Lifecycle Controller User's Guide

December 2021
Rev. A00

DELL Technologies

Notes, cautions, and warnings

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

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

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

© 2023 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Chapter 1: Introduction 6
Advantages of using Lifecycle Controller 6
Benefits of using iDRAC with Lifecycle Controller 6
Key features 7
Licensable features in Lifecycle Controller 7
Viewing iDRAC license information 8
Other documents you may need 8
Social Media Reference 9
Accessing documents from the Dell Support site 9
Contacting Dell 10

Chapter 2: Using Lifecycle Controller 11
Starting Lifecycle Controller 11
Start messages during POST, causes, and resolutions 11
Enabling Lifecycle Controller 12
Disabling Lifecycle Controller 12
Canceling Lifecycle Controller actions 12
Using Lifecycle Controller for the first time 13
Setting up Lifecycle Controller using Initial Setup Wizard 13
Setting up Lifecycle Controller from the home page 15
Lifecycle Controller features 16

Chapter 3: Operating system deployment 17
Installing an operating system 17
Using the optional RAID configuration 19
Configuring RAID using the operating system deployment wizard 19
Unattended installation 19
UEFI Secure Boot 19
Driver access 20
Installing an operating system on iSCSI LUN and FCoE LUN 20
Post reboot scenarios 20

Chapter 4: Monitor 22
Hardware inventory view and export 22
About view and export current inventory 22
About view and export factory-shipped inventory 22
Viewing hardware inventory — current or factory shipped 23
Exporting hardware inventory — current or factory shipped 23
Exporting hardware inventory to a USB drive 23
Exporting hardware inventory to network share 24
Viewing or exporting hardware inventory after part replacement 24
Viewing or exporting current inventory after resetting Lifecycle Controller 25
Lifecycle Controller log 25
Viewing Lifecycle Log history 25

Exporting Lifecycle Log.... 26
Adding a work note to the Lifecycle Log....28

Chapter 5: Firmware update....29
Firmware update methods....30
Version compatibility....31
Updating firmware....31
Selecting the type of update and update source....33
Using single component DUPs....36
Selecting and applying updates....36
System Configuration Lockdown mode....37
Firmware rollback....37
Rolling back to previous firmware versions....37

Chapter 6: Configure....39
System control panel access options....39
Controlling access to the front panel....39
Configuring iDRAC....40
Configuring system time and date....40
Configuring RAID....40
Foreign configuration found....41
Viewing current RAID configuration....41
Selecting RAID levels....42
Selecting physical disks....42
Setting virtual disk attributes....43
Viewing summary....44
Configuring RAID using software RAID....44
Creating a secure virtual disk on a RAID controller....45
Key encryption....45
Applying the local key on a RAID controller....46
Local key encryption mode....46
Encrypting unsecure virtual disks....46
Rekey controller with new local key....47
Removing encryption and deleting data....47
Breaking mirrored drives....47
System setup — Advanced Hardware Configuration....47
Modifying device settings....48
Collect system inventory on restart....49
Updating server inventory information....49
Configuring a local USB drive....49
Copying repository to a local FTP server from the Dell server Updates DVD....49
Using Dell Repository Manager to create the repository and copy it to a local FTP server....49
Configuring NFS and CIFS servers....50
Configuring NFS servers....50
Configuring CIFS servers....50
Conditions while configuring an HTTP or HTTPS server....50

Chapter 7: Maintain....52
Platform restore....52

Import server license....52
Part replacement configuration....52
Applying firmware and configuration updates to replaced parts....53
Supported devices....53
Repurpose or retire system....53
Deleting server information....54
Hardware diagnostics....54
Performing hardware diagnostics....54
SupportAssist Collection....55
Exporting the SupportAssist Collection....56

Chapter 8: Easy-to-use system component names....58

Chapter 9: Using the system setup and boot manager....61
Choosing the system boot mode....61
Entering System Setup....62
Responding to error messages....62
Using the system setup navigation keys....62
System Setup options....63
System and setup password features....69
Assigning system and setup password....69
Deleting or changing an existing system and setup password....70
Using your system password to secure your system....70
Operating with a setup password enabled....71
Entering the UEFI boot manager....71
Using the boot manager navigation keys....71
Boot Manager screen....72
UEFI Boot menu....72
Embedded systems management....72
iDRAC settings utility....72
Entering the iDRAC settings utility....72

Chapter 10: Troubleshooting and frequently asked questions....73
Error messages....73
Frequently asked questions....73

1

Introduction

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

Lifecycle Controller has the following components:

- GUI:
  - Is an embedded configuration utility that resides 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.
  - Enables server and storage management tasks from an embedded environment throughout the life cycle of the server.
- Remote Services (WS-Man and iDRAC RESTful API with Redfish) simplify end-to-end server life cycle management by using the one-to-many method. It can be accessed over the network by using the secure web services interfaces and can be used by applications and scripts. Also, it provides a single view of all the system settings that can be imported and exported from the server to perform one-to-many cloning operations. For more information about remote services features, see *Lifecycle Controller Remote Services Quick Start Guide* available on the iDRAC manuals page..

Topics:

- Advantages of using Lifecycle Controller
- Benefits of using iDRAC with Lifecycle Controller
- Key features
- Licensable features in Lifecycle Controller
- Viewing iDRAC license information
- Other documents you may need
- Accessing documents from the Dell Support site
- Contacting Dell

Advantages of using Lifecycle Controller

The iDRAC with Lifecycle Controller technology in the server's embedded management allows you to perform useful tasks such as configuring BIOS and hardware settings, deploying operating systems, changing RAID settings, and saving hardware profiles. Together, iDRAC and Lifecycle Controller provide a robust set of management functions that can be used throughout the entire server lifecycle.

Lifecycle controller simplifies server lifecycle management — from provisioning, deployment, patching and updating to servicing and user customization — both locally and remotely. Lifecycle Controller includes managed and persistent storage that embeds systems management features and Operating System device drivers directly on the server. This eliminates the media-based system management tools and utilities traditionally needed for systems management.

Benefits of using iDRAC 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 number of distant servers can make the 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 — Lifecycle Controller provides deployment and simplified serviceability through the LC GUI for local deployment, Remote Services WS-Man and iDRAC RESTful API with Redfish interfaces for remote deployment integrated with OpenManage Enterprise, OpenManage Essentials, and partner consoles.

For more information on iDRAC, see the Integrated Dell Remote Access Controller User's Guide. For more information on wsman, see *Dell Lifecycle Controller User's Guide* available at iDRAC manuals .

Key features

The key features of Lifecycle Controller are:

- Provisioning—Entire pre-operating system configuration from a unified interface.
- Deploying—Simplified operating system installation with the embedded drivers on Lifecycle Controller. Unattended installation mode is available for Microsoft Windows and Red Hat Enterprise Linux 7 operating systems.
- Download drivers for operating system installation from the Dell Support site.
- Patching or updating — Operating system agnostic, and reduced maintenance downtime with direct access to updates from . It simplifies firmware updates by maintaining a working version for rollback.
- Servicing—Continuous availability of diagnostics without depending on a hard-disk drive. Ability to flash firmware automatically, while replacing components such as a PowerEdge storage controller, NIC, and power supply unit. Support for VLAN in network configuration.
- System erase — Deletes the server and storage-related data on selected components of a server. You can delete information on BIOS, Lifecycle Controller data (LC logs, configuration database and rollback firmware versions), iDRAC settings, and storage components on the server.

  NOTE:
  - You cannot delete the iDRAC license file.
  - Secure erase does not erase iDRAC rollback firmware from the partition when command racadm `systemerase lcdata` is used.

- Security—Support local key encryption.
- Enhanced Security—Support for TLS 1.3, 1.2, and 1.1. To enhance security, default setting is TLS 1.1 and higher.
- Hardware inventory—Provides information about the current and factory system configuration.
- Lifecycle Controller logs for troubleshooting.
- CIFS operations—CIFS operations from LCUI uses SMBv2 protocol but is displayed as CIFS on the GUI.

Licensable features in Lifecycle Controller

Lifecycle Controller features are available based on the type of license (iDRAC Basic, iDRAC Express, iDRAC Express for Blades, iDRAC Enterprise and iDRAC Datacenter) that you purchase. Only licensed features are available in the Lifecycle Controller GUI. For more information about managing licenses, see the Integrated Dell Remote Access Controller User's Guide.The following table lists the Lifecycle Controller features available based on the license purchased.

Table 1. Licensable Features in Lifecycle Controller

Feature	iDRAC Basic	iDRAC Express (Rack and Tower Servers)	iDRAC Express (Blade Servers)	iDRAC Enterprise / Datacenter
Firmware Update	Yes	Yes	Yes	Yes
Secure Enterprise Key Manager	—	—	—	Yes (With SEKM license)
Operating system deployment	Yes	Yes	Yes	Yes
Device configuration	Yes	Yes	Yes	Yes
Diagnostics	Yes	Yes	Yes	Yes

Table 1. Licensable Features in Lifecycle Controller (continued)

Feature	iDRAC Basic	iDRAC Express (Rack and Tower Servers)	iDRAC Express (Blade Servers)	iDRAC Enterprise / Datacenter
Part replacement	—	Yes	Yes	Yes
Local updates	Yes	Yes	Yes	Yes
Driver packs	Yes	Yes	Yes	Yes
Hardware inventory	Yes	Yes	Yes	Yes
Remote services (through WS-MAN)	Yes	Yes	Yes	Yes
SupportAssist Collection	Yes	Yes	Yes	Yes
Repurpose or retire system	Yes	Yes	Yes	Yes

Viewing iDRAC license information

After you open the **Lifecycle Controller GUI** page, you can view details about the iDRAC installed on a server. To view the iDRAC license information:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. On any page of Lifecycle Controller, click **About** in the upper-right corner.
3. On the **About** page, click **License Information**.
   The following information is displayed on the **iDRAC License Report** page:

Table 2. : License Information

Field	Description
Device ID	Indicates the Service Tag of the server on which iDRAC is installed.
License	• **Entitlement ID** — Indicates a unique ID provided by the manufacturer. • **Status** — Indicates the status of the installed license. • **Description** — Indicates the license details. • **License Type** — Indicates the type of license of the device. For example, Evaluation, Evaluation Extension, or Perpetual. • **Expiration** — Indicates the date and time at which the license expires.

Other documents you may need

In addition to this guide, you can access the following guides available at Dell Manuals page.

- The **Lifecycle Controller Online Help** provides detailed information about the fields available on the UI and the descriptions for the same. To view the online help information, click **Help** in the upper-right corner of all Lifecycle Controller pages, or press <F1>.
- The **Lifecycle Controller Release Notes** is available from within the product. To read through the Release Notes within Lifecycle Controller, click **About** in the upper-right corner, and then click **View Release Notes**. A web version is also given to provide last-minute updates to the system or documentation or advanced technical reference material that is intended for experienced users or technicians.
- This document provides an overview of iDRAC digital licensing and how it is different from iDRAC available in the PowerEdge servers. It also provides an understanding on iDRAC Express and Enterprise value offerings.
- The **Lifecycle controller Remote Services For PowerEdge Servers Quick Start Guide** provides information about using remote services.

- The **Systems Management Overview Guide** provides brief information about the various Dell software available to perform systems management tasks.
- The **Integrated Dell Remote Access Controller (iDRAC) User's Guide** provides information about configuring and using an iDRAC 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 consisted 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 target systems.
- The **PowerEdge RAID Controller (PERC) 9 User's Guide** provides specification and configuration-related information about the PERC 9 controllers.
- The **Glossary** provides information about the terms that are used in this document.
- The **OpenManage Server Update Utility User's Guide** provides information about using the DVD-based application for identifying and applying updates to the system.

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. 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.**

Social Media Reference

To know more about the product, best practices, and information about Dell solutions and services, you can access the social media platforms such as Dell TechCenter and YouTube. You can access blogs, forums, white papers, how-to videos, and so on from the Lifecycle Controller knowledge base at iDRAC9_support.

For Lifecycle Controller documents and other related firmware documents, see ESM Manuals.

Accessing documents from the Dell Support site

Click the following links to access the documents from the Dell Support site:

- Enterprise Systems Management and OpenManage Connections documents
- OpenManage documents
- iDRAC and Lifecycle Controller documents
- Serviceability Tools documents
- Client Command Suite Systems Management documents

Accessing documents using the product search

1. Go to the Dell support site.
2. In the **Enter a Service Tag**, **Serial Number...** search box, type the product name. For example, **PowerEdge** or **iDRAC**. A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **DOCUMENTATION**.
5. Click **MANUALS AND DOCUMENTS**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to Dell support.
2. Click **Browse all products**.

3. Click the required product category, such as Servers, Software, Storage, and so on.
4. Click the required product and then click the version if applicable.

   NOTE: For some products, you may have to navigate through the subcategories.

5. Click **DOCUMENTATION**.
6. Click **MANUALS AND DOCUMENTS**.

Contacting Dell

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

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

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

2

Using Lifecycle Controller

This section provides information about starting, enabling, and disabling Lifecycle Controller. Before using Lifecycle Controller, make sure that the network and iDRAC are configured. For more information, see the **Integrated Dell Remote Access Controller User's Guide** at ESM Manuals.

NOTE: Certain operations done in the iDRAC can cause **Reset To Defaults** operation initiated from the LCUI to not be allowed. Examples: iDRAC firmware update, ISM install from iDRAC GUI, or any MASER operation that utilizes the scratchpad (200+MB partition) for temporary storage.

Topics:

- Starting Lifecycle Controller
- Using Lifecycle Controller for the first time
- Lifecycle Controller features

Starting Lifecycle Controller

To start Lifecycle Controller, restart the system and press **<F10>** during POST to select Lifecycle Controller from the list displayed. When Lifecycle Controller is started for the first time, it displays the **Initial Setup** wizard that allows you to configure the preferred language and network settings.

NOTE: If the system does not start Lifecycle Controller, see Start messages during POST, causes, and resolutions.

Start messages during POST, causes, and resolutions

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

Table 3. Start messages during POST, 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 power is connected to the system. ○ The system is restarted immediately after resetting iDRAC. ○ Lifecycle Controller is manually disabled	Wait for a minute after resetting iDRAC to restart the system, so that iDRAC initializes. Press <F2> during POST, select **System Setup** > **iDRAC Settings** > **Lifecycle Controller** > **Enable.**
Lifecycle Controller in Recovery mode	• The embedded device that has a backup of the product may contain corrupted data. • Ungracefully exits Lifecycle Controller for three consecutive times if one of the following conditions occur: ○ 3 consecutive unsuccessful attempts to enter Lifecycle Controller GUI.	Enable Lifecycle Controller. For more information, see Enabling Lifecycle Controller

Table 3. Start messages during POST, cause, and resolution (continued)

Message	Cause	Resolution
	○ 3 consecutive unsuccessful attempts to complete inventory collection. ○ 3 consecutive unsuccessful attempts to perform tasks in Automated Task applications.	
Lifecycle Controller not available	Another process is using iDRAC.	Wait for 30 minutes for the current process to complete, restart the system, and then retry. You can use the iDRAC GUI to check the job queue and the status.

Enabling Lifecycle Controller

To enable access to Lifecycle Controller during system startup:

1. Press **<F2>** during POST.
   The **System Setup Main Menu** page is displayed.
2. Select **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Select **Lifecycle Controller**.
4. Under **Lifecycle Controller**, select **Enabled**.
5. On the **System Setup Main Menu** page, select **Finish** to save the settings.
6. Select **Yes** to restart the system.

Disabling Lifecycle Controller

To disable access to Lifecycle Controller at system startup:

1. Press **<F2>** during POST.
   The **System Setup Main Menu** page is displayed.
2. Select **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Select **Lifecycle Controller**.
4. Under **Lifecycle Controller**, select **Disabled**.
5. On the **System Setup Main Menu** page, select **Finish** to save the settings.
6. Select **Yes** to restart the system.

Canceling Lifecycle Controller actions

If Lifecycle Controller causes the system to restart twice, cancel the Lifecycle Controller actions. However, if Lifecycle Controller causes the system to restart the third time, the message `Lifecycle Controller update required` is displayed, you must enable Lifecycle Controller. For more information on enabling Lifecycle Controller, see Enabling Lifecycle Controller.

CAUTION: This action cancels all tasks that are being performed by Lifecycle Controller. It is recommended that you cancel the Lifecycle Controller actions only when absolutely necessary.

1. Press **<F2>** during POST.
   The **System Setup Main Menu** page is displayed.
2. In the **System Setup Main Menu** page, select **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
3. Select **Lifecycle Controller**.
4. Under **Cancel Lifecycle Controller Actions**, select **Yes**.

5. On the **System Setup Main Menu** page, select **Finish** to save the settings.
6. Select **Yes** to restart the system.

Using Lifecycle Controller for the first time

After you start Lifecycle Controller for the first time, by default the **Initial Setup Wizard** page is launched.

Use this wizard to set up the **Language** ,**Keyboard Type**, **Network Settings**, and **iDRAC Network and Credentials**.

Setting up Lifecycle Controller using Initial Setup Wizard

Use the **Initial Setup Wizard** to select the language and default keyboard settings, configure network settings, iDRAC network and credential configuration, and view the summary of the settings.

Specifying language and keyboard type

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. On the left pane, click **Settings**.
3. On the **Settings** pane, click **Language and Keyboard**. Use the up-and down-arrow keys to select options.
   - From the **Language** drop-down menu, select the language.
   - From the **Keyboard Type** drop-down menu, select the keyboard type.
4. Click **Next** to save the new settings.

Viewing Product Overview

Use this page to see the overview of Lifecycle Controller and iDRAC. Click **Next** to continue.

