Dell Lifecycle Controller Integration Version 3.3 for Microsoft System Center Configuration Manager

User's Guide

1

January 2017
Rev. A00

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.

Contents

1

Introduction to Dell Lifecycle Controller Integration (DLCI) for Microsoft System Center Configuration Manager

Dell Lifecycle Controller Integration (DLCI) for Microsoft System Center Configuration Manager (Configuration Manager) enables the administrators to leverage the remote enablement capabilities of Dell Lifecycle Controller, available as part of the Integrated Dell Remote Access Controller (iDRAC).

Configuration Manager is used in this document with reference to the following products:

- Microsoft System Center Configuration Manager Version 1610
- Microsoft System Center 2012 SP2 Configuration Manager
- Microsoft System Center 2012 R2 SP1 Configuration Manager
- Microsoft System Center 2012 R2 Configuration Manager
- Microsoft System Center 2012 SP1 Configuration Manager
- Microsoft System Center 2012 Configuration Manager

NOTE:

This document contains information on the prerequisites and supported software necessary for installing DLCI version 3.3 for Configuration Manager. If you are installing this version of DLCI for Microsoft Configuration Manager after a long time after its release date, check to see if there is an updated version of this document at `Dell.com/support/home`.

At a high level, the remote enablement capabilities include:

- Autodiscovery
- Hardware configuration
- Firmware comparison and updates
- Remote operating system deployment for a collection of Dell systems

Topics:

What's new in this release

This release of DLCI for Configuration Manager provides support for the following features:

Table 1. New features and functionalities

New feature	Description
Support for Microsoft System Center Configuration Manager Version 1610	Allows you to install DLCI 3.3 for Configuration Manager Version 1610
Support for Agent-free properties	Displays the Dell Lifecycle Controller Agent-free properties for configuration manager
Support for deployment of Windows 2016, ESXi 6.0 U2 and RHEL 6.8	Allows you to install Windows 2016, ESXi 6.0 U2 and RHEL 6.8 operating systems
Support for 64–bit firmware update	Supports 64–bit Dell Update Packages

Table 1. New features and functionalities (continued)

New feature	Description
Support for Dell's 13th generation of PowerEdge servers	With this version, you can configure the 13th generations of Dell PowerEdge servers through Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC)

Existing features and functionalities

Table 2. Features and functionalities

Feature	Functionality
Configuration Manager distributed environment	Support for Configuration Manager, when the configuration manager is set up in a distributed environment.
Configure and deploy operating system on Dell's 11th generation and 12th generation of PowerEdge servers.	You can configure Dell's 11th generation or 12th generation of PowerEdge servers using DLCI through Lifecycle Controller. All the features of previous version of DLCI are supported for 12th generation or 11th generation PowerEdge servers.
A single installer to install and configure DLCI	You can use the single installer to install DLCI 3.3 in environments (Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012) based on the version of Configuration Manager present in the system. If a DLCI 3.2 is present, then the installer initiates an upgrade. The installer deploys appropriate components based on the Configuration Manager version.
Automatically configure Dell Provisioning Server	You can automatically configure Dell Provisioning Server for non-administrator users by selecting the **Automatically configure Dell Provisioning Server user permissions** option during installation.
Deploying customized images using Dell driver CAB files	You can create and deploy customized images on Dell Enterprise servers. For more information, see Adding Dell driver packages on page 25.
Platform Restore	You can restore a profile for a system or a collection that includes: • Scheduling a backup, and exporting system profiles to an external share/vFlash. • Importing the saved system profiles from an external share/vFlash. • Configuring Part Replacement properties for a system or a collection. For more information, see Platform restore for a system on page 62 and Platform restore for a collection on page 46.
Viewing and exporting the Lifecycle Controller logs	You can view the Lifecycle Controller logs of a system or a collection in a readable format and save or export the logs to a .CSV file. In addition, you can filter logs and view the number of logs based on the search string. For more information, see Viewing Lifecycle Controller logs on page 59 and Viewing and exporting Lifecycle Controller logs for a collection on page 44.
Configure network interface cards (NICs) and converged network adapters (CNAs)	You can configure different attributes of specific NICs or CNAs in the system and save them to a profile. The saved profiles can later be applied to a collection as part of the hardware configuration or operating system deployment, or both.

Table 2. Features and functionalities (continued)

Feature	Functionality
	You can also compare the applied NIC/CNA profiles against the NIC/CNA configurations of the systems and generate comparison reports. For more information, see: ● Configuring NICs and CNAs for a system on page 54. ● Applying a NIC or CNA profile on a collection on page 39. ● Comparing NIC or CNA profiles against systems in a collection on page 47.
Configure iDRAC profiles for a system or collection	You can define iDRAC configurations for a system and save it as part of a hardware configuration profile of the system. The saved profiles are applied later to the collection as part of the hardware configuration or operating system deployment, or both. For more information, see Configuring iDRAC profiles for a system on page 53.
Connect to Dell FTP for Firmware updates	You can now connect to the FTP site and perform the following tasks: ● Download firmware updates for a system or a collection. ● Determine the status of the firmware if the firmware of your collection is compliant, or needs an update. ● Schedule a firmware update for a single system or a collection of systems. ● Export an inventory of chassis and servers from DLCI and use this information to create repository using Dell Repository Manager (DRM). For more information, see: ● Comparing and updating firmware inventory on page 58. ● Comparing and updating firmware inventory for systems in a collection on page 43.
Import Dell Servers and System Variables	You can import Dell servers that are not auto-discovered by DLCI for Configuration Manager. The imported servers appear under the All Dell Lifecycle Controller Servers. You can use the DLCI utilities to perform the various activities on the servers. You can also import system variables present in a .CSV file to systems present within a collection on the Configuration Manager console. For more information, see Using the Import Server Utility on page 48.
Access iDRAC using Active Directory credentials for authentication	You can provide Active Directory credentials to get authenticated on iDRAC.
Schedule firmware updates and perform selective firmware update	You can schedule updates for firmware. Also, you can select the server components that need to be updated. For more information, see Comparing and updating firmware inventory on page 58.
Configure certificate authority (CA) and common name (CN) checks	You can configure CA and CN checks for DLCI communication with the targets.
Auto-discovery and Handshake	This feature enables the iDRAC on bare metal systems to locate the provisioning service and establish communication with the Site Server. For more information, see Auto-discovery and handshake on page 22.

Table 2. Features and functionalities (continued)

Feature	Functionality
System Viewer utility	This feature enables you to configure individual systems by using the remote enablement capabilities of DLCI. For more information, see Using the System Viewer Utility on page 51.
Config Utility	This feature enables you to configure a collection of systems by using the remote enablement capabilities of Lifecycle Controller. For more information, see Using the Configuration Utility on page 34.
Launching the iDRAC Console	This feature enables you to launch the iDRAC console from the Task Viewer and from a system in the collection that contains Dell's 11th generation to 13th generation of PowerEdge systems. For more information, see Launching the integrated Dell Remote Access Controller console on page 26.
Support Unified Extensible Firmware Interface (UEFI) boot mode	This feature supports configuration of UEFI boot mode and BIOS attribute settings. For more information, see Changing the BIOS or UEFI boot sequence and hard disk drive sequence on page 53.
Task Viewer	This feature enables you to track the status of the tasks handled by DLCI for Configuration Manager. For more information, see Task Viewer.
Support for viewing and configuring Fibre Channel (FC) host bus adapters (HBA) for servers	Allows you to inventory and configure FC HBA cards.
Support for configuring Storage area network (SAN) boot attributes	Allows you to configure SAN boot attributes.
Support for exporting the system profiles before and after hardware configuration	Allows you to back up the system profiles for a collection of systems by exporting the profile to an iDRAC vFlash card or a network share.
Compare the applied FC HBA profiles against the systems in a collection and generate comparison reports	Allows you to view the comparison report between an FC HBA profile and a selected server.
Support for ESXi 5.5 Update 3	Allows you to deploy ESXi operating systems on a collection.
Support for Red Hat Enterprise Linux (RHEL) 7.2 versions	Allows you to deploy RHEL operating systems on a collection.

Supported operating systems

For information on supported operating systems, see the *Dell Lifecycle Controller Integration Version 3.3 for Microsoft System Center Configuration Manager Installation Guide* at `Dell.com/support/home`.

Supported Microsoft .NET versions

For information on supported Microsoft .NET versions, see the *Dell Lifecycle Controller Integration Version 3.3 for Microsoft System Center Configuration Manager Installation Guide* at `Dell.com/support/home`.

Supported target systems

For the list of supported target systems and the operating systems (Windows only) that you can deploy on the target systems, see the *Unified Server Configurator/Unified Server Configurator-Lifecycle Controller Enabled- Supported Dell Systems and Operating Systems matrix* available at **Dell.com/support/home**. On the Manuals page, click **Software and Security** > **Enterprise System Management** > **OpenManage Software**. Select the OpenManage relevant release version and click the appropriate link. Click **Dell System Software Support Matrix** > **Dell System Software Support Matrix** > **View** >

Supported Dell Systems and Operating Systems. In the Support Matrix, view the target systems and operating systems that are supported by Unified Server Configurator – Lifecycle Controller Enabled.

Windows Preinstallation Environment (WinPE) compatibility matrix

The following table lists the operating systems that can be deployed by DLCI for Configuration Manager and their respective WinPE environments.

Table 3. Compatible operating systems for WinPE

Configuration Manager	WinPE version	Operating system
Configuration Manager Version 1610	10	• Windows Server 2012 R2 • Windows Server 2016
Configuration Manager 2012 SP2	5.0 and 10	• Windows Server 2008 R2* • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
Configuration Manager 2012 R2 SP1	5.0 and 10	• Windows Server 2008 R2* • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
Configuration Manager 2012 R2	5.0	• Windows Server 2008 R2* • Windows Server 2012 • Windows Server 2012 R2
Configuration Manager 2012 SP1	4.0	• Windows Server 2008 R2* • Windows Server 2012
Configuration Manager 2012	3.0	• Windows Server 2008 • Windows Server 2008 R2

Legend:

* — For Windows Server 2008 R2 support, visit **support.microsoft.com/kb/2853726**.

2

Use case scenarios

This section describes typical use cases and tasks that you can perform with DLCI for Microsoft System Center Configuration Manager (Configuration Manager).

Topics:

Common prerequisites

Before working on the user scenarios, Dell recommends that you complete the following prerequisites.

- In Configuration Manager, make sure that the system is discovered and present under **Assets and Compliance** > **Device Collections** > **All Dell Lifecycle Controller Servers**. For more information, see Auto-discovery and handshake on page 22.
- Install the latest BIOS version on the system.
- Install the latest version of Lifecycle Controller on the system.
- Install the latest version of iDRAC firmware on the system.

NOTE: Always launch the Configuration Manager console with administrator privileges.

Editing and exporting the BIOS configuration profile of a system

You can edit and export the BIOS configuration of a system as a profile and apply it when you are deploying the operating system to a collection of systems on the Configuration Manager console. For 13th generation of the Dell PowerEdge servers, you can only view the BIOS attributes and boot sequence of currently saved boot mode.

For more information, see Common prerequisites on page 12.

The following steps outline the workflow sequence:

1. Launch the **System Viewer** utility on the Configuration Manager console for a particular system. For more information, see System Viewer utility on page 25.
2. Select **BIOS Configuration** on the **System Viewer** utility to load the BIOS configuration of the system. For more information, see Viewing and editing BIOS configuration on page 51.
3. Create a profile or change an existing profile. For more information, see Creating a new profile on page 52 or Editing an existing profile on page 52.
4. Add, edit, or update the attributes in the profile. For more information, see Adding a new attribute on page 52 and Editing an existing BIOS attribute on page 52.
5. (Optional) Change the BIOS or UEFI boot sequence and hard disk drive sequence. For more information, see Changing the BIOS or UEFI boot sequence and hard disk drive sequence on page 53.

6. Save the profile as a .XML file to any folder location on the local system.

Comparing and updating the firmware inventory

You can use DLCI for Configuration Manager to compare and update the firmware inventory of a single system, or a collection of systems. You can compare the firmware inventory against a given inventory profile, Dell FTP site, or a PDK catalog created by Repository Manager.

Prerequisites

- Common prerequisites on page 12.
- Make sure that you have access to the Common Internet File System (CIFS) share where the Plug-in Deployment Kit (PDK) catalog is located or Dell FTP site (**`ftp.Dell.com`**).
- To compare against an existing profile, create a Hardware inventory profile. For more information, see Creating a new profile on page 52.

Prerequisites for CMC firmware update:

- Dell PowerEdge M1000e CMC 5.0 or later versions are supported.
- Dell CMC PowerEdge VRTX 2.0 or later versions are supported.
- The target system must have iDRAC7 with Enterprise licenses (12th generation and later versions).
- Dell Repository Manager 1.8 or later versions are supported.

  NOTE:
  - 11th generation servers support 32–bit Dell update package (DUP).
  - 12th generation servers support 32–bit DUP earlier than iDRAC 1.51.51 versions.
  - 12th generation servers with iDRAC 1.51.51 and later versions supports 64–bit DUP.
  - 13th generation servers support 64–bit DUP.

Workflow sequence for comparing and updating the firmware inventory

The following steps outline the workflow sequence:

1. To compare and update the Firmware inventory of a single target system, launch the **System Viewer** utility. To compare and update the Firmware inventory of a collection of systems, launch the **Config Utility**. For more information, see System Viewer utility on page 25 or Configuration utility on page 26.
2. Select **Firmware Inventory, Compare, and Update** from the **System Viewer** utility or **Config Utility**.
3. For a single system, see Comparing and updating firmware inventory on page 58.
4. For a collection, see Comparing and updating firmware inventory for systems in a collection on page 43.

Creating, editing, and saving a RAID profile of a system

You can create, edit, and save the RAID profile of a system and apply it when you deploy an operating system to a collection of systems on the Configuration Manager console.

Prerequisites

- Common prerequisites on page 12
- RAID controller and firmware that supports Local Key Management

The following steps outline the workflow sequence:

1. Launch the **System Viewer** utility on the Configuration Manager console for a particular system. For more information, see System Viewer utility on page 25.

2. Select **RAID Configuration** on the **System Viewer** utility to load the RAID configuration of the system. For more information, see Viewing and configuring RAID on page 53.
3. Launch **Array Builder** to create a RAID profile. For more information, see Creating a RAID Profile using Array Builder on page 29.
4. (Optional) Import and edit an existing profile. For more information, see Importing a profile on page 33.
5. Save the newly created RAID profile as a .XML file to any folder location on the local system.

Deploying operating system on collection

You can use DLCI for Configuration Manager to deploy an operating system on a collection of systems on the Configuration Manager console.

Prerequisites

- Common prerequisites on page 12.
- Select the Driver CAB which is compatible with the boot image (WinPE version). You can view the DTK README to select the correct version of the CAB file for specific WinPE or OS architecture, and provide the location of the DTK Self-Extracting EXE. For more information, see Importing Dell driver files on page 20.
- Create a task sequence boot media for the collection of systems with an iDRAC to boot to the task sequence ISO. For more information, see Creating a task sequence media bootable ISO on page 25.
- For prerequisites on the non-Windows operating systems deployment task, see section "Software Prerequisites and Requirements" in the *Dell Lifecycle Controller Integration for Microsoft System Center Configuration Manager Version 3.3 Installation Guide*.

  NOTE:

  In Configuration Manager 2012, operating system deployment is not supported in UEFI boot mode. For more information, see **technet.microsoft.com/en-in/library/jj591552.aspx**.

The following steps outline the workflow sequence:

1. In the Configuration Manager console, under **Device Collections,** right-click **Managed Dell Lifecycle Controllers (OS Unknown)** and select **Dell Lifecycle Controller Launch Config Utility**.
2. In the **Dell Lifecycle Controller Configuration Utility**, select **Deploy Operating System**.
3. Update the firmware from a Dell repository. For more information, see Updating firmware during OS deployment on page 38.
4. Configure or edit the BIOS/NIC profiles. For more information, see Configuring hardware during OS deployment on page 38.
5. Apply FC HBA profiles and FC SAN boot attributes on a collection. For more information, see Applying FC HBA profiles and FC SAN boot attributes on a collection on page 40.
6. Configure or edit the RAID profiles. For more information, see Configuring RAID on page 39.
7. Apply NIC/CNA profiles to the collection. For more information, see Applying a NIC or CNA profile on a collection on page 39.
8. Apply iDRAC profiles to the collection. For more information, see Applying an integrated Dell Remote Access Controller profile on a collection on page 41.
9. Deploy the operating system and boot the systems to the media of your choice. For more information, see step 15 in Hardware configuration and OS deployment workflow on page 37.

Exporting server profile to iDRAC vFlash card or network share

You can backup the server profile as an image file for a single system or a collection of systems by exporting the profile to an iDRAC vFlash card or to an external source or a network share.

Prerequisites

- Common prerequisites on page 12
- Target system with valid seven character service tag

- iDRAC vFlash card:
  - Installed as a license, enabled, and initialized

    NOTE: The iDRAC vFlash card is required only for Dell's 11th generation of PowerEdge servers. For the 12th and 13th generation of PowerEdge servers, you must have an Enterprise license.
  - With a minimum free space of 384 MB available.
- Network Share:
  - Permissions and firewall settings are provided for the iDRAC to communicate with the system that has the network share.
  - With a minimum free space of 384 MB available
- Administrator privileges on the iDRAC of the target systems

Before you begin

Before you begin exporting the system profile for a single system or a collection:

- Make sure that operations such as firmware update, operating system deployment, and firmware configurations are not running.
- After you deploy the operating system using Lifecycle controller, the Original Equipment Manufacturer Drive (OEMDRV) is open for 18 hours as the Lifecycle Controller does not have the status of the operating system installation. If you need to perform the operations such as update, configuration, or restore after you deploy the operating system, remove the OEMDRV partition. To remove the partition, reset iDRAC or cancel System Services.

  For more information on resetting iDRAC or cancelling system services, see the *Dell Lifecycle Controller Remote Services User's Guide* available at **Dell.com/support/home**.
- If you have scheduled the backup, then do not schedule any other remote services jobs such as BIOS updates or RAID configuration on the target systems.
- Make sure that the backup image file is not tampered with, either during export or after export.

Workflow for exporting server profile

The following steps outline the workflow sequence:

1. To export the system profile of a single target system, launch the **System Viewer** utility. To export the system profiles of a collection of systems, launch the **Config Utility**. For more information, see System Viewer utility on page 25 or Configuration utility on page 26.
2. Select the **Platform Restore** on the **System Viewer** utility or the **Config Utility**.
3. For a single system, see Exporting the system profile on page 62.
4. For a collection, see Exporting the system profiles in a collection on page 46.

Importing server profile from iDRAC vFlash card or network share

You can restore the backup of a system profile for a single system or a collection of systems from an iDRAC vFlash card or a network share using DLCI for Configuration Manager.

Prerequisites

- Common prerequisites on page 12
- iDRAC vFlash card:
  - Is installed as a license, enabled and has the SRVCNF partition. In Lifecycle Controller, during backup, a partition with a label name SRVCNF is automatically created on the vFlash SD card to store the backup image file. If a partition with the label name SRVCNF already exists, it is overwritten. For more information, see Lifecycle Controller documentation at **Dell.com/support/manuals**.
  - Has minimum free space of 384 MB available.

