Dell Lifecycle Controller Integration Version 1.3 for Microsoft System Center Configuration Manager

User’s Guide

Notes and Cautions

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

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

Information in this publication is subject to change without notice.

Trademarks used in this text: Dell™, the DELL logo are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries.

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

2011 - 11

Contents

1

Introduction

Dell Lifecycle Controller Integration for Microsoft System Center 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.

At a high level, the remote enablement capabilities consists of:

- Autodiscovery
- Hardware configuration
- Firmware comparison and updates
- Remote OS-Deployment for individual or a collection of Dell systems

What is New

This release of Dell Lifecycle Controller Integration for ConfigMgr supports the following features:

Table 1-1. New Features and Functionalities

New Feature	Functionality
Platform Restore	You can perform tasks with respect to restoring a platform for a system or a collection that includes: • Exporting system profiles to an external location. • Importing the saved system profiles from an external location. • Configuring Part Replacement properties for a system or a collection. For more information, see Platform Restore for a System and Platform Restore for a Collection.

Table 1-1. New Features and Functionalities *(continued)*

New Feature	Functionality
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. For more information, see Viewing Lifecycle Controller Logs and Viewing and Exporting Lifecycle Controller Logs for a Collection.
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. You can later apply these saved profiles to a collection as part of the workflow while deploying an operating system. 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 • Applying a NIC or CNA Profile on a Collection • Comparing NIC/CNA Profiles Against Systems in a Collection
Configure integrated Dell Remote Access Controller profiles for a system or collection	You can define integrated Dell Remote Access Controller configurations for a system and save it as part of the hardware configuration profile of the system. You can later apply these saved profiles to a collection as part of the workflow while deploying an operating system. For more information, see Configuring Integrated Dell Remote Access Controller Profiles for a System.
Connect to Dell FTP for Firmware updates	You can now connect to the FTP site to download firmware updates for a system or collection. You can also schedule a firmware update for a collection. For more information, see: • Comparing and Updating Firmware Inventory. • Comparing and Updating Firmware Inventory for Systems in a Collection.

Table 1-1. New Features and Functionalities *(continued)*

New Feature	Functionality
Importing Dell Servers and System Variables	You can import Dell servers, that are not auto-discovered by Dell Lifecycle Controller Integration for ConfigMgr. The imported servers appear under the All Dell Lifecycle Controller Servers and you can use the Dell Lifecycle Controller Integration 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 ConfigMgr console. For more information, see Using the Import Server Utility.
Access Integrated Dell Remote Access Controller using Active Directory credentials for authentication	You can provide active directory credentials to get authenticated on Integrated Dell Remote Access Controller.
Schedule firmware updates	You can schedule updates for firmware. For more information, see Comparing and Updating Firmware Inventory.
Configure certificate authority (CA) and common name (CN) checks	You can configure CA and CN checks for Dell Lifecycle Controller Integration communication with the targets.

Existing Features and Functionalities

Table 1-2. Features and Functionalities

Feature	Functionality
Auto-discovery and Handshake	This feature enables the Integrated Dell Remote Access Controller on bare metal systems to locate the provisioning service and establish communication with the Site Server. For more information, see Auto-Discovery and Handshake.
System Viewer Utility	This feature enables you to configure individual systems by using the remote enablement capabilities of Dell Lifecycle Controller Integration. For more information, see Using the System Viewer Utility.
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.
Launching the Integrated Dell Remote Access Controller Console	This feature enables you to launch the Integrated Dell Remote Access Controller console from the Task Viewer and from a system in the collection that contains Dell 11g systems. For more information, see Launching the Integrated Dell Remote Access Controller Console.
Task Viewer	This feature enables you to track the status of the tasks handled by Dell Lifecycle Controller Integration for ConfigMgr. For more information, see Task Viewer.

Supported Operating Systems

For information on supported operating systems, see the *Dell Lifecycle Controller Integration 1.3 for Microsoft System Center Configuration Manager Installation Guide*.

Supported Microsoft .NET Versions

For information on supported Microsoft .NET versions, see the *Dell Lifecycle Controller Integration Version 1.3 for Microsoft System Center Configuration Manager Installation Guide*.

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 **support.dell.com/manuals**. On the Manuals page, click **Software→ Systems Management→ Dell OpenManage Releases**. Select the OpenManage release version relevant to you 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.

2

Use Case Scenarios

This section describes typical use cases and tasks that you can perform with Dell Lifecycle Controller Integration for Microsoft System Center Configuration Manager (ConfigMgr).

Common Prerequisites

Before working on the user scenarios, it is recommended that you complete the following prerequisites.

- Make sure that the system is discovered and present under **All Dell Lifecycle Controller Servers** collection under **Computer Management→ Collections**. For more information, see Auto-Discovery and Handshake.
- Install the latest BIOS version on the system for which you are editing the BIOS profile and exporting the same.
- Install the latest version of Lifecycle Controller on the system.
- Install the latest version of Integrated Dell Remote Access Controller firmware on the system.

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 under the **All Dell Lifecycle Controller Servers** on the ConfigMgr console.

Prerequisites

For more information, see Common Prerequisites.

Workflow

1. Launch the **System Viewer** Utility on the ConfigMgr console for a particular system. For more information, see Configuration Utility.
2. Select Hardware Configuration on the **System Viewer** Utility to load the BIOS configuration of the system. For more information, see Viewing and Editing Hardware Configuration.
3. Create a new profile or make changes to an existing profile. For more information, see Creating a New Profile or Editing an Existing Profile.
4. Add, edit, or update the attributes in the profile. For more information, see Adding a New Attribute.
5. (Optional) Change the BIOS boot sequence and hard disk drive sequence. For more information, see Changing the BIOS Boot Sequence and Hard Disk Drive Sequence.
6. Save the profile as a **.XML** file to any folder location on the local system.

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 under the **All Dell Lifecycle Controller Servers** on the ConfigMgr console.

Prerequisites

- Common Prerequisites.
- RAID Controller and firmware that supports Local Key Management.

Workflow

1. Launch the **System Viewer** Utility on the ConfigMgr console for a particular system. For more information, see System Viewer Utility.
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.
3. Launch the Array Builder to create a RAID profile. For more information, see Creating a RAID Profile Using Array Builder.

4. (Optional) Import and edit an existing profile. For more information, see Importing a Profile.
5. Save the newly created RAID profile as a .XML file to any folder location on the local system.

Comparing and Updating the Firmware Inventory

You can use Dell Lifecycle Controller Integration for ConfigMgr 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.
- 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.

Workflow

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 or Configuration Utility.
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.
4. For a collection, see Comparing and Updating Firmware Inventory for Systems in a Collection.

Deploying Operating System on Collection

You can use Dell Lifecycle Controller Integration for ConfigMgr to deploy an operating system on a collection of systems under the **All Dell Lifecycle Controller Servers** on the ConfigMgr console.