NOTE: For more information about the product, scan the QR code provided on this page by using a supported QR reader or scanner and navigate to iDRAC Manuals.

The **Lifecycle Controller Network Settings** page is displayed.

Configuring Lifecycle Controller Network Settings

Use this page to configure network settings for a NIC.

1. Start Lifecycle Controller. For more information, seeStarting Lifecycle Controller.
2. On the left pane, click **Settings**.
3. On the **Settings** pane, click **Network Settings**.
4. From the **NIC Card** drop-down menu, select the NIC port that you want to configure.

   NOTE: You can use only one NIC at a time to communicate with the network.

5. From the **IPV4 Network Settings→ IP Address Source** drop-down menu, select one of the following options:
   - **DHCP** — indicates that the NIC must be configured by using an IP address from a DHCP server. DHCP is the default option and the DHCP IP address is displayed on the **Network Settings** page.
   - **Static IP** — indicates that the NIC must be configured by using a static IP. Type the **IP Address Properties** — **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Address**. If you do not have this information, contact your network administrator.
   - **No Configuration** — indicates that the NIC must not be configured.
6. From the **IPV6 Network Settings→ IP Address Source** drop-down menu, select one of the following options:
   - **DHCPv6** — indicates that the NIC must be configured by using an IP address from a DHCPv6 server. If DHCPv6 is selected, a DHCPv6 IP address is displayed on the **Network Settings** page.

     NOTE: While configuring DHCP server with IPv6, the configuration fails if you disable forwarding or advertising options.

- **Static IP** — indicates that the NIC must be configured by using a static IP. Type the **IP Address Properties** — **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Address**. If you do not have this information, contact your network administrator.

  NOTE: When you configure a static IPv6 address, the address remains visible after changing the **IP Address Source** to **No Configuration**. To clear the static IPv6 address, switch the **IP Address Source** to **DHCPv6** and enable the system to obtain an IP address. Then, revert to **No Configuration**. This behavior is expected and does not affect functionality.

7. Click **Enabled** and type the **VLAN ID** and **Priority** under **Lifecycle Controller VLAN Settings** to configure the VLAN settings of a NIC.
8. Click **Next**.

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

   NOTE: If you are unable to connect to a network, verify the settings. For information about correct network settings, contact your network administrator.

Configuring iDRAC Network and Credentials

Use this page to configure remote access parameters for iDRAC.

1. From the **IP Address Source** menu, select one of the following options:
   - **Static** — indicates that the network must be configured by using a static IP. Type the IP Address Properties such as **IP Address, Subnet Mask, Default Gateway, DNS Address Source, and DNS Address.** If you do not have this information, contact your network administrator.
   - **DHCP** — indicates that the NIC must be configured using an IP address from a DHCP server. DHCP is the default option and the DHCP IP address is displayed on the **Network Settings** page.
2. Enter the following credentials:
   - **Account Username**— The user name to access iDRAC network
   - **Password**— The password to access iDRAC network
   - **Confirm Password**— The password to access iDRAC network
3. Click **Next**

Recommended characters in user names and passwords

This section provides details about the recommended characters while creating and using user names and passwords.

Use the following characters while creating user names and passwords:For recommended characters while accessing network shares, see Recommended characters while accessing network shares.

Table 4. Recommended characters for user names

Characters	Length
• 0-9 • A-Z • a-z • - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-16

Table 5. Recommended characters for passwords

Characters	Length
• 0-9 • A-Z • a-z • ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-20

NOTE: You may be able to create user names and passwords that include other characters. However, to ensure compatibility with all interfaces, Dell recommends using only the characters listed here.

NOTE: To improve security, it is recommended to use complex passwords that have 8 or more characters and include lower-case alphabets, upper-case alphabets, numbers, and special characters. It is also recommended to regularly change the passwords, if possible.

Table 6. Recommended characters while accessing network shares

Characters	Length
• 0-9 • A-Z • a-z • - * / : ? @ \ _ |	• User name: 1-16 • Password: 1-20

Viewing summary of network settings

This page provides a summary of the Lifecycle Controller and iDRAC IP configurations. Verify the configurations and click **Finish** to save the settings and exit from the Settings wizard.

Accessing help

Each Lifecycle Controller page has a help associated with it. Press **<F1>** or click **Help** (in the upper-right corner) to view the help information about the features available on a page.

Viewing release notes

1. To view the release notes, click **About** on any page of Lifecycle Controller.

   NOTE: The **About** option is not available from the help pages.

2. Click **View Release Notes**.

Setting up Lifecycle Controller from the home page

If you miss to make any changes in the **Initial Setup Wizard**, or if you want to make any configuration changes later, restart the server, press F10 to launch Lifecycle Controller, and select **Settings** from the home page.

Specifying language and keyboard type

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. On the left pane, click **Settings**.
3. On the **Settings** pane, click **Language and Keyboard**. Use the up-and down-arrow keys to select options.
   - From the **Language** drop-down menu, select the language.
   - From the **Keyboard Type** drop-down menu, select the keyboard type.
4. Click **Next** to save the new settings.

Configuring Lifecycle Controller Network Settings

Use this page to configure network settings for a NIC.

1. Start Lifecycle Controller. For more information, seeStarting Lifecycle Controller.
2. On the left pane, click **Settings**.
3. On the **Settings** pane, click **Network Settings**.
4. From the **NIC Card** drop-down menu, select the NIC port that you want to configure.

NOTE: You can use only one NIC at a time to communicate with the network.

5. From the **IPV4 Network Settings→ IP Address Source** drop-down menu, select one of the following options:
   - **DHCP** — indicates that the NIC must be configured by using an IP address from a DHCP server. DHCP is the default option and the DHCP IP address is displayed on the **Network Settings** page.
   - **Static IP** — indicates that the NIC must be configured by using a static IP. Type the **IP Address Properties** — **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Address**. If you do not have this information, contact your network administrator.
   - **No Configuration** — indicates that the NIC must not be configured.
6. From the **IPV6 Network Settings→ IP Address Source** drop-down menu, select one of the following options:
   - **DHCPv6** — indicates that the NIC must be configured by using an IP address from a DHCPv6 server. If DHCPv6 is selected, a DHCPv6 IP address is displayed on the **Network Settings** page.

     NOTE: While configuring DHCP server with IPv6, the configuration fails if you disable forwarding or advertising options.

   - **Static IP** — indicates that the NIC must be configured by using a static IP. Type the **IP Address Properties** — **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Address**. If you do not have this information, contact your network administrator.

     NOTE: When you configure a static IPv6 address, the address remains visible after changing the **IP Address Source** to **No Configuration**. To clear the static IPv6 address, switch the **IP Address Source** to **DHCPv6** and enable the system to obtain an IP address. Then, revert to **No Configuration**. This behavior is expected and does not affect functionality.

7. Click **Enabled** and type the **VLAN ID** and **Priority** under **Lifecycle Controller VLAN Settings** to configure the VLAN settings of a NIC.
8. Click **Next**.

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

   NOTE: If you are unable to connect to a network, verify the settings. For information about correct network settings, contact your network administrator.

Lifecycle Controller features

This section provides a brief description about the Lifecycle Controller features and helps you understand how to use the Lifecycle Controller wizards most effectively. Each feature is a wizard in Lifecycle Controller, which supports the following tasks:

- **Home** — Navigate back to the **Home** page.
- **Lifecycle Log** — View and export the Lifecycle Controller log, and add a work note to the log.
- **Firmware Update** — Apply updates or perform firmware rollback for the system components, and view the firmware version available on a server.
- **Hardware Configuration** — Configure, view, or export the hardware inventory of a system, and repurpose or retire a system.
- **OS Deployment** — Install an operating system in manual mode or unattended mode by using an answer file.
- **Hardware Diagnostics** — Perform diagnostics to validate the memory, I/O devices, CPU and physical disks and export support assist report and other peripherals.
- **Settings** — Specify the language, keyboard layout, and network settings while using Lifecycle Controller.
- **System Setup** — Configure settings for devices or components such as iDRAC, BIOS, RAID, and NIC.

3

Operating system deployment

The **OS Deployment** feature allows you to deploy standard and custom operating systems on the managed system. You can also configure RAID before installing the operating system if it is not already configured.

Lifecycle Controller allows deploying the operating system using the following options:

- Manual installation
- Unattended installation. For more information on unattended installation, see Unattended installation
- UEFI Secure Boot. For more information on UEFI Secure Boot, see UEFI Secure Boot

NOTE: Driver packs are available for the deployment of Windows and Linux operating systems supported by Lifecycle Controller. Before deploying these operating systems, make sure that Lifecycle Controller is updated with the latest driver packs. You can download the latest drivers pack from Dell Support page.

NOTE: When drivers are mounted from driver pack using iDRAC/RACDM/WSMAN or other interfaces, you can not launch LC UI or it may not be available.

NOTE: FAT32 limits the size of a single file to 4 GB. If you are using a Windows image file that is more than 4 GB, split the file in to multiple files. For more information see the documentation available at **Docs.microsoft.com**.

NOTE: UEFI environment doesn't support NTFS file format. USB Boot Media must be MBR disk with FAT32 filesystem.

Once a Lifecycle Controller job such as OS Deployment, System configuration job, etc is triggered, then no other LC job like BIOS config job is allowed to perform. Before initiating any LC job, please check the status using the command `racadm getremoteservicesstatus`. The LC Status output of the command must show **Ready** in order to proceed.

Topics:

- Installing an operating system
- Using the optional RAID configuration
- Configuring RAID using the operating system deployment wizard
- Unattended installation
- UEFI Secure Boot
- Driver access
- Installing an operating system on iSCSI LUN and FCoE LUN
- Post reboot scenarios

Installing an operating system

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

- Optical DVD drive, virtual media, RFS, or a bootable USB drive is connected to a server.
- Software RAID or PowerEdge RAID controller is installed with the latest firmware, and at least two hard-disk drives are available for creating the virtual disk. For information about the supported controllers and related firmware, see the operating system documentation.

  NOTE: You can install the operating system on media such as Dual SD or PCIe SSD. However, RAID configuration is not supported on these media. This option is not available on servers with iDRAC 5.00.00.00 and above.

- For installing an operating system in an unattended mode, make sure that you copy the required configuration file (**autounattend.xml** for Windows and **ks.cfg** for RHEL 7) to a USB or network share.
- Ensure the Lifecycle Controller Operating System Driver pack is installed.

To install an operating system:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
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** — Click to configure a RAID connected to the server. For information about configuring a RAID, see Using the optional RAID Configuration .

     NOTE: Configuring RAID is optional if an already-connected virtual disk is present.

   - **Go Directly to OS Deployment** — Click to launch the operating system deployment wizard and start installing an operating system.
4. On the **Select an Operating System** page, select the following and click **Next**:
   - **Boot Mode** — Choose either **UEFI** or **BIOS** boot mode depending on the boot configuration of the system for operating system installation.
   - **Secure Boot** — Allows you to enable or disable the **Secure Boot** option. Click **Enabled** to secure the boot process by checking if the drivers are signed with an acceptable digital signature. This option is available only for the **UEFI** boot mode. For more information about Secure Boot, see UEFI Secure Boot

     NOTE: The **Secure Boot** option is available only if the **Load Legacy Video Option ROM** setting is set to disabled. To disable the Load Legacy Video Option ROM setting, click **System Setup** > **System BIOS Settings** > **Miscellaneous Settings** > **Load Legacy Video Option ROM** > **Disabled.**

   - **Secure Boot Policy** — Allows you to specify the policy or digital signature that BIOS uses to authenticate. By default **Standard** secure boot policy is applied.
     - **Standard** — BIOS uses the default set of certificates to validate the drivers and operating system loaders during the boot process.
     - **Custom** — BIOS uses the specific set of certificates that you import or delete from the standard certificates to validate the drivers and operating system loaders during the boot process.

     NOTE: The secure boot policy settings made on the BIOS can also be changed on the Lifecycle Controller UI.

     NOTE: The **Secure Boot** option is available only if the BIOS of the system supports the feature.

   - **Available Operating Systems** — Displays the list of operating systems depending on the boot mode selected. Select the operating system to install on the server. The drivers pack for deploying the Windows and Linux operating systems that are supported by Lifecycle Controller are available and extracted to a local repository (OEMDRV). These driver packs contain the drivers required for installing an operating system.

     NOTE: If you select **Any Other Operating System** option, make sure that you have prepared the necessary drivers for your system. See Dell Support page for more information about operating system installation images and drivers for these operating systems.

5. On the **Select Installation Mode** page, select any one of the following:
   - **Unattended Install**
   - **Manual Install**

   NOTE: The **Unattended Install** option is enabled only if the operating system is compatible for an unattended installation. If the operating system is not compatible, the option is grayed out. For more information about unattended install mode, see Unattended installation.

   NOTE: A detailed procedure for installing an operating system using the unattended installation mode is provided in the video about unattended installation of an operating system on YouTube .

6. On the **Select Installation Mode** page, select or enter the appropriate data to import the operating system configuration file and then click **Next**. For more information about the fields available on the **Select Installation Mode** page, see the online help by clicking **Help** in the upper-right corner of the Lifecycle Controller UI.
7. On the **Select OS Media** page, insert the appropriate operating system media and click **Next**.

   Lifecycle Controller validates the media and displays an error message if the verification process is not successful. The verification may be unsuccessful if:

   - An incorrect operating system media is inserted.
   - An operating system media is damaged or corrupted.
   - The optical drive in the system cannot read the media.

8. On the **Reboot the System** page, the summary of selections is displayed. Verify the selections and click **Finish**.
   The system reboots and starts the operating system installation. For more information about the post-reboot scenarios, see Post reboot Scenarios

Using the optional RAID configuration

When you install an operating system, you can:

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

Alternatively, you can configure RAID through the RAID configuration page from the **Hardware Configuration** > **Configuration Wizards** > **RAID Configuration**.

Configuring RAID using the operating system deployment wizard

To configure RAID using the **OS Deployment** page:

NOTE: If the system has a RAID controller, you can configure a virtual disk as the boot device. Create boot virtual disk only from disk drives populated across 0–3 of the system. For slot information, see the system Owner's Manual at Dell Support page.

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **OS Deployment**.
3. On the **OS Deployment** page, click **Deploy OS**.
4. On the **Deploy OS** page, click **Configure RAID First**, and then click **Next**.
   The storage controllers available for configuration are displayed in the **RAID Configuration** page.
   NOTE: Make sure that the selected controller is not in a non-RAID mode.
5. Select a storage controller.
   The RAID configuration options are displayed.
6. Follow the instruction on the screen, complete the RAID setting tasks, and then click **Finish.**
   The RAID configuration is applied to the virtual disks, and the **Select an Operating System** page is displayed. You can proceed with installing the operating system. For information on installing the operating system, see Installing an Operating System.

Unattended installation

An unattended installation is a scripted operating system installation process that allows you to install an operating system using the configuration file with minimal intervention. A scripted configuration file that contains the desired operating system setting information is required for this option. The **Unattended Install** option is available only if the operating system that you have selected for installation is compatible for an unattended installation. To deploy an operating system using the unattended mode, see Installing an operating system

You can also see the **Unattended Installation of operating systems from Lifecycle Controller on PowerEdge Servers** white paper at Dell TechCenter.

NOTE: The unattended installation feature is supported only for the Microsoft Windows and Red Hat Enterprise Linux version 6.9 and 7 onwards. If you select any other operating systems, the **Unattended Install** option is grayed out.

UEFI Secure Boot

The UEFI Secure Boot is a technology that secures the boot process by verifying if the drivers and operating system loaders are signed by the key that is authorized by the firmware. When enabled, Secure Boot makes sure that:

- BIOS boot option is disabled.

- Only UEFI-based operating systems are supported for operating system deployment in all management applications.
- Only authenticated EFI images and operating system loaders are started from UEFI firmware.

You can enable or disable the Secure Boot attribute locally or remotely using Dell management applications. Lifecycle Controller supports deploying an operating system with the Secure Boot option only in the UEFI boot mode.

There are two BIOS attributes that are associated with Secure Boot:

- **Secure Boot**—Displays if the **Secure Boot** is enabled or disabled.
- **Secure Boot Policy**—Allows you to specify the policy or digital signature that BIOS uses to authenticate. The policy can be classified as:
  - **Standard**—BIOS uses the default set of certificates to validate the drivers and operating system loaders during the boot process.
  - **Custom**—BIOS uses the specific set of certificates that you import or delete from the standard certificates to validate the drivers and operating system loaders during the boot process.

  NOTE: The secure boot policy settings made on BIOS can also be changed on the Lifecycle Controller GUI.

NOTE: For more information on UEFI, go to **uefi.org**.

Driver access

Lifecycle Controller provides a local repository for drivers that are required for installing the operating system. Based on the operating system you want to install, the **OS Deployment** wizard extracts these drivers and copies them to a temporary directory (OEMDRV) on the managed system. These files are deleted after 18 hours or when you:

- Refresh the AC power cycle, which resets the iDRAC.
- Press **<F2>** select iDRAC Settings or Lifecycle Controller to cancel the Lifecycle Controller actions.

NOTE: Before installing an operating system, make sure that Lifecycle Controller is updated with the latest driver packs. You can download the latest Lifecycle Controller drivers at Dell Support page.

Installing an operating system on iSCSI LUN and FCoE LUN

Install an operating system on an iSCSI LUN and FCoE LUN by using the **System Setup** page.

