Dell™ Unified Server Configurator User Guide

Notes and Cautions

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

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

Contents

1

Overview

The Dell™ Unified Server Configurator (USC) is an embedded configuration utility that enables systems and storage management tasks from an embedded environment throughout your system's lifecycle.

Residing on an embedded flash memory card, USC is similar to a BIOS utility in that it can be started during the boot sequence and can function independently of an installed operating system.

Using USC, you can quickly identify, download, and apply system updates without searching the Dell Support website (**support.dell.com**). You can also configure BIOS and system devices (such as NIC, RAID, and iDRAC), deploy an operating system, and run diagnostics to validate the system and attached hardware.

NOTE: Certain platforms or systems may not support the full set of features provided by USC.

What's New

The following features are new in this release of USC:

- Ability to configure the BIOS, iDRAC, and Network Interface Controllers (NICs)
- Ability to update the BIOS and iDRAC, RAID, power supply, and NIC firmware

Launching USC

To launch USC, press the <F10> key within 10 seconds of the Dell logo being displayed during the system boot process to enter **System Services**.

If your system is in one of the following states, pressing <F10> will not allow you to enter **System Services**:

- **System Services disabled** — If you power on or restart your system while iDRAC is initializing, the message System Services disabled will display during the system boot process. This situation happens if you power on your system immediately after AC is applied to the system, or if you restart the system immediately after resetting iDRAC. To avoid this issue, wait about a minute after resetting iDRAC to restart your system, thus allowing enough time for iDRAC to complete initialization.

  If the message System Services disabled still displays, then USC may have been manually disabled. See "Disabling USC" for information on how to enable USC.

- **System Services update required** — If the message System Services update required appears when you boot your system, the embedded device that stores USC may contain corrupted data. To resolve the issue, update USC by executing the USC Dell Update Package (DUP). For more information, see the *Dell Update Packages User Guide* at **support.dell.com/manuals**.

  If an operating system is not installed on the system or if executing the USC DUP does not fix the problem, run the USC repair package. See "USC Repair" for more information.

- **System Services not available** — Another process is currently using iDRAC. Dell recommends waiting 30 minutes for the current process to complete; then, reboot your system and try to enter USC again.

  NOTE: If you believe the system is in an error condition or if you cannot wait the recommended 30-minute time period, see "Canceling a Request to Enter System Services." After rebooting, try to enter USC again.

The first time you launch USC, it displays the User Settings wizard that allows you to configure your preferred language and network settings. See "Setting Up USC" for more information.

Using the USC Wizards

Wizard Description

USC provides the following wizards:

- **Platform Update** — Enables you to download and apply updates for your system. You can access the updates from **ftp.dell.com** or a USB device attached to your system. See "Updating the Platform" and "Configuring a Local USB Device for Platform Updates" for more information.

- **Hardware Configuration** — Enables you to configure system devices. See "Hardware Configuration" for more information.

- **OS Deployment** — Enables you to install an operating system. See "Deploying the Operating System" for more information.

- **Diagnostics** — Enables you to perform diagnostics to validate the memory, I/O devices, CPU, physical disks, and other peripherals. See "Running Diagnostics" for more information.

- **Settings** — Enables you to specify the language, keyboard layout, and network settings to be used with USC. See "Setting Up USC" for more information.

The USC wizards contain check boxes, text-entry boxes, and drop-down menus to assist in making your selections. The wizards also have the following buttons to assist with navigation or to cancel or complete a task:

- **Back** — Returns to the previous screen

- **Next** — Advances to the next screen

- **Cancel** — Cancels any changes made on the current screen and returns you to the **Welcome** screen

- **Finish** — Completes the configuration activity using the settings you specified

- **Apply** — Saves changes made on the current screen

Launching a Wizard

USC displays the available wizards in the left pane. Click the wizard you want to launch, and then follow the instructions displayed in the right pane.

Wizard Task Flow

When using USC for the first time, you should run the User Settings wizard. You do not need to run the User Settings wizard again unless you need to change the language, keyboard, or network settings.

After you run the User Settings wizard, Dell recommends that you run the Platform Update wizard to download and apply any updates. Be certain to run the Platform Update wizard on a frequent basis to ensure that your system is up to date.

Next, run the OS Deployment wizard and configure RAID as necessary.

