Dell Lifecycle Controller Remote Services (LC RS) Version 2.00.00.00 For 13th Generation Dell PowerEdge Servers
Quick Start Guide

Notes, Cautions, and Warnings

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

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

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

Contents

Introduction

The Dell Lifecycle Controller provides advanced embedded systems management. It includes a 1GB–managed and persistent storage that embeds systems management features in addition to the iDRAC features.

The Dell Lifecycle Controller Remote Services further enables remote systems management in a one-to-many method. Remote services is accessible over the network using the secure web services interface and can be programmatically utilized by applications and scripts. Remote services enable management consoles to perform one-to-many bare-metal server provisioning. The combination of the Auto-discovery feature to identify and authenticate the attached Dell system to the network and integration with one-to-many management consoles reduces the manual steps required for server setup and management. The Server Configuration Profiles provide a single view of all the system settings that can be imported and exported from the server to perform one-to-many cloning operations. The interface is aimed at simplifying many tasks, some of which include remotely deploying an operating system, remote update and inventory, and remotely automating the setup and configuration of new and already-deployed Dell systems.

Lifecycle Controller reduces the time and number of steps taken to accomplish tasks, reduces potential for error, enhances server and application uptime and security, and results in more efficient IT management. Developed on the industry standard Unified Extensible Firmware Interface (UEFI) platform and Web Services for Management (WSMAN) interfaces, Lifecycle Controller provides an open environment for console integration that also allows custom scripting for Lifecycle Controller. Leading systems management consoles such as, Microsoft System Center Configuration Manager, BMC Software BladeLogic Operations Manager, Symantec Deployment Solution, and Dell Management Console have integrated Dell Lifecycle Controller to utilize its features and capabilities to an existing infrastructure, where these consoles are installed.

Benefits of using iDRAC with Lifecycle Controller

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

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

The benefits include:

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

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

Key features

You can perform the following systems management tasks using Lifecycle Controller-Remote Services:

- Install operating systems and drivers
- Manage licensing
- Perform BIOS firmware updates
- Part Replacement and automatic restore of server configuration
- Perform component firmware updates
- Get hardware inventory information
- Get and set NIC/CNA and RAID configuration
- Get and set BIOS configuration and BIOS passwords
- Full export of Lifecycle log and add work notes
- Export current- and factory-shipped hardware inventory log
- Manage, attach, and boot to vFlash SD card partitions
- Lock the controllers using the local key
- Export and import the server profile
- Import server license
- View firmware details during server update
- Export and import Server Configuration Profiles
- Schedule and track the status of the update and configuration
- Import and export Server Configuration Profiles file that contains information about a component configuration
- Backplane and enclosure firmware update
- Faster iDRAC firmware update
- Shutdown job type
- Support for Fibre Channel (FC) HBA cards
- Monitor out-of-band performance
- Enhance security using hash password
- View logs, monitoring, and server information, and configure the network parameters of a server using a mobile device
- Delete server-related information

- View the managed system using Physical Computer System View
- Manage the web server certificate
- Configure the USB management port
- View embedded tech support report to resolve business-critical issues
- Configure storage devices in real time
- Replace motherboard using Import Server Profile feature
- Support for PCIeSSD devices

What's new in this release?

The highlights of this release of Lifecycle Controller-Remote Services are:

- Monitor the out-of-band performance
- Advance security using hash password
- Delete server-related information
- View the managed system using Physical Computer System View
- Manage web server certificate
- Support Near Field Communication (NFC) using QuickSync feature
- Configure USB management port
- View embedded tech support report to resolve business-critical issues
- Support for PCIeSSD devices
- Configure storage devices in real time
- Support for 12GBps SAS HBAs and PERC 9.1 controllers
- Update iDRAC and Lifecycle Controller firmware using a single firmware image

Why use Lifecycle Controller Remote Services?

When Dell examined the most common management tasks and the inefficiencies associated with them, it discovered that the additional time taken for performing management tasks was not because of the tools, but it was because of how the functions were split between several tools. For example, the most common tasks such as provisioning, deploying, and updating required not only multiple tools and multiple media format, but also searching the Web for tools such as drivers and firmware. This traditional delivery model resulted in inefficient use of time, potential errors, and possible security risks. Lifecycle Controller-Remote Services addresses all these system management issues.

Licensable features in Lifecycle Controller

The Web Services-Management (WS-MAN) License and Privilege Specification encompasses all the license and privilege information required to utilize the WSMAN API provided by the integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller.

It was delivered as part of the iDRAC (Express and Enterprise licenses, and vFlash SD card feature) starting with the 11th generation of Dell PowerEdge servers. On 12th and 13th generation of PowerEdge servers, the vFlash feature is included with the iDRAC Enterprise license, so you need not separately license vFlash with Lifecycle Controller 2.0 and later. The 12th and 13th generation of PowerEdge servers of Dell use only Express or Enterprise licensing.

The Lifecycle Controller management capabilities are partitioned into distinct areas and represented by the Dell Common Information Model (DCIM) profile specifications that provide comprehensive details

about each manageability feature or capability. These features may be free, partially licensed, or fully licensed. Also, the accessibility of a feature is defined by the credentials provided with the WS-MAN request and maps to the user-assigned privilege credentials, such as administrator- or read-only access.

What is the Web Service API?

Web Services-Management (WS-MAN) is a Distributed Management Task Force (DMTF) open standard, defining a Simple Object Access Protocol (SOAP) — based protocol for managing servers, devices, applications, and various web services. WS-MAN provides a common way for systems to access and exchange management information across the IT infrastructure.

DMTF is an industry organization that develops, maintains, and promotes standards for systems management in enterprise IT environments. The DMTF data model is complex and typically requires multiple transactions to accomplish simple operations such as specifying a user name and password, or giving administrator privileges to a user account. To reduce the number of transactions, Lifecycle Controller also offers a Dell data model for management that is based on an attribute model.

Where can the Lifecycle Controller API be used from?

Lifecycle Controller-Remote Services is a standards-based interface that enables consoles to integrate, for example, bare-metal provisioning and one-to-many operating system deployments for remotely located servers. Dell's Lifecycle Controller takes advantage of the capabilities of both Lifecycle Controller GUI and Lifecycle Controller-Remote Services to deliver significant improvement and simplification of
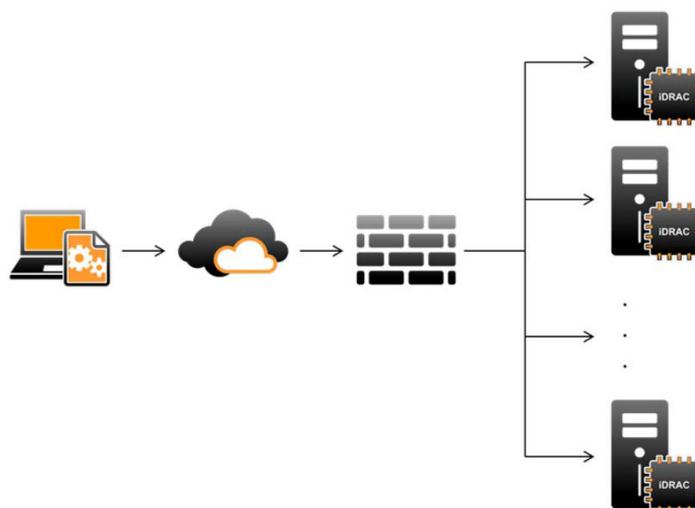
server deployment.