Post reboot scenarios

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

Table 7. Post reboot scenarios

Scenario	User Action and Impact
During POST, the system prompts you to press a key to boot to the operating system installation media.	Press any key to begin the operating system installation; else, the system boots to the hard-disk drive and not the operating system installation media.
Operating system installation is interrupted and the system restarts before the installation is completed.	The system prompts you to press a key to boot from the operating system installation media.
Cancel operating system installation.	Press **<F10>**. **NOTE:** If you press **<F10>** during the installation process or a restart, the drivers provided by the operating system deployment wizard are removed.
During the 18-hour period when drivers are extracted to a temporary location after the operating system is installed, you cannot update the component firmware	Lifecycle Controller does not allow DUP after the operating system installation. However, if you disconnect the power supply to the managed system, the OEMDRV directory is erased.

Table 7. Post reboot scenarios (continued)

Scenario	User Action and Impact
using a DUP. If you attempt a DUP through the operating system during this time period, the DUP displays a message that another session is active.	

4

Monitor

Using Lifecycle Controller, you can monitor the hardware inventory and events of a server throughout its life cycle.

Topics:

- Hardware inventory view and export
- About view and export current inventory
- About view and export factory-shipped inventory
- Viewing hardware inventory — current or factory shipped
- Exporting hardware inventory — current or factory shipped
- Viewing or exporting hardware inventory after part replacement
- Viewing or exporting current inventory after resetting Lifecycle Controller
- Lifecycle Controller log

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 information about the installed hardware components that are internal to the system chassis and the configuration for each component. All the installed hardware components such as fans, PCI devices, NICs, DIMMs, PSU, and their properties and values are displayed. You can export this information from a JSON file to a USB drive or network share. The JSON file is saved in the following format: `HardwareInventory_<servicetag>_<timestamp>.json`.

For more information about 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 a system erase. For viewing the correct inventory data, see Viewing and Exporting Current Inventory After Resetting Lifecycle Controller.

NOTE: The inventory that is displayed in the Lifecycle Controller GUI may not be the same as that of any iDRAC interfaces. To get the updated inventory, run the CSIOR, wait for 2 minutes, reboot the host, and then enter the LCUI.

NOTE: Some attributes like Primary status/Rollup status might show as **Unknown** while collecting inventory data from LCUI. This is expected based on the availability of RTCEM inventory.

About view and export factory-shipped inventory

You can view information about the factory-installed hardware components and their configuration. You can export this information in an XML format to a USB drive or a network share. The XML file is saved in this format: `FactoryShippedHWInventory_<servicetag>.xml`.

For more information about 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 the **Repurpose or Retire System** option is selected, which permanently deletes the factory-shipped inventory.

Viewing hardware inventory — current or factory shipped

NOTE: For factory-shipped inventory, the status of few parameters for the installed components is displayed as **Unknown**.

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

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Hardware Inventory**.
4. To view the current- or factory-shipped inventory, click **View Current Inventory** or **View Factory Shipped Inventory** respectively.
   A list of hardware components are displayed on the **View Current Hardware Inventory** page.
   NOTE: Lifecycle Controller does not provide the driver version for the RAID controller. To view the driver version, use iDRAC, OpenManage Server Administrator Storage Service, or any other third-party storage management application.
5. Select from the **Filter by Hardware Component** drop-down menu to filter the components. The Fully Qualified Device Descriptor (FQDD) property of a component is also listed along with other properties of a hardware component.
   NOTE: You can also filter data by a FQDD property of the hardware component. By default, the **FQDD Device Description** property value is displayed for every hardware component listed.

Exporting hardware inventory — current or factory shipped

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

- If you use the network share (shared folder), configure the **Network Settings**. For more information, see Configuring Network for a NIC.
- If you are storing the exported file on a USB drive, make sure that a USB drive is connected to the managed system.

To export the current or factory-shipped hardware inventory:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Hardware Inventory**.
4. Click **Export Current Inventory** or **Export Factory Shipped Hardware Inventory**.
5. If you are exporting the inventory to a local USB drive, select **USB Drive**. If you are exporting the file to a shared folder on a network, select **Network Share**.

   For more information, see Exporting hardware inventory to a USB drive or Exporting hardware inventory to network share

   To verify that using Lifecycle Controller, you can connect to the IP address, click **Test Network Connection**. Using Lifecycle Controller you can ping the Gateway IP, DNS server IP, and the host IP.
   NOTE: If the domain name is not resolved in the DNS, then you cannot use Lifecycle Controller to ping the domain name and view the IP address. Make sure that the DNS issue is resolved, and then retry.
6. Click **Finish** to export the inventory.
   The **HardwareInventory _<servicetag>_<timestamp>.xml** or **FactoryShippedHWInventory_<servicetag>.xml** file is copied to the specified location. For the current inventory, the time stamp is in the format **yyyy-mm-ddthh:mm:ss**, where 't' indicates time.
   NOTE: For factory-shipped inventory, the status of few parameters for the installed components is displayed as **Unknown**.

Exporting hardware inventory to a USB drive

To export hardware-related inventory to a USB drive:

1. From the **Select Device** drop-down menu, select a USB drive.
2. Click **Browse**, and in folder selection widget, select the folder path where the file is stored in the root location of the device.

Exporting hardware inventory to network share

To export to a network share, select **CIFS**, **NFS**, **HTTP**, or **HTTPS** and type the required details.

CIFS

1. **Share Name**—Type the server IP or host name followed by the root of the network share. Examples: **\ \192.168.0.120\sharename** or **\\hostname\sharename**.
2. **Domain and User Name**—Type the domain and user name required to log in the network share. If there is no domain, type the user name.
3. **Password**—Type the correct password.
4. **File Path**—Type the sub-directories, if any. For example, 2015\Nov.

   NOTE: The following characters are supported for user name and password:
   - Digits (0–9)
   - Alphabets (a-z, A-Z)
   - Special Characters (-, _.)

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

NFS

For NFS, type the following details:

1. **Share Name**—Type the server IP or hostname followed by the root of the network share. Examples: **\ \192.168.0.120\sharename** or **\\hostname\sharename**
2. **File Path**—Type the subdirectories path, if any. For example, 2015\Nov.

   The examples that are provided for **Share Name** and **File Path** are in the correct format even though it does not follow the mount behavior for NFS shares.

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

HTTP and HTTPS

For HTTP/HTTPS, type the following details:

1. **Share Name/Address**—Type the IP address of the local HTTP/HTTPS server. Examples: **\\192.168.0.120** or **IP address**
2. **File Path**—Type the subdirectories path, if any.

Viewing or exporting hardware inventory after part replacement

To view or export the hardware inventory after part replacement:

1. Start Lifecycle Controller. For more information, see Starting 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. Restart the server and relaunch Lifecycle Controller.
6. On the **Hardware Inventory** page, click **View Current Hardware Inventory** to view the latest inventory, or click **Export Current Inventory** to export the latest inventory to an external location.

Viewing or exporting current inventory after resetting Lifecycle Controller

NOTE: The system automatically turns off after you select the **Repurpose or Retire System** option.

