iDRAC7 Version 1.30.30 With Lifecycle Controller 2 Version 1.1
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.

2012 - 12

Rev. A00

Overview

This Quick Start Guide provides the basic steps to set up and use the Integrated Dell Remote Access Controller 7 (iDRAC7) version 1.30.30 with Lifecycle Controller 2 version 1.1. For links to detailed information on all available features, see Additional Information.

The following terms are used in this document:

- Managed System - The PowerEdge server containing the iDRAC7.
- Management Station - A workstation used to manage the iDRAC7 remotely through a Web browser.

Configuring Initial iDRAC7 Network Settings

You must configure the initial network settings based on your network infrastructure to enable communication with the iDRAC7 from your management station.

1. Turn on or reboot the managed system.
2. During Power-On Self-Test (POST), press <F2> when **F2 = System Setup** is displayed in the upper right corner of the screen as shown in the following figure.

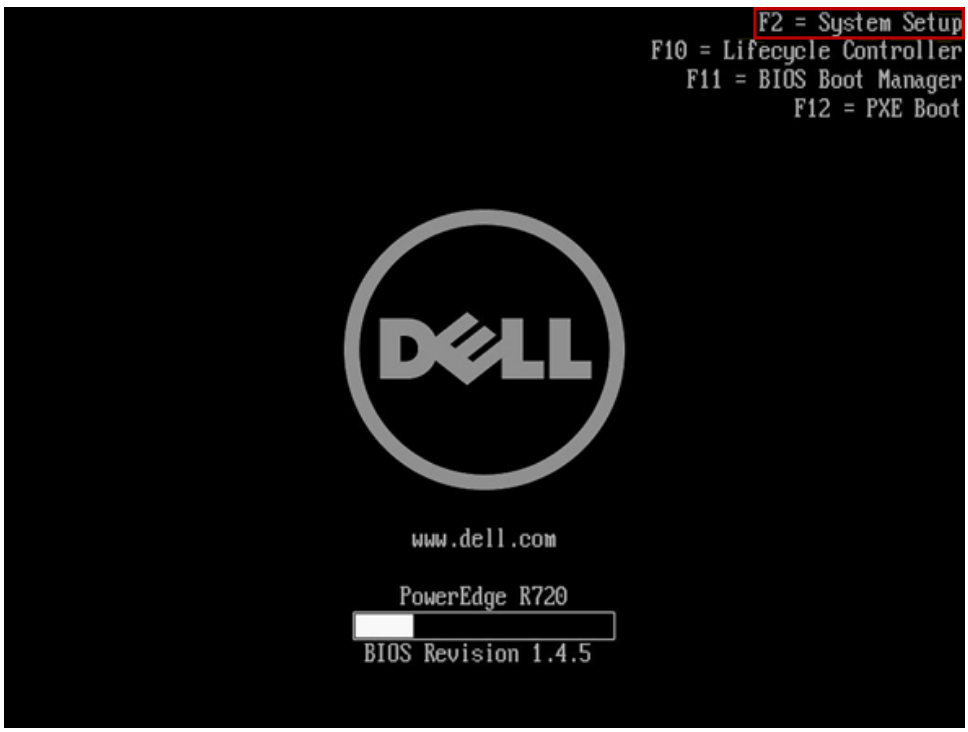

Figure 1. Selecting F2 to Enter System Setup

3. On the **System Setup Main Menu** page, click **iDRAC Settings**, and then click **Network**.
   The **iDRAC Settings.Network** page is displayed.

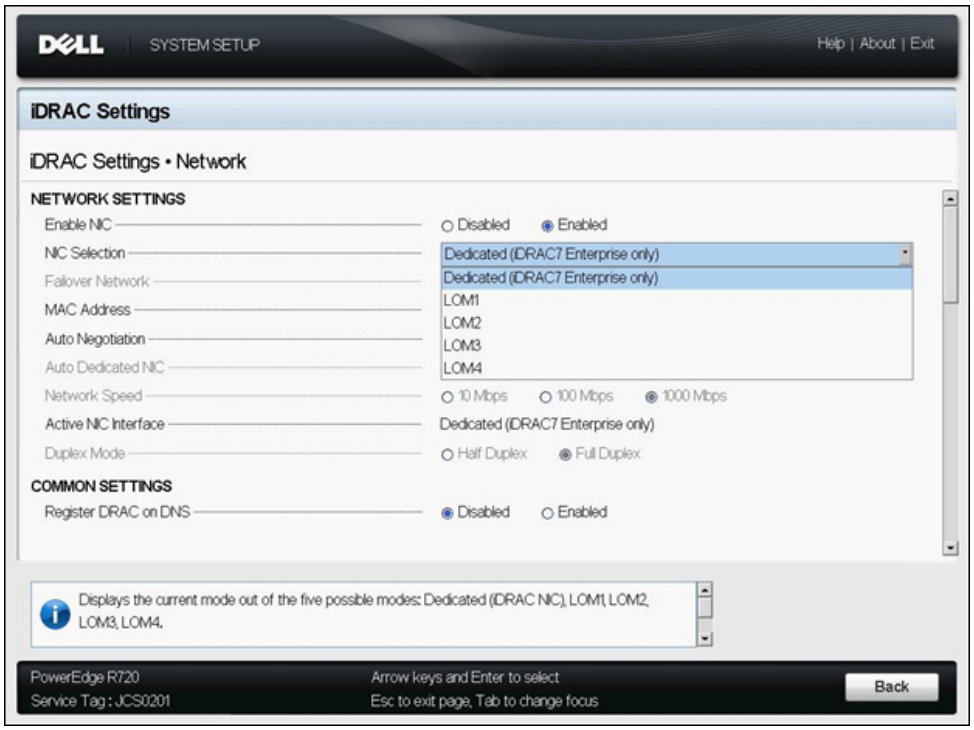

Figure 2. Network Settings

4. Specify the following settings:

   – **Network Settings**:

      * **Enable NIC** — Set this to **Enabled**.
      * **NIC Selection** (rack and tower servers only) – Select the **Dedicated (iDRAC7 Enterprise only)** option if it is available. Otherwise, select one of the listed LOMs to be used for the iDRAC traffic (the selected LOM is shared with the operating system). Make sure a network cable is connected to the appropriate port.

        NOTE: The **Dedicated (iDRAC7 Enterprise only)** option is available only on rack or tower systems with iDRAC7 Enterprise license.

