop-down menu and type the path to the folder.

If the path is not provided, the file is stored in the root location of the device.

b   Click **Finish**.

Network Share

Select **Network Share** if you want to store the file in a shared folder on a network.

To update using Network Share, select either **CIFS** or **NFS** and type the following details:

For CIFS

- **Share Name** — Type the path to the shared folder where you must store the file. For example, type **xxx.xxx.xx.xx\LifCyLog**.

- **Domain and User Name** — Type the correct domain and user name required to log on to the network share. For example, **myDomain\login-name**, and if there is no domain, type the login-name.

- **Password** — Type the correct password.

- **File Location** — Type the sub-directories if any. For example, **2010\Apr**.

For NFS

- **Share Name** — Type the path to the shared folder where you must store the file. For example, type **xxx.xxx.xx.xx\LifCyLog**.

- **File Location** — Type the sub-directories if any. For example, **2010\Apr**.

4   Click **Test Network Connection** to verify if USC-LCE is able to connect to the IP address that you provided. By default, it pings the Gateway and DNS server IP.

5   Click **Next**.

Adding a Comment to Lifecycle Log

Use to this feature to record comments that is usable at a later date. For example, scheduled downtime information.

NOTE: You can type a maximum of 100 characters in the **Lifecycle Log** field.

To add comments:

1 Click **Lifecycle Log** on the left pane.

2 Click on **Add a comment to Lifecycle Log** on the right pane.

3 In the **Add a comment to Lifecycle Log** field, enter your comments and click **OK**.

Upgrading 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 also upgrades USC to USC-LCE.

NOTE: This is applicable only to Dell System Series *y21x-y51x*.

NOTE: Some links and features are not accessible if an older version of iDRAC firmware is used. Ensure that the latest iDRAC firmware is installed.

Installing the iDRAC6 Express Card

1 Power 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 Turn 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 upgrade the 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" on page 42 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 packs, lifecycle log, and the rollback related files are deleted if the iDRAC6 Express card is transferred to a different Dell system. For example, if moving the iDRAC6 Express card from Dell PowerEdge R410 system to Dell PowerEdge T410 system.

    NOTE: Ensure that you export the lifecycle log to a different location before you transfer the iDRAC6 Express card.

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   Turn on the system, and then press **<F10>** to enter USC.

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 ensure 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 "Deploying the Operating System" on page 31 for more information.

Copying the Repository to a Local FTP Server from the Dell Server Updates DVD

1   Download the *Dell Server Updates* ISO to your system from **support.dell.com**, and burn it to a DVD.

2   Copy the repository folder of the DVD to the root directory of the local FTP server.

3   Use this local FTP server for Platform Update.

Using the Dell Repository Manager to Create the Repository and Copy it to a Local FTP Server

1   Copy the repository created using the Dell Repository Manager to the root directory of the local FTP server.

> **NOTE:** See the *Dell Repository Manager User Guide* at support.dell.com/manuals for information on creating a repository for your system.

2   Use this local FTP server for Platform Update.

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
- 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.

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 who 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 **support.dell.com**.

Copying the Repository to a Local USB Device from the Dell Server Updates DVD

1 Download the *Dell Server Updates* ISO to your system from **support.dell.com**, and burn it to a DVD.

2 Copy the repository folder of the DVD to the root directory of the USB device.

3 Use this USB device for Platform Update.

Using the Dell Repository Manager to Create the Repository and Copy it to a USB Device

1 Copy the repository created using the Dell Repository Manager to the root directory of the USB device.

   NOTE: See the *Dell Repository Manager User Guide* at support.dell.com/manuals for information on creating a repository for your system.

2 Use this USB device for Platform Update.

A

Troubleshooting and Frequently Asked Questions

This section describes the error messages commonly generated by Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE), and provides suggestions for resolving the errors. It also answers questions that are frequently asked by USC and USC-LCE users.

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-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	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: • 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. To resolve this issue, click **Exit and Reboot** and shut down the system. Then, ensure you have at least one device on which to install an operating system before launching USC or USC-LCE again.