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

1. Turn on the system and wait for a few minutes for iDRAC to start functioning.
2. Press **<F10>** during POST to start Lifecycle Controller and the system inventory is collected as Collect System Inventory On Restart (CSIOR) is enabled by default.
3. After Lifecycle Controller starts, click **Hardware Configuration** > **View Current Hardware Inventory** or **Export Current Hardware Inventory** to view or export current hardware inventory respectively. If the following message is displayed, click **No**, reboot the system, and then 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?
   ```

Lifecycle Controller log

Lifecycle Controller Log provides a record of past activities on a managed system. Using the **Lifecycle Log** wizard, you can view and export life cycle log, and add a work note to a log history. The log contains the following:

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

NOTE: If you initiate configuration jobs using RACADM CLI or iDRAC web interface, the Lifecycle log displays information about the user, interface used, and the IP address of the system from which you initiate the job.

Viewing Lifecycle Log history

Use the **Lifecycle Log** feature to view:

- System event logs
- History of firmware updates

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

- User work notes

You can use the filtering and sorting options to view the Lifecycle Log.

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

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

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Lifecycle Log**.
3. In the right pane, click **View Lifecycle Log History**.
   The following details are displayed:

- **No.** — The serial number of the event.
- **Category** — The category to which the events belong. The available categories are:
  - **All** — Events related to all categories are listed.
  - **System Health** — Events related to the installed hardware such as fan, PSUs, NIC/LOM/CNA link, BIOS errors, and so on.
  - **Storage** — Events related to the external or internal storage components such as storage controller, enclosure, HDDs, and software RAID.
  - **Configuration** — Events related to the hardware and software changes such as addition or removal of hardware in the system, configuration changes made using Lifecycle Controller or system management tools.
  - **Audit** — Events related to a user login, intrusion, licenses, and so on.
  - **Updates** — Events related to updates or rollback of firmware and drivers.
  - **Work Notes** — Events logged by you.

    NOTE: These options are available in the **Filter by Category** drop-down menu. Select the category to filter the data depending on the category option selected.
- **Severity**
  - **Critical** — Indicates the events that are business-critical.
  - **Informational** — Indicates the events that are generated only for information purpose.
- **Message ID** — Each event is represented with a unique Message ID. For example, SWC0001.
- **Description** — A brief description about the event. For example, `Dell OS Drivers Pack, v.6.4.0.14, X14 was detected`.

  NOTE: If you initiate configuration jobs using RACADM CLI or iDRAC web interface, the Lifecycle log description displays the information about the user, interface used, and the IP address of the system from which you initiate the job.
- **Date and Time** — Indicates the date and time when an event occurred.

4. You can also view feature specific logs using the filter option. For viewing logs for specific category (Power Supply, Audit, Storage, Updates etc), select the required category from the **Filter by Category** drop down. For further more filtering of the feature (CPU, Slot number, BIOS etc), you can use **Keyword Search** option.

Exporting Lifecycle Log

Use the **Export Lifecycle Log** feature to export the Lifecycle Log information to a compressed file (.gz format) that has log files in an .xml file. You can save the XML file in a USB drive or on a network share. For more information about the schema, see en.community.dell.com/techcenter/extras/m/white_papers/20270305 . Before exporting the Lifecycle Log, make sure that the following prerequisites are met:

- To export the file to a USB drive, make sure that a USB drive is connected to the managed server.
- To export the file to a network share (shared folder), set the correct network settings. For more information, see Configuring Network Settings for a NIC.

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

NOTE: The log data is exported to a compressed file (.gz format) only if iDRAC version 1.50.50 or later is installed. Else, the data is exported as an .xml file.

To export the Lifecycle Log:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller
2. In the left pane, click **Lifecycle Log**.
3. In the right pane, click **Export Lifecycle Log**.
4. Select either **USB Drive** or **Network Share**.
   For more information, see Exporting hardware inventory to a USB drive or Exporting hardware inventory to network share

   When you select **Network Share**, to verify connection, click **Test Network Connection**. Lifecycle Controller pings the Gateway IP, DNS server IP, and host IP.

NOTE: Lifecycle Controller cannot ping the domain name and cannot display the 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.

Exporting Lifecycle Log to a USB drive

To export the Lifecycle Log to a USB drive:

1. From the **Select Device** drop-down menu, select a USB drive.
2. Click **Browse** , to select the respective folder where the file is stored.

For example, **Logs\LCLogs**.

NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

Exporting Lifecycle Log to network share

To export to a network share, select **CIFS**, **NFS**, **HTTP**, or **HTTPS** and type the necessary details.

CIFS

1. **Share Name**—Type the server IP or host name followed by the root of the network share. Examples: **\ \192.168.0.120\sharename** or **\\hostname\sharename**.
2. **Domain and User Name**—Type the domain and user name required to log in the network share. If there is no domain, type the user name.
3. **Password**—Type the correct password.
4. **File Path**—Type the sub-directories, if any. For example, 2015\Nov.

   NOTE: The following characters are supported for user name and password:
   - Digits (0–9)
   - Alphabets (a-z, A-Z)
   - Special Characters (-, _.)

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

NFS

For NFS, type the following details:

1. **Share Name**—Type the server IP or hostname followed by the root of the network share. Examples: **\ \192.168.0.120\sharename** or **\\hostname\sharename**
2. **File Path**—Type the subdirectories path, if any. For example, 2015\Nov.
   The examples that are provided for **Share Name** and **File Path** are in the correct format even though it does not follow the mount behavior for NFS shares.

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

HTTP and HTTPS

For HTTP/HTTPS, type the following details:

1. **Share Name/Address**—Type the IP address of the local HTTP/HTTPS server. Examples: **\\192.168.0.120** or **IP address**
2. **File Path**—Type the subdirectories path, if any.

Adding a work note to the Lifecycle Log

You can add a work note to the Lifecycle Log to record comments for your reference. You can enter comments such as scheduled downtime or changes made by administrators who work in different shifts for later reference.

NOTE: You can type a maximum of 50 characters in the **Lifecycle Log** field. The special characters such as <, >, &, and % are not supported.

To add a work note:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Lifecycle Log**.
3. In the right pane, click **Add a work note to Lifecycle Log**.
4. In the **Enter a work note** field, enter the comments and click **OK**.

5

Firmware update

With Lifecycle Controller, the system can be updated using the repositories accessible through FTP, a network share or on a locally attached USB drive or a DVD. Use the **Firmware Update** page to:

- View the current version of the installed applications and firmware.
- View a list of available updates.
- Select the required updates, downloads (automatic), and then apply the updates to the following components listed in the table:

NOTE: When you update the firmware on a BCM57xx and 57xxx adapters, you notice that the cards are displayed as QLogic. This is due to the acquisition of Broadcom NetXtreme II by QLogic.

The following table lists the components that support the **Firmware Update**feature:

NOTE: When multiple firmware updates are applied through out-of-band methods or using the Lifecycle Controller UI, the updates are ordered in the most efficient possible manner to reduce unnecessary restarting of a system.

NOTE: Firmware update for SAS and SATA hard drives or solid state drives is not supported from the Lifecycle Controller GUI.

NOTE: When a firmware update is in progress, do not reboot or shutdown or AC power cycle the host or iDRAC by any mechanism (manual or "Ctrl+Alt+Del" keys or options provided through iDRAC interfaces). The system (host and iDRAC) should always be rebooted or shutdown gracefully when no tasks/ jobs are running in iDRAC or host. Ungraceful or interrupting an operation can cause unpredictable results such as firmware corruption, generate core files, RSODs, YSODs, error events in LCL, so on.

Table 8. Firmware Update—Supported Components

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?
Diagnostics	No	No
Operating system Driver Pack	No	No
BIOS	Yes	Yes
RAID Controller	Yes	Yes
SAS HBA	Yes (HBA345 and higher)	Yes
Backplanes**	Yes	Yes
Enclosures	Yes	Yes
NIC	Yes	Yes
iDRAC	Yes	Yes
Power Supply Unit	Yes	Yes
CPLD	No	Yes
NOTE: After the CPLD firmware upgrade is complete, iDRAC restarts automatically.		
FC Cards	Yes	Yes
HHHL NVMe adapter	Yes	Yes
NVMe PCIe SSD drives	Yes	Yes
Intel® Optane™ DC Persistent Memory	Yes	No

Table 8. Firmware Update—Supported Components (continued)

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?
CMC*	No	Yes
Operating System Collector	No	No
BOSS	Yes	Yes
NVDIMM	Yes	Yes
Systems Management Application	No	Yes
Storage Enclosure Processor	Yes	Yes
IDSDM	No	Yes
Firmware Inventory/Firmware Version	No	No
NOTE: Since release 5.10.00.00, there is no support for FW version display even for SAS/SATA HDD in LCUI.		
NOTE: Error message may not be proper while updating Pensendo firmware from LCUI.		

* Indicates that though a system restart is not required, iDRAC must be restarted to apply the updates. iDRAC communication and monitoring will temporarily be interrupted.

** The backplanes that cannot be updated are not listed.

***Applicable only for FX2 modular systems.

An expander backplane FW update requires the primary SAS RAID/HBA controller to be enabled. If the controller is disabled via the enable/disable internal RAID controller or the PCI-e slot is disabled at the BIOS level, the backplane FW update job is expected to fail.

The SAS controller must be re-enabled to allow the expander backplane firmware to update successfully. After the update has been applied, the controller can be returned to its previous disabled state.

NOTE: The firmware update is not supported for the following components in LC UI:

- TPM
- GPU
- SAS and SATA
- Software Defined Persistent Memory (SDPM)
- Vault Optimized Storage Solution (VOSS)
- DPU
- FPGA
- Power Distribution Board (PDB) CPLD
- iDRAC SDK plugin

Topics:

- Firmware update methods
- Version compatibility
- Updating firmware
- System Configuration Lockdown mode
- Firmware rollback

Firmware update methods

The following table lists the various locations or media and methods to perform the updates:

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

NOTE: For Dell online catalog update, downloads.dell.com only supports **https** protocol.

Table 9. Firmware update methods

Firmware update methods	
Method	Dell Website
Location	FTP
Methods	• Non-proxy (Internal) • Proxy (Internal)
Media	Local Drive • Dell server Update Utility DVD • USB Drive
Methods	• Virtual Console (Mapped on Client) • Attached Locally

Location	• Network Share
	  ○ CIFS
	  ○ NFS
	  ○ HTTP
	  ○ HTTPS

NOTE: If you select a local drive for updates, you will not get an option to browse the device you have selected. You must know the name or path of the filename before selecting the local drive.

The following table lists the supported interfaces, image-file types, and whether Lifecycle Controller must be in enabled state for the firmware to be updated:

Table 10. Image file types and dependencies

.D9 Image			**iDRAC DUP**	
Interface	**Supported**	**Requires LC enabled**	**Supported**	**Requires LC enabled**
BMCFW64.exe utility	Yes	No	No	N/A
Racadm FWUpdate (old)	Yes	No	No	N/A
Racadm Update (new)	Yes	Yes	Yes	Yes
iDRAC UI	Yes	Yes	Yes	Yes
WSMAN	Yes	Yes	Yes	Yes
In-band OS DUP	No	N/A	Yes	No

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 the update.

Updating firmware

You can update to the latest version of Lifecycle Controller using the **Firmware Update** wizard. It is recommended that you run the **Firmware Update** wizard regularly to access the latest updates. You can update the component firmware by either using update repositories or individual DUPs—single component DUP.

NOTE:

- The firmware for iDRAC and Lifecycle Controller is combined in a single package.
- Make sure that the file name for the single component DUPs does not have any blank space.
- If Collect System Inventory On Restart (CSIOR) is disabled while performing an update, Lifecycle Controller automatically updates the system inventory.
- Both 32–bit and 64–bit DUPs and catalog are supported. If both the 32-bit and 64-bit DUPs are available in a catalog, the 64-bit DUP is preferred for the firmware update. 32-bit DUP is used for firmware update only when 64-bit DUP is not available in a catalog.
- When you check for updates, all compatible versions are listed. Before you install the update, ensure that you select the latest available version and also ensure that it is newer than the version currently installed. If you want to control the version that iDRAC detects, create a custom repository using Dell Repository Manager (DRM) and configure iDRAC to use that repository to check for updates.

NOTE:
- When SEKM mode is enabled on a controller, iDRAC Firmware downgrade/upgrade shall fail when tried from a SEKM to a non-SEKM iDRAC version. iDRAC Firmware upgrade/downgrade shall pass when done within the SEKM versions.
- PERC firmware downgrade to a non-SEKM version shall fail when SEKM encryption mode is enabled on PERC controller.
- SEKM functionalities require iDRAC Datacenter or Enterprise license with SEKM license.

To update the firmware:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Firmware Update**.
3. In the right pane, click **Launch Firmware Update**.
4. Select any one of these update repositories: **FTP Server**, **Local Drive (CD, DVD, or USB)**, or **Network Share (CIFS, NFS, HTTP, or HTTPS)**, and click **Next**.
   The **Enter Access Details** page is displayed.
   NOTE: If you select **FTP Server**, you can verify the connection by clicking **Test Network Connection**. If the domain name is provided, then the server IP address and the domain name is displayed. If proxy IP is provided, then the proxy IP along with the server IP is displayed.

   NOTE: If you select **Network Share (CIFS, NFS, HTTP, or HTTPS)**, you can verify the connection by clicking **Test Network Connection**. By default, Lifecycle Controller pings the host and proxy IP.
5. Type or select the appropriate data.
   NOTE: In the **FilePath** or **Update Package Path** field, you can directly enter the customized name for the catalog file. For example DUP\adc.xml.
6. Click **Next**.
   The **Select Updates** page is displayed with the catalog file, catalog version, and component names for which the updates are available.
7. Select the components that require an update, and then click **Apply**.
   The update process is initiated, and the firmware update is completed. After restart, the system is ready to use.
   NOTE: The system does not restart if operating system driver packs, OS collector tool, or hardware diagnostics are updated.

   NOTE: When applying more than one update, the system may restart between updates. In this case, Lifecycle Controller restarts the server and automatically continues the update process.

   NOTE: iDRAC resets while updating iDRAC. If the iDRAC firmware update is interrupted for any reason, wait for up to 30 minutes before you attempt another firmware update.

   NOTE: After the CPLD firmware is updated on the modular servers, on the **View Current Versions** page, under **Firmware Update**, the firmware update date is displayed as 2000-01-01, regardless of the actual update date. The updated date and time are displayed based on the time zone that is configured on the server.

   NOTE: On a PowerEdge server, if you use Lifecycle Controller to update the Intel network card firmware from version 15.0.xx to 16.5.xx or conversely, reboot the server to view the updated firmware.

   NOTE: If you update the Intel Network Card firmware from version 14.5.x to 16.5.xx or vice versa on a PowerEdge server by using Lifecycle Controller, the **Firmware Rollback** page may display the firmware version as 15.0.xx instead of

14.5.x . However, the **Firmware Rollback** page displays the version 14.5.x if you update the firmware by using the Intel Network firmware DUPs on the OS.

NOTE: During firmware update, the timeout displayed on the **Automated Task Application** page under LC (showing Task is in progress), the **Task Time Limit** field shows a much greater value for the same firmware being updated in the idrac version 5.10.25.00 and later.

Selecting the type of update and update source

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

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).

1. FTP server—Local FTP, or FTP server using a proxy server.
2. Local Drive—Use a USB drive, **Dell server Updates** DVD, or **Lifecycle Controller OS Driver Packs** DVD.
3. Network Share (CIFS, NFS, HTTP, and HTTPS)

Using a local drive

Lifecycle Controller allows you to perform firmware updates using locally available DVDs or USB drives, or virtual media. This flexibility improves the efficiency of the update process when there is a high network traffic. After selecting the update repository, the Lifecycle Controller automatically detects any necessary updates, and performs those updates on components you select.

To access the repository on the local drive: .

Create a repository on a DVD or USB drive and attach it to the server locally or using a virtual media.

Using a DVD

Use either the Server Update Utility (SUU) DVDs or custom DVDs (SUU ISO downloaded from Dell support site and written to a DVD) to perform the firmware updates. The available DVDs are:

- **OpenManage SUU** DVD to update all the server components such as Lifecycle Controller, Dell Diagnostics, BIOS, RAID controller, NIC, iDRAC, and Power Supply Unit.
- **Lifecycle Controller OS Driver Pack**s DVD (Windows only) to update the operating system driver packs.

To access the updates from a DVD:

1. Insert the appropriate DVD in the locally attached CD/DVD drive. Alternatively, insert the appropriate DVD in the client and use the **Virtual Media** feature to access the attached CD/DVD drive. For more information, see the Integrated Dell Remote Access Controller User's Guide.
2. From the **Local Drive** drop-down menu, select the drive that contains the updated DVD.
3. In the **File Path or Update package path** field, enter the location or subdirectory where the catalog is available.

   NOTE: If the catalog file is located in the root folder, do not enter the file name in the **File Path** or **Update package path** field. However, if the catalog file is located in a subdirectory, enter the subdirectory name.

   NOTE: If the catalog file or DUP is downloaded from downloads.dell.com, do not copy them to a subdirectory.

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

Using a USB drive

You can download the repository from the SUU DVD or from an FTP location to a USB drive, and then access the updates from this drive.

Before downloading the repository to the USB drive, make sure that the following prerequisites are met:

- The updates are downloaded using the **Dell Repository Manager** and the repository is created on a USB drive.

  NOTE: To download the complete repository, make sure that the USB drive has 8 GB free space.

- Connect the USB drive to the system.

To update using a USB drive:

1. Insert a USB drive to the managed system. Alternatively, you can insert the USB drive to the client system and use the **Virtual Media** feature to access the USB drive. For more information about this feature, see Integrated Dell Remote Access Controller User's Guide.
2. From the **Select Device** drop-down menu, select the USB drive that contains the updates (DUP or repository).
3. Click **Browse** to select the file or update package.

   NOTE: If the catalog file or DUP is downloaded from downloads.dell.com, do not copy them to a subdirectory.

   NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

Using an FTP server

Lifecycle Controller provides options to update a server using firmware available on an internal FTP server. To use local FTP that is configured as proxy or nonproxy, use the following options:

1. Using Non-Proxy FTP Server
2. Using Proxy FTP Server

Using a non-proxy FTP server

Lifecycle Controller can access the latest firmware from the downloads page. It downloads the DUPs from this location to perform firmware update.

Before performing an update using a non-proxy FTP server, make sure that the following prerequisites are met:

- The network settings are configured (**Settings** > **Network Settings**).
- The updates are downloaded using **Dell Repository Manager**, and the repository is created on an internal FTP server.

To update the system using an internal FTP server, enter the following details:

- **User Name**—The user name to access the FTP location.
- **Password**—The password to access the FTP location.
- **File Path or Update package path** — Name of the DUP location or subdirectory where the catalog is available.

  This step is optional for operating system driver source.

  NOTE: If the catalog file is located in the root folder, do not enter the file name in the **File Path** or **Update package path** field. However, if the catalog file is located in a subdirectory, enter the subdirectory name.

  NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

Using proxy FTP server

Using Lifecycle Controller, you can update the firmware by using downloads.dell.com , or by using an internal FTP server, when you are connected to the Internet through a proxy server.

NOTE: FTP protocol doesnot support firmware update from **ftp.dell.com**.

Before performing an update using a proxy FTP server, make sure that the following prerequisites are met:

- The network settings are configured—**Settings** > **Network Settings**.
- The updates are downloaded using the **Dell Repository Manager**, and the repository is created on an internal FTP server.
- The proxy server supports either HTTP, SOCKS4, or SOCKS5 protocols.
- Information related to proxy server such as IP address or host name of the proxy server, login credentials, and the port number are readily available.

NOTE: Lifecycle Controller does not support CCproxy. It supports only Squid proxy.

To update the system using the an internal FTP server in a proxy environment:

1. Internal FTP server — Enter the following details:
   - **User Name**—The user name to access the FTP location.
   - **Password**—The password to access the FTP location.
   - **File Path** or **Update package path** — Name of the DUP location or subdirectory where the catalog is stored.

     NOTE: If the catalog file is located in the root folder, do not enter the file name in the **File Path** or **Update package path** field. However, if the catalog file is located in a subdirectory, enter the subdirectory name (for example, subdirectory).

     NOTE: If the catalog file or DUP is downloaded from downloads.dell.com, do not copy them to a subdirectory.

     NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

2. **Enable Settings** — Select this option to enter the following details:
   - **Server**—The host name of the proxy server.
   - **Port**—The port number of the proxy server.
   - **User Name**—The user name required to access the proxy server.
   - **Password**—The password required to access the proxy server.
   - **Type**—The type of proxy server. Lifecycle Controller supports HTTP, HTTPS, and SOCKS 4 proxy server types.

Using network share

To use a shared folder over a network, select **Network Share (CIFS, NFS, HTTP, or HTTPS)** and enter the details

1. For CIFS, type the following details:
   a. **Share Name/Address**—Enter IP address or hostname and the root shared folder location. For example,

      ```
      \\192.168.20.26\shared_folder or \\hostname\share_folder
      ```

   b. **Domain and User Name**—Type the correct domain and user name required to log in to the network share. For example, `login-name@myDomain`, and if there is no domain, type only the login name. For example, `login-name`.
   c. **Password**—Password to access the share.
   d. **File Path** or **Update package path**—Name of the DUP location or subdirectory, where the catalog is stored.
2. For NFS, type the following details:
   a. **Share Name**—Path to the repository or the shared folder where the DUPs are stored. For example,

      ```
      \\192.168.20.26\sharename or \\servername\sharename
      ```

   b. **File Path** or **Update package path**—Name of the DUP location or subdirectory, where the catalog is stored.

   NOTE: If the catalog file is located in the root folder, do not enter the filename in the **File Path** or **Update package path** field. However, if the catalog file is located in a subdirectory, enter the subdirectory name.

   NOTE: If the catalog file and DUP are downloaded from downloads.dell.com, do not copy them to a subdirectory.

NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for the file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

3. For HTTP or HTTPS, type the following details:
   a. **Share Name/Address**—Path to the address where the DUPs or repository is located. For example,

      ```
      192.168.20.26 or servername
      ```

   b. **File Path** or **Update package path**—Name of the DUP location or subdirectory, where the catalog is stored.

      NOTE: There is no option to browse to the folder. To access the file, type the complete URL of the HTTP or HTTPS web server.

   c. **Enable Settings**—Select this option to enter the following details:
      - **Server**—The hostname of the proxy server.
      - **Port**—The port number of the proxy server.
      - **User Name**—The user name required to access the proxy server.
      - **Password**—The password required to access the proxy server.
      - **Type**—The type of proxy server. Lifecycle Controller supports HTTP, SOCKS 4, and SOCKS 5 proxy server types.

      NOTE: HTTP, SOCKS 4, and SOCKS 5 (for IPv6) proxy server types are supported in this release.

   Share Name/Address—Enter IP address or hostname and the root shared folder location. For example,

   ```
   \\192.168.20.26\shared_folder or \\hostname\share_folder
   ```

Using single component DUPs

To use single component Dell Update Packages (DUP), download the Dell Update Package (only .exe) from the downloads.dell.com, or copy from the **Server Update Utility** DVD, or from Dell Support page to a local hard disk drive or network share.

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

NOTE: Both 32–bit and 64–bit DUPs are supported.

NOTE: If you perform multiple jobs for various components and iDRAC DUP is one of the jobs, ensure that the iDRAC job is the last job in the queue. Ensure that all other jobs are either in SCHEDULED or COMPLETED state before you perform the iDRAC job.

In the **File Path or Update package** path field, enter the name of the DUP (for example, `APP_WIN_RYYYZZZ.EXE`) or if the DUP is present in a subdirectory, enter both the subdirectory name and name of the DUP (for example, `subdirectory\APP_WIN_RYYYZZZ.EXE`.

NOTE: Lifecycle Controller allows 256 characters in a path that includes the file name and file extension. For example, if 56 characters are used for file name and extension, only 200 characters can be used for the path. Lifecycle Controller does not support these characters -:, *,?,",<,>,|,#,%,^, and SPACE.

Selecting and applying updates

1. To select and apply the updates, from the **Available System Updates** table, select the check box beside the component that has the firmware you want to update. After you select the catalog ID, details of the firmware selected are displayed in the following format:

   ```
   Release Date: YYYY-MM-DD
   ```