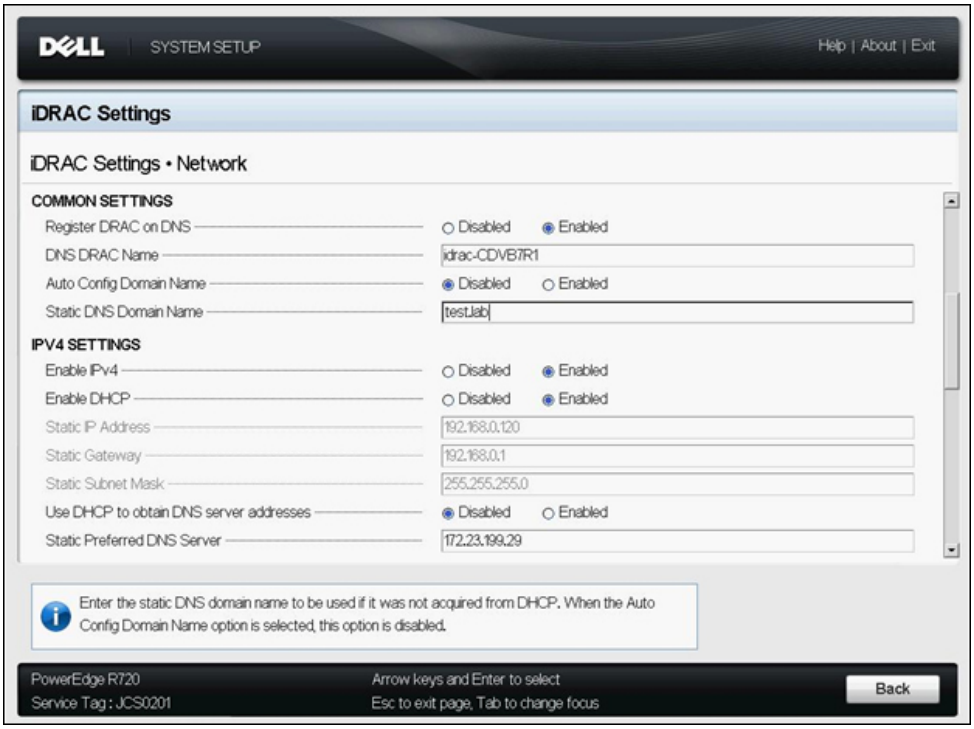

Figure 3. Common Settings and IPv4 Settings

- **Common Settings (Optional)**:
  - **Register DRAC on DNS** — Select **Enabled** for the iDRAC7 to automatically register itself with the DNS server, if the DNS server is configured to allow dynamic updates.

    NOTE: If this field is grayed-out, then to edit the field, either the **Enabled DHCP** option under **IPv4 Settings** or the **Enable Auto-configuration** option under **IPv6 Settings** must be enabled.
  - **DNS DRAC Name** — The default name is idrac-<Dell Service Tag #>. Use the default name or specify a unique name for the iDRAC.
  - **Auto Config Domain Name** — Set this to **Enabled** if you are using a DCHP server that is configured to provide the domain name.
  - **Static DNS Domain Name** — Specify the domain name, for example test.lab, if **Auto Config Domain Name** is set to **Disabled**.
- **IPv4 Settings**:

  NOTE: You can also use the **IPv6 Settings** section instead of IPv4. See the *iDRAC7 User's Guide* available at **dell.com/support/manuals** for the IPv6 configuration.
  - **Enable IPv4** — Set this to **Enabled**.
  - **Enable DHCP** — Select **Enabled** if you are using a DHCP server to assign the IP address, gateway, and subnet mask. Else, select **Disabled** and enter the values for **IP Address**, **Gateway**, and **Subnet Mask**.
  - **Use DHCP to obtain DNS server addresses** — Set this to **Enabled** if you are using a DHCP server that is configured to provide DNS server addresses. Else, select **Disabled** and enter the IP addresses for the **Static Preferred DNS Server** and optionally the **Static Alternate DNS Server**.

5. Click **Back**, **Finish**, and then click **Yes** when prompted to save changes.

   The network settings are configured.
6. Exit and allow the server to reboot.

NOTE: If you have enabled DHCP and are not connecting to iDRAC7 using the Fully Qualified Domain Name (FQDN) of the iDRAC, you can obtain the iDRAC's DHCP address from:

- The front LCD panel on systems that have them.
- Go back to **F2 = System Setup**, click **iDRAC Settings** and then click **System Summary**. Under the **Current IPv4 Settings** section, view the **Current IP Address** value.

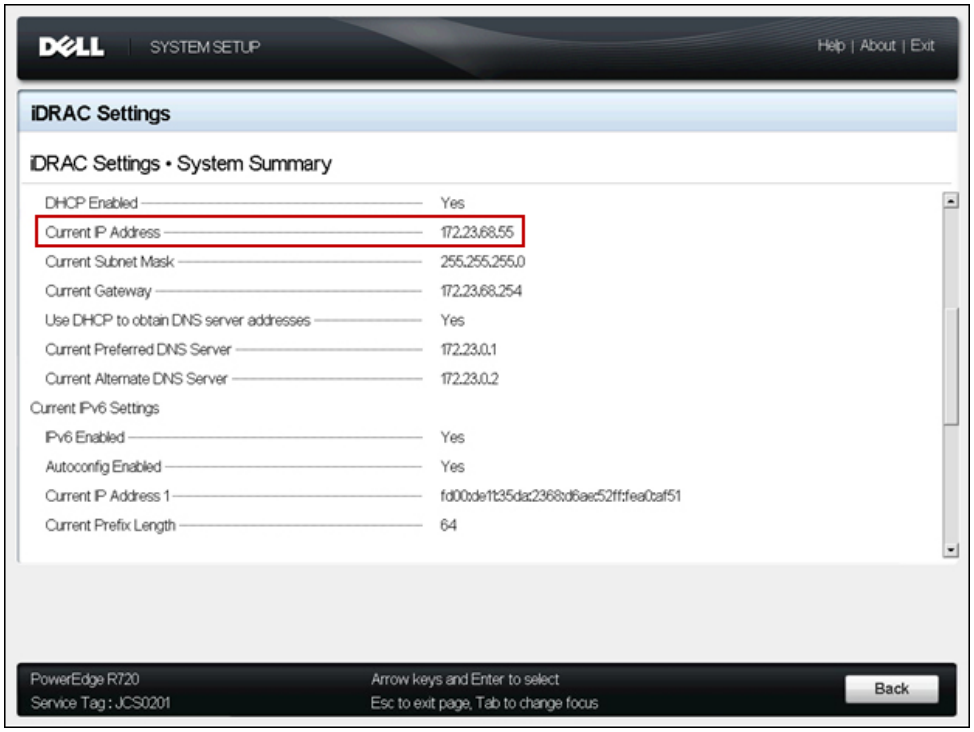

Figure 4. Viewing iDRAC IP Address

Logging in to iDRAC7 Web Interface

After configuring the basic iDRAC7 network settings during POST, you can remotely access the iDRAC7 using a supported Web browser such as Internet Explorer, Firefox, Google Chrome, or Safari. For the list of supported browser versions, and management station operating system versions, see the iDRAC7 readme file. The readme file is posted along with the *iDRAC7 User's Guide* at **dell.com/support/manuals**.

To log in to the iDRAC7 Web interface:

1. On the management station, open the Web browser and connect to the iDRAC7 using:

   https://<IP address or FQDN of iDRAC>

   For example:

   https://192.168.0.120

   https://idrac-CDVB7R1.test.lab

   A certificate warning page is displayed. Continue to the iDRAC7 Web page by following the options displayed in the page.