Prerequisites

- Common Prerequisites.
- Install Dell Server Deployment Pack version 1.2, available as an additional plugin and then create a task sequence using Dell Server Deployment Pack to apply drivers from Lifecycle Controller. For more information, see Applying Drivers From Lifecycle Controller.
- Apply drivers from a ConfigMgr repository, for more information, see Dell Server Deployment Pack documentation available at **support.dell.com/manuals**.
- Create a task sequence boot media for the collection of systems with an Integrated Dell Remote Access Controller to boot to the task sequence ISO. For more information, see Creating a Task Sequence Media (Bootable ISO).

Workflow

1. From the ConfigMgr console, under **Computer Management→ Collections**, right-click on **Managed Dell Lifecycle Controllers (OS Unknown)** and select **Dell Lifecycle Controller Launch Config Utility**.
2. On 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.
4. Configure or edit the BIOS/NIC profiles. For more information, see Configuring Hardware During OS Deployment.
5. Configure or edit the RAID profiles. For more information, see Configuring RAID.
6. Apply NIC/CNA profiles to the collection. For more information, see Applying a NIC or CNA Profile on a Collection.

7. Apply Integrated Dell Remote Access Controller profiles to the collection. For more information, see Applying an Integrated Dell Remote Access Controller Profile on a Collection.
8. Deploy the operating system and boot the systems to the media of your choice. For more information see, step 10.

Exporting the Server Profile to Integrated Dell Remote Access Controller vFlash Card or a Network Share

You can backup the server profile as an image file for a single system or a collection of systems by exporting the server profile to an Integrated Dell Remote Access Controller vFlash media or to an external source or a network share.

Prerequisites

- Common Prerequisites.
- Target system with valid seven character service tag.
- Integrated Dell Remote Access Controller vFlash card:
  - Is installed as a license, enabled, and initialized.
  - Minimum free space of 384 MB is available.
- Network Share:
  - Permissions and firewall settings are provided for the Integrated Dell Remote Access Controller to communicate with the system that has the network share.
  - Minimum free space of 384 MB is available.
- Administrator privileges on the Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller or cancel System Services.

  For more information on resetting Integrated Dell Remote Access Controller or cancelling system services, See the *Dell Lifecycle Controller Remote Services User's Guide* available at **support.dell.com/manuals**.
- 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

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 or Configuration Utility.
2. Select the **Platform Restore** on the **System Viewer** Utility or the Config Utility.
3. For a single system, see Exporting the System Profile.
4. For a collection, see Exporting the System Profiles in a Collection.

Importing the Server Profile from an Integrated Dell Remote Access Controller vFlash Card or a Network Share

You can restore the backup of a system profile for a single system or a collection of systems from an Integrated Dell Remote Access Controller vFlash media or a network share using Dell Lifecycle Controller Integration for ConfigMgr.

Prerequisites

- Common Prerequisites.
- The service tag of the server is either blank or same as when the backup was taken.
- Integrated Dell Remote Access Controller vFlash card:
  - Is installed as a license, enabled and has the SRVCNF partition.
  - Minimum free space of 384 MB is available.
- If you are importing from an Integrated Dell Remote Access Controller vFlash media, 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 Integrated Dell Remote Access Controller and BIOS installed.

Before You Begin

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

- 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, 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 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 Integrated Dell Remote Access Controller or cancel System Services.

Workflow

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 or Configuration Utility.
2. Select the **Platform Restore** on the **System Viewer** Utility or the Config Utility.
3. For a single system, see Importing the System Profile.
4. For a collection, see Importing the System Profiles in a Collection.

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.

Prerequisites

- Common Prerequisites.
- Network Share:
  - Integrated Dell Remote Access Controller can access the network share.
  - Integrated Dell Remote Access Controller 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.

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

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 or Configuration Utility.
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.
4. For a collection, see Viewing and Exporting Lifecycle Controller Logs for a Collection.

Working With NIC/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.

Workflow

1. Launch the **System Viewer** Utility on the ConfigMgr console for a particular system. For more information, see System Viewer Utility.
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/CNA Profile.
   - Edit an existing profile — to edit an existing NIC/CNA profile. For more information, see Editing a NIC/CNA Profile.
   - 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.
4. Add an adapter to the profile or remove an adapter from the profile. For more information, see step 4 in Creating a NIC/CNA Profile.
5. Select the adapter on the grid and configure it. For more information, see Configuring Adapters.
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.
7. Save the NIC or CNA profile.

3

Using Dell Lifecycle Controller Integration

This chapter discusses the various operations that you can perform after you install Dell Lifecycle Controller Integration on Microsoft System Center Configuration Manager (ConfigMgr).

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

Dell Lifecycle Controller Integration for ConfigMgr enables you to perform the following operations on all Dell systems under the **All Dell Lifecycle Controller Servers** collection:

- Configure the target systems. For more information, see Configuring Target Systems.
- Apply drivers on the task sequence. For more information, see Applying Drivers on the Task Sequence.

  NOTE: Select the checkbox **Apply Drivers from Lifecycle Controller** 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).
- Use the **System Viewer** Utility on specific systems in a collection. For more information, see Configuration Utility.
- Use the Config Utility on a collection of Dell systems. For more information, see Configuration Utility.

- Launch the Integrated Dell Remote Access Controller console by right-clicking on any system discovered under **All Dell Lifecycle Controller Servers** on the ConfigMgr console, or any system on the Task Viewer. For more information, see Launching the Integrated Dell Remote Access Controller Console.
- Use the Task Viewer to view the status of tasks handled by Dell Lifecycle Controller Integration for ConfigMgr. For more information, see Task Viewer.

Configuring Target Systems

Dell Lifecycle Controller Integration for ConfigMgr supports only *yx1x* systems and later. For each system in the collection, enable **Collect System Inventory on Restart** (**CSIOR**) in the BIOS 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, in the *Dell Lifecycle Controller Integration Version 1.3 for Microsoft System Center Configuration Manager User's Guide*, see the section *Configuring Part Replacement Properties for a System*.

To enable CSIOR:

1. Re-start the system.
2. During Power-on Self Test (POST), when the system prompts you to enter the Integrated Dell Remote Access Controller 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**.

Auto-Discovery and Handshake

The auto-discovery and handshake feature enables the Integrated Dell Remote Access Controller 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 ConfigMgr with the new system. The Dell Lifecycle Controller Utility for ConfigMgr uses the provisioned account to communicate with the Integrated Dell Remote Access Controller of target systems, to invoke the enabled features.

After Dell Lifecycle Controller Integration for ConfigMgr discovers a system with Integrated Dell Remote Access Controller, it creates the **All Dell Lifecycle Controller Servers** collection under **Computer Management→ Collections** in the ConfigMgr console. 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: Dell Lifecycle Controller Integration for ConfigMgr does not support auto-discovery of modular systems with flex-addressing.