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" on page 37).
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 *Dell Server Updates* DVD (see "Configuring a Local USB Device" on page 79) 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" on page 91"or "Repairing USC-LCE" on page 91.
Network is not configured	Network settings must be configured for USC or USC-LCE to work correctly. See "Operating System Deployment" on page 21 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 "Selecting the Download Method" on page 38 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.

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

Error Message	Resolution
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.
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.
Mount partition failed during OS deployment	Retry the operation. If the issue persists, reboot iDRAC.
Ping Test Failed	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.

Table A-2. USC Error Messages and Resolutions

Error Message	Resolution
Unable to find a device capable of reading the OS install media	USC cannot detect a device to read the operating system media. One of the following situations is probably causing the error: • 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	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" on page 77) or provide an alternate repository.

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" on page 37).
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: • 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 *Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide* 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" on page 79) 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" on page 79) 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" on page 79) 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" on page 79) or provide an alternate repository.
Unable to resolve host name	This error is probably caused by one of the following: • You have specified an invalid name for the platform update FTP server. See "Selecting the Download Method" on page 38. • The Domain Name Server (DNS) specified in the **Network Settings** page is invalid. See "Operating System Deployment" on page 21.
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" on page 79) 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" on page 50.
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" on page 50.

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" on page 50.
Please enter a valid IPv6 DNS Server 1 Address	Enter a valid IPv6 DNS Server1 address. See "IPv6 Configuration" on page 50.
Please enter a valid IPv6 DNS Server 2 Address	Enter a valid IPv6 DNS Server2 address. See "IPv6 Configuration" on page 50.
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" on page 47.
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" on page 47.
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: **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: **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: **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. Re-open the **Advanced Configuration** screen.
This feature is not supported in this configuration	Your modular system does not support the feature you selected.
NFS Support is not present	Type the correct NFS share name and retry.
No Share Name/Details present	Type the correct share name or username and password, and retry.
Failed to authenticate. Invalid share name, username, or password.	Type the correct share name or username and password, and retry.
Invalid Catalog File	Type the correct path to the catalog file, or the correct catalog name.
Could not Connect the Share	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.
Network Share Mount Failed	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.

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

Error Message	Resolution
Requested operation completed successfully. Error occurred while shutting down the system. Shutdown manually.	Press the power button on the system to shutdown manually.
One or more of following links will be disabled if the required hardware is not present in the system.	Ensure that a healthy and licensed vFlash SD card is present in the system.
Failed to copy to Network Share	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.
Failed to log the message	Ensure that these characters are not used in the message: <, >, &, and %. If the issue persists, reboot iDRAC.
Failed to Open Dell Update Package File	Use the correct DUP, name, and path.
Invalid USB Folder Location	Provide the valid folder location.
Invalid Network Share Folder Location	Provide the valid folder location.
Invalid USB and Network Share Folder Location	Provide the valid folder location.
Failed to copy to USB Device. Destination folder not present	Ensure that the folder exits, or create the folder and retry.
Failed to copy to Network Share. Destination folder not present	Ensure that the folder exists, or create a folder and retry.

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

Error Message	Resolution
The Update Package is not supported for this System	Ensure that the DUP is supported on the system.
Invalid Update Package	Ensure that the DUP is not corrupt or tampered.

Repairing the USC and USC-LCE

Repairing USC

If the message `System Services update required` appears during power-on self-test (POST), the embedded device that stores USC may contain corrupted data. To resolve the issue, try to update USC by executing USC Dell Update Package (DUP) from the operating system. 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 during power-on self-test (POST), 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_1.4.0_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" on page 37 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.

Ø **NOTE:** Updates that are required for a complete system recovery are pre-selected by USC-LCE. It is highly recommended that you run all the selected updates on the system.

Frequently Asked Questions

1 **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.

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

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

3 **What is virtual media?**

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

4 **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**.

5 **What is vFlash SD card?**

vFlash SD card is a formatted SD (Secure Digital) card that plugs into iDRAC6 Enterprise. vFlash SD card can be formatted and enabled via iDRAC to make it accessible as a USB drive for data storage. Virtual flash is a partition on vFlash SD card 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.