Lifecycle controller also supports local one-to-one system management tasks through a graphical user interface (GUI) using the server's KVM or the **Virtual Console** in iDRAC for operating system installation, updates, configuration, and for running diagnostics on single and local servers. This eliminates the need for multiple option ROMs for hardware configuration. For more information, see *Lifecycle Controller*

User's Guide, available at **delltechcenter.com/lc**.
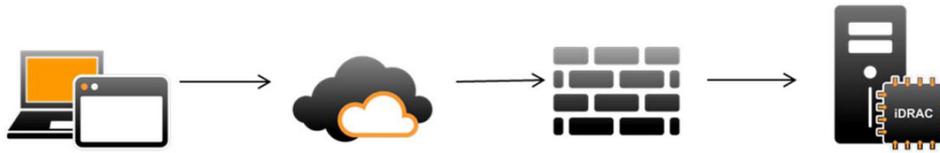
Who can use the API?

Lifecycle Controller-Remote Services features are available based on the type of license (that is, Basic Management, iDRAC Express, iDRAC Express for Blades, or iDRAC Enterprise) you purchase. Only licensed features are available in the iDRAC web interface and Lifecycle Controller-Remote Services. For more information about managing licenses, see *iDRAC User's Guide*. For more information about Lifecycle Controller-Remote Services licensing, see Licensing.

> NOTE: Special characters can be used in user name and password. However, they must be percent-encoded. For example, @ should be entered as %40.

How is one-to-many management achieved?

A management station sends WS-MAN commands over a network and the WS-MAN commands pass securely through the network from outside the firewall and maintain security.
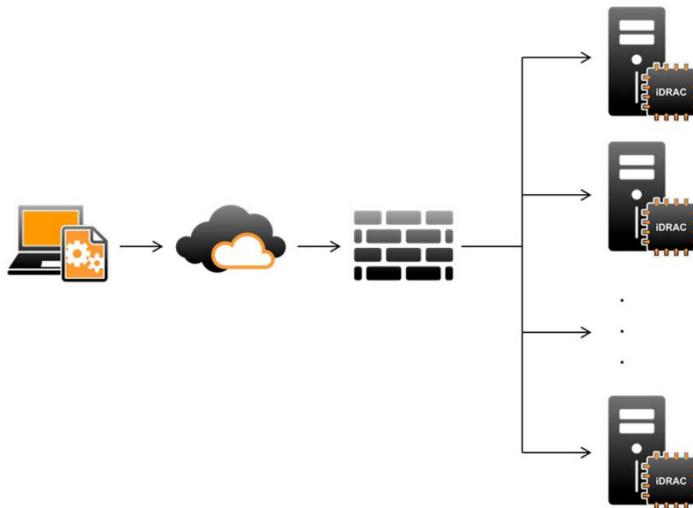
Other documents you may need

Along with this Quick Start Guide, you can access the following guides.

- The *Lifecycle Controller Online Help* provides information about using the Lifecycle Controller through the graphical user interface (GUI). To access the Online Help, click **Help** in the upper-right corner of Lifecycle Controller GUI or press <F1>.
- The *Dell Lifecycle Controller GUI User's Guide* provides information about using the Lifecycle Controller features using the GUI.
- The WS-MAN profile documents available at Dell TechCenter (**delltechcenter.com/lc**) provides detailed information about the WS-Man commands used to perform Lifecycle Controller related tasks.

- The *Lifecycle Controller Release Notes* provides last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- The *iDRAC User's Guide* available at Dell TechCenter (**delltechcenter.com/iDRAC)** provides information about using iDRAC web interface and RACADM.

Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:

  - For all Systems Management documents — **dell.com/softwaresecuritymanuals**
  - For Remote Enterprise Systems Management documents — **dell.com/esmmanuals**
  - For Enterprise Systems Management documents — **dell.com/openmanagemanuals**
  - For Client Systems Management documents — **dell.com/clientsystemsmanagement**
  - For Serviceability Tools documents — **dell.com/serviceabilitytools**
  - For OpenManage Connections Enterprise Systems Management documents — **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - For OpenManage Connections Client Systems Management documents — **dell.com/connectionsclientsystemsmanagement**
- From the Dell Support site:

  a. Go to **dell.com/support/manuals**.

  b. Under **General support** section, click **Software & Security**.

  c. In the **Software & Security** group box, click the required link from the following:
     - **Serviceability Tools**
     - **Enterprise Systems Management**
     - **Client Systems Management**
     - **Remote Enterprise Systems Management**
     - **Connections Client Systems Management**

  d. To view a document, click the required product version.
- Using search engines:

  - Type the name and version of the document in the search box.

Contacting Dell

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

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

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

2

Remote Services Features

Using Lifecycle Controller-Remote Services, you can perform the following operations:

- Deploy and Configure
- Monitor
- Maintain
- Create and schedule jobs

Deployment and configuration

Using various Lifecycle Controller-Remote Services' capabilities, you can perform different configurations on a system throughout its lifecycle. You can perform operations such as BIOS, iDRAC, RAID, and NIC configurations, and operating system deployment on the system.

Server configuration profiles

The server configuration profiles file contains the component configuration information that is used to apply the configuration for BIOS, iDRAC, RAID, NIC, FC-HBA, System, and Lifecycle Controller by importing the file to a target system. For more information and white papers, see *Server Cloning with Server Configuration Profiles* and *Creating and Managing Server Configuration Profiles* documents available at **delltechcenter.com/iDRAC** and **en.community.dell.com/techcenter/systems-management/w/wiki/1906.aspx**.

BIOS configuration

The BIOS and boot configuration feature gets and sets any of the configurable BIOS attributes that are exposed in BIOS UEFI HII. You can perform the following operations:

- Retrieve current configuration of BIOS inventory
- Retrieve current boot configuration settings
- Manage the boot order configuration
- Change the BIOS boot mode or UEFI boot mode
- Manage BIOS Passwords
- Change the boot order
- Enable or disable boot sources

iDRAC configuration

The iDRAC configuration feature is used to manage the properties and interfaces for running system management tasks related to the management of basic properties of iDRAC. The remote access controller properties and attributes are divided into views to provide a simple methodology for the clients to query the iDRAC views and set the iDRAC attributes.