`Source: USB Drive or CD or DVD (<device type>):\<firmware file name in .exe format`By default, the Lifecycle Controller selects the components for which the current updates or higher version of the current installed version is available.

2. Click **Apply**. The system may restart after the update process is complete. When applying more than one update, the system may restart between the updates and launch back to Lifecycle Controller, and go to the other selected updates.

   NOTE: The system does not restart after updating the operating system driver pack and hardware diagnostics.

   NOTE: While using Lifecycle Controller to update the Power Supply Unit (PSU) firmware, the system turns off after the first task. It takes a couple of minutes to update the PSU firmware, and then automatically turns on the server.

System Configuration Lockdown mode

System configuration Lockdown mode prevents OS based updates from changing the firmware configurations. Enabling this feature blocks the firmware update of the third party I/O cards.

You can enable this feature using interfaces like iDRAC GUI, LC UI, RACADM, Redfish, WSMAN, BIOS, and iSM.

NOTE: You must have Configure iDRAC and System Control privilege to enable / disable lockdown mode.

NOTE: This feature is supported for Enterprise license.

Firmware rollback

Lifecycle Controller allows you to roll back to a previously installed version of component firmware such as BIOS, iDRAC with Lifecycle Controller, RAID Controller, NIC, Enclosure, Backplane, Fibre Channel cards, BOSS-S1, NVDIMM, and Power Supply Unit (PSU). Use this feature if you are facing an issue in the current version, and want to revert to the previously-installed version.

NOTE: Firmware rollback for HBA is supported for HBA345 and later.

All servers supported by this release have a single iDRAC and Lifecycle Controller firmware. Rolling back the iDRAC firmware also rolls back the Lifecycle Controller firmware.

- Dell Diagnostics, operating system driver packs, CPLD, and operating system collector tool cannot be rolled back to earlier versions.
- The earlier version is available only if the component firmware is updated at least once to a different version.
- Except for iDRAC firmware, the earlier version of the firmware is not displayed if the current version and the earlier version are the same.
- Every time a firmware image is updated, the earlier version of the firmware image is backed up.
- Every time a rollback operation is performed, the previously installed firmware becomes the current version. However, for iDRAC, the previously installed version becomes the current version and the current version is stored as the previous version.
- The earlier version of the firmware is available only if any of the following tools are used to update the firmware: Lifecycle Controller **Firmware Update** feature, Lifecycle Controller-Remote Services, or the Dell Update Package (DUP) from operating system.

  NOTE:
  - When SEKM mode is enabled on a controller, iDRAC Firmware rollback shall fail when tried from a SEKM to a non-SEKM iDRAC version. iDRAC Firmware rollback shall pass when done within the SEKM versions.
  - PERC firmware rollback to a non-SEKM version shall fail when SEKM encryption mode is enabled on PERC controller.

Rolling back to previous firmware versions

You can roll back to earlier versions of a firmware using the **Firmware Rollback** wizard.

NOTE: If you update any 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 a firmware:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller
2. In the left pane, click **Firmware Update**.
3. In the right pane, click **Launch Firmware Rollback**.
   The **Firmware Rollback** page displays a list of components for which roll back is available and the later versions are selected by default.
   NOTE: In Firmware Rollback page, the Component names may vary in iDRAC GUI and Lifecycle Controller GUI.
4. Select the required rollback image and click **Apply**.
   After the update process is complete, the system may restart. When applying more than one update, the system may restart between updates and launch back to Lifecycle Controller and continue updating.

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 corresponding to the component that you want to update.
- **Current** — Displays the component version currently installed on the system.
- **Available** — Displays the version of the available firmware.

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 drive that contains a recovery key is inserted during the next system restart. For information on how to set TPM settings, see the *BIOS User Guide* available at Dell Support page.

When Lifecycle Controller detects that TPM security is set to **On with Pre-boot Measurements** in the TPM version 1.2 or **TPM Security On** in the TPM version 2.0, the message indicates that certain updates require the recovery password or USB drive with the recovery key. The message also indicates components that affect the BitLocker.

You can choose not to update or roll back those components by navigating to the **Select Updates** page, and then clearing the options for the appropriate components.

6

Configure

Lifecycle Controller provides various system configuration wizards. Use the configuration wizards to configure system devices. The Configuration Wizards has:

- **System Configuration Wizards** — This wizard includes **LCD Panel Security**, **iDRAC Settings**, and **System Date and Time Configuration**.
- **Storage Configuration Wizards** — This wizard includes **RAID Configuration**, **Key Encryption**, and **Break Mirror**.

NOTE: It is recommended not to perform any storage configuration operation during host booting. Doing so may result in unexpected result.

Topics:

- System control panel access options
- Configuring iDRAC
- Configuring system time and date
- Configuring RAID
- Configuring RAID using software RAID
- Creating a secure virtual disk on a RAID controller
- Key encryption
- Local key encryption mode
- Breaking mirrored drives
- System setup — Advanced Hardware Configuration
- Collect system inventory on restart
- Configuring a local USB drive
- Configuring NFS and CIFS servers
- Conditions while configuring an HTTP or HTTPS server

System control panel access options

Lifecycle Controller front panel security configuration enables an administrator to restrict access to system 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.
- **Disable** — You do not have access to information or control, other than the information displayed by the management controller, and you cannot specify actions.

Controlling access to the front panel

To control access to the front panel:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. From the Lifecycle Controller **Home** page, select **Hardware Configuration**.
3. In the right pane, select **Configuration Wizards**.
4. On the **System Configuration Wizards** page, click **LCD Panel Security**.
5. Set **System Control Panel Access** to one of the following options:
   - **View and Modify**
   - **View Only**
   - **Disable**
6. 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 Settings** wizard.

NOTE: You can also use the **System Setup** utility during startup for configuring iDRAC. For more information about the **System Setup** utility, see Using the System Setup Program and Boot Manager.

To configure and manage the iDRAC parameters:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane of **Home** page, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. On the **System Configuration Wizards** page, click **iDRAC Settings**, and then click the following options to configure the different iDRAC parameters.

   For more information about configuring iDRAC settings, see the Integrated Dell Remote Access Controller User's Guide.

   NOTE: Click **System Summary** to view the parameters and their values.

   - **Network**
   - **OS to iDRAC Pass Through**
   - **Alerts**
   - **System Event Log**
   - **Virtual Media**
   - **Thermal**
   - **System Location**
   - **Front Panel Security**
   - **User Configuration**
   - **Smart Card**
   - **Lifecycle Controller**
   - **Remote Enablement**
   - **Reset iDRAC Configuration to defaults**
5. Click **Back** after setting the parameters for each option to return to the main menu.
6. Click **Finish** to apply the changes.

Configuring system time and date

To set the time and date for the managed system:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. From the Lifecycle Controller **Home** page, select **Hardware Configuration**.
3. In the right pane, select **Configuration Wizards**.
4. Under **System Configuration Wizards**, click **System Time and Date Configuration**.
   The default system time and system date displayed in Lifecycle Controller is the date and time reported by the system BIOS.
5. Modify the **System Time** and **System Date** (HH:MM:SS AM or PM), as required.
6. Click **Finish** to apply the changes.

Configuring RAID

If your system has one or more supported PERC RAID controllers with PERC 8 firmware or later, or software RAID controllers, use the **RAID Configuration** wizard to configure a virtual disk as the boot device.

NOTE: Create boot virtual disk only from disk drive populated across slots 0–3 of the system. For slot information, see the server Owner's Manual at PowerEdge Manuals.

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

NOTE: Autoconfigure to RAID 0 is not supported in Lifecycle controller.

NOTE: Lifecycle controller does not support VD creation when the controller is in eHBA mode.

To configure RAID using LC:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard.
   The **View Current RAID Configuration and Select Controller** page is displayed.
   NOTE: BOSS-S1 controller is supported at RAID 1 level only.
5. Select the controller and click **Next**.
   The **Select RAID Level** page is displayed.
6. Select the RAID level and click **Next**.
   The **Select Physical Disks** page is displayed.
7. Select the physical disk's properties and click **Next**.
   The **Virtual Disk Attributes** page is displayed.
8. Select the virtual disk parameters and click **Next**.
   The **Summary** page is displayed.
9. To apply the RAID configuration, click **Finish**.

Foreign configuration found

The **Foreign Configuration Found** page is displayed only if a foreign configuration physical disk drive resides on the selected RAID controller or any uninitialized physical disk drives present on the system.

A foreign configuration is a set of physical disk drives containing a RAID configuration that is introduced to the system, but is not managed by the RAID controller to which it is attached. You may have a foreign configuration if physical disk drives have been moved from one RAID controller to another RAID controller.

NOTE: Import Foreign Configuration is supported from **System Setup** > **Advanced Hardware Configuration** > **Device Settings**.

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

- If the foreign configuration contains data that you require, click **Ignore Foreign Configuration**. If you click this option, the disk drive space containing the foreign configuration is not available for use in a new virtual drive.
- To delete all data on the physical disk drives containing the foreign configuration, click **Clear Foreign Configuration**. This option deletes the hard-disk drive space containing the foreign configuration and makes it available for use in a new virtual drive.

After selecting one of the above options, click **Next**.

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 changing. 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 a single new virtual disk to be used as the new boot device. To select this option, click **Next**.

  NOTE: RAID 0 does not provide data redundancy and hot spare. Other RAID levels provide data redundancy and enable you to reconstruct data in the event of a disk-drive 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 or POST.

Selecting a 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**.

Selecting RAID levels

Select a **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 60 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.

NOTE: Depending on the type of controllers, some RAID levels are not supported.

Minimum disk requirement for different RAID levels

Table 11. RAID level and number of disks

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

* For PERC S140 / S150 RAID controllers, a minimum of two hard-disk drives are required.

Selecting physical disks

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

- **Protocol** — Select the protocol for the disk pool: **Serial Attached SCSI (SAS)**, **Serial ATA (SATA)**, or **NVM Express (NVMe)**. SAS drives are used for high performance, while SATA drives are used for a more cost-effective solution. A disk pool is a logical grouping of physical disk drives on which one or more virtual drives can be created. The protocol is the type of technology used to implement RAID.
- **Media Type** — 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.
- **Disk Boot Size** — Select one of the following disk block sizes:
  - 512 — indicates that the 512 bytes block size hard drives (HDD) are selected.
  - 4K — indicates that the 4K block size hard disk drives (HDD) are selected. 4K block HDDs allow the faster data transfer with fewer commands.
- **T10 Protection Information (T10 PI) Capability**— It is known as DIF (Data Integrity Fields) and the supporting HDDs are referred to DIF drives. The T10 enabled HDDs validates and stores the data integrity fields for each block. It performs this action when you write the data on the disk and return these values on a read request. When you read or write the data from the HDD, the data is checked for the errors. Select one of the following types of T10 protection information capabilities:
  - All — indicates that both the T10 PI capable and non-capable HDDs are selected.
  - T10 PI Capable — indicates that only T10 PI capable HDDs are selected.
  - Non-T10 Capable — indicates that only non-T10 capable HDDs are selected.

  NOTE: PERC 9 with version 9.3.2 and above doesn't support T10 PI capabilities.
- **Encryption Capability** — Select **Yes** to enable encryption capability.
- **Encryption Protocol** — Select the type of encryption protocol. Select one of the following types of encryption protocol type:
  - **TCG Enterprise SSC** — indicates only TCG Enterprise SSC Capable drives are selected.
  - **TCG Opal SSC** — indicates only TCG Opal SSC Capable drives are selected.
  - **Non-Encryption Capable** — indicates only non-encryption capable drives are selected.
- **Select Span Length** — Select the span length. The span length value refers to the number of physical disk drives included in each span. Span length applies only to RAID 10, RAID 50, and RAID 60. The **Select Span Length** — Setting span length is only supported in RAID 10, RAID 50, and RAID 60. And in a RAID 10 configuration, the default value is set to 2 and the option Span Length is not available is the storage controller supports Uneven span.
- Select the physical disk-drives using the check boxes at the bottom of the screen. The physical disk-drive selection must meet the requirements of the RAID level and span length. To select all the physical disk-drives, click **Select All**. After you select the option, the option changes to **Deselect**.

Setting virtual disk attributes

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

- **Size** — Specify the size of the virtual drive.
- **Stripe Element Size** — Select the stripe element size. The stripe element size is the amount of drive space a stripe consumes on each physical-disk drive in the stripe. The **Stripe Element Size** list may contain more options than initially displayed on the screen. Use the up arrow and down arrow keys to view all available options.
- **Read Policy** — Select the read policy:
  - **Read Ahead** — The controller reads sequential sectors of the virtual drives when seeking data. The Read Ahead policy may improve system performance if the data is written to sequential sectors of the virtual drives.
  - **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-recently-read requests accessed sequential sectors of the disk drive. If the most-recently-read requests access random sectors of the disk drive, then the controller uses the No Read Ahead policy.
- **Write Policy** — Select the write policy.
  - **Write Through** — The controller sends a write-request-completion signal only after the data is written to the disk drive. The Write Through policy provides better data security than the Write Back policy, because the system assumes that the data is available only after it has been written to the disk drive.
  - **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 the disk drive. The Write Back policy may provide faster 'write' performance, but it provides less data security, because a system failure can prevent the data from being written to the disk drive.
  - **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.
- **Disk Cache Policy**— Select the write policy.

- **Enabled** — The controller enables physical disk cache setting while creating virtual disks.
- **Disabled** —The controller disables physical disk cache setting while creating virtual disks.

- **Assign a Hot Spare Disk if available** — Select this option to assign a hot spare to the virtual drive. A hot spare is an unused backup physical disk drive that is used to rebuild data from a redundant virtual drive. A hot spare can be used only with a redundant RAID level. Hot spares also have physical disk-drive size requirements. The hot spare must be as large as or bigger than the smallest physical disk-drive included in the virtual drive. If the RAID level and physical disk-drive availability do not meet these requirements, a hot spare is not assigned.

  NOTE: Assign a hot spare only from disk drives populated across slots 0–3 of the system. For slot information, see the PowerEdge Owner's manual at PowerEdge Manuals.

- **Hot Spare Disk** — Select a disk that is used as a hot spare. Only one dedicated hot spare is supported in Lifecycle Controller.
- **Secure Virtual Disk** — Select to secure the virtual drive using the controller's security key.

  NOTE: The secure virtual drive 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 selections.

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

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

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

Configuring RAID using software RAID

For the S140 / S150 controllers, ensure to change the SATA settings in the system BIOS to **RAID Mode**. To change the setting using the BIOS, the latest BIOS version must be installed.

NOTE:

- For more information about RAID configuration, see the **Creating RAID using Lifecycle Controller** white paper here.
- If you have an older BIOS, you can configure RAID only through option ROM.
- Software RAID creation using NVMe/HHHL drives supports only on UEFI mode.
- Software RAID doesn't support any encryption method such as SEKM, LKM, TCG OPAL etc.

Use this feature to configure RAID, if a PERC S140 / S150 controller is enabled on the system. If you select the software RAID option, you cannot create partial virtual disk through the Lifecycle Controller interface and it displays the physical disk-drives as the Non-RAID disks or RAID-ready disks.

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

  NOTE: From Lifecycle Controller UI, you can deploy only Windows server operating system using software RAID controller.

To configure software RAID:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard.
   The **View Current RAID Configuration and Select Controller** page is displayed.

   Select the **Windows** or **Linux RAID** option to install the appropriate operating system. This option is available only for the software RAID controller, which enabled only if the software RAID controller is supported.

NOTE: Windows RAID supports RAID levels 0, 1, 5, and 10, but, the Linux RAID supports RAID level 1 only. After the **RAID type** is initialized, this option is grayed out in the LCUI. To enable the **RAID type**, go to BIOS F2 settings, convert the RAID Type to **Non-RAID disk**.

5. Select the controller, and click **Next**.
   NOTE: If the non-RAID disk drives are attached to the selected controller, select the non-RAID physical disk-drives, and then click **Next** to initialize them. Else, the **Select RAID Level** page is displayed.

   NOTE: During initialization, all the data on the non-RAID disk drives are deleted.
6. Select the RAIDlevel and click **Next**.
   The **Select Physical Disks** page is displayed.
7. Select the physical disk properties and click **Next**.
   The **Virtual Disk Attributes** page is displayed.

   Select NVMe protocoltype to enable software RAID creation on the NVMe disks. To enable software RAID, go to BIOS F2 settings, and change the interface type to NVMe on the NVMe disks.
8. Select the virtual disk parameters and click **Next**.
   The **Summary** page is displayed.
9. To apply the RAID configuration, click **Finish**.

Creating a secure virtual disk on a RAID controller

Make sure that the controller is set to use either Local Key Management (LKM) or Secure Enterprise Key Manager (SEKM).

To create a secure virtual disk on a RAID controller:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. Under **Storage Configuration Wizards**, click **RAID Configuration** to launch the wizard.
   The **View Current RAID Configuration** and **Select Controller** page is displayed along with the information on whether the displayed virtual disk is secure.
   NOTE: PERC controller name will be associated with phrase **SEKM**, if the controller is set to Secure Enterprise Key Manager (SEKM) mode.
5. Select a security capable controller and click **Next**.
   If the non-RAID disks are attached to the selected controller, select the non-RAID physical disk-drives, and then click **Next** to initialize them. Else, the **Select RAID Level** page is displayed.
   NOTE: During initialization, all the data on the non-RAID disk drives are deleted.
6. Select the RAID level and click **Next**.
   The **Select Physical Disks** page is displayed.
   NOTE: Create boot virtual disks only from disk drives populated across slots 0–3 of the system. For slot information, see the system Owner's Manual.
7. From the **Encryption Capability** drop-down menu, select **Self-encryption**.
   The self-encryption disks (SEDs) are displayed.
8. From the **Encryption Protocol** drop-down menu, select either **TCG Opal SSC** or **TCG Enterprise SSC**.
9. Select the SEDs and specify the properties, and then click **Next**.
   The **Virtual Disk Attributes** page is displayed.
10. Select the virtual disk parameters, select the **Secure Virtual Disk** option, and click **Next**.
    The **Summary** page is displayed.
11. To apply the RAID configuration, click **Finish**.

Key encryption

Use the **Key Encryption** feature to:

- Apply local encryption for PERC H730, H730P, H740, H740P, H745, H755, H755N, and H840 RAID controllers.
- Delete the local encryption key.

- Encrypt the existing unsecured virtual drives.
- To change an existing encryption key to another one.

NOTE: When PERC controllers are set to Secure Enterprise Key Manager (SEKM) mode, they are not listed under Key Encryption feature.

Applying the local key on a RAID controller

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

To apply the local key on a RAID controller:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. Under **Storage Configuration wizards**, click **Key Encryption**.
5. Select the controller to apply a local key and click **Next**.
6. Click **Set up local key encryption** and click **Next**.

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

7. 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 this hint.
8. In the **New Passphrase** field, enter a passphrase.

   NOTE: The controller uses the passphrase to encrypt the disk drive data. A valid passphrase contains 8–32 characters. It must include a combination of uppercase and lowercase letters, numbers, and symbols without spaces.

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

Local key encryption mode

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

NOTE: For more information on the specification and configuration-related information for the PERC H740, H730, H840, and PERC 9 controllers, see the *PERC H740, H730, and H840 Technical Guidebooks*.

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

  NOTE: This option is available if there are secure-capable 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 drives along with its data. After deletion, controller state changes to **No encryption** mode.

Encrypting unsecure virtual disks

Make sure that the following prerequisites are met:

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

To encrypt the unsecure virtual drives:

NOTE: All virtual drives created on the same physical disk-drives are automatically encrypted when any one of the virtual drives is encrypted.

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.

3. In the right pane, click **Configuration Wizards**.
4. On the **Storage Configuration wizards** page, click **Key Encryption**.
5. Select the controller that is encrypted and click **Next**.

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

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

Rekey controller with new local key

To rekey the controller with a new local key:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards**.
4. On the **Storage Configuration wizards** page, click **Key Encryption**.
5. On the Select Controller Select the controller to which the local key is applied and click **Next**.
6. In the **Existing Passphrase** field, enter the existing passphrase associated with the displayed Encryption Key Identifier.
7. In the **New Encryption Key Identifier** field, enter the new identifier. The **Encryption Key Identifier** is a passphrase hint; you must enter the passphrase when Lifecycle Controller prompts this hint.
8. In the **New Passphrase** field, enter the passphrase that is associated with the new encryption key identifier.

Removing encryption and deleting data

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

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

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, click **Configuration Wizards** and click **Key Encryption**.
4. Select the controller on which you must remove the key that was applied and click **Next**.
5. In the right pane, select **Remove encryption and delete data** and click **Next**.
6. Select **Delete encryption key and all secure virtual disks** and click **Finish**.

Breaking mirrored drives

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

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

   NOTE: The **Break Mirror** feature does not support PERC 10.5, PERC 11, and software RAID controllers.

   The system automatically turns off even if one mirrored array is successfully delinked.

System setup — Advanced Hardware Configuration

The 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.

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

NOTE: When you update the firmware on a BCM57xx and 57xxx adapters, you will notice that the cards are displayed as QLogic. This is due to the acquisition of Broadcom NetXtreme II by QLogic.

The **Advanced Hardware Configuration** wizard allows you to configure the following:

NOTE: You can also use **System Setup** utility during startup to configure the following devices. For more information about the **System Setup** utility, see Using the system setup program and boot manager.

- System BIOS Settings
- iDRAC Device Settings
- NICs

NOTE: You can configure only one NIC at a time. For more information about the supported NIC cards, see white paper about Network Adapter at downloads.dell.com/solutions/general-solution-resources.

If the System Configuration Lockdown mode is enable from iDRAC UI, any configuration on the particular system will not be permitted.

NOTE: This feature is available in Enterprise license.

Following are the exceptions for this feature:

- Power operations (System power on, power off, reset)
- Setting power budget, power profiles
- Identify operations to blink an LED
- Run diagnostics

Integrated Broadcom NICs are controlled by both BIOS and the 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.
- **Enabled with iSCSI** to use the NIC to boot from an iSCSI target.

Modifying device settings

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

NOTE: You can also modify the device settings by using the **System Setup** utility during startup. For more information about the **System Setup** utility, see Using the system setup program and boot manager.

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, select **System Setup**.
3. In the right pane, click **Advanced Hardware Configuration**.
4. Select the device you want to configure.
   Based 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?
   ```