6 **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" on page 37 for more information on updating the drivers that are used for operating system installation.

7 **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.

8 **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 *Dell Server Updates* DVD's are supported. See "Configuring a Local USB Device" on page 79 for more information.

9 **Can I delete USC or USC-LCE?**

No.

10 **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**).

11 **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**).

12 **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.

13 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" on page 25 for more information.

Advanced Configuration allows you to configure Human Interface Infrastructure (HII) enabled devices (for example, NICs and BIOS). See "HII Advanced Configuration" on page 65 for more information.

14 Does USC or USC-LCE support configuration of all RAID levels and all RAID cards for *y*x1*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)

15 Does USC-LCE support rollback of BIOS and firmware?

Yes. See "Platform Rollback" on page 25 for more information.

16 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" on page 37 for more information.

17 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" on page 25 for more information.

18 **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 appears. 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" on page 91 of "Repairing USC-LCE" on page 91. If that does not resolve the problem, contact Dell for technical assistance.

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

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

20 **What should I do if I have an issue with mouse synchronization when I access USC LCE over the iDRAC Virtual Console?**

Ensure that the **Single Cursor** option under Tools in the iDRAC Virtual Console menu is selected on the iDRAC Virtual Console 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.

21 **Why should I use Microsoft Windows-based DUPs for USC-LCE 1.4 feature enhancements instead of Linux-based DUPs?**

Only Microsoft Windows-based DUP updates are available for USC-LCE version 1.4 and above. When using a local repository to upgrade from USC-LCE version 1.3 to version 1.4, ensure to create a catalog with Linux-based DUPs.

22 **Why should I keep CSIOR enabled?**

The Collect System Inventory On Restart (CSIOR) must be enabled so that USC-LCE invokes part firmware update and hardware configuration automatically on system startup.

23 **Why are some features not accessible in USC or USC-LCE?**

The features like Lifecycle Log, Hardware Inventory (View and Export), Part Replacement, and vFlash SD card configuration are dependent on latest iDRAC firmware. Ensure that the latest iDRAC firmware is installed.

B

Schema

This section displays a typical lifecycle log schema.

Lifecycle Log Schema

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:dm=
"http://www.w3.org/2001/XMLSchema" targetNamespace=
"http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
```