- If you are importing from an iDRAC vFlash card, make sure that the card is installed and has the backup image in the SRVCNF partition. This image is from the same platform that you are importing.
- If you are importing from a network share, make sure that the network share where the backup image file is stored is still accessible.
- If you replace the motherboard before performing import, make sure that the motherboard has the latest iDRAC and BIOS installed.

NOTE: The service tag of the server is either blank or same as when the backup was taken.

Before you begin

Before you begin importing the backup file to a system or collection, ensure that:

- User Data is not present in the backup image file. If you overwrite the existing configuration with the backup image file, the user data is not restored.
- During import, operations such as firmware update, operating system deployment, and firmware configurations are not running.
- After you deploy the operating system using Lifecycle controller, the OEMDRV is open for 18 hours. If you need to perform the operations such as update, configuration, or import after operating system deployment, remove the OEMDRV partition. To remove the partition, reset iDRAC or cancel **System Services**.

Workflow for importing server profile

The following steps outline the workflow sequence:

1. To import the system profile of a single target system, launch the **System Viewer** utility. To import the system profiles of a collection of systems, launch the **Config Utility**. For more information, see System Viewer utility on page 25 or Configuration utility on page 26.
2. Select the **Platform Restore** on the **System Viewer** utility or the **Config Utility**.
3. For a single system, see Importing the system profile on page 63.
4. For a collection, see Importing the system profiles in a collection on page 46.

Viewing and exporting Lifecycle Controller logs

You can view the Lifecycle Controller Logs for a single system or a collection and also export them in a .CSV format to a network share folder. You can search and filter the Lifecycle Controller logs using **Search** field.

Prerequisites

- Common prerequisites on page 12
- Network Share:
  - iDRAC can access the network share.
  - iDRAC has the necessary permissions to write information to network share.
  - Minimum free space of 384 MB is available.
- Configure the number of log files you want to view at a time in the DLCSystemview.exe.config or the DLCConfigUtility.exe.config files. For more information, see Viewing Lifecycle Controller logs on page 59.

Before you begin

Before you begin viewing or exporting the Lifecycle Controller logs for a single system or a collection:

- If the Lifecycle Controller on the target systems is running other tasks such as firmware update, operating system deployment, firmware configurations, exporting a system profile or importing a system profile, wait for the tasks to complete before you retrieve the logs.
- Check the permissions on the network share and make sure the share is accessible from the Lifecycle Controller on the target systems.

Workflow for viewing and exporting Lifecycle Controller logs

The following steps outline the workflow sequence:

1. To view the Lifecycle Controller logs of a single target system, launch the **System Viewer** utility. To view the Lifecycle Controller logs of a collection of systems, launch the **Config Utility**. For more information, see System Viewer utility on page 25 or Configuration utility on page 26.
2. Select **View Lifecycle Controller Logs** on the **System Viewer** utility or the **Config Utility**.
3. For a single system, see Viewing Lifecycle Controller logs on page 59.
4. For a collection, see Viewing and exporting Lifecycle Controller logs for a collection on page 44.

Working With NIC or CNA Profiles

You can configure the different attributes of specific network interface cards (NICs) or converged network adapters (CNAs) embedded in the system and save them to a profile. You can create and edit NIC or CNA profiles using the **System Viewer** utility.

Prerequisites

For more information, see Common prerequisites on page 12.

Workflow for configuring and saving NIC or CNA

The following steps outline the workflow sequence:

1. Launch the **System Viewer** utility on the Configuration Manager console for a particular system. For more information, see System Viewer utility on page 25.
2. Select **Network Adapter Configuration**.
3. Select one of the following options:
   - Create a profile — to create a new NIC or CNA profile. For more information, see Creating a NIC or CNA profile on page 55.
   - Edit an existing profile — to edit an existing NIC/CNA profile. For more information, see Editing a NIC or CNA profile on page 57.
   - Scan collection to identify adapters — to scan the collection and list the configured adapters in the collection. For more information, see Comparing and updating firmware inventory on page 58.
4. Add an adapter to the profile or remove an adapter from the profile. For more information, see steps 3–4 in Creating a NIC or CNA profile on page 55.
5. Select the adapter on the grid and configure it. For more information, see Configuring adapters on page 55.
6. Set the NIC and iSCSI parameters for the personalities you have chosen for each partition. For more information, see Configuring NIC and iSCSI parameters on page 56.
7. Save the NIC or CNA profile.

Working with Fibre Channel profiles

You can configure different attributes of Fibre Channel (FC) host bus adapter (HBA) cards in the system and save them as a profile. You can create, and edit FC HBA profiles by using the **System Viewer** utility and apply it when you are deploying the operating system to a collection of systems on the Configuration Manager console.

For more information, see Common prerequisites on page 12.

The following steps outline the workflow sequence:

1. Launch the **System Viewer** utility on the Configuration Manager console for a particular system. For more information, see System Viewer utility on page 25.
2. In the left pane, select **FC HBA Configuration**.
3. Select one of the following options:

- Create a profile — to create a new FC HBA profile. For more information, see Creating an FC HBA profile on page 57.
- Edit an existing profile — to edit an existing FC HBA profile. For more information, see Editing an FC HBA profile on page 58.

4. Add new adapter port or remove an adapter port from the profile. For more information, see steps 3 through 5 in Creating an FC HBA profile on page 57.
5. Select the adapter on the grid and configure it. For more information, see step 6 in Creating an FC HBA profile on page 57.
6. Save the FC HBA profile.

Selecting Fibre Channel storage area network in boot sequence

Once the SAN boot device is visible as a hard disk drive in the hard disk drive sequence, select the SAN boot device as the first boot device in hard disk drive sequence of BIOS or UEFI boot sequence.

For more information, see Common prerequisites on page 12.

Before changing the boot sequence, ensure that operating system is already installed and is present on the logical unit number (LUN) assigned to the server.

The following steps outline the workflow sequence:

1. In the **BIOS Configuration** screen, change the boot sequence for SAN boot device as the first boot device. Click **Save As Profile** to save the updated profile. For more information, see Changing the BIOS or UEFI boot sequence and hard disk drive sequence on page 53.
2. From the **Dell Lifecycle Controller Configuration Utility**, select **Hardware Configuration and Operating System Deployment**. In BIOS Configuration page, select **Configure BIOS**, and click **Browse**, to select the BIOS or UEFI profile updated in step 1.
3. Select **Do not deploy operating system** in the advertisement screen, to skip deploying the operating system on the collection and click **Reboot targeted collection**.
4. Launch the **Task Viewer**, to view the status of the completed tasks. For more information, see Task Viewer on page 27.

3

Using Dell Lifecycle Controller Integration

This chapter discusses the various operations that you can perform after you install DLCI on Configuration Manager.

Before you begin using DLCI for Configuration Manager, ensure that the target system is auto-discovered and present in the **All Dell Lifecycle Controller Servers** collection on the Configuration Manager console.

DLCI for Configuration Manager enables you to perform the following operations on all Dell systems under a collection:

- Configure the target systems. For more information, see Configuring target systems on page 21.
- Apply drivers on the task sequence. For more information, see Applying Drivers from the task sequence on page 22.
  NOTE: Select the **Apply Drivers from Lifecycle Controller** check box if you want to apply drivers from Lifecycle Controller while deploying operating systems.
- Create a task sequence media. For more information, see Creating a task sequence media bootable ISO on page 25.
- Use the **System Viewer** utility on specific systems in a collection. For more information, see System Viewer utility on page 25.
- Use the **Config Utility** on a collection of Dell systems. For more information, see Configuration utility on page 26.
- Launch the iDRAC console by right-clicking on any system discovered under **All Dell Lifecycle Controller Servers** on the Configuration Manager console, or any system on the **Task Viewer**. For more information, see Launching the integrated Dell Remote Access Controller console on page 26.
- Use the **Task Viewer** to view the status of tasks handled by DLCI for Configuration Manager. For more information, see Task Viewer on page 27.

Topics:

Licensing for DLCI

This release of DLCI is licensed. For more information on licensing; In Configuration Manager select **Assets and Compliance** > **Overview** > **Device Collections** > **Dell Lifecycle Controller** > **License Instructions**.

Dell Deployment ToolKit

The Dell Deployment Toolkit (DTK) includes a set of utilities, sample scripts, and sample configuration files that you can use to deploy and configure the Dell systems. You can use DTK to build script-based and RPM-based installation for deploying large number of systems on a pre-operating system environment in a reliable way, without changing their current deployment processes. Using DTK you can install operating systems on Dell systems in BIOS or Unified Extensible Firmware Interface (UEFI) mode.

NOTE: If the folders containing boot critical drivers are not present, then the wizard displays an error message.

Dell Driver CAB files

A cabinet (`.cab`) file is a compressed file that contains other distribution files, such as drivers and system files.

The Dell Driver CAB file provides new levels of flexibility for creating and deploying customized boot images.

Importing Dell driver files

1. Download the latest DTK file from **Dell.com/support**.

   NOTE:
   - Make sure that you import a DTK file package from the site server and not from the admin console.
   - Support for DTK self-executable zip file.

2. Launch the **Configuration Manager Console**.
3. In the left pane, select **Software Library** > **Overview** > **Application Management** > **Packages**.
4. Right-click **Packages** and select **DLCI Server Deployment** > **Import DLCI Dell Driver Cabs.**
   The **DLCI WinPE Driver Configuration Wizard screen** is displayed.
5. Click **Browse** and navigate to the file or self-extractable zip file that you downloaded.
   The selected CAB file version, Windows PE version, and architecture are displayed in **Cab Selection for Import** section on **DLCI WinPE Driver Configuration Wizard**.

   NOTE: If the WinPE drivers are already installed on this system, then the following message is displayed:

   WinPE drivers are already present on this system, importing Cab file will be overwriting the existing WinPE drivers. Are you sure you want to continue?
6. Follow steps 7 to 11 in the Upgrading Dell driver CAB files on page 20 section for creating a boot image.

Upgrading Dell driver CAB files

1. Launch **Configuration Manager Console**.
2. In the left pane, select **Software Library** > **Overview** > **Application Management** > **Packages**.
3. Right-click **Packages** and select **DLCI Server Deployment** > **Import DLCI Dell Driver Cabs.**
   The **DLCI WinPE Driver Configuration Wizard** screen is displayed. If there is an existing CAB file package on the server, then the CAB file version, Windows PE version, and architecture is displayed under CAB Selection for Import section.
4. Click **Browse** and navigate to the CAB file self-extractable zip file that you downloaded. Click **Next**.
   The selected CAB file version, Windows PE version, and architecture are displayed in **Cab Selection for Import** section.
5. In **Boot Image Selection**, select any one of the following options:

   NOTE: Make sure that you import a 64-bit CAB file before selecting x64 boot images in any of the following options.

Use Boot Image from WAIK/ADK tools	Select this option to create both x64 and x86 Dell boot images. The source for the boot image creation is obtained from Windows Automated Installation Kit (WAIK) or Windows Assessment and Deployment Kit (ADK), depending on the configuration, and all the Windows PE custom install packages are added to the boot image.

Use existing Boot Image from Configuration Manager	This option allows you to select an existing boot image in Configuration Manager. Select an existing boot image from the drop-down list and use it to create a Dell boot image.
Use a custom Boot Image	Select this option to import a custom boot image from any other location. Specify the Universal Naming Convention (UNC) path of the Windows Imaging (WIM) file and select the boot image from the drop-down list.

NOTE: Only finalized images are supported if you select the **Use a Custom Boot Image** option for WinPE.

NOTE: The Windows PE custom boot image should have **XML**, **Scripting**, and **WMI** packages installed on it. For more information on how to install these packages, see the *Microsoft Windows AIK* or *Windows ADK* documentation.

6. Click **Next**.
   The **Boot Image Property** screen is displayed.
7. In the **Boot Image Property**, enter a name for the Dell boot image.
   The **Version** and **Comments** fields are optional.
8. Click **Create**.
   The boot image creation process begins. A progress bar shows the status of the boot image creation. After the boot image is created, the boot image details are displayed on the **Summary** screen, the information includes DTK or CAB file details, and success state.
9. Right-click each of the newly created boot images and perform the update and manage distribution points operations.
   The drivers imported from Dell driver CAB files are injected into WinPE. This process depends on the Configuration Manager and ADK. It is recommended that you read the limitations documented for these products before creating a boot image. For example, **technet.microsoft.com/en-us/library/hh825070.aspx**

   NOTE: You can view the DTK configuration details only by using the **Import DLCI Dell Driver Cabs**.

Configuring target systems

DLCI for Configuration Manager supports only *yx1x* systems and later. For each system in the collection, enable **Collect System Inventory on Restart (CSIOR)** in the iDRAC settings.

NOTE: In the server name format yx1x; y denotes alphabets, for example M, R, or T; and x denotes numbers.

By default, CSIOR is OFF. The part replacement feature provides the option to set the CSIOR.

To enable CSIOR on multiple systems, see Configuring part replacement properties for a system on page 64.

To enable CSIOR for earlier server generations:

1. Restart the system.
2. During Power-on Self-Test (POST), when the system prompts you to enter the iDRAC Utility, press <**CTRL**>< **E**>.
3. Select **System Services** from the options available and press <**Enter**>.
4. Select **Collect System Inventory on Restart** and press the right or down keys and set it to **Enabled**.

To enable CSIOR for Dell's 12th and later generation of PowerEdge servers:

1. Select <**F2**> during POST to enter **System Setup**.
2. Select **iDRAC Settings** and click **Lifecycle Controller**.
3. Select **Collect system inventory on Restart (CISOR)**.

Auto-discovery and handshake

The auto-discovery and handshake feature enables the iDRAC on target systems to locate the provisioning service and establish communication with the Site Server. The Dell Provisioning service provisions a management account and updates Configuration Manager with the new system. The Dell Lifecycle Controller Utility (DLCU) for Configuration Manager uses the provisioned account to communicate with the iDRAC of target systems, to invoke the enabled features.

After DLCI for Configuration Manager discovers a system with iDRAC, it creates the **All Dell Lifecycle Controller Servers collection** under **Devices Collections** in Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012. There are two sub-collections within the collection:

- **Managed Dell Lifecycle Controller (OS Deployed)** — displays the systems on which you have deployed the operating system.
- **Managed Dell Lifecycle Controller (OS Unknown)** — displays the systems on which the operating system is not deployed.

  NOTE:
  - DLCI for Configuration Manager does not support auto-discovery of modular systems with flex-addressing.
  - Duplicate collections may get created when Auto-Discovery and Import Dell Server operations are done simultaneously. Dell recommends that you delete duplicate DLCI Collections.

Applying Drivers from the task sequence

Based on the operating system you want to deploy, either apply drivers from the Lifecycle Controller or the Configuration Manager repository. Use the drivers in the Configuration Manager repository as backup.

Applying drivers from Lifecycle Controller

To apply drivers from the Lifecycle Controller:

NOTE: If you edit the task sequence to which drivers are exposed from the Lifecycle Controller option checked, the errors in step 7 might not be reflected in the step status and in the Missing Objects dialog box. Configure the **Apply Drivers** from **Dell Lifecycle Controller** option before you apply the changes.

1. Create a new task sequence if there is no existing task sequence, or edit the task sequence to which drivers are exposed from the Lifecycle Controller.
2. Select **Apply Operating System Images**.
3. Under the **Apply operating system from a captured image**, select and verify the image package and image.
4. Clear the **Use an unattended or sysprep answer file for a custom installation** check box.
5. Select **Apply Windows Settings**.
6. Type the licensing model, product key, administrator password, and time zone.
7. Select **Apply Drivers from Dell Lifecycle Controller** and select an operating system from the drop-down list.
8. Type the user name and password with administrator credentials to access the Configuration Manager console.
9. Select **Apply Driver Package**. Click **Browse** and select a driver package from the list of driver packages available in Configuration Manager.
10. Click **OK** to close the **Task Sequence Editor**.
11. Advertise the task sequence that you have edited.
12. Create a Lifecycle Controller Boot Media. For more information, see Creating a Lifecycle Controller boot media on page 34.

Importing DLCI Dell server driver packages

DLCI provides a wizard to create driver packages in Configuration Manager, based on the server-operating system combination from the drivers available in the *Dell Systems Management Tools and Documentation* DVD. These packages are used in the task sequences that are used for operating system deployment.

1. In the left pane, select **Software Library** → **Overview**→**Operating Systems** → **Driver Packages**.

2. Right-click **Driver Packages**, select **DLCI Server Driver Package** → **Import Dell DLCI Server Driver Package**. The **Dell DLCI Server Driver Package Import Wizard** is displayed asking for the location of the Systems Management DVD.

   NOTE: If you have downloaded an ISO image, then create a physical disk or mount it on a virtual drive.

3. Select the drive in which you inserted the DVD and click **Next**.
   A list of driver packages for a combination of servers and operating systems is displayed.
4. Select the required packages and click **Finish**.
   A progress bar displays the status of the import. After the import is complete, the import summary is displayed.

   NOTE: The import of drivers may take more time and the progress bar may not be updated immediately.

5. Click **Close**.

Viewing the condition for a fallback step

The condition **DriversNotAppliedFromLC** is automatically added by DLCI for Configuration Manager while creating a task sequence. This condition is used as a fallback action if the application of drivers from Lifecycle Controller fails.

NOTE: Dell recommends that you do not disable or delete the condition.

To view the condition for a fallback step:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, select **Software Library** > **Overview** > **Operating Systems** > **Task Sequence**.
2. Right-click the task sequence and click **Edit**.
3. Select **Apply Driver Package** or **Apply Device Drivers**.
4. Click the **Options** tab. You can view the **DriversNotAppliedFromLC** condition.

Creating a task sequence

You can create a task sequence in two ways to configure your server:

- Create a Dell-specific task sequence using DLCI Deployment template.
- Create a custom task sequence.

The task sequence proceeds to the next task sequence step irrespective of the success or failure of the command.

Creating a Dell specific task sequence

To create a Dell-specific task sequence using DLCI Server Deployment template:

1. Launch **Configuration Manager Console**.
   The **Configuration Manager Console** screen is displayed.
2. In the left pane, select **Software Library** > **Overview** > **Operating Systems** > **Task Sequences**.
3. Right-click **Task Sequences**, and then click **DLCI Server Deployment** > **Create DLCI Server Deployment Template.**
   The **DLCI Server Deployment Task Sequence Wizard** is displayed.
4. Type the name of the task sequence in **Task Sequence Name** field.
5. Select the boot image that you want to use from the drop-down list.

   NOTE: Dell recommends that you use the Dell custom boot image that you created.

6. Under **Operating System Installation**, select the operating system installation type. The options are:
   - **Use an OS WIM image**
   - **Scripted OS install**
7. Select an operating system package from the **Operating system package to use** drop-down menu.
8. If you have a package with **unattend.xml**, then select it from the **Package with unattend.xml info** menu. Else, select **<do not select now>**.
9. Click **Create.**

The **Task Sequence Created** window is displayed with the name of the task sequence you created.

10. Click **Close** in the confirmation message box that is displayed.

Creating a custom task sequence

1. Launch the **Configuration Manager Console**.
   The **Configuration Manager Console** screen is displayed.
2. In the left pane, select **Software Library** > **Overview** > **Operating Systems** > **Task Sequences**.
3. Right-click **Task Sequences**, and then click **Create Task Sequence**.
   The **Create Task Sequence Wizard** is displayed.
4. Select **Create a new custom task sequence**, and click **Next**.
5. Enter a name for the task sequence in the **Task sequence name** text box.
6. Browse for the Dell boot image that you had created, and click **Next**.
   The **Confirm the Settings** screen is displayed.
7. Review your settings and click **Next**.
8. Click **Close** in the confirmation message box that is displayed.