   NOTE: For detailed information on browser settings or using certificates with the iDRAC7, see the *iDRAC7 User's Guide* available at **dell.com/support/manuals**.

The **Login** page is displayed.

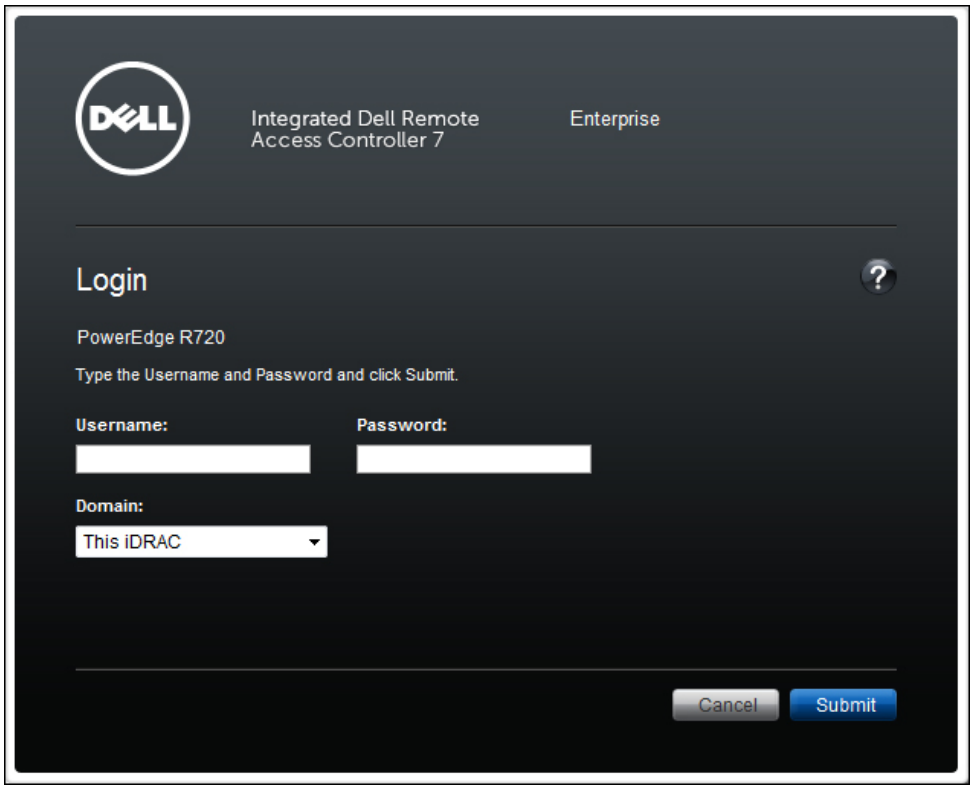

Figure 5. iDRAC7 Login Page

2. Log in with the default credentials: **Username**: root, **Password**: calvin.

   NOTE: Both **Username** and **Password** is case-sensitive.

   The **Default Password Warning** page is displayed.

Figure 6. Default Password Warning Page

3. It is recommended that you change the default password for the user root. Enter the new password in the **New Password** and **Confirm Password** fields, and click **Continue**.

   Click the icon for information about password length and supported characters.

   The new password is configured and you are logged in to iDRAC7.

Checking License Level or Upgrading License

The system license level appears on the **Login** page and at the top of all the iDRAC7 pages in the Web interface as shown in the following example.

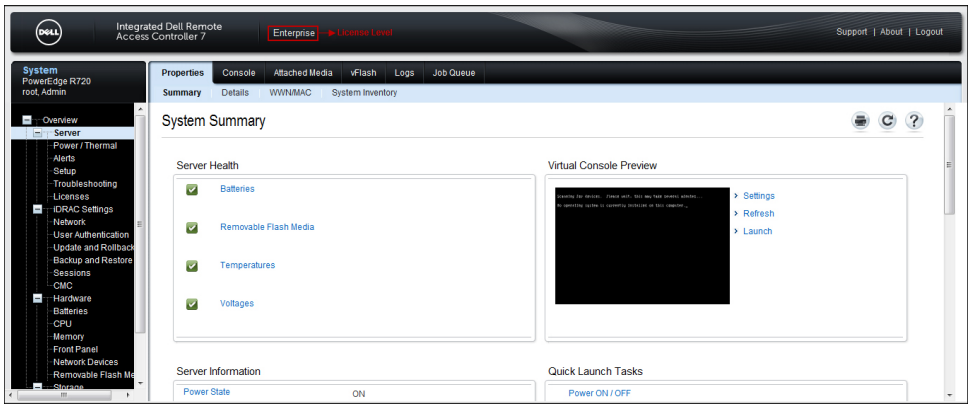

Figure 7. Checking License Level

The iDRAC7 Enterprise license level supports all the iDRAC7 with Lifecycle Controller features. If the system shows the license level as Basic Management or Express, certain features are not available. For information on the list of licensable features based on the license level, see the *iDRAC7 User's Guide* available at **dell.com/support/manuals**.

You can upgrade the license level from Basic Management to Express, Basic Management to Enterprise, or from Express to Enterprise.

If you purchased a license with the server, you can retrieve it. To do this, go to **Overview** → **Server** → **Licenses** and click the **License Self-Service Portal** link. Otherwise, contact your Dell sales representative to purchase an upgrade license. The license is sent to you as an XML file.

To install a license:

1. Store the purchased license file at a location accessible from the management station.
2. In the iDRAC7 Web interface, go to **Overview** → **Server** → **Licenses** .
3. Under **License Options**, from the **Select** drop-down menu, select **Import**.
4. Click **Browse**, select the license file, and click **Apply**.
   A message indicating the license was successfully imported is displayed.
5. Click **OK** to close the message.
6. Log out and log in to iDRAC7 Web interface.
   The new license level is displayed at the top of the Web interface pages.

Managing User Accounts

You can setup user accounts with specific privileges (role-based authority) to manage your system using the iDRAC7 and maintain system security. As an administrator, you can setup user accounts to allow other users to access iDRAC7. iDRAC7 supports role-based access to users with a set of associated privileges. The role defines the maximum privileges available.

Changing Root User's Name

For additional security, it is recommended that you change the default administrative user name from **root** to another name.

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Local Users** .
   The **Users** page is displayed.
2. In the **User ID** column, click User ID **2**.

3. On the **User Main Menu: User ID 2** page, click **Next**.
4. Change the **User Name** from root to another name.
5. If you did not change the password after logging into iDRAC7, you can change it by selecting the **Change Password** option and entering the new password in the **New Password** and **Confirm New Password** fields.
6. Since this is the only administrator account at this time, do not change the iDRAC User Privileges.
7. Click **Apply** to save the changes.