Applying Drivers on the Task Sequence

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

Applying Drivers From Lifecycle Controller

NOTE: If you edit the task sequence to which drivers are exposed from the Lifecycle Controller option checked, the errors in step 6 may 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.

To apply drivers from the Lifecycle Controller:

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.

To create a task sequence, see the *Dell Server Deployment Pack for Microsoft System Center Configuration Manager User's Guide* available available at **support.dell.com/manuals**.

To edit the task sequence:

a Right-click on the task sequence and select **Edit** to open the **Task Sequence Editor**.

b Click **Add→ Dell Deployment→ Apply Drivers from Lifecycle Controller** and click **Next**.

A message is displayed that lists objects referenced in the task sequence that are not found.

NOTE: This step requires a fallback step for the inclusion of either the **Apply Driver Package** or **Auto Apply Drivers** step of ConfigMgr. Ensure that you have one of these steps configured with a condition in the task sequence. For more information on configuring a condition for the fallback step, see Viewing the Condition for a Fallback Step.

c Click **OK** to close this message.

2 Select **Apply Operating System Images**.

3 Under the **Apply operating system from a captured image**, reselect and verify the image package and image.

4 Clear the **Use an unattended or sysprep answer file for a custom installation** checkbox.

5 Select **Apply Windows Settings**. Enter the licensing model, product key, administrator password, and time zone.

NOTE: The default option is to randomly generate the administrator password.This may not allow you to log in to the system if you do not map the system to a domain. Alternatively, you can select the **Enable the account and specify the local administrator password** option and enter an administrator password.

6 Select **Apply Drivers from Dell Lifecycle Controller** and select an operating system from the drop-down list.

7 Enter a user name and password with administrator credentials to access the ConfigMgr console.

8 Select **Apply Driver Package**. Click **Browse** and select a driver package from the list of driver packages available in ConfigMgr.

NOTE: Depending on the hardware and operating system being deployed, you may need to select a mass storage device to correctly deploy the operating system. For example, Microsoft Windows 2003 operating system does not carry compatible drivers for the Serial Attached SCSI (SAS) or PowerEdge Expandable RAID Controllers (PERC).

9 Click **OK** to close the **Task Sequence Editor**.

10 Advertise the task sequence that you have edited. For information on how to advertise a task sequence, see the *Dell Server Deployment Pack for Microsoft System Center Configuration Manager User's Guide* available at **support.dell.com/manuals**.

NOTE: It is required that you set the task sequence advertisement to mandatory.

NOTE: If multiple advertisements to the same collection are made mandatory, the choice of advertisement to run is up to the ConfigMgr.

11 Create a Lifecycle Controller Boot Media. For more information, see Creating a Lifecycle Controller Boot Media.

Applying Drivers From the ConfigMgr Repository

To apply drivers from the ConfigMgr repository:

1 Add a **Set Boot Order** step manually before each of the **Reboot to PXE** or **USB** steps. The **Set Boot Order** step instructs the systems to boot to a virtual CD on the next boot. For more information, see Adding a Set Boot Order Step.

2. Apply driver packages for the selected operating systems in ConfigMgr. For more information on applying driver packages, see *Dell Server Deployment Pack for Microsoft System Center Configuration Manager User's Guide* available at **support.dell.com/manuals**.

Adding a Set Boot Order Step

To add a **Set Boot Order** step manually:

1. Right-click on the task sequence and select **Add→ Dell Deployment→ PowerEdge Server Configuration**.
2. Select **Boot Order** from the **Configuration Action Type** drop-down list.
3. Select **Set** from the **Action** drop-down list.
4. A new drop-down list for **Configuration file / Command line parameters** appears. Select **— nextboot=virtualcd.slot.1**.
5. Click **Apply**. The name of the step changes to **Set Boot Order**.
6. Select and drag the **Set Boot Order** step to just before the **Reboot to PXE / USB** step.
7. Repeat this process to create a **Set Boot Order** step before each **Reboot to PXE / USB** step.
8. Click **OK** to close the task sequence.

Viewing the Condition for a Fallback Step

The condition **DriversNotAppliedFromLC** is automatically added by Dell Lifecycle Controller Integration for ConfigMgr while creating a task sequence. This condition is used as a fallback step if the application of drivers from Lifecycle Controller fails.

NOTE: It is recommended that you do not disable or delete this condition.

To view the condition for a fallback step:

1. On the ConfigMgr console, select **Computer Management→ Operating System Deployment→ Task Sequence**.
2. Right-click on the task sequence and click **Edit**. The **Task Sequence Editor** appears.
3. Select **Apply Driver Package** or **Auto Apply Drivers**.

4 Click the **Options** tab. You can view the **DriversNotAppliedFromLC** condition.

Creating a Task Sequence Media (Bootable ISO)

Dell Lifecycle Controller Integration for ConfigMgr does not depend on a Pre-execution Environment (PXE) to boot a collection of systems with an Integrated Dell Remote Access Controller to the task sequence ISO available on a Common Internet File System (CIFS) share. You must provide credentials to access this ISO on the CIFS share.

To create a task sequence ISO:

1 On the ConfigMgr console, under **Computer Management→ Operating System Deployment**, 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.

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. Click **Next**.

4 Clear the **Protect Media with a Password** checkbox and click **Next**.

5 Browse and select **Dell PowerEdge Server Deployment Boot Image**.

6 Select the distribution point from the drop-down menu, and select the **Show distribution points from child sites** checkbox.

7 Click **Next**. The **Summary** screen appears with the task sequence media information.

8 Click **Next**. The Progress bar is displayed.

9 On completion, click **Close** and eject the media.

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 ConfigMgr console. This utility works on a one-to-one relationship and you can perform the operations on target systems one at a time.

You must change the Integrated Dell Remote Access Controller credentials of the target system before you launch the **System Viewer** Utility to perform the various tasks.

To change the Integrated Dell Remote Access Controller credentials and launch the **System Viewer** Utility:

1. Under a collection, right-click on a Dell *yx1x* system and select **Dell Lifecycle Controller→ Launch System Viewer**.
2. The **iDRAC Authentication Information** screen displays the default credentials known to the ConfigMgr. Clear **Use Credentials Known to ConfigMgr (Default)** and do any 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 the valid credentials for Integrated Dell Remote Access Controller. You can provide credentials authenticated on the active directory.
   - **Skip CA check -** This option is selected by default, clear this option to secure communication between the ConfigMgr 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.

Configuration Utility

The Config 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 ConfigMgr 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 the various operations on all the target systems at one time.

To launch the Configuration Utility:

1. From the ConfigMgr console, under **Computer Management→ Collections**, right-click on **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, the left-hand pane lists the following options:

   - Overview
   - Create new 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

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

Launching the Integrated Dell Remote Access Controller Console

Dell Lifecycle Controller Integration for ConfigMgr enables you to launch the Integrated Dell Remote Access Controller console for any of the Dell systems from the ConfigMgr console, to view or modify the Integrated Dell Remote Access Controller configuration of the selected system.