Editing a task sequence

1. Launch the **Configuration Manager Console**.
   The **Configuration Manager Console** screen is displayed.
2. In the left pane, select **Software Library** > **Operating Systems** > **Task Sequence**.
3. Right-click the task sequence that you want to edit and click **Edit**.
   The **Task Sequence Editor** window is displayed.
4. Click **Add** > **Dell Deployment** > **Apply Drivers from Dell Lifecycle Controller.**
   The custom action for your Dell server deployment is loaded. You can now make changes to the task sequence.

   NOTE: When editing a task sequence for the first time, the error message, **Setup Windows and Configuration Manager** is displayed. To resolve the error, create and select the Configurations Manager Client Upgrade package. For more information about creating packages, see the Configuration Manager documentation at **technet.microsoft.com**.

Configuring the task sequence steps to apply operating system image and driver package

The scope of this document includes information only on the DLCI feature to apply operating system image and add Dell drivers.

Applying the operating system image

NOTE: Before you begin this task, make sure that you have the required operating system image file (`.wim` file) within the **Operating System Images** tree in the Configuration Manager.

To apply the operating system image:

1. In the left pane of the **Task Sequence Editor**, under **Deploy Operating System**, click **Apply Operating System Image.**
2. Select one of the following options:
   - **Apply operating system from a captured image**
   - **Apply operating system from an original installation source**
3. Browse and select the operating system location and click **OK**.

Adding Dell driver packages

1. In the left side of the **Task Sequence Editor**, under **Deploy Operating System**, click **Apply Driver Package**.
2. Click **Browse**.
   The **Select a Driver Package** window is displayed.
3. Click **DLCI Driver Packages<OM Version>**.
   A list of driver packages available in the **Dell Lifecycle Controller Integration** is displayed.
4. Select a package for a Dell PowerEdge server, such as **Dell PEM630-Microsoft Windows 2012 R2-OM8.1.0**.
5. Click **Apply**.

   NOTE: After operating system deployment, make sure that the mass-storage driver installed is same as that specified in the Task Sequence. If you find any differences, then update the driver manually.

Deploying a task sequence

After saving the task sequence, assign it to the collection of servers by deploying it. For the steps to deploy a task sequence, visit **www.technet.microsoft.com/en-in/library/gg712694.aspx**

NOTE: DLCI does not support the Standalone Media method to create Task Sequence Media.

Creating a task sequence media bootable ISO

To create a task sequence ISO:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012 under **Software Library**, right-click **Task Sequences** and select **Create Task Sequence Media**.

   NOTE:
   - Ensure that you manage and update the boot image across all distribution points before starting this wizard.
   - Dell Lifecycle Controller Integration does not support the Standalone Media method to create Task Sequence Media.

2. From the **Task Sequence Media Wizard**, select **Bootable Media** and click **Next**.
3. Select **CD/DVD Set**, and click **Browse** and select the location to save the ISO image.
4. Click **Next**.
5. Clear the **Protect Media with a Password** check box and click **Next**.
6. Browse and select **Dell PowerEdge Server Deployment Boot Image**.
7. Select the distribution point from the drop-down menu, and select the **Show distribution points from child sites** check box.
8. Click **Next**.
   The **Summary** screen appears with the task sequence media information.
9. Click **Next**.
   The progress bar is displayed.
10. On completion, close the wizard.

System Viewer utility

The **System Viewer** utility allows you to perform various operations from the source system to a single target system discovered under **All Dell Lifecycle Controller Servers** on the Configuration Manager console. This utility works on a one-to-one relationship and you can perform the operations on target systems, one at a time.

If necessary, you can change the iDRAC credentials of the target system before you launch the **System Viewer** utility to perform various tasks.

To change the iDRAC credentials and launch the **System Viewer** utility:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012 under **Device Collections**, right-click a Dell yx1x system or later and select **Dell Lifecycle Controller** > **Launch System Viewer**.

   The **iDRAC Authentication Information** screen displays the default credentials known to the Configuration Manager.

2. Clear **Use Credentials Known to Configuration Manager (Default)** and do one of the following:
   - **Do not modify the existing account** — This option is selected by default, clear this option to provide credentials, else existing credentials are maintained. Make sure that you enter valid credentials for iDRAC. You can provide credentials authenticated on the active directory.

     NOTE:

     You can enter only specific special characters in the user name field. For more information on the special characters that you can use in the iDRAC user name field, see the iDRAC documentation available at `Dell.com/support/home`.
   - **Skip CA check** — This option is selected by default, clear this option to secure communication between the Configuration Manager and the target systems. Clearing this option will check that the certificate on the target system is issued by a trusted certificate authority (CA). Clear this option only if you trust the target systems.
   - **Skip CN check** — Clear this option to enhance security; authenticate system names and prevent impersonation. The common name (CN) need not match the host name of the target system. Clear this option only for trusted target systems.
3. Click **OK** to launch the **System Viewer** utility.

For more information on using the System Viewer utility, see Using the System Viewer Utility on page 51.

Configuration utility

The Configuration Utility allows you to perform various operations from the source system to the entire collection of Dell systems discovered under **All Dell Lifecycle Controller Servers** on the Configuration Manager console. This utility works on a one-to-many relationship and uses the Remote Enablement feature of the Lifecycle Controller present on Dell systems. You can perform various operations on all the target systems at one time.

To launch the Configuration Utility:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012 under **Device Collections**, right-click on **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.

   NOTE: You can launch Configuration Utility for any collection.
2. In the **Dell Lifecycle Controller Configuration Utility** window, the left-hand pane lists the following options:
   - Overview
   - Create Lifecycle Controller Boot Media
   - Hardware Configuration and Deploy operating system
   - Firmware Inventory, Compare, and Update
   - Hardware Inventory
   - Session Credentials, Verify Communication
   - Modify Credentials on Lifecycle Controllers
   - View Lifecycle Controller Logs
   - Platform Restore
   - Network Adapter Comparison Report

For more information on using the Configuration Utility, see Using the Configuration Utility on page 34.

Launching the integrated Dell Remote Access Controller console

Configuration Manager of DLCI enables you to launch the iDRAC console for any of the Dell systems, you can view or modify the iDRAC configuration for the selected systems.

After you install DLCI for Configuration Manager, you can view **Dell Lifecycle Controller** > **Launch iDRAC Console** menu option when you right-click on any system in the collection. You can also find the **Launch iDRAC Console** option when you select a system in the Task Viewer and right-click on it.

To launch the iDRAC console for a system under the collection:

1. Select any system under **Device Collections** > **All Dell Lifecycle Controller Servers** in Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012.
2. Right-click the system and select the **Dell Lifecycle Controller** > **Launch iDRAC Console** menu option.
   The iDRAC console of the system is launched on your default browser.
3. Provide the credentials to log in to the iDRAC console and view or edit the details of the iDRAC configuration of the system. You can provide credentials authenticated on the active directory.

Launching the integrated Dell Remote Access Controller Console from the Task Viewer

To launch the iDRAC console from the **Task Viewer:**

1. Launch the **Task Viewer** by clicking the Dell icon on the task bar. This icon is displayed when you are deploying the operating system on the Dell systems, or you are applying firmware updates on the systems, or performing both the actions. For more information on deploying the operating system, see Configuring hardware and deploying the operating system on page 35. For more information on applying firmware updates, see Comparing and updating firmware inventory for systems in a collection on page 43 or Comparing and updating the firmware inventory on page 13.
2. Select any system on the **Task Viewer**, right-click and select the **Launch iDRAC Console** option.
3. Provide the credentials to login to the iDRAC console and view or edit the details of the iDRAC configuration of the system.

Task Viewer

The **Task Viewer** is an asynchronous component that hides in the task bar and displays the status of tasks handled by the DLCI for Configuration Manager. All the tasks are displayed in the Task Viewer. For example, long-running tasks such as operating system deployment, or applying firmware updates to systems. The Task Viewer maintains a queue of tasks and displays up to twenty tasks at one time.

The task viewer displays the following details:

- **Name:** Displays the name or the service tag of the system on which the task is running.
- **Task:** Displays which task is running on the system.
- **Status:** Displays the status of the task running on the system.
- **Start Date/Time:** Displays the date and time when the task started.
- **Time Elapsed:** Displays the time taken by the task after it started.

The **Task Viewer** also displays a status summary of the total number of tasks that are running at the bottom right hand corner.

When you start running a set of tasks on a single system or a collection of systems, the Dell icon appears on the task bar at the bottom right hand corner of your screen. Click the Dell icon to launch the **Task Viewer** and perform the various actions.

The following table lists the actions that you can perform in the **Task Viewer**.

Button	Action
Close	Click to close the **Task Viewer**. When you close the **Task Viewer**, it cancels all the tasks that are running. Therefore, Dell recommends not to close the Task Viewer when you have tasks that are still running.
Clear Completed	Click to clear all the completed or failed tasks from the grid.
Export Queue	Click to export the current state of the tasks in the **Task Viewer** to a .CSV file. You can use the .CSV to view the summary of the total number of DLCI tasks that are running.

Button	Action
View Log	Click to view the log file that contains the details of the tasks that are running.
Send to Taskbar	Click to minimize the **Task Viewer** and send it to the task bar.

Additional tasks you can perform with Dell Lifecycle Controller Integration

Configuring security

To configure security for DLCI, you must:

- Validate a Dell factory-issued Client Certificate on (iDRAC). For more information, see Validating a Dell factory-issued Client Certificate on the Integrated Dell Remote Access Controller for auto-discovery on page 28.
- Preauthorize systems for auto-discovery. For more information, see Pre-authorizing systems for auto-discovery on page 28.
- Change administrative credentials. For more information, see Changing the administrative credentials used by Dell Lifecycle Controller Integration for Configuration Manager on page 28.

You can also use the GUI to configure the security. For more information, see Using the Graphical User Interface on page 29.

Validating a Dell factory-issued Client Certificate on the Integrated Dell Remote Access Controller for auto-discovery

This security option requires that a system being discovered by the provisioning website during the discovery and handshake process has a valid factory-issued client certificate which is deployed to the iDRAC. This feature is enabled by default. To disable the feature, run the following command:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -CheckCertificate false
```

NOTE: By default, the **CheckCertificate** value is set to **true**. Ensure that you set the **CheckCertificate** value to **false** if you are not using unique certificates.

Pre-authorizing systems for auto-discovery

This security option checks the service tag of the system being discovered against a list of authorized service tags you have imported. To import the authorized service tags, create a file containing a comma-separated list of service tags, and import the file by running the following command:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -add
[file_with_comma_delimited_service_tags].
```

Running the command creates a record for each service tag in the repository file `Program Files]\Dell\DPS\Bin\Repository.xml`.

This feature is disabled by default. To enable this authorization check, run the following command:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -CheckAuthorization true.
```

Changing the administrative credentials used by Dell Lifecycle Controller Integration for Configuration Manager

Use the following commands to change the administrative credentials for Configuration Manager used by DLCI:

To set the user name:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -CIuserID [New Console
Integration Admin User ID]
```

To set the password:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -CIpassword [New Console
Integration Admin Password]
```

NOTE: The commands are case sensitive.

Using the Graphical User Interface

You can also use the Graphical User Interface (GUI) to change the security configurations.

Use the following command to open the GUI screen:

```
C:\Program Files (x86)\Dell\DPS\ProvisionWS\bin\import.exe -DisplayUI
```

NOTE: The **DisplayUI** term is case sensitive.

Using the Array Builder

The **Array Builder** allows you to define arrays and disk sets with all available RAID settings, logical drives or virtual disks of varying sizes or use all available space, and assign hot spares to individual arrays or assign global hot spares to the controller.

When a controller is created, a default variable condition, array and disk(s) are created to ensure a valid configuration. You can choose to leave the controller un-configured with disks set to non-RAID, or you can add arrays or perform other actions.

Defining rules with the Array Builder

You can define rules to match configurations based on the following:

- Detected slot number that the controller is in or just the embedded controller, if any.
- Number of disks that are attached to the controller.
- Apply a blanket configuration to any controller the **Array Builder** finds.

You can also apply configuration rules based on the RAID profiles detected on the server. This allows you to define different configurations to different servers even if the detected hardware is identical.

Creating a RAID Profile using Array Builder

To create a RAID Profile:

You can also import an existing profile and modify the configurations using the Array Builder. For more information on importing a profile, see Importing a profile on page 33.

1. Launch the **System Viewer** utility, click **RAID Configuration** > **Create RAID Profile**.
   When you launch the **Array Builder**, a default embedded controller is created.
2. Type the configuration rule name in the **Configuration rule name** field.
3. Select **Error handling rule** from the drop-down menu. You can choose from:
   - **Fail the task if any controller does not match a configuration rule** — Reports a failure if any of the detected controllers are not configurable by a rule.
   - **Fail the task only if the first controller does not match a configuration rule** — Reports a failure if the first controller detected (usually the embedded controller) is not configurable by a rule.
   - **Fail the task only if none of the array controllers match a configuration rule** — Reports a failure only if all of the controllers in the system fail to match a rule; in other words, none of the controllers are configured. This rule also fails if a controller does not have sufficient disks to configure a RAID.
4. You can:
   - Add new controllers and define rules for them, or edit the default controller and define the rules. For more information, see Controllers on page 30.
   - Add or edit variable conditions for the default controller or the controller that you add. For more information, see Variable conditions on page 31.

- Create new arrays from a variable condition, if required. For more information, see Arrays on page 31.
- You can create an array, add additional disks, hot spares, or global hot spares to the array.

5. Click **Save** to save the profile as a .XML file.

You can also import an existing profile and modify the configurations using the **Array Builder**. For more information on importing a profile, see Importing a profile on page 33.

About creating Array Builder

When you use the RAID profile that you created using **Array Builder** as part of the operating system deployment of DLCI for Configuration Manager, it detects the existing controller(s) on the server as well as the disks attached to each controller. It then tries to match the physical configuration(s) that the utility detected, to the logical configurations you defined in the configuration rules. These array configuration rules are defined using a graphical, logical layout that allows you to visualize how your array controllers will be configured. Rules are processed in the order displayed in the **Array Builder** tree, so you know exactly which rules have priority.

Controllers

Controller elements contain variable condition elements. Controllers can be one of several configuration types:

- The embedded controller
- A controller in slot "X"
- Any controller with "X" disks
- Any controller with "X" disks or more
- All remaining controllers

NOTE: If the disk(s) is set to non-RAID, the existing RAIDs are cleared when the variable condition is not met.

Adding a Controller

To add a controller:

1. Select a controller from the list, or select an embedded controller.
   The **Controllers** drop-down menu to your left is enabled.
2. Click **Controllers** → **New Controller**.
   The **Controller Configuration** window is displayed.
3. Under **Controller Selection Criteria**, select from the following options:
   - **Select the controller located in slot** — Enter the slot number of the controller.
   - **Select any controller with** *<exactly, atleast>* *<number of>* **disks attached** — Set a rule to select any controller which matches exactly, or at least the number of disks you have selected.
   - **Select all remaining controllers in the system regardless of configuration**
4. Under **Variable Matching Criteria**, you can set a rule to apply this configuration only if it matches certain criteria that you select. Select **Apply this configuration only when the variable** to enable the rule setting options apply.
5. Click **OK**.

Editing a Controller

To edit a controller:

Select the controller and click **Controllers** > **Edit Controller.** The **Controller Configuration** window is displayed where you can make changes to your controller.

Deleting a Controller

To delete a controller:

1. Select the controller and click **Controllers** > **Delete Controller** .
   A warning informing that all the attached arrays and disks will be deleted is displayed.
2. Click **Yes** to delete or **No** to cancel.

NOTE: At least one controller is required on the server. If there is only one controller and you delete it, a message is displayed that the default controller was inserted because the last controller was deleted.

Variable conditions

To provide the ability to use the same RAID configuration in multiple logical configurations, variable evaluation is provided so that a different configuration for arrays and logical drives can be applied to different situations.

Variable condition elements contain arrays and global hot spares, and are of two types:

- **No variables defined**: This is the default configuration inserted with every controller, and cannot be removed or moved from last in the order.
- **Variables defined**: This is where any variable is compared to a value using one of the pre-defined operators.

  NOTE: DLCI for Configuration Manager does not support variables created in an encrypted format.

Adding a new variable condition

To add a new variable condition:

1. Under an embedded controller, expand **Embedded Controller**, and select **[No variable conditions defined]**.
2. Click **Variables** → **New Variable Condition**.
   The **Variable Condition Configuration** window is displayed.
3. Under **Variable Matching Criteria**, you can set a rule to apply this variable only if it matches certain criteria that you select.
4. Click **OK** to apply the variable condition, or **Cancel** to return to the Array Builder.

Editing a variable condition

To edit a variable condition:

1. Select the variable condition and click **Variables** → **Edit Variable Condition**.
   The **Variable Condition Configuration** window is displayed where you can make changes to your variable condition.
2. Click **OK** to apply the variable condition, or **Cancel** to return to **Array Builder**.

Deleting a variable condition

To delete a variable condition:

1. Select the variable condition and click **Variables** → **Delete Variable Condition**.
   A message that all the attached arrays and disks will be deleted is displayed.
2. Click **Yes** to delete or **No** to cancel.

Arrays

Array nodes include both RAID arrays and non-RAID disk groups that are indicated by the different icons for RAID arrays and non-RAID disks. By default, a non-RAID disk group is created when a controller is created. If the controller configuration specifies the number of disks required, the same number of disks is added to the non-RAID group.

Arrays can be added, modified or deleted depending on the controller configuration and number of disks available.

Array elements contain logical drives and physical disks.

Adding a new array

To add a new array:

1. Under a variable condition, select a variable condition and click **Arrays** → **New Array**.
   The **Array Settings** window is displayed.
2. Set the required RAID level from the **Desired RAID Level** drop-down menu.
3. On RAID levels 50 and 60, enter the span length of the array.

4. Click **OK** to apply the array, or **Cancel** to return to **Array Builder**.

Editing an array

To edit an array:

1. Select the array and click **Arrays** → **Edit Array**.
   The **Array Settings** window is displayed. You can select a different RAID level for the array.
2. Click **OK** to apply the changes, or **Cancel** to return to **Array Builder**.

Deleting an array

To delete an array:

1. Select the array and click **Arrays** → **Delete Array**.
   A message is displayed that all the attached disks will be deleted.
2. Click **Yes** to delete or **No** to cancel.

Logical drives also known as virtual disks

Logical drives can be present on RAID arrays and non-RAID groups. You can configure them by specifying the size (in GB) or consume all available (or remaining) space in the array. By default, a single logical drive is created for all new arrays and is set to use all the available space.

When specific-size logical drives are defined, the **using all remaining space** logical drive will consume any remaining space after other logical drive(s) have allocated their space on the array.

NOTE: Array Builder does not support creating logical drives of sizes 10, 50, and 60 GB, and does not support creating logical drives under Non-RAID groups.

Adding a new logical drive

To add a new logical drive under an array:

1. Select the array and click **Logical Drives** → **New Logical Drive**.
   The **Logical Drive Settings** window is displayed.
2. Under **Create a logical drive**, enter the exact number of gigabytes the logical drive must contain.
3. Click **OK** to create the logical drive, or click **Cancel** to return to **Array Builder**.

Editing a logical drive

To edit a logical drive:

1. Select the logical drive and click **Logical Drives** → **Edit Logical Drive**.
   The **Logical Drive Settings** window is displayed.
2. Change the size of the logical drive.
3. Click **OK** to apply the changes, or click **Cancel** to return to **Array Builder**.

Deleting a logical drive

To delete a logical drive:

1. Select the logical drive and click **Logical Drives** → **Delete Logical Drive**.
   A message is displayed to confirm the delete operation.
2. Click **Yes** to delete or **No** to cancel.

Disks (array disks)

Disks can be part of arrays (or the non-RAID disks node) and are of the following types:

- **Standard disks** — These are the basic, non-defined disk type that make up the storage on arrays.
- **Hot Spares** — These disks provide online redundancy if a RAID disk fails while assigned to a specific array.
- **All Remaining Disks** — These disks provide an option to define an array without specifying the exact number of disks.

If the controller configuration specifies the number of disks required, an equivalent number of disks are added to the non-RAID group. If the controller specifies the exact quantity, disks cannot be added or removed from the controller – they can only be moved from array to array (or the non-RAID group). If the controller specifies a minimum number of disks, you can add or remove disks, but you cannot remove disks below the lower limit of the controller configuration.

Adding a new disk

To add a new disk to an array, select the array and click **Disks** > **New Disk**.

You can choose from the following:

- **Single disk**
- **Multiple disks**
- **Hot spare** (only for the current array)
- **Global hot spare** (all arrays)

Changing a disk

To change a disk, click on the disk and select **Disks** > **Change Disk**.

You can change a disk to:

- **Standard disk**
- **Hot spare** (only for the current array)
- **Global hot spare** (all arrays)

Deleting a disk

To delete a disk, click on the disk and select **Disks** > **Delete Disk**.

Importing a profile

This menu item allows you to search for, and import an existing **Array Builder** profile. The XML profile file must be properly formatted. If it is not formatted correctly, Configuration Manager automatically modifies the XML file and sends a notification of the change.

To import an existing Array Builder XML file from another location, click **Import a Profile**.

4

Using the Configuration Utility

This section describes the various operations that you can perform with the Dell Lifecycle Controller Configuration Utility.

You can use the **Config Utility** from the Configuration Manager console to:

- Create a new Lifecycle Controller boot media to deploy operating systems remotely. For more information, see Creating a Lifecycle Controller boot media on page 34.
- Configure hardware and deploy the operating system on the target systems in the collection. For more information, see Configuring hardware and deploying the operating system on page 35.
- View the firmware inventory, compare it against a baseline, and update the firmware using a repository for all the systems in the collection. For more information, see Comparing and updating firmware inventory for systems in a collection on page 43.

  NOTE:

  You can create a repository using the Dell Repository Manager. For more information on Dell Repository Manager, see the *Dell Repository Manager User's Guide* available at `Dell.com/support/manual`.
- View the current hardware inventory for all the systems in the collection. For more information, see Viewing the hardware inventory on page 44.
- Set Lifecycle Controller credentials for the current session and verify communication and user accounts with Dell LCs. For more information, see Verifying Communication with Lifecycle Controller on page 44.
- Modify and set the Lifecycle Controller credentials on the targeted collection of Dell systems. For more information, see Modifying credentials on Lifecycle Controllers on page 45.
- View and export the Lifecycle Controller logs for a collection. For more information, see Viewing and exporting Lifecycle Controller logs for a collection on page 44.
- Perform tasks to restore the platform information for systems in a collection that includes:
  - Exporting the system profiles of all the systems in the collection.
  - Importing the system profiles of all the systems in the collection.
  - Configuring Part Replacement properties for a collection.

  For more information, see Platform restore for a collection on page 46.
- Compare a NIC configuration profile against systems in a collection. For more information, see Comparing NIC or CNA profiles against systems in a collection on page 47.

  NOTE: DLCI performs all the preceding actions for 20 systems at a time. If you have 100 systems in a collection, the first 20 systems are updated first, then the next 20, and so on.

Topics:

Creating a Lifecycle Controller boot media

Create a Lifecycle Controller boot media to deploy operating systems remotely.

To create a Lifecycle Controller boot media:

1. In Configuration Manager Version 1610, Configuration Manager 2012, under **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.

NOTE: You can launch Config Utility for any collection.

2. In the **Dell Lifecycle Controller Configuration Utility** window, select **Create new Lifecycle Controller Boot Media** on the left-hand pane.
3. Click **Browse** and select the bootable ISO that you created. For more information, see Creating a task sequence media bootable ISO on page 25.
4. Specify the folder or path to save the Dell Lifecycle Controller boot media.

   NOTE: Dell recommends to save the boot media to the local drive, and if necessary copy it to a network location.

5. Click **Create**.

Setting a default share location for the Lifecycle Controller boot media

To set a default share location for the Lifecycle Controller boot media:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, select **Administration** > **Site Configuration** > **Sites** > **Right-click <site server name>** > **Configure Site Components** > **Out of Band Management**. The **Out of Band Management Component Properties** window is displayed.
2. Click the **Dell Lifecycle Controller** tab.
3. Under **Default Share Location for Custom Lifecycle Controller Boot Media**, click **Modify** to modify the default share location of the custom Lifecycle Controller boot media.
4. In the **Modify Share Information** window, enter a new share name and share path.
5. Click **OK**.

Configuring hardware and deploying the operating system

Remote operating system deployment is the ability to execute an unattended installation of a target operating system on any auto-discovered system using iDRAC.

This feature:

- Updates the firmware from a Dell repository.
- Changes the BIOS configuration.
- Enables you to apply a NIC or CNA profile to a set of target systems.
- Enables you to apply an FC HBA profile and FC SAN boot attributes to a set of target systems.
- Changes the RAID configuration.
- Enables you to apply an iDRAC profile to a set of target systems.
- Enables you to export the system profiles before and/or after hardware configuration.
- Enables you to select the advertisement and the operating system to be deployed.
- Enables you to select the bootable media to deploy the operating system.

Deploying operating systems

You can deploy Windows and non-Windows operating systems on a collection and the operating system deployment is only supported for deploying operating systems on multiple servers.

During the operating system deployment, the status and progress of installation is displayed in the DLCI task viewer.

After installing the operating system, the system is added to a collection and is identified as **Managed Dell Lifecycle Controller Servers***<OS Name>*.

Where *OS Name* is any of the following:

- Windows operating systems

- Red Hat Enterprise Linux
- ESXi

  NOTE: After deploying non-windows operating systems, the service tag of the system name is displayed as host name in Configuration Manager console.

ESXi installation is supported only on a hard disk for this release.

For ESXi, Red Hat Enterprise Linux, the operating system is installed on the first disk with default configuration.

For Red Hat Enterprise Linux, the following are set:

- Language is set to US
- Keyboard is set to US (U.S. English)
- By default, Time zone is set to America, New York

For deploying the Red Hat Enterprise Linux 6.5, Red Hat Enterprise Linux 7.0 operating systems, DLCI requires all the drivers on the given ISO and DLCI assumes that all the drivers are available on the given ISO for the given platform. Only packages available in the Red Hat Enterprise Linux repository are installed.

NOTE: For deploying RHEL, use the Dell customized ISO.

During deployment, the following packages are installed in Red Hat Enterprise Linux repository:

- @base
- @client-mgmt-tools
- @console-internet
- @core
- @debugging
- @directory-client
- @hardware-monitoring
- @java-platform
- @large-systems
- @network-file-system-client
- @performance
- @perl-runtime
- @server-platform
- @server-policy
- pax
- python-dmidecode
- oddjob
- sgpio
- certmonger
- pam_krb5
- krb5-workstation
- perl-DBD-SQLite

For deploying ESXi, use the Dell customized ISO available at `Dell.com/support/home`.

Provide the ISO share on an NFS share. This share is used by DLCI to extract the ISO and create a custom ISO. The custom ISOs are saved on the same share.

Dell recommends that the machine with the NFS share is not connected to the internet.

DLCI clears all the partitions on the target system before installing any non-Windows operating system.

The pre-operating system image is mounted as a virtual media over the network and the drivers for the target host operating system are applied, either from the Configuration Manager console repository or the Lifecycle Controller.

If you select drivers from the Lifecycle Controller, the list of operating systems supported is based on the current driver pack flashed on the iDRAC. You can also download an ISO image to the vFlash SD card on the target system and boot the system to the downloaded ISO image.

NOTE: vFlash features can only be used on rack and tower servers with Integrated Dell Remote Access Controller version 1.3 firmware or later, or on blade servers with Integrated Dell Remote Access Controller version 2.2 or later.

For more information on remote operating system deployment and staging and booting to operating system image on vFlash, see the *Dell Lifecycle Controller User Guide* available at `Dell.com/support/home`.

Hardware configuration and OS deployment workflow

To deploy the operating system to a collection:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, in **Device Collections**, right-click any appropriate Dell collection and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. From the **Dell Lifecycle Controller Configuration Utility**, select **Hardware Configuration and Operating System Deployment**.
3. Click **Next**.
4. Select **Update Firmware from a Dell Repository** if you want to update the Firmware on the collection. For more information, see Updating firmware during OS deployment on page 38.
5. Click **Next**.
6. In BIOS Configuration, select **BIOS or UEFI** and click **Browse**, to select the path where the BIOS or UEFI profile is saved. Click **Next**.

   Select **Continue on Error** to continue the deployment, even if there is an error.
7. Select **Configure Hardware** if you want to change the hardware settings. For more information, see Configuring hardware during OS deployment on page 38.
8. Click **Next**.
9. Select **Configure FC HBA** if you want to apply an FC HBA profile and FC SAN boot attributes to a collection.
   a. Select the **FC adapter profile** check box to apply an FC HBA profile to a collection. For more information, see Applying a FC HBA profile on a collection on page 40.

      and
   b. Select the **SAN boot settings** check box to apply FC SAN boot attributes to a collection. For more information, see Applying FC SAN boot attributes on a collection on page 41.

   Select **Continue on Error** to continue the deployment, even if there is an error.
10. Select **Configure RAID** to configure RAID on the servers. For more information, see Configuring RAID on page 39.
11. Click **Next**.
12. Select **Configure network adapter** if you want to apply a Network adapter profile to the collection. For more information, see Applying a NIC or CNA profile on a collection on page 39.
13. Click **Next.**
14. Select **Configure iDRAC** if you want to apply an iDRAC profile to the collection. For more information, see Applying an integrated Dell Remote Access Controller profile on a collection on page 41.
15. Select **Export hardware configuration** to create a backup of the system profiles and export it to an iDRAC vFlash Card or a Network share. For more information, see Exporting the system profiles before and after hardware configuration on page 42.

    NOTE: Always ensure to select at least one hardware profile to enable the **Export hardware configuration** page.
16. Select **Do not deploy operating system** in the advertisement screen if you want to skip deploying the operating system on the collection.

    In this case, the **Next** button is disabled and you can directly click **Reboot targeted collection**. The hardware configuration tasks are submitted based on the selections you made in the previous steps and you can view the status of tasks on Task Viewer on page 27.

    NOTE: If you select a server to boot from a SAN device, you should skip deploying the operating system on a collection from the Configuration Utility.
17. If you want to deploy the operating system:
    - To deploy Windows operating systems: Select **Windows Operating System**, then select the advertisement to advertise the task sequence to the collection, and the operating system for deployment on the collection.
    - To deploy non-Windows operating systems: Select **Non-Windows Operating System**, select the operating system, provide details, and then click **Next**.
    - Other option to the Boot, Credentials, and Browse button are disabled for Non-windows deployment in **Select ISO Image**.
18. Under **Select Lifecycle Controller bootable media**, select one of the following options:
    - **Boot to Network ISO** — Reboots specified ISO.
    - **Stage ISO to vFlash and Reboot** — Downloads the ISO to vFlash and reboots.

- **Reboot to vFlash (ISO Must be present on vFlash)** — Reboots to vFlash. Ensure that the ISO is present in the vFlash.
  NOTE: To use the **Reboot to vFlash (ISO Must be present on vFlash)** option, the label name of the partition created on vFlash must be **ISOIMG**.
- Select the **Use Network ISO as Fallback** check box if you want the network ISO to be a fallback step.
- Click **Browse** and select the path where the Dell Lifecycle Controller bootable media is saved.

NOTE: If you have set a default share location for the Lifecycle Controller boot media, the default location populates automatically. For more information, see Setting a default share location for the Lifecycle Controller boot media on page 35.

19. Type the user name and password for accessing the share where the Dell Lifecycle Controller bootable media is located.
20. Click **Reboot Targeted Collection**. This selection sends the jobs for each system in the collection to the Task Viewer. To view the current tasks in the queue and their status, open the Task Viewer by clicking the Dell icon on the task bar. For more information on Task Viewer, see Task Viewer on page 27.

    After a system with iDRAC receives the **WS-MAN** command, it reboots to Windows PE and runs the advertised task sequence. It then automatically boots to the Lifecycle Controller boot media, depending on the boot order you created in the task sequence.

    NOTE: If you want to update a system after you deploy the operating system, and the system services are still unavailable, then you can reset the iDRAC using the iDRAC web-based interface. For more information, see the *Dell Lifecycle Controller Remote Services User's Guide* available at **Dell.com/support/home**.

    NOTE: If a yellow bang appears under device manager after you deploy Windows 2016 operating system, then download and install appropriate drivers from **Dell.com/support/home**.

    After the deployment is successful, the system with iDRAC moves to the **Managed Dell Lifecycle Controller (OS Deployed)** collection under **All Dell Lifecycle Controller Servers**.

    NOTE: If you change the host name of the target systems after you deploy the operating system, the system continues to appear under the **Managed Dell Lifecycle Controller (OS Deployed)** collection on the Configuration Manager console. You do not need to re-discover the system when you change the host name.

Updating firmware during OS deployment

To update the firmware:

1. Select one of the following options:
   - **Dell PDK catalog** — to specify a Dell PDK catalog that you can use to compare the firmware inventory. To specify a PDK catalog, do the following:
     - Click **Browse** to navigate to the file location where you have saved the catalog. Ensure that the catalog resides on a CIFS share that is accessible to the Dell Lifecycle Controller of the system.
     - Specify the **User Name** and **Password** to the CIFS share where your catalog resides if you want to update the firmware inventory from the catalog. You do not need to specify the user name and password if you are viewing or comparing against the catalog.
   - **FTP: ftp.Dell.com** — to connect to the Dell FTP site and download the updates.
   - **Firmware inventory profile** — to compare against an existing profile and update the firmware of the system. Click **Browse** and navigate to the location where you have saved the profile.
2. Click **Next**.
   The screen displays the firmware details of the servers in your collection and also the baseline version of the firmware.
3. Select the servers, which you want to update with newer firmware and click **Next**.
   The next screen displays the firmware download progress.
4. When the firmware download is complete, click **Next** to proceed to configure the hardware of the systems.

Configuring hardware during OS deployment

To configure the hardware:

1. Click **Browse** and select the hardware profile that you created using the **System Viewer**. This profile is applied during the operating system deployment process. For more information on creating hardware profiles, see Creating a new profile on page 52.
2. Select **Continue on Error** if you want to proceed to the next step even if this step fails. This option is selected by default. If you clear this option, the hardware configuration process is aborted when it encounters an error.
3. Click **Next** to configure RAID.

Configuring RAID

To configure RAID:

1. Click **Browse** and select the RAID profile that you created using the **System Viewer** utility. This profile is applied during the operating system deployment process. For more information on creating RAID profiles, see Using the Array Builder.
2. Click **Next** to configure network adapters.

NOTE: When you configure RAID settings on a system, the original controller settings of the system are reset and the virtual disks (VDs) that are configured, or any other configuration are cleared.

Applying a NIC or CNA profile on a collection

NOTE: In **Config Utility**, if you apply an attribute value, the dependent attribute value is not checked.

See Lifecycle Controller documentation for supported CNAs.

To configure Network Adapters and apply a NIC/CNA profile on a collection:

1. Click **Browse** and select the NIC/CNA profile that you created using the **System Viewer** utility. This profile is applied during the hardware configuration process. For more information on creating NIC/CNA profiles, see Creating a NIC or CNA profile on page 55.
2. If you select a simple NIC profile you can validate if all the settings in the profile are applied on the target system by launching the Unified Server Configurator on the target system.
3. If you select a Broadcom CNA profile, you can validate if the settings are applied based on the Table 4:

Table 4. Broadcom profile settings

S.No	Target Server Setting	Profile Settings	What is Applied
1.	Dual Port NIC (partition disabled)	Dual Port NIC Dual Port Quad Partition NIC	Dual Port Quad Partition NIC Partition is enabled when the system reboots.
2.	Dual Port NIC (partition disabled)	Dual Port NIC	Dual Port NIC Port level settings are applied when the system reboots.
3.	Dual Port NIC (partition disabled)	Dual Port Quad Partition NIC	Dual Port Quad Partition NIC Partition is enabled when the system reboots.
4.	Dual Port Quad Partition NIC	Dual Port NIC Dual Port Quad Partition NIC	Dual Port Quad Partition
5.	Dual Port Quad Partition NIC	Dual Port NIC	Nothing is applied as there is no match between the target server setting and profile setting.
6.	Dual Port Quad Partition NIC	Dual Port Quad Partition NIC	Dual Port Quad Partition

4. Click **Next** to apply an iDRAC profile.

NOTE: If there is an error while applying a NIC/CNA profile, the operating system deployment process continues to the next step. While applying an attribute using **Config Utility**, it does not check the dependent attributes value. After the hardware configuration task is complete, use **Network Adapter Comparison Report** in Config Utility to check if the attributes have been applied successfully.