You can perform the following operations:

- Retrieve current card configuration and iDRAC inventory
- Get and set any configurable iDRAC attribute
- Manage iDRAC user accounts

RAID configuration

The RAID configuration feature is used to manage the properties and capabilities of the RAID storage. The RAID storage is modeled using a collection of attributes, where there are collections for the enclosures, storage adapters, logical disks, physical disk drives, and PCIeSSD devices. Additionally, there is a configuration service that contains all the methods used to configure the RAID storage.

You can perform the following operations:

- Retrieve current configuration of RAID inventory.
- Delete all virtual disks and unassign all the hot spare physical disk drives.
- Prepare any foreign physical disk drives for inclusion in the local configuration.
- Manage hot spares.
- Manage keys for self-encrypting drives.
- Manage virtual disks. You can perform the following:

  - Create a single virtual disk. After the virtual disk is created, the FQDD of the virtual disk changes.
  - Initialize (fast or slow) the virtual disk using the physical disk drives attached to the PERC controller.
  - Delete a virtual disk from the PERC controller.

- Configure the following RAID attributes:

  - Virtual disks — Read Policy, Write Policy, and Disk Cache Policy
  - Controllers — Background Initialization Rate, Check Consistency Mode, Check Consistency Rate, Copy Back Mode, Possible load balance modes, Patrol Read Mode, Rebuild Rate, and Reconstruction Rate.

- Change RAID-ready states of the physical disk drives.
- View PCIeSSD and extended card information.
- Reset PERC controller configuration.
- Import foreign configurations such that virtual disks are not lost after moving physical disks. The controllers provide support for auto import of foreign configuration.
- Clear foreign configuration on physical disk drives attached to a controller.
- Set patrol read mode to avoid disk failures and data loss or corruption.
- Assign or unassign a global hot spare for a physical disk drive.
- Check the consistency of the redundancy information for redundant virtual disks.
- Cancel the check consistency operation that is in progress on a virtual disk.
- Blink or unblink the LEDs on the physical disk drives included in the virtual disk.
- Create, change, or delete the security key using the Local Key Management (LKM) feature on controllers that support encryption of the drives.

For more information on RAID configuration, see the *SimpleRaid* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**. Also, see the *iDRAC User's Guide* available at **dell.com/esmmanuals**.

NIC configuration

Network Interface Controller (NIC) configuration feature is used to set up or modify configuration settings for supported NIC cards (for example, Intel, QLogic, and Broadcom). These configuration settings can be set or updated both locally and remotely using Lifecycle Controller-Remote Services.

The NICs supported by Lifecycle Controller provide an array of networking features converged into a single controller:

- Traditional NIC capabilities
- Internet Small Computer System Interface over Ethernet (iSCSI) capabilities
- Fibre Channel over Ethernet (FCoE) capabilities

You can configure various device capabilities such as:

- Personalities (FCoE, ISOE, Layer 2 NIC)
- NIC partition bandwidth allocation
- Boot versus Offload
- I/O Identity

Operating system deployment

The operating system deployment feature is used to remotely deploy and manage an operating system using WSMAN web services protocols that use CIFS and NFS network file sharing protocols. Remote activation of locally exposed embedded drivers such as a USB drive eliminates the need for physical media.

📝 **NOTE:** By default the drivers are available with iDRAC and Lifecycle Controller for all the Dell supported operating systems.

You can perform the following operations:

- Get installed driver pack version and list of supported operating systems.
- Remote activation of locally exposed embedded drivers for the selected operating system as an emulated USB device to the server that is automatically installed during installation.
- Remote acquisition of embedded drivers for the selected operating system to a CIFS or NFS network share that can be used later for operating system deployment.
- Boot to an ISO image on a CIFS or NFS network share to initiate an operating system installation.
- Download ISO to vFlash SD card and boot from the card to initiate an operating system installation.
- Connect an ISO from CIFS or NFS network share, attaching it as virtual USB CD-ROM device to the server, and booting the server to the ISO, every time the server restarts.
- One time boot to PXE.
- One time boot to hard disk.
- Get the list of MAC addresses of all the NICs present on the server.
- Deploy operating system on iSCSI and FCoE LUN.

Near Field Communication (NFC) using the QuickSync feature

Using the QuickSync feature, you can:

- View basic server information such as Service Tag, MAC address, NIC data, firmware versions, operating system, and so on.
- View log and monitoring information of a server.
- Configure network parameters of a server.

After viewing or editing the information, you can troubleshoot or configure using a mobile device. To use this feature, you must install the OpenManage Mobile (OMM) software application on your mobile device and enable the bezel on the server. The QuickSync feature enables your mobile device to act as a proximity reader which reads data on the server when held at a distance of less than 20 mm from the server front panel. You can perform most of the tasks that you complete by using an LCD panel. The system information is the basic hardware inventory information retrieved from NFC. The attributes allow you to set the access, check the presence of QuickSync feature, enable or disable the Inactivity Timer, set the inactivity timeout value.

> **NOTE:** This feature is supported on the mobile devices with Android, iOS, Windows, or Java platforms.

For more information on the QuickSync feature, see the *System QuickSync* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**. Also, see *iDRAC User's Guide* available at **dell.com/esmmanuals**.

Configuring advance security using hash password

You can set user passwords and BIOS passwords using a one-way hash format in iDRAC available on the 13th generation Dell PowerEdge servers. The user authentication mechanism is not affected (except for SNMPv3 and IPMI) and you can provide the password in plain text format.

With the new password hash feature, you can:

- Generate your own SHA256 hashes to set iDRAC user passwords and BIOS passwords. New attributes for a Class type assist to generate the hash password. When you provide the SHA256 password values, you cannot authenticate through SNMP v3 and IPMI.
- Export the Server Configuration Profiles file with the password that has the hash values. To do this, use the ExportSystemConfiguration method and include the password hash values that should be exported to the IncludeInExport parameter.

The hash password can be generated with and without Salt using SHA256. If the salt string is used or null, it should always be set along with the SHA256SystemPassword.

> **NOTE:** If the iDRAC user account's password is set with the SHA256 password hash (SHA256Password) only and not the other hashes (SHA1v3Key, MD5v3Key), authentication through SNMPv3 is lost. Authentication through IPMI is always lost when hash is used to set the user account's password.

For more information on using hash password, see the *iDRAC Card* and *BIOS and BootManagement* profile documents available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**.