After you install Dell Lifecycle Controller Integration for ConfigMgr, you can see the **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 Integrated Dell Remote Access Controller console for a system under the collection:

1. Select any system under **Collections → All Dell Lifecycle Controller Servers**.
2. Right-click on the system and select the **Dell Lifecycle Controller → Launch iDRAC Console** menu option. The Integrated Dell Remote Access Controller console of the system is launched on your default browser.
3. Provide the credentials to login to the Integrated Dell Remote Access Controller console and view or edit the details of the Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller 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. For more information on applying firmware updates, see Comparing and Updating Firmware Inventory for Systems in a Collection, or Comparing and Updating Firmware Inventory.

2. Select any system on the Task Viewer, right-click and select the **Launch iDRAC Console** menu option.
3. Provide the credentials to login to the Integrated Dell Remote Access Controller console and view or edit the details of the Integrated Dell Remote Access Controller 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 Dell Lifecycle Controller Integration for ConfigMgr. All long-running tasks such as operating system deployment, or applying firmware updates to systems are displayed in the Task Viewer. It 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.

Table 3-1 lists the actions that you can perform in the Task Viewer.

Table 3-1. Task Viewer Actions

Button	Action
Close	Click this to close the Task Viewer. When you close the Task Viewer, it cancels all the tasks that are running. Therefore, it is recommended not to close the Task Viewer when you have tasks that are still running.
Clear Completed	Click this to clear all the completed or failed tasks from the grid.
Export Queue	Click this to export the current state of the tasks in the Task Viewer to a .CSV file. You can use this file to view the summary of the total number of Dell Lifecycle Controller Integration tasks that are running.
View Log	Click this to view the log file that contains the details of the tasks that are running.
Send to Taskbar	Click this 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 Dell Lifecycle Controller Integration, you must:

- Validate a Dell factory-issued Client Certificate on Integrated Dell Remote Access Controller. For more information, see Validating a Dell Factory-Issued Client Certificate on the Integrated Dell Remote Access Controller for Auto-Discovery.
- Pre-authorize systems for auto-discovery. For more information, see Pre-authorizing Systems for Auto-Discovery.

- Change administrative credentials. For more information, see Changing the Administrative Credentials Used by Dell Lifecycle Controller Integration for ConfigMgr.

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

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 Integrated Dell Remote Access Controller. This feature is enabled by default. To disable the feature, run the following command:

```
[Program Files]\Dell\DPS\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:

```
[Program Files]\Dell\DPS\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:

```
[Program Files]\Dell\DPS\bin\import.exe
-CheckAuthorization false.
```

Changing the Administrative Credentials Used by Dell Lifecycle Controller Integration for ConfigMgr

Use the following commands to change the administrative credentials for ConfigMgr used by Dell Lifecycle Controller Integration:

To set the user name:

```
[Program Files]\Dell\DPS\Bin\import.exe –CIuserID
[New Console Integration Admin User ID]
```

To set the password:

```
[Program Files]\Dell\DPS\Bin\import.exe -CIpassword
[New Console Integration Admin Password].
```

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:

```
[Program Files]\Dell\DPS\Bin\import.exe -DisplayUI
```

Using Import.exe to Update Target System Information

If you have discovered systems with Dell Lifecycle Controller Integration for ConfigMgr version 1.0 or 1.1 and updated the firmware after upgrading to version 1.2 or later, then you must re-discover the systems if you have changed their hostname during operating system deployment.

To avoid re-discovering the systems and avail the hostname change functionality:

1. Launch the command prompt on the target system.
2. Navigate to *Program Files\Dell\DPS\Bin* folder.
3. Type the command: `import.exe -Servers.`

The ConfigMgr database is updated with the latest firmware information from the target systems. You can verify if the information of all the systems is correctly updated by viewing the **import.log** file in the *Program Files\Dell\DPS\Logs* folder.

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:

1. Launch the **Array Builder** by clicking **Create a RAID Profile** in the **RAID Configuration** screen in the **System Viewer** Utility.

   When you launch the **Array Builder** a default embedded controller is created.

2. Enter the configuration rule name in the **Configuration Rule Name** field.
3. Select the 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 cannot be configured 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) cannot be configured 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. Add new controllers and define rules for them, or edit the default controller and define the rules. For more information, see Controllers.
5. Add or edit variable conditions for the default controller or the controller that you add. For more information, see Variable Conditions.
6. Create new arrays from a variable condition, if required. For more information, see Arrays.
7. If you create an array, add additional disks, hot spares or global hot spares to the array.
8. 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.

About Creating Array Builder

When you use the RAID profile that you created using Array Builder as part of the operating system deployment of Dell Lifecycle Controller Integration for ConfigMgr, 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

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: There must be at least one controller present 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: Dell Lifecycle Controller Integration for ConfigMgr 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 is displayed that all the attached arrays and disks will be deleted.

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. Here 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 (also known as 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, ConfigMgr 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 ConfigMgr console to:

- Create a new Lifecycle Controller boot media to deploy operating systems remotely. For more information, see Creating a Lifecycle Controller Boot Media.
- 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.
- 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.

  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 **support.dell.com/manuals**.
- View the current hardware inventory for all the systems in the collection. For more information, see Viewing the Hardware Inventory.
- 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.
- Modify and set the Lifecycle Controller credentials on the targeted collection of Dell systems, For more information see, Modifying Credentials on Lifecycle Controllers.
- View and export the Lifecycle Controller logs for a collection. For more information, see Viewing and Exporting Lifecycle Controller Logs for a Collection.
- 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.

- Compare a NIC configuration profile against systems in a collection. For more information, see Comparing NIC/CNA Profiles Against Systems in a Collection.

NOTE: Dell Lifecycle Controller Integration performs all of the above 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 and so forth.

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. From the ConfigMgr console, under **Computer Management→ Collections**, right-click on **All Dell Lifecycle Controller Servers** and select **Dell Lifecycle Controller→ Launch Config Utility**.

   NOTE: Config Utility can be launched 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).
4. Specify the folder/path to save the Dell Lifecycle Controller boot media.

   NOTE: It is recommended to save the boot media to the local drive, and if required 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. From the ConfigMgr console, select **System Center Configuration Manager→ Site Database→ Site Management→** <*site server name*>→ **Site Settings→ Component Configuration**.

2 In the **Component Configuration** window, right-click **Out of Band Management** and select **Properties**. The **Out of Band Management Properties** window appears.

3 Click the **Dell Lifecycle Controller** tab.

4 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.

5 In the **Modify Share Information** window, enter a new share name and share path. 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 Integrated Dell Remote Access Controller.