Applying FC HBA profiles and FC SAN boot attributes on a collection

You can apply FC HBA profiles and FC SAN boot attributes from Configuration utility. You can create a FC HBA profile in the System Viewer utility, and provide the FC SAN boot attributes as a CSV file while applying the settings in Configuration utility.

Applying a FC HBA profile on a collection

To apply a FC HBA profile on a collection, perform the following steps:

1. Click **Browse** and select the FC adapter port profile that you created by using the **System Viewer** utility. This profile is applied during the hardware configuration process. For more information on creating FC HBA profiles, see Creating an FC HBA profile on page 57.
2. After you select FC adapter port profile, you can validate if the configuration is applied based on the following rules mentioned in Table 5:

Table 5. FC HBA profile settings

S.No	Target system	FC adapter port profile setting	What is applied
1	One adapter port	More than one adapter port is configured	FC adapter port profile settings are applied on the matched ports.
2	More than one adapter port	More than one adapter port is configured	Each adapter port in the target system is matched against the FC adapter port profile and FC adapter port profile settings are applied on the matched adapter ports.
3	More than one adapter port	One adapter port is configured	Each adapter port in the target system is matched against the FC adapter port profile and if match occurs, profile is applied on the adapter port.

NOTE: A match is based on location, slot number, and port number.

3. Click **Next** to configure an FC HBA profile.

NOTE: If any of the FC HBA attributes are not available from Lifecycle Controller, those attributes are not applied on FC adapter port.

After the hardware configuration task is complete, use Comparing FC HBA profile against a target system on page 65 in System Viewer to check if the attributes have been applied successfully.

Creating a CSV file

You can create or edit a CSV file in any CSV editor. In the CSV file, list values in the following format:

- Separate values by using comma as the delimiter. For example: <ServiceTag>, <FQDD>, <AttributeName>, <AttributeValue>

- Include attributes in separate lines. For example:
  - New line: <ServiceTag>, <FQDD>, <AttributeName>, <AttributeValue>
  - New line: <ServiceTag>, <FQDD>, <AttributeName>, <AttributeValue>

Provide the following FC SAN boot attributes for each HBA as mentioned in the CSV format:

- BootScanSelection — Specify the boot scan selection attribute.
- FirstFCTargetWWPN — Specify the first FC target world wide port name attribute.
- FirstFCTargetLUN — Specify the first FC target LUN attribute.
- SecondFCTargetWWPN — Specify the second FC target world wide port name attribute.
- SecondFCTargetLUN — Specify the second FC target LUN attribute.

Applying FC SAN boot attributes on a collection

To apply SAN boot attributes on a collection, perform the following steps:

1. Click **Browse** to navigate to the location where you have saved the CSV file that you created in a CSV editor. This profile is applied during the hardware configuration process. For more information on creating CSV files, see Creating a CSV file on page 40.
2. After you select a CSV file, the FC SAN boot attribute values are applied to the servers and adapter ports.

   NOTE:
   - The FC SAN boot attribute values are applied to the target servers and adapter ports that are specified in the CSV file.
   - If a target server is not specified in the CSV file, a warning message is prompted.
   - If an additional server is added to the CSV file that is not present in the collection, a warning message is prompted and the added server is not configured.

3. Click **Next** to apply the FC SAN boot attribute values.

   NOTE: After the hardware configuration task is complete, you can check manually whether the FC SAN boot attribute settings are applied to a server.

   NOTE: If you select a server to boot from a SAN device, skip the operating system installation.

While applying FC HBA configuration settings and SAN boot attributes, the status and progress of applying the configuration settings is displayed in the DLCI task viewer. If there is a failure while applying an FC HBA profile and SAN boot attributes, relevant log files are created and the status of the task is displayed on the task viewer. For more information about the status of the FC HBA and SAN boot attribute settings configuration task, see Task Viewer on page 27.

Applying an integrated Dell Remote Access Controller profile on a collection

To configure iDRAC and apply an iDRAC profile on a collection:

1. Click **Browse** and select the iDRAC profile that you created using the **System Viewer** utility. This profile is applied during the hardware configuration process. For more information on creating iDRAC profiles, see Creating an integrated Dell Remote Access Controller profile on page 53.
2. After you select an iDRAC profile, you can validate if the configuration is applied based on the following parameters:

Table 6. iDRAC profile settings

S.No	Target Server	Profile Settings	What is Applicable
1.	Rack and Tower systems	All four types of attributes are configured.	All attributes in the iDRAC profile.
2.	Blade systems	All four types of attributes are configured.	• All attributes in Common IP settings. • All attributes in IPv4 settings.

Table 6. iDRAC profile settings (continued)

S.No	Target Server	Profile Settings	What is Applicable
			• Only vLAN ID and vLAN priority attributes from Advanced LAN settings.
3.	Rack, Tower, or Blade system with Static IP address	IPv4 Configuration attributes only.	IPv4 address source is updated.
4.	Rack, Tower, or Blade systems	LAN Settings attributes only.	Applied only to Rack and Tower systems and not to Blade systems.
5.	Rack, Tower, or Blade systems	Advanced LAN Settings attributes only.	All Advanced LAN Settings attributes are applied to Rack and Tower systems. Only vLAN ID and vLAN priority attributes are applied to Blade systems.
6.	Rack, Tower, or Blade systems	Common IP Configuration attributes only.	Common IP Configuration attributes.
7.	Rack, Tower, or Blade systems without iDRAC6 enterprise card	LAN Settings with NIC mode set to **Dedicated**.	Nothing is applied as this attribute needs the iDRAC6 enterprise card.
8.	Rack, Tower, or Blade systems	LAN Settings with NIC mode set to **Shared**.	Attribute is applied only to Rack and Tower systems and only if the host operating system is configured for NIC teaming.
9.	Rack, Tower, or Blade systems	IPv4 Configuration where IP range specified is less than the number of systems.	Nothing is applied and an error is displayed in the OS deployment workflow.
10.	Rack, Tower, or Blade systems booted to Unified Server Configurator	All four types of attributes are configured.	All attributes applicable to the systems.

3. Click **Next** to select an advertisement.

   NOTE: If there is an error while applying an iDRAC profile, the operating system deployment process stops.

Exporting the system profiles before and after hardware configuration

You can use this option to create a backup of the system profiles and export it to an iDRAC vFlash Card or a Network share.

To export the system profiles, perform the following:

1. Select **Configure when to Export Hardware Configuration**.

   NOTE: All the controls and options are enabled in this page if this option is selected.

2. Select the options **Before** and/or **After** to export the system profiles before and/or after hardware configuration.

   NOTE: You can either select both the Before and After option or any one of the options. If you do not select any option, the **Do not Export** option is considered and a warning is displayed before proceeding.

3. Enter an **Export File Passphrase**. See step 4 in Exporting the system profile on page 62 to include an Export file passphrase that should be in a specific format.
4. Enter an **Export File Name Prefix**.

   NOTE: You can specify a file name prefix that is the same as an earlier Export file and in such situations, the Export file is overwritten.

   The Export files are appended with the hostname of the system and saved before hardware configuration in the following format: *<Before>_<prefix>-<node_id>*

   The Export files after hardware configuration are saved in the following format: *<After>_<prefix>-<node_id>*
5. Select **Continue on error** to continue the deployment, even if there is an error.
6. Select **vFlash media** or **Network share**. See step 3 in Exporting the system profile on page 62 for more information about share selection.
7. Click **Next** to export the system profiles.

To restore the backup files or system profiles, use the Platform restore for a system on page 62 option on the System Viewer to import a system profile or Platform restore for a collection on page 46 option on the Configuration Utility to import the system profiles in a collection.

Comparing and updating firmware inventory for systems in a collection

This feature enables you to retrieve, compare, and update firmware inventory on the Dell systems with Lifecycle Controllers in a collection.

NOTE: To compare and update firmware remotely, you must ensure that the Dell systems have iDRAC6 firmware version 1.5 or higher. For more information on upgrading to firmware version 1.5, see the *Integrated Dell Remote Access Controller 6 (iDRAC6) Version 1.5 User Guide* available at **Dell.com/support/home**.

To compare and update firmware inventory:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, under **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility.**
2. From the left pane of the **Dell Lifecycle Controller Configuration Utility**, select **Firmware Inventory, Compare,** and **Update.**
3. Select a baseline from the following options:
   - Dell PDK Catalog — to specify a Dell PDK catalog to compare with the firmware inventory. To specify a PDK catalog:
     - Click **Browse** to navigate to the file location where you have saved the catalog. Ensure that the catalog resides on a CIFS share that is accessible to the Dell Lifecycle Controllers.
     - Specify the **User Name** and **Password** to the CIFS share where your catalog resides if you want to update the firmware inventory from the catalog. You do not need to specify the user name and password if you are viewing or comparing against the catalog.

       NOTE: To update the firmware inventory, you must point to a local repository.
   - **FTP: ftp.Dell.com** — to connect to a catalog on the Dell FTP site to compare the firmware inventory.
   - **Firmware Inventory Profile** — to specify an existing profile that you have saved and use it to compare and update the firmware inventory for the collection.
4. Click **Next**.

   The **Firmware Inventory, Compare, and Update** screen displays the following information:
   - **Name** — displays the name of the systems in the collection.
   - **Model** — displays the system model information.
   - **Component** — displays the components available on the servers.
   - **Version** — displays the firmware versions of the components.
   - **Baseline** — displays the baseline firmware version of the components.
   - **Criticality** — displays the status of the firmware and indicates if the firmware of your collection is compliant, or needs an update.

5. Click **Copy to Clipboard** to copy the information to clipboard, or click **Export to CSV** to export the information in comma-separated values format.
6. Select the systems that you want to update with newer firmware and click **Next**.
   The screen displays the firmware download progress.
7. After the download is complete, click **Next** and choose one of the following options:
   - **Start now** — to start the update immediately.
   - **Start on next boot** — to start the update when the systems boot next.
   - **Schedule update** — to specify a date and time and schedule an update on that date.
8. Click **Finish** to complete the firmware update process.

Viewing the hardware inventory

You can use the Configuration Utility to view the hardware inventory details of all the systems in the collection.

To view the hardware inventory:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. On the **Dell Lifecycle Controller Configuration Utility**, select **Hardware Inventory.**
   The following details are displayed on the right pane of the **Dell Lifecycle Controller Configuration Utility**:
   - **Name** : displays the name of the Dell system, which is part of the collection.
   - **Hardware**: displays the hardware components of the system. For example, Memory, CPU, iDRAC, and FC HBA cards.
   - **FQDD**: displays the fully qualified device description of the hardware component.
   - **Description**: displays the properties of the hardware component.

   NOTE: When the Configuration Utility is fetching the hardware inventory details of the collection, and there is a disruption in the network connectivity, close the utility and launch it again when the network connectivity is restored. The hardware inventory details do not get refreshed automatically.

   NOTE: For the yx1x systems, the Slot Length and Slot Type fields may show the status as Not Applicable instead of Unknown.

Verifying Communication with Lifecycle Controller

Use the following steps to verify the credentials of the discovered systems with iDRAC:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility.**
2. From the left pane of the **Dell Lifecycle Controller Configuration Utility**, select **Session Credentials, Verify Communication.**
3. Click **Run Check** to verify communication with the iDRACs of the discovered systems.
   A list of iDRACs discovered on the network appears along with their communication status.
4. Once the check is complete, click **Export to CSV** to export the results in CSV format.
   `Provide the location on your local drive or Click Copy to Clipboard to copy the results to the clipboard and save it in plain text format.`

Viewing and exporting Lifecycle Controller logs for a collection

You can view the Lifecycle Controller logs for a collection in a readable format and save or export the logs to a .CSV file in a Unified Naming Convention (UNC) or Common Internet File System (CIFS) share.

To view the Lifecycle Controller logs for a collection:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. Select the **View Lifecycle Controller Logs** option.

   The steps to view and export the log files for a collection are similar to viewing and exporting the log files for a single system.

   Follow step 2 to step 7 as given in Viewing Lifecycle Controller logs on page 59.

   The screen displays the latest 100 logs of each system in the collection by default. For example, if there are 10 systems in the collection, the screen displays 1000 log files.

   NOTE: The number in the **Display** drop-down list is always the total number for the collection. For example, if there are 10 systems in the collection, the drop-down list displays 1000, 2500, 5000, and All.

Modifying credentials on Lifecycle Controllers

On systems with iDRAC, use the following steps to verify and/or modify the WS-MAN credentials configured with the DLCI for Configuration Manager:

NOTE: Dell recommends that you modify the credentials on the Lifecycle Controller and the Configuration Manager database simultaneously.

To modify the credentials on Lifecycle Controllers:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. From the left pane of the **Dell Lifecycle Controller Configuration Utility**, select **Modify Credentials on Lifecycle Controllers.**
3. Type the current user name and password, and the new user name and password. You can provide user credentials authenticated on active directory.

   NOTE: You cannot enter specific special characters in the user name field. For more information on the special characters that you can use in the user name field, see the iDRAC documentation available at **Dell.com/support/home**.

   - **Skip CA check** — this option is selected by default, clear this option to secure communication between the Configuration Manager and the target systems. Clearing this option checks that the certificate on the target system is issued by a trusted certificate Authority (CA). Clear this option only if you trust the target systems.
   - **Skip CN check** — clear this option to enhance security; authenticate system names and prevent impersonation. The common name (CN) need not match the host name of the target system. Clear this option only for trusted target systems.
4. Click **Update**.

   A list of iDRACs that are discovered on the network appears along with their communication status.

   To change the user name and password credentials, and to indicate the change, a series of WS-MAN commands are sent to all systems with iDRAC that are in the collection.
5. After the update is complete, click **Export to CSV** to export the results in CSV format. Provide the location on your local drive.

   or

   Click **Copy to Clipboard** to copy the results to the clipboard and save it in plain text format.

Modifying credentials of Lifecycle Controllers on the Configuration Manager database

To modify the credentials on the Configuration Manager database:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012 console, select **Administration** > **Site Configuration** > **Sites** > **Right-click <site server name>** > **Configure Site Components** > **Out of Band Management**.

The **Out of Band Management Component Properties** window is displayed.

2. Click the **Dell Lifecycle Controller** tab.
3. Under **Local User Account on Lifecycle Controllers**, click **Modify**.
4. In the **New Account Information** window, enter the new user name and new password. Confirm the new password and click **OK**.

You have updated the new user name and password credentials in the Configuration Manager Database.

Platform restore for a collection

You can use this option on the Configuration Utility to perform the following tasks:

- Export the system profiles in a collection. For more information, see Exporting the system profiles in a collection on page 46.
- Import the system profiles in a collection. For more information, see Importing the system profiles in a collection on page 46.
- Manage profiles for a collection.
- Configure Part Replacement properties for a collection. For more information, see Configuring Part Replacement properties for a collection on page 47.

Exporting the system profiles in a collection

You can use this option to take a backup of the system configurations of all the systems in a collection.

To launch the Platform Restore screen for a collection:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. Select the **Platform Restore** option.
   The steps to take a backup of the system configuration for a collection are similar to that of taking a backup of the system configuration of a single system.
3. Follow step 1 to step 6 as given in Exporting the system profile on page 62.

When the backup files for a collection are created, the backup file for each system is created with the prefix you specify, followed by the service tag of the system. This format is to manage the backup files created to ease out the restoring process.

Importing the system profiles in a collection

You can import the system profiles/backup files that you have created. This option is applicable only if you have created backup images/profiles of the systems in the collection.

To launch the **Platform Restore** screen for a collection:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012 in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility.**
2. Select the **Platform Restore** option.
   The steps to import the backup files for a collection are similar to that of importing a backup file for a single system.
3. Follow step 2 to step 6 as given in Importing the system profile on page 63.
   The list of systems for which the backup files exist are displayed in a grid.
4. Select the systems for which you want to import the backup files and click **Next**.
   A task is submitted to the Task Viewer. You can launch the Task Viewer to view the status of the tasks.

   NOTE: If a valid backup file is not available on the network share location for any system, the grid displays the system with the value **No** in the **Backup File** column and the check box is disabled.

Configuring Part Replacement properties for a collection

The steps to configure Part Replacement properties for a collection of systems are similar to that of configuring the properties for a single system. However, the check for valid licenses for the collection of systems is performed only after you complete configuring the other properties and submit the task.

For the 11th generation of PowerEdge servers, the utility checks for a valid license of the Dell vFlash SD card on the Lifecycle Controller of the system and for the 12th generation of PowerEdge servers, the utility checks for an Enterprise license.

To launch the Platform Restore screen for a collection:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. Select the **Platform Restore** option.

   For more information about configuring Part Replacement properties, see Configuring part replacement properties for a system on page 64.

Comparing NIC or CNA profiles against systems in a collection

This feature enables you to generate a comparison report of how a NIC/CNA profile is applied to systems and identify any mismatches from the target systems.

To generate a comparison report:

1. In Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012, in **Device Collections**, right-click **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller** > **Launch Config Utility**.
2. Select the **Network Adapter Comparison Report** option.
3. On the **Network Adapter Comparison Report** screen, click **Browse** and select the NIC or CNA profile file that you have applied to the collection.
   A progress bar indicates that the target systems are scanned and a comparison report is generated.
4. After the comparison report is generated, the following colors are displayed:
   - **White** — indicates that the profile that was applied and the profile on the target system are matching.
   - **Red** — indicates that there is a mismatch while applying the profile to the target system.
   - **Grey** — indicates that either the profile you applied is not configured, or the attribute is missing in the target system.

   The following details are also displayed:
   - **Target System** — the name of the target system against which you are comparing the profile.
   - **Target Adapter** — the type of adapter present on the target system. A target system can have multiple adapters.
   - **Configuration Applied** — the configuration is applied to the target system.
5. Select any record on the comparison report and click **View Details** to view the **Port Comparison** details. The details of the ports on the system are displayed. The color coding is similar to the **Comparison Report** screen. See step 4.
6. Select the port and click **View Details** to view the **Personality Comparison** details. The following details are displayed:
   - **Partition** — the partition number on the port.
   - **Personality** — original personality of the target system on the partition.
   - **Personality Applied** — the personality applied from the NIC/CNA profile to the partition.
   - **Min. Bandwidth** — the minimum bandwidth that was available on the partition.
   - **Min. Bandwidth Applied** — the minimum bandwidth applied to the partition.
   - **Max. Bandwidth** — the maximum bandwidth that was available on the partition.
   - **Max. Bandwidth Applied** — the maximum bandwidth applied to the partition.

   The color coding is similar to the **Comparison Report** screen. See step 4 for details.
7. Select any of the partitions and click **View Port Details**. The Port Details screen displays NIC and iSCSI attribute details. The following details are displayed:
   - **Attribute** — the list of NIC or iSCSI attributes.
   - **System Value** — the attribute value that was present on the system.
   - **Value Applied** — the attribute value applied from the profile.

5

Using the Import Server Utility

This section describes the various activities that you can perform using the Import Server utility. This utility is installed when you install DLCI for Configuration Manager. For information on installing Dell Lifecycle Controller Integration for Configuration Manager, see the Installation Guide.

The Import Server utility enables you to:

- Import Dell servers that are not auto-discovered by DLCI for Configuration Manager, but are already part of the Configuration Manager environment. After import, these servers are displayed under **All Dell Lifecycle Controller Servers** > **Dell Imported Servers** and you can then use the DLCI for Configuration Manager features to perform the various operations. For more information, see Importing Dell Servers.
- Import system variables from an external file saved in a .CSV format to systems within a collection. These variables are used when you create a task sequence for deploying the operating system on servers. For more information, see Importing System Variables.

Topics:

Importing Dell servers

To import Dell Servers that are not auto-discovered by DLCI for Configuration Manager:

1. In the Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, or Configuration Manager 2012 console:
   a. Navigate to **Assets and Compliance** and right-click **Devices.**
   b. Select **Dell Lifecycle Controller** > **Import Dell PowerEdge Server.**
2. On the **Import Dell Servers** screen, select the **Import Dell Servers** option.
3. Select **Specify an iDRAC IP address range** and provide an IP address range. This is the range of iDRAC IP addresses of the servers that you are importing.

   You can also select Specify iDRAC IP addresses from a file separated by commas or new lines. Click **Browse** to navigate to the location where you have saved the file in .CSV format.

   In the .CSV file, list IP addresses in one of the following:
   - Separate IP addresses using comma as the delimiter. For example: 172.16.2.5,172.16.2.38,172.16.1.1.
   - Include IP addresses in separate lines. For example:
     - New Line: 172.16.1.1
     - New Line: 72.16.1.5
     - New Line: 172.16.1.45
4. In **Collection Name**, enter or type the name of the collection. Make sure that the unique collection name is provided. If you provide the existing collection name, the error message **<collection name> already exists** is displayed .
5. Click **Next**.

   The iDRAC Authentication process verifies the iDRAC credentials that you have provided when you install DLCI for Configuration Manager against each of the iDRAC IP addresses you have specified. The grid displays the IP Address, name of the server, and the status of the authentication.

   You can provide user credentials authenticated on active directory.

   If the iDRAC user you have specified is not present on the iDRAC of any of the servers you want to import, then the status is displayed as Authentication failed, and you cannot import that server.

   Licensing Information
   Licensed nodes: Number for nodes provided.
   Nodes in use: Number of nodes assigned to servers.

The managed server is displayed in green color.

6. Click **Next** and select the servers that you want to import. By default, all systems where the Authentication status is **Success** are selected.
7. Click **Save As** to save the report as a .CSV file in any location.
8. Specify the Target Collection under which you want the imported servers to be displayed and click **Next**.
9. Click **Save As** to save the report as a .CSV file in any location.
10. After the import process is complete, click **Close** to close the utility.

Importing system variables

To import system variables from an external file saved in .CSV format:

1. On the Configuration Manager Version 1610, Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Configuration Manager 2012 R2, Configuration Manager 2012 SP1, Configuration Manager 2012 console:
   a. Navigate to **Assets and Compliance** and right-click **Devices.**
   b. Select **Dell Lifecycle Controller** > **Import Dell PowerEdge Server.**
2. In the **Import Dell Servers** screen, select the **Import System Variables** option.
3. Click **Browse** to select the **.CSV** file that contains the variables.
4. Click **Next**.

   The screen displays a comparison report of the variable values already present in the system and the variable values present in the .CSV file.

   The variables should be defined in the following format in the file:

   <System Name>, <variable1 name> = <variable1 value>, <variable2 name>=<variable2 value>.
   For Example:
   ```
   <System Name1>, InstallOSVer=Win2K3,CountDisks=5
   <System Name2>, InstallOSVer=Win2K8,CountDisks=4
   <System Name3>, CountDisks=4,RAIDController=H700
   ```

5. Click **Next**.

   The screen displays a comparison report of the variable values already present in the system and the variable values present in the .CSV file. The following details are displayed:
   - **Name** — the name of the system.
   - **Variable Name** — the name of the variable.
   - **Value in the .CSV file** — the value of the variable in the .CSV file. If the variable is not present in the file, this column displays the value NA.
   - **Value in the System** — the value of the variable in the system. If the variable is not present on the system, this column displays the value NA.
   - **Action** — the action to be taken for the variable. This action always gives precedence to the variables and the values present in the .CSV file.

Table 7. Action And Description

Action	Description
ADD	Add the variable to the target system. Indicates that the variable is present on the file and not available on the system.
DELETE	Delete the variable from the target system. Indicates that the variable is not present on the file but available on the system.
UPDATE	Update the variable on the target system with the value from the .CSV file. Indicates to replace the variable on the system with the variable on the file.
NONE	Take no action.

Table 7. Action And Description (continued)

Action	Description
NA	Not applicable

6. Select the variables you want to import.

   By default, the records with **ADD** and **UPDATE** actions on the grid are selected. The records with the **DELETE** action are not selected. You must select the record if you want to delete it from the system.

   You can also filter the records on the grid based on the system name.

7. Click **Next**.
8. Click **Save As** to save the report as a .CSV file in any location.
9. After the import process is complete, click **Close** to close the utility.

6

Using the System Viewer Utility

This chapter describes the operations that you can perform with the **System Viewer** Utility.

You can use the **System Viewer** Utility to:

- View and edit the hardware configuration. For more information, see Viewing and editing BIOS configuration on page 51.
- View and edit the RAID configuration. For more information, see Viewing and configuring RAID on page 53.
- Create and edit iDRAC configuration profiles for your system. For more information, see Configuring iDRAC profiles for a system on page 53.
- Create configurations for network adapters such as NICs and CNAs and save them to a profile. For more information, see Configuring NICs and CNAs for a system on page 54.
- Create configurations for FC HBA cards and save them as a profile. For more information, see Configuring FC HBA cards for a system on page 57.