Configuring USB management port

On the 13th generation of PowerEdge servers monitored by iDRAC, you can perform the following functions on a USB port and USB drive:

- Manage the status of the server's USB port. If the status is disabled, iDRAC does not process a USB device or host connected to the managed USB port.
- Configure the USB Management Port Mode to determine whether the USB port is used by iDRAC or the operating system.
- View the overcurrent alert generated when a device exceeds the power requirement permitted by USB specification. Configure the overcurrent alert to generate the WS-Events.
- View the inventory of the USB device such as FQDD, device description, protocol, vendor ID, product ID, and so on, when the device is connected.
- Configure a server by using files stored on a USB drive that is inserted in to a USB port, which is monitored by an iDRAC. This configuration allows creation of a job to track progress and logging the results in the Lifecycle log.

NOTE: The USB configuration setting controls whether the configuration of the system is allowed from a USB drive.

For more information about the USB device management, see the *USB device profile* document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**.

Monitor

Using various Lifecycle Controller-Remote Services capabilities, you can monitor a system throughout its lifecycle. Current and factory-shipped hardware inventory, Lifecycle Log, System Event Log, Firmware Inventory are some of the features that help you monitor the system.

Hardware inventory

The hardware inventory information is cached on the persistent storage of Lifecycle Controller and is available to iDRAC and UEFI applications. It is used to export the hardware inventory from Lifecycle Controller to a text file on a remote share.

You can remotely query the inventory of hardware components. Each hardware inventory class contains important attributes about the hardware components.

For example, the `LastSystemInventoryTime` attribute identifies the last time a Collect System Inventory on Restart (CSIOR) was run. It is an important attribute as it indicates how recently the inventory was updated.

Hardware inventory and configuration information is available for the following components:

- Power Supply Unit
- Fan
- Memory
- CPU
- iDRAC
- PCI Device
- Video Card
- vFlash SD Card
- NIC
- RAID

- BIOS
- System
- Sensor

Lifecycle log

Lifecycle logs contain entries for configuration and firmware updates of BIOS, Storage Controllers, LOMs, and add-in NIC cards, if supported. The Lifecycle log can be exported to a network share or saved to a USB drive. The Lifecycle Log is accessible through the iDRAC web interface, RACADM, and WS-MAN interface.

The Lifecycle log provides the following information:

- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Error message IDs

For more information about Event and Error Messages, see the *Dell Event Message Reference Guide* available at **dell.com/support/home**.

System event log

The Lifecycle Log contains events related to system, storage devices, network devices, firmware updates, configuration changes, license messages, and so on. However, the system events are also available as a separate log called the System Event Log (SEL).

When a system event occurs on a managed system, it is recorded in the SEL. The same SEL entries are also available in the Lifecycle Log.

Firmware inventory

Lifecycle Controller-Remote Services provide information about each of the component firmware installed on the target system and the available firmware images are cached in the Lifecycle Controller.

Additional information contained in the available properties is:

- Firmware type
- Firmware version
- Installation date
- Vendor IDs
- Revision number

Event alerts

Alerts and actions can be set for certain events that occur on a managed system. An event occurs when the status of a system component has changed to the predefined condition. If an event matches an event filter and this filter is configured to generate an alert (email, SNMP trap, or IPMI alert), an alert is sent to one or more configured destinations. If the same event filter is also configured to perform an action (such

as reboot, power cycle, or power off the system), the action is performed. You can set only one action for an event.

Embedded Tech Support Report

Embedded Tech Support Report is used to provide information about health report of Hardware, Operating System (OS), and software applications installed on a server. This feature includes application information collected by Dell System E-Support Tool (DSET). This report is used by administrators to resolve business-critical issues. Examples of data collected in an Embedded Tech Support Report are:

- Hardware and inventory
- Info related to the server, Lifecycle Controller, and its components
- BIOS order boot information
- Lifecycle Controller log entries
- Firmware-related information
- vFlash SD Card partition information

Monitoring the out-of-band performance

Using this feature, you can monitor the performance index of CPU, memory, and I/O. Intel ME supports Compute Usage Per Second (CUPS) functionality for monitoring the performance. The monitoring is independent of the OS and does not use CPU resources. The Intel ME displays a platform CUPS sensor that provides the Computation, Memory and I/O resource utilization value in the form of a platform "CUPS Index". iDRAC monitors this CUPS index for overall system utilization and also the instant value of CPU, Memory, and I/O utilization index.

> NOTE: To use this feature, iDRAC enterprise license is required.

For more information about monitoring the out-of-band performance, see the *Base Metrics* and *Sensors* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**.

Maintain

Using various Lifecycle Controller-Remote Services capabilities, you can maintain the health of a system throughout its lifecycle. You can use features such as remote firmware management, part replacement, server profile import or export, and auto-discovery to maintain a system using Lifecycle Controller-Remote Services.

Server configuration profiles — export or import

Lifecycle Controller-Remote Services can export or import a Server Configuration Profiles file. The export operation collects the configuration information for BIOS, iDRAC, RAID, NIC, FC-HBA, System, and Lifecycle Controller and stores it in a single file that is copied to a network share. The Import operation imports the file from a network share, and applies the previously saved or updated configurations to a system. For more information, see *Server Cloning with Server Configuration Profiles* and *Creating and Managing Server Configuration Profiles* documents available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.aspx**.

Firmware update

You can perform firmware updates from a network source to either update or rollback component firmware. A rollback operation is used to install the previous version of a component firmware. It also provides the ability to update using a repository and schedule automatic updates.

The firmware update operations or firmware rollback operations are performed in the following order:

1. Initiate and download an image.
2. Create a reboot job.
3. Schedule an update job.
4. Monitor a job until the job is finished.

> **NOTE:** There are some components for which the updates are immediately applied after the firmware is downloaded, after which the system automatically restarts.

For more information about automatic update, see *Automatic Updates in Dell PowerEdge 12th Generation Servers* white paper available at **delltechcenter.com.**

Part replacement

The Part Replacement feature is used to automatically update a firmware, configuration, or both for a newly replaced component, such as a RAID controller, NIC, or power supply, to match with the original part. It is a licensed feature that is disabled by default, and can be enabled if required.

When a component is replaced and the part replacement feature is enabled, the actions performed by Lifecycle Controller are locally displayed on the system monitor during POST. You can remotely configure part replacement-related properties through the web services interface using the WSMAN protocol.

When a motherboard is replaced, the system configuration is automatically restored. However, if the Service Tag of a system is deleted for any reason, then you can manually enter the Service Tag.

Server profile — export or import

Lifecycle Controller-Remote Services can export (backup) or import (restore) the server profile of the host system. These operations are commonly used during motherboard replacement.

The export feature gathers system information, firmware images, hardware configuration, Lifecycle Controller configuration, iDRAC firmware and configuration, and stores the information to a single file on the local vFlash SD card or a remote network share. The import feature applies the saved configurations to a system from the local vFlash SD card, or from a network share. It also provides the ability to automatically back up to the vFlash SD card or a network share.