5. Select **No** to continue making additional configuration changes or select **Yes** to save the changes and exit the wizard.
   All changes are applied during the next system restart.

Collect system inventory on restart

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

NOTE: By default, the **CSIOR** property is enabled.

Updating server inventory information

To enable collecting system inventory on restart:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**.
3. In the right pane, select **Hardware Inventory**.
4. Click **Collect System Inventory on Restart**.
5. Under **Collect System Inventory on Restart**, click **Enabled**, and then click **Finish**.
   The system inventory is updated after the next restart.

Configuring a local USB drive

If you are using a private network that does not have access to external sites, you can provide updates from a locally configured USB drive.

The USB drive used as a repository must have at least 8 GB free space.

NOTE: A USB drive is not required for users who have access to the Drivers and Downloads page through a proxy server.

For the latest updates, download the most recent Dell server Updates ISO images for your system from the Dell Support page.

NOTE: Lifecycle Controller supports internal SATA optical drives, USB 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 FTP server from the Dell server Updates DVD

To copy the repository:

1. Download the Dell server Updates ISO image to your system from Dell Support page.
2. Copy the repository folder of the DVD to the root directory of the local FTP server.
3. Use this local FTP server for firmware 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 about creating a repository for your system, see the Dell Repository Manager User's Guide at OpenManage Manuals > Repository Manager.
2. Use this local FTP server for firmware update.

Configuring NFS and CIFS servers

If you are using a private network that does not have access to external sites such as downloads.dell.com, you can provide updates from a locally-configured NFS and CIFS servers.

Configuring NFS servers

To configure an NFS server, perform the following tasks:

1. Open the `/etc/exports` configuration file and add an NFS entry.

   For example:

   ```
   [root@localhost ~]# cat /etc/exports
   /nfs_share *(rw,fsid=0,insecure,sync,no_root_squash,no_subtree_check)
   ```

2. Save the configuration file and restart the NFS service.

   NOTE: To use a shared folder over a network, see the section Using network share

Configuring CIFS servers

To configure an CIFS server, perform the following tasks:

1. Right-click the folder that you want to configure as CIFS share and select **Properties** > **Sharing**.
2. Click the **Advanced Sharing** tab and select **Share this folder**.
3. Click the **Permissions** tab.
4. Click **Add** to add names of the users for whom you want to provide access to the CIFS share.
5. Type the names and click **OK**.
6. In the **Permissions** section under **Allow** column, select **Full Control**.

NOTE: The SMB2 option-*RequireSecuritySignature* must be set to `False`. The command to set the value from PowerShell is `Set-SmbServerConfiguration -RequireSecuritySignature $false`. For more information on SMB2 support in iDRAC and LC, see the white paper available here.

Now the selected folder is shared over network and it can be accessed over CIFS protocol by using the `\\<ip address>\share_name` folder path.

NOTE: Ensure that the folder is accessible and folder names doesn't have any space. If the problem persists, check the network settings or retry using a share with fewer files and folders.

Disabling the Digitally sign communications option

To disable the **Digitally sign communications (always)** option, perform the following tasks:

1. Open Control Panel and select **Administrative Tools**.
2. Click **Local Security Policy**.
3. On the left navigation pane, expand the **Local Policies** option and select **Security Options**.
4. Double-click the **Microsoft network server: Digitally sign communications (always)** option.
5. Select **Disabled** and click **OK**.

Conditions while configuring an HTTP or HTTPS server

While configuring the HTTP or HTTPS servers, ensure that:

- The HTTP servers are configured to the default port 80, whereas the HTTPS server is configured to the default port 443. The Lifecycle Controller web interface accesses the web server using the default port. If the web server is configured to a port other than the default, the Lifecycle Controller cannot access the web server.
- The Apache web server is set as the default web server. Using other web servers may result in unexpected behavior or errors.

7

Maintain

Using Lifecycle Controller, you can maintain the health of a system throughout its life cycle using the features such as **Part Replacement Configuration** and **Platform Restore**.

Topics:

- Platform restore
- Import server license
- Part replacement configuration
- Repurpose or retire system
- Hardware diagnostics
- SupportAssist Collection

Platform restore

The following features are available to maintain a server:

- **Import Server License**—Allows you to import an iDRAC license from a network share or a USB drive. Use this feature to import an iDRAC license from the Lifecycle Controller GUI. The scenarios in which you may want to import a license are when you set up a new server shipped from the factory, while upgrading an Express license to an Enterprise license, and so on. You can import the license that is stored on a USB drive or on the network share such as CIFS or NFS.
- **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: Part replacement does not support RAID operations such as resetting configuration, recreating VDs, setting controller key, or changing controller mode.

NOTE: This feature is licensed. You must acquire the required license to enable this feature. For more information about acquiring and using the licenses, see Integrated Dell Remote Access Controller User's Guide.

Import server license

NOTE: vFlash, and Backup and Restore operation is not supported on PowerEdge R6515, PowerEdge R7515, PowerEdge C6525 and PowerEdge 6525.

Use the **Import Server License** feature to import an iDRAC license from the Lifecycle Controller GUI. The scenarios in which you may want to import a license are when you set up a new server shipped from the factory, while upgrading an Express license to an Enterprise license, and so on. You can import the license that is stored on a USB drive or on the network share such as CIFS or NFS.

Part replacement configuration

Use the **Part Replacement** 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: Part replacement does not support RAID operations such as resetting configuration, recreating VDs, setting controller key, or changing controller mode.

Applying firmware and configuration updates to replaced parts

Before configuring replaced parts, make sure that the following prerequisites are met:

- Click the **Collect System Inventory On Restart** option, so that Lifecycle Controller automatically invokes **Part Firmware Update** and **Part Configuration Update** when the system is started.

  NOTE: If **Collect System Inventory On Restart** 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 manual mode, press **<F10>** after the part replacement during a system restart.

- Make sure that the **Disabled** option under **Part Firmware Update** and **Part Configuration Update** are cleared.
- The previous component and the new device must be identified as the same part .
- If the current adapter on the system is NPAR enabled and is replaced with a new adapter, after the host server is turned on, press **<F2>** and select **System Setup** > **Device Settings** and make sure that the **NPAR** is enabled. NPAR must be enabled on the new adapter before using the **Part Replacement** feature.

To apply part firmware and configuration to replaced parts:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Platform Restore**.
3. In the right pane, click **Part Replacement**.
   The **Part Replacement Configuration** page is displayed.
4. From the part firmware update drop-down menu, select one of the following:
   - **Disabled** — Firmware update on replaced parts is not performed.
   - **Allow version upgrade only** — Firmware update on replaced parts is performed only if the firmware version of the new part is earlier than the existing part.
   - **Match firmware of replaced part** — Firmware on the new part is updated to the version of the original part.

     NOTE: Match firmware of replaced part is the default setting.

5. From the part configuration update drop-down menu, 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.

     NOTE: Apply always is the default setting.

   - **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.

Supported devices

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

- Fibre Channel cards
- NICs
- PERC series 9 and 10
- SAS series 7 and 8
- System board
- Power Supply Unit (PSU)

NOTE: PSUs support only firmware update and not part replacement.

Repurpose or retire system

You can erase selective system information by using the Lifecycle Controller **Repurpose or Retire System** option. This feature permanently deletes server and storage-related data on selected components of a server before you repurpose or retire a server. The selected components are then returned to their default state.

NOTE: The **Repurpose or Retire System** option resets the state of the inventory collection to **Enabled**, and then permanently deletes the iDRAC and BIOS configuration information, factory-shipped inventory, configurations, Lifecycle Log information (historical data and work notes), non-volatile (NV) cache, NVDIMM, operating system driver packs, disk erase, and diagnostics. Click on this link for more details on System erase - Data Security by using the System Erase feature of iDRAC9 on PowerEdge servers . During this operation, it deletes the hardware and software inventory data related to the system. However, they are recreated during the next restart of the server. It also deletes the firmware and previous versions, which will not be available for firmware rollback

NOTE:

- The **Repurpose or Retire System** feature does not allow deletion of iDRAC-related license information.
- PERC NV cache is displayed only if PERC card is available on the server.

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.

NOTE:

- If BIOS (reset default and clear NVRAM) is selected, then the system powers off the second time after LC wipe is complete.
- After the system is repurposed or retired, the Lifecycle controller UI logs LC log event `HWC0017: Unable to start Lifecycle Controller because Lifecycle Controller cannot communicate with iDRAC`. Because of internal issues this error code is expected when iDRAC is not ready."

Deleting server information

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Configuration**, and then click **Repurpose or Retire System**.
3. On the **Select Components** page, select the features and components to delete from **Server Features** and **Storage Components**.

   NOTE: The supported erase options for each storage device are displayed on the screen.

   NOTE: Storage disk erase may take a longer time depending on the disk size and speed.

4. Click **Next**.
   A summary of the features and components selected for deletion is displayed.
5. Read the information about the **Summary** page and click **Finish**.
6. The host server turns off when the operation is completed, iDRAC will reset.

When the iDRAC is backed up, you must manually turn on the host server. If you select BIOS component for System Erase, a flag is set to reset the BIOS to default during POST and the server turns off again.

Hardware diagnostics

It is recommended that you run diagnostics using the **Hardware Diagnostics utility**, as part of a regular maintenance plan to validate whether or not the system and the attached hardware are functioning properly. As 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 disk drives, and other peripherals.

Performing hardware diagnostics

To perform hardware diagnostics:

1. Start Lifecycle Controller. For more information, see Dell Support page
2. In the left pane of Lifecycle Controller, click **Hardware Diagnostics**.
3. In the right pane, click **Run Hardware Diagnostics**.

The diagnostics utility is launched.

4. Follow the instructions on the screen.

   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 dell.com/support.

   NOTE: To close the **Hardware Diagnostics** page, restart the system, and press **<F10>** during POST to start Lifecycle Controller.

Performing hardware diagnostics on selected components

You can run targeted hardware diagnostics in Lifecycle Controller (LC) for a specific server component.

1. Start Lifecycle Controller.
2. In the left pane of Lifecycle Controller, click **Hardware Diagnostics**.
3. In the right pane, click **Run Hardware Diagnostics**.
   The diagnostics utility is launched.
4. Pause testing, click the right arrow, and then click **Advanced Options**.
   The **Advanced Options** dialog box is displayed.
5. Deselect the components for which you do not want to run hardware diagnostics.
6. Select the number of **Test Iterations**.

   NOTE: Select **0** for infinite iterations.

7. Close the **Advanced Options** dialog box.
8. Select the **Thorough Test Mode** checkbox, and then click the center arrow to run the diagnostics on the selected component.

SupportAssist Collection

If you have to work with Dell technical support on an issue with a server but the security policies restrict direct Internet connection, you can provide technical support with necessary data to facilitate successful troubleshooting of the problem without having to install any software or download tools from Dell and without having access to the Internet from the server operating system or Lifecycle Controller. You can send the report from an alternate system and make sure that the data collected from your server is not viewable by unauthorized individuals while sending it to technical support.

You can generate a health report of the server and using Lifecycle Controller, you can export the report to a location on the management station (local) or to the following shared network location:

- CIFS - Common Internet File System
- NFS - Network File Share
- USB
- HTTP/HTTPS

You can then share this report directly with technical support.

Lifecycle Controller allows you to collect data from the following options:

- **System Information**
- **Debug logs**
- **Storage logs**
- **SMART Data logs** - SMART logs are collected in a file and added as part of SupportAssist collection. This feature sends SMART data for SATA disk to support assist in order to analyze the connected SATA disk.

  NOTE: You need to select **Storage logs** to collect SMART data.

- **Operating System and Application Data** - Operating System (operating system) and Application Data option will also be enabled if iDRAC Service Module (iSM) is installed and running in operating system and the operating system Collector (OSC) is present in iDRAC. As OSC is factory installed, it will be present in iDRAC unless it is removed by user via System Erase or LC Wipe. You can select this option to retrieve either cached or live data. Live data collection from the OS required iDRAC Service Module (iSM) to be installed and running in the operating system. For more information about collecting **Operating System and Application Data** using the OS collector tool in iDRAC, see the Integrated Dell Remote Access Controller User's Guide.

- **Telemetry reports**

  NOTE: This feature needs a Datacenter License.

SupportAssist Collection is exported in the standard ZIP format. The report contains information that is similar to the information available in the DSET report such as:

- Hardware and inventory for all components
- System, Lifecycle Controller, and component attributes
- BIOS boot order information
- Installed and available component firmware versions
- Fresh Air and component statistics (for applicable servers)
- Operating system and application information
- Active Lifecycle Controller logs (archived entries are not included)
- Component hardware logs
- Trace logs
- Storage controller logs

After Lifecycle Controller exports the SupportAssist Collection file, you can delete information that you do not want to share with technical support. Each time the data is collected, an event is recorded in the Lifecycle Controller Log. The event includes information such as the interface used, the date and time of export, and iDRAC user name.

Exporting the SupportAssist Collection

Before exporting a report, make sure that:

- **Collect System Inventory On Reboot** (CSIOR) is enabled.
- You have login and server control rights.

To export a SupportAssist Collection:

1. Start Lifecycle Controller. For more information, see Starting Lifecycle Controller.
2. In the left pane, click **Hardware Diagnostics,** and then click **Export SupportAssist Collection**.
3. On the **Terms and Conditions** page, read the conditions and select the **I agree to allow Technical Support to use tech support report data** option.
4. Click **Next**.
   Lifecycle Controller checks the availability of hardware, operating system and application data, and RAID controller logs, and then displays the options listed in step 5. If the operating system and application data, or RAID controller logs are unavailable, the relevant options are grayed out. The duration to collect the selected data is displayed next to the options listed in step 5.
5. On the **Select Report Data** page, select the options for which you want to create a SupportAssist Collection:
   - **Hardware** — Collects data pertaining to the server and component inventory, firmware installed on the server, configuration information, and hardware logs.
   - **RAID Controller Logs** — Collects information about the storage logs.

     NOTE: RAID Controller logs will be exported only if the following steps are performed:
     - Power on the system.
     - Ensure POST is complete.
     - Warm reboot to enter LC.

   - **Operating System and Application Data** — Collects information about the operating system and application. The OS and application data may contain sensitive and personal information. You can choose to exclude this data while collecting the information.

     NOTE: Operating System (OS) and Application Data option will also be enabled if iDRAC Service Module (iSM) is installed and running in OS and OS Collector (OSC) is present in iDRAC. As OSC is factory installed, it will be present in iDRAC unless it is removed by user via System Erase or LC Wipe. You can select this option to retrieve either cached or live data. Live data collection from OS required iDRAC Service Module (iSM) to be installed and running in the OS. For more information on collecting **Operating System and Application Data** using the OS collector tool in iDRAC, see the Integrated Dell Remote Access Controller User's Guide.

   - **Debug Logs** — Collects information about the iDRAC debug logs.

- **Telemetry Reports** — Collects the information / reports for the features through telemetry. You can set the preferences for telemetry reports through iDRAC UI.

6. Click **Next**.
7. On the **Select Export Settings** page, type or select the required information and click **Next**.

   For information about the fields on this page, see the Online Help by clicking **Help** in the upper-right corner of the Lifecycle Controller application.
8. On the **Summary** page, verify your selections and click **Finish**.

8

Easy-to-use system component names

The following is the list of most commonly used Fully Qualified Device Descriptors (FQDD) used in all the interfaces including GUI, iDRAC RESTful API with Redfish, WSMAN, and RACADM.

- ALL
- iDRAC
- System
- LifecycleController
- EventFilters
- BIOS
- NIC
- FC
- RAID
- NVDIMM
- BOSS-S1
- BOSS DISK

The following table lists the FQDD of the system components and the equivalent easy-to-use names.