```
 <xs:element name="Description" type="xs:string"/>
```

```
 <xs:element name="MessageID" type="xs:string"/>
```

```
 <xs:element name="Arg" type="xs:string"/>
```

```
 <xs:element name="MessageArguments">
```

```
   <xs:complexType>
```

```
     <xs:sequence minOccurs="0">
```

```
       <xs:element ref="dm:Arg" minOccurs="0"/>
```

```
     </xs:sequence>
```

```
   </xs:complexType>
```

```
  </xs:element>
```

```
 <xs:element name="Event">
```

```
   <xs:complexType>
```

```
     <xs:sequence minOccurs="0">
```

```
       <xs:element ref="dm:Description" minOccurs="0"/>
```

```
       <xs:element ref="dm:MessageID" minOccurs="0"/>
```

```
       <xs:element ref="dm:MessageArguments" minOccurs="0"/>
```

```
     </xs:sequence>
```

```
       <xs:attribute name="TimeStamp" type="xs:string" use=
"required"/>
```

```
        <xs:attribute name="AgentID" type="xs:integer" use=
"required"/>
          <xs:attribute name="Severity" type="xs:integer" use="required"/>
          <xs:attribute name="s" type="xs:string" use="required"/>
      </xs:complexType>
    </xs:element>
    <xs:element name="Events">
      <xs:complexType>
        <xs:sequence minOccurs="0">
          <xs:element ref="dm:Event" minOccurs="0" maxOccurs=
"unbounded"/>
        </xs:sequence>
          <xs:attribute name="lang" type="xs:string" use="optional"/>
          <xs:attribute name="schemaVersion" type="xs:string" use=
"optional"/>
          <xs:attribute name="timeStamp" type="xs:dateTime" use=
"optional"/>
      </xs:complexType>
    </xs:element>
</xs:schema>
```

C

Easy-to-use System Component Names

Table C-1.   Easy-to-use Names of System Components

System Component Name	Easy-to-use Name
RAID.Integrated.1	Integrated RAID Controller 1
	Integrated RAID Controller 2
RAID.Slot.1-1	RAID Controller in Slot 1
NIC.Mezzanine.1B-1	
NIC.Mezzanine.1C-1	NIC in Mezzanine 1 (Fabric B)
NIC.Mezzanine.1C-2	
NIC.Mezzanine.3C-2	
NonRAID.Integrated.1-1	Integrated Storage Controller 1
	Integrated Storage Controller 2
NonRAID.Slot.1-1	Storage Controller in Slot 1
NonRAID.Mezzanine.2C-1	Storage Controller in Mezzanine 1 (Fabric C)
NIC.Embedded.1	Embedded NIC 1
NIC.Embedded.2	Embedded NIC 2
NIC.Embedded.1-1	Embedded NIC 1 Port 1
NIC.Embedded.1-1-1	Embedded NIC 1 Port 1 Partition 1
NIC.Slot.1-1	NIC in Slot 1 Port 1
NIC.Slot.1-2	NIC in Slot 1 Port 2
Video.Embedded.1-1	Embedded Video Controller
HostBridge.Embedded.1-1	Embedded Host Bridge 1
ISABridge.Embedded.1-1	Embedded ISA Bridge 2
P2PBridge.Embedded.1-1	Embedded P2P Bridge 3

Table C-1.   Easy-to-use Names of System Components *(continued)*

System Component Name	Easy-to-use Name
P2PBridge.Mezzanine.2B-1	Embedded Host Bridge in Mezzanine 1 (Fabric B)
USBUHCI.Embedded.1-1	Embedded USB UHCI 1
USBOHCI.Embedded.1-1	Embedded USB OHCI 1
USBEHCI.Embedded.1-1	Embedded USB EHCI 1
Disk.SATAEmbeded.A-1	Disk on Embedded SATA Port A
Optical.SATAEmbeded.B-1	Optical Drive on Embedded SATA Port B
TBU.SATAExternal.C-1	Tape Back-up on External SATA Port C
Disk.USBFront.1-1	Disk connected to front USB 1
Floppy.USBBack.2-1	Floppy-drive connected to back USB 2
Optical.USBFront.1-1	Optical drive connected to front USB 1
Disk.USBInternal.1	Disk connected to Internal USB 1
Optical.iDRACVirtual.1-1	Virtually connected optical drive
Floppy.iDRACVirtual.1-1	Virtually connected floppy drive
Disk.iDRACVirtual.1-1	Virtually connected disk
Floppy.vFlash.<string>	vFlash SD Card Partition 2
Disk.vFlash.<string>	vFlash SD Card Partition 3
iDRAC.Embedded.1-1	iDRAC
System.Embedded.1-1	System
HardDisk.List.1-1	Hard Drive C:
BIOS.Embedded.1-1	System BIOS
BIOS.Setup.1-1	System BIOS Setup
PSU.Slot.1	Power Supply 1
Fan.Embedded.1	Fan 1
	Fan 2
System.Chassis.1	Blade Chassis
LCD.Chassis.1	LCD

Table C-1. Easy-to-use Names of System Components *(continued)*

System Component Name	Easy-to-use Name
Fan.Slot. 1	Fan 1
Fan.Slot. 2	Fan 2
…	…
Fan.Slot. 9	Fan 9
MC.Chassis.1	Chassis Management Controller 1
MC.Chassis.2	Chassis Management Controller 2
KVM.Chassis.1	KVM
IOM.Slot.1	IO Module 1
…	…
IOM.Slot.6	IO Module 6
PSU.Slot.1	Power Supply 1
…	...
PSU.Slot.6	Power Supply 6
CPU.Socket.1	CPU 1
System.Modular.2	Blade 2
DIMM.Socket.A1	DIMM A1

Index

W