This feature:

- Updates the firmware from a Dell repository.
- Makes changes to the hardware configuration.
- Enables you to apply a NIC or CNA profile to a set of target systems.
- Makes changes to the RAID configuration.
- Enables you to apply an Integrated Dell Remote Access Controller profile to a set of target systems.
- 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.

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 ConfigMgr 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 Integrated Dell Remote Access Controller. 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 newer, or on blade servers with Integrated Dell Remote Access Controller version 2.2 or newer.

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 **support.dell.com/manuals**.

Hardware Configuration and OS Deployment Workflow

To deploy the operating system to a collection:

1. From the ConfigMgr console, under **Computer Management→ Collections**, right-click on **Managed Dell Lifecycle Controllers (OS Unknown)** and select **Dell Lifecycle Controller→ Launch Config Utility**.
2. From the Dell Lifecycle Controller Configuration Utility, select **Deploy Operating System**.
3. 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. Click **Next**.
4. Select **Configure Hardware** if you want to make changes to the hardware settings. For more information, see Configuring Hardware During OS Deployment. Click **Next**.
5. Select **Configure RAID** to configure RAID on the servers. For more information, see Configuring RAID. Click **Next.**
6. 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. Click **Next**.
7. Select **Configure iDRAC** if you want to apply an Integrated Dell Remote Access Controller profile to the collection. For more information, see Applying an Integrated Dell Remote Access Controller Profile on a Collection.
8. Select **Do not deploy operating system** in the advertisement screen if you wish 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.

9. If you wish to deploy the operating system, select the advertisement to advertise the task sequence to the collection, and the operating system to be deployed on the collection.
10. Under **Select Lifecycle Controller bootable media**, select one of the following options:
    - **Boot to Network ISO** — Reboots to the ISO specified by you.
    - **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.
    - Select the **Use Network ISO as Fallback** checkbox 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.
11. Enter the user name and password for accessing the share where the Dell Lifecycle Controller bootable media is located.
12. Click **Reboot Targeted Collection**. This sends the reboot 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.

After a system with Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller using the iDRAC6 web-based interface. For more information, see the *Dell Lifecycle Controller Remote Services User's Guide* available at **support.dell.com/manuals.**

After the deployment is successful, the system with Integrated Dell Remote Access Controller moves to the **Managed Dell Lifecycle Controller (OS Deployed)** collection under **Computer Management→ Collections→ All Dell Lifecycle Controller Servers**.

NOTE: If you change the hostname 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 ConfigMgr console. You do not need to re-discover the system when you change the hostname.

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:
     - 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.

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 proceed 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 ConfigUtility, if you apply an attribute value, the dependent attributes' value is not checked.

Refer 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/CNA Profile.

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 Table 4-1:

Table 4-1. 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 Integrated Dell Remote Access Controller profile.

NOTE: If there is an error while applying a NIC/CNA profile, the OS Deployment process continues to the next step. While applying an attribute using ConfigUtility, it does not check the dependent attributes value.

Applying an Integrated Dell Remote Access Controller Profile on a Collection

To configure Integrated Dell Remote Access Controller and apply an Integrated Dell Remote Access Controller profile on a collection:

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

Table 4-2. Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller profile.
2.	Blade systems	All four types of attributes are configured.	• All attributes in Common IP settings. • All attributes in IPv4 settings. • 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.

Table 4-2. Integrated Dell Remote Access Controller Profile Settings *(continued)*

S.No	Target Server	Profile Settings	What is Applicable
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 Integrated Dell Remote Access Controller profile, the OS Deployment process stops.

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 **support.dell.com/manuals**.

To compare and update firmware inventory:

1. From the ConfigMgr console, under **System Center Configuration Manager→ Site Database→ Computer Management→ Collections**, right-click on **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 names 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 wish 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.

   Click **Finish** to complete the firmware update process.

Viewing the Hardware Inventory

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

To view the hardware inventory:

1 On the ConfigMgr console, right-click on **System Center Configuration Manager→ Site Database→ Computer Management→ Collections→ 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, Integrated Dell Remote Access Controller Card, and so on.

   – **FQDD**: displays the fully qualified device description of the hardware component.

   – **Description**: displays the properties of the hardware component.

NOTE: When the Config 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.

Verifying Communication With Lifecycle Controller

Use the following steps to verify the credentials of the discovered systems with Integrated Dell Remote Access Controller:

1. On the ConfigMgr console, right-click on **System Center Configuration Manager→ Site Database→ Computer Management→ Collections→ 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.

Modifying Credentials on Lifecycle Controllers

On systems with Integrated Dell Remote Access Controller, use the following steps to verify and/or modify the **WS-MAN** credentials configured with the Dell Lifecycle Controller Integration for ConfigMgr:

NOTE: It is recommended that you modify the credentials on the Lifecycle Controller as well as the ConfigMgr database simultaneously.

To modify the credentials on Lifecycle Controllers:

1. On the ConfigMgr console, right-click on **System Center Configuration Manager→ Site Database→ Computer Management→ Collections→ 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. Enter the current user name and password, and the new user name and password. You can provide user credentials authenticated on active directory.
   - **Skip CA check -** This option is selected by default, clear this option to secure communication between the ConfigMgr 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.
4. Click **Update**. A list of iDRACs that are discovered on the network appears along with their communication status.

   A series of **WS-MAN** commands are sent to all systems with Integrated Dell Remote Access Controller that are in the collection, to change the user name and password credentials, and to indicate the change.

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 ConfigMgr Database

To modify the credentials on the ConfigMgr database:

1. On the ConfigMgr console, select **System Center Configuration Manager→ Site Database→ Site Management→ <***site server name***>→ Site Settings→ Component Configuration**.
2. In the **Component Configuration** window, right-click **Out of Band Management** and select **Properties**. The **Out of Band Management Properties** window is displayed.
3. Click the **Dell Lifecycle Controller** tab.
4. Under **Local User Account on Lifecycle Controllers**, click **Modify**.
5. 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 ConfigMgr Database.

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. On the ConfigMgr console, right-click on **Computer ManagementCollections→ 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.

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.

Platform Restore for a Collection

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

- Export the system profiles in a collection. For more information, see Exporting the System Profiles in a Collection.
- Import the system profiles in a collection. For more information, see Importing the System Profiles in a Collection.
- Manage profiles for a collection.
- Configure Part Replacement properties for a collection. For more information, see Configuring Part Replacement Properties for a Collection.

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. On the ConfigMgr console, right-click on **Computer ManagementCollections→ 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 2 to step 6 as given in Exporting the System Profile.

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 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. On the ConfigMgr console, right-click on **Computer ManagementCollections→ 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.

   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.**

   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.

   A task is submitted to the Task Viewer. You can launch the Task Viewer to view the status of the tasks.

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.

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

1 On the ConfigMgr console, right-click on **Computer ManagementCollections→ 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.