Table 12. 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 • NIC.Embedded.2	• Embedded NIC 1 • 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.Slot.1-2	• NIC in Slot 1 Port 1 • 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

Table 12. Easy-to-use Names of System Components (continued)

FQDD of System Component Name	Easy-to-use Name
USBEHCI.Embedded.1-1	Embedded USB EHCI 1
Disk.SATAEmbedded.A-1	Disk on Embedded SATA Port A
Optical.SATAEmbedded.B-1	Optical Drive on Embedded SATA Port B
TBU.SATAExternal.C-1	Tape Back-up on External SATA Port C
Disk.USBFront.1-1	Disk connected to front USB 1
Floppy.USBBack.2-1	Floppy-drive connected to back USB 2
Optical.USBFront.1-1	Optical drive connected to front USB 1
Disk.USBInternal.1	Disk connected to Internal USB 1
Optical.iDRACVirtual.1-1	Virtually connected optical drive
Floppy.iDRACVirtual.1-1	Virtually connected floppy drive
Disk.iDRACVirtual frsy.1-1	Virtually connected disk
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.Slot. 2 • Fan.Slot. 3 • Fan.Slot. 4 • Fan.Slot. 5 • Fan.Slot. 6 • Fan.Slot. 7 • Fan.Slot. 8 • Fan.Slot. 9	• Fan 1 • Fan 2 • Fan 3 • Fan 4 • Fan 5 • Fan 6 • Fan 7 • Fan 8 • Fan 9
• MC.Chassis.1 • MC.Chassis.2	• Chassis Management Controller 1 • Chassis Management Controller 2
KVM.Chassis.1	KVM
• IOM.Slot.1 • IOM.Slot.2 • IOM.Slot.3 • IOM.Slot.4 • IOM.Slot.5 • IOM.Slot.6	• IO Module 1 • IO Module 2 • IO Module 3 • IO Module 3 • IO Module 5 • IO Module 6
• PSU.Slot.1 • PSU.Slot.2 • PSU.Slot.3 • PSU.Slot.4	• Power Supply 1 • Power Supply 2 • Power Supply 3 • Power Supply 4

Table 12. Easy-to-use Names of System Components (continued)

FQDD of System Component Name	Easy-to-use Name
• PSU.Slot.5 • PSU.Slot.6	• Power Supply 5 • Power Supply 6
CPU.Socket.1	CPU 1
System.Modular.2	Blade 2
DIMM.Socket.A1	DIMM A1
NVDIMM	DIMM.Socket.A7
BOSS-S1	AHCI.Integrated.1-1
BOSS DISK	AHCI.Embedded.1-1

9

Using the system setup and boot manager

System Setup enables you to manage your system hardware and specify BIOS-level options.

The following keystrokes provide access to system features during startup:

Table 13. System setup keystrokes

Keystroke	Description
<F2>	Opens the **System Setup** page.
<F10>	Opens and starts Lifecycle Controller, which supports systems management features such as operating system deployment, hardware diagnostics, firmware updates, and platform configuration, using a GUI. The feature set available in Lifecycle Controller is determined by the iDRAC license installed.
<F11>	Opens the BIOS Boot Manager or the Unified Extensible Firmware Interface (UEFI) Boot Manager, depending on the boot configuration of the system.
<F12>	Starts Preboot Execution Environment (PXE) boot.

From System Setup, you can:

- Change the NVRAM settings after you add or remove hardware
- View the system hardware configuration
- Enable or disable integrated devices
- Set performance and power management thresholds
- Manage system security

You can access System Setup using the:

- Standard graphical browser, which is enabled by default
- Text browser, which is enabled using **Console Redirection**

To enable **Console Redirection**, in **System Setup**, select **System BIOS** > **Serial Communication screen** > **Serial Communication**, select **On with Console Redirection**.

NOTE: By default, help text for the selected field is displayed in the graphical browser. To view the help text in the text browser, press **<F1>**.

Topics:

- Choosing the system boot mode
- Entering System Setup
- System and setup password features
- Entering the UEFI boot manager
- Embedded systems management
- iDRAC settings utility

Choosing the system boot mode

System Setup enables you to specify one of the following boot modes for installing your operating system:

- BIOS boot mode (the default) is the standard BIOS-level boot interface.

NOTE: Dell Storage NAS supports only BIOS mode. You must not change the boot mode to UEFI because the system does not boot.

- Unified Extensible Firmware Interface (UEFI) (the default) boot mode is an enhanced 64-bit boot interface. If you have configured your system to boot to UEFI mode, it replaces the system BIOS.

NOTE: The system supports only BIOS boot mode.

1. From the **System Setup Main Menu**, click **Boot Settings**, and select **Boot Mode**.
2. Select the UEFI boot mode you want the system to boot into.

CAUTION: Switching the boot mode may prevent the system from booting if the operating system is not installed in the same boot mode.

3. After the system boots in the specified boot mode, proceed to install your operating system from that mode.

NOTE: Operating systems must be UEFI-compatible to be installed from the UEFI boot mode. DOS and 32-bit operating systems do not support UEFI and can only be installed from the BIOS boot mode.

NOTE: For the latest information about supported operating systems, go to OS support.

Entering System Setup

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

Responding to error messages

If an error message is displayed while the system is booting, make a note of the message. For more information, see System Error Messages.

NOTE: After installing a memory upgrade, it is normal for your system to display a message the first time you start your system.

Using the system setup navigation keys

Table 14. Using the system setup navigation keys

Keys	Action
Up arrow	Moves to the previous field.
Down arrow	Moves to the next field.
<Enter>	Allows you to type in a value in the selected field (if applicable) or follow the link in the field.
Spacebar	Expands or collapses a drop-down menu, if applicable.
<Tab>	Moves to the next focus area. **NOTE:** For the standard graphics browser only.
<Esc>	Moves to the previous page till you view the main screen. Pressing **<Esc>** in the main screen displays a message that prompts you to save any unsaved changes and restarts the system.
<F1>	Displays the System Setup help file. **NOTE:** For most of the options, any changes that you make are recorded but do not take effect until you restart the system.

System Setup options

System Setup Main screen

NOTE: Press <Alt><F> to reset the BIOS or UEFI settings to their default settings.

System BIOS	This option is used to view and configure BIOS settings.
iDRAC Settings	This option is used to view and configure iDRAC settings.
Device Settings	This option is used to view and configure device settings.

System BIOS screen

NOTE: The options for System Setup change based on the system configuration.

NOTE: System Setup defaults are listed under their respective options in the following sections, where applicable.

System Information	Displays information about the system such as the system model name, BIOS version, Service Tag, and so on.
Memory Settings	Displays information and options related to installed memory.
Processor Settings	Displays information and options related to the processor such as speed, cache size, and so on.
SATA Settings	Displays options to enable or disable the integrated SATA controller and ports. **NOTE:** The SATA setting is not available on the PowerEdge R720xd server.
Boot Settings	Displays options to specify the boot mode (BIOS or UEFI). Enables you to modify UEFI and BIOS boot settings.
Integrated Devices	Displays options to enable or disable integrated device controllers and ports, and to specify related features and options.
Serial Communication	Displays options to enable or disable the serial ports and specify related features and options.
System Profile Settings	Displays options to change the processor power management settings, memory frequency, and so on.
System Security	Displays options to configure the system security settings like, system password, setup password, TPM security, and so on. It also enables or disables support for local BIOS update, the power and NMI buttons on the system.
Miscellaneous Settings	Displays options to change the system date, time, and so on.

System information screen

You can use the **System Information** screen to view system properties such as Service Tag, system model name, and the BIOS version.

To view the **System Information** screen, click **System Setup Main Menu** > **System BIOS** > **System Information**.

The **System Information** screen details are explained as follows:

System Model Name	Displays the system model name.
System BIOS Version	Displays the BIOS version installed on the system.
System Service Tag	Displays the system Service Tag.
System Manufacturer	Displays the name of the system manufacturer.

System Manufacturer Contact Information	Displays the contact information of the system manufacturer.

Memory Settings screen

System Memory Size	Displays the amount of memory installed in the system.
System Memory Type	Displays the type of memory installed in the system.
System Memory Speed	Displays the system memory speed.
System Memory Voltage	Displays the system memory voltage.
Video Memory	Displays the amount of video memory.
System Memory Testing	Specifies whether system memory tests are run during system boot. Options are **Enabled** and **Disabled**. By default, the **System Memory Testing** option is set to **Disabled**.
Memory Operating Mode	Specifies the memory operating mode. The options available are **Optimizer Mode**, **Advanced ECC Mode**, **Mirror Mode**, **Spare Mode**, **Spare with Advanced ECC Mode**, and **Dell Fault Resilient Mode**. By default, the **Memory Operating Mode** option is set to **Optimizer Mode**. **NOTE:** The **Memory Operating Mode** can have different defaults and available options based on the memory configuration of your system. **NOTE:** The **Dell Fault Resilient Mode** establishes an area of memory that is fault resilient. This mode can be used by an operating system that supports the feature to load critical applications or enables the operating system kernel to maximize system availability.
Node Interleaving	If this field is **Enabled**, memory interleaving is supported if a symmetric memory configuration is installed. If **Disabled**, the system supports Non-Uniform Memory architecture (NUMA) (asymmetric) memory configurations. By default, **Node Interleaving** option is set to **Disabled**.
Serial Debug Output	By default, it is set to disabled.

Processor settings screen

NOTE: Depending on the platform, some attributes may or may not be displayed.

Logical Processor	Allows you to enable or disable logical processors and display the number of logical processors. If the **Logical Processor** option is set to **Enabled**, the BIOS displays all the logical processors. If this option is set to **Disabled**, the BIOS only displays one logical processor per core. By default, the **Logical Processor** option is set to **Enabled**.
QPI Speed	Allows you to set the QuickPath Interconnect (QPI) data rate settings. By default, the **QPI Speed** option is set to **Maximum data rate**. **NOTE: QPI Speed** displays only when both the processors are installed.
Alternate Requestor Transaction ID (RTID) Setting	Allows you to allocate more RTIDs to the remote socket, increasing cache performance between the sockets or work in normal mode for NUMA. By default, the **Alternate RTID (Requestor Transaction ID) Setting** is set to **Disabled**.
Virtualization Technology	Allows you to enable or disable the additional hardware capabilities provided for virtualization. By default, the **Virtualization Technology** option is set to **Enabled**.
Adjacent Cache Line Prefetch	Allows you to optimize the system for applications that require high utilization of sequential memory access. By default, the **Adjacent Cache Line Prefetch** option is set to **Enabled**. You can disable this option for applications that require high utilization of random memory access.

Hardware Prefetcher	Allows you to enable or disable the hardware prefetcher. By default, the **Hardware Prefetcher** option is set to **Enabled**.
DCU Streamer Prefetcher	Allows you to enable or disable the Data Cache Unit (DCU) streamer prefetcher. By default, the **DCU Streamer Prefetcher** option is set to **Enabled**.
DCU IP Prefetcher	Allows you to enable or disable the Data Cache Unit (DCU) IP prefetcher. By default, the **DCU IP Prefetcher** option is set to **Enabled**.
Execute Disable	Allows you enable or disable execute disable memory protection technology. By default, the **Execute Disable** option is set to **Enabled**.
Logical Processor Idling	Allows you to enable or disable the OS capability to put logical processors in the idling state in order to reduce power consumption. By default, the option is set to **Disabled**.
Number of Cores per Processor	Allows you to control the number of enabled cores in each processor. By default, the **Number of Cores per Processor** option is set to **All**.
Processor 64-bit Support	Specifies if one or more processors support 64-bit extensions.
Processor Core Speed	Displays the maximum core frequency of the processor.
Processor Bus Speed	Displays the bus speed of the processors. **NOTE:** The processor bus speed option displays only when both the processors are installed.
Processor 1	**NOTE:** The following settings are displayed for each processor installed in the system.
Family-Model-Stepping	Displays the family, model, and stepping of the processor as defined by Intel.
Brand	Displays the brand name reported by the processor.
Level 2 Cache	Displays the total L2 cache.
Level 3 Cache	Displays the total L3 cache.
Number of Cores	Displays the number of cores per processor.
Dell Controlled Turbo	Allows you to control turbo engagement. This feature is also referred to as Dell Processor Acceleration Technology (DPAT).

NOTE: Depending on the platform, some attributes may or may not be displayed.

SATA Settings Screen

Embedded SATA	Allows the embedded SATA to be set to Off, ATA, AHCI, or RAID mode. By default, Embedded SATA is set to **AHCI Mode**.
Port A	Auto enables BIOS support for the device attached to SATA port A. By default, Port A is set to **Auto**.
Port B	Auto enables BIOS support for the device attached to SATA port B. By default, Port B is set to **Auto**.
Port C	Auto enables BIOS support for the device attached to SATA port C. By default, Port C is set to **Auto**.
Port D	Auto enables BIOS support for the device attached to SATA port D. By default, Port D is set to **Auto**.
Port E	Auto enables BIOS support for the device attached to SATA port E. By default, Port E is set to **Auto**.
Port F	Auto enables BIOS support for the device attached to SATA port F. By default, Port F is set to **Auto**.

NOTE: Ports A, B, C, and D are used for the backplane drives, port E for the optical drive (CD/DVD), and port F for the tape drive.

Boot Settings screen

Boot Mode	Allows you to set the boot mode of the system.

CAUTION: Switching the boot mode may prevent the system from booting if the operating system is not installed in the same boot mode.

If the operating system supports UEFI, you can set this option to UEFI. Setting this field to BIOS allows compatibility with non-UEFI operating systems. By default, the **Boot Mode** option is set to **BIOS**.

NOTE: Setting this field to UEFI disables BIOS Boot Settings menu. Setting this field to BIOS disables the UEFI Boot Settings menu.

Boot Sequence Retry	Allows you to enable or disable the boot sequence retry feature. If this field is enabled and the system fails to boot, the system reattempts the boot sequence after 30 seconds. By default, the **Boot Sequence Retry** option is set to **Disabled**.
BIOS Boot Settings	Allows you to enable or disable BIOS Boot options. **NOTE:** This option is enabled only if the boot mode is BIOS.
UEFI Boot Settings	Allows you to enable or disable UEFI Boot options. The Boot options include **IPv4 PXE** and **IPv6 PXE**. By default, the **UEFI PXE boot protocol** is set to **IPv4**. **NOTE:** This option is enabled only if the boot mode is UEFI.
One-Time Boot	Allows you to enable or disable a one-time boot from a selected device.

Integrated devices screen

Integrated RAID Controller	Allows you to enable or disable the integrated RAID controller. By default, the **Integrated RAID Controller** option is set to **Enabled**.
User Accessible USB Ports	Allows you enable or disable the user accessible USB ports. Selecting **Only Back Ports On** disables the front USB ports and selecting **All Ports Off** disables both front and back USB ports. By default, the **User Accessible USB Ports** option is set to **All Ports On**.
Internal USB Port	Allows you to enable or disable the internal USB port. By default, the **Internal USB Port** option is set to **On**.
Internal SD Card Port	Enables or disables the system's internal SD card port. By default, the **Internal SD Card Port** option is set to **On**. **NOTE:** This option is displayed only if IDSDM is installed on the system board.
Internal SD Card Redundancy	If set to **Mirror** mode, data is written on both SD cards. If any one of the SD card fails, data is written to the active SD card. Data from this card is copied to the replacement SD card at the next boot. By default, **Internal SD Card Redundancy** option is set to **Mirror**. **NOTE:** This option is displayed only if IDSDM is installed on the system board.
Integrated Network Card 1	Allows you to enable or disable the integrated network card 1. By default, the **Integrated Network Card 1** option is set to **Enabled**.
OS Watchdog Timer	Allows you to enable or disable the OS watchdog timer. When this field is enabled, the operating system initializes the timer and the OS watchdog timer helps in recovering the operating system. By default, the **OS Watchdog Timer** option is set to **Disabled**.
Embedded Video Controller	Allows you to enable or disable the **Embedded Video Controller**. By default, the embedded video controller is set to **Enabled**.
SR-IOV Global Enable	Allows you to enable or disable the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. By default, the **SR-IOV Global Enable** option is set to **Disabled**.
Memory Mapped I/O above 4GB	Allows you to enable support for PCIe devices that require large amounts of memory. By default, the option is set to **Enabled**.
Slot Disablement	Allows you to enable or disable available PCIe slots on your system. The **Slot Disablement** feature controls the configuration of PCIe cards installed in the specified slot.

CAUTION: Slot disablement must be used only when the installed peripheral card is preventing booting into the Operating System or causing delays in system startup. If the slot is disabled, both the Option ROM and UEFI driver are disabled.

Serial communications screen

Serial Communication	Allows you to select serial communication devices (Serial Device 1 and Serial Device 2) in the BIOS. BIOS console redirection can also be enabled and the port address can be specified. By default, **Serial Communication** option is set to **On without Console Redirection**.
Serial Port Address	Allows you to set the port address for serial devices. By default, the **Serial Port Address** option is set to **Serial Device 1=COM2, Serial Device 2=COM1**. **NOTE:** Only Serial Device 2 can be used for Serial Over LAN (SOL). To use console redirection by SOL, configure the same port address for console redirection and the serial device.
External Serial Connector	Allows you to associate the external serial connector to serial device 1, serial device 2, or remote access device. By default, the **External Serial Connector** option is set to **Serial Device1**. **NOTE:** Only Serial Device 2 can be used for SOL. To use console redirection by SOL, configure the same port address for console redirection and the serial device.
Failsafe Baud Rate	Displays the failsafe baud rate for console redirection. The BIOS attempts to determine the baud rate automatically. This failsafe baud rate is used only if the attempt fails and the value must not be changed. By default, the **Failsafe Baud Rate** option is set to **11520**.
Remote Terminal Type	Allows you to set the remote console terminal type. By default, the **Remote Terminal Type** option is set to **VT 100/VT 220**.
Redirection After Boot	Allows you to enable or disable to the BIOS console redirection when the operating system is loaded. By default, the **Redirection After Boot** option is set to **Enabled**.

System Profile Settings screen

You can use the **System Profile Settings** screen to enable specific system performance settings such as power management.

To view the **System Profile Settings** screen, click **System Setup Main Menu** > **System BIOS** > **System Profile Settings**.