Creating a New User

To create a new user:

1. In the iDRAC7 Web interface, go to **Overview** → **iDRAC Settings** → **User Authentication** → **Local Users** .
   The **Users** page is displayed.
2. In the **User ID** column, click on an available User ID. For example, User ID **3**.
3. On the **User Main Menu: User ID 3** page, click **Next**.
4. On the **User Configuration** page, select the **Enable User** option.
5. In the **User Name** field, enter a user name.
6. In the **New Password** and **Confirm New Password** fields, enter a password.
   For information on the password length and characters, click the icon
7. In the **iDRAC User Privileges** section, select a **Role** to assign to the user.
   There are four pre-configured roles: **Administrator**, **Operator**, **Read Only**, and **None**. You can customize the privileges by selecting the individual privileges. The role automatically changes to **Operator** (if the selected privileges do not match a pre-configured role).

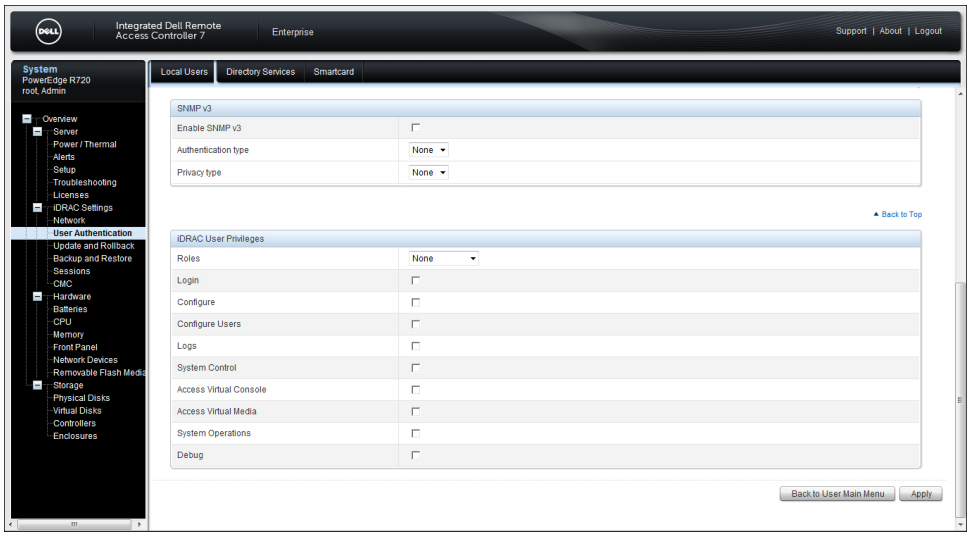

Figure 8. Assigning User Privileges

8. Click **Apply** to save the changes.

Updating iDRAC7 and Lifecycle Controller Firmware

NOTE: This section covers remote update, which uses the Update Package for Microsoft Windows (32-bit) regardless of the operating systems installed on your managed system or management station.

Before updating the iDRAC7 and Lifecycle Controller firmware

1. Check the currently installed firmware versions. To do this, go to **Overview** → **Server** → **Properties** → **Summary** .

   The **System Summary** page is displayed. Under the **Server Information** section, check the **Firmware Version** and **Lifecycle Controller Firmware version** information.

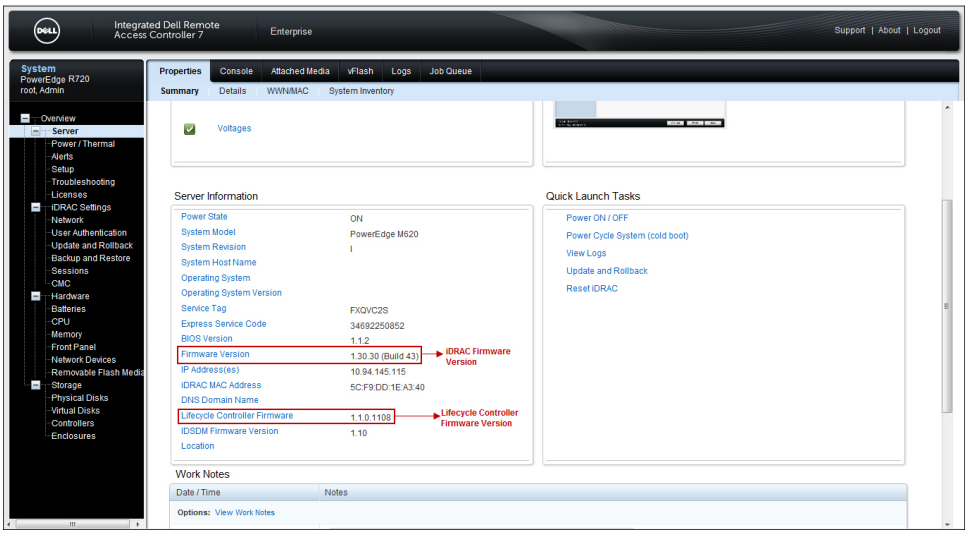

Figure 9. Server Information on iDRAC7 Home Page

2. Download the required firmware.

   To do this, see Downloading Firmware section.
3. From the management station, log in to the iDRAC Web interface and go to **Overview** → **iDRAC Settings** → **Update and Rollback** .
4. Click **Choose File**, browse and select the iDRAC Firmware Update Package for Microsoft Windows, and then click **Upload**.
5. After the upload is complete, the **Update Details** section displays the firmware file uploaded to iDRAC.
6. If you have downloaded Lifecycle Controller firmware, repeat steps 3 and 4.

   NOTE: You can upload one or both packages to iDRAC in any order.
7. After the files are uploaded, select the box(es) next to the file name(s) and click **Install**.

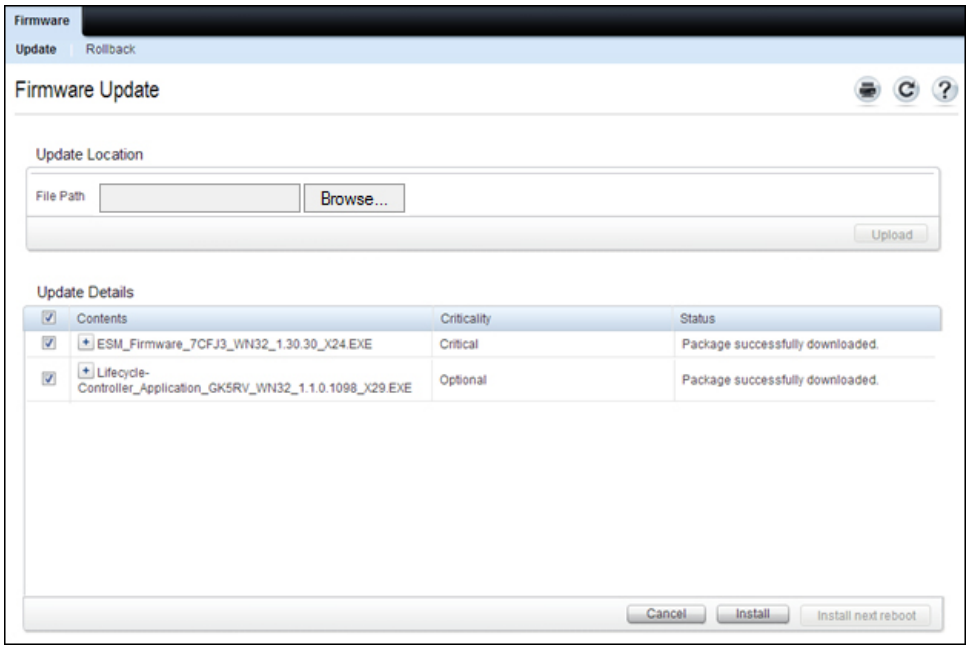

Figure 10. Firmware Update

The message indicating **Updating Job Queue** is displayed. Click **OK** to close. The update takes about five minutes. If the iDRAC firmware is being updated, the iDRAC reboots and connectivity to iDRAC7 is lost temporarily.