Be certain to maintain your system by running diagnostics on a regular basis.

Accessing Help

Each USC screen has a **Help** button in the upper-right corner. Click the **Help** button ![?] to display help for the current screen.

Clicking the **Help** button on the **Welcome** screen displays the *Readme* file.

Updating USC

You can update to the latest version of USC using the Platform Update wizard. Dell recommends running the Platform Update wizard on a regular basis to access updates as they become available. For more information, see "Updating the Platform."

Disabling USC

You can disable USC to prevent your system from entering it on start-up.
To disable USC:

1   Press <Ctrl><e> when prompted during system start-up.

    ✎ **NOTE:** You must press <Ctrl><e> within 5 seconds of when the message displays.

    The **Firmware Setup** menu displays.

2   In the menu, navigate to **System Services**.

3   Select **Disable System Services**.

4   Save your changes and exit the **Firmware Setup** menu. The system reboots automatically.

To re-enable USC, repeat step 1 and step 2, and then select **Enable System Services**.

Canceling a Request to Enter System Services

If USC causes the system to repeatedly reboot, you can cancel a request to enter System Services.

⚠ **CAUTION: This action cancels all tasks USC is in the process of executing. Dell strongly recommends that you cancel the request to enter System Services only when absolutely necessary.**

1   Press <Ctrl><e> when prompted during system start-up.

    ✎ **NOTE:** You must press <Ctrl><e> within 5 seconds of when the message displays.

    The **Firmware Setup** menu displays.

2   In the menu, navigate to **System Services**.

3   Select **Cancel System Services**.

4   Save your changes and exit the **Firmware Setup** menu. The system reboots automatically.

Other Documents You May Need

In addition to this *User Guide*, you can find the following guides on the Dell Support website (**support.dell.com/manuals**) or on the *Dell Systems Management Tools and Documentation* DVD:

- The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides information about installing, configuring, and maintaining the Integrated Dell Remote Access Controller 6 (iDRAC6) on managed systems.

- The *Dell Systems Build and Update Utility User Guide* provides best practices in streamlining your deployment and update procedures for Dell systems.

- The *Dell Update Packages User Guide* provides information on obtaining and using Dell Update Packages (DUPs) as part of your system update strategy.

- White papers available from **support.dell.com**.

2

Setting Up USC

The User Settings wizard enables you to specify the language, keyboard layout, and network settings for Unified Server Configurator (USC).

NOTE: The user settings apply only to USC and do not apply to the system or any other application running on the system.

Step 1: Launch the User Settings Wizard

1 Start USC by booting the system and pressing the <F10> key within 10 seconds of the Dell logo being displayed.

2 Click **Settings** in the left pane.

Step 2: Select Language and Keyboard Type

NOTE: Use the up-arrow and down-arrow keys to access all options on the **Language** and **Keyboard Type** drop-down menus.

1 Select the language for USC from the **Language** drop-down menu.

2 Select the type of keyboard you are using with USC from the **Keyboard** drop-down menu.

3 Click **Finish**.

Step 3: Select Network Settings

1   Use the **NIC** drop-down menu to select the NIC card you want to configure on your system.

2   Use the **IP Address Source** drop-down menu to indicate whether you are obtaining an IP address from a DHCP server or using a static IP address.

DHCP

    a   Select **DHCP** if you are obtaining an IP address from a DHCP server.

    b   Click **Finish**. This action applies the settings you have specified and returns you to the USC **Welcome** screen.

Static IP

    a   Select **Static IP** if you are using a static IP address.

    b   Specify the following IP address properties. If you do not have this information, see your network administrator.

- IP Address
- Subnet Mask
- Default Gateway
- DNS Address

3   Click **Finish**. This action applies the settings you have specified and returns you to the USC **Welcome** screen.

3

Updating the Platform

Use the Platform Update wizard to display a list of available updates for your system. After you select the updates you want to apply, Unified Server Configurator (USC) downloads and applies the updates.

NOTE: To ensure optimal system performance and avoid system problems, Dell recommends that you download and apply updates on a regular basis.

The Platform Update wizard requires access to the Dell File Transfer Protocol (FTP) server (**ftp.dell.com**). Alternatively, your system administrator may provide the updates on a local USB device. Contact your system administrator to find out the preferred method for accessing updates in your organization. For more information, see "Configuring a Local USB Device for Platform Updates."