For more information about automatic backup, see *Automatic Backup Server Profile in Dell PowerEdge 12th Generation Servers* white paper available at **delltechcenter.com**.

Server license — import

Lifecycle Controller-Remote Services can import (restore) the server license of a host system. These operations are commonly used during motherboard replacement. You can import the license that is stored on a USB drive or on the network share such as CIFS or NFS.

Auto discovery

The Auto Discovery feature in iDRAC allows newly installed servers to automatically discover the remote management console that hosts the Provisioning Server. The Provisioning Server provides custom administrative user credentials to iDRAC so that the management console can discover and manage the newly installed managed system.

If you order a Dell system with the Auto Discovery feature enabled (factory default setting is disabled), then iDRAC is delivered with DHCP enabled and user accounts disabled. If the Auto Discovery feature is disabled, you can manually enable this feature and disable the default administrative account using the **iDRAC Settings** utility. For more information about the iDRAC Settings utility, see *iDRAC User's Guide*.

For more information about Auto Discovery, see the *Lifecycle Controller Management* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.aspx**.

Deleting server-related information using Lifecycle Controller

By using this feature, server-related data such as system configuration, hard-disk drives, Self-Encrypting Devices (SED), logs, PowerEdge RAID Controller Non-Volatile (PERC NV) cache (if available), and other data that are stored on a server can be deleted. iDRAC license cannot be deleted by using this feature. Log in to the Lifecycle Controller first, and then enter BIOS setup password to use this feature. You can select components based on your requirement. You can delete data under three categories:

- System
- Storage
- Physical disk drive

Data cannot be retrieved after you delete, because the deletion process is permanent.

Managing the web server certificate

On the 13th generation of PowerEdge servers, the iDRAC web server certificate management methods are introduced. By default a self-signed certificate is available on iDRAC. You can generate a certificate signing request (CSR) and use the CSR to create a Certificate Authority (CA) signed certificate. To use this feature, the following methods are introduced in the iDRACCard profile:

- GenerateSSLCSR
- ExportSSLCertificate
- ImportSSLCertificate
- DeleteSSLCertificate

The method to support Export and import operations are:

- Web Server Certificate

- CA certificate for Directory Service
- Custom Signing Certificate

To use the new certificate, restart iDRAC and a new method iDRACReset are added.

For more information about managing the web server certificate, see the *iDRAC Card* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.aspx**.

Viewing the managed computer system using the Physical Computer System View

Physical Computer System View (PCSV) provides the view of a managed system such as current state and configuration. You can directly access PCSV using PowerShell commands. Using PCSV you can:

- Receive information about the managed elements.
- Directly enumerate the CIM_PhysicalComputerSystem from the console without any prior knowledge of a particular class.
- Use a registered profile to enumerate the implemented features.
- Invoke certain method based on implemented features.

For more information about viewing the managed computer system using PCSV, see the *Physical Computer System View* profile document available at **en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.aspx**.

Job management

Lifecycle Controller allows you to create, schedule, track, and manage system management tasks that are referred to as "jobs".

A single job or array of jobs can be run immediately or scheduled to run later. Multiple jobs are listed in the order of job execution sequence. If a system must reboot at the scheduled start time, a reboot job must be added to the job list.

Remote Services provides the following functions to manage Lifecycle Controller jobs:

- Creating Jobs — Create specific types of jobs to apply configurations.
- Scheduling Jobs and Job Queues — Run multiple jobs in a single restart of the system using the SetupJobQueue() method. If a job is created without setting the start time, use the SetupJobQueue() method to set the schedule and order of execution. The job is set up for execution at the time that was specified.
- Deleting Jobs — Delete a specified existing job or all jobs at once.
- Reporting all Jobs — Report all jobs using a single command.
- Reporting scheduled Jobs — Generate a report of all scheduled jobs using a selection filter of JobStatus = Scheduled.

Job types

There are two types of jobs, system-created jobs (implicit) and user-created jobs (explicit):

- System-created jobs are created when you run specific Remote Services tasks. For example, Remote Services features such as export hardware inventory, export license, create persistent storage

partition, and so on create a job and return the job ID. Polling the job status determines the completion status of the task.

- User-created jobs such as CreateTargetedConfigJob, CreateRebootJob, and InstallFromURI are used to apply user configurations for RAID, NIC, BIOS, and so on. They can be scheduled to run immediately or at a scheduled time.

Table 1. System and User Created Jobs

System-created jobs	User-created jobs
- Export Factory Configuration - Export Hardware Inventory - Export Lifecycle log - vFlash (Initialize) - vFlash (Create Partition) - vFlash (Format Partition) - vFlash (Attach Partition) - vFlash (Detach Partition) - vFlash (Export Data from Partition) - vFlash (Create Partition using Image)	- RAID configuration - BIOS configuration - NIC configuration - iDRAC configuration - System configuration - Software update (BIOS, NIC, RAID, and so on) - Reboot

System status

This feature is used to remotely obtain the overall Remote Services API status that includes both the host system status and as well as the remote services (Data Manager) status. The overall status is displayed in the Status output parameter.

After the job is complete in Automated Task Application (previously SSM), the job status is immediately updated in the job store. The job is immediately moved to the Completed state and synchronization starts. After the synchronization is successful, the system is in the *Ready* state.

Getting started with API collateral and links

Getting started with any feature of Lifecycle Controller begins at the Dell TechCenter Lifecycle Controller home page — **delltechcenter.com/LC**.

The home page contains various sections that reference URLs, and these referenced URLs are direct links to the corresponding sections.

You can follow these steps to get started using the Lifecycle Controller API:

1. Identify the feature or the required management operation.
2. Determine how the API is constructed for the desired management activity.
3. Utilize a client to access the API.
4. Use the best practices work flows for the client to interact with the API to accomplish the activity.

Profiles

Profiles describe the behavior of each feature and necessary classes, properties, methods, and configurable management attributes that represent the feature. The Profile documents explain the features supported by the Lifecycle Controller-Remote Services provided within the context of the CIM architecture. Profile specifications are organized around different management areas or domains.

Lifecycle Controller-related profiles

> **NOTE:** To view the profile documents, on the Dell TechCenter (**delltechcenter.com/LC**) page, under **Reference Specifications**, click **Profiles**. Alternatively, go to **en.community.dell.com/techcenter/systems-management/w/wiki/1906.aspx.**

Table 2. Profiles

Profile Name	Description
Active Directory	The Active Directory Client Profile extends the management capabilities of referencing profiles by adding the capability to represent the configuration of Active Directory client service and the groups managed by the service.
Base Metrics	The DMTF Common Interface Model (DCIM) Base Metrics Profile extends the DMTF Base Metrics Profile to add Dell-specific implementation requirements for power-related metrics. The profile standardizes the units and description for the metrics, and provides static methodology for the clients to query the metrics without substantial traversal of the model.
Base Server and Physical Asset	The Base Server Profile is the autonomous profile that defines the classes used to describe basic server hardware and its related software.