The **System Profile Settings** screen details are explained as follows:

System Profile	Sets the system profile. If you set the **System Profile** option to a mode other than **Custom**, the BIOS automatically sets the rest of the options. You can only change the rest of the options if the mode is set to **Custom**. This option is set to **Performance Per Watt Optimized (DAPC)** by default. DAPC is Dell Active Power Controller.**Performance Per Watt (OS)**. **NOTE:** All the parameters on the system profile setting screen available only when the **System Profile** option is set to **Custom**.
CPU Power Management	Sets the CPU power management. This option is set to **System DBPM (DAPC)OS DBPM** by default. DBPM is Demand-Based Power Management.
Memory Frequency	Sets the speed of the system memory. You can select **Maximum Performance**, **Maximum Reliability**, or a specific speed.
Turbo Boost	Enables or disables the processor to operate in turbo boost mode. This option is set to **Enabled** by default.
C States	Enables or disables the processor to operate in all available power states. This option is set to **Enabled** by default.
Monitor/Mwait	Enables the Monitor/Mwait instructions in the processor. This option is set to **Enabled** for all system profiles, except **Custom** by default. **NOTE:** This option can be disabled only if the **C States** option in the **Custom** mode is set to **disabled**.

NOTE: When **C States** is set to **Enabled** in the **Custom** mode, changing the Monitor/Mwait setting does not impact the system power or performance.

Memory Patrol Scrub	Sets the memory patrol scrub frequency. This option is set to **Standard** by default.
Memory Refresh Rate	Sets the memory refresh rate to either 1x or 2x. This option is set to **1x** by default.
Memory Operating Voltage	Sets the DIMM voltage selection. When set to Auto, the system automatically sets the system voltage to the optimal setting based on the DIMM capacity and the number of DIMMs installed. By default, the Memory Operating Voltage option is set to Auto.
Collaborative CPU Performance Control	Enables or disables the CPU power management. When set to **Enabled**, the CPU power management is controlled by the OS DBPM and the System DBPM (DAPC). This option is set to **Disabled** by default.

System security screen

Intel AES-NI	Improves the speed of applications by performing encryption and decryption using the Advanced Encryption Standard Instruction Set and is set to **Enabled** by default.
System Password	Allows you to set the system password. This option is set to **Enabled** by default and is read-only if the password jumper is not installed in the system.
Setup Password	Allows you to set the setup password. This option is read-only if the password jumper is not installed in the system.
Password Status	Allows you to lock the system password. By default, the **Password Status** option is set to **Unlocked**.
TPM Security	Allows you to control the reporting mode of the Trusted Platform Module (TPM). By default, the **TPM Security** option is set to **Off**. You can only modify the TPM Status, TPM Activation , and Intel TXT fields if the **TPM Status** field is set to either **On with Pre-boot Measurements** or **On without Pre-boot Measurements**. NOTE: TPM update is blocked form LC UI.
TPM Activation	Allows you to change the operational state of the TPM. By default, the **TPM Activation** option is set to **No Change**.
TPM Status	Displays the TPM status.
TPM Clear	CAUTION: **Clearing the TPM results in the loss of all keys in the TPM. The loss of TPM keys may affect booting to the operating system.** Allows you to clear all the contents of the TPM. By default, the **TPM Clear** option is set to **No**.
Intel TXT	Allows you to enable or disable Intel Trusted Execution Technology (TXT). To enable **Intel TXT**, Virtualization Technology must be enabled and TPM Security must be **Enabled** with Pre-boot measurements. By default, the **Intel TXT** option is set to **Off**.
BIOS Update Control	Allows you to update the BIOS using either DOS or UEFI shell-based flash utilities. For environments that do not require local BIOS updates, it is recommended to set this option to **Disabled**. By default, the **BIOS Update Control** option is set to **Unlocked**. NOTE: BIOS updates using the Dell Update Package are not affected by this option.
Power Button	Allows you to enable or disable the power button on the front of the system. By default, the **Power Button** option is set to **Enabled**.
NMI Button	Allows you to enable or disable the NMI button on the front of the system. By default, the **NMI Button** option is set to **Disabled**.
AC Power Recovery	Allows you to set how the system reacts after AC power is restored to the system. By default, the **AC Power Recovery** option is set to **Last**. NOTE: Set the **AC Power Recovery** option to **On** or **Last** to enable or disable the **AC Power Recovery Delay** option.

AC Power Recovery Delay	Allows you to set how the system supports staggering of power up after AC power is restored to the system. By default, the **AC Power Recovery Delay** option is set to **Immediate**. **NOTE:** Set the **AC Power Recovery Delay** option to **User** to enable or disable the **User Defined Delay** option.
User Defined Delay (60s to 240s)	Allows you to set the **User Defined Delay** when the **User Defined** option for **AC Power Recovery Delay** is selected.

Miscellaneous settings

System Time	Allows you to set the time on the system.
System Date	Allows you to set the date on the system.
Asset Tag	Displays the asset tag and allows you to modify it for security and tracking purposes.
Keyboard NumLock	Allows you to set whether the system boots with the NumLock enabled or disabled. By default the **Keyboard NumLock** is set to **On**. **NOTE:** This option does not apply to 84-key keyboards.
Report Keyboard Errors	Allows you to set whether keyboard-related error messages are reported during system boot. By default, the **Report Keyboard Errors** option is set to **Report**.
F1/F2 Prompt on Error	Allows you to enable or disable the F1/F2 prompt on error. By default, **F1/F2 Prompt on Error** is set to **Enabled**.
In-System Characterization	This option enables or disables **In-System Characterization**. By default, **In-System Characterization** is set to **Enabled**.

System and setup password features

You can create a system password and a setup password to secure your system. To enable creation of the system and setup password, the password jumper must be set to enabled. For more information on the password jumper settings, see System Board Jumper Settings.

System password	This is the password that you must enter before you can boot your system.
Setup password	This is the password that you must enter to access and make changes to the BIOS or UEFI settings of your system.

CAUTION: Avoid leaving your system running and unattended. Enabling the password feature provides a basic level of security for the data on your system.

NOTE: Your system is shipped with the system and setup password feature disabled.

Assigning system and setup password

The password jumper enables or disables the system password and setup password features. For more information about the password jumper settings, see the System board jumper settings.

NOTE:

You can assign a new system password or setup password or change an existing system password or setup password only when the password jumper setting is enabled and **Password Status** is set to **Unlocked**. If the Password Status is set to **Locked**, you cannot change the system password or setup password.

If the password jumper setting is disabled, the existing system password and setup password is deleted and you need not provide the system password to boot the system.

1. To enter **System Setup**, press F2 immediately after a power-on or reboot.
2. In the **System Setup Main Menu**, select **System BIOS** and press Enter.
3. In the **System BIOS** screen, select **System Security** and press Enter.

4. In the **System Security** screen, verify that **Password Status** is **Unlocked**.
5. Select **System Password**, enter your system password, and press Enter or Tab.

   Use the following guidelines to assign the system password:
   - A password can have up to 32 characters.
   - The password can contain the numbers 0 through 9.
   - Only the following special characters are allowed: space, ("), (+), (,), (-), (.), (/), (;), ([), (\), (]), (`).

   A message prompts you to reenter the system password.
6. Reenter the system password and click **OK**.
7. Select **Setup Password**, enter your system password, and press Enter or Tab.
   A message prompts you to reenter the setup password.
8. Reenter the setup password click **OK**.
9. Press Esc to return to the System BIOS screen. Press Esc again, and a message prompts you to save the changes.

   NOTE: Password protection does not take effect until the system reboots.

Deleting or changing an existing system and setup password

Ensure that the Password jumper is set to enabled and the **Password Status** is **Unlocked** before attempting to delete or change the existing System and/or Setup password. You cannot delete or change an existing System or Setup password if the **Password Status** is **Locked**.

To delete or change the existing System and/or Setup password:

1. To enter System Setup, press **<F2>** immediately after a power-on or restart.
2. In the **System Setup Main Menu**, select **System BIOS** and press **<Enter>**.
   The **System BIOS** screen is displayed.
3. In the **System BIOS Screen**, select **System Security** and press **<Enter>**.
   The **System Security** screen is displayed.
4. In the **System Security** screen, verify that **Password Status** is **Unlocked**.
5. Select **System Password**, alter or delete the existing system password and press **<Enter>** or **<Tab>**.
6. Select **Setup Password**, alter or delete the existing setup password and press **<Enter>** or **<Tab>**.

   NOTE: If you change the System and/or Setup password a message prompts you to re-enter the new password. If you delete the System and/or Setup password, a message prompts you to confirm the deletion.
7. Press **<Esc>** to return to the System BIOS screen. Press **<Esc>** again, and a message prompts you to save the changes.

NOTE: You can disable password security while logging on to the system. To disable the password security, turn on or reboot your system, type your password and press **<Ctrl><Enter>**.

Using your system password to secure your system

Support site link

If you have assigned a setup password, the system accepts your setup password as an alternate system password.

1. Turn on or reboot your system.
2. Type the system password and press Enter.

When **Password Status** is set to **Locked**, type the system password and press Enter when prompted at reboot.

NOTE: If an incorrect system password is typed, the system displays a message and prompts you to reenter your password. You have three attempts to type the correct password. After the third unsuccessful attempt, the system displays an error message that the system has stopped functioning and must be turned off. Even after you turn off and restart the system, the error message is displayed until the correct password is entered.

Operating with a setup password enabled

If **Setup Password** is set to **Enabled**, type the correct setup password before modifying the system setup options.

If you do not type the correct password in three attempts, the system displays the following message:

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must
power down.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of
password attempts exceeded.System halted.
```

Even after you turn off and restart the system, the error message is displayed until the correct password is typed. The following options are exceptions:

- If **System Password** is not set to **Enabled** and is not locked through the **Password Status** option, you can assign a system password. For more information, see the System Security Settings screen section.
- You cannot disable or change an existing system password.

NOTE: You can use the password status option with the setup password option to protect the system password from unauthorized changes.

Entering the UEFI boot manager

NOTE: Operating systems must be 64-bit UEFI-compatible (for example, Microsoft Windows Server 2008 x64 version) to be installed from the UEFI boot mode. DOS and 32-bit operating systems can only be installed from the BIOS boot mode.

The Boot Manager enables you to:

- Add, delete, and arrange boot options.
- Access System Setup and BIOS-level boot options without restarting.

To enter the Boot Manager:

1. Turn on or restart your system.
2. Press **<F11>** after you see the following message:

   ```
   <F11> = UEFI Boot Manager
   ```

   If your operating system begins to load before you press **<F11>**, allow the system to finish booting, and then restart your system and try again.

Using the boot manager navigation keys

Up arrow	Moves to the previous field.
Down arrow	Moves to the next field.
<Enter>	Allows you to type in a value in the selected field (if applicable) or follow the link in the field.
Spacebar	Expands or collapses a drop-down list, if applicable.
<Tab>	Moves to the next focus area. **NOTE:** For the standard graphics browser only.
<Esc>	Moves to the previous page till you view the main screen. Pressing <Esc> in the main screen exits the Boot Manager and proceeds with system boot.
<F1>	Displays the System Setup help file.

NOTE: For most of the options, any changes that you make are recorded but do not take effect until you restart the system.

Boot Manager screen

Continue Normal Boot	The system attempts to boot to devices starting with the first item in the boot order. If the boot attempt fails, the system continues with the next item in the boot order until the boot is successful or no more boot options are found.
BIOS Boot Menu	Displays the list of available BIOS boot options (marked with asterisks). Select the boot option you wish to use and press <Enter>.
UEFI Boot Menu	Displays the list of available UEFI boot options (marked with asterisks). Select the boot option you wish to use and press <Enter>. The UEFI Boot Menu enables you to **Add Boot Option**, **Delete Boot Option**, or **Boot From File**.
Driver Health Menu	Displays a list of the drivers installed on the system and their health status.
Launch System Setup	Enables you to access the System Setup.
System Utilities	Enables you to access the BIOS Update File Explorer, run the Dell Diagnostics program, and reboot the system.

UEFI Boot menu

Select UEFI Boot Option	Displays the list of available UEFI boot options (marked with asterisks), select the boot option you wish to use and press <Enter>.
Add Boot Option	Adds a new boot option.
Delete Boot Option	Deletes an existing boot option.
Boot From File	Sets a one-time boot option not included in the boot option list.

Embedded systems management

The Lifecycle controller provides advanced embedded systems management throughout the system's lifecycle. The Lifecycle controller can be started during the boot sequence and can function independently of the operating system.

NOTE: Certain platform configurations may not support the full set of features provided by the Lifecycle controller.

For more information about setting up the Lifecycle controller, configuring hardware and firmware, and deploying the operating system, see the Lifecycle controller documentation at Dell Lifecycle Controller Overview White Paper.

iDRAC settings utility

The iDRAC Settings utility is an interface to set up and configure the iDRAC parameters using UEFI. You can enable or disable various iDRAC parameters using the iDRAC Settings Utility.

NOTE: Accessing some of the features on the iDRAC Settings Utility requires the iDRAC Enterprise License upgrade.

For more information on using iDRAC, see Integrated Dell Remote Access Controller User's Guide.

Entering the iDRAC settings utility

1. Turn on or restart the managed system.
2. Press <F2> during POST.
3. In the **System Setup Main Menu** page, click **iDRAC Settings**.
   The iDRAC Settings screen is displayed.

10

Troubleshooting and frequently asked questions

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

Topics:

- Error messages
- Frequently asked questions

Error messages

Each error message that is generated from Lifecycle Controller has a Message ID, Message Description, and Recommended Response Action in a single dialog box. If you want to view the detailed description about a message, see the Dell Event Message Reference Guide at Dell Support page.

Frequently asked questions

1. **When Lifecycle Controller downloads updates where are the files stored?**

   The files are stored in a volatile memory, on the main system board. This memory is not removable and is not accessible through the operating system.
2. **Is a virtual media device 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 disk drives that a server identifies as local media.
4. **What should I do if an update fails?**

   If an update fails, the Lifecycle Controller restarts, and then attempts all the pending updates that are selected. After the final restart, the system opens the Lifecycle Controller **Home** page. Launch **Firmware Update** again, select the updates that failed, and then click **Apply**.

   NOTE: If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another iDRAC firmware update.
5. **Can I add my own drivers to use for operating system installation?**

   No, you cannot add your own drivers for operating system installation. For more information about updating the drivers that are used for operating system installation, see Updating Platform.
6. **Can I update the drivers used by an already-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.
7. **Can I add my own drivers and firmware for updating Lifecycle Controller to a local USB drive?**

   No, only drivers and firmware downloaded from the **Dell server Updates**DVD are supported. For more information, see Configuring Local USB Drive.
8. **Can I delete Lifecycle Controller?**

   No.
9. **Can I use a virtual media for the operating system media source during installation?**

Yes. For more information about iDRAC, see

Integrated Dell Remote Access Controller User's Guide.

10. **Can I use a virtual USB drive to update the repository?**

    Yes. For more information about using a virtual USB drive to update the repository, see

    Integrated Dell Remote Access Controller User's Guide.

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

    Unified Extensible Firmware Interface (UEFI) is a specification that defines a model for the interface between the operating systems and firmware on a server. The interface consists of data tables that contain platform-related information, along with boot and runtime calls available to the operating system and operating system loaders. This interface provides a standard environment for booting an operating system and running preboot applications. Lifecycle Controller complies with the UEFI version 2.3. For more information, go to
    UEFI page.

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

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

    Configuration Wizards guide you through a sequence of tasks to configure your system devices. The Configuration Wizards include iDRAC, RAID, System Date/Time, and Physical Security. For more information, see Configuring System and Advanced Hardware Configuration.

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

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

    Yes. For more information, see Firmware Rollback.

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

    Currently, Lifecycle Controller supports updates to the BIOS, iDRAC firmware, power supply firmware, and certain RAID and NIC controller firmware. For more information, see Updating Firmware.

15. **What should I do if my system stops responding while using Lifecycle Controller?**

    If your system stops responding while using Lifecycle Controller, a black screen with red text is displayed. To resolve this problem, try restarting your system and enabling Lifecycle Controller. If the issue persists, contact your service provider. For more information about recovering Lifecycle Controller from the
    Lifecycle Controller Update Required mode, see the
    Recovery from Lifecycle Controller Update Required white paper.

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

    Click
    About on the upper right corner of the Lifecycle Controller home page.

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

    Make sure that the
    Single Cursor option under
    Tools menu is selected on the iDRAC Virtual Console client. For more information, see

    Integrated Dell Remote Access Controller User's Guide.

18. **Why should the CSIOR be enabled?**

    The Collect System Inventory On Restart (CSIOR) option must be enabled so that the Lifecycle Controller can automatically collect the details of the hardware and software available on the system, update the database, and invoke part firmware update and hardware configuration at system startup. If you do not enable CSIOR, you must boot into the Lifecycle Controller GUI and exit to sync and update software or hardware inventory.

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

    The features such as Lifecycle Log, Hardware Inventory (View and Export), and Part Replacement depend on the latest iDRAC firmware. Make sure that the latest iDRAC firmware with Enterprise license is installed.

20. **What should I do when 'LC in Use RED023' error screen shows up ?**

LC in use RED023 message is displayed in LCL if the host is not in the operating system or if not at POST. Screen shows the F11/F12/F10 option. You see this behavior if the host is in LC and any update or configuration operation is triggered. To come out of LC in use, reboot the host or enter the OS. Follow these steps to fix this issue:

- Make sure all other Lifecycle Controller operations are finished and retry the operation.
- Using the iDRAC Web UI, select **Server** and then click **Job Queue**, check the job queue for unfinished jobs and wait for the jobs to finish before retrying the operation.
- Also, check whether there are update packages being performed in the server operating system and wait for those operations to finish before retrying the operation.
- For remote web service API access, make sure that the `GetRemoteServicesAPIStatus` method returns **Ready** status, and then retry the operation.
- If operating system Deploy has been enabled, then boot the server into LC UI to clear. Always exit LC UI by clicking **Exit** and not by powering off.

21. **The Select Media option in Lifecycle Controller GUI may display unknown characters in media file name**—To fix this issue, reformat the ISO with the volume name and mount it again.