8. Reconnect to the iDRAC7 Web interface and go to **Overview** → **Server** → **Job Queue**.
9. Expand the [+] icon next to each job to confirm that the firmware update jobs were completed successfully.

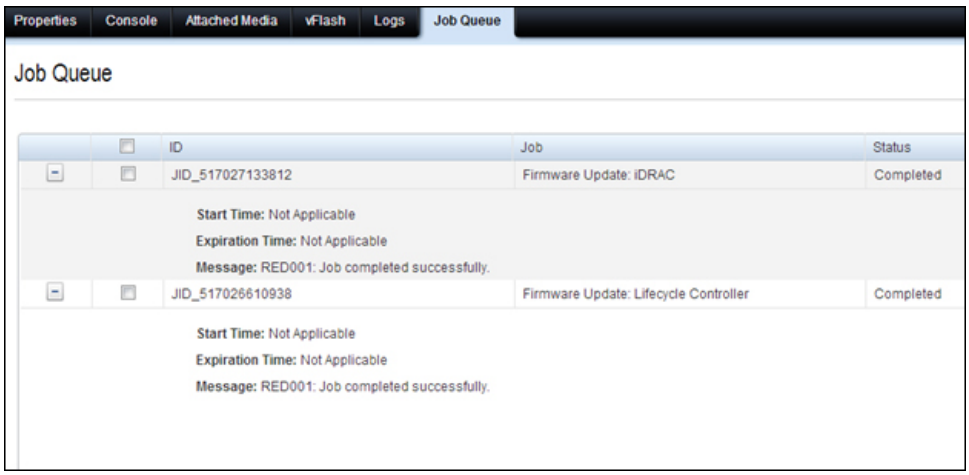

Figure 11. Job Queue Page

Downloading Firmware

To download the firmware:

1. Go to **http://support.dell.com**.
2. If prompted, select **Start Here** under **Small Businesses** or **Enterprise IT**.

3. Enter the **Service Tag** of the managed system and click **Submit**, or use one of the choose options to locate your system model.
4. Click **Drivers and Downloads**.
5. On the **Drivers and Downloads** page, expand **Enterprise Systems Management (ESM)** and locate the iDRAC7 Firmware. If a newer version is available, click **Download File**.
6. In the window that opens, make sure that the **Update Package for Microsoft Windows (32–bit)** is selected. It is recommended that you also select the iDRAC7 readme file. Click **Continue**.
7. Save the iDRAC firmware file to a location accessible from your management station.
8. Return to the **Drivers and Downloads** page, expand **Lifecycle Controller** and repeat the steps for the Lifecycle Controller application firmware. If a newer version is available, make sure to download the Update Package for Microsoft Windows (32–bit).

Using Virtual Console

You can use the Virtual Console to manage a remote system using the keyboard, video, and mouse on your management station to control the corresponding devices on a managed system.

NOTE: The Virtual Console feature is available on Monolithic (Rack or Tower) systems with Enterprise Licenses or Modular (Blade) systems with Express or Enterprise Licenses only. To upgrade your license, see Checking License Level or Upgrading the License.

To launch the Virtual Console from the iDRAC7 Web interface:

1. Go to **Overview** → **Server** → **Properties** → **Summary** and under **Virtual Console Preview** section, click **Launch**.

   NOTE: If you are using Internet Explorer, you may be prompted to install an ActiveX control. Other browsers require Java. If you prefer to use Java with Internet Explorer, go to **Overview** → **Server** → **Console** , change the **Plug-in Type** from **Native** to **Java**, and then click **Apply**. When launching Virtual Console, browsers such as Firefox and Chrome may ask for the program to use. Choose **Java Web Start Launcher** and click **OK**.

2. If a certificate warning message is displayed, click **Run**. Acknowledge any other certificate warnings that may be displayed. See the *iDRAC7 User's Guide* for more information on certificates.

   The Virtual Console opens and the managed system's console appears regardless of the state or presence of the operating system.

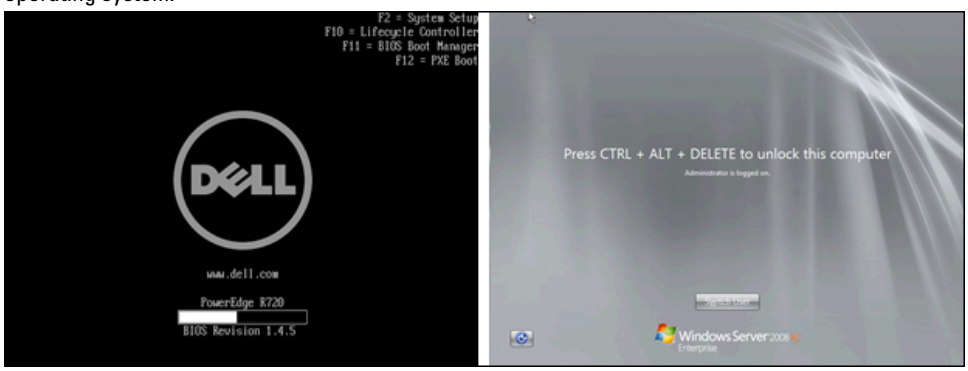

Figure 12. Virtual Console - Independent of Operating System State

Use the **Macros** menu at the top of the Virtual Console for the <Ctrl> + <Alt> + <Del> key combination. For more information, see the *iDRAC7 User's Guide*.

Virtual Console - Using Virtual Media Menu

The devices located on the management station such as CD/DVD drives, USB flash drives, folders, and **.iso** images can be mounted as virtual media for use by the managed system.

The following example uses a USB flash drive:

1. Connect the USB flash drive to the management station.
2. Launch the Virtual Console.
3. At the top of the **Virtual Console Viewer** window, select **Virtual Media** → **Launch Virtual Media**.
4. If a certificate warning is displayed, click **Run**. For more information on certificates, see the *iDRAC7 User's Guide* available at **dell.com/support/manuals**.

   The **Virtual Media Client View** window is displayed that provides a list of devices available for mapping.
5. In the **Mapped** column, select the box next to the drive letter (Windows management stations), or /dev name (Linux management stations) assigned to the USB flash drive on the management station as shown

   The USB Flash Drive is now mapped and it can be accessed from the operating system of the managed system.

   NOTE: On Windows-based managed systems, the drive is auto-mounted and assigned the next available drive letter. On Linux-based managed systems, the device is auto-mounted if the system is in run level 5.

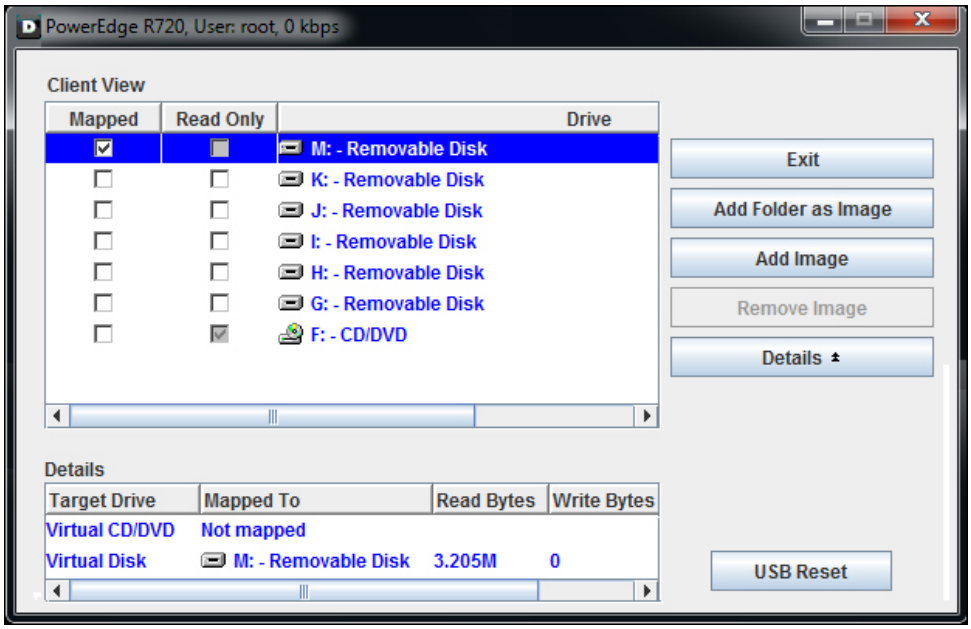

Figure 13. Virtual Media Mapped to Windows Management Station Drive M:

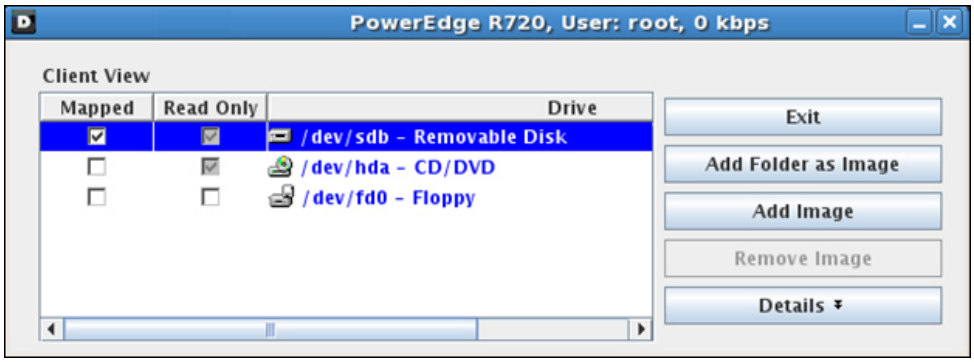

Figure 14. Virtual Media Mapped to Linux Management Station /dev/sdb

If the flash drive is bootable, the managed system can be booted from the flash drive. An example is provided in Virtual Console - Using Next Boot Menu section.

6. To end the session, click **Exit**, and then click **Yes** when prompted.

Virtual Console - Using Power Menu

You can use the **Power** menu available in the Virtual Console Viewer to perform power operations on the managed system. To do this:

1. Launch the Virtual Console.
2. At the top of the Virtual Console Viewer, click **Power** and select the required option:
   - **Power On System** – Turns on the managed system (the equivalent of pressing the physical power switch when the server power is off). This option is disabled if the system is already turned on.
   - **Power Off System** – Turns off the managed system.

     CAUTION: A running operating system does not shutdown gracefully.
   - **Graceful Shutdown** — Shuts down the operating system and turns off the managed system. Graceful shutdown requires an Advanced Configuration and Power Interface (ACPI)-aware operating system, which allows system directed power management. Make sure that the shutdown option is configured for the operating system before you perform a graceful shutdown using this option. If you use this option without configuring it on the operating system, it reboots the managed system instead of performing a shutdown operation.
   - **Reset System (warm boot)** — Reboots the system without turning it off.

     CAUTION: A running operating system does not shutdown gracefully.
   - **Power Cycle System (cold boot)** — Turns off and then reboots the system.

     CAUTION: A running operating system does not shutdown gracefully.
3. When prompted to confirm the action, click **OK**. The managed system performs the selected power operation.

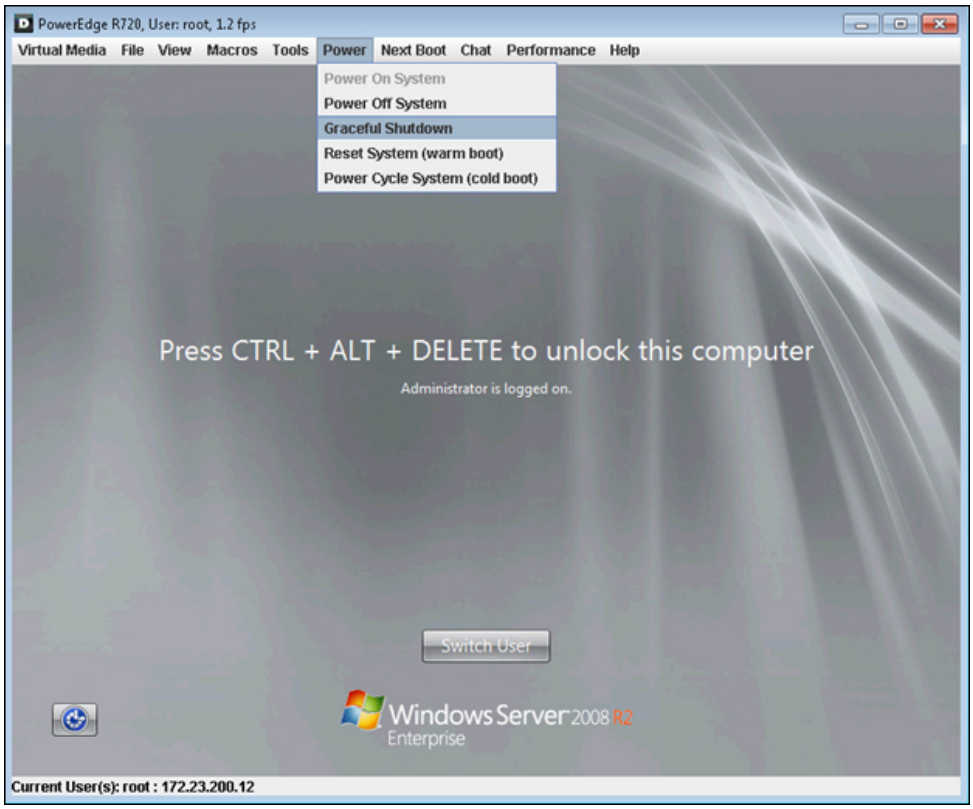

Figure 15. Virtual Console — Power Menu

Using Virtual Console — Next Boot Menu

You can use the **Next Boot** menu available in the Virtual Console Viewer to select the device to boot from as the managed system is being viewed. This feature sets a one-time boot option that overrides the BIOS boot order on the managed system. In addition to the standard local and virtual boot devices, this menu includes options to launch BIOS Setup or the Lifecycle Controller interface on the next boot.