- View the current firmware inventory, compare it against a baseline, and update the firmware. For more information, see Comparing and updating the firmware inventory on page 13.
- Compare the hardware configuration profiles. For more information, see Comparing hardware configuration profile on page 59.
- View and export the Lifecycle Controller logs. For more information, see Viewing Lifecycle Controller logs on page 59.
- View the hardware inventory for the system. For more information, see Viewing the hardware inventory for the system on page 62.

  NOTE: You can only edit the hardware configuration and RAID configuration profiles directly, and not edit the system configurations directly.
- Perform tasks to restore a platform that includes:
  - Exporting the system profile to an external location.
  - Importing the saved system profile from an external location.
  - Configuring Part Replacement properties for the system.

  For more information, see Platform restore for a system on page 62.
- Compare an FC HBA configuration profile against a target system. For more information, see Comparing FC HBA profile against a target system on page 65.

Topics:

Viewing and editing BIOS configuration

This feature enables you to view and modify the current BIOS configuration of a system or a collection of systems and save them as a profile.

NOTE: Applying boot sequence across target systems works only if the target systems have the same, equal, or less number of boot devices as it appears on the profile.

NOTE: In Configuration Manager 2012, Operating system Deployment using UEFI boot mode is not supported.

Creating a new profile

To create a new profile:

1. In the **BIOS Configuration** screen, select **Create a New Profile** and click **Next.**
   The **BIOS Attributes** tab displays the BIOS attributes and current settings of the system. The **Boot Sequence** tab displays the boot sequence information of the system.
2. In the **BIOS Attributes** tab, select the attributes to be included in your profile by selecting the check box against each attribute. If you check **Select All,** all the attributes in the list are selected.

   NOTE: You can leave the BIOS attributes in a profile unchecked. If you do not select any of the BIOS attributes in a profile, then only the boot sequence information is considered when you import the profile.

3. Click **Save As Profile** to save the profile as an XML file.

Editing an existing profile

To edit an existing profile:

1. In the **BIOS Configuration** screen, select **Edit an Existing Profile**, and click **Browse** to browse for the profile.
2. Select the profile that you want to edit and click **Next.**
   The **BIOS Attributes** tab displays the BIOS attributes of the selected profile.
3. Select the attributes that you want to edit, and click **Edit Attribute**.
   The **Custom Attribute Editor** displays all the attributes in the drop-down list against the **Attribute Name** field.
4. Select the attribute that you want to edit, and make the necessary changes.
5. Click **OK** to save the changes and exit the **Custom Attribute Editor.**

   NOTE: Click **Reset** to reset any changes made.

Adding a new attribute

To add a new attribute:

1. In the **BIOS Configuration** screen, select **Create a New Profile** or **Edit an Existing Profile**, and click **Browse** to browse for the profile.
2. In the **BIOS Attributes** tab, click **Add Attribute.**
3. In **Custom Attribute Editor**, enter the attribute name in the **Attribute Name** field. A value in this field is mandatory.
4. Select the type of attribute that you want to add from the **Attribute Type** drop-down list. Attributes are of three types:
   - **Enum Attribute** — displays a combo box with multiple values. At least one value should be selected.
   - **Text Attribute** — displays a field with text values. This field can be empty.
   - **Numeric Attribute** — displays a field with integer values. This field cannot be empty.
5. Enter the values of the attributes based on the type of attribute that you select. Let us assume that you have selected the attribute type **Enum Attribute**.
   - To add a value, enter the value of the enumeration attribute in the **Possible Value** field, and click **Add**.
   - To update the value of the attribute, select the value that you want to update, make the necessary changes in the **Possible Values** field, and click **Update.**
   - To delete a value, select the value and click **Delete**. A dialog box appears asking for confirmation. Click **Yes** to delete the value.
6. Click **OK** to close the **Custom Attribute Editor** and go back to the **BIOS Attributes** tab.

Editing an existing BIOS attribute

To edit an existing BIOS attribute, follow the step 2 to step 5 of Editing an Existing Profile.

Changing the BIOS or UEFI boot sequence and hard disk drive sequence

To change the BIOS boot sequence and hard disk drive sequence:

1. In the **BIOS Configuration** screen, select **Create a New Profile** or **Edit an Existing Profile**, and click **Browse** to browse for the profile.
2. Click the **Boot or UEFI Sequence** tab.
   The current BIOS or UEFI boot sequence and hard disk drive sequence is displayed.
3. Use the **Move Up** and **Move Down** to change the BIOS or UEFI boot sequence or the hard disk drive sequence.
   After you manually map SAN boot device in server, it is visible as hard disk drive sequence. To change the boot sequence for SAN boot device, use **Move Up** to move up the SAN boot device in the hard disk drive sequence until it is the first boot device in the hard disk drive sequence.
   NOTE: If more than one SAN boot device is present in the hard disk drive sequence and you select a specified device as the first boot device, the selection of the first boot device is based on the sequence in the Lifecycle Controller.
4. Click **OK** to save the changes.
   NOTE:
   - For 13th generation of Dell PowerEdge servers, you can view the BIOS attributes and boot sequence of the currently saved boot mode only.
   - Click **Reset** to reset any changes made.
   - The following task sequence works: Boot Mode with Boot Sequence followed by any of these configuration tasks, NIC, or RAID; Optionally included with iDRAC configuration tasks.
   - The following task sequence does not work: Boot Mode with Boot Sequence followed by only an iDRAC and only an OSD configuration task does not work.
   - The following task sequence partially works: If boot mode and boot sequence are applied together, then only boot mode works.

Viewing and configuring RAID

This feature enables you to view and configure RAID on the server. To configure RAID:

1. On the **System Viewer** utility, click **RAID Configuration**.
   The **RAID Configuration** screen displays the RAID information of your system, such as number of virtual disks, their controller IDs, RAID levels, and physical disks.
2. Click **Create RAID profile** to create a new RAID configuration profile using **Array Builder**. For more information on using the Array Builder, see Using the Array Builder.

Configuring iDRAC profiles for a system

This features enables you to define the iDRAC configuration and save it and apply the profile to a collection as part of the workflow while deploying an operating system.

You can create or edit iDRAC profiles for a system using the **System Viewer** utility.

Creating an integrated Dell Remote Access Controller profile

To create an iDRAC profile:

1. On the **System Viewer** utility, click **iDRAC Configuration**.
   The iDRAC Configuration options are displayed.
2. Select **Create a New Profile** and click **Next**.
3. Click the **Network Configuration** tab.
4. Select the attributes you want to configure from the drop-down list. You can configure the following attributes:

- **LAN Settings**
- **Advanced LAN Settings**
- **Common IP Configuration**
- **IPv4 Configuration**

NOTE: For more information on the various parameters that you can set for the above attributes, see the *Integrated Dell Remote Access Controller7/8 with Lifecycle Controller Version 2.30.30.30* available at **Dell.com/support/home**.

5. Click the **Users** tab.
   The grid retrieves the list of iDRAC users from the system and displays them.
6. You can add a user account or edit an existing user account. iDRAC has 16 users out of which you can configure 15.
   - To add a new user account, select a user account that is not configured.
   - To edit a user account, select the account on the grid and click **Edit**, or double-click the user account.

     The **Edit User** screen is displayed.

   NOTE: You cannot edit the user account that DLCI uses to access the iDRAC of the system.

7. Specify the following details:
   - **General Details** — Type the user name and password. You must specify the password when you create or edit a user account.
   - **IPMI LAN user Privilege granted** — Select the type of user from the drop-down list to grant the IPMI LAN user privilege.
   - **Other Privilege** — Select the Integrated Dell Remote Access Controller group from the drop-down list and select the privileges that you want to assign to that group.

     For more information on the privileges, see the *Integrated Dell Remote Access Controller7/8 with Lifecycle Controller Version 2.30.30.30* available at **Dell.com/support/home**.

8. Click **OK** to save the user account configuration and revert to the **Users** tab.
9. Click **Save As Profile** to save the Integrated Dell Remote Access Controller configuration profile.

Editing an integrated Dell Remote Access Controller profile

To edit an iDRAC profile:

1. On the **System Viewer** utility, click **iDRAC Configuration**.
   The iDRAC configuration options are displayed.
2. Select **Edit an Existing Profile**.
3. Click **Browse** and navigate to the location where you have saved the iDRAC configuration profile, and click **Next**.
4. In the **Network Configuration** tab, select the attribute you want to edit.

   NOTE: For more information on the various parameters that you can set for the preceding attributes, see the *Integrated Dell Remote Access Controller7/8 with Lifecycle Controller Version 2.30.30.30* available at `Dell.com/support/home`.

5. Click the **Users** tab.
   The grid retrieves the list of iDRAC users on the existing profile and displays them.
6. You can add a user account or edit an existing user account. For more information, see step 6 and step 7 in Creating an integrated Dell Remote Access Controller profile on page 53.
7. Click **Save As Profile** to save the modified iDRAC configuration profile.

Configuring NICs and CNAs for a system

This feature enables you to configure the different attributes of specific network interface cards (NICs) or converged network adapters (CNAs) in the system and save them to a profile. You can create NIC or CNA profiles for a system but the profiles can be applied only to a collection. This feature enables NIC partitioning in the collection.

Each type of NIC is associated with a template. This template does not contain any specific instance information and is agnostic of any system. For example, a **DualPort-QuadPartition-NIC** template enables you to configure the eight partitions of CNA to various roles.

For information on NICs supported by Lifecycle Controller, see the *Dell Lifecycle Controller Unified Server Configurator/Unified Server Configurator-Lifecycle Controller Enabled User's Guide* available at **Dell.com/support/manuals**.

Creating a NIC or CNA profile

To create a NIC/CNA profile:

1. On the **System Viewer** utility, click **Network Adapter Configuration**.
   The options to create a new profile, edit an existing profile, or scan a collection to identify the adapters are displayed.
2. Select **Create new profile** and click **Next**.
   The **Network Adapter Configuration** screen is displayed.
3. Click **Add** to add an adapter.
4. In the **Add Adapter** dialog box, perform the following:
   - Select the **Adapter type** from the drop-down list.
   - Select the adapter location and specify the slot number.
   - Click **OK**.

     The adapter is now added to the **Network Adapter Configuration** screen.
5. If you want to remove any of the adapters from the profile, select the adapter and click **Remove**.
6. Select the adapter and click **Configure** to configure it. For more information on configuring the adapter, see Configuring Adapters.
7. After you complete configuring the adapters, click **Save as profile** to save the NIC profile.
   If you have not configured any of the adapters in the profile, the following message is displayed:

   ```
   No Adapter is configured. Please configure before saving.
   ```

   Click **OK** and configure some of the adapters before saving the profile.

   If you have configured some of the adapters and not all of them, the following message is displayed:

   ```
   You have not configured all adapters and settings. Are you sure you want to save the profile?
   ```

   Click **OK** to continue saving the profile, or click **Cancel** to configure all the adapters.

Scanning a collection

You can scan a collection and identify configured adapters and list the NIC or CNA profiles to edit them. To scan a collection:

1. On the **System Viewer** utility, click **Network Adapter Configuration**.
2. Select **Scan collection to identify adapters** and click **Next**.

   NOTE: Before the utility scans the collection, a warning is displayed that indicates that the process may take a long time. If you click **Cancel**, the scan process is aborted and the **Scan collection to identify adapters** option is not selected.
3. The utility scans the collection and a progress bar displays the progress of the task. Click **Next** after the task is complete.
4. The **Network Adapter Configuration** screen displays the adapters in the collection.
5. Select the adapters you want to configure and click **Configure**. For more information, see Configuring adapters on page 55.
6. If you want to remove any of the adapters from the profile, select the adapter and click **Remove**.
7. You can also click **Add** to add an adapter to the profile. For more information, see step 4 in Creating a NIC or CNA profile on page 55.
8. Click **Save as profile** to save the modified NIC profile.

Configuring adapters

To configure the adapters:

1. Select the adapter on the **Network Adapter Configuration** screen and click **Configure**.

The **Adapter Configuration** dialog box is displayed.

2. Select one of the following options:
   - **Configure adapter settings** — to configure the settings.
   - **Copy settings from adapter** — to copy the configuration settings from an adapter that is already configured.
3. Click **Configure**.
   The **Configure Adapter** dialog box is displayed.
4. Select the port that you want to configure and click **Configure**.
5. Select one of the following options:
   - **Configure port settings** — to configure the port settings. Proceed to the next step if you want to configure the port settings manually.
   - **Copy settings from port** — to copy the port settings from a port that is already configured. Proceed to step 7 if you are copying the port settings.
6. You need to choose the personalities for each partition on the port, enter bandwidth and configure settings for each personality. One port can have up to four partitions with one personality assigned to each partition.

   Under **Personalities and Settings**, select the personality against each partition and set the minimum and maximum bandwidth. You can select from one of the following options:
   - **NIC**
   - **iSCSI**
   - **FCoE**

   NOTE: You can select the personalities only for CNAs and not for NICs.
7. Click **Port Settings** to configure the NIC and iSCSI parameters. For more information, see Configuring NIC and iSCSI Parameters.
8. Click **OK** to save the configurations.

Configuring NIC and iSCSI parameters

You can configure the NIC and iSCSI parameters from the Port Settings screen.

To configure the NIC and iSCSI parameters:

1. In the **Port Settings** screen, on the NIC tab, specify the following parameters:
   - **Select All** — select to check all the options available for NIC.
   - **Boot protocol** — select the protocol for booting the system. You can choose from PXE, iSCSI, or FCoE.
   - **Wake on LAN** — select to switch on the system throughout your LAN. You can choose to enable or disable this option.
   - **Wake on LAN link speed** — specify the Wake on LAN link speed from the drop-down list.
   - **VLAN mode** — select to add your system to a VLAN if it is not located on the same network switch. You can choose to enable or disable this option.
   - **Link speed** — select the NIC link speed.
   - **Flow Control** — select the data flow control.
   - **IP auto configuration** — select to automatically configure the IP address for the system. You can choose to enable or disable this option.
   - **SRIOV configuration** — select to configure Single Root Input/Output Virtualization for the system. You can choose to enable or disable this option.

   Click **OK** to save the settings.
2. Click the **iSCSI** tab and specify the following parameters:
   - **CHAP authentication** — enable or disable the challenge handshake authentication protocol (CHAP) for the system while discovering an iSCSI target. If you enable this option, you must type the CHAP ID and CHAP Secret throughout the iSCSI Initiator Parameters Configuration screen.
   - **CHAP mutual authentication** — enable or disable a two way CHAP authentication between systems within a network while discovering an iSCSI target.
   - **iSCSI via DHCP** — enable or disable discovering the iSCSI target using DHCP.
   - **Windows Boot HBA Mode** — disable this attribute when the host operating system is configured for software initiator mode and to enable this for HBA mode. This option is available on NetXtreme adapters.
   - **Boot to Target** — enable or disable this attribute. If you enable this option, the iSCSI boot host software attempts to boot from the iSCSI target.

- **DHCP Vendor ID** — specify the DHCP Vendor ID in this field. If the Vendor Class ID field in the DHCP Offer packet matches the value in this field, the iSCSI boot host software looks for the required iSCSI boot extensions. You do not need to set this value if the iSCSI via DHCP option is disabled.
- **LUN Busy Retry Count** — specify the number of connection retries the iSCSI Boot initiator should attempt if the iSCSI target LUN is busy.

3. Click **OK** to save the configurations.

Editing a NIC or CNA profile

To edit a NIC/CNA profile:

1. On the **System Viewer** utility, click **Network Adapter Configuration**.
2. Select **Edit an Existing Profile**.
3. Click **Browse** and navigate to the location where you have saved the NIC profiles.
4. Select the profile that is saved as a .XML file and click **Next**.
   The **Network Adapter Configuration** screen displays the adapters that you have configured in the profile.
5. Select the adapter you want to edit and click **Configure**. For more information on configuring the adapter, see Configuring adapters on page 55.
6. If you want to remove any of the adapters from the profile, select the adapter and click **Remove**.
7. You can also click **Add** to add an adapter to the profile. For more information, see step 4 in Creating a NIC or CNA profile on page 55.
8. Click **Save as profile** to save the modified NIC profile.

Configuring FC HBA cards for a system

This feature enables you to configure different attributes of FC HBA cards in a system and save them as a profile. The attributes available for FC HBA configuration are static set of attributes. You can create FC HBA profiles for a system but the profiles can be applied only to a collection.

Creating an FC HBA profile

To create an FC HBA profile, perform the following steps:

1. On the **System Viewer** utility, click **FC HBA Configuration**.
   The options to create a new profile or edit an existing profile are displayed.
2. Select **Create a New Profile** and click **Next**.
   The **FC HBA Configuration** screen is displayed.
3. Click **Add** to add an FC HBA adapter port.
4. In the **Add Adapter** dialog box, specify the following details:
   - Select the adapter port location as **Embedded** or **Mezzanine** from the drop-down list.
   - Specify the slot number and port number.

   The adapter port is now added to the **FC HBA Configuration** screen.
5. In the **FC HBA Configuration** screen, select an adapter port and click **Remove** to remove any of the adapter ports from the profile.
6. In the **FC HBA Configuration** screen, select an adapter port and click **Configure** to configure it.
   The **Port Settings** dialog box is displayed, which enables you to configure the FC HBA attributes.
   In the **Port Settings** dialog box, on the **FC** tab, specify the following attributes:
   - **Select All** — Select to check all the available options for FC HBA.
   - **Port Speed** — Select the port speed from the drop-down list. The number indicates the speed in Gbps. The default value is Auto.
   - **FC Tape Enable** — Select **Enabled** to enable FC tape. You can choose to enable or disable this option. The default value is Enabled.
   - **Loop Reset Delay** — Select to specify loop reset delay.
   - **Frame Payload Size** — Select to specify frame payload size.

- **Port Login Retry Count** — Select to specify the number of times you try to log in.
- **Port Login Timeout** — Select to specify port login timeout.
- **Port Down Retry Count** — Select to specify port down retry count.
- **Link Down Timeout** — Select to specify link down timeout.
- Click **OK** to save the port settings and return to the **FC HBA Configuration** screen and configure other FC adapter ports before saving the profile.

NOTE: See relevant vendor documentation to determine the possible values while setting the link down timeout and port login timeout of FC HBA.

7. After you complete configuring all the FC adapter ports, click **Save as Profile** to save the FC HBA profile as an XML file.

Editing an FC HBA profile

To edit an FC HBA profile:

1. On the **System Viewer** utility, click **FC HBA Configuration**.
2. Select **Edit an Existing Profile**.
3. Click **Browse** and navigate to the location where you have saved the FC HBA profiles.
4. Select the FC HBA profile that is saved as a .XML file and click **Next**.
   The FC HBA adapter ports that you have configured in the profile are displayed in the **FC HBA Configuration** screen.
5. Select the FC HBA adapter port you want to edit and click **Configure**. For more information on configuring the adapter port, see step 6 of Creating an FC HBA profile on page 57.
6. If you want to remove any of the adapter ports from the profile, select the FC HBA adapter port and click **Remove**.
7. Click **Save as profile** to save the modified FC HBA profile.

Comparing and updating firmware inventory

This feature enables you to view, compare, and update current firmware versions for specific systems. It also enables you to compare the BIOS and firmware versions of your system against another system, Dell FTP site, or against a PDK catalog that you downloaded from the Dell Support site.

To compare and update the firmware inventory of a system:

1. On the **System Viewer** utility, click **Firmware Inventory, Compare, and Update**.
   The system components and their current firmware versions are displayed in the right-hand pane.
2. Click **Export Profile** to export the software inventory information in XML format.
3. Click **Next** and select one of the following options to specify the baseline against which you want to compare the firmware inventory of the collection of servers:
   - **Dell PDK Catalog** — to specify a Dell PDK catalog that you can use to compare the firmware inventory. To specify a PDK catalog:
     - Click **Browse** to navigate to the file location where you have saved the catalog. Ensure that the catalog resides on a CIFS share that is accessible to the Dell Lifecycle Controller of the system.
     - Specify the **User Name** and **Password** to the CIFS share where your catalog resides if you want to update the firmware inventory from the catalog. You do not need to specify the user name and password if you are viewing or comparing against the catalog.

       NOTE: To update the firmware inventory, you must point to a local repository.
   - **FTP: ftp.Dell.com** — to connect to the Dell FTP site to compare and update the firmware inventory of the system.
   - **Firmware Inventory Profile** — to specify an existing profile that you have saved and use it to compare and update the firmware inventory for the system.
4. Click **Next**. The screen displays the following baseline details against which you can compare the firmware of your collection:
   - **Selective Firmware Update —** Enables you to select the components that needs to be updated. Only selected components are updated. All components are selected by default other than the components which contains the status as **Unavailable**, **Not Updatable**, and **Coequal**.
   - **CMC —** Click **Export to XML**, to export an inventory of chassis and servers from DLCI. You can use this information to create repository using DRM. Once the repository is created, select the CMC and then initiate the firmware update using the repository bundle created by DRM.

CMC firmware cannot be updated directly from DLCI console.

CMC cannot be updated using catalog, you can update the CMC using `.bin` or `.cmc` file from DRM repository.

- **Component —** displays the component names.
- **Version —** displays the firmware versions of the components.
- **Baseline Version** — displays the baseline versions of the components.
- **Status** — displays the status of the firmware and indicates whether the firmware of the system is same, or needs an update based on the repository selected.

Following are the status of the firmware:

- **Urgent**: Indicates the critical updates that are used to resolve security, performance, or break-fix situations in a component.
- **Recommended**: Indicates the bug fixes and feature enhancements of the product.
- **Optional**: Indicates about the new features or any specific configuration updates.
- **Same**: Indicates the same baseline version.
- **Downgrade**: Indicates the downgrade of the current version.
- **Not Updatable**: Indicates the baseline version is not updatable.
- **Not Available**: Indicates the baseline version is not available.

5. You can filter the information based on any of the baseline details, set schedule based on the available options and then click **Update** to update your system with the latest firmware.
   - **start now** — to start the update.
   - **start on next reboot** — to start the update when the target system reboots.
   - **schedule update** — to set a date and time for the update. If the updates are scheduled in sequence within an hour of each other, then a warning message is displayed.

Comparing hardware configuration profile

This feature enables you to compare and report the BIOS or iDRAC configuration profiles that are applied on a system.

To compare the hardware configuration profile:

1. On the **System Viewer** utility, click **Compare Hardware Configuration Profile**.
2. After the comparison report is generated, the screen displays the following colors to indicate the status of the comparison:
   - **White** — indicates that the profile applied matches the profile on the target system .
   - **Red** — indicates that there is a mismatch while applying the profile to the target system.
   - **Grey** — indicates that either the profile you applied is not configured, or the attribute is missing in the target system.
3. The **Compare Hardware Configuration Profile** screen displays the following fields:
   - **Attribute Name** — lists the BIOS or iDRAC attributes depending on the profile you have selected.
   - **System Value** — lists the current value of the BIOS or iDRAC attribute. If there are no values, the value displayed is NA.
   - **Profile Value** — lists the value of the attributes in the profile. If there are no values, the value displayed is NA.

Viewing Lifecycle Controller logs

This feature enables you to view the Lifecycle Controller logs in a readable format and save or export the logs to a .CSV file. The Lifecycle Controller logs contains details such as history of firmware upgrades, changed events for updates and configuration, and user comments.

To view the Lifecycle Controller logs:

1. On the **System Viewer** utility, select **View Lifecycle Controller Logs**. The **View Lifecycle Controller Logs** screen displays the following fields:
   - **Existing Share**— Specify the UNC or CIFS share where you want to save the file in the following format: \\<IPAddress>\<share>\filename. The filename is provided by default and you cannot change the filename. This information is cached for subsequent viewing. It is recommended that you specify an empty share each time you want to view the Lifecycle Controller log files. If you use an existing location then make sure that the location is empty.
   - **Domain\User Name** — Specify the correct domain and user name required by Lifecycle Controller to access the UNC or CIFS share.

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

2. Click **Next**.

   The **View Lifecycle Controller Logs** screen is displayed.

   The screen displays the latest 100 logs by default. You can modify the number of logs to be displayed only when you click **Pause** or after all the 100 logs are displayed on the screen. The following details are displayed:

Table 8. Lifecycle Controller log details

Column	Description
Hostname	This is the hostname of the system for which you are viewing the Lifecycle Controller logs. This is displayed only in the case of a collection of systems and not a single system.
No.	This is the sequence number of the log.
Category	The category of the Lifecycle Controller Log. For example, Configuration Service, iDRAC, Inventory, and so on.
ID	This is the ID associated with an error message. Click the hyperlink to get more information on the error and the recommended action. You can periodically download the latest message registry from the Dell support website available at **Dell.com/support/manuals**. For more information, see Downloading and Updating the Latest Message Registry. If the ID is missing in the local message registry, an error is displayed and you must download the latest message registry file from **Dell.com/support/manuals**.
Description	The message/description of the Lifecycle Controller Log.
Timestamp	The date/time stamp when the Lifecycle Controller log was created.

   You can configure the default number of log files you want to view. This is a global setting that defines the maximum number of logs to be displayed on the grid. To configure the default number of log files:

   a. Open the **DLCSystemview.exe.config** or the **DLCConfigUtility.exe.config** from the folder where you have installed DLCI for Configuration Manager.

   b. Search for the **MAX_LC_LOGS_TO_DISPLAY** parameter and specify a number.

   When you choose **All** in the Lifecycle Controller Logs Viewer, the number of logs you have specified are displayed.

3. Click **View** after specifying the number of records you want to view.

   NOTE: This step is applicable only when you manually enter the number of records without selecting from the drop-down list. If you select the number from the drop-down list, the records are displayed automatically. You cannot specify any value lesser than the number of records that can be viewed at a time. If you want to view reduced number of records, then you must sort and filter the records per system or close the **System Viewer** utility (Config Utility in the case of a collection) and reopen the same.

   When loading the logs, if there are more records to be loaded, the following message is displayed:

```
More records to be displayed.
```

   When all the records are loaded, the following message is displayed:

```
There are no more records to be displayed.
```

4. To filter the logs based on the text you entered, provide details in the **Search**.
   - If you do not provide the search string, then all the logged information is displayed. Logs are filtered based on information present only under description.

- In the search field, filter information for the number of logs you have selected in the preceding step is displayed.

5. (Optional) To fetch fresh Lifecycle Controller logs from the system, click **Refresh**.
6. (Optional) When you are loading a large number of logs, you can click **Pause** to temporarily stop the loading of log files. During this phase, you can change the number of records you want to view by selecting the number from the drop-down list.
7. Click **Resume** to resume the loading of logs.
8. Click **Export to CSV** to save the file in CSV format at a specific location. This option exports only the log files that are displayed on the grid. If you have filtered the data on the grid, this option exports only the filtered data.

Downloading and updating the 11th and 12th generation message registry

Dell recommends that you close all the DLCI utilities such as the **System Viewer** Utility, Config Utility, and Task Viewer before you download and extract the message registry.

The message registry does not contain detailed information for user defined Logs of type **Work notes** (for example, WRK001) or Logs with category **Other**.

To download the 11th and 12th generation Message Registry on the system where you have installed DLCI for Configuration Manager:

1. Visit **delltechcenter.com/LC**.
2. Navigate to **Lifecycle Controller 2 (LC2) Home**.
3. On the **Lifecycle Controller 2 (LC2)** page, in the **Dell Event / Error Message Reference** section, click **Dell Message Registry - English (2.1)**.

   For the 11th generation of PowerEdge servers, click **Dell Message Registry - English (1.6)**.
4. Click the **Dell Event / Error Message Reference 2.1** download link.

   For the 11th generation of PowerEdge servers, click the **Dell Event / Error Message Reference for iDRAC6, LC 1.6** download link.
5. Extract the `PLC_emsgs_en_2.1.zip` file to an empty folder.

   For 11th generation of PowerEdge servers, extract the `PLC_emsgs_en_1.6.zip` file to an empty folder.
6. Copy all the files and folder under the extracted folder to the following folder location: `C:\Program Files\Microsoft Configuration Manager\AdminUI\XmlStorage\Extensions\DLCPlugin\emsgs_en`.
7. When you update the message registry, make sure you extract, copy the fresh files and folders, and overwrite the files and folders under the `emsgs_en` folder.

Downloading and updating the 13th generation message registry

To download the 13th generation Message Registry on the system where you have installed DLCI for Configuration Manager:

1. Visit **delltechcenter.com/LC**.
2. In the **Dell Event / Error Message Reference** section, click **Dell Message Registry - English (2.2)**.
3. Click the **iDRAC8 with Lifecycle Controller Dell Event / Error Message Registry 2.2** download link.
4. Extract the `MSG_REG_2.20.20.20.zip` file to an empty folder.
5. Copy all the files and folders from `MSG_REG_2.20.20.20.zip\MSG_REG_2.20.20.20\MSG_REG_en_WAVE4_XML_XSL_XSD_July14` to the following folder location: `C:\Program Files\Microsoft Configuration Manager\AdminUI\XmlStorage\Extensions\DLCPlugin\emsgs_en`.
6. When you update the message registry, make sure you extract, copy the fresh files and folders, and overwrite the files and folders under the `emsgs_en` folder.
7. Rename `MSG_REG_en.xml` to `emsg_en.xml`.

NOTE: The 13th generation message registry does not contain the 11th generation and 12th generation message registries.

Viewing the hardware inventory for the system

You can use the **System Viewer** utility to view the hardware inventory details of the selected system.

To view the hardware inventory for the system:

On the **System Viewer** utility, select **Hardware Inventory**.

The right-hand pane of the **System Viewer** utility displays the following details:

- **Hardware Component** — displays the name of the hardware component.
- **Properties** — displays the attributes of the hardware component.
- **Value** — displays the value against each attribute of the hardware component.

NOTE: For the PowerEdge 11G systems, the **Slot Length** and **Slot Type** fields may show the status as **Not Applicable** instead of **Unknown.**

Platform restore for a system

You can use this option on the **System Viewer** utility to perform the following functions:

- Export a system profile. For more information, see Exporting the system profile on page 62.
- Import a system profile. For more information, see Importing the system profile on page 63.
- Manage profiles.
- Configure Part Replacement properties for a system. For more information, see Configuring part replacement properties for a system on page 64.

Prerequisites to export or import a system profile

You must upgrade the firmware to the following versions:

- iDRAC Firmware for blade systems to version 3.30 or higher.
- iDRAC Firmware for rack and tower systems to version 1.80 or higher.
- Lifecycle controller firmware to version 1.5 or higher.
- When exporting a system profile, if you want to schedule a backup, then you must have administrative privileges to access the iDRAC vFlash Card or a Network share.

For more information on updating you firmware versions, see Comparing and Updating the Firmware Inventory.

Exporting the system profile

You can create a backup of the system profiles and export it to an iDRAC vFlash Card or a Network share. This feature backs up the following:

- Hardware and firmware inventory such as BIOS, LOMs, and Storage Controllers (RAID level, virtual disk, and controller attributes).
- System information such as service tag, system type, and so on.
- Lifecycle Controller firmware images, system configuration, and iDRAC system profiles.

To export the system profile:

1. On the **System Viewer** utility, select **Platform Restore**.

   For the 11th generation of PowerEdge servers, the utility checks for a valid license of the Dell vFlash SD card on the Lifecycle Controller of the system and for 12th and 13th generations of PowerEdge servers, the utility checks for an Enterprise license, and also the firmware version. If a valid license is present, the **Platform Restore** screen is displayed.

   NOTE: This feature is available only for Lifecycle Controller version 1.5 and later.

2. On the **Platform Restore** screen, select the **Export Server Profile** option and click **Next.** The options to select the vFlash media or location are displayed.
3. Select one of the following options:
   - **vFlash media**: backs up on the iDRAC vFlash Card.

NOTE: In a vFlash card, an existing system profile is overwritten when you export a system profile.

- **Network share**: backs up on a shared location on the network. If you choose this option you must specify the following information:
  - **Existing share**: Specify share location if you are creating a backup for the first time. This information is cached for subsequent backups and you can select the existing location from the drop-down box.
  - **User name**: Specify the user name to access the share location. You must specify the user name in the following format: Domain\<username>. This information is also cached after the first backup. You can use the same name for subsequent backups.
  - **Password**: Specify the password to access the share location and re-type the password to confirm it.

NOTE: Ensure the share location that you specify is writable and there is enough disk space to allow Lifecycle Controller to save the backup file.

4. Enter a backup file passphrase. This is used to lock the encrypted portions of the backup file. For a successful backup operation, the backup file passphrase has to be in a specific format, which is as follows:
   - the passphrase must contain a minimum of 8 characters.
   - the passphrase must contain the following combination of characters— at least 1 title case character, at least 1 lower case character, at least 1 special character, and at least one numeric character.

   If the Export File location is a network share, you have to specify the backup file prefix. This prefix must be unique for a system or a collection.

   The backup file is appended with the hostname of the system and saved in the following format: *<prefix>-<hostname>*. For example, if the prefix you specify is ABC123, and the hostname of the system is ABCDEFG, the backup file is saved as ABC123-ABCDEFG.

   Click the **View previous backup files** link to view any previously created backup files prefixes.

   NOTE: If you have specified a file name prefix that is the same as an earlier backup file, the utility prompts you to specify a different file name to avoid overwriting an existing file. If the same file name prefix is given at the System Level and also at the Collection Level, for a same share location, it is overwritten without a prompt.

5. The backup is scheduled.

   The options available are:
   - **Start now**: used to instantly backup system profiles to an iDRAC vFlash Card or a Network share.
   - **One time**: used to schedule a backup once. Set date and time to backup system profile once to an iDRAC vFlash Card or a Network share.
   - **Recur**: used to schedule a backup multiple times periodically. Provide the frequency you want to set to backup system profiles, using **days** and **Number of occurrences** , to an iDRAC vFlash Card or a Network share.

6. Click **Next.**
   A summary screen is displayed.
7. Click **Finish** to submit the backup process to the task viewer.
   The following message is displayed: `Task submission complete.` You can launch the Task Viewer to view the status of the task.

Importing the system profile

This feature enables you to import the backup of the firmware and configuration of a system, and restore it to the same system where the backup was taken from.

You can use this feature only if you have taken a backup image of the system profile before.

NOTE: If you replace the motherboard of the system, make sure you re-install the hardware back in the same location. For example, install the NIC PCI card in the same PCI slot that you used during backup.

Optionally, you can delete the current virtual disk configuration and restore the configuration from the backup image file.

To import the system profile:

1. On the **System Viewer** utility, select **Platform Restore**.
   The **Platform Restore** screen is displayed.
2. On the **Platform Restore** screen, select the **Import Server Profile** option and click **Next**. The options to select the vFlash media or share location are displayed.

3. Select one of the following options:
   - **vFlash media**: to restore the backup image from the iDRAC vFlash Card.
   - **Network share**: to restore the backup image from a shared location on the network. If you choose this option, you must specify the following information:
     - **Existing share**: specify share location where you have saved the backup image. The drop-down list contains the list of shares where you had previously created backup files for the system or collection.
     - **User name**: specify the user name to access the share location. You must specify the user name in the following format: Domain\<username>.
     - **Password**: Specify the password to access the share location and re-type the password to confirm it.

   NOTE: While importing a backup file created using the **Recur** scheduling option, ensure that you prefix the backup file with `<Recurrence number>_<Prefix>`.

4. Click **Next**. Type the backup file passphrase that you specified while taking a backup.
5. Click **Next**. While importing the backup file, you can choose to retain the current RAID controller configuration, or restore the backed up configuration from the backup file. Choose one of the following options:
   - **Preserve**: Retains the existing RAID controller configuration.
   - **Delete**: Deletes the existing RAID controller configuration and import the configuration from the backup file.

   NOTE: This operation does not restore content that was on the virtual disk during the backup. For example, Operating System. This operation only creates a blank virtual disk and sets the attributes.

6. Click **Next**.
   A summary screen is displayed.
7. Click **Finish** to start the importing the backup file and submit the task to the **Task Viewer**.
   You can launch the **Task Viewer** to view the status of the task.

Configuring part replacement properties for a system

The Part Replacement feature provides an automatic update of firmware, or configuration, or both of a newly replaced component in a system, to match that of the original part. The newly replaced components could include a PowerEdge RAID controller, NIC or power supply, to match that of the original part. This feature is disabled by default on Lifecycle Controller and may be enabled if required through DLCI. It is a licensed feature and requires the Dell vFlash SD card.

Use the **System Viewer** Utility to configure the Part Replacement properties for a system.

To configure the Part Replacement properties:

1. On the **System Viewer** Utility, select **Platform Restore.**
   For the11th generation of PowerEdge servers, the utility checks for a valid license of the Dell vFlash SD card on the Lifecycle Controller of the system and for the 12th and 13th generation of PowerEdge servers, the utility checks for an Enterprise license. If a valid license is present, the **Platform Restore** screen is displayed.
2. On the **Platform Restore** screen, select the **Configure Part Replacement** option and click **Next.**
   The Part Replacement attributes are displayed.
3. Select the options for the properties as displayed in the following table:

Table 9. Property and options

Property	Options
Collect System Inventory on Start (CSIOR)	• **Disabled**: Disables CSIOR for the replaced part. • **Enable**: Enables CSIOR for the replaced part. • **Do Not Change**: Retains the default settings.
Part firmware update	• **Disabled**: Disables the firmware updates for the replaced part. • **Allow version upgrade only**: Performs firmware update on replaced parts if the firmware version of the new part is lower than the original part. • **Match firmware of replaced part**: Performs firmware update on replaced parts to the version of the original part. • **Do Not Change**: Retains the default settings.

Table 9. Property and options (continued)

Property	Options
Part configuration update	• **Disabled**: Disables the operation that applies the current configuration to a replaced part. • **Apply always:** Applies the current configuration to the replaced part. • **Apply only if firmware matches**: Applies the current configuration only if the current firmware matches with the firmware of the replaced part. • **Do Not Change**: Retains the default settings.

4. Click **Finish** after selecting the required options.
   The following message is displayed: `Task submission complete`.

   A task is submitted to the **Task Viewer**. You can launch the **Task Viewer** to view the status of the task. The task configures the Lifecycle Controller of the system with the Part Replacement configuration. This configuration takes effect when you replace any part for the system.

   If you have updated the Part Replacement Attributes, sometimes the updates are not set immediately. Wait for couple of minutes and check to see if the updates are set.

Comparing FC HBA profile against a target system

This feature enables you to generate a comparison report of how an FC HBA profile is applied to a target system and identify any mismatches from the target system.

To generate a comparison report:

1. On the **System Viewer** utility, click **Compare FC HBA Configuration Profile**.
2. On the **Compare FC HBA Configuration Profile** screen, click **Browse** and select the FC HBA profile file that you have applied to the collection.
   A progress bar indicates that the target systems are scanned and an FC HBA comparison report is generated.
3. After the FC HBA comparison report is generated, the following colors are displayed on the screen to indicate the status of comparison:
   - **White** — indicates that the FC HBA profile that was applied and the profile on the target system are matching.
   - **Red** — indicates that there is a mismatch while applying the FC HBA profile to the target system.
   - **Grey** — indicates that either the FC HBA profile you applied is not configured, or the attribute is missing in the target system.
4. The **Compare FC HBA Configuration Profile** screen displays the following fields:
   - **Target Adapter** — the type of FC HBA adapter present on the target system. A target system can have multiple adapters.
   - **Location Applied** — the location that is applied on the target system.
5. Select any record on the comparison report and click **View Details** to view the port details. The following fields are displayed.
   - **Attribute** — lists the FC HBA attributes depending on the profile you have selected.
   - **System Value** — lists the current value of the FC HBA attribute in the target system. If there are no values, the value displayed is NA.
   - **Profile Value** — lists the value of the FC HBA attributes in a profile. If there are no values, the value displayed is NA.

   The color coding is similar to the **Comparison Report** screen. See step 3 for details.

7

Troubleshooting

This topic list the issues and steps to troubleshoot them.

Topics:

Configuring Dell provisioning web services on IIS

The installer configures the Dell Provisioning Web Services for Internet Information Services (IIS) automatically during installation.

This section contains information to configure Dell Provisioning Web Services for IIS manually.

Dell provisioning web services configuration for IIS 7.0 or IIS 7.5 or IIS 8.0 or IIS 8.5

To configure Dell provisioning web services for IIS 7.0 or IIS 7.5 or IIS 8.0 or IIS 8.5:

1. Create a new application pool called **Provisioning Web Site** and assign it to the website.
2. Perform the following steps on the **Provisioning Web Site**:
   - In **IIS Manager**, right-click **Provisioning Web Site**, and select **Properties**.
   - Click the **Home Directory** tab.
   - Under **Application Pool**, select **Provisioning Web Site**.
3. On the website, set the default document to **handshake.asmx** and remove any other default documents.
4. Using the Certificates MMC plug-in, install the **PS2.pfx** certificate into the system's **Personal** store.
5. Install the **RootCA.pem** into the system's **Trusted Root Certificate Authorities** store.
6. Import the **ProvisioningCTL.stl Certificate Trust List** file to **Intermediate Certificate Authorities**.
7. Create an SSL certificate configuration that applies the imported **Certificate Trust List**. At the command prompt, paste the following command:
   ```
   netsh http add sslcert ipport=0.0.0.0:4433 appid={6cb73250-820b-11de-8a39-0800200c9a66}
   certstorename=MY certhash=fbcc14993919d2cdd64cfed68579112c91c05027 sslctlstorename=CA
   sslctlidentifier="ProvisioningCTL"
   ```
8. To enforce SSL and client certificates for the website, do the following:
   - Add an SSL binding to set the port to 4433 and to use the **DellProvisioningServer** certificate. A warning displays that the certificate is assigned to another program.
   - Click **OK**.
   - Remove the HTTP binding for port 4431.
   - Select the required SSL option.
   - Select the required client certificates option.
   - Click **Apply**.

Dell auto-discovery network setup specification

For information on auto-discovery error messages, descriptions, and response actions, see the *Dell Auto-Discovery Network Setup Specification* document at **delltechcenter.com**

Troubleshooting the viewing and exporting of Lifecycle Controller logs

When you view the Lifecycle Controller logs for a single system or a collection, the grid view can display the following values — **-1** in the **No. Column**, **Not Available** in the **Category**, **Description**, and **ID** columns.

The possible reasons and resolutions are as follows:

- Lifecycle Controller is running other tasks or processes and hence cannot retrieve the Lifecycle Controller logs for the system or collection.

  Resolution: Wait for sometime and retry retrieving or refreshing the logs for the system or collection to view the logs again.

- Lifecycle Controller cannot access the given CIFS share.

  Resolution: Check the permissions on CIFS share and make sure that the share is accessible from Lifecycle Controller target systems.

- The Site Server cannot access the given CIFS share.

  Resolution: Check the permissions on CIFS share and make sure that the share is accessible from Site server.

- The given CIFS share is read-only share.

  Resolution: Provide the details for a share location with both read and write enabled.

- The exported .XML file is not formed.

  Resolution: For more information, see the *Dell Lifecycle Controller 2 Version 1.00.00 User's Guide* available at **Dell.com/support/home**.

- Upgrading the target system from Lifecycle Controller version 1.3 or 1.4 to Lifecycle Controller version 1.5.

  Resolution: Export the Lifecycle Controller logs, run a Lifecycle Controller wipe through Unified Server Configurator, reinstall Unified Server Configurator, and re-generate the Lifecycle Controller Logs.

Deploying the operating system on Dell's 13th generation of PowerEdge servers using WinPE 3.0

As the drivers for USB3.0 are not available in WinPE 3.0, the OS deployment may fail if the BIOS config settings for **USB 3.0 Setting** and **Memory Mapped I/O above 4 GB** are enabled.

Solution: To boot to winPE3.x (32–bit and 64–bit) in BIOS boot mode on Dell's 13th generation of PowerEdge servers, disable **USB 3.0 Setting** and **Memory Mapped I/O above 4 GB**.

You can update disable the **Usb3Setting** and **MmioAbove4Gb** settings in the **BIOS Config** window by creating a profile on the**System Viewer** and use it for deployment. For more information, refer to the *Dell OpenManage Deployment Toolkit Readme*.

Issues and resolutions

Issue 1

Issue: When you deploy an operating system on a target system with iDRAC configured in a shared network mode, the Windows PE environment may fail to startup on the network drivers, causing the system to restart before reaching the task sequence.

Resolution: This is because the network does not assign IP addresses fast enough. To avoid this issue, ensure that you enable **Spanning Tree** and **Fast Link** on the network switch.

Issue 2

Issue: If the Lifecycle Controller of a system is in use, the system is not discovered.

Resolution: If a system does not show up in a collection, verify whether the log file contains the following error message: `Lifecycle Controller in use.` If it contains the error message:

1. Ensure that the system is not in Power On Self Test (POST) state. A system is in POST state after it is powered on and until it boots to an operating system through any media.
2. Power off the system and wait for ten minutes for it to show up in the collection.

Issue 3

Issue: The **Create Lifecycle Controller Boot Media** option may fail if you have not specified local folder locations for the source and destination folders.

Resolution: Ensure that the source and destination paths used are local paths. For example, **C:** *<folder name>*.

Issue 4

Issue: If the iDRAC version is older than the supported versions in any of the target systems, the **Boot to vFlash** option in the Deploy Operating Systems workflow may fail.

Resolution: On a rack and tower server, ensure that it has iDRAC version 1.3 firmware or later. On a blade server, ensure that it has iDRAC version 2.2 or later.

Issue 5

Issue: When you are deploying an operating system using the **Launch Config Utility**, the advertisements of the task sequence are not displayed on the screen.

Resolution: Ensure that you advertise against the exact collection you plan to deploy to, as advertisements against a parent collection does not apply to the child collection(s).

Issue 6

Issue: While deploying Microsoft Windows Server 2008 R2 from Configuration Manager SP1 R2 with Windows Automated Installation Kit (Windows AIK) 1.1, the following error message is displayed:

```
Operation failed with 0X80070002. The system cannot find the file specified.
```

Resolution: This issue occurs if you use a Windows PE 2.X based boot image created with Windows AIK 1.X for deploying Microsoft Windows Server 2008 R2. Ensure that the task sequence deploying Microsoft Windows Server 2008 R2 uses a Windows PE 3.0 or later based boot image created with Windows AIK 2.X or later. For more information, see the Microsoft Technet site at **technet.microsoft.com**.

Issue 7

Issue: If the target system has an older version of BIOS that does not support a particular method, the following error message is displayed in the DLCTaskManager.log file:

```
Installed BIOS version does not support this method.
```

Resolution: Update the BIOS to the latest supported version.

Issue 8

Issue: If the Lifecycle Controller on the target system is locked by another process, the following error message is displayed in the DLCTaskManager.log file:

```
Lifecycle Controller is being used by another process.
```

Resolution: Ensure that the iDRAC of your system is not in POST state.

Issue 9

Issue: If you do not enter the service tag name of the target system correctly, the discovery and handshake fails and the following error message is displayed:

```
[Server Name] - Handshake - getCredentialsInternal():[Server Name]: NOT AUTHORIZED: No credentials returned
```

Resolution: The service tag name is case sensitive. Ensure that the service tag name imported through the **import.exe** utility matches the service tag name in the iDRAC GUI.

Issue 10

Issue: During Discovery and Handshake, the DPS.log displays an empty *Site code:* followed by a cryptography exception.

Resolution: This issue occurs when the account entered to access Configuration Manager does not have permissions to query WMI and retrieve the site code, or when the server cannot authenticate to the Site Server or domain controller. Verify the Dell Provisioning Server user permissions and perform a **WBEMTest** connection to validate the account, and then reset and rediscover your systems.

Issue 11

Issue: During Discovery and Handshake, the DPS.log displays numerous `createDellCollecions() Either Connection Mgr param is NULL or Collection not yet created` messages.

Resolution: This issue occurs when the account entered to access Configuration Manager does not have permissions to create collections. For more information on setting permissions, see Dell Auto-Discovery Network Setup Specification.

Issue 12

Issue: When an account is cloned from an existing account in Configuration Manager, it is not automatically added to the SMS_Admins group.

Resolution: Verify that the account exists in this group. Verify the Dell Provisioning Server user permissions and perform a **WBEMTest** connection to validate your account. Reset and rediscover your systems.

Issue 13

Issue: Installation fails while installing DLCI for Configuration Manager version 1.3 on Microsoft Windows 2008 32-bit SP2 with the User Account Controller (UAC) option turned on.

Resolution: Turn off UAC and reinstall DLCI for Configuration Manager version 1.3. Alternatively, you can install DLCI for Configuration Manager using the Command Line Interface (CLI). Before you do so, right-click the installer, select **Properties**, click on the **Compatibility** tab and select the **Run as Administrator** option.

Issue 14

Issue: The **Deploy** option does not appear in an existing task sequence after uninstalling and reinstalling DLCI for Configuration Manager.

Resolution: Open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option appears again.

To re-enable the **Apply** option:

1. Right-click the task sequence and select **Edit**.
2. Select **Restart in Windows PE**. In the **Description** section, type any character and delete it so the change is not saved.
3. Click **OK**.
   This re-enables the **Apply** option.

Issue 15

Issue: The **System Viewer** Utility does not display the latest RAID configuration.

Resolution: When you are viewing the RAID configuration for a system using the **System Viewer** Utility, the information is cached. When you update the RAID configuration of the same system, you must close the **System Viewer** Utility and re-open it to view the updated RAID configuration.

Issue 16

Issue: The Modular systems cannot use the hostname in the path to the CIFS share but monolithic systems can use the hostname.

Resolution: For Modular systems you must specify the IP address of the CIFS share.

Issue 17

Issue: When you are updating the systems with the latest firmware, if the Dell Update Packages (DUPS) take longer than 50 minutes to download over a WAN, then the update task may fail.

Resolution: If you face this problem, then you must copy the repository that contains the updates to the local network of the systems you are updating.

Issue 18

Issue: If you have discovered systems with Dell Lifecycle Controller Integration for Configuration Manager version 1.0 or 1.1 and updated the firmware after upgrading to version 1.2 or 1.3, then you must re-discover the systems if you change their hostname during OS deployment.

Resolution: Ensure that you upgrade Lifecycle Controller of the target systems to version 1.4 or later and upgrade iDRAC on the target systems to version 1.5 or later for monolithic systems and version 3.02 or later for modular systems.

Issue 19

Issue: When you are importing the backup image for a system or a collection, and you specify an invalid backup file passphrase, the following error is displayed on the Task Viewer:

```
Backup File passphrase is invalid. Host system has shut down due to invalid passphrase.
Specify a valid passphrase and rerun the task.
```

Resolution: To resolve this issue, restart the workflow to import the backup image and re-submit the task to the Task Viewer. For more information, see Importing the System Profile.

Issue 20

Issue: When the Backup or Restore operations are in progress for a collection, you cannot view the Lifecycle Controller Logs for the collection. The cause for this is that the Lifecycle Controller is busy running the Backup or Restore tasks that are running.

Resolution: To view the Lifecycle Controller Logs, click Refresh on the Lifecycle Controller Logs screen after the Backup or Restore tasks are complete.

Issue 22

Issue: When you continuously add Lifecycle Controller Logs, or one or more of the components continuously create log entries, you may not view the Lifecycle Controller Logs for the collection.

Resolution: To view the Lifecycle Controller Logs, click **Refresh** on the Lifecycle Controller Logs screen after waiting for a short period.

Issue 22

Issue: Creation of unattended operating system media takes a long time in a non-windows operating system deployment.

Resolution: During non-windows operating system deployment, Dell Lifecycle Controller Utility creates the unattended operating system media using the NFS share. If NFS share responds slow, this step takes more time. Use NFSv3 preferably on a server running Red Hat Linux operating system.

ESXi or RHEL deployment on Windows systems moves to ESXi or RHEL collection, but not removed from Windows Managed Collection

A system with Windows operating system deployed is moved to collection **Managed Collection (OS-Deployed)**. And, when you deploy a non-Windows operating system (ESXi or RHEL) on the system, the system gets into **Managed Dell Lifecycle Controller(RHEL)** or **Managed Dell Lifecycle Controller(ESXi)**. However, the machine remains in the **Managed Collection (OS-Deployed)** with the same name.

Resolution: Delete the server before deploying the non-Windows operating system(ESXi/RHEL) and re-import or re-provision the server having the Windows operating system.

8

Related documentation and resources

For more information on Configuration Manager such as installation, features, and functionalities, see the Microsoft TechNet site at **technet.microsoft.com**.

In addition to this guide, you can access the following guides available at Dell.com/support/manuals. On the Manuals page, click **Software and Security** > **System Management**. Click the appropriate product link on the right-side to access the documents:

- *Dell Lifecycle Controller User's Guide*
- *Integrated Dell Remote Access Controller 6 User's Guide*
- *Integrated Dell Remote Access Controller 7 User's Guide*
- *Integrated Dell Remote Access Controller 8 User's Guide*

You can find the following white papers at **Delltechcenter.com**. On the Dell TechCenter Wiki Home Page, click **OpenManage Systems Management** > **LifeCycle Controller**.

- *Dell Lifecycle Controller Remote Services Overview*
- *Dell Lifecycle Controller Web Services Interface Guideline*
- *Dell Auto-Discovery Network Setup Specification*

Topics:

Obtaining Technical Support

For assistance and information about DLCI for Configuration Manager, see **Dell.com/support**.

For customers in the United States, call 800-WWW-DELL (800-999-3355).

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.

For information on technical support, visit URL: **Dell.com/contactus**.

Additionally, Dell Enterprise Training and Certification is available at URL: **Dell.com/training**.

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.

- Direct links:
  - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—https://www.dell.com/esmmanuals
  - For Dell EMC Virtualization Solutions—https://www.dell.com/SoftwareManuals
  - For Dell EMC OpenManage—https://www.dell.com/openmanagemanuals
  - For iDRAC—https://www.dell.com/idracmanuals
  - For Dell EMC OpenManage Connections Enterprise Systems Management—https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Dell EMC Serviceability Tools—https://www.dell.com/serviceabilitytools
- Dell EMC support site:
  1. Go to https://www.dell.com/support.

2. Click **Browse all products**.
3. From the **All products** page, click **Software**, and then click the required link.
4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.