Profile Name	Description
BIOS and Boot Management	The BIOS and Boot Management Profile extends the management capabilities of referencing profiles by adding the capability to represent the configuration of the system BIOS setup and to manage the boot of the system.
CPU	The DCIM CPU Profile describes the properties and interfaces for executing system management tasks related to the management of processors within a system.
Ethernet Port	The Ethernet Port Profile extends the management capability of referencing profiles by adding the ability to represent an Ethernet port, its associated controller, and Ethernet interfaces.
Event Filter	The Dell Event Filter Profile provides the management capabilities to view the event filters and set actions and notifications for the events.
Fan	The DCIM Fan Profile describes the properties and interfaces for executing system management tasks related to the management of fans within a system.
Fibre Channel	The Fibre Channel Profile extends the management capabilities of referencing profiles by adding the capability to represent the configuration of Fibre Channel host bus adapters (FC HBA).
iDRAC Card	The DCIM iDRAC Card Profile describes the properties and interfaces for performing system management tasks related to the management of basic properties of iDRAC card. DCIM_iDRACCardEnumeration class has attributes PTMode and AdminState to support configuration of iDRAC Network Bridge in LOM-P2P or USB-P2P modes. VNC server configuration is possible by setting attributes of Port, Timeout, Password, Enable and LowerEncryptionBitLength. DCIM_iDRACCardInteger has new attribute SMTPPort for SMTP configuration and AlertPort and DiscoveryPort for SNMP configuration. DCIM_iDRACCardEnumeration class has attributes PTMode and AdminState to support configuration of iDRAC Network Bridge in LOM-P2P or USB-P2P modes. Basic OMSA Equivalency: Some features (such as WatchdogResetTime andLCLReplication) currently provided by OMSA is available on iDRAC service module (iSM).
Job Control	The Job Control Profile extends the management capabilities of referencing profiles by adding the capability to create, schedule, track, and manage jobs that represent platform management operations.
LC Management	The Lifecycle Controller (LC) Management Profile describes the management of the Dell Lifecycle Controller and its configuration attributes. The ExportCertificate() method is used to export unique generated SSL Certificates from the Lifecycle Controller to a file in remote share location. The DCIM_LCService. ExportHealthReport() method is used to collect the EHR. That is, hardware, operating system and application data, compress the zip file, and then to save in to the respective remote share path (cifs/nfs).

Profile Name	Description
	The DCIM_LCService.ImportSystemConfigurationPreview() method is used to preview the results of the application of the XML template ahead of the actual application without any restart. It also gives the information about the failure. The successful invocation of this method returns a job.

The methods DCIM_SoftwareInstallationService:SetUpdateSchedule(), DCIM_SoftwareInstallationService:GetUpdateSchedule(), and DCIM_SoftwareInstallationService:ClearUpdateSchedule() allow for automatic firmware updates at scheduled intervals.

The DCIM_LCEnumeration class supports an attribute "BIOS Reset To Defaults Requested" to reset BIOS to its default property.

The methods DCIM_LCService.SetBackupSchedule(), DCIM_LCService.GetBackupSchedule(), and DCIM_LCService.ClearBackupSchedule() allow for scheduling automated backup of server profiles.

The DCIM_LCService.ExportCompleteLCLog() method allows you to export full lifecycle log.

The DCIM_LCService.ImportSystemConfigurationPreview method allows for previewing before applying an XML template.

DCIM_LCService provider adds the following methods: RunePSADiagnostics () and ExportePSADiagnosticsResult() for the automatic diagnostics.

DHCP-based configuration: Along with getting the IP address from the DHCP server, when the server comes up, user can set any configuration attribute of iDRAC using an OEM field |
License Management	The License Management Profile is an autonomous profile for modeling the Dell Product License Manager (License Manager). It extends the management capabilities of referencing profiles by adding the capability to represent the devices and Licenses managed by the Dell Product Licensing Manager.
Memory	The DCIM Memory Profile describes the properties and interfaces for executing system management tasks related to the management of memories (DIMMs) within a system.
OS Deployment	OS deployment profile describes how to remotely download, setup, and monitor an operating system on a bare metal machine.
PCI	The DCIM PCI Device Profile describes the properties and interfaces for executing system management tasks related to the management of PCI devices within a system.
Persistent Storage	The Persistent Storage Profile extends the management capabilities of referencing profiles by adding the capability to represent and manage the partitions on the Virtual flash media on Dell platforms.
Physical Computer System View	This profile includes a specification of the physical computer system view, extrinsic methods for management operations, and its associated relationships.
Power State Management	The Power State Management Profile describes the classes, associations, properties, and methods used to manage the power of a system.

Profile Name	Description
Power Supply	The DCIM Power Supply Profile describes the properties and interfaces for executing system management tasks related to the management of power supplies within a system.
Profile Registration	The DCIM Profile Registration Profile defines the classes used to describe the DCIM and DMTF profile registration and the version information of the profiles advertised as implemented for a managed system and components of the system.
RAID	The RAID Profile extends the management capabilities of referencing profiles by adding the capability to represent the configuration of RAID storage. PERC9 support features provide the following features: • RAID10−UnevenSpan support: This is a new feature that supports uneven spans (spans with different span length) for RAID 10 virtual disk (VD). This is required to support creation of RAID 10 VD with all possible number of physical disk drives. With this feature the RAID firmware automatically handles the creation of spans and therefore span information is hidden from end end users. • PERC 12 GBPS speed: PERC 9 controllers provide support for 12 Gbps speed and hence can support 12 Gbps physical disk drives. • Auto Import of foreign config: PERC9 controllers provide support for enhanced auto import of foreign config without requiring user interactions. This is ideal in a headless server environment. This feature enables PERC controller to auto import foreign config, when there is an existing configuration. • ControllerBootMode: PERC9 controllers provide support for setting controller boot mode. This is ideal in a headless server environment. This feature enables PERC controller to either wait for user interaction on error, or to continue boot on error, or headless mode continue boot on error or boot to headless safe mode. In each boot mode, the PERC either ignores or takes default action and continues on error. • 4K sector drives: PERC 9 is introducing support for hard disk drives with 4k sector size. The purpose of this feature is to allow customers to use new 4k sector HDDs, which allow faster data transfer using fewer commands.
Record Log	The DCIM Record Log Profile provides the management capabilities to represent logs of a managed system element.
Role Based Authorization	The DCIM Role Based Authorization Profile describes the properties and interfaces for executing system management tasks related to the authorization.
Sensors	The DCIM Sensors Profile describes the properties and interfaces for executing system management tasks related to the management of sensors within a system.
Simple ID Management	The DCIM Simple Identity Management Profile describes the properties and interfaces for executing system management tasks related to the management of accounts and identities.
Simple Raid	The profile extends the management capabilities to represent the configuration of RAID storage. The RAID storage is modeled as collections of attributes for the storage adaptors, physical disks, logical disks, end enclosures, and parent-child relationships between the collections.
Service Processor	The DCIM Service Processor Profile describes the properties and interfaces for executing system management tasks related to the management of the service processor and iDRAC.

Profile Name	Description
Simple NIC	The Simple NIC Profile extends the management capabilities of referencing profiles by adding the capability to represent the configuration of NIC network controllers. Virtual Address Management is supported by setting attributes of VirtMacAddr, VirtIscsiMacAddr, VirtFIPMacAddr, VirtWWN, VirtWWPN, and VirtualizationMode.
Software Inventory	The Dell Software Inventory Profile extends the management capabilities of referencing profiles by adding the capability to represent the software inventory of system.
Software Update	The Software Update Profile extends the management capabilities of referencing profiles by adding the capability to update platform firmware or software. DCIM_SoftwareInstallationService: installfromRepository and DCIM_SoftwareInstallationService: GetRepoBasedUpdateList allows updates from update repository. Solid-state Drive (SSD) wear-level odometer: Ability to provide lifetime/wear out of SSD drives attached to PERC controller. DIF drive reporting: PowerEdge RAID Controller 9 (PERC 9) is adding support for PI (Protection Information) drives. These protection fields are known as DIF (Data Integrity Fields) and drives supporting PI are also referred to as DIF drives. The data integrity field provides additional data robustness by providing CRC such as data validation at every level in the RAID stack.
System Info	The DCIM System Info Profile describes the properties and interfaces for executing system management tasks related to the management of the host system.
System QuickSync	The DCIM System QuickSync profile document describes the properties and interfaces used for system management tasks related to the management of QuickSync or NFC devices within a system.
USB device	The DCIM USB Device profile describes the properties and interfaces for the system management tasks related to the USB devices within a system.
Video	The DCIM Video Profile describes the properties and interfaces for executing system management tasks related to the management of video controllers within a system.
Virtual Media	The DCIM Virtual Media Profile describes the properties for executing system management tasks related to managing the Virtual Media functionality.

MOF WSDL and XSD API definitions

A complement to the profile documentation is the Managed Object File (MOF) that documents the class implementation of the Dell-specific CIM classes. Web Service Description Language (WSDL) and XML Schema Definition (XSD) files describe the resulting functionality.

Managed object file

The Common Information Model (CIM) is an open standard that defines how managed elements in an IT environment are represented as a common set of objects and relationships between them. This is

intended to allow consistent management of these managed elements, independent of their manufacturer or provider.

Files that contain the normative description for classes, properties, and methods are contained within the Managed Object File (MOF).

NOTE: To access the MOFs, on the Dell TechCenter (**delltechcenter.com/LC**) page, under **Reference Specifications**, click **MOFs**.

Web service description language

The Web Services Description Language (WSDL) is an XML-based language that is used for describing the functionality offered by a web service. A WSDL description of a web service (also referred to as a WSDL file) provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns.

XML schema description

An XML schema (also known as XSD) is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntactical constraints imposed by XML itself. These constraints are generally expressed using some combination of grammatical rules governing the order of elements.

NOTE: To access the XSD, use the link **en.community.dell.com/dell-groups/dtcmedia/m/ mediagallery/20074445.aspx**

Web services interface guide

The web Services Interface Guide (WSIG) serves as a guideline for utilizing the functionality available from embedded Lifecycle Controller Remote Services web Services interfaces. It provides information and examples for utilizing the web services for WSMAN protocol using Windows WinRM and open source WSMANCLI command-line utilities.

- Windows Version — **en.community.dell.com/techcenter/extras/m/white_papers/20066174.aspx**
- Windows batch file examples — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066179.aspx**
- Linux Version — **en.community.dell.com/techcenter/extras/m/white_papers/20066176.aspx**
- Linux WSMAN shell script examples — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066181.aspx**

Best practices guide

The *Best Practices Guide* provides the work flows that group smaller WSMAN operations to achieve a particular task. To access the *Best Practices Guide*, from the Dell TechCenter (**delltechcenter.com/LC**) page, under the **Web Services Integration Tools**, click **Best Practices Guide**. Alternatively, go to **en.community.dell.com/techcenter/extras/m/white_papers/20066173.aspx**

Sample scripts corresponding to all sections in the document are also provided, using WinRM on Windows and wsmancli on Linux.

The *Best Practice Guide* contains the detailed instructions of common work flows to perform various tasks utilizing WinRM or WSMAN. The PYTHON scripting language is used to provide a software

development kit (SDK) for the Lifecycle Controller API methods. The following primary objectives are addressed through the SDK:

- Work flows documented in the *Best Practices Guide* provide guidance to established, known, and working API methodologies.
- The corresponding PYTHON sample scripts are separately provided. After invoking these scripts, the output log can be used to provide approximate timing on a particular system configuration, as well as raw WinRM or Open-WSMAN input and output.

  NOTE: The scripts are located here — **en.community.dell.com/techcenter/extras/m/ white_papers/20066173.aspx**

Attribute registry XML

The attribute registry lists all the attributes and properties for the particular component in XML format. The attribute registries are located in the following locations:

- RAID Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066218.aspx**
- NIC Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066216.aspx**
- iDRAC Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066215.aspx**
- BIOS Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20066214.aspx**
- FC HBA Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20439052.aspx**
- PCIeSSD Attribute Registry — **en.community.dell.com/techcenter/extras/m/white_papers/ 20439051.aspx**

Event message registry XML

The message registry XML describes all messages, message IDs, and message arguments from all profiles.

This zipped file contains the iDRAC and Lifecycle Controller event and error message data in XML, conforming to the DMTF DSP0228 message registry XML schema. The zipped file also includes an XSL file provided by Dell that enables content searching and reading easier.

To view the *Dell Event Message Reference Guide* document, go to **http://www.dell.com/ openmanagemanuals** and click the latest OpenManage Software version. The Event Message Reference document contains the error and event information generated by firmware and other agents that monitor system components. These events are logged and displayed to the user on one of the system management consoles, or both logged and displayed.

XML schemas

The *Lifecycle Controller XML Schema Guide* provides interpretation of XML used by the Lifecycle Controller to describe various Lifecycle Controller output XML content such as:

- Logs
- Configuration results

- Hardware Inventory
- Attributes
- Server Configuration Profiles

> NOTE: To access the *Lifecycle Controller XML Schema Guide,* use the link **en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/20074445.aspx**

Authorization and licensing requirements for API access

There are four levels of iDRAC licensing:

> NOTE: Use the link **en.community.dell.com/techcenter/extras/m/white_papers/20067632.aspx** to download the *WSMAN License and Privilege Specification* white paper.