Comparing NIC/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 On the ConfigMgr console, right-click on **Computer ManagementCollections→ 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/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 that got 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** — the personality that the target system originally had on that partition.
   - **Personality Applied** — the personality that was applied from the NIC/CNA profile to that partition.
   - **Min. Bandwidth** — the minimum bandwidth that the partition originally had.
   - **Min. Bandwidth Applied** — the minimum bandwidth that was applied to the partition.
   - **Max. Bandwidth** — the maximum bandwidth that the partition originally had.
   - **Max. Bandwidth Applied** — the maximum bandwidth that was 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 originally present on the system.
   - **Value Applied** — the attribute value that was 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 Dell Lifecycle Controller Integration for Microsoft System Center Configuration Manager. For information on installing Dell Lifecycle Controller Integration for ConfigMgr, see the *Installation Guide*.

The Import Server Utility enables you to:

- Import Dell servers that are not auto-discovered by Dell Lifecycle Controller Integration for ConfigMgr, but are already part of the ConfigMgr environment. After import, these servers are displayed under **All Dell Lifecycle Controller Servers→ Dell Imported Servers** and you can then use the Dell Lifecycle Controller Integration for ConfigMgr 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.

Importing Dell Servers

To import Dell Servers that are not auto-discovered by Dell Lifecycle Controller Integration for ConfigMgr:

1. On the ConfigMgr console, navigate to **Operating System Deployment→ Computer Associates.**
2. Right-click on **Computer Association** and select **Import Dell Servers** from the menu.
3. On the Import Dell Servers screen, select the **Import Dell Servers** option.
4. Select **Specify an iDRAC IP address range** and provide an IP address range. This is the range of Integrated Dell Remote Access Controller 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 these formats:

- 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

5 Click **Next**.

The Integrated Dell Remote Access Controller Authentication process verifies the Integrated Dell Remote Access Controller credentials you have provided when you install Dell Lifecycle Controller Integration for ConfigMgr against each of the Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller user you have specified is not present on the Integrated Dell Remote Access Controller of any of the servers you want to import, then the status is displayed as **Authentication failed**, and you cannot import that server.

6 Click **Save As** to save the report as a .CSV file in any location.

7 Click **Next** and select the servers that you want to import. By default all systems where the Authentication status was **Success,** are selected.

8 Specify the Target Collection under which you want the imported servers to be displayed and click **Next**.

The progress bar on the screen displays the progress of the server import process and the grid displays the status of the import process. If there are any errors while importing a server, then the **Failed** status is displayed.

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 ConfigMgr console, navigate to **Operating System Deployment→ Computer Associates.**

2 Right-click on **Computer Association** and select **Import Dell Servers** from the menu.

3 On the Import Dell Servers screen, select the **Import System Variables** option.

4 Click Browse to select the **.CSV** file that contains the variables.

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.

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.
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.**

The progress bar on the screen displays the progress of the variable import process and the grid displays the status of the import process. If there are any errors while importing a system variable, then the **Error** status is displayed.

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 Hardware Configuration.
- View and edit the RAID configuration. For more information, see Viewing and Configuring RAID.
- Create and edit Integrated Dell Remote Access Controller configuration profiles for your system. For more information, see Configuring Integrated Dell Remote Access Controller Profiles for a System.
- 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.
- View the current firmware inventory, compare it against a baseline, and update the firmware. For more information, see Comparing and Updating Firmware Inventory.
- Compare the hardware configuration profiles. For more information, see Comparing Hardware Configuration Profile.
- View and export the Lifecycle Controller logs. For more information, see Viewing Lifecycle Controller Logs.
- View the hardware inventory for the system. For more information, see Viewing the Hardware Inventory for the System.

  NOTE: You can only edit the hardware configuration and RAID configuration profiles directly, and not edit the system configurations directly.

- Perform tasks with respect to restoring 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.

Viewing and Editing Hardware Configuration

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

By default, the **System Viewer** Utility displays the **Hardware Configuration** screen. Select **Create New Profile** to create a new profile, or **Edit an Existing Profile** to edit an existing profile. The **BIOS Attributes** tab displays the BIOS attributes and current settings of the system. The **Boot Sequence** tab displays the system's boot sequence information.

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.

Creating a New Profile

To create a new profile:

1 In the **Hardware Configuration** screen, select **Create a New Profile** and click **Next**.

2 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.

3 In the **BIOS Attributes** tab, select the attributes to be included in your profile by selecting the checkbox 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.

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

Editing an Existing Profile

To edit an existing profile:

1 In the **Hardware 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**.

3. The **BIOS Attributes** tab displays the BIOS attributes of the selected profile. Select the attributes that you want to edit, and click **Edit Attribute**.
4. The **Custom Attribute Editor** displays all the attributes in the drop-down list against the **Attribute Name** field. 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 **Hardware 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 the **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, see step 2 to step 5 of Editing an Existing Profile.

Changing the BIOS Boot Sequence and Hard Disk Drive Sequence

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

1 In the **Hardware Configuration** screen, select **Create a New Profile** or **Edit an Existing Profile**, and click **Browse** to browse for the profile.

2 Click on the **Boot Sequence** tab. The current BIOS boot sequence and hard disk drive sequence is displayed.

3 Use the **Move Up** and **Move Down** buttons to change the BIOS boot sequence or the hard disk drive sequence.

4 Click **OK** to save the changes.

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

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 on **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 Integrated Dell Remote Access Controller Profiles for a System

This features enables you to define Integrated Dell Remote Access Controller configuration and save it as an Integrated Dell Remote Access Controller configuration profile, then apply to a collection as part of the workflow while deploying an operating system.

You can create or edit Integrated Dell Remote Access Controller profiles for a system with the **System Viewer** Utility.

Creating an Integrated Dell Remote Access Controller Profile

To create an Integrated Dell Remote Access Controller profile:

1. On the **System Viewer** Utility, click **iDRAC Configuration.** The Integrated Dell Remote Access Controller Configuration options are displayed.
2. Select **Create a New Profile** and click **Next**.

   The Integrated Dell Remote Access Controller configuration of the system is retrieved and displayed.
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 *Dell Lifecycle Controller Unified Server Configurator/Unified Server Configurator-Lifecycle Controller Enabled Version 1.5 User's Guide* available at **support.dell.com/manuals**.

5 Click the **Users** tab. The grid retrieves the list of Integrated Dell Remote Access Controller users from the system and displays them.

6 You can add a user account or edit an existing user account. Integrated Dell Remote Access Controller 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 Dell Lifecycle Controller Integration uses to access the Integrated Dell Remote Access Controller of the system.

7 Specify the following details:

- **General Details** — that includes 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 *Dell Lifecycle Controller Unified Server Configurator/Unified Server Configurator-Lifecycle Controller Enabled Version 1.5 User's Guide* available at **support.dell.com/manuals**.

8 Click **OK** to save the user account configuration and revert back 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 Integrated Dell Remote Access Controller profile:

1 On the **System Viewer** Utility, click **Integrated Dell Remote Access Controller Configuration.** The Integrated Dell Remote Access Controller Configuration options are displayed.