For example, consider a bootable USB flash drive:

1. Launch the Virtual Console from the management station.
2. Insert a bootable USB flash drive in the management station and map the drive using Virtual Media.
3. Select **Next Boot** → **Virtual Floppy** (the USB flash drive emulates a floppy drive in BIOS in this case)

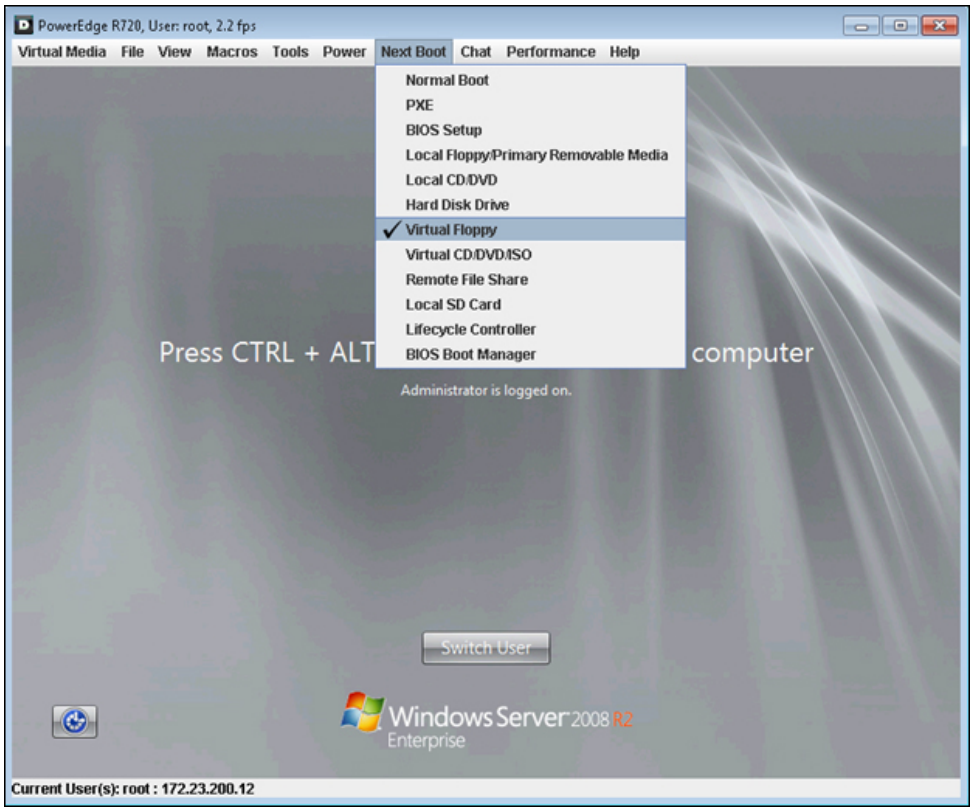

Figure 16. Virtual Console — Next Boot Menu

4. Click **OK** when prompted to confirm the selection.
5. Reboot the managed system using the **Power** menu.

   The managed system boots to the USB flash drive installed in the management station.
6. When complete, click **Exit**, and then click **Yes** in the **Virtual Media Viewer** window and close this window.

Viewing Logs

iDRAC7 provides the System Event Log (SEL) and the Lifecycle log. The SEL contains only the system events. The Lifecycle Log contains events related to system, storage devices, network devices, firmware updates, configuration changes, license messages, and so on.

- **System Event Log** — To view the System Event Log (SEL), go to **Overview** → **Server** → **Logs** → **Logs**. The **System Event Log** page displays a severity indicator, a time stamp, and a description for each event logged. The log can be sorted by clicking the column headings. If you have sufficient privileges, **Clear Log** is available at the bottom of the page that allows you to clear the SEL.
- **Lifecycle Log** — The Lifecycle Log provides the history of changes related to the components installed on a managed system. To view the Lifecycle log, go to **Overview** → **Server** → **Logs** → **Lifecycle Logs**. The **Lifecycle Log** page is displayed.

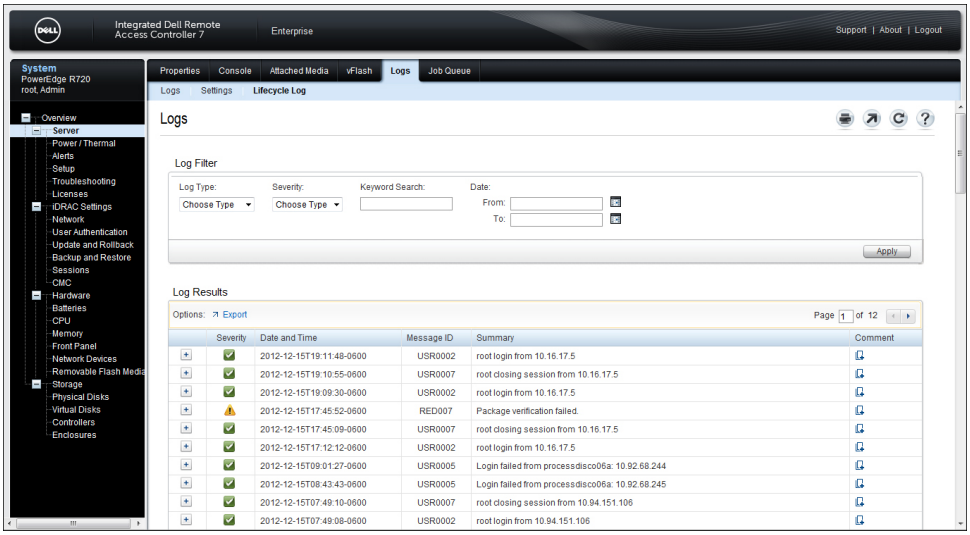

Figure 17. Lifecycle Log Page

You can use the **Log Filter** section at the top of the page to filter and search for events based on the selected criteria.

The Date and Time of each event is shown with the iDRAC's timestamp followed by the time zone offset of the iDRAC. Events are listed with the most recent on top. Click the + for an event to view a detailed description and recommended action if applicable.

Under **Log Results** section, click **Export** to export the Lifecycle Log in XML format to a location of your choice.

NOTE: The events in the exported log are sorted with the oldest events on top.

For detailed information about each message ID, see the *Event Message Reference Guide Version 2.0*.