- Base Management with IPMI
- Express
- Express for blades
- Enterprise

Table 3. Licensing

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

White papers

White papers help you to know in-depth information about a business-critical process that you can complete by using firmware products such as Lifecycle Controller, iDRAC and so on. You can perform these processes by using GUI features, RACADM commands, and WS-MAN commands.

Lifecycle Controller and iDRAC white papers

To access the white papers about Lifecycle Controller and iDRAC, go to **delltechcenter.com/LC**.

Integrating the Lifecycle Controller API

This section outlines the resources required to integrate the Lifecycle Controller API into an application:

- API Clients – Lists the API clients that are available to support WinRM or WSMAN. The API clients enable a you to create an application in a variety of programming languages.
- Best Practices Guide — Provides information about the common work flows, where in ready-to-use Python scripts are provided for all the common work flows.
- Sample Scripts and Tools — Provides additional working examples and reference.
- Applications Using Lifecycle Controller-Remote Services — Lists several existing applications that are already integrated with the Lifecycle Controller API.
- WinRM and OpenWSMAN Installation and Configuration — Identifies resources for configuring WinRM and WSMAN.

API clients

The links to various API clients:

- WinRM Scripting API, MSDN — **msdn.microsoft.com/en-us/library/aa384469(VS.85).aspx**
- Openwsman CLI — **openwsman.org/project/wsmancli**
- Windows PowerShell blog — **blogs.msdn.com/PowerShell**
- Windows PowerShell ScriptCenter — **microsoft.com/technet/scriptcenter/hubs/msh.mspx**
- Ruby bindings for WSMAN — **rwsman.rubyforge.org**
- Recite — Interactive WSMAN Scripting Environment — **en.community.dell.com/techcenter/systems-management/w/wiki/3757.recite-interactive-ws-man-scripting-environment.aspx**
- Intel® WSMAN Java Client Library — **software.intel.com/en-us/articles/download-the-latest-intel-ws-management-java-client-library**

Best practices workflow references

For more information, see Best Practices Guide.

Sample scripts and tools

A few sample scripts to use Lifecycle Controller API are available for use with **Recite**. Recite is a Python-based tool that provides a simple and fast interface for using the Dell Lifecycle Controller API. It has an interactive mode that is useful to run a single command on a server or run batch commands to automate the sequence of operations.

- Interactive Recite environment — **en.community.dell.com/techcenter/systems-management/w/wiki/3757.recite-interactive-ws-man-scripting-environment.aspx**
- Other scripting examples — **en.community.dell.com/techcenter/systems-management/w/wiki/1981.scripting-the-dell-lifecycle-controller.aspx**

Applications using Lifecycle Controller-Remote Services

The following applications use Lifecycle Controller-Remote Services

- Dell Compellent | Fluid Data Network Storage Solution — **compellent.com**
- Dell Lifecycle Controller Integration v2.0 for System Center Configuration Manager — **dell.com/support/drivers/us/en/555/DriverDetails/DriverFileFormats?DriverId=Y6J43**
- Virtual Integrated System (VIS) — **dell.com/content/topics/topic.aspx/global/products/landing/en/virtual-integrated-system?c=us&l=en**
- OpenManage Essentials - Systems Management — **en.community.dell.com/techcenter/systems-management/w/wiki/1989.openmanage-essentials.aspx**
- Chassis Management Controller (CMC) — **en.community.dell.com/techcenter/systems-management/w/wiki/1987.dell-chassis-management-controller.aspx**

WinRM and OpenWSMAN installation and configuration

It is recommended to use WinRM 2.0 on Windows Management Stations. WinRM 2.0 is installed by default as a part of Windows 7 and Windows Server 2008 R2. It can also be installed as a part of the Windows Management Framework Core package on the following operating systems:

- Windows Server 2008 SP1
- Windows Server 2008 SP2
- Windows Server 2003 SP2
- Windows Vista SP1
- Windows Vista SP2
- Windows XP SP3

For more information on how to install WinRM 2.0 as a part of the Windows Management Framework Core package, see article 968929 in the Microsoft Knowledge Base at **go.microsoft.com/fwlink/?LinkId=186253**.

To install and configure Windows Remote Management, see **msdn.microsoft.com/en-us/library/windows/desktop/aa384372(v=vs.85).aspx**.

OpenWSMAN CLI is an open source Linux WS-MAN client. The OpenWSMAN CLI source code and installation information are available at **sourceforge.net/projects/openwsman/files/wsmancli**.

Social media reference

To obtain the most up-to-date information, go to the Dell TechCenter and search for the required information.

Product Name and Topic	Link on Dell TechCenter
Lifecycle Controller	http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx
integrated Dell Remote Access Controller (iDRAC)	http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac.aspx
Dell Chassis Management Controller	http://en.community.dell.com/techcenter/systems-management/w/wiki/1987.dell-chassis-management-controller.aspx
Contributing to Dell TechCenter Community and Best Practices	http://en.community.dell.com/techcenter/extras/w/wiki/3836.contributing-to-dell-techcenter-community.aspx
Systems Management General Forum	http://en.community.dell.com/techcenter/systems-management/f/4469.aspx

Systems Management forum section

The Dell systems management page on Dell TechCenter contains information about the full range of Dell OpenManage products, Dell embedded management, Dell KACE, and integration with third-party Systems Management consoles. Additionally, Systems Management Wiki, Forums, and Blogs are being updated daily to answer questions and expand on topics and details from IT professionals and administrators.

Systems Management General Forum — http://en.community.dell.com/techcenter/systems-management/f/4469.aspx.

6

Terms and definitions

The following table lists the terms used in this document and their definitions.

Term	Definition
LC	Lifecycle Controller
Enumerate	Refers to WS-MAN ENUMERATE operation as described in Section 8.2 of DSP0226_V1.1 and Section 9.1 of DSP0227_V1.0
Get	Refers to WS-MAN GET operation as defined in Section 7.3 of DSP00226_V1.1 and Section 7.1 of DSP0227_V1.0
iDRAC	Integrated Dell Remote Access Controller management controller for blades, rack, and tower servers
USC	Unified Server Configurator
iSCSI	Internet Small Computer System Interface, an Internet Protocol (IP) based storage networking standard for linking data storage facilities
SSM	System Services Manager
CSIOR	Collect System Inventory on Restart
SSIB	System Services Information Block
UEFI	Unified Extensible Firmware Interface
BIOS	Basic Input/Output System
NIC	Network Interface Controller
FQDD	Fully Qualified Device Description
LCL	Lifecycle Log
WSIG	Web Services Interface Guide
WSMAN	Web Service–Management