2 Select **Edit an Existing Profile.**

3 Click **Browse** and navigate to the location where you have saved the Integrated Dell Remote Access Controller configuration profile, and click **Next**.

The Integrated Dell Remote Access Controller configuration of the saved profile is retrieved and displayed.

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 above attributes, see the *Dell Lifecycle Controller Unified Server Configurator/Unified Server Configurator-Lifecycle Controller Enabled Version 1.5 User's Guide* available at **support.dell.com/manuals.**

5 Click the **Users** tab. The grid retrieves the list of Integrated Dell Remote Access Controller 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.

7 Click **Save As Profile** to save the modified Integrated Dell Remote Access Controller 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 **support.dell.com/manuals**.

For information on CNAs supported by Dell Lifecycle Controller Integration, see the *Dell Lifecycle Controller Integration Version 1.3 for Microsoft System Center Configuration Manager Readme* available at **support.dell.com/manuals**.

Creating a NIC/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.** The **Network Adapter Configuration** screen is displayed.
3. Click **Add** to add an adapter.
4. In the **Add Adapter** dialog box:
   a. Select the **Adapter type** from the drop-down list.
   b. Select the adapter location and specify the slot number.
   c. 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 the adapters before saving the profile.`

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 unchecked.

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.

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/CNA Profile.

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. Select the port that you want to configure and click **Configure**.
4. 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 yourself.
   - **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.
5. 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.
6. Click **Port Settings** to configure the NIC and iSCSI parameters. For more information, see Configuring NIC and iSCSI Parameters.
7. 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 this 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** — This option allows you 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** — This option allows you 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** — Specify the NIC link speed by selecting from the drop-down list.
   - **Flow Control** — Specify the data flow control by selecting from the drop-down list.
   - **IP auto configuration** — This option allows you to automatically configure the IP address for the system. You can choose to enable or disable this option.
   - **SRIOV configuration** — This option allows you 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 enter 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 via 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/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.

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/CNA Profile.

8 Click **Save as profile** to save the modified NIC 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:

   - **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 if the firmware of your system is compliant, or needs an update.

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 Integrated Dell Remote Access Controller 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**.

   Under **Select Profile to Compare**, click **Browse** and select any previously saved BIOS or Integrated Dell Remote Access Controller configuration profile to compare.

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 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.
3. The **Compare Hardware Configuration Profile** screen displays the following fields:
   - **Attribute Name** — lists the BIOS or Integrated Dell Remote Access Controller attributes depending on the profile you have selected.
   - **System Value** — lists the current value of the BIOS or Integrated Dell Remote Access Controller 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 6-1. 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 **support.dell.com/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 the Dell support site.
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 Dell Lifecycle Controller Integration for ConfigMgr.

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 fetch fresh Lifecycle Controller logs from the system, click **Refresh**.

5 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.

6 Click **Resume** to resume the loading of logs.

7 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 Latest Message Registry

It is recommended that you close all the Dell Lifecycle Controller Integration utilities such as the **System Viewer** Utility, Config Utility, and Task Viewer before you download and extract the message registry.

To download the latest Message Registry on the system where you have installed Dell Lifecycle Controller Integration for ConfigMgr:

1. Go to the Dell Support Website available at **support.dell.com/manuals**.
2. Select **Software**→ **Systems Management**→ **Dell Unified Server Configurator and Lifecycle Controller**.
3. On the **Lifecycle Controller Releases** page, click the link to the latest version of Lifecycle Controller.
4. On the **Lifecycle Controller** page, click the **Error Messages and Troubleshooting List** link under **Remote Services - One-to-many-Server Management**.
5. Click **English** and on the **Error Messages and Troubleshooting List** page, click the **Download** link.
6. Extract the **emsgs_en.zip** file to an empty folder.
7. 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**.
8. 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.

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.

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.
- Import a system profile. For more information, see Importing the System Profile.
- Manage profiles.
- Configure Part Replacement properties for a system. For more information, see Configuring Part Replacement Properties for a System.

Prerequisites to Export or Import a System Profile

You must upgrade the firmware to the following versions:

- Integrated Dell Remote Access Controller Firmware for blade systems to version 3.30 or higher.
- Integrated Dell Remote Access Controller Firmware for rack and tower systems to version 1.80 or higher.
- Lifecycle controller firmware to version 1.5.1.0 or higher.

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

Exporting the System Profile

You can create a backup of the firmware and configuration and export it to an Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller firmware and configuration.

To export the system profile:

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

  The utility checks for a valid license of the Dell vFlash SD card on the Lifecycle Controller of the system, 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:** to take the back up on the Integrated Dell Remote Access Controller vFlash Card.

  – **Network share:** to take the back 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 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 Click **Next**. A summary screen is displayed.

6 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 Integrated Dell Remote Access Controller 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 have 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.
4. Click **Next**. Enter the backup file passphrase that you had specified when you took the backup.

   If you have used a network share to save the backup file, specify the backup file prefix that you had specified when you took the 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:** to retain the existing RAID controller configuration.
   - **Delete:** to delete the existing RAID controller configuration and import the configuration from the backup file.

   NOTE: This 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 Dell Lifecycle Controller Integration. 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**.

The utility checks for a valid license of the Dell vFlash SD card on the Lifecycle Controller of the system. 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 given in the table below:

Table 6-2. Part Replacement Attributes

Property	Options
Collect System Inventory on Start (CSIOR)	• **Disabled**: Select this option to disable CSIOR for the replaced part. • **Enable**: Select this option to enable CSIOR for the replaced part. • **Do Not Change**: Select this option to leave the default settings as is. This is selected by default.

Table 6-2. Part Replacement Attributes *(continued)*

Property	Options
Part Firmware Update	• **Disabled:** Select this option if you do not want firmware updates to the replaced part. • **Allow version upgrade only:** Select this option to perform firmware update on replaced parts if the firmware version of the new part is lower than the original part. • **Match firmware of replaced part:** Select this option to perform firmware update on replaced parts to the version of the original part. • **Do Not Change:** Select this option to leave the default settings as is. This is selected by default.
Part Configuration Update	• **Disabled:** Select this option if you do not want to apply the current configuration to a replaced part. • **Apply Always:** Select this option to apply the current configuration to the replaced part. • **Apply only if firmware matches**: Select this option to apply the current configuration only if the current firmware matches with the firmware of the replaced part. • **Do Not Change:** Select this option to leave the default settings as is. This is selected by default.

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.

7

Troubleshooting

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 6.0

To configure Dell provisioning web services for IIS 6.0:

1 After installing Dell Lifecycle Controller Integration for ConfigMgr, go to **C:\Program Files\Dell\DPS\ProvisionWS** directory and verify that the folder **ProvisionWS** is present along with the files. Reinstall Dell Lifecycle Controller Integration for ConfigMgr if the folder and files are not present.

