

Dell Lifecycle Controller
USC/USC-LCE
Version 1.5
User's Guide



Notes and Cautions



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



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

Information in this document is subject to change without notice.

© 2011 Dell Inc. All rights reserved.

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

Trademarks used in this text: Dell™, the DELL logo, OpenManage™, PowerEdge™, and PowerVault™ are trademarks of Dell Inc. Intel® is a registered trademark of Intel Corporation in the U.S. and other countries. Boradcom® is either a trademark or registered trademark of Broadcom Corporation in the United States and/or other countries. Microsoft®, Windows®, and Windows Server® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® and ESX™ are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Novell® and SUSE® are registered trademarks of Novell, Inc. in the United States and other countries. Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries. Citrix™ is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. The term Linux® is a registered trademark of Linus Torvalds, the original author of the Linux kernel.

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

Contents

1	Introduction	11
	Why Use USC/USC-LCE?	12
	USC and USC-LCE Features and Product Classification	13
	What's new in USC/USC-LCE 1.5	16
	Upgrading to USC or USC-LCE	16
	Other Documents You May Need	17
2	Using USC or USC-LCE	19
	Launching USC or USC-LCE	19
	Launch Messages—Causes and Resolutions.	20
	Enabling USC or USC-LCE	21
	Disabling USC or USC-LCE	21
	Canceling Request to Enter System Services	21
	Using USC for the First Time	22
	Using USC-LCE for the First Time	22
	Using USC Settings Wizard.	22

3	USC and USC-LCE Features	25
	Lifecycle Log	26
	USC-LCE Platform Update	26
	FTP Authentication	27
	Platform Rollback	27
	Hardware Configuration	28
	Configuration Wizards	28
	HII Advanced Configuration	28
	Hardware Inventory–View and Export	28
	Delete Configuration and Reset Defaults.	30
	Operating System Deployment	30
	Driver Access	30
	Driver Extraction	31
	Driver Installation Methods.	31
	RAID Configuration	31
	Platform Restore	32
	Part Replacement Configuration	32
	Backup Server Profile	32
	Export Server Profile	33
	Import Server Profile	34
	Hardware Diagnostics	34
	USC or USC-LCE Repair	35
	RAID Configuration.	35
	Key Encryption	36
	Local Key Encryption Mode.	36

4 USC and USC-LCE Operations	37
Viewing Hardware Inventory–Current or Factory Shipped	37
Exporting Hardware Inventory–Current or Factory Shipped	37
Prerequisites	37
Workflow	38
Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller	39
Updating Platform	40
Version Compatibility	40
Viewing Current Version Information.	40
Launching Platform Update Wizard	40
Selecting Download Method	41
Selecting and Applying Updates	44
Rolling Back to Previous BIOS and Firmware Versions	45
Updating Hardware Diagnostics Utility.	47
Performing Hardware Diagnostics	48
Installing Operating System	48
Prerequisites	48
Workflow	48
Selecting Operating System Driver Source Location (for USC only)	49
Online Repository.	49
Local Drive	50
Using Optional RAID Configuration	51
Configuring RAID Using Operating System Deployment Wizard.	51

Bypass RAID configuration:	51
Selecting Operating System	52
Selecting an Operating System Available in the List	52
Selecting Custom Operating System	53
Selecting an Operating System Not Available in the List	53
Driver Extraction and Installation.	54
Installing Drivers for RHEL 4.8 Operating System	54
Rebooting System	55
Post Reboot Scenarios	55
Operating System–Post Installation Scenarios	56
Assigning a Windows-Bootable System Partition to Drive C	56
Installing Red Hat Enterprise Linux 4.8 on a System with SAS7 (H200) Controller.	56
Controlling Access to the System Control Panel	57
System Control Panel Access Options	57
Configuring System Date/Time.	58
Configuring iDRAC	58
LAN Configuration	59
Advanced LAN Configuration.	61
Common IP Configuration.	62
IPv4 Configuration	63
IPv6 Configuration	65
Virtual Media Configuration	67
LAN User Configuration.	67
Summary and Confirmation.	70
Configuring RAID using Hardware RAID	70

Important	70
Workflow	70
View Current Configuration.	71
Select RAID Controller	71
Foreign Configuration Found	72
Express or Advanced Wizard.	72
Select Basic Settings.	73
Express Wizard Only - Assign a Hot Spare.	75
Express Wizard Only - Review Summary.	76
Advanced Wizard Only - Select Physical Disks.	76
Advanced Wizard Only - Additional Settings	77
Advanced Wizard Only - Review Summary	78
Configuring RAID using Software RAID.	79
Prerequisites	79
Workflow	79
Creating a Secure Virtual Disk on Series 7 Controller.	80
Configuring vFlash SD Card	81
HII Advanced Configuration	82
Encrypting Unsecure Virtual Disks	84
Prerequisites	84
Workflow	85
Applying the Local Key on the RAID Controller.	85
Prerequisites	85
Workflow	85
Rekey Controller with a New Local Key	86
Remove Encryption and Delete Data	86

Upgrading to an iDRAC6 Express Card	87
Installing iDRAC6 Express Card.	87
Transferring an iDRAC6 Express Card	88
Removing iDRAC6 Express Card	88
Configuring a Local FTP Server	89
Requirements for a Local FTP Server.	89
Copying Repository to a Local FTP Server from the Dell Server Updates DVD	89
Using Dell Repository Manager to Create the Repository and Copy it to a Local FTP Server	90
Accessing Updates on a Local FTP Server.	90
Configuring a Local USB Device.	91
Copying Repository to a Local USB Device from the Dell Server Updates DVD	91
Using the Dell Repository Manager to Create the Repository and Copy it to a USB Device	92
Part Replacement Configuration.	92
Prerequisites	92
Supported Devices	93
Collect System Inventory on Restart	93
Part Firmware Update	93
Part Configuration Update	94
Back Up Server Profile.	94
Prerequisites	94
Workflow	94
Exporting Server Profile to a USB Device or Network Share	95
Prerequisites	95
Workflow	95

Importing Server Profile from a vFlash SD Card, Network Share, or USB Device	96
Prerequisites	96
Workflow	97
Post-import Scenario	98
Importing Server Profile after Motherboard Replacement	99
Prerequisites	99
Workflow	99
Post-requisites	99
Viewing Lifecycle Log History	100
Exporting Lifecycle Log	101
Prerequisites	101
Workflow	101
Adding a Work Note to Lifecycle Log	103
Deleting Configuration and Resetting Defaults	103
5 Troubleshooting and Frequently Asked Questions	105
Error Messages	105
Repairing the USC and USC-LCE	116
Repairing USC	116
Repairing USC-LCE	116
Frequently Asked Questions.	118

A Lifecycle Log Schema	123
B Easy-to-use System Component Names	125
Index	129

Introduction

The Dell Lifecycle Controller provides advanced embedded systems management and is delivered as part of iDRAC Express card and embedded Unified Extensible Firmware Interface (UEFI) applications in the 11th generation Dell servers. 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.



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

The Lifecycle Controller has the following components:

- Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE):
 - Are an embedded configuration utility that reside on an embedded flash memory card.
 - Are similar to the BIOS utility that is started during the boot sequence, and can function in a pre-operating system environment.
 - Enable systems and storage management tasks from an embedded environment throughout the system's life cycle.

USC and USC-LCE simplify end-to-end server lifecycle management using the one-to-one method:

- Provisioning — Entire pre-operating system configuration from a unified interface.
- Deploying — Simplified operating system installation with embedded drivers on the Lifecycle Controller.
- Download drivers for operating system installation from one of the following sources:
 - Dell FTP website at <ftp.dell.com>
 - USB mass storage device
 - *Dell Lifecycle Controller OS Driver Packs* DVD

- *Dell Server Updates DVD*
 - *Dell Systems Build and Update Utility DVD (for USC only).*
 - Network share
- Patching/Updates (USC-LCE only) — Operating system agnostic and reduced maintenance downtime with direct access to updates from **ftp.dell.com**. It simplifies BIOS and firmware updates by maintaining a working version for rollback.
 - Servicing (USC-LCE only) — Continuous availability of diagnostics without the hard drive dependency. Ability to flash firmware automatically while replacing field replaceable components such as a Dell PowerEdge RAID controller, NIC, or power supply.
 - Security (USC-LCE only) — Supports local key encryption.
 - Restoring Platform — Backup the server profile (including RAID configuration) and restore the server to a previously known state.
- Remote Services simplifies end-to-end server lifecycle management using the one-to-many method. For more information, see *Dell Lifecycle Controller Remote Services User's Guide*.

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. Prior to the release of USC and USC-LCE, an administrator had to use many tools such as DSA, SBUU, and DTK shipped on multiple CDs/DVD. Maintaining and using the multiple disks in their many versions was time consuming for the administrator.

To resolve these problems, Dell now provides the Lifecycle Controller, a flash chip embedded on the system 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 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

your 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 Product Classification

Table 1-1. USC and USC-LCE Features

Features	USC	USC-LCE
Base-level product uses BMC and provides the following capabilities:	Yes	Yes
<ul style="list-style-type: none"> • Operating System Deployment • Hardware Diagnostics • USC Settings 		
Fully-featured product uses iDRAC6 Express and Enterprise cards, and provides the following capabilities:	No	Yes
<ul style="list-style-type: none"> • Operating System Deployment • Hardware Diagnostics • USC Settings • Platform Update • Hardware Configuration • View and Export Hardware Inventory • View and Export Lifecycle Log • Platform Restore 		

USC or USC-LCE displays the features that the system supports, depending on the system configuration. Table 1-2 shows the product classifications for USC/USC-LCE. For example, for a Dell system *y1lx* 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
	Standard	Embedded BMC	USC	BMC - Operating System Deployment, Hardware Diagnostics, USC Settings
y21x to y51x	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 (current and factory shipped)
		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 (current and factory shipped) iDRAC6 Enterprise - adds Full Remote Management, Dedicated NIC port, Virtual Console, Virtual Media, part replacement, vFlash SD card management, Platform Restore

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 (current and factory shipped)
	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 (current and factory shipped) iDRAC6 Enterprise - adds Full Remote Management, Dedicated NIC port, Virtual Console, Virtual Media, part replacement, vFlash SD card management, Platform Restore

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

What's new in USC/USC-LCE 1.5

The new features are:

- Backup and Export server profile
- Import server profile
- View and export factory shipped inventory
- Configure and upgrade firmware for Converged Network Adapters (CNA) cards. Supported on the following CNA card:
Broadcom:
 - M710HD Dual Port 10Gig 57712 NDC
- Software RAID configuration¹
- Enhancement to the RAID configuration feature — Virtual disk slicing support
- Driver packs support for new operating systems¹. For more information, see *USC/USC-LCE – Supported Dell Systems and Operating Systems* section in the *Dell Systems Software Support Matrix* available at support.dell.com/manuals.

1. Indicates the newly introduced feature for USC.

Upgrading to USC or USC-LCE

Depending on the 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 upgrades the USC to USC-LCE. See [Updating Platform](#) for more information.



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

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 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 *USC/USC-LCE Supported Dell Systems and Operating Systems* section in the *Dell Systems Software Support Matrix* provides the list of Dell systems and operating systems that you can deploy on the target systems.
- The *PERC H700 and H800 Technical Guidebook* for specification and configuration related information about the PERC H700 and H800 controllers.
- The *Dell Systems Build and Update Utility (SBUU) User's Guide* provides information to deploy and update Dell systems.
- The *Glossary* provides information about the terms used in this document.

Using USC or USC-LCE

Before using USC/USC-LCE, you must ensure that the following prerequisites are met:

- Ensure that your network is configured.
- Ensure that the system has the latest versions of iDRAC and BIOS installed. See *Readme* for more information.

Launching USC or USC-LCE

To launch USC or USC-LCE during the system boot, press <F10> key within 10 seconds of the Dell logo being displayed to enter **System Services**. When USC or USC-LCE is launched for the first time, it displays **USC Settings** wizard that allows you to configure the preferred language and network settings. See [Using USC Settings Wizard](#) for more information.



NOTE: If the system does not enter **System Services**, see Table 2-1 for cause and resolution.

Launch Messages—Causes and Resolutions

Table 2-1 lists the messages that appear during system launch, and their cause and resolution.

Table 2-1. Launch Error Messages—Causes and Resolutions

Message	Cause	Resolution
System Services disabled	<ul style="list-style-type: none"> • The system is turned on or restarted while iDRAC is initializing. This occurs if: <ul style="list-style-type: none"> – The system is turned on immediately after AC is applied to the system. – The system is restarted immediately after resetting iDRAC. • The product is manually disabled. 	<ul style="list-style-type: none"> • Wait for a minute after resetting iDRAC to restart the system, so that iDRAC initializes. • See Disabling USC or USC-LCE for information on disabling USC or USC-LCE.
System Services update required	The embedded device that stores the product may contain corrupted data.	<p>Update the product using USC or USC-LCE Dell Update Package (DUP). See the <i>Dell Update Packages User's Guide</i> at support.dell.com/manuals for more information.</p> <p>If an operating system is not installed on the system or if running the DUP does not fix the problem, run the USC or USC-LCE repair package. See Repairing USC or Repairing USC-LCE for more information.</p>
System Services not available	Another process is currently using iDRAC.	Wait for 30 minutes for the current process to complete, reboot the system, and retry. Alternatively, see Canceling Request to Enter System Services .

Enabling USC or USC-LCE

- 1 Press <Ctrl> <E> within five seconds after system start-up.
The iDRAC6 Configuration Utility is displayed.
- 2 Navigate to System Services.
- 3 Select Disable System Services.
- 4 Save your changes and exit the iDRAC6 Configuration Utility. The system reboots automatically.


Disabling USC or USC-LCE

To prevent the system from entering USC or USC_LCE during startup, do the following:

- 1 Press <Ctrl> <E> within five seconds after system start-up.
The iDRAC6 Configuration Utility is displayed.
- 2 Navigate to System Services.
- 3 Select Disable System Services.
- 4 Save your changes and exit the iDRAC6 Configuration Utility. The system reboots automatically.

Canceling Request to Enter System Services

If USC or USC-LCE causes the system to repeatedly reboot, you can cancel the 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 five seconds after system start-up.
The iDRAC6 Configuration Utility page is displayed.
- 2 Navigate to System Services.
- 3 Select Cancel System Services.
- 4 Save your changes and exit the iDRAC6 Configuration Utility. The system reboots automatically.

Using USC for the First Time

When using USC for the first time, it is recommended that you run the wizards:

- 1 **USC Settings** — Run the wizard to change the language, keyboard, or network settings.
- 2 **OS Deployment** — Run to install the operating system.
- 3 **Hardware Diagnostics** — Run diagnostics-check regularly to maintain the system.

See Also:

[USC and USC-LCE Features](#)

Using USC-LCE for the First Time

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

- 1 **USC Settings** — Run the wizard only to change the language, keyboard, or network settings.
- 2 **Platform Update** — Apply updates.

See also:

- [Using USC Settings Wizard](#)
- [Updating Platform](#)

Using USC Settings Wizard

Use **USC Settings** wizard to specify the language, keyboard layout, and network settings for USC or USC-LCE only. This does not change system or other application settings.

Specifying Language, and Keyboard Type

- 1 In the left pane, click **USC Settings**.
- 2 In the right pane, click **Language and Keyboard**. Use the up-arrow and down-arrow keys to select the options.
 - a From the **Language** drop-down menu, select the language.
 - b From the **Keyboard Type** drop-down menu, select the keyboard type.
- 3 Click **Finish** to save the new settings.

Configuring Network Settings (NIC Card)

- 1 In the left pane, click **USC Settings**.
- 2 In the right pane, click **Network Settings**.
 - a From the **NIC card** drop-down menu, select the NIC card to configure.
 - b In the **IP Address Source** drop-down menu, select one of the following options:



NOTE: The IP Address Source function only supports IPv4.


- **No Configuration** — Does not configure the NIC.
- **DHCP** — Obtains an IP address from a DHCP server.
- **Static IP** — Uses a static IP address. Specify the following IP address properties — **IP Address**, **Subnet Mask**, **Default Gateway**, **DNS Address**. If you do not have this information, contact the network administrator.

- 3 Click **Finish** to save the settings.



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

Accessing Help

Each USC or USC-LCE screen has a **Help** icon 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.

USC and USC-LCE Features

This chapter provides a brief description of the Unified Server Configurator (USC) and Unified Server Configurator-Lifecycle Controller Enabled (USC-LCE) features. Also helps you familiarize with USC and USC-LCE wizards to use USC-LCE most effectively. Table 3-1 lists the features that USC and USC-LCE supports. Each feature is a wizard in USC and USC-LCE.

Table 3-1. USC and USC-LCE Wizards

Wizards/Menu	Description	USC	USC-LCE
Home	Navigate back to Home screen.	Yes	Yes
Lifecycle Log	View and export lifecycle log, and add a work note to lifecycle log.	No	Yes
USC-LCE Platform Update and Platform Rollback	Apply updates or perform platform rollback for the system.	No	Yes
Hardware Configuration	Configure system devices.	No	Yes
Operating System Deployment	Install an operating system.	Yes	Yes
Platform Restore	Backup, export, and restore system profile.	No	Yes
Hardware Diagnostics	Perform diagnostics to validate the memory, I/O devices, CPU, physical disks, and other peripherals.	Yes	Yes
Using USC Settings Wizard	Specify the language, keyboard layout, and network settings while using USC or USC-LCE.	Yes	Yes
About	View the version information of USC-LCE and UEFI.	Yes	Yes

Lifecycle Log

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

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

Using this wizard, you can view, export, and add a work note to a log history.

See Also:

- [Viewing Lifecycle Log History](#)
- [Exporting Lifecycle Log](#)
- [Adding a Work Note to Lifecycle Log](#)

USC-LCE Platform Update

Use the **Platform Update** wizard to:

- View the current versions of the installed applications and firmware.
- Display the list of available updates.
- Select the required updates, downloads (automatic), and apply the updates.

To ensure optimal system performance and avoid system failures, it is recommended that you download and apply updates on a regular basis.

Contact your IT administrator for the preferred method to access the updates in your organization. The IT administrator can provide the updates on any of the following locations or media:

- FTP server
- Local USB device
- *Dell Server Updates* DVD
- Network share

If the FTP server or network share is used for update, configure the network card using **USC Settings** wizard before accessing the updates.

See Also:

- [Updating Platform](#)

FTP Authentication

USC supports anonymous login by authenticating the blank username, a password of your choice, and the FTP server address with the FTP server 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 be configured to accept incoming FTP response traffic.

See Also:

- [Using USC Settings Wizard](#)
- [Updating Platform](#)
- [Configuring a Local FTP Server](#)

Platform Rollback

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



NOTE: You cannot roll back the hardware diagnostics application, and operating system driver pack installation to earlier versions.

This feature is available:

- 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.



NOTE: If you have used other update methods, this feature is not available.

See Also:

- [Rolling Back to Previous BIOS and Firmware Versions](#)

Hardware Configuration

USC-LCE provides different wizards for configuring hardware, and they are:

Configuration Wizards

Use the configuration wizards to configure system devices. The Configuration Wizards include Physical Security Configuration, System Date/Time Configuration, iDRAC Configuration, RAID Configuration, Key Encryption, and vFlash SD card Configuration.

See Also:

- [Controlling Access to the System Control Panel](#)
- [Configuring System Date/Time](#)
- [Configuring iDRAC](#)
- [RAID Configuration](#)



NOTE: You can also configure RAID through the **OS Deployment** wizard. For more information, see [Configuring RAID Using Operating System Deployment Wizard](#).

- [Creating a Secure Virtual Disk on Series 7 Controller](#)
- [Configuring vFlash SD Card](#)
- [Key Encryption](#)

HII Advanced Configuration

Use the Human Interface Infrastructure (HII) to configure BIOS, and certain devices such as NIC. See [HII Advanced Configuration](#) for more information.

Hardware Inventory—View and Export



NOTE: The Hardware Inventory feature is disabled if the iDRAC firmware is not updated to the supported version. Make sure to install iDRAC firmware version 3.2 for Blade systems and 1.7 for Rack and Tower systems.

About View and Export Current Inventory

You can view the hardware information about the currently installed hardware components that are internal to the system chassis and the configuration for each component. The table lists all the currently installed hardware

components (for example, fans, PCI devices, NICs, DIMMs, PSU, and so on), and their properties and values. From the **Filter by Hardware Component** drop-down menu, select the hardware component to view its properties and values. You can export this information in the XML format into a **USB Device** or **Network Share**. The XML file is saved in this format - *HardwareInventory_<servicetag>_<timestamp>.xml*.

For more information on the easy-to-use names of the hardware components, see Table B-1.



NOTE: Incorrect inventory data is displayed or exported after performing **Delete Configuration and Reset Defaults**. See [Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller](#) for displaying correct inventory data.

See Also:

- [Viewing Hardware Inventory—Current or Factory Shipped](#)
- [Exporting Hardware Inventory—Current or Factory Shipped](#)

About View and Export Factory Shipped Inventory

You can view the hardware information about the factory installed hardware components and their configuration. The table lists all the factory installed hardware components (for example, fans, PCI devices, NICs, DIMMs, PSU, and so on), and their properties and values. From the **Filter by Hardware Component** drop-down menu, select the hardware component to view its properties and values. You can export this information in this XML format into a **USB Device**, or **Network Share**, or both the locations.

For more information on the easy-to-use names of the hardware components, see Table B-1.

View and Export factory shipped inventory feature may be grayed-out on the system due to one of the following:

- This feature requires factory installed data. Although the current version supports this feature, the factory installed data is not present on the system.
- Delete Configuration and Reset Defaults was applied and this has permanently deleted the Factory Shipped Inventory.

See Also:

- [Viewing Hardware Inventory—Current or Factory Shipped](#)
- [Exporting Hardware Inventory—Current or Factory Shipped](#)

Delete Configuration and Reset Defaults

You can delete the current iDRAC settings and reset iDRAC to factory defaults. It also deletes lifecycle logs and the factory shipped inventory information on the managed node. For more information, see [Deleting Configuration and Resetting Defaults](#).

Operating System Deployment

Driver Access

For USC

USC does not provide local drivers repository or does not support single Dell Update Package (DUP.) Use one of the following options to access the driver packages:

- ftp.dell.com
- Local FTP
- USB device
- *Dell Systems Build and Update Utility DVD*

See Also:

[Selecting Operating System Driver Source Location \(for USC only\)](#)

For USC-LCE

USC-LCE provides a local repository for drivers that are required for operating system installation. Based on the operating system being installed, the OS **Deployment** wizard extracts these drivers and copies them to a staging directory.



NOTE: Although, USC-LCE has embedded drivers that are factory installed, there may be latest drivers available. Before installing the operating system, run the **Platform Update** wizard to ensure that the latest drivers are available. See [Updating Platform](#) for more information.

Driver Extraction

The drivers required for the operating system, or updates recommended for updating the 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 displays a message that another session is active.

Driver Installation Methods

Table 3-2 lists the driver installation methods for different operating systems.

Table 3-2. Driver Installation Method

Operating System	Installation Methods
Microsoft Windows operating systems NOTE: See USC-LCE readme for more information.	Extracted drivers are installed during the operating system installation.
Red Hat Linux Enterprise Linux version 4.8	Manually install the extracted drivers after the operating system installation.
Red Hat Enterprise Linux version 5.5, SUSE Linux Enterprise Server version 10 SP3, SUSE Linux Enterprise Server version 11 SP1 and later versions	Extracted drivers are installed during the operating system installation.

RAID Configuration

During operating system installation, you can do one of the following:

- Deploy the operating system without configuring RAID
- Configure the disks using the optional RAID configuration wizard and deploy the operating system.

Table 3-3 lists the operations USC or USC-LCE performs based on the availability of the RAID controller and the option selected.

Table 3-3. RAID Configuration

RAID Controller Availability	Operations
<ul style="list-style-type: none">• System does not have a RAID controller• Bypass the optional RAID configuration	OS Deployment wizard installs the operating system to a default location, which is typically the disk identified as Disk 0 in the BIOS utility.
<ul style="list-style-type: none">• System has a RAID controller and you selected the optional RAID configuration	Configure a virtual disk and select a virtual disk as the boot device.

Platform Restore

Part Replacement Configuration

Use this feature to automatically update a new part to the firmware version or the configuration of the replaced part, or both.

See Also:

- [Part Replacement Configuration](#)

Backup Server Profile

Use this feature to do the following and store the backup image files in the vFlash SD card:

- Back up the following:
 - Hardware and firmware inventory such as BIOS, LOMs, USC supported add-in NIC cards, and Storage Controllers (RAID level, virtual disk, and controller attributes)
 - System information
 - Lifecycle Controller firmware images, data and configuration, and iDRAC firmware and configuration.
- Optionally secure the backup image file with a passphrase

System or Feature Behavior During Backup

- System Services is not available.
- A partition with a label name SRVCNF is automatically created on the vFlash SD card to store the backup image file. If a partition with the label name SRVCNF already exists, it is overwritten.
- Takes up to 45 minutes depending on the server configuration.
- Takes a back up of everything; you cannot back up information for one device (for example, backup only LOM firmware and configuration).
- Does not back up diagnostics or driver pack information.

See Also:

[Back Up Server Profile](#)

Export Server Profile

Use this feature to export the backup image file on the vFlash SD card to a USB device or network share.

System or Feature Behavior during Export

- Takes up to 15 minutes depending on the server configuration.
- USC -LCE exports the backup image file in the **DELLBR** `_<service_tag>_time_stamp format. The <service_tag> is copied from the backup image file name. The <time_stamp> is the time when the backup was initiated.`
- After a successful export, the event is logged in the Lifecycle Log.

See Also

- [Exporting Server Profile to a USB Device or Network Share](#)
- [Viewing Lifecycle Log History](#)

Import Server Profile

Use this feature to import and restore the server to a previously known working state from a backup image file that is either located on a vFlash SD card, network share, or USB.



NOTE: You can cancel a restore job using Ctrl-E during POST and select **Cancel System Services**, or reset the iDRAC. This initiates the recovery process and restores the system to a previously known state. Recovery process must not take more than five minutes. To check if the recovery process is complete, view the Lifecycle logs.

System or Feature Behavior During Import

- The System Services that is not available during restore, is enabled after system shutdown.
- Restores everything that was backed up.
- Import may take up to 45 minutes depending on the server configuration.
- Diagnostics or driver pack information is not restored.
- If extra reboots occur during tasks executed in System Services, it is because there was an issue while trying to set the device configuration, which attempts to run the task again. Check the Lifecycle Logs for information on the failed device.
- Import operation for a card fails if the slot in which it was installed earlier has changed.
- System restores all Lifecycle controller content.

See Also

- [Importing Server Profile from a vFlash SD Card, Network Share, or USB Device](#)
- [Importing Server Profile after Motherboard Replacement](#)

Hardware Diagnostics

It is recommended that you run diagnostics as part of a regular maintenance plan to validate that the system and the 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, it is able to

identify hardware problems that the operating system and other online tools cannot identify. You can use the hardware diagnostics utility to validate the memory, I/O devices, CPU, physical disks, and other peripherals.

See Also:

- [Performing Hardware Diagnostics](#)
- [Updating Hardware Diagnostics Utility](#)

USC or USC-LCE Repair

During Power-On Self-Test (POST), if the system displays the message `System Services update required`, the embedded device that stores USC or USC-LCE may contain corrupt data. To resolve this issue, see the following sections:

- [Repairing USC](#)
- [Repairing USC-LCE](#)

RAID Configuration

USC-LCE supports both software RAID and hardware RAID options.

See Also:

- [Configuring RAID using Hardware RAID](#)
- [Configuring RAID using Software RAID](#)

Key Encryption

Use this feature to:

- Set the encryption for PERC H700/H800 RAID controllers in one of the following modes:
 - Local Key Encryption — Applies a local key on the RAID controller and remove the keys.
 - No Encryption — No encryption is applied on the controller and the **Set up local key encryption** option is available.

See Also:

- [Applying the Local Key on the RAID Controller](#)
- Encrypt the existing unsecure virtual disks. To do this, enable the encryption on the controller.

Local Key Encryption Mode

You can perform the following tasks while the controller is in Local Key Encryption mode:



NOTE: For more information on the specification and configuration related information for the PERC H700 and H800 controllers, see the *PERC H700 and H800 Technical Guidebook*.

- Encrypt unsecure virtual disks — Enable data encryption on all the security capable unsecure virtual disks.



NOTE: This option is available if there are virtual disks connected to a security capable controller.

- Rekey controller and encrypted disks with a new key — Replace the existing local key with a new key.
- Remove encryption and delete data — Delete the encryption key on the controller and all the secure virtual disks along with its data. After deletion, controller state changes to No encryption mode.

See Also:

- [Encrypting Unsecure Virtual Disks](#)
- [Rekey Controller with a New Local Key](#)
- [Remove Encryption and Delete Data](#)

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).

Viewing Hardware Inventory—Current or Factory Shipped

To view the currently installed or factory installed hardware components and their configuration:

- 1 From the left pane, click **Hardware Configuration**.
- 2 Click **View Current Inventory** or **View Factory Shipped Inventory** to view the current or factory shipped inventory.

See Also:

- [About View and Export Current Inventory](#)
- [About View and Export Factory Shipped Inventory](#)

Exporting Hardware Inventory—Current or Factory Shipped

To export the currently installed or factory installed hardware components and their configuration:

Prerequisites

- If you use the network share, set the correct **Network Settings**. See [Using USC Settings Wizard](#) 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.

Workflow

To export the current or factory shipped hardware inventory:

- 1 In the left pane, click **Hardware Configuration**.
- 2 Click **Export Current Hardware Inventory** or **Export Factory Shipped Hardware Inventory**.
- 3 Select **USB Device** or **Network Share**.

USB Device

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

- a From the **Choose Device** drop-down menu, select the required device and enter the path to the folder on the device.

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

- b Click **Finish** to export the inventory.

Network Share

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

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

For CIFS

- **Share Name** — Type the path to the shared folder to export the file. For example, type `\\xxx.xxx.xx.xx\sharename`.
- **Domain and User Name** — Type the domain and user name required to log on to the network share. For example, `login-name@myDomain`. 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, `\\xxx.xxx.xx.xx\sharename`.
 - **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 **Finish** to export the inventory.

See Also:

- [About View and Export Current Inventory](#)
- [About View and Export Factory Shipped Inventory](#)

Viewing and Exporting Hardware Inventory after Resetting Lifecycle Controller



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

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

- 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 after 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.

Updating Platform

You can update to the latest version of USC-LCE using the **Platform Update** wizard. It is recommended that you run the **Platform Update** wizard on a regular basis to access the latest updates. For USC-LCE, you can update the firmware and BIOS using individual DUPs (single component DUP.)



NOTE: Make sure that the file name for the single component DUPs does not have any blank space.

See Also:

- [Launching Platform Update Wizard](#)
- [Selecting Download Method](#)
- [Viewing Current Version Information](#)

Version Compatibility

The version compatibility feature enables you to install the Lifecycle Controller, BIOS, and iDRAC versions that are compatible with system components. In case of compatibility issues during update, Lifecycle Controller displays upgrade or downgrade error messages.

Viewing Current Version Information

To view the current versions and time stamp of various system components firmware:

- 1 In the left pane, click **Platform Update**.
- 2 In the right pane, click **View Current Versions**.

Launching Platform Update Wizard

To launch the platform update wizard:

- 1 In the left pane, click **Platform Update**.
- 2 In the right pane, click **Launch Platform Update**.

Selecting Download Method

To download the updates using the **Platform Update** wizard, use one of the following sources:

- FTP server
 - [Dell FTP Server](#)
 - [Configuring Proxy Server](#)



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.

- Local FTP — For more information, see [Accessing Updates on a Local FTP Server](#).
- [Local Drive](#)
- [Network Share](#)
- *Dell Server Updates DVD*

Dell FTP Server

To download drivers from the Dell FTP server, enter ftp.dell.com in the **Address** field.

Configuring Proxy Server

To download drivers from an FTP server using a proxy server:

- 1 Select **FTP Server**.
- 2 Enter the following details.
 - **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.

This step is optional for operating system driver source.



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 is provided. By default, it pings the Gateway and DNS server IP, and also pings any host and proxy IP.

See Also:

[FTP Authentication](#)

Local Drive (CD/DVD/USB)

To perform platform updates from a local drive (USB device or *Dell Server Updates DVD*), use one of the methods:

- Single component DUPs.
 -  **NOTE:** Make sure that the file name for the single component DUPs does not have any blank space.
- Repository
 -  **NOTE:** If the catalog file and DUP are downloaded from **ftp.dell.com**, do not copy them into a sub-directory.

Using Single Component DUPs

- 1 From the drop-down menu, select the volume label.
- 2 In the **Catalog Location** or **Update package path**, enter the name of the DUP (for example, **APP_WIN_RYYYYZZZ.EXE**) or if the DUP is present in a sub-directory, enter both the sub-directory name and name of the DUP (for example, **subdirectory\APP_WIN_RYYYYZZZ.EXE**).

Using Repository

- 1 From the drop-down menu, select the volume label.
- 2 In the **Catalog Location** or **Update package path**, if the catalog file is located in the root folder, do not enter the file name. However, if the catalog file is located in a sub-directory, enter the sub-directory name (for example, **subdirectory**).

See Also:

[Configuring a Local USB Device](#)

Network Share

To perform platform updates from a shared folder over a network, select **Network Share (CIFS or NFS)** and enter the details:

- 1 Enter the network share details. For more information, see Table 4-1.
- 2 Click **Test Network Connection** to verify if USC-LCE is able to connect to the IP address that you provided. By default, it connects to the Gateway and DNS server IP.
- 3 Click **Next**.

Table 4-1. Network Share Details

For CIFS	For NFS
Share Name — Path to the shared folder where the DUPs or repository is located. For example, <code>\\xxx.xxx.xx.xx\sharename</code> .	
Domain and User Name — Type the correct domain and user name required to log on to the network share. For example, <code>login-name@myDomain</code> , and if there is no domain, type the <code>login-name</code> .	NA
Password — Type the correct password	NA

Table 4-1. Network Share Details

For CIFS	For NFS
Catalog Location or Update package path	
NOTE: If the catalog file and DUP are downloaded from ftp.dell.com , do not copy them into a sub-directory.	
Using Single Component DUPs	
NOTE: Make sure that the file name for the single component DUPs does not have any blank space.	
Enter the name of the DUP (for example, <code>APP_WIN_RYYYYZZZ.EXE</code>) or if the DUP is present in a sub-directory, enter both the sub-directory name and name of the DUP (for example, <code>subdirectory\APP_WIN_RYYYYZZZ.EXE</code>).	
Using Repository	
If the catalog file is located in the root folder, do not enter the file name. However, if the catalog file is located in a sub-directory, enter the sub-directory name (for example, <code>subdirectory</code>).	

Selecting and Applying Updates

To select and apply the updates:

- 1 In the left pane of the **Home** page, click **Select Updates**. The list of available updates is displayed.
- 2 Select the required updates and click **Apply**. By default, USC-LCE selects the components for which the current updates are available.
- 3 Click **Apply**.

The system reboots after the update process is complete. When applying more than one update, the system may reboot between updates directly into USC-LCE and continue updating.

If the iDRAC firmware update is interrupted, you may need to wait up to 30 minutes before attempting another firmware update.

See Also:

- [Comparing Versions](#)
- [Updating Devices That Affect Trusted Platform Module Settings](#)
- [Updating RAID Controller Firmware](#)

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. To ensure this error does not occur, upgrade to the latest BIOS and iDRAC versions.



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

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 update the BIOS or firmware only once, the rollback feature provides the option to revert to the factory-installed BIOS or firmware image. If you update the BIOS or firmware more than once, the factory-installed images are overwritten and you cannot revert to them.

Launching Rollback Wizard

To launch the platform rollback wizard:

- 1 Boot the system and press the <F10> key within 10 seconds after the Dell logo appears. USC-LCE is launched.
- 2 In the left pane, click **Platform Update**.
- 3 In the right pane, click **Launch Platform Rollback**. The **Platform Rollback** page displays a list of available rollback components.

Selecting and Applying Rollbacks

To select and apply the rollbacks:

- 1 In the **Platform Rollback** page, select the required rollback image(s).
- 2 Click **Apply**.

After the update process is complete, the system reboots. When applying more than one update, the system may reboot between updates directly into USC-LCE and continue updating.

See Also:

- [Comparing Versions](#)
- [Updating Devices That Affect Trusted Platform Module Settings](#)
- [Updating RAID Controller Firmware](#)

Comparing Versions

If you want to compare the version of the update or rollback 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.

Updating RAID Controller Firmware

To update RAID controller firmware:

- 1 In the left pane of the **Home** page, click **Platform update**.
- 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.

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 indicate components that affect the BitLocker.

You can choose either not to update or to roll back those components by navigating to the **Select Updates** page and deselecting the check boxes for the components.

Updating Hardware Diagnostics Utility

You can update the **Hardware Diagnostics** utility using the Dell Update Packages (DUPs) or **Platform Update** wizard.

Table 4-2. Updating the Hardware Diagnostics Utility

For USC	For USC-LCE
Download the required Dell Update Package (DUP) from support.dell.com , and run the DUP as an executable in the installed operating system.	Use the Platform Update wizard to update. or Download the required Dell Update Package (DUP) from support.dell.com , and run the DUP as an executable in the installed operating system.

See Also:

- [Hardware Diagnostics](#)
- [Updating Platform](#)

Performing Hardware Diagnostics

To perform hardware diagnostics:

- 1 To start the Hardware Diagnostics utility:
 - a In the left pane of USC or USC-LCE, click **Hardware Diagnostics**.
 - b In the right pane, click **Run Hardware Diagnostics**. When the diagnostics utility launches, follow the on-screen instructions.
- 2 To exit the Hardware Diagnostics utility, reboot the system and press <F10> to re-enter USC or USC-LCE.

When the tests are complete, results of the diagnostics tests are displayed on the screen. To resolve the problems reported in the test results, search the resolutions at support.dell.com.

See Also:

[Hardware Diagnostics](#)

Installing Operating System


Prerequisites

- Optical DVD drive is connected.
- Hard disks must be connected. For PERC controllers, at least one physical disk must be available for virtual disk creation.

Workflow

To install the operating system:

- 1 To launch USC/USC-LCE, boot your system and press the <F10> key within 10 seconds after the Dell logo appears.
- 2 In the left pane, click **OS Deployment**.
- 3 In the right pane, click **Deploy OS** and select one of the following:
 - Go directly to **OS Deployment** and click **Next**.
 - Optional: **Configure RAID First** and click **Next**, if the system has a RAID controller. See [Using Optional RAID Configuration](#) for more information

- 4 For USC — Select the driver source. See [Selecting Operating System Driver Source Location \(for USC only\)](#) for more information.
- 5 Select the operating system from the list, insert the operating system media, and complete the remaining tasks. See [Selecting Operating System](#) for more information.
 **NOTE:** If you select an operating system that supports UEFI boot mode, options–BIOS or UEFI are provided for selecting the boot mode.
- 6 Reboot the system. See [Rebooting System](#) for more information.

See Also:

- [Installing Drivers for RHEL 4.8 Operating System](#)
- [Operating System–Post Installation Scenarios](#)
 - [Assigning a Windows-Bootable System Partition to Drive C](#)
 - [Installing Red Hat Enterprise Linux 4.8 on a System with SAS7 \(H200\) Controller](#)

Selecting Operating System Driver Source Location (for USC only)

For USC, download the operating system drivers from an [Online Repository](#) or a [Local Drive](#) (USB, network share, or DVD).

Online Repository

To download drivers from an online repository:

- 1 Select the **Online Repository**.
- 2 Select the **FTP Repository**.
- 3 Download the drivers using one of the following methods:
 - [Dell FTP Server](#)
 - [Locally Configured Online Repository](#)
 - [Configuring Proxy Server](#)

- 4 To save the drivers locally from the online repository, select **Save Locally**.
- 5 From the **Save Locally** drop-down menu, select the USB drive to save the system drivers.

Make sure to connect a USB device to the USB drive.

- 6 Click **Next**.

See Also:

[Selecting Download Method](#)

Locally Configured Online Repository

To download drivers from a locally-configured online repository, in the **Address** field, enter the server host name or the IP address of the server that has the drivers.

See Also:

- [Configuring a Local FTP Server](#)
- [FTP Authentication](#)

Local Drive

To download the drivers from a USB device or *Dell Lifecycle Controller OS Driver Packs DVD*, select **Local Drive** and click **Next**.



NOTE: 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 not detect the presence of a media. In this case, an error message is displayed stating that no media is available. **For USC-LCE:** Virtual Media is supported through iDRAC. See the *iDRAC User's Guide* for your system's iDRAC device for more information on setting up Virtual Media through iDRAC.

See Also:

[Configuring a Local USB Device](#)

Using Optional RAID Configuration

If the system has a RAID controller, you can configure a virtual disk as the boot device.

Configuring RAID Using Operating System Deployment Wizard

Important

- For USC, the **Raid Configuration** wizard is available only through the **OS Deployment** wizard.
- For USC-LCE, you can configure RAID through the RAID configuration page from the **Hardware Configuration Tab**→**Configuration Wizards**→**RAID Configuration**.



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

To configure RAID using OS Deployment wizard:

- 1** In the left pane of the **Home** page, click **OS Deployment**.
- 2** Select **Configure RAID Now**. This option launches the **RAID Configuration** wizard that displays 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, and USC or USC-LCE returns to the **OS Deployment** wizard.

Bypass RAID configuration:

Select **Go Directly to OS Deployment** and click **Next**. This option launches the **OS Deployment** wizard and the operating system is installed on the default boot device identified in the BIOS utility.

See Also:

- [Selecting Operating System](#)
- [Installing Operating System](#)

Selecting Operating System

You can select an operating system based on its availability and user preference. Take any one of the following action:

- [Selecting an Operating System Available in the List](#)
- [Selecting Custom Operating System](#)
- [Selecting an Operating System Not Available in the List](#)

Selecting an Operating System Available in the List

To install an operating system that is available in the list:

- 1 From the list, select the required operating systems, and click **Next**.
- 2 If a UEFI capable operating system is selected, USC-LCE displays two installation modes — **UEFI** or **BIOS**. Select one of options and click **Next**.
- 3 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.

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



Selecting Custom Operating System

To install a custom operating system:

- 1 From the list, select the required operating system and click **Next**.
The drivers are extracted and USC or USC-LCE prompts you to insert the operating system installation media.
- 2 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.
- 3 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.

Selecting an Operating System Not Available in the List

To install an operating system that is not available in the list:

- 1 Select the option **Any Other Operating System**, and click **Next**.
The drivers are not extracted. Therefore, prepare the drivers for the required operating system.
- 2 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.
- 3 Click **Next** to continue.
 **NOTE:** USC or USC-LCE does not validate the media.

Driver Extraction and Installation

Table 4-3. Driver Extraction and Installation for Different Operating Systems

Operating System	Method of Extraction
Microsoft Windows operating system	The drivers are extracted to an internal USB drive named OEMDRV.
Red Hat Enterprise Linux 4.8	The drivers are extracted to OEMDRV under <code>/oemdrv/*.rpm</code> . Manually install the extracted drivers after the installation is complete.

See Also:

- [Driver Extraction](#)
- [Rebooting System](#)

Installing Drivers for RHEL 4.8 Operating System

To install the drivers:

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

```
mkdir OEMDRV
```

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



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


```
/oemdrv/*.rpm
```

- 2 Use the following command to install the drivers:

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

Rebooting 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](#).

Post Reboot Scenarios

Table 4-4 lists the post reboot scenarios, its user actions, and impact.

Table 4-4. Post Reboot Scenarios and User Actions

Scenario	User Action and Impact
USC or USC-LCE prompts you to press a key before booting to the operating system installation media	Press any key, else the system boots to the hard-disk and not the operating system installation media.
Operating system installation is interrupted and the system reboots before installation is completed.	USC or USC-LCE prompts you to press a key to boot from the operating system installation media.
Want to cancel operating system installation.	Press the <F10> key. NOTE: 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.
Cannot update USC or USC-LCE by running a DUP in the operating system environment for the next 18 hours	USC or USC-LCE does not allow this after the operating system installation.

Operating System—Post Installation Scenarios

Post installation of operating system, complete the following USC or USC-LCE tasks for Microsoft Windows Server 2003 and Red Hat Enterprise Linux 4.8 operating systems:

- [Assigning a Windows-Bootable System Partition to Drive C](#)
- [Installing Red Hat Enterprise Linux 4.8 on a System with SAS7 \(H200\) Controller](#)

Assigning a Windows-Bootable System Partition to Drive C

After completing the Microsoft Windows Server 2003 operating system installation through USC or USC-LCE, the server reboots and begins the text-mode portion of the installation.

To ensure that Microsoft Windows installs on drive C:



NOTE: The Windows Server 2003 setup displays a list of existing drive partitions and unpartitioned space available on the system.

- 1 Create a hard-disk partition: select the unpartitioned space, and press <c>. Follow the on-screen instructions.



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

- 2 Delete the partition: select the newly-created partition, and press <d>. Follow the on-screen instructions.
- 3 Create a primary hard-disk partition: select the unpartitioned space again, and press <c>. Follow the on-screen instructions.

Microsoft Windows installs on drive C.

For more information, see support.microsoft.com/kb/896536.



NOTE: The partition is now enumerated as drive C.

Installing Red Hat Enterprise Linux 4.8 on a System with SAS7 (H200) Controller

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 On the OS Deployment page, select Red Hat Enterprise Linux 4.8.

- 3 After USC reboots to the operating system installer CD/DVD, enter the command: `> linux dd`
- 4 Insert the Driver Update Disk (DUD) when prompted, and specify the location of the USB drive and press **<Enter>**.
- 5 Follow the on-screen instructions to complete the installation.

Controlling Access to the System Control Panel

To control access to the system control panel:

- 1 From the USC/USC-LCE Home page, select **Hardware Configuration**.
- 2 In the right pane, select **Configuration Wizards**
- 3 Click **Physical Security Configuration**.
- 4 Set System Control Panel Access to one of the following options:
 - Disabled
 - View Only
 - View and Modify
- 5 Click **Finish** to apply the changes.

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

System Control Panel Access Options

USC's physical security configuration enables an administrator to restrict system control panel interface access. The options available are:

- **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.

Configuring System Date/Time

To set the date and time for the system:

- 1 From the USC/USC-LCE **Home** page, select **Hardware Configuration**.
- 2 In the right pane, select **Configuration Wizards**.
- 3 Click **System Date/Time Configuration**.
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), as required.
- 5 Click **Finish** to apply the changes.
- 6 To return to the **Configuration Wizards**, click **Back** or click **Cancel** to exit.

Configuring iDRAC

To configure iDRAC parameters applicable to the system, such as LAN, common IP settings, IPv4, IPv6, Virtual Media, and LAN user configuration use the **iDRAC Configuration Wizard**.

To configure and manage iDRAC parameters:

- 1 In the left pane of **Home** page, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards**.
- 3 Click **iDRAC Configuration**, and configure the following parameters.
 - [LAN Configuration](#)
 - [Advanced LAN Configuration](#)
 - [Common IP Configuration](#)
 - [IPv4 Configuration](#)
 - [IPv6 Configuration](#)
 - [Virtual Media Configuration](#)
 - [LAN User Configuration](#)
 - [Summary and Confirmation](#)

LAN Configuration

To view and configure:

- 1 From iDRAC Configuration, select **LAN Configuration**.
- 2 Enter details for iDRAC LAN, IPMI Over LAN, MAC Address, and NIC Selection.

Table 4-5. LAN Configuration Attributes

Attributes	Description	Values
iDRAC LAN	Enabling iDRAC LAN activates the remaining controls. Disabling iDRAC LAN deactivates the controls.	Enable or Disable
IPMI Over LAN	Enables or disables Intelligent Platform Management Interface (IPMI) commands on the iDRAC Local Area Network (LAN) channel.	Enable or Disable
MAC Address	View the Media Access Control (MAC) address that uniquely identifies each node in a network (read-only).	Enable or Disable
NIC Selection	View or edit the NIC mode	Enable or Disable

NIC Mode

The different types of NIC mode for enabling NIC are:

- [Dedicated](#)
- [Shared with failover](#)
- [Shared with failover - LOM 2](#)
- [Shared with failover - All LOMS](#)

Dedicated

This option enables remote access to utilize the dedicated network interface available on the Dell Remote Access Controller (DRAC). The DRAC interface is not shared with the host operating system and routes management traffic to a separate physical network, thus separating it from the application traffic.



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

Shared with failover

This option enables remote access 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

This option enables remote access 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

This option enables remote access 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

To set advanced LAN configuration:

- 1 From **iDRAC Configuration**, select **Advanced LAN Configuration**.
- 2 Set additional attributes for **VLAN**, **VLAN ID**, **VLAN priority**, **Auto Negotiate**, **LAN speed**, and **LAN duplex**.
- 3 Click **OK** to save your settings and return to the **LAN Configuration** menu.

Table 4-6. Advanced LAN Configuration Attributes

Attribute	Description	Values
VLAN	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.	Enable or Disable
VLAN ID	Sets the VLAN ID value. Legal values are defined by IEEE 801.11g specification.	1 to 4094
VLAN Priority	Sets the VLAN ID priority value. Legal values are defined by IEEE 801.11g specification.	0 to 7

Table 4-6. Advanced LAN Configuration Attributes

Attribute	Description	Values
Auto Negotiate	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.	On or Off
LAN Speed	Configures the network speed to match the user's network environment. This option is not available if Auto-Negotiate is set to On.	10 MB or 100MB
LAN Duplex	Configures the duplex mode to match the user's network environment. This option is not available if Auto-Negotiate is set to On.	Full or Half

Common IP Configuration

To set common IP configuration:

- 1** From **iDRAC Configuration**, select **IP Configuration**.
- 2** Register the iDRAC name.
- 3** Set the domain name from DHCP.
- 4** Specify the domain name.
- 5** Specify the host name string.
- 6** Click **OK** to save your settings and return to the **iDRAC Configuration** menu.

The information set during the configuration is erased if iDRAC is reset to the original defaults or if the iDRAC firmware is updated.

Table 4-7. Common IP Configuration Attributes

Attribute	Description	Values
Register iDRAC Name	Register the iDRAC name with the Domain Name System (DNS)	Yes or No
iDRAC Name	View or edit the iDRAC name used for registering the DNS. The name string can contain up to 63 printable ASCII characters. You can edit the name string when Register iDRAC Name is set to No .	Enable or Disable
Domain Name from DHCP	iDRAC acquires the domain name from the Dynamic Host Configuration Protocol (DHCP) server. If set to No , you must enter the domain name manually.	Yes or No
Domain Name	View or edit the iDRAC domain name used if it is not acquired from DHCP. You can specify a domain name when Domain Name from DHCP is set to No .	Enable or Disable
Host Name String	Specify or edit the host name associated with iDRAC. The Host Name string can contain up to 62 ASCII printable characters.	Enable or Disable

IPv4 Configuration

To set IPv4 configuration:

- 1** From **IP Configuration**, select **IPV4**, and enable or disable the protocol.
- 2** Set the RMCP+ encryption key.
- 3** Specify the **IP Address Source**.
- 4** Specify user-configured settings for **Alternate IP Address**.
- 5** Click **Next** to proceed.

Attribute	Description	Values
IPv4	iDRAC NIC IPv4 protocol support. Disabling IPv4 deactivates the controls	Enable or Disable
RMCP+ Encryption Key	RMCP+ encryption key configuring (no blanks allowed). The default setting is all zeros (0)	0 to 40 hexadecimal
IP Address Source	The ability of the iDRAC NIC to acquire an IPv4 address from the DHCP server. Disabling IP Address Source deactivates the Ethernet IP Address , and other user-configured controls.	Enable or Disable

To specify user-configured controls, click **Ethernet IP Address** settings, and enter appropriate values for the following:

- **Ethernet IP Address** — Maximum value of 255.255.255.255
- **Subnet Mask** — Maximum value of 255.255.255.255
- **Default Gateway** — Maximum value of 255.255.255.255
- **Get DNS Servers from DHCP** — Yes/No
 - If set to **Yes**, the iDRAC NIC acquires the 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 (Primary DNS Server)**— Maximum value of 255.255.255.255
- **DNS Server 2 (Secondary DNS Server)**— Maximum value of 255.255.255.255

IPv6 Configuration

To set IPv6 configuration:

- 1 From **IP Configuration**, select **IPv6**, and enable or disable the protocol.
- 2 Specify the **IP Address Source**.
- 3 Specify user-configured settings for alternate Ethernet IP Address.
- 4 Click **Next** to save your settings and proceed.

Attribute	Description	Values
IPv6	iDRAC NIC IPv6 protocol support. Disabling IPv6 deactivates the remaining controls	Enable or Disable
IP Address Source	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.	Enable or Disable

To specify user-configured controls, click **Ethernet IP Address** settings, and enter appropriate values for the following:

- **Ethernet IP Address** — Maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
 - The multi-cast (ff00/8) and loopback (::1/128) values are not valid addresses for the Ethernet IP address and/or the other address related fields described in this section.
 - IPv6 Address forms supported:
 - **X:X:X:X:X:X:X** — In this form, **X** represents the hexadecimal values of the eight 16-bit pieces of the address. You can omit leading zeros in individual fields, but you must include at least one numeral in every field.

- **::** (two colons) — Using this form, you can represent a string of contiguous zero fields in the preferred form. The **::** can only appear once in the address. You can also use this form to represent unspecified addresses (0:0:0:0:0:0:0:0).
- **x:x:x:x:d.d.d.d** — This form is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes. In this form, **x** represents the hexadecimal values of the six high-order 16-bit pieces of the address, and **d** represents the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).
- **Prefix Length** — Maximum value of 128. T
- **Default Gateway** — Maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- **Get DNS Servers from DHCP** — Yes/No
 - If set to **Yes**, the iDRAC NIC acquires the 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 (Primary DNS Server)**— Maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- **DNS Server 2 (Secondary DNS Server)**— Maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Virtual Media Configuration

The Virtual Media is available only if the system includes iDRAC6 Enterprise. Use the Virtual Media Configuration wizard to set control modes for the available Virtual Media devices. 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.

To set the:

- 1 From **iDRAC Configuration**, select **Virtual Media Configuration**.
- 2 Select one of the control modes:
 - Attached
 - Detached
 - Auto-Attached
- 3 Click **Next** to proceed.

Virtual Media Connection Mode

The connection modes available for Virtual Media configuration:

Table 4-8. VM Connection Mode

Mode	Description
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.

LAN User Configuration

Use this to configure LAN user settings such as: account access, account-related attributes, and smart card authentication. To do this:

- 1 From **iDRAC Configuration**, select **LAN User Configuration**.
- 2 Set user settings.
- 3 Click **Next** to proceed.

Table 4-9. LAN User Configuration

Parameter	Description	Value
Auto-Discovery	Auto discovers the provisioning server	Enable or Disable
Provisioning Server Address Criteria	Enter provision server address	IPV4 or IPV6 or Host Name
Account Access	Disabling account access deactivates all other fields on the LAN User Configuration	Enable or Disable
Account Username	Enables the modification of an iDRAC username	maximum of 16 printable ASCII characters
Password	Enables an administrator to specify or edit the iDRAC user's password (Encrypted)	Maximum of 20 characters
Confirm Password	Re-enter the iDRAC user's password to confirm	Maximum of 20 characters
Account Privilege	Assigns the user's maximum privilege on the IPMI LAN channel to the user groups	Admin, Operator, User, or No Access
Smart Card Authentication	Smart Card Authentication for iDRAC log in. If enabled, a Smart Card must be installed to access the iDRAC.	Enable, Disable or Enable with RACADM

Provisioning Server Address Criteria

- 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 Privilege

Table 4-10. Account Privilege

Privileges	Admin	Operator	User	No Access
Login to iDRAC	Yes	Yes	Yes	-
Configure iDRAC	Yes	Yes	-	-
Configure Users	Yes	Yes	-	-
Clear Logs	Yes	-	-	-
Execute Server Control Commands	Yes	Yes	-	-
Access Console Redirection	Yes	Yes	-	-
Access Virtual Media	Yes	Yes	-	-
Test Alerts	Yes	Yes	-	-
Execute Diagnostic Commands	Yes	Yes	-	-

Smart Card Authentication

- **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.

Summary and Confirmation

To view the summary of changes and apply them:

- 1 From **iDRAC Configuration**, select **Summary**.
View the summary of the changes you have made.
- 2 Click **Confirm** to apply the changes, or click **Cancel** to cancel all changes and exit the iDRAC Configuration.
If you apply the changes, a **Please Wait** message appears while your changes are saved. When the operation is complete, a final **Confirmation** screen displays the changes that was applied successfully, left unchanged, or failed.
- 3 Click **Finish** to save your settings and return to the main wizard.

Configuring RAID using Hardware RAID

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

Important

- 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.

Workflow

To launch the **RAID Configuration Wizard**:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards**.
- 3 Click **RAID Configuration** to launch the wizard and do the following tasks:
 - a [Creating a Secure Virtual Disk on Series 7 Controller](#)
 - b [Select RAID Controller](#)

- c [Foreign Configuration Found](#)
- d [Express or Advanced Wizard](#)
- e [Select Basic Settings](#)
- f [Express Wizard Only - Assign a Hot Spare](#)
- g [Express Wizard Only - Review Summary](#)
- h [Advanced Wizard Only - Select Physical Disks](#)
- i [Advanced Wizard Only - Additional Settings](#)
- j [Advanced Wizard Only - Review Summary](#)

View Current Configuration

The **View Current Configuration** page 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.
- Use the **RAID configuration** wizard to delete all the existing virtual disks and create a single and 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.



NOTE: You can create only one virtual disk using USC or USC-LCE. To create multiple virtual disks, use Option ROM. To access Option ROM, press CTRL+R.

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.



NOTE: If you have selected an S100 and S300 RAID controller, the foreign disks are displayed as Non-RAID disks in USC-LCE. You must initialize them to create a virtual disk.

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.

Express or Advanced Wizard

Create a virtual disk using either the **Express Wizard** or the **Advanced Wizard**.

Select the Express 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**.

Select Advanced Wizard

The **Advanced Wizard** enables you to specify which protocol is used when creating the disk pool for the virtual disks. A disk pool is a logical grouping of disks attached to a RAID controller on which one or more virtual disks can be created. In addition to the RAID level, the **Advanced Wizard** allows more flexibility with physical disk selection, span configuration, cache policy, and other virtual disk attributes. Select **Advanced Wizard** to specify all virtual disk settings.



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

Click **Next** after making the 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.
- **Volume** — A single disk drive or segment without any RAID level or redundancy.

If you are using the **Express Wizard**, proceed to [Express Wizard Only - Assign a Hot Spare](#).

If you are using the **Advanced Wizard**, click **Next** and proceed to [Advanced Wizard Only - Select Physical Disks](#).

Minimum Disk Requirement for Different RAID Levels

Table 4-11. RAID Level and Number of Disks

RAID Level	Minimum Number of Disks
0	1
1	2
5	3
6	4
10	4
50	6
60	8

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.

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.


- Specify the size of the virtual disk in the **Size** box
- 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 using Software RAID

Use this feature to configure RAID if a PERC S100 controller on the motherboard or a PERC S300 RAID controller card is present in the system. If the software RAID option is selected, USC-LCE displays the physical disks as Non-RAID disks or RAID-ready disks.

- Non-RAID disk — A single disk without any RAID properties. Needs initialization to apply RAID levels.
- RAID-ready disk — The disk is initialized and a RAID level can be applied.



NOTE: Linux and VMware operating systems cannot be installed using Software RAID controllers (S100 and S300).

Prerequisites

- S100 controller
 - In Option ROM, change the SATA Controller option to RAID Mode.
 - Latest BIOS version must be installed. For more information on the BIOS versions for different systems, see *USC-LCE Readme*.



NOTE: If you have an older BIOS, you can configure RAID only through Option ROM.

- S300 — Latest firmware version for S300 controller must be installed.


Workflow


To set up software RAID, do the following tasks:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards**.

3 Click **RAID Configuration** to launch the wizard and do the following tasks:

- a** [Select RAID Controller.](#)
- b** Select the non-RAID physical disks attached to the controller and click **Next** to initialize them.

 **NOTE:** This step is not available if the controller has no non-RAID disks attached to it.

 **CAUTION:** During initialization, all the data on the non-RAID disks are deleted.

- c** [Select Advanced Wizard](#)
- d** [Select Basic Settings](#)
- e** [Advanced Wizard Only - Select Physical Disks](#)
- f** [Advanced Wizard Only - Additional Settings](#)
- g** [Advanced Wizard Only - Review Summary](#)

Creating a Secure Virtual Disk on Series 7 Controller

 **NOTE:** The controller must be encrypted with a Local Key.

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

- 1** In the left pane, click **Hardware Configuration**.
- 2** Select **RAID Configuration** and click **Next**.
The number of virtual disks present on every controller is displayed, along with information on whether the virtual disk is secure.
- 3** Select the controller and click **Next**.
- 4** Select **Advanced Wizard** and click **Next**.
- 5** Select the required RAID level and click **Next**.
- 6** Select **Self-encryption** from the Encryption Capability drop-down. The self-encryption disks (SEDs) are displayed.
- 7** Select the required physical disks and click **Next**.

- 8 In the **Additional Settings** page, select the **Secure Virtual Disk** box and click **Next**.

The **Summary Page** is displayed with details of the virtual disk attributes.

- 9 Click **Finish**.

- 10 To verify the virtual disk creation, repeat the first two steps.

Configuring vFlash SD Card

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 4-12. 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

To modify advanced settings using the **HII Advanced Configuration**:

- 1 In the left pane, select **Hardware Configuration**.
- 2 In the right pane, click **HII Advanced Configuration**.
- 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.

The *HII Advanced Configuration* wizard has setups for these device types that are supported in : **BIOS**, **NIC**, and **CNA**.

- 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
- Broadcom 57712 (Dual Port) 10GigE

Important

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

Encrypting Unsecure Virtual Disks

Prerequisites

- Selected controller is security-capable
- Security capable virtual disks must be attached to the controller.
- Controller must be in Local Key encryption mode.

Workflow



NOTE: All virtual disks created under the same physical disk are automatically encrypted.

To encrypt the unsecure virtual disks:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards** and click **Key Encryption**.
- 3 Select the controller that is encrypted and click **Next**.



NOTE: The encryption mode (Local Key Encryption) applied to the selected controller does not change.

- 4 Select **Encrypt unsecure virtual disks** and click **Next**.
- 5 To enable encryption, select the unsecure virtual disks and click **Finish**.

Applying the Local Key on the RAID Controller

Prerequisites

- The controller must be security capable.


Workflow

To apply the local key on the RAID controller:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards** and click **Key Encryption**.
- 3 Select the controller to apply a local key and click **Next**.
- 4 Click **Set up local key encryption** and click **Next**.



NOTE: Some controller options are disabled if they do not support encryption.

- 5 Enter the **Encryption Key Identifier** that will be associated with the entered passphrase. The Encryption Key Identifier is a passphrase hint; you must enter the passphrase when USC-LCE prompts with this hint.
- 6 In the **New Passphrase** text box, enter a passphrase.
 **NOTE:** The controller uses the passphrase to encrypt the disk data. A valid passphrase contains 8 to 32 characters. It must include a combination of uppercase and lowercase letters, numbers, symbols, and without spaces.
- 7 In the **Confirm Passphrase** text box, re-enter the passphrase, and click **Finish**.

Rekey Controller with a New Local Key

To rekey the controller with a new local key:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards** and click **Key Encryption**.
- 3 Select the controller to which the local key is applied and click **Next**.
- 4 In the **Existing Passphrase** text box, enter the existing passphrase associated with the displayed Encryption Key Identifier.
- 5 In the **New Encryption Key Identifier** text box, enter the new identifier. The Encryption Key Identifier is a passphrase hint; you must enter the passphrase when USC-LCE prompts with this hint.
- 6 In the **New Passphrase** text box, enter the passphrase that will be associated with the new encryption key identifier

Remove Encryption and Delete Data

To remove the encryption and delete the data on the virtual disks:

- 1 In the left pane, click **Hardware Configuration**.
- 2 In the right pane, click **Configuration Wizards** and click **Key Encryption**.
- 3 Select the controller on which you must remove the key that was applied and click **Next**.

- 4 In the right pane, select **Remove encryption and delete data** and click **Next**.
- 5 Select **Delete encryption key and all secure virtual disks** and click **Finish**.



CAUTION: The existing encryption, virtual disks, and all the data are permanently deleted.

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 iDRAC6 Express Card

To install 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](#) 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 iDRAC6 Express Card

To remove 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.

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

To copy the repository:

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



NOTE: For updating the OS driver packs, use the *Dell Lifecycle Controller OS Driver Packs* 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 Dell Repository Manager to Create the Repository and Copy it to a Local FTP Server

To create and copy the repository:

- 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 through USC and **Platform Update** through USC-LCE.

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 used as a repository must hold at least 8 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**.



NOTE: 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.

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

To copy the repository:

- 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

To create and copy the repository:

- 1 Copy the repository created using the Dell Repository Manager to the root directory of the USB device.
- 2 Use this USB device for Platform Update.



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

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)
- 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. To do this:

- 1 In the left pane, click **Platform Restore**.
- 2 Click **Part Replacement Configuration**.
- 3 Click either **Enabled** or **Disabled** from the **Collect System Inventory on Restart** drop-down.

Part Firmware Update

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.

Back Up Server Profile

Prerequisites

- The server must have a valid service tag (7 characters).
- vFlash SD card must be installed, initialized, and enabled.
- vFlash SD card must have a minimum free space of 384 MB.
- Use only one iDRAC virtual console during backup operation.

Workflow

To back up the server profile:

- 1 In the left pane, select **Platform Restore**.
- 2 In the right pane, select **Backup Server Profile**.
- 3 To generate the backup file without entering the passphrase, click **Finish**.
Alternatively, to generate the encrypted backup file using a passphrase, enter the following details and click **Finish**.
- 4 In the **Backup File Passphrase** field, enter a passphrase. For example, `Rt@#12tv`.



NOTE: A valid passphrase contains 8 to 32 characters. It must include a combination of uppercase and lowercase letters, numbers, symbols, and without spaces. The passphrase is optional and if used for backup, it must be used during restore.

- 5 In the **Confirm Passphrase** field, re-enter the passphrase and click **Finish**.



NOTE: You can check the iDRAC RAC logs for backup server profile status. After the backup profile is completed, check the Lifecycle Logs for all Export entries. To view the log, see [Viewing Lifecycle Log History](#).

See Also

[Backup Server Profile](#)

Exporting Server Profile to a USB Device or Network Share

Prerequisites

- vFlash SD card must have the latest backup image file.
- USB device must have a minimum free space of 384 MB.
- Network share must be accessible and must have a minimum free space of 384 MB.
- Use the same vFlash SD card used during backup.

Workflow

To export the server profile to a USB device or a Network Share:

- 1 In the left pane, select **Platform Restore**.
- 2 In the right pane, select **Export Server Profile**.
- 3 Select either [USB Device](#) or [Network Share](#), enter the details and click **Finish**.

USB Device

- From the **Choose Device** drop-down menu, select the attached USB device.
- In the **File Location** text box, enter the directory or sub-directory path, where the backup image file must be stored on the selected device. By default, the file is stored in the root location of the device if the directory or sub-directory is not provided.

Network Share

CIFS

- Share Name — Network share name. For example, \\xxx. xxx. xxx. xxx or \\DataServer\ServerBkp.
- Domain and User Name — Network share domain and user name. For example, login-name@myDomain. If there is no domain, enter only the user name.
- Password — Network share login password.
- File Location — Sub-directory path. For example, 2010\Aug. By default, the file is stored in the root directory.

NFS

- Share Name — Network share name. For example, \\xxx. xxx. xxx. xxx or \\DataServer\ServerBkp.
- File Location — Sub-directory path. For example, 2010\Aug. By default, the file is stored in the root directory.

See Also

[Export Server Profile](#)

Importing Server Profile from a vFlash SD Card, Network Share, or USB Device

Prerequisites

- The service tag of the server must be same as when the backup was taken.
- If you are restoring from a the Dell vFlash SD card, it must be installed and must contain the backup image in a folder labeled SRVCNF. This image must be from the same platform that you are trying to restore.
- If you are restoring from a network share, make sure that the network share where the backup image file is stored is still accessible.
- Use only one iDRAC virtual console during restore operation.
- A licensed Dell vflash SD card must be installed.

Workflow

To import the server profile from a vFlash SD card, Network Share, or a USB device:

vFlash SD Card

- 1 In the left pane, select **Platform Restore**.
- 2 In the right pane, select **Import Server Profile**.
- 3 Select vFlash Secure Digital (SD) Card and click **Next**.
- 4 Select either **Preserve configuration** or **Delete Configuration**.
 - Preserve configuration — Preserves the RAID level, virtual disk and controller attributes.
 - Delete configuration — Deletes the RAID level, virtual disk and controller attributes.
- 5 If you have secured the backup image file with a passphrase, in the **Backup File Passphrase** text box, enter the passphrase entered during backup and click **Finish**.

Network Share

- 1 In the left pane, select **Platform Restore**.
- 2 In the right pane, select **Import Server Profile**.
- 3 Select Network Share and click **Next**.
- 4 Select **CIFS** or **NFS**, enter the details and click **Next**.
- 5 Select either **Preserve configuration** or **Delete Configuration**.
 - Preserve configuration — Preserves the RAID level, virtual disk and controller attributes.
 - Delete configuration — Deletes the RAID level, virtual disk and controller attributes.
- 6 If you have secured the backup image file with a passphrase, in the **Backup File Passphrase** text box, enter the passphrase entered during backup and click **Finish**.

USB Device

- 1 From the left pane, select **Platform Restore**.
- 2 From the right pane, select **Import Server Profile**.
- 3 Select **USB Device** and click **Next**.
- 4 From the **Choose Device** drop-down menu, select the attached USB device.
- 5 In the **File Location** text box, enter the directory or sub-directory path, where the backup image file must be stored on the selected device. By default, the file is stored in the root location of the device.
- 6 Select either **Preserve configuration** or **Delete Configuration**.
 - **Preserve configuration** — Preserves the RAID level, virtual disk and controller attributes.
 - **Delete configuration** — Deletes the RAID level, virtual disk and controller attributes.
- 7 If you have secured the backup image file with a passphrase, in the **Backup File Passphrase** text box, enter the passphrase entered during backup and click **Finish**.

Post-import Scenario

- 1 System powers off if turned on. If the system boots into an operating system, it attempts to perform a graceful shutdown. If unable to, it will perform a forced shutdown after 15 minutes.
- 2 System powers on and boot into System Services to execute tasks to perform firmware restore for supported devices (BIOS, Storage Controllers and Add-in NIC cards).
- 3 System reboots and goes into System Services to execute tasks for firmware validation, configuration restore for supported devices (BIOS, Storage Controllers and Add-in NIC cards) and the final verification of all tasks executed.

- 4 System powers off and perform iDRAC configuration and firmware restore. After completion, iDRAC resets and takes up to 10 minutes before the system powers on.
- 5 System powers on and restore process is complete. Check the Lifecycle logs for the restore process entries.

See Also

[Import Server Profile](#)

Importing Server Profile after Motherboard Replacement

Prerequisites

- A backup of the server with the old motherboard.
- If you are restoring from a the Dell vFlash SD card, it must be installed and must contain the backup image in a folder labeled SRVCNF. This image must be from the same platform that you are trying to restore.
- If you are restoring from a network share, make sure that the network share where the backup image file is stored is still accessible.

Workflow

After replacing the motherboard, follow the steps under [vFlash SD Card](#), [Network Share](#), or [USB Device](#) to restore the system information.

Post-requisites

- See [Post-import Scenario](#)
- The Service tag is restored from the backup file on the new motherboard.

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 In the left pane, click **Lifecycle Log**.
- 2 In the right pane, click **View Lifecycle Log History**.

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**. See [Lifecycle Log Schema](#) for more information on the schema.

Prerequisites

- If you use a network share, set the correct Network Settings. See [Using USC Settings Wizard](#) 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.

Workflow

To export the Lifecycle Log:

- 1** In the left pane, click **Lifecycle Log**.
- 2** In the right pane, click **Export Lifecycle Log**.
- 3** Select either **USB Device** or **Network Share**.

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, **login-name@myDomain**, 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 Work Note 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 50 characters in the **Lifecycle Log** field.

To add comments:

- 1 In the left pane, click **Lifecycle Log**.
- 2 In the right pane, click **Add a work note to Lifecycle Log**.
In the **Add a work note to Lifecycle Log** field, enter the comments and click **OK**.

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, IP address configuration settings, and encryption certificates. It also deletes all the Lifecycle Controller content such as lifecycle logs that contain the history of all the change events, firmware upgrades and rollback, user comments, and current and factory shipped hardware and firmware inventory. 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 A message is displayed, click **Yes** to continue or **No** to cancel the operation.

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

This section provides a list of error messages and the resolutions for each message. Table 5-1 lists the messages specifically to USC and USC-LCE. Table 5-2 lists messages specific to USC and Table 5-3 lists messages specific to USC-LCE.

Table 5-1. USC and USC-LCE Error Messages and Resolutions

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

Table 5-1. USC and USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
The inserted OS media is invalid	The operating system media is damaged or corrupted, or the optical device used to read the media is not functioning correctly.
The updates you are trying to apply are not Dell-authorized updates	USC or USC-LCE has detected that one or more of the DUPs used to update your system are not Dell authorized. If you are using a local USB device for your update repository and this problem persists, create it again using DUPs from the <i>Dell Server Updates</i> DVD (see Configuring a Local USB Device) or provide an alternate repository.
Fatal error launching USC has occurred. The system will reboot.	A fatal error occurred when launching USC or USC-LCE. The system will automatically reboot and attempt to enter USC or USC-LCE again. If the problem persists after rebooting, see Repairing USC or Repairing USC-LCE .
Network is not configured. Do you want to configure now?	Network settings must be configured for USC or USC-LCE to work correctly. See Operating System Deployment 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: <ol style="list-style-type: none">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 Download Method for more information.
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.
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.
Enter a valid Subnet Mask	Enter a valid Subnet Mask that is between 0.0.0.0 and 255.255.255.255.

Table 5-1. USC and USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
Enter a valid Default Gateway Address	Enter a valid default gateway address that is between 0.0.0.0 and 255.255.255.255.
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.
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.
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.
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.
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 5-2. USC Error Messages and Resolutions

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

Table 5-3. 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 Platform).
Unable to find a device capable of reading the OS install media	<p>USC-LCE cannot detect a device to read the operating system media. One of the following situations is probably causing the error:</p> <ul style="list-style-type: none">• No optical device is available on the system. Shut down the system and add a SATA optical device or USB optical device.• If an optical device is present, it may not be properly connected. Check to ensure the device cables are adequately seated.• If an optical device is present, it is disabled in the BIOS. Reboot the system, enter the BIOS setup utility, and enable the SATA ports for the optical device.• iDRAC virtual media is disabled. See the <i>Integrated Dell Remote Access Controller 6 (iDRAC6) User's Guide</i> for your system available at support.dell.com/manuals.
The repository you selected as a source for the updates has failed an integrity check	This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see Configuring a Local USB Device) or provide an alternate repository.
Decompression of the catalog file failed	The catalog downloaded to compare currently installed versions with the latest available versions cannot be decompressed. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see Configuring a Local USB Device) or provide an alternate repository.

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

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

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
Please enter the IPv6 Default Gateway address	Enter the IPv6 default gateway address. See IPv6 Configuration .
Please enter a valid IPv6 DNS Server 1 Address	Enter a valid IPv6 DNS Server1 address. See IPv6 Configuration .
Please enter a valid IPv6 DNS Server 2 Address	Enter a valid IPv6 DNS Server2 address. See IPv6 Configuration .
Please enter a valid iDRAC Name of up to 63 characters	Enter a valid iDRAC name that is less than or equal to 63 characters.
Please enter a valid Domain Name of up to 64 characters	Enter a valid domain name that is less than or equal to 64 characters.
Please enter a valid Host Name of up to 62 characters	Enter a valid host name that is less than or equal to 62 characters.
Please enter a value in the range of 1 to 4094	Enter a VLAN ID between 1 and 4094. See Advanced LAN Configuration .
Please enter a value in the range of 0 to 7	Enter a VLAN ID priority value between 0 and 7. See Advanced LAN Configuration .
iDRAC communication failure. Please power down, unplug the system, wait 5 seconds, apply power and power on	Communication with iDRAC has failed. To resolve this issue: <ol style="list-style-type: none">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: <ol style="list-style-type: none">1 Turn off the system, and then unplug it.2 Wait 5 seconds.3 Plug the system back in, and then turn it on.
RAID configuration failed	USC-LCE failed when creating the RAID configuration. To resolve this issue: <ol style="list-style-type: none">1 Reboot the system.2 Re-enter USC-LCE by pressing the <F10> key.3 Try again to create the RAID configuration.

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

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

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
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.
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.

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
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 exists, 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.
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.
The backup operation that was initiated from USC completed with errors. For more information, refer to the RAC log.	The RAC log contains the names of the components that failed during backup. Verify the firmware information and retry.
Initiating backup failed. Retry after few minutes.	Perform A/C power cycle and retry.
Copying backup file to the SRVCNF partition on the vFlash SD card failed.	Make sure that the vFlash SD card is installed, initialised, and enabled.

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
The restore operation which was initiated from USC completed with errors. For more information, refer RAC log.	The RAC log contains the names of the components that failed during restore. Verify the firmware information and retry.
Initiating restore failed. Retry restore operation after sometime.	Perform A/C power cycle and retry.
An error occurred. Could not validate the image on vFlash SD card.	Use a valid backup image and retry.
This operation cannot be completed. Licensed SD Card is not present in the system.	Install the licensed vFlash SD card and retry the operation.
There is not enough space on vFlash to perform this operation. It needs at least 384 MB of available space.	Delete the existing partitions and unwanted files, so that 384 MB of free space is available.
This operation cannot be completed because the SD Card is not present. Insert the SD card and retry.	Install the licensed vFlash SD card and retry the operation.
This operation cannot be completed because one or more partitions are locked. Unlock the partition and retry.	Use the iDRAC vFlash SD card wizard to unlock the partitions, and retry the operation.
This operation cannot be completed because one or more partitions are in use. Retry after waiting a few minutes.	Complete the other operations that are using the partitions, and retry the operation.

Table 5-3. USC-LCE Error Messages and Resolutions (continued)

Error Message	Resolution
This operation cannot be completed because the SD Card is not present. Insert the SD card and retry.	Install and enable the licensed vFlash SD card and retry the operation.
The backup operation that was initiated from USC could not be completed. Check iDRAC RAC logs for more information.	The RAC log contains the names of the components that failed during backup. Verify the firmware information and retry.
Rekey failed. Retry.	Make sure that the latest version of the storage controller firmware is installed.
Failed to encrypt unsecure virtual disks.	Make sure that the latest version of the storage controller firmware is installed.

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 Platform](#) for more information. When updates are complete, your system automatically reboots.
- 8 While the system reboots, press the <F10> key again to enter USC - LCE.

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

 **NOTE:** Updates that are required for a complete system recovery are pre-selected by USC-LCE. 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 Platform](#) 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](#) 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](#) for more information.

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

14 Does USC or USC-LCE support configuration of all RAID levels and all RAID cards for *pxl* 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](#) 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 Platform](#) 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](#) 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](#) or [Repairing USC-LCE](#). 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.

Lifecycle Log Schema

This section displays a typical 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:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

```

        <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>

```

B

Easy-to-use System Component Names

Table B-1 lists the Fully Qualified Device Descriptor (FQDD) of the system components and the equivalent easy-to-use names.

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

FQDD of System Component Name	Easy-to-use Name
RAID.Integrated.1	Integrated RAID Controller 1
RAID.Slot.1-1	RAID Controller in Slot 1
NIC.Mezzanine.1B-1	
NIC.Mezzanine.1C-1	NIC in Mezzanine
NIC.Mezzanine.1C-2	
NIC.Mezzanine.3C-2	
NonRAID.Integrated.1-1	Integrated Storage Controller 1
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 B-1. Easy-to-use Names of System Components (continued)

FQDD of 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.SATAEmbedded.A-1	Disk on Embedded SATA Port A
Optical.SATAEmbedded.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
System.Chassis.1	Blade Chassis
LCD.Chassis.1	LCD

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

FQDD of 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

B

Backup Server Profile
about, 32
how to, 94

BIOS

configuring with HII, 83
rolling back, 27, 45

BitLocker, 47

D

DUP, 20, 116

E

error messages, 105

Export Server Profile
about, 33
how to, 95

F

FAQs, 118

firmware
adding custom, 119
interrupting install, 44
rolling back, 27, 45

FTP

configuring a local server for
updates, 89, 91

H

hardware

advanced configuration, 82
configuration wizards, 28
configuring, 28

hardware diagnostics

updating the utility, 47

HII, 83

I

iDRAC

configuring, 58
Enterprise, 67, 118

Import Server Profile

about, 34
how to, 96

Motherboard Replacement, 99

L

LAN

advanced configuration, 61

Lifecycle Log

adding comments, 103

- exporting lifecycle log, 101
- viewing history, 100

Linux

- RHEL 4.8 drivers, 54

Local Key Encryption

- about, 36
- applying the local key, 85
- encrypt unsecure disks, 84
- rekey, 86
- remove local key, 86

N

Network

- hardware inventory, 38
- lifecycle log, 101
- platform update, 43

O

operating system

- adding custom drivers, 118
- any other operating system, 53
- custom OS, 53
- deploying, 30, 49
- launching the wizard, 48
- using virtual media for installation, 119

P

part replacement

- configuration, 92

R

RAID

- configuration wizard, 51
- configuring, 70
- Hardware RAID, 70
- Software RAID, 79

S

- system crashes, 120

- system date/time, 58

system services

- canceling request to enter, 21
- disabled, 20
- not available, 20

systems services

- update required, 20

T

- TPM, 47

- troubleshooting, 105

U

- UEFI, 83, 119

USC

- deleting, 119
- disabling, 21
- repair package, 116
- storing update files, 118
- updating, 21

V

vFlash, 118

vFlash SD card configuration, 81

virtual disk

 configuring as a boot device, 51

virtual media

 using for operating system
 installation, 119

W

Windows

 drivers, 31

 installing to C drive, 56