- Click here to view the XML files.
- Click here to view the PDF file.

Setting iDRAC7 Time Zone and NTP

The iDRAC sets its time from the system BIOS unless a Network Time Protocol (NTP) server is used.

To view the current iDRAC time, go to **Overview → iDRAC Settings → Properties → Summary** and view the **RAC Time**.

To set the time zone, go to **Overview → iDRAC Settings → Properties → Settings**. From the **Time Zone** drop-down menu, select the required time zone and click **Apply**.

NOTE: Changing the time zone does not change the iDRAC time unless an NTP server is used. Daylight savings time is applied automatically, if a time zone that supports daylight savings time is selected.

To configure NTP, select **Enable Network Time Protocol (NTP)**, enter up to three NTP server addresses, and click **Apply**.

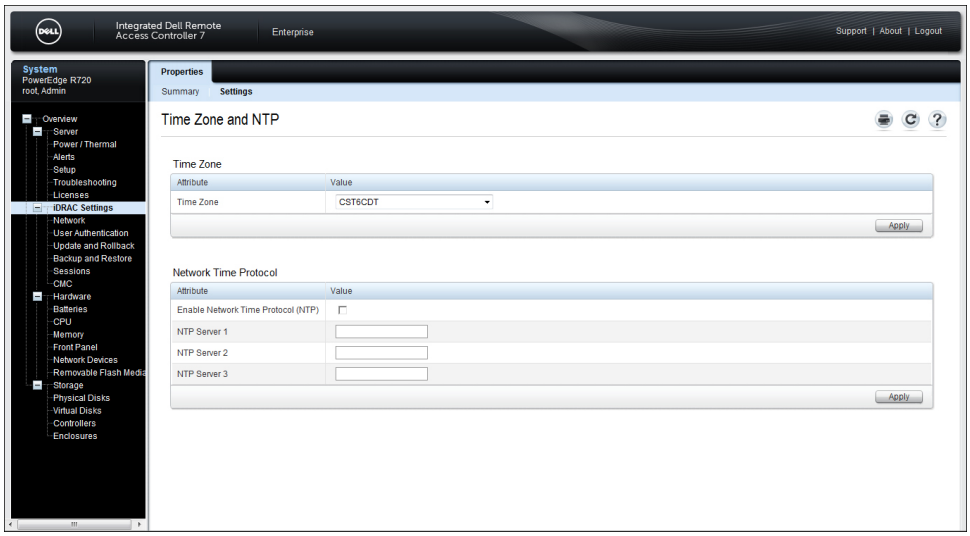

Figure 18. Time Zone and NTP Page

Summary

Congratulations, you have successfully completed the basic set up and used some of the popular features for the iDRAC7 with Lifecycle Controller technology. As you continue to explore the options and additional settings, see Additional Information section for more information

Resetting iDRAC7 to Default Settings

If required, the iDRAC7 can be reset to its default factory settings:

1. Turn on or reboot the managed system.
2. During Power-On Self-Test (POST), press <F2> when **F2 = System Setup** appears in the upper right corner of the screen.
3. On the **System Setup Main Menu**, click **iDRAC Settings** → **Reset iDRAC Configurations to Defaults**.

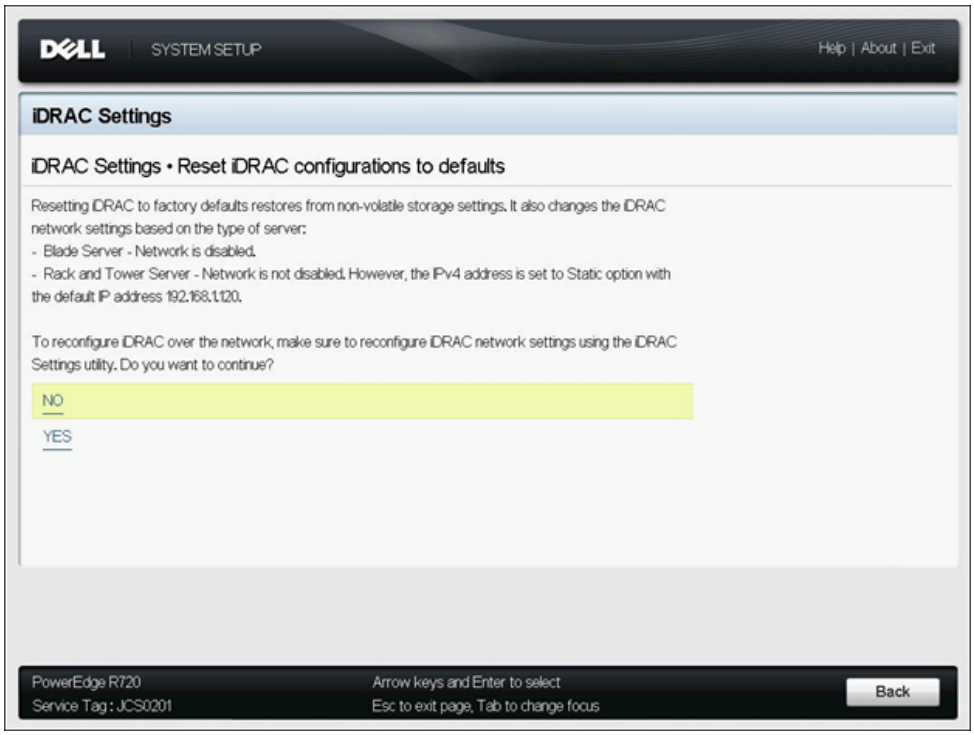

Figure 19. Reset iDRAC to Defaults Page

4. Click **Yes**. If you are working remotely, connectivity is lost while the iDRAC resets. Reset to defaults takes approximately five minutes.
5. To re-establish network connectivity to the iDRAC, you must reconfigure the network settings as mentioned in Configuring Initial iDRAC7 Network Settings section.

Additional Information

The following User's Guides are available at **dell.com/support/manuals**:

- iDRAC7 User's Guide
- Lifecycle Controller User's Guide

The following whitepapers are available at **delltechcenter.com**:

- iDRAC7 Pages and White Papers:
  - Dell 12th Generation Power Edge Server Resources
  - Agent-free Inventory and Monitoring for Storage and Network Devices in Dell PowerEdge 12th Generation Servers
  - Integrating iDRAC 7 with Microsoft Active Directory
  - iDRAC7 Networking and Improved Remote Access Performance
  - OS-to-BMC Pass-through: A New Chapter in System Manageability
  - LCD Info Screen and LED Alert Panel on PowerEdge 12th Generation Servers
- Security — New Security Features in Integrated Dell Remote Access Controller 7
- iDRAC7 Licensing:

  - Dell iDRAC7 Licensing Whitepaper - Differences between iDRAC6 and iDRAC7
  - Dell OpenManage License Manager (DLM)

- vFlash:
  - Dell vFlash: An Overview
  - Scripting vFlash Partition Management
  - Dell's vFlash SD Flash Media Card – Better Endurance and Performance via Over-Provisioning