2 In **IIS Manager**, create a new application pool called **Provisioning Web Site** and assign it to the website.

   To assign the application pool to the Provisioning Web Site:

   a In **IIS Manager**, right-click **Provisioning Web Site**, and select **Properties**.

   b Click the **Home Directory** tab.

   c Under **Application Pool**, select **Provisioning Web Site**.

3 In **IIS Manager**, right-click **Provisioning Web Site**, select **Properties**, and click on the **Documents** tab. Set the default document to **handshake.asmx** and remove any other default documents.

4 Using the Certificate's 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 To enforce SSL and client certificates for the website:

   a Assign the **DellProvisioningServer** certificate to the website.

   b Set the SSL port to 4433.

   c Select the required SSL option.

   d Select the required client certificates option.

   e Create a **Certificate Trust List** with only the **iDRAC RootCA** in the trust list.

NOTE: The certificate files (**SITE_PFX_PASSWORD = "fW7kd2G"**) are present at the following location after running the installer: **[ConfigMgrPath]\AdminUI\XmlStorage\Extensions\bin\Deployment\Dell\PowerEdge\LC\IISsetup.**

Dell Provisioning Web Services Configuration for IIS 7.0 or IIS 7.5

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

1 On a ConfigMgr console installed with Dell Server Deployment Pack, launch the **Dell_Lifecycle_Controller_Integration_1.1.0.msi** and select the default values. A new virtual website called **Provisioning Web Site** is created.

2 Create a new application pool called **Provisioning Web Site** and assign it to the website.

3 Perform the following steps on the **Provisioning Web Site**.

   a If your system is running on a 64-bit operating system, set **Enable 32 Bit Applications** to **True**.

   b Set **Managed Pipeline Mode** to **Integrated**.

   c Set **Identity** to **Network Service**.

4 On the website, set the default document to **handshake.asmx** and remove any other default documents.

5 Using the Certificates MMC plug-in, install the **PS2.pfx** certificate into the system's **Personal** store.

6 Install the **RootCA.pem** into the system's **Trusted Root Certificate Authorities** store.

7 Import the **ProvisioningCTL.stl Certificate Trust List** file to **Intermediate Certificate Authorities**.

8 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"
```

9 To enforce SSL and client certificates for the website:

   a Add a 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.

   b Click **OK**.

   c Remove the HTTP binding for port 4431.

   d Select the required SSL option.

   e Select the required client certificates option.

   f 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**.

Upgrade or Repair Issues

If you have upgraded or repaired the Dell Server Deployment Pack after installing Dell Lifecycle Controller Integration for ConfigMgr 1.2 or later:

1. Copy the **CustomReboot.vbs** from **[ConfigMgrRoot]\AdminUI\XmlStorage\Extensions\Bin\Deployment\Dell\PowerEdge\LC\** to **[ConfigMgrRoot]\OSD\Lib\Packages\Deployment\Dell\PowerEdge\CustomReboot\.** Override the file in the destination folder.
2. Copy the **DellPowerEdgeDeployment.xml** from **[ConfigMgrRoot]\AdminUI\XmlStorage\Extensions\Bin\Deployment\Dell\PowerEdge\LC\** to **[ConfigMgrRoot]\AdminUI\XmlStorage\Extensions\Bin\Deployment\Dell\PowerEdge\**. Override the file in the destination folder.

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 could 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:

1. 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.

2. Lifecycle Controller cannot access the given CIFS share.

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

3. The Site Server cannot access the given CIFS share.

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

4. The given CIFS share is read-only share.

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

5. The exported **.XML** file is not well formed.

Resolution: For more information, see the *Dell Lifecycle Controller User's Guide* available at **support.dell.com/manuals**.

6 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 an Lifecycle Controller wipe through Unified Server Configurator, reinstall Unified Server Configurator, and re-generate the Lifecycle Controller Logs.

Issues and Resolutions

- *Issue*: When you deploy an operating system on a target system with Integrated Dell Remote Access Controller 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*: 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:

  a 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.

  b Power off the system and wait for ten minutes for it to show up in the collection.

- *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*: If the Integrated Dell Remote Access Controller 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 Integrated Dell Remote Access Controller version 1.3 firmware or newer. On a blade server, ensure that it has Integrated Dell Remote Access Controller version 2.2 or newer.

- *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*: While deploying Microsoft Windows 2008 R2 from ConfigMgr 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 2008 R2. Ensure that the task sequence deploying Microsoft Windows 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*: 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*: 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 Integrated Dell Remote Access Controller of your system is not in POST state.

- *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 Integrated Dell Remote Access Controller GUI.

- *Issue*: When you deploy Microsoft Windows Server 2003 operating systems and you select the **Apply Drivers from Lifecycle Controller** option, a blue screen is displayed or the deployment fails.

  Resolution: To resolve this issue:

  a Right-click the task sequence and click **Edit**. The **Task Sequence Editor** window appears.

  b Select **Add→ Drivers→ Apply Driver Package**.

  c Check the mass storage driver option.

  d Select the applicable SAS or PERC driver.

  e Select the model of the SAS or PERC driver.

  f Save the task sequence and re-deploy the operating system.

- *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 ConfigMgr 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*: 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 ConfigMgr does not have permissions to create collections. For more information on setting permissions, see Dell Auto-Discovery Network Setup Specification.

- *Issue*: When an account is cloned from an existing account in ConfigMgr, 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*: Installation fails while installing Dell Lifecycle Controller Integration for ConfigMgr 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 Dell Lifecycle Controller Integration for ConfigMgr version 1.3. Alternatively, you can install Dell Lifecycle Controller Integration for ConfigMgr though 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*: The **Advertise** option does not appear in an existing task sequence after uninstalling and reinstalling Dell Lifecycle Controller Integration for ConfigMgr.

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

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

  a Right-click the task sequence and select **Edit**.

  b Select **Restart in Windows PE**. In the **Description** section, type any character and delete it so the change isn't saved.

  c Click **OK**. This re-enables the **Apply** option.

- *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*: 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:* 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:* If you have discovered systems with Dell Lifecycle Controller Integration for ConfigMgr 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 Integrated Dell Remote Access Controller on the target systems
  to version 1.5 or later for monolithic systems and version 3.02 or later for modular systems.

- *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*: 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:* 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.

8

Related Documentation and Resources

For more information on ConfigMgr 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 **support.dell.com/manuals**. On the **Manuals** page, click **Software→ Systems Management**. Click the appropriate product link on the right-side to access the documents:

- *Dell Server Deployment Pack for Microsoft System Center Configuration Manager User's Guide*
- *Dell Lifecycle Controller User's Guide*
- *Integrated Dell Remote Access Controller 6 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*

Obtaining Technical Support

For assistance and information about Dell Lifecycle Controller Integration for ConfigMgr, see **support.dell.com**.

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.

Index