NOTE: If you are not using a DHCP network, you must configure the network card using the USC User Settings wizard before accessing the updates. See "Step 1: Launch the User Settings Wizard" in "Setting Up USC."

Step 1: Launch the Platform Update Wizard

1 Start USC by booting the system and pressing the <F10> key within 10 seconds of the Dell logo being displayed.

2 Click **Platform Update** in the left pane.

3 Click **Launch Platform Update** in the right pane.

Step 2: Select Download Method

You can download updates from Dell's FTP server (**ftp.dell.com**) using the Platform Update wizard or from a local USB device.

NOTE: The text boxes and drop-down menus under **FTP Server** and **USB Device** do not become active until you select the corresponding **FTP Server** or **USB Device** check box.

1 Select either **FTP Server** or **USB Device**.

FTP Server

Select **FTP Server** to download updates from Dell's FTP server using the Platform Update wizard. Enter the appropriate information according to the method you are using to access the FTP server. You must enter **ftp.dell.com** in the **Address** field.

NOTE: If you use a firewall, you should configure it to allow outgoing FTP traffic on port 21. The firewall must also be configured to accept incoming FTP response traffic.

To download updates by using a proxy server to access **ftp.dell.com**, you must specify:

- **Proxy Server** — The server host name or the IP address of the proxy server
- **Proxy Port** — The port number of the proxy server
- **Proxy Type** — The type of proxy server
- **Proxy User Name** — The user name required for authentication on the proxy server
- **Proxy Password** — The password required for authentication on the proxy server

USB Device

Select **USB Device** if you are accessing the updates from a local USB device. Select the appropriate USB device from the **USB Device** drop-down menu. See "Configuring a Local USB Device for Platform Updates" for more information.

NOTE: To access updates on a USB device, the USB device must be attached to your system before launching USC. See "Configuring a Local USB Device for Platform Updates" for information on setting up a USB device for updates.

2 Click **Next**.

Step 3: Select and Apply Updates

The **Select Updates** screen displays a list of available updates.

1 Select the check box for each update that you want to apply to the system. The components for which a more current update is available are selected by default.

   If you want to compare the version of the update with the version currently installed on the system, compare the versions in the **Current** and **Available** fields.

   NOTE: An ellipsis (…) appearing at the end of the displayed field indicates that the full value is not displayed. To view more detailed information, select the field; the information appears below the comparison report.

   • **Component** — Displays the available updates. Select the check box for each update you want to apply.

   • **Current** — Displays the component version currently installed on the system.

   • **Available** — Displays the version of the available update.

2 Click **Apply**.

NOTE: The system reboots after the update process is complete. When applying more than one update, the system may need to reboot between updates. In this case, the system boots directly into USC and continues the update process. No action on your part is required when the system reboots to complete the update process.

NOTE: If the iDRAC firmware update is interrupted for any reason, you may be required to wait for up to 30 minutes before you can attempt another firmware update.

Rolling Back to Previous BIOS and Firmware Versions

USC enables you to roll back to a previously-installed version of BIOS or firmware. Dell recommends that you use this feature if you have a problem with the currently-installed version and want to revert to the previously-installed version.

NOTE: Only BIOS and firmware can be rolled back. USC, the Dell Diagnostics application, and drivers needed for operating system (OS) installation cannot be rolled back to earlier versions.

This feature is available only if you have used the USC update feature to update BIOS and firmware, or if you have updated the system BIOS or firmware using a post-OS Dell Update Package. If you have used other update methods, this feature is not available.

NOTE: Power supply firmware does not support creation of a rollback image if it is updated using a post-OS Dell Update Package.

NOTE: If you have updated your system's BIOS or firmware only once, the rollback feature offers the option of reverting to the factory-installed BIOS or firmware images. If you have updated your BIOS or firmware more than once, the factory-installed images are overwritten and you cannot revert to them.

Step 1: Launch the Rollback Wizard

1   Boot your system to launch USC. When the Dell logo displays, press the <F10> key within 10 seconds.

2   Click **Platform Update** in the left pane.

3   Click **Launch Rollback Update** in the right pane.

Step 2: Select and Apply Rollbacks

The **Select Rollbacks** screen displays a list of available rollback images.

1   Select the check box of each rollback image that you want to apply to the system.

 To compare the version of the rollback image with the version currently installed on the system, compare the versions in the **Current** and **Previous** fields.

 📝 **NOTE:** An ellipsis (...) appearing at the end of the displayed field indicates that the full value is not displayed. To view more detailed information, select the field; the information appears below the comparison report.

 • **Component** — Displays the available updates; select the check box of each update you want to apply.

 • **Current** — Displays the component version currently installed on the system.

 • **Previous** — Displays the version of the rollback image.

2   Click **Apply**.

 📝 **NOTE:** The system reboots after the update process is complete. When applying more than one update, the system may need to reboot between updates. In this case, the system boots directly into USC and continues the update process. No action on your part is required when the system reboots to complete the update process.

Updating Devices That Affect Trusted Platform Module Settings

If BitLocker protection is enabled on your system, updating certain components requires you to enter a recovery password or insert a USB flash drive containing a recovery key during the next system boot. This situation occurs only if the Trusted Platform Module (TPM) security setting is set to **On with Pre-boot Measurements**.

NOTE: For information on how to set TPM settings, see the *BIOS User Guide* available at **support.dell.com/manuals**.

When USC detects that TPM security is set to **On with Pre-boot Measurements**, a warning message displays indicating that certain updates require the recovery password or USB flash drive with the recovery key. The warning message also indicates which components affect the BitLocker.

You may opt not to update or roll back those components by navigating to the **Select Updates** screen and deselecting the check boxes for the components.

4

Hardware Configuration

Unified Server Configurator (USC) provides two different methods for configuring your hardware, both of which are available from the main **Hardware Configuration** screen:

- **Configuration Wizards** guide you through setting up system devices. The Configuration Wizards include: Physical Security Configuration, System Date/Time Configuration, iDRAC Configuration, and RAID Configuration.

- **Advanced Configuration** allows you to configure certain devices, such as Network Interface Controllers (NICs) and the BIOS, using Human Interface Infrastructure (HII).

  NOTE: Be certain to understand the implications of HII before using the Advanced Configuration feature. HII is part of the UEFI standard; USC complies to UEFI version 2.1. See "Advanced Configuration" for more information.

Physical Security Configuration

Use the Physical Security Configuration Wizard to control access to the system control panel.

To launch the Physical Security Configuration Wizard:

1 Click **Hardware Configuration** in the left pane.

2 Click **Configuration Wizards** in the right pane.

3 Click **Physical Security Configuration** to launch the wizard.

4 Set **System Control Panel Access** to one of the following options:

- **Disabled** — You do not have access to information or control, other than the information displayed by the management controller, and you cannot specify actions.

- **View Only** — You can move through the data screens to obtain information using the system control panel interface.

- **View and Modify** — You can obtain information and make changes using the system control panel interface.

5 Click **Finish** to apply the changes.

To return to the **Configuration Wizards** screen, click **Back**.

To exit the wizard, click **Cancel**.

System Date/Time Configuration

Use the System Date/Time Configuration Wizard to set the date and time for the system.

To launch the System Date/Time Configuration Wizard:

1 Click **Hardware Configuration** in the left pane.

2 Click **Configuration Wizards** in the right pane.

3 Click **System Date/Time Configuration Wizard** to launch the wizard.

The default system date and system time shown in USC is the date and time reported by the system BIOS.

4 Modify the **System Date** and **Time** (HH:MM:SS AM/PM) values as needed.

5 Click **Finish** to apply the changes.

To return to the **Configuration Wizards** screen, click **Back**.

To exit the wizard, click **Cancel**.

iDRAC Configuration

Use the iDRAC Configuration Wizard to configure and manage iDRAC parameters.

This wizard is similar to the iDRAC Configuration Utility in the legacy BIOS operation. You can use the wizard to configure iDRAC parameters applicable to the system, such as LAN, common IP settings, IPv4, IPv6, virtual media, and LAN user configuration.

To launch the iDRAC Configuration Wizard:

1 Click **Hardware Configuration** in the left pane.
2 Click **Configuration Wizards** in the right pane.
3 Click **iDRAC Configuration** to launch the wizard.

The following steps will walk you through the iDRAC Configuration Wizard:

- Step 1: LAN Configuration
- Step 1 (Continued): Advanced LAN Configuration
- Step 2: Common IP Configuration
- Step 3: IPv4 Configuration
- Step 4: IPv6 Configuration
- Step 5: Virtual Media Configuration
- Step 6: LAN User Configuration
- Step 7: Confirmation

Step 1: LAN Configuration

View or configure iDRAC LAN, IPMI over LAN, MAC address, and NIC selection.

- **iDRAC LAN** — Enables or disables the iDRAC NIC. Disabling iDRAC LAN deactivates the remaining controls.
- **IPMI Over LAN** — Enables or disables Intelligent Platform Management Interface (IPMI) commands on the iDRAC Local Area Network (LAN) channel.
- **MAC Address** — Enables you to view the Media Access Control (MAC) address that uniquely identifies each node in a network (read-only).

- **NIC Selection** — Enables you to view or edit the NIC mode using the following mode options:

  – **Dedicated** — This option enables remote access to utilize the dedicated network interface available on the Dell Remote Access Controller (DRAC). Because the DRAC interface is not shared with the host operating system and routes management traffic to a separate physical network, it can be separated from the application traffic.

  NOTE: This option is available only if an iDRAC6 Enterprise controller is present in the system.

  – **Shared with failover** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through the LAN on motherboard LOM 1 and LOM 2, but it transmits data only through LOM 1. If LOM 1 fails, the remote access device fails over to LOM 2 for all data transmission. The remote access device continues to use LOM 2 for data transmission. If LOM 2 fails, the remote access device fails over all data transmission back to LOM 1.

  – **Shared with failover LOM 2** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through the LAN on Motherboard LOM 1 and LOM 2, but transmits data only through LOM 2. If LOM 2 fails, the remote access device fails over to LOM 1 for all data transmission. The remote access device continues to use LOM 1 for data transmission. If LOM 1 fails, the remote access device fails over all data transmission back to LOM 2.

  NOTE: If one LOM fails but is later restored, you can manually revert back to the original LOM settings by editing the NIC selection through the iDRAC Hardware Configuration wizard.

Step 1 (Continued): Advanced LAN Configuration

Set additional attributes for VLAN, VLAN ID, VLAN priority,
Auto Negotiate, LAN speed, and LAN duplex.

- **VLAN** — Enables or disables the VLAN mode of operation and
  parameters. When VLAN is enabled, only matched VLAN ID traffic is
  accepted. When disabled, VLAN ID and VLAN Priority are not available,
  and any values present for those parameters are ignored.

- **VLAN ID** — Sets the VLAN ID value. Legal values fall in the range of 1 to
  4094, as defined by IEEE 801.1g specification.

- **VLAN Priority** — Sets the VLAN ID priority value. Legal values fall in the
  range of 0 to 7, as defined by IEEE 801.11g specification.

- **Auto Negotiate** — Turns the auto-negotiate feature on or off. When
  auto-negotiate is on, it determines whether iDRAC automatically sets the
  Duplex Mode and **Network Speed** values by communicating with the
  nearest router or hub. When auto-negotiate is off, you must set the
  Duplex Mode and **Network Speed** values manually.

- **LAN Speed** — Configures the network speed to 100 Mb or 10 Mb to
  match the user's network environment.

  NOTE: This option is not available if **Auto-Negotiate** is set to **On**.

- **LAN Duplex** — Configures the duplex mode to **Full** or **Half** to match the
  user's network environment.

  NOTE: This option is not available if **Auto-Negotiate** is set to **On**.

Click **OK** to save your settings and return to the **LAN Configuration** menu.

Click **Next** to proceed to **Step 2: Common IP Configuration**.

Step 2: Common IP Configuration

Register the iDRAC name, set the domain name from DHCP, and specify the domain name and host name string.

- **Register iDRAC Name** — If set to **Yes**, the iDRAC name is registered with the Domain Name System (DNS). If set to **No**, no registration takes place.

- **iDRAC Name** — Enables you to view or edit the iDRAC name to be used when registering with DNS. The **iDRAC Name** string can contain up to 63 printable ASCII characters. You can edit the **iDRAC Name** string when **Register iDRAC Name** is **No**. The information in this field is erased after updating the iDRAC firmware.

- **Domain Name from DHCP** — If set to **Yes**, iDRAC acquires the domain name from the Dynamic Host Configuration Protocol (DHCP) server. If set to **No**, you must enter the domain name manually.

- **Domain Name** — Enables you to view or edit the iDRAC domain name to be used if it is not acquired from DHCP. You can specify a domain name when **Domain Name from DHCP** is set to **No**. The information in this field is erased after updating the iDRAC firmware. The **Domain Name** string can contain up to 256 ASCII characters.

- **Host Name String** — Enables you to specify or edit the host name associated with iDRAC. The information in this field is erased if iDRAC is reset to the original defaults or if the iDRAC firmware is updated. The **Host Name** string can contain up to 62 ASCII printable characters.

Click **Next** to proceed to **Step 3: IPv4 Configuration**.

Step 3: IPv4 Configuration

Enable or disable IPv4, and set the RMCP+ encryption key, IP address source, subnet mask, default gateway, and DNS server values.

- **IPv4** — Enables or disables iDRAC NIC IPv4 protocol support. Disabling IPv4 deactivates the remaining controls.

- **RMCP+Encryption Key** — Configures the RMCP+ encryption key using 0 to 40 hexadecimal digits (no blanks allowed). The default setting is all zeros (0).

- **IP Address Source** — Enables or disables the ability of the iDRAC NIC to acquire an IPv4 address from the DHCP server; deactivate or activate the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** controls.

- **Ethernet IP Address** — Enables you to specify or edit a static IPv4 address for the iDRAC NIC. The IP address you enter in the **Ethernet IP Address** field is reserved, and used only when DHCP fails to resolve and assign an available IP address. The **Ethernet IP Address** field is limited to a maximum value of 255.255.255.255.

- **Subnet Mask** — Enables you to specify or edit the static subnet mask for the iDRAC NIC. The subnet mask defines the significant bit positions in the IPv4 address. The **Subnet Mask** string should be in the form of a netmask, where the more significant bits are all ones (1) with a single transition to all zeros (0) in the lower-order bits. For example: 255.255.255.0. The **Subnet Mask** field is limited to a maximum value of 255.255.255.255.

- **Default Gateway** — Enables you to specify or edit the static IPv4 default gateway for the iDRAC NIC. Requests that cannot be resolved locally are routed to this address. The **Default Gateway** field is limited to a maximum value of 255.255.255.255.

- **Get DNS Servers from DHCP** — If set to **Yes**, the iDRAC NIC acquires the Domain Name System (DNS) server information from the DHCP server, and deactivates the **DNS Server 1** and **DNS Server 2** controls. If set to **No**, the iDRAC NIC does not acquire the DNS Server information from the DHCP server, and you must manually define the **DNS Server 1** and **DNS Server 2** fields.

- **DNS Server 1** — Enables you to specify or edit the static IPv4 address for a primary DNS server. This IPv4 address is that of a DNS server utilized for name-to-IPv4 address resolution. The **DNS Server 1** field is limited to a maximum value of 255.255.255.255.

- **DNS Server 2** — Enables you to specify or edit the static IPv4 address for a secondary DNS server. In the event that DNS Server 1 does not produce results, the **DNS Server 2** IPv4 address serves as a backup utilized for name-to-IPv4 address resolution. This field is limited to a maximum value of 255.255.255.255.

Click **Next** to proceed to **Step 4: IPv6 Configuration**.

Step 4: IPv6 Configuration

Set IPv6, IP address source, ethernet IP address, IPv6 address, prefix length, default gateway, and DNS server values.

- **IPv6** — Enables or disables the iDRAC NIC IPv6 protocol support. Disabling IPv6 deactivates the remaining controls.

- **IP Address Source** — Enables or disables the ability of the iDRAC NIC to acquire an IPv6 address from the DHCP server. Disabling **IP Address Source** deactivates the **Ethernet IP Address**, **Prefix Length**, and **Default Gateway** controls.

- **Ethernet IP Address** — Enables you to specify or edit the static IPv6 address for the iDRAC NIC when not provided by DHCP. This field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The multi-cast (ff00:/8) and loopback (::1/128) values are not valid addresses for the ethernet IP address and/or the other address related fields described in this section.

  IPv6 Address forms supported:

  – **X:X:X:X:X:X:X:X** — In this preferred form, **X** represents the hexadecimal values of the eight 16-bit pieces of the address. You can omit leading zeros in individual fields, but you must include at least one numeral in every field.

  – **::** (two colons) — Using this form, you can represent a string of contiguous zero fields in the preferred form. The "::" can only appear once in the address. You can also use this form to represent unspecified addresses (0:0:0:0:0:0:0:0).

  – **x:x:x:x:x:x:d.d.d.d** — This form is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes. In this form, **x** represents the hexadecimal values of the six high-order 16-bit pieces of the address, and **d** represents the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).

- **Prefix Length** — Enables you to specify or edit the number of significant bits in the IPv6 address to be used as a prefix, up to a maximum of 128. The prefix length number of bits in the Ethernet IP address is the netmask for the IPv6 network to which the iDRAC NIC belongs. The more significant bits that are defined, the fewer IPv6 addresses will be available on the network with the specified prefix.

- **Default Gateway** — Enables you to specify or edit the static IPv6 default gateway for the iDRAC NIC when not provided by DHCP. This is the address that will be used to route requests when they cannot be resolved locally. The **Default Gateway** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

- **Get DNS Servers from DHCP** — If set to **Yes**, the iDRAC NIC acquires the Domain Name System (DNS) server information from the DHCP server and deactivates the DNS Server 1 and DNS Server 2 controls. If set to **No**, the iDRAC NIC does not acquire the DNS server information from the DHCP server, and you must manually specify the **DNS Server 1** and **DNS Server 2** fields.

- **DNS Server 1** — Enables you to specify or edit the static IPv6 address for a primary DNS server when not provided by DHCP. The **DNS Server 1** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The iPv6 address is that of a DNS server utilized for name-to-IPv6 address resolution.

- **DNS Server 2** — Enables you to specify or edit the static IPv6 address for a secondary DNS server when not provided by DHCP. In the event that DNS Server 1 does not produce results, the DNS Server 2 iPv6 address serves as a backup DNS server utilized for name-to-IPv6 address resolution. The **DNS Server 2** field is limited to a maximum value of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Click **Next** to proceed to Step 5: Virtual Media Configuration.

Step 5: Virtual Media Configuration

Set Virtual Media and Virtual Flash parameters.

✐ **NOTE:** The Virtual Media and Virtual Flash features are available only if the system includes iDRAC 6 Enterprise. The Virtual Flash feature is only available if an SD card is installed and enabled in the iDRAC.

- **Virtual Media** — Select attached or detached mode. If set to **Attached**, the virtual media devices are available for use in the current operating environment. Virtual Media enables a floppy image, floppy drive, or CD/DVD drive from your system to be available on the managed systems console, as if the floppy image or drive were present (attached or connected) on the local system. If set to **Detached**, you cannot access virtual media devices.

- **Virtual Flash** — Enable or disable the use of flash memory that resides in the iDRAC file system. This memory can be used for persistent storage and accessed by the system. If set to **Enabled**, the virtual flash card is configured as a virtual drive; it appears in the boot order, allowing you to boot from the virtual flash card. If set to **Disabled**, virtual flash is not accessible.

   ✐ **NOTE:** To boot from the virtual flash, the virtual flash image must be bootable. The virtual flash feature of iDRAC requires a formatted secure digital (SD) card that is 256 MB or greater. This feature can be enabled only if a valid image is present on the SD card. See the *User Guide* for your system's iDRAC device for more information.

   ✐ **NOTE:** Dell-branded vFlash media is required for the virtual flash partition.

Click **Next** to proceed to **Step 6: LAN User Configuration**.

Step 6: LAN User Configuration

Set account access, account-related attributes, and smart card authentication.

- **Account Access** — Enables or disables account access. Disabling account access deactivates all other fields on the **LAN User Configuration** screen.

- **Account Username** — Enables the modification of an iDRAC username. The **Account Username** field accepts a maximum of 16 printable ASCII characters.

- **Password** — Enables an administrator to specify or edit the iDRAC user's password. The **Password** string is encrypted and cannot be seen or displayed after this property is set. The **Password** field accepts a maximum of 20 characters.
- **Confirm Password** — Re-enter the iDRAC user's password to confirm.
- **Account Privilege** — Assigns the user's maximum privilege on the IPMI LAN channel to one of the following user groups: Administrator, Operator, User, or No Access.
  - **Administrator** — Privