Dell Lifecycle Controller 2
Version 1.00.00 User's Guide

Notes, Cautions, and Warnings

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.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

© 2012 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, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

Other trademarks and trade names may be used in this publication 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.

2012 - 03

Rev. A00

Contents

1

Introduction

The Dell Lifecycle Controller provides advanced embedded systems management to perform systems management tasks such as deploy, configure, update, maintain, and diagnose through a graphical user interface. It is delivered as part of iDRAC7 out-of-band solution and embedded Unified Extensible Firmware Interface (UEFI) applications in the latest Dell servers. The iDRAC7 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:

- GUI-based Lifecycle Controller:
  - Is an embedded configuration utility that reside on an embedded flash memory card.
  - Is 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.
- Remote Services (WS-Management) simplifies end-to-end server lifecycle management using the one-to-many method. It interfaces for remote deployment integrated with Dell OpenManage Essentials and partner consoles. For more information, see *Dell Lifecycle Controller Remote Services User's Guide*.

Benefits of Using iDRAC7 with Lifecycle Controller

The benefits include:

- Increased Availability — Early notification of potential or actual failures that help prevent a server failure or reduce recovery time after failure.
- Improved Productivity and Lower Total Cost of Ownership (TCO) — Extending the reach of administrators to larger numbers of distant servers can make IT staff more productive while driving down operational costs such as travel.
- Secure Environment — By providing secure access to remote servers, administrators can perform critical management functions while maintaining server and network security.
- Enhanced Embedded Management through Lifecycle Controller – Lifecycle Controller provides deployment and simplified serviceability through Lifecycle Controller GUI for local deployment and Remote Services (WS-Management) interfaces for remote deployment integrated with Dell OpenManage Essentials and partner consoles.

  For more information on iDRAC7, see *Integrated Dell Remote Access Controller User's Guide* available at **support.dell.com/manuals**.

Key Features

The key features in Lifecycle Controller include:

- Easy-to-use GUI with logical grouping of features.

- Custom branding — Rebranding the interface with the customer-centric branding information.
- Provide service tag of the system
- 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
  - Network share
- Patching or Updates — Operating system agnostic and reduced maintenance downtime with direct access to updates from **ftp.dell.com**. It simplifies firmware updates by maintaining a working version for rollback.
- Servicing — 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 — Supports local key encryption.
- Restoring Platform — Backup the server profile (including RAID configuration) and restore the server to a previously known state.

Why Use Lifecycle Controller

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 Lifecycle Controller, an administrator had to use many tools such as Dell OpenManage Server Administrator (DSA), Dell Systems Build Update Utility (SBUU), and Dell Deployment Toolkit (DTK) shipped on multiple CDs or DVD. Maintaining and using the multiple disks in their many versions was time consuming for the administrator.

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

Licensable Features in Lifecycle Controller

Lifecycle Controller features are available based on the type of license (Basic Management, iDRAC7 Express, iDRAC7 Express for Blades, or iDRAC7 Enterprise) you purchase. Only licensed features are available in the Lifecycle Controller Web interface. For more information on managing licenses, see *iDRAC7 User's Guide*. The following table provides the Lifecycle Controller features available based on the license purchased.

Feature	Base Management with IPMI	iDRAC7 Express	iDRAC7 Express for Blades	iDRAC7 Enterprise
Firmware Update	Yes	Yes	Yes	Yes
Operating System Deployment	Yes	Yes	Yes	Yes
Device Configuration	Yes	Yes	Yes	Yes
Diagnostics	Yes	Yes	Yes	Yes
Server Profile Export and Import	-	-	-	Yes
Part Replacement	-	-	-	Yes
Local Updates	Yes	Yes	Yes	Yes
Driver Packs	Yes	Yes	Yes	Yes
Remote Services (through WS-MAN)	-	Yes	Yes	Yes

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 *Lifecycle Controller Online Help* provides detailed information about the fields available on the GUI and the descriptions for the same.
- The *Lifecycle Controller Readme* is available from within the product. A Web version is also provided to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- The *Dell Lifecycle Controller Remote Services User's Guide* provide information on using Remote Services.
- The *Systems Management Overview Guide* provides brief information about the various software available to perform systems management tasks.
- The *iDRAC7 Overview and Feature Guide* provides information about iDRAC7, its licensable features, and license upgrade options.
- The *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* provides information about configuring and using an iDRAC7 for rack, tower, and blade 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 *Lifecycle Controller 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 H710, H710P, and H810 Technical Guidebook* for specification and configuration related information about the PERC H710, H710P, and H810 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.

The following system documents are available to provide more information:

- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at dell.com/regulatory_compliance. Warranty information may be included within this document or as a separate document.
- The *Rack Installation Instructions* included with your rack solution describe how to install your system into a rack.
- The *Getting Started Guide* provides an overview of system features, setting up your system, and technical specifications.
- The *Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.
- *Lifecycle Controller Web Services Interface Guide–Windows and Linux*

Contacting Dell

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

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

1. Visit **support.dell.com**.
2. Select your support category.
3. If you are not a U.S. customer, select your country code at the bottom of the **support.dell.com** page, or select **All** to see more choices.
4. Select the appropriate service or support link based on your need.

2

Using Lifecycle Controller

This section provides information about launching Lifecycle Controller, enabling or disabling it, and launching it for the first time. Before using Lifecycle Controller, make sure that the network and iDRAC7 are configured. For more information, see *iDRAC7 User's Guide*.

Launching Lifecycle Controller

To launch Lifecycle Controller during the system boot, press **<F10>** key within 10 seconds after the manufacturer or service provider's logo is displayed. When Lifecycle Controller is launched for the first time, it displays **LC Settings** wizard that allows you to configure the preferred language and network settings.

NOTE: If the system does not enter Lifecycle Controller, see Launch Messages Causes and Resolutions.

Related Links

Using LC Settings

Launch Messages Causes and Resolutions

The table lists the messages that appear during system launch, and their cause and resolution.

Message	Cause	Resolution
Lifecycle Controller disabled	• The system is turned on or restarted while iDRAC is initializing. This occurs if: – 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.	Wait for a minute after resetting iDRAC to restart the system, so that iDRAC initializes.
Lifecycle Controller Update Required	The embedded device that stores the product may contain corrupted data.	Update the product using Lifecycle Controller Dell Update Package (DUP). See the *Dell Update Packages User's Guide* at **support.dell.com/manuals** for more information. If an operating system is not installed on the system or if running the DUP does not fix the problem, run the Lifecycle Controller repair package.

Message	Cause	Resolution
Lifecycle Controller not available	Another process is currently using iDRAC.	Wait for 30 minutes for the current process to complete, reboot the system, and retry.
Lifecycle Controller in Recovery Mode (3-strike policy)	Ungracefully exit Lifecycle Controller for 3 consecutive times.	Update Lifecycle Controller using Lifecycle Controller repair package through iDRAC or run the repair package DUP through the operating system.

Related Links

Disabling Lifecycle Controller
Repairing Lifecycle Controller

Enabling Lifecycle Controller

To boot into Lifecycle Controller during startup:

1. Press **<F2>** within five seconds after system start-up.
   The **System Setup Main Menu** is displayed.
2. Click **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Click **Lifecycle Controller**.
4. Select **Enabled**.
5. Go back to the **System Setup Main Menu** page and click **Finish** to save the settings.
   The system reboots automatically.

Disabling Lifecycle Controller

To prevent the system from entering Lifecycle Controller during startup:

1. Press **<F2>** within five seconds after system start-up.
   The **System Setup Main Menu** is displayed.
2. Click **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Click **Lifecycle Controller**.
4. Under **Lifecycle Controller**, select **Disabled**.
5. Go back to the **System Setup Main Menu** page and click **Finish** to save the settings.
   The system reboots automatically.

Canceling Lifecycle Controller

If Lifecycle Controller causes the system to reboot twice, cancel the Lifecycle Controller actions. However, if Lifecycle Controller causes the system to reboot the third time, the message `LC Update required` is displayed and you must use Lifecycle Controller repair package to recover Lifecycle Controller.

CAUTION: This action cancels all tasks Lifecycle Controller is in the process of executing. It is strongly recommended that you cancel the Lifecycle Controller actions only when absolutely necessary.

1. Press **<F2>** within five seconds after system start-up.
   The **System Setup Main Menu** is displayed.
2. In the **System Setup Main Menu** page, click **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Click **Lifecycle Controller**.
4. Under **Cancel Lifecycle Controller Actions**, select **Yes**.
5. Go back to the **System Setup Main Menu** page and click **Finish** to save the settings.
   The system reboots automatically.

Using Lifecycle Controller for the First Time

When using Lifecycle Controller for the first time, it is recommended that you run the following wizards:

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

Related Links

Using LC Settings
Updating Platform

Using LC Settings

Use LC Settings wizard to specify the language, keyboard layout, and network settings for Lifecycle Controller only. This does not change the system or other application settings.

Specifying Language and Keyboard Type

1. In the left pane, click **LC Settings**.
2. In the right pane, click **Language and Keyboard**. Use the up-arrow and down-arrow keys to select the options.
   - From the **Language** drop-down menu, select the language.
   - 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 **LC Settings**.
2. In the right pane, click **Network Settings**.
3. From the **NIC Card** drop-down menu, select the NIC card to configure.
4. From 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 these IP address properties: **IP Address**, **Subnet Mask**, **Default Gateway**, **DNS Address**. If you do not have this information, contact the network administrator.
5. Click **Finish** to save the settings.

NOTE: If Lifecycle Controller Settings are not configured correctly, an error message is displayed.

Accessing Help

Each Lifecycle Controller screen has a **help** associated with it. Click **Help** (in the upper-right corner) to display help for the current screen.

Viewing Readme

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

3 Lifecycle Controller Features

This section provides a brief description of the Lifecycle Controller features and helps you familiarize with the wizards to use Lifecycle Controller most effectively. Each feature is a wizard in Lifecycle Controller. Lifecycle Controller supports the following features:

- **Home —** Navigate back to Home screen.
- **Lifecycle Log** — View and export lifecycle log, and add a work note to lifecycle log.
- **Platform Update** — Apply updates or perform platform rollback for the system.
- **Hardware Configuration** — Configure system devices.
- **OS Deployment** — Install an operating system.
- **Platform Restore** — Backup, export, and restore system profile.
- **Hardware Diagnostics** — Perform diagnostics to validate the memory, I/O devices, CPU, physical disks, and other peripherals.
- **LC Settings** — Specify the language, keyboard layout, and network settings while using Lifecycle Controller.
- **System Setup** — View the version information of Lifecycle Controller and UEFI.

Related Links

Lifecycle Log
Platform Update
Platform Rollback
Hardware Configuration
Operating System Deployment
Platform Restore
Hardware Diagnostics
Using LC Settings
System Setup

Lifecycle Log

Lifecycle Controller provides the history of firmware changes of the related components installed on a managed system. Using this wizard, you can view and export lifecycle log, and add a work note to a log history. The log contains the following:

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

Related Links

Viewing Lifecycle Log History
Exporting Lifecycle Log
Adding Work Note to Lifecycle Log

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 for the following components:
  - LC
  - Diagnostics
  - Operating System Driver Pack
  - BIOS
  - NIC
  - iDRAC
  - PSU
  - RAID Controller

Related Links

Download Methods
Updating Platform

Download Methods

Access one of the following locations or media to perform the updates:

- FTP server (Non-proxy and proxy)
- Local Drives — USB flash drive, *Dell Server Updates* DVD, and the *Dell Lifecycle Controller OS Driver Packs* DVD.
- Network share (CIFS or NFS)

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

Version Compatibility

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

Platform Rollback

Lifecycle Controller enables you to roll back the component 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, Lifecycle Controller, and operating system driver pack installation to earlier versions.

The previous version of a component is available if the firmware is updated at least once for that component either using Lifecycle Controller or Dell Update Package.

Related Links

Rolling Back to Previous Firmware Versions

Hardware Configuration

Lifecycle Controller provides different wizards to configure the various system components, and they are:

- Configuration Wizards
- Hardware Inventory
- Delete Configuration and Reset Defaults

Configuration Wizards

Use the configuration wizards to configure system devices. The Configuration Wizards has:

- **System Configuration Wizards** — This includes **Front Panel Security**, **iDRAC Configuration**, **System Date/Time Configuration**, and **vFlash SD card Configuration**.
- **Storage Configuration Wizards** — This includes **RAID Configuration**, **Key Encryption**, and **Break Mirror**.

Related Links

Controlling Access to Front Panel
Configuring iDRAC
Configuring System Time And Date
Configuring vFlash SD Card
Configuring RAID Using Hardware RAID
Configuring RAID Using Software RAID
Creating a Secure Virtual Disk on Series 7 Controller
Applying the Local Key On RAID Controller
Breaking Mirrored Disk

Hardware Inventory View and Export

Lifecycle Controller provides the following wizards to manage the system inventory:

- View Current Inventory
- Export Current Inventory
- View Factory Shipped Inventory
- Export Factory Shipped Inventory
- Collect System Inventory on Restart

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. You can export this information in an XML format into a USB flash drive 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 Easy-to-use System Component Names.

NOTE: Incorrect inventory data is displayed or exported after performing **Delete Configuration and Reset Defaults**. See Viewing and Exporting Current Inventory After Resetting Lifecycle Controller for displaying correct inventory data.

Related Links

Viewing Hardware Inventory-Current or Factory Shipped
Exporting Hardware Inventory-Current or Factory Shipped
Viewing or Exporting Hardware Inventory After Part Replacement

About View and Export Factory Shipped Inventory

You can view the hardware information for the factory installed hardware components and their configuration. You can export this information in an XML format to a USB flash drive, network share, or both the locations.

For more information on the easy-to-use names of the hardware components, see Easy-to-use System Component Names.

NOTE: View and export factory shipped inventory feature is grayed-out if Delete Configuration and Reset Defaults was applied that permanently deletes the factory shipped inventory.

Related Links

Viewing Hardware Inventory-Current or Factory Shipped
Exporting Hardware Inventory-Current or Factory Shipped

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.

Related Links

Updating Server Inventory Information

Delete Configuration and Reset Defaults

You can delete the current iDRAC settings and reset iDRAC to factory defaults. It also deletes lifecycle logs, factory shipped inventory information, and licenses on the managed node.

Related Links

Deleting Configuration and Resetting Defaults

Operating System Deployment

Using the operating system deployment wizard, you can deploy various custom and standard operating systems on the managed system including configuring RAID during installation.

Related Links

Installing Operating System
Updating Platform

Driver Access

Lifecycle Controller 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 temporary directory on the managed system. 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 Lifecycle Controller after rebooting.

NOTE: Although, Lifecycle Controller has embedded drivers that are factory installed, there are latest drivers available. Before installing the operating system, run the **Platform Update** wizard to make sure that the latest drivers are available.

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.

The table lists the Lifecycle Controller operations that are performed based on the availability of the RAID controller and the option selected.

RAID Controller Availability	Operations
• 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.
System has a RAID controller and you selected the optional RAID configuration	Configure a virtual disk and select it as the boot device.

Platform Restore

Lifecycle Controller provides wizards to backup, export, and restore system configuration, and manage firmware on the replaced parts.

NOTE: The feature is licensed. Acquire the license to enable the feature. For more information on acquiring and using the licenses, see *iDRAC7 User's Guide*.

Backup Server Profile

Use this licensed 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, NDCs, Lifecycle Controller 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.

Related Links

Back Up Server Profile

Export Server Profile

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

Related Links

Exporting Server Profile to USB Flash Drive or Network Share
USB Device
Network Share

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 located on a vFlash SD card, network share, or USB device.

You can cancel a restore job using iDRAC Settings utility by pressing F2 during POST and click **Yes** under **Cancel Lifecycle Controller Actions**, or reset iDRAC7. This initiates the recovery process and restores the system to a previously known state. Recovery process may take more than five minutes depending on the system configuration. To check if the recovery process is complete, view the Lifecycle logs in iDRAC Web interface.

Related Links

Importing Server Profile from a vFlash SD Card Network Share or USB Flash Drive
Importing Server Profile After Motherboard Replacement
vFlash SD Card
Network Share
USB Device

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. The update occurs automatically when you reboot your system after replacing the part. It is activated through a license, and can be disabled remotely using Lifecycle Controller-Remote Services, or through the Lifecycle Controller.

NOTE: The feature is licensed. Acquire the license to enable the feature. For more information on acquiring and using the licenses, see *iDRAC7 User's Guide*.

Related Links

Configuring Replaced Parts

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
- PERC, SAS, and CERC series 6 and 7
- Power Supply Units

Hardware Diagnostics

It is recommended that you run diagnostics using the **Hardware Diagnostics utility**, as part of a regular maintenance plan to validate whether the system and the attached hardware are functioning properly. Since the diagnostics utility has a physical (as opposed to logical) view of the attached hardware, it can 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.

Related Links

Performing Hardware Diagnostics

System Setup

Advanced Hardware Configuration

Lifecycle Controller **Advanced Hardware Configuration** wizards allow you to configure BIOS, iDRAC, and certain devices such as NIC, and RAID controllers 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 may have different pre-boot configuration utilities. The utilities also provide localized versions of devices such as the BIOS setup.

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

The **Advanced Hardware 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

NOTE: 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**, and then select **Integrated Devices**. In the list for 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.

Related Links

Modifying Device Settings

Lifecycle Controller Repair

During Power-On Self-Test (POST), if the system displays the message `Lifecycle Controller update required`, the embedded device that stores Lifecycle Controller may contain corrupt data. To resolve this issue, see the Repairing Lifecycle Controller.

About RAID Configuration

Lifecycle Controller supports both software RAID and hardware RAID options.

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

Related Links

Configuring RAID Using Hardware RAID
Configuring RAID Using Software RAID
Creating a Secure Virtual Disk on Series 7 Controller
Applying the Local Key On RAID Controller
Breaking Mirrored Disk

Key Encryption

Use this feature to:

- Set the encryption for PERC H710, H710P, and H810 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.
- Encrypt the existing unsecure virtual disks. To do this, enable the encryption on the controller.

Related Links

Applying the Local Key On RAID 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 H710, H710P, and H810 controllers, see the *PERC H710, H710P, and H810 Technical Guidebooks*.

- 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.

Related Links

Encrypting Unsecure Virtual Disks
Rekey Controller With New Local Key

4

Lifecycle Controller Operations

This section provides the tasks required to perform different operations on the Lifecycle Controller.

Viewing Hardware Inventory-Current or Factory Shipped

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

NOTE: For factory shipped inventory, the state of few parameters for the installed components displays **Unknown**.

1. **In t**he left pan**e**, click **Hardware Configuration**.
2. In the right pane, click **Hardware Inventory**.
3. Click **View Current Inventory** or **View Factory Shipped Inventory** to view the current or factory shipped inventory.

NOTE: Lifecycle Controller does not provide the driver version for the RAID controller. To view the driver version, use iDRAC7, OpenManage Server Administrator Storage Service, or any other third party storage management application.

Related Links

About View and Export Current Inventory
About View and Export Factory Shipped Inventory

Viewing or Exporting Hardware Inventory After Part Replacement

To view or export the hardware inventory after part replacement:

1. Launch Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Hardware Inventory**.
4. Click **View Current Inventory**.
   Lifecycle Controller displays the old hardware inventory.
5. Reboot the server and relaunch Lifecycle Controller.
6. Access **Hardware Inventory** and click **View Current Inventory** to view the latest inventory or click **Export Current Inventory** to export the latest inventory to an external location.

Related Links

About View and Export Current Inventory

Exporting Hardware Inventory-Current or Factory Shipped

Before exporting the currently installed or factory installed hardware components and their configuration, make sure the following prerequisites are met:

- If you use the network share (shared folder), configure the **Network Settings**. See Using LC Settings for more information.

- If you are storing the exported file in a USB flash drive, make sure that a USB flash drive is connected to the managed system.

To export the current or factory shipped hardware inventory:

NOTE: For factory shipped inventory, the state of few parameters for the installed components displays **Unknown**.

1. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Hardware Inventory**.
3. Click **Export Current Inventory** or **Export Factory Shipped Hardware Inventory**.
4. Select **USB Device** if you are exporting the inventory log to a local USB flash drive or **Network Share** if you are exporting the file to a shared folder on a network.
5. Click **Test Network Connection** to verify if Lifecycle Controller is able to connect to the IP address that you provided. By default, it pings the Gateway IP, DNS server IP, and host IP.

NOTE: Lifecycle Controller cannot ping to the domain name and does not display its IP address if the DNS is not able to resolve the domain name. Make sure that the issue with DNS is resolved and then retry.

6. Click **Finish** to export the inventory.

   The **HardwareInventory _<servicetag>_<timestamp>.xml** or **FactoryShippedHWInventory_<servicetag>.xml** is copied to the specified location. For the current inventory, the time stamp is in the format yyyy-mm-ddthh:mm:ss, and 't' indicates time.

NOTE: Lifecycle Controller does not provide the driver version for the RAID controller. To view the driver version, use iDRAC7, OpenManage Server Administrator Storage Service, or any other third party storage management application.

Related Links

About View and Export Current Inventory
About View and Export Factory Shipped Inventory
USB Device
Network Share

USB Device

To export to a USB flash drive:

1. From the **Select Device** drop-down menu, select the USB device (USB flash drive).
2. In the **File Location** text box, enter a valid directory or sub-directory path on the device. For example, 2011\Nov. If the path is not provided, the file is stored in the root location of the device.

NOTE: Lifecycle Controller allows 256 characters in a path, and does not support special characters such as :, *, ?, ", <, >, |, #, %, and ^ in folder names.

Network Share

To export to a Network Share, select **CIFS** or **NFS** and type the required details.

Related Links

CIFS
NFS

CIFS

For CIFS, type the following details:

- **Share Name** — Type the path to the shared folder to export the file. For example, type \\192.168.20.26\sharename or \\servername\sharename.
- **Domain and User Name** — Type the domain and user name required to log on to the network share. For example, loginname@myDomain or domain\user name. If there is no domain, type the user name.
- **Password** — Type the correct password.
- **File Location** — Type the sub-directories if any. For example, 2011\Nov.

NOTE: Lifecycle Controller allows 256 characters in a path, and does not support special characters such as :, *, ?, ", <, >, |, #, %, and ^ in folder names.

NFS

For NFS, type the following details:

- **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, 2011\Nov.

NOTE: Lifecycle Controller allows 256 characters in a path, and does not support special characters such as :, *, ?, ", <, >, |, #, %, and ^ in folder names.

Viewing and Exporting Current Inventory After Resetting Lifecycle Controller

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

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

1. Turn on the system and wait for a couple of minutes for iDRAC to start functioning.
2. Press <F10> to launch Lifecycle Controller and the system inventory is collected as CSIOR is enabled by default.
3. After Lifecycle Controller launches, go to **Hardware Configuration** and click **View Current Hardware Inventory** or **Export Current Hardware Inventory** to view or export current hardware inventory respectively. If the following message is displayed, click **Yes**, reboot the system, and retry.

   ```
   Hardware change is detected on the system. The current hardware inventory
   does not contain the latest updates as the hardware inventory update is in
   progress. To view or export the latest hardware inventory, relaunch
   Lifecycle Controller and retry. Do you want to continue with the old current
   hardware inventory information?
   ```

Related Links

Viewing Hardware Inventory-Current or Factory Shipped

Exporting Hardware Inventory-Current or Factory Shipped

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**.

Updating Platform

You can update to the latest version of Lifecycle Controller using the **Platform Update** wizard. It is recommended that you run the **Platform Update** wizard on a regular basis to access the latest updates. You can update the component firmware either using update repositories or individual DUPs (single component DUP.)

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

To update the platform:

1. In the left pane, click **Platform Update**.
2. In the right pane, click **Launch Platform Update**.
3. Select the type of update and one of these update repositories: FTP Server, Local Drive, or Network Share.
4. Specify the details.
5. To verify if Lifecycle Controller is able to connect to the IP address that is provided, click **Test Network Connection**. By default, it pings the Gateway IP, DNS server IP, host IP, and proxy IP.

NOTE: Lifecycle Controller cannot ping to the domain name and does not display its IP address if the DNS is not able to resolve the domain name. Make sure that the issue with DNS is resolved and retry.

6. Click **Next**.

   The **Select Updates** page is displayed with the component names for which the updates are available.
7. Select the components that require an update, and click **Apply**.

   The update process is initiated and the firmware update is completed after rebooting the system several times depending on the number of components selected.

NOTE: The system does not reboot if OS driver packs or hardware diagnostics are updated.

Related Links

Platform Update
Download Methods
Selecting Type of Update And Update Source
Selecting and Applying Updates
Updating or Rolling Back Devices That Affect Trusted Platform Module Settings

Selecting Type of Update And Update Source

To perform the updates, you can download single component DUPs or repository (**Catalog.xml**) using the **Platform Update** wizard to one of the following sources:

NOTE: The **Catalog.xml** file contains the individual server bundles. Each bundle consists of all the DUP information (md5 security key, date and time, path, Release ID, version, and so on.)

- FTP server — Dell FTP Server, Local FTP, or FTP server using a proxy server.

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

- Local Drive — Use a USB flash drive, *Dell Server Updates* DVD, *Lifecycle Controller OS Driver Packs* DVD.
- Network Share

Related Links

Accessing Updates on a Local FTP Server
Configuring Local USB Flash Drive

Using Single Component DUPs

To use single component DUPs:

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

In the **Catalog Location or Update package path** box, enter the name of the DUP (for example, APP_WIN_RYYYZZZ.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_RYYYZZZ.EXE).

NOTE: Lifecycle Controller allows 256 characters in a path, and does not support special characters such as :, *, ?, ", <, >, |, #, %, and ^ in folder names.

Using Repository

To use the repository:

If the catalog file is located in the root folder, do not enter the file name in the **Catalog Location or Update package path** box. However, if the catalog file is located in a sub-directory, enter the sub-directory name (for example, subdirectory).

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

NOTE: Lifecycle Controller allows 256 characters in a path, and does not support special characters such as :, *, ?, ", <, >, |, #, %, and ^ in folder names.

Using Local Drive

1. From the **Select Device** drop-down menu, select the USB device (USB flash drive) that contains the updates (DUP or repository).
2. In the **Catalog Location or Update package path** box, enter the location or sub-directory where the catalog is stored.

Using Local or FTP Server

To use local FTP, Dell FTP, local FTP that uses proxy settings, or service provider's FTP that is configured as a proxy server, enter the following details:

- **Address —** The IP address of the local FTP server or **ftp.dell.com**.

NOTE: If the Dell FTP is used, do not specify any other information.

- **User Name** — The user name to access the FTP location.
- **Password** — The password to access the FTP location.
- **Catalog Location or Update package path** — Name of the DUP location or sub-directory where the catalog is stored.

  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.

- **Server** — The server host name of the proxy server.
- **Port** — The port number of the proxy server.

- **User Name** — The user name required for authentication on the proxy server.
- **Password** — The password required for authentication on the proxy server.
- **Type** — The type of proxy server. HTTP and SOCKS 4 proxy types are supported by Lifecycle Controller.

Related Links

Using Repository
Using Single Component DUPs

Using Network Share

To use a shared folder over a network, select **Network Share (CIFS or NFS)** and enter the details provided in the following table:

Table 1. Network Share Details

For CIFS	For NFS
Share Name — Path to the shared folder where the DUPs or repository is located. For example, \\xxx.xxx.xx.xx \sharename.	
Domain and User Name — Type the correct domain and user name required to log on to the network share. For example, loginname@myDomain, and if there is no domain, type the loginname.	NA
Password — Type the correct password	NA
Catalog Location or Update package path — Name of the DUP of the location/sub-directory where the catalog is stored.	

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

Selecting and Applying Updates

To select and apply the updates, select the required updates and click **Apply**. By default, Lifecycle Controller selects the components for which the current updates are available. For more information, see the *Lifecycle Controller online help*.

The system reboots after the update process is complete. When applying more than one update, the system reboots between updates directly into Lifecycle Controller and continues with the other selected updates.

NOTE: The system does not reboot after updating the OS driver pack and hardware diagnostics.

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

NOTE: While using Lifecycle Controller 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 Firmware Versions

You can roll back to previous firmware versions using the **Rollback** wizard.

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

To roll back the platform:

1. In the left pane, click **Platform Update**.
2. In the right pane, click **Launch Platform Rollback**.
   The **Platform Rollback** page displays a list of components for which rollback is available and the later versions are selected by default.
3. Select the required rollback image(s) and 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 Lifecycle Controller and continue updating.

Related Links

Platform Rollback
Comparing Firmware Versions
Updating or Rolling Back Devices That Affect Trusted Platform Module Settings

Comparing Firmware Versions

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 name of the components. 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 or Rolling Back Devices That Affect Trusted Platform Module Settings

Enabling Trusted Platform Module (TPM) with pre-boot measurement enables the BitLocker protection on the system. When BitLocker protection is enabled, updating or rolling back the components such as RAID controller, NIC, and BIOS require that a recovery password is entered or a USB flash drive that contains a recovery key is inserted during the next system boot. For information on how to set TPM settings, see the *BIOS User Guide* available at **support.dell.com/manuals**.

When Lifecycle Controller 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 not to update or to roll back those components by navigating to the **Select Updates** page and deselecting the check boxes for the components.

Performing Hardware Diagnostics

To perform hardware diagnostics:

1. In the left pane of Lifecycle Controller, click **Hardware Diagnostics.**
2. In the right pane, click **Run Hardware Diagnostics**. The diagnostics utility is launched, and follow the on-screen instructions.
   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**.
   To exit the Hardware Diagnostics utility, reboot the system and press F10 to re-enter Lifecycle Controller.

Related Links

Hardware Diagnostics

Installing Operating System

Before installing the operating system, make sure that the following prerequisites are met:

- Optical DVD drive is connected.
- Hard disk is connected.
- Virtual media is connected. For more information, see *iDRAC User's Guide*.
- Software RAID or PERC controller is installed with the latest firmware, and at least one physical disk is available for creating the virtual disk. For more information on the supported controllers and related firmware, see operating system documentation.

To install the operating system:

1. To launch Lifecycle Controller, boot the 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:
   - **Configure RAID First** (optional) and click Next, if the system has a RAID controller.
   - **Go directly to OS Deployment** and click **Next** to bypass the RAID configuration.
4. Select the operating system from the list, insert the operating system media, and complete the remaining tasks.

NOTE: If you select an operating system that supports UEFI boot mode, BIOS or UEFI options are provided for selecting the boot mode.

5. Reboot the system.

   The operating system is automatically installed on the selected virtual drive.

Related Links

Selecting Operating System
Rebooting System
Using Optional RAID Configuration

Using Optional RAID Configuration

You can configure RAID if there are no existing configurations, else you can bypass RAID configuration and deploy the operating system. Alternately, you can configure RAID through the RAID configuration page from the **Hardware Configuration Tab → Configuration Wizards → RAID Configuration** .

Configuring RAID Using Operating System Deployment Wizard

To configure RAID using OS Deployment wizard:

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

1. In the left pane of the **Home** page, click **OS Deployment**.
2. Select **Configure RAID First**.

   The RAID Configuration wizard is launched. It displays all the storage controllers available for configuration.
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 OS Deployment wizard navigates to the **Select an Operating System** page.

Selecting Operating System

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

- 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 system, and click **Next**.
   The drivers are extracted to the OEMDRV directory, and Lifecycle Controller prompts you to insert the operating system installation media.
2. Lifecycle Controller displays two installation modes — **UEFI** or **BIOS**. Select one of the options and click **Next**.
   If the selected operating system does not support UEFI mode, the UEFI option is grayed-out. However, if the operating system that is being installed has partial support for UEFI based installation, it may fail and you may not be able to boot into the operating system. Make sure to see the operating system documentation before installing the operating system in UEFI mode. Else, set the boot mode to BIOS and install the operating system.
3. Insert the standard operating system installation media when prompted, and click **Next**. Lifecycle Controller validates the media.
4. If the standard operating system installation media is validated, continue with the installation. Else, insert the correct media and click **Next**.
   The Reboot the System page is displayed.

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 into the OEMDRV directory and Lifecycle Controller 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**.
3. If the validation check fails, the following message appears:
   `The selected media doesn't match the standard media certification of the OS <name of the selected operating system>`
4. Click **Yes** to continue, else **No** to insert a different media and retry.
   The Reboot the System page is displayed.

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**.

   No drivers are 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: Lifecycle Controller does not validate the media.

The **Reboot the System** page is displayed

Related Links

Rebooting System
Driver Access

Rebooting System

Click **Finish** to reboot the system and continue with the operating system installation. The system boots to the operating system installation media.

Post Reboot Scenarios

The following table lists the post reboot scenarios, its user actions, and impact.

Scenario	User Action and Impact
During POST, the system prompts you to press a key to boot into the operating system installation media	Press any key to begin the operating system installation, 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 the installation is completed.	The system 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.
During the 18-hour period when drivers are extracted to a temporary location after the operating system is installed, you cannot update Lifecycle Controller, drivers, or hardware diagnostics using a DUP. If you attempt a DUP update through the operating system during this time period, the DUP displays a message that another session is active.	Lifecycle Controller does not allow this after the operating system installation. However, if you disconnect the power supply to the managed system, the OEMDRV directory is erased.

Controlling Access to Front Panel

To control access to the front panel:

1. From the Lifecycle Controller **Home** page, select **Hardware Configuration**.
2. In the right pane, select **Configuration Wizards**.
3. Under **System Configuration Wizards**, click **Front Panel Security**.
4. Set System Control Panel Access to one of the following options:
   - View and Modify

- View Only
- Disable

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

System Control Panel Access Options

Lifecycle Controller front panel security configuration enables an administrator to restrict access to control panel interface. The options available are:

- **View and Modify** — You can obtain information and make changes using the system control panel interface.
- **View Only** — You can move through the data screens to obtain information using the system control panel interface.
- **Disabled** — You do not have access to information or control, other than the information displayed by the management controller, and you cannot specify actions.

Configuring System Time And Date

To set the time and date for the managed system:

1. From the Lifecycle Controller **Home** page, select **Hardware Configuration**.
2. In the right pane, select **Configuration Wizards**.
3. Under **System Configuration Wizards**, click **System Time/Date Configuration**.

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

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. Under **System Configuration Wizards**, 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
4. In the **Summary** page, view the summary of all the changes, and click **Apply** to save the changes.

   A `Please Wait` message appears while your changes are saved. When the operation is complete, a final **Confirmation** screen displays a table with the three values: Unchanged, Success, or Failed for all the modified parameters.

5. Click **Finish** to apply the new iDRAC settings.

LAN Configuration

To view and configure LAN:

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

Table 2. : 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).	-
NIC Selection	View or edit the NIC mode	-

NIC Modes

The different types of NIC mode for enabling NIC are:

- Dedicated — This licensed option enables the remote access device to utilize the dedicated network interface available on the Remote Access Controller (RAC). This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic.
- LOM1, LOM2, LOM3 or LOM4 — Enables network interface to remotely access the system based on the LOM selected.

Advanced LAN Configuration

To set advanced LAN configuration:

1. From **iDRAC Configuration**, select and **LAN Configuration** and then 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 3. : Advanced LAN Configuration Attributes

Attribute	Description	Values
VLAN	Indicates 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
Auto Negotiate	When auto-negotiate is on, it determines whether iDRAC automatically sets the Duplex Mode and Network Speed values by	On or Off

Attribute	Description	Values
	communicating with the nearest router or hub. When auto-negotiate is off, you must set the Duplex Mode and Network Speed values manually.	
LAN Speed	Configures the network speed to match the user's network environment. This option is not available if Auto-Negotiate is set to On.	10 Mb, 100 Mb, and 1000 Mb
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**, go to **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. : 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. **NOTE:** You cannot 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.	-

IPv4 Configuration

To set IPv4 configuration:

1. From **IP Configuration**, go to IPv4 Configuration and enable or disable the protocol.
2. Set the RMCP+ encyption key.
3. Specify the **IP Address Source**.
4. Specify user-configured settings.
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 iDRAC NIC can acquire an IPv4 address from the DHCP server or from a manually set Static IP. Setting the **IP Address Source** to DHCP deactivates Ethernet IP Address, Subnet Mask, and Default Gateway options.	DHCP or Static

Ethernet IP Address Settings for IPv4

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

Table 5. Ethernet IP Address Settings for IPv4

Settings	Values and Description
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 or 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:

NOTE: The feature is licensed. Acquire the license to enable the feature. For more information on acquiring and using the licenses, see *iDRAC7 User's Guide*.

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

Ethernet IP Address Settings for IPv6

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

Table 6. Ethernet IP Address Settings for IPv6

Settings	Values and Description
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: • IPv6 Address forms supported: – **X:X:X:X:X:X:X:X** — In this form, **X** represents the hexadecimal values of the eight 16-bit addresses. You can omit the leading zeros in individual fields, but you must include at least one numeral in every field. – **::** (two colons) — Using this form, you can represent a string of contiguous zero fields in the preferred form. The **::** can only appear once in the address. You can also use this form to represent unspecified addresses (0:0:0:0:0:0:0:0). – **x:x:x:x:x:x:d.d.d.d** — This form is sometimes more convenient when in a data center with 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.
Default Gateway	Maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Get DNS Servers from DHCP	Yes or 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.

Settings	Values and Description
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 iDRAC7 Enterprise. Use the Virtual Media Configuration wizard to set control modes for the available Virtual Media devices. See the *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* available at **support.dell.com/manuals** for more information on supported Virtual Media devices.

NOTE: The feature is licensed. Acquire the license to enable the feature. For more information on acquiring and using the licenses, see *iDRAC7 User's Guide*.

To set the virtual media configuration:

1. From **iDRAC Configuration**, go to **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 7. : 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**, go to **LAN User Configuration**.
2. Set user settings.
3. Click **Next** to proceed.

Table 8. : LAN User Configuration

Parameter	Description	Value
Provisioning Server Address Criteria	Enter provision server address.	IPV4 or IPV6 or Host Name
Auto-Discovery	Discovers the provisioning server.	Enable or Disable
Account Access	Disabling account access deactivates all other fields on the **LAN User Configuration.** **NOTE:** The option is available only for the 'root' user.	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 host names and ports separated by comma.
- Host name can be fully qualified.
- IPv4 address – starts with '(' and ends with ')' when specified at the same time with a host name.
- Each IP address or host name can be optionally followed by a ':' and a port number.
- Example of valid strings are - hostname, hostname.domain.com

Account Privilege

Table 9. : Account Privilege

Privileges	Admin	Operator	User	No Access
Login to iDRAC	Yes	Yes	Yes	-
Configure iDRAC	Yes	Yes	-	-
Configure Users	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

You can set the following values for 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.

Configuring RAID Using Hardware RAID

If your system has one or more supported PERC RAID controller(s) with PERC 8 firmware or greater, or SAS RAID controller(s), use the **RAID Configuration** wizard to configure a virtual disk as the boot device.

NOTE: If there are any internal storage controller cards on the system, all other external cards cannot be configured. If there are no internal cards present, then external cards can be configured.

To configure RAID:

NOTE: It is recommended that you have a good knowledge of RAID and your hardware configuration to perform RAID configuration.

1. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizards**.
3. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard.
   The **View Current RAID Configuration and Select Controller** page is displayed.
4. Select the controller and click **Next**.
   The **Select RAID Level** page is displayed.
5. Select the RAID level and click **Next**.
   The **Select Physical Disks** page is displayed.
6. Select the physical disk properties and click **Next**.
   The **Virtual Disk Attributes** page is displayed.
7. Select the virtual disk parameters and click **Next**.
   The **Summary** page is displayed.
8. To apply the RAID configuration, click **Finish**.

Related Links

Viewing Current RAID Configuration
Selecting RAID Controller
Foreign Configuration Found
Selecting RAID Levels
Selecting Physical Disks
Setting Virtual Disk Attributes
Viewing Summary

Viewing Current RAID Configuration

The **View Current RAID Configuration and Select Controller** 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 have to install the operating system on an existing virtual disk, make sure that the virtual disk size and RAID level are correct.
- Use the **RAID configuration** wizard to delete all the existing virtual disks and create only 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 enable you to reconstruct data in the event of a disk failure.

NOTE: You can create only one virtual disk using Lifecycle Controller. To create multiple virtual disks, use option ROM. To access option ROM, press **CTRL+R** during boot.

Selecting RAID Controller

The **View Current RAID Configuration and Select Controller** page 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** page is displayed only if a foreign configuration disk resides on the selected RAID controller.

NOTE: If you have selected an S110 RAID controller, the foreign disks are displayed as Non-RAID disks in Lifecycle Controller. 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 require, 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 clears the disk space containing the foreign configuration and makes it available for use in a new virtual disk.

Click **Next** after selecting one of the options.

Selecting RAID Levels

From the **RAID Level** drop-down menu, select the RAID level for the virtual disk:

- **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 zero 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 good data redundancy and read performance but slower write performance.
- **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, its performance decreases, data or program access gets slower, and transfer speeds on the array are affected when a physical disk fails and reconstruction takes place.
- **RAID 60** — Combines the straight block level striping of RAID 0 with the distributed double parity of RAID 6. The system must have at least eight physical disks to use RAID 60. 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 two physical disks on either span must fail for data loss to occur.

Minimum Disk Requirement for Different RAID Levels

Table 10. : 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

* For S110 RAID controller, a minimum of 2 disks are required.

Selecting Physical Disks

Use the **Select Physical Disks** screen to select the physical disks to be used for the virtual disk and select the physical disk related properties.

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.

- From the **Protocol** drop-down menu, select the protocol for the disk pool: **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.
- From the **Media Type** drop-down menu, select the media type for the disk pool: **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.
- From the **Select Span Length** drop-down menu, select the span length. 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**.

Setting Virtual Disk Attributes

Use this page to specify the values for the following virtual disk attributes:

- In the **Size** box, specify the size of the virtual disk.
- From the **Stripe Element Size** drop-down menu, select the stripe element size. 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.
- From the **Read Policy** drop-down menu, select the read policy:
  - **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.
- From the **Write Policy** drop-down menu, select the write policy.
  - **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 **Assign a Hot Spare Disk if available**.

  A hot spare is an unused backup physical disk that is 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 is not assigned.
- To secure the virtual disk with the controller's security key.

NOTE: The secure virtual disk is created only if the controller security key is created and the selected disks are Self-Encrypting Drives (SEDs).

Viewing Summary

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

CAUTION: Clicking Finish deletes all existing virtual disks except any foreign configurations that you specified. All data residing on the virtual disks is lost.

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

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

Configuring RAID Using Software RAID

For the S110 controller, make sure to change the SATA Controller option to RAID Mode. To do this through BIOS, the latest BIOS version must be installed. For more information on the BIOS versions for different systems, see *Lifecycle Controller Readme*.

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

Use this feature to configure RAID if a PERC S110 controller on the motherboard is present in the system. If the software RAID option is selected, Lifecycle Controller 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 controller (S110).

To configure software RAID, do the following tasks:

1. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizards**.
3. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard:
   The **View Current RAID Configuration and Select Controller** page is displayed.
4. Select the controller and click **Next**.
   If the non RAID disks are attached to the selected controller, select the non-RAID physical disks and click **Next** to initialize them. Else, the **Select RAID Level** page is displayed.

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

5. Select the RAID level and click **Next**.
   The **Select Physical Disks** page is displayed.
6. Select the physical disk properties and click **Next**.
   The **Virtual Disk Attributes** page is displayed.
7. Select the virtual disk parameters and click **Next**.
   The **Summary** page is displayed.
8. To apply the RAID configuration, click **Finish**.

Related Links

Selecting RAID Controller
Foreign Configuration Found
Selecting RAID Levels
Selecting Physical Disks
Setting Virtual Disk Attributes
Viewing Summary

Creating a Secure Virtual Disk on Series 7 Controller

Make sure that the controller is encrypted with a Local Key.

To create a secure virtual disk on series 7 controller:

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

3. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard.
   The **View Current RAID Configuration** and **Select Controller** page is displayed and along with information on whether the displayed virtual disk is secure.
4. Select the controller and click **Next**.
   If the non RAID disks are attached to the selected controller, select the non-RAID physical disks and click **Next** to initialize them. Else, the Select RAID Level page is displayed.

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

5. Select the RAID level and click **Next**.
   The **Select Physical Disks** page is displayed.
6. **From the Encryption Capability drop-down menu, select Self-encryption**. The self-encryption disks (SEDs) are displayed.
7. Select the SEDs and specify the properties, and click **Next**.
   The **Virtual Disk Attributes** page is displayed.
8. Select the virtual disk parameters and select the Secure Virtual Disk option, and click **Next**.
   The **Summary** page is displayed.
9. To apply the RAID configuration, click **Finish**.

Related Links

Selecting RAID Controller
Foreign Configuration Found
Selecting RAID Levels
Selecting Physical Disks
Setting Virtual Disk Attributes
Viewing Summary
Applying the Local Key On RAID Controller

Configuring vFlash SD Card

Use the licensed feature to enable or disable the vFlash SD card, check the health and properties, and initialize the vFlash SD card. Lifecycle Controller support vFlash SD cards of sizes 1 GB, 2 GB, 8 GB, and 16 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 7 (iDRAC7) 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 feature to:

- Enable or disable vFlash SD card.
- Determine the vFlash SD card properties:
  - Name
  - Health — The response actions for health state such as **OK**, **Warning**, and **Critical** are None, Initialize and try again, and Remove, reset, and try again or Initialize and try again respectively
  - 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.
  - 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.

Enabling or Disabling vFlash

Make sure to set the write-protect latch on the vFlash SD card to **Off** position.

If set to **Enabled**, the vFlash SD card is configured as a virtual drive that 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:

1. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizards**.
3. Under **System Configuration Wizards**, click **vFlash SD Card Configuration**.
   The **vFlash SD Card** page is displayed.
4. From the vFlash Media drop-down menu, select **Enabled** or **Disabled**.
5. Click **Finish** to apply the changes.

Initializing vFlash

1. Under **System Configuration Wizards**, click **vFlash SD Card Configuration**.
   The **vFlash SD Card** page is displayed.
2. Click **Initialize vFlash** to erase all the data present on the vFlash SD card.

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

Modifying Device Settings

To modify device settings using the **Advanced Hardware Configuration**:

1. In the left pane, select **System Setup**.
2. In the right pane, click **Advanced Hardware 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?
   ```
4. Select **No** to continue making additional configuration changes.
   All changes are applied during the next system boot.

Related Links

Advanced Hardware Configuration

Encrypting Unsecure Virtual Disks

Make sure that the following prerequisites are met:

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

To encrypt the unsecure virtual disks:

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

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

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

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

Related Links

Local Key Encryption Mode

Applying the Local Key On RAID Controller

Before applying the local key on the RAID controller, make sure that the controller is security capable.

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**.
3. Under **Storage Configuration wizards**, click **Key Encryption**.
4. Select the controller to apply a local key and click **Next**.
5. Click **Set up local key encryption** and click **Next**.

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

6. Enter the **Encryption Key Identifier** that is associated with the entered passphrase. The Encryption Key Identifier is a passphrase hint; you must enter the passphrase when Lifecycle Controller prompts with this hint.
7. 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.

8. In the **Confirm Passphrase** text box, re-enter the passphrase, and click Finish.

Related Links

Key Encryption
Selecting RAID Controller
Foreign Configuration Found
Selecting RAID Levels
Selecting Physical Disks
Setting Virtual Disk Attributes
Viewing Summary

Rekey Controller With 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**.

3. Under **Storage Configuration wizards**, click **Key Encryption**.
4. Select the controller to which the local key is applied and click **Next**.
5. In the **Existing Passphrase** text box, enter the existing passphrase associated with the displayed Encryption Key Identifier.
6. 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 Lifecycle Controller prompts with this hint.
7. In the **New Passphrase** text box, enter the passphrase that will be associated with the new encryption key identifier

Related Links

Local Key Encryption Mode

Removing Encryption and Deleting 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.

Related Links

Local Key Encryption Mode

Breaking Mirrored Disk

To split the mirrored array of RAID-1 virtual disks:

1. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizards**.
3. Under **Storage Configuration wizards**, click **Break Mirror**.
   The **Break Mirror** page is displayed with the mirrored virtual disks.
4. Select the related controller and click **Finish**.

NOTE: Break Mirror feature does not support software RAID controllers.

The system shuts down even if one mirrored array is successfully delinked.

Configuring Local FTP Server

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

FTP Authentication

Although you must provide the user name and password for the FTP server, Lifecycle Controller supports anonymous login to the FTP server using the FTP server address 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.

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 **LC 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: For information on creating a repository for your system, see the *Dell Repository Manager User Guide* at **support.dell.com/manuals**.

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 to specify the online repository when using the **OS Deployment** wizard through Lifecycle Controller and Platform Update through Lifecycle Controller.

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 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 Lifecycle Controller.
- **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 Local USB Flash Drive

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 flash drive.

The USB flash drive used as a repository must hold at least 8 GB of content.

A USB flash drive 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: Lifecycle Controller supports internal SATA optical drives, USB optical drives, and Virtual Media devices. If the installation media is corrupt or not readable, then Lifecycle Controller 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 Flash Drive from the Dell Server Updates DVD

To copy the repository:

1. Download the *Dell Server Updates* ISO from **support.dell.com**, and copy it to a DVD.
2. Copy the repository folder of the DVD to the root directory of the USB flash drive.
3. Use this USB flash drive for platform update.

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

To create and copy the repository:

1. Copy the repository created using the Dell Repository Manager to the root directory of the USB flash drive.
2. Use this USB flash drive for platform update.

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

Configuring Replaced Parts

Before performing part replacement configuration, make sure that the following prerequisites are met:

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

NOTE: Make sure that Part Firmware Update and Part Configuration Update are not disabled.

- Enable **Collect System Inventory On Restart**. If it is disabled, the cache of system inventory information may become stale if new components are added without manually entering Lifecycle Controller after turning the system on. In the manual mode, you must press <F10> after part replacement during reboot.
- The replaced card or part must belong to the same family as the previous component.

To perform part firmware and configuration update:

1. In the left pane, click **Platform Restore**.
2. In the right pane, click **Part Replacement**.

   The **Part Replacement Configuration** page is displayed.
3. 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.
4. 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.

Related Links

Part Replacement Configuration

Updating Server Inventory Information

To enable collecting system inventory on restart:

1. In the left pane, click **Hardware Configuration**.
2. On the right pane, select **Hardware Inventory**.
3. **C**lick **Collect System Inventory on Restart**.
4. Under **Collect System Inventory on Restart**, click **Enabled** or **Disabled**.

Related Links

Collect System Inventory on Restart

Back Up Server Profile

Before you back up the server profile, make sure that the following prerequisites are met:

- The server has a valid service tag (7 characters).
- vFlash SD card is installed, initialized, and enabled.
- vFlash SD card has a minimum free space of 500 MB.
- Use only one iDRAC virtual console during backup operation.

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 without using a passphrase, 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**.

   The system reboots and Lifecycle Controller is disabled. You cannot access Lifecycle Controller until the backup process is complete. A success message is displayed when you launch Lifecycle Controller after backup is complete.

NOTE: You can check the Lifecycle logs in iDRAC Web interface for backup server profile status. To view the log in Lifecycle Controller after the backup is completed, click **Lifecycle Log** → **View Lifecycle Log History** .

Related Links

Backup Server Profile
System or Feature Behavior During Backup

System or Feature Behavior During Backup

- Lifecycle Controller is disabled.
- 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 all configuration information.
- Does not back up diagnostics and driver pack information.
- Backup fails if an AC power cycle is performed.

Exporting Server Profile to USB Flash Drive or Network Share

Before exporting the server profile, make sure that the following prerequisites are met:

- vFlash SD card is installed in the system and must contain the backup image file.
- USB flash drive has a minimum free space of 500 MB.
- Network share is accessible and has a minimum free space of 500 MB.
- Use the same vFlash SD card that was used during backup.

To export the server profile to a USB flash drive 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**.

   The *Backup_<service_tag>_<time_stamp>.img* file is exported to the specified location.

Related Links

System or Feature Behavior during Export
Export Server Profile
USB Device
Network Share

System or Feature Behavior during Export

- Takes up to 15 minutes depending on the server configuration.
- Lifecycle Controller exports the backup image file in the *Backup _<service_tag>_<time_stamp>.img* 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.

Importing Server Profile from a vFlash SD Card Network Share or USB Flash Drive

Before importing the server profile, make sure that the following prerequisites are met:

- The service tag of the server is same as when the backup was taken.
- If you are restoring from a the 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 accessible.
- Use only one iDRAC virtual console during restore operation.

You can import the server profile from a vFlash SD card, Network Share, or a USB flash drive.

Related Links

System or Feature Behavior During Import
vFlash SD Card
Network Share
USB Device
Post-import Scenario
Import Server Profile

vFlash SD Card

To import from a 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, enter the passphrase (entered during backup) in the **Backup File Passphrase** box, and click **Finish**.

Related Links

System or Feature Behavior During Import
Import Server Profile
Importing Server Profile After Motherboard Replacement

Network Share

To import from a 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 backup file name along the with directory, sub-directory path, 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, enter the passphrase (entered during backup) in the **Backup File Passphrase** box, and click **Finish**.

Related Links

System or Feature Behavior During Import
Import Server Profile
Importing Server Profile After Motherboard Replacement

USB Device

To import from a USB flash drive:

1. In the left pane, select **Platform Restore**.
2. In 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 flash drive.
5. In the **File Location** text box, enter the directory or sub-directory path, where the backup image file is stored on the selected 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, enter the passphrase (entered during backup) in the **Backup File Passphrase** box, and click **Finish**.

Related Links

System or Feature Behavior During Import
Import Server Profile
Importing Server Profile After Motherboard Replacement

System or Feature Behavior During Import

- Lifecycle Controller is not available during restore, and is enabled after the import operation is complete.
- Restores everything that was backed up including Lifecycle controller content.
- 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 Lifecycle Controller, 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.
- The import operation restore only Perpetual license. The evaluation and permanent licenses are not restored.

Post-import Scenario

The managed system performs the following operations:

1. System powers off if turned on. If the system boots into an operating system, it attempts to perform a graceful shutdown. If it is not able to perform a graceful shutdown, it performs a forced shutdown after 15 minutes.
2. System powers on and boots 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 performs 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 the restore process is complete. Check the Lifecycle logs for the restore process entries.

Related Links

Importing Server Profile from a vFlash SD Card Network Share or USB Flash Drive

Importing Server Profile After Motherboard Replacement

Before importing the server profile after motherboard replacement, make sure that the following prerequisites are met:

- A backup image of the server with the old motherboard is present.
- 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.

After replacing the motherboard, import the server profile from a vFlash SD card, Network Share, or a USB device.

- See Post-import Scenario
- The Service tag is restored on the new motherboard from the backup file.

Related Links

Import Server Profile
vFlash SD Card
Network Share
USB Device

Viewing Lifecycle Log History

Use this feature to view:

- Firmware inventory
- History of firmware updates
- Update and configuration events

NOTE: The details of the configuration changes are not displayed.

- User work notes

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

NOTE: As the lifecycle logs are generated by various systems management tools, you may not view the events in lifecycle log immediately after they were logged.

To view the Lifecycle Log history and use the filtering options:

1. In the left pane, click **Lifecycle Log**.
2. In the right pane, click **View Lifecycle Log History**.
   - **No** — The serial number of the event.
   - **Category** — The category under which the events belong. The available categories are:
     * System Health — Events related to installed hardware such as Fan, Power Supplies NIC/LOM/CNA Link, BIOS Errors, and so on.
     * Storage — Events related to external or internal storage components such as Controller, Enclosure, Physical Disks, Software RAID.
     * Configuration — Events related to hardware and software changes such as addition or removal of hardware in the system, configuration changes made using Lifecycle Controller or operating system, and so on.
     * Audit — Events related to user login, intrusion, licenses, and so on.
     * Updates — Events related to updates or rollback of firmware and, drivers.
     * Work Notes — Events logged by the user.
   - Message ID - Each event is represented with a unique Message ID. For example, SWC0001.
   - Description — A brief description of the event. For example, Dell OS Drivers Pack, v.6.4.0.14, X14 was detected.
   - Date and Time — When the event occurred.
3. Use the following options in **Filter by Category** to see specific information related to the each of the categories:
   - All — Displays all the data in the Lifecycle Log
   - **Any Other Event** — Displays the data based on the event selected. For example, Audit, Configuration, Storage, System Health, Updates, and so on.

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. Before exporting the lifecycle log, make sure the following prerequisites are met:

NOTE: As the lifecycle logs are generated by various systems management tools, you may not view the events in lifecycle log immediately after they were logged.

- If you need to store the exported file in a USB flash drive, make sure that a USB flash drive is connected to the managed node.
- If you use a network share (shared folder), set the correct Network Settings. See Using LC Settings for more information.

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**.
4. If you select **Network Share** option, click **Test Network Connection** to verify if Lifecycle Controller is able to connect to the IP address that you provided. By default, it pings the Gateway IP, DNS server IP, and host IP.

NOTE: Lifecycle Controller cannot ping to the domain name and does not display its IP address if the DNS is not able to resolve the domain name. Make sure that the issue with DNS is resolved and retry.

5. Click **Finish**.

   The Lifecycle Log is exported to the specified location.

Related Links

USB Device
Network Share

Adding Work Note to Lifecycle Log

Use this feature to record comments that can be used at a later date. For example, scheduled downtime information or for administrators (working in different shifts) to communicate about the changes made by each of them.

NOTE: You can type a maximum of 50 characters in the **Lifecycle Log** field.

To add a work note:

1. In the left pane, click **Lifecycle Log**.
2. In the right pane, click **Add a work note to Lifecycle Log**.
3. 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 system.
- Reuse a managed system for a different application.
- Move a managed system to a non-secure location.

CAUTION: This feature resets the iDRAC to factory defaults, and deletes all iDRAC user credentials, IP address configuration settings, encryption certificates, and licenses. 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 to 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. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Delete Configuration and Reset Defaults**.
3. Select **Reset Lifecycle Controller**.
4. Click **Finish**.

   A message is displayed.
5. Click **Yes** to continue or **No** to cancel the operation.

Related Links

Delete Configuration and Reset Defaults

5
Troubleshooting and Frequently Asked Questions

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

Error Messages

The following table lists some of the errors:

Error Message	Resolution
Failed to Copy Driver Files	The drivers required to install the operating system are corrupted. To resolve this issue, perform a platform update (see Updating Platform). See Updating Platform for more information.
Network is not configured. Do you want to configure now?	Network settings must be configured for Lifecycle Controller to work correctly. See Operating System Deployment for information on configuring Lifecycle Controller network settings from the Network Settings page.
Cannot set new date and time.	Lifecycle Controller was unable to change the system date and time. To resolve this issue: 1. Reboot the system. 2. Re-enter Lifecycle Controller 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.
Enter a valid Encryption Key of up to 40 Hex digits	Enter a valid encryption key that contains less 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 Default Gateway Address	Enter a valid default gateway 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 Help 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, it is recommended to use 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, it is recommended to use only digits (0–9), alphanumeric characters (a–z, A–Z), and hyphens (–) in the password string.
Ping Test Failed	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.

Error Message	Resolution
Drivers pack not found OR Error populating OS list	Lifecycle Controller cannot find the drivers required to install the operating system. To resolve this issue, perform a platform update. See Updating Platform for more information.
The repository you selected as an update source failed an integrity check. Recreate the repository, download it again, or provide an alternate source to be used.	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 Local USB Flash Drive) or provide an alternate repository.
Decompression of the catalog file failed	The catalog downloaded to compare the 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 (seeConfiguring Local USB Flash Drive) or provide an alternate repository.
Unable to resolve host name	This error is probably caused by one of the following: • Invalid name is specified for the platform update FTP server. For more information, see Selecting Type of Update And Update Source. • Invalid Domain Name Server (DNS) specified in the Network Settings page. For more information, see Operating System Deployment.
Update Package Corrupted	Lifecycle Controller has detected that one or more of the DUPs used to update the 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 Local USB Flash Drive) or provide an alternate repository.
Enter a valid IPv6 Address for this iDRAC.	Enter a valid IPv6 network address for iDRAC. See IPv6 Configuration. For more information, see IPv6 Configuration.
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. For more information, see IPv6 Configuration.
Enter the IPv6 Default Gateway address.	Enter the IPv6 default gateway address. For more information, see IPv6 Configuration.
Enter a valid IPv6 DNS Server 1 Address.	Enter a valid IPv6 DNS Server1 address. For more information, see IPv6 Configuration.
Enter a valid IPv6 DNS Server 2 Address.	Enter a valid IPv6 DNS Server2 address. For more information, see IPv6 Configuration.
Enter a valid iDRAC Name of up to 63 characters.	Enter a valid iDRAC name that is less than or equal to 63 characters.
Enter a valid Domain Name of up to 64 characters.	Enter a valid domain name that is less than or equal to 64 characters.
Enter a valid Host Name of up to 62 characters.	Enter a valid host name that is less than or equal to 62 characters.
The VLAN ID in the range of 1 to 4094, as defined by IEEE 801.1g specification.	Enter a VLAN ID between 1 and 4094. See Advanced LAN Configuration. For more information, see Advanced LAN Configuration.
The VLAN ID Priority in the range of 0 to 7, as defined by IEEE 801.1g specification.	Enter a VLAN ID priority value between 0 and 7. For more information, see Advanced LAN Configuration.

Error Message	Resolution
RAID configuration failed	Lifecycle Controller failed when creating the RAID configuration. To resolve this issue: 1. Reboot the system. 2. Re-enter Lifecycle Controller by pressing the **<F10>** key. 3. Try again to create the RAID configuration.
Generic Failure	Lifecycle Controller experienced an unidentified error when creating the RAID configuration. To resolve this issue: 1. Reboot the system. 2. Re-enter Lifecycle Controller by pressing the **<F10>** key. 3. Try again to create the RAID configuration.
No physical disk was selected for this virtual disk	The number of physical disks 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 valid RAID level found	The number of physical disks attached to the system is insufficient for the RAID level 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: 1. Reboot the system. 2. Re-enter Lifecycle Controller by pressing the **<F10>** key. 3. Change the settings.
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 Lifecycle Controller by pressing the **<F10>** key. 3. Re-open the Advanced Configuration screen.
This feature is not supported in this configuration. Please update your BIOS and iDRAC7 Firmware to the latest version and retry.	The blade server does not support the selected feature.
No Share Name/Details present	Type the correct share name or username and password, and retry.
Cannot authenticate the login credentials and share name.	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.
Cannot mount the network share	This error may occur due to temporary network problems. If this issue persists, check the network connection and then retry.
The operation completed successfully, but the system cannot automatically shut down. Shut the system down manually.	Press the power button on the system to shutdown manually.
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.
Invalid USB Folder Location	Provide the valid folder location.
Invalid Network Share Folder Location	Provide the valid folder location.

Error Message	Resolution
Invalid USB and Network Share Folder Location	Provide the valid folder location.
The Update Package is not supported for this System	Ensure that the update package is supported on the system.
Invalid Update Package	Ensure that the update package is not corrupt or tampered.
The Server Profile backup operation that was initiated from Lifecycle Controller completed with errors.	The RAC log contains the names of the components that failed during backup. Verify the firmware information and retry.
Failed to copy the backup server profile to the SRVCNF partition on the vFlash SD card.	Make sure that the vFlash SD card is installed, initialized, and enabled.
The restore operation initiated from Lifecycle Controller has 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 AC power cycle and retry.
Cannot complete the operation as the vFlash SD Card is not present. Insert the vFlash SD card and retry.	Install the vFlash SD card and retry the operation. Upload the required license to enable vFlash SD card and retry.
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 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.
This operation cannot be completed because the SD Card is not present. Insert the SD card and retry.	Make sure the card is present and the system has the required license uploaded to enable vFlash feature.
The Server Profile backup operation that was initiated from Lifecycle Controller 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 Lifecycle Controller

If the message `Lifecycle Controller update required` appears during power-on self-test (POST), the embedded device that stores Lifecycle Controller may contain corrupted data. To resolve the issue, you must first attempt to update Lifecycle Controller by executing Lifecycle Controller 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 Lifecycle Controller repair package:

1. Go to **ftp.dell.com** → **LifecycleController** and download the file named **LC2_Repair_Package_1.a.b.c.d.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 7(iDRAC7) User's Guide*.
3. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **iDRAC Firmware Update**.
   The **Firmware Update** page is displayed.
4. Click **Browse** and select the Lifecycle Controller Repair Package you downloaded from **ftp.dell.com**.
   The **Status (Step 2 of 3)** page is displayed.
5. Click **Next**.
   The **Updating (Step 3 of 3)** page is displayed.
6. After the update is complete, reboot the system.
7. Press the **<F10>** key within 10 seconds after the Dell logo appears to launch the Lifecycle Controller.
8. Complete the installation of all recommended updates. See Updating Platform for more information. When updates are complete, your system automatically reboots.
9. While the system reboots, press the **<F10>** key again to relaunch Lifecycle Controller.

Frequently Asked Questions

1. **When Lifecycle Controller 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 such as 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, Lifecycle Controller reboots and then attempts all the pending updates selected. After the final reboot, the system returns to the Lifecycle Controller **Home** page. Launch **Platform Updates** again, and re-select the update that had failed and click **Apply**.

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

5. **What is vFlash SD card?**
   vFlash SD card is a formatted SD (Secure Digital) card that plugs into iDRAC7 Enterprise. vFlash SD card can be formatted and enabled through 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 7 (iDRAC7) 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 Lifecycle Controller?**
   No. Lifecycle Controller 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 Lifecycle Controller to a local USB device?**
   No. Only drivers and firmware downloaded from the *Dell Server Updates* DVD is supported. See Configuring Local USB Flash Drive for more information.

9. **Can I delete Lifecycle Controller?**

   No.

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

    Yes. See the *iDRAC7 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 *iDRAC7 User's Guide* for more information (available at **support.dell.com/manuals**).

12. **What is UEFI? With which version does Lifecycle Controller comply?**

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

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

    Lifecycle Controller offers two ways to configure hardware: **Configuration Wizards** and **Advanced Configuration**.

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

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

14. **Does Lifecycle Controller support rollback of BIOS and firmware?**

    Yes. See Platform Rollback for more information.

15. **Which devices support system updates?**

    Lifecycle Controller currently supports updates to the BIOS, iDRAC firmware, power supply firmware, and certain RAID and NIC controller firmware. See Updating Platform for more information.

16. **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 Ad vanced Configuration if they support the HII configuration standard. See Hardware Configuration for more information.

17. **What should I do if my system crashes while using Lifecycle Controller?**

    If your system crashes while using Lifecycle Controller, a black screen with red text appears. To resolve this problem, first try rebooting your system and re-entering Lifecycle Controller. If that does not resolve the problem, perform the steps under Repairing Lifecycle Controller. If that does not resolve the problem, contact Dell for technical assistance.

18. **How do I find out the current installed version details of the Lifecycle Controller product?**

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

19. **What should I do if I have an issue with mouse synchronization when I access Lifecycle Controller over the iDRAC Virtual Console?**

    Make sure 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 7 (iDRAC7) User's Guide* available on the Dell Support site at **support.dell.com/manuals** for more information.

20. **Why should I keep CSIOR enabled?**

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

21. **Why are some features not accessible in Lifecycle Controller?**

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

6

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:element ref="dm:MessageArguments"inOccurs="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>
```

7

Easy-to-use System Component Names

The following table lists the Fully Qualified Device Descriptor (FQDD) of the system components and the equivalent easy-to-use names.

Table 11. Easy-to-use Names of System Components

FQDD of System Component Name	Easy-to-use Name
RAID.Integrated.1-1	Integrated RAID Controller 1
RAID.Slot.1-1	RAID Controller in Slot 1
NIC.Mezzanine.1B-1	NIC in Mezzanine
NIC.Mezzanine.1C-1	
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
P2PBridge.Mezzanine.2B-1	Embedded Host Bridge in Mezzanine 1 (Fabric B)
USBUHCI.Embedded.1-1	Embedded USB UHCI 1
USBOHCI.Embedded.1-1	Embedded USB OHCI 1
USBEHCI.Embedded.1-1	Embedded USB EHCI 1
Disk.SATAEmbeded.A-1	Disk on Embedded SATA Port A
Optical.SATAEmbeded.B-1	Optical Drive on Embedded SATA Port B
TBU.SATAExternal.C-1	Tape Back-up on External SATA Port C
Disk.USBFront.1-1	Disk connected to front USB 1
Floppy.USBBack.2-1	Floppy-drive connected to back USB 2

FQDD of System Component Name	Easy-to-use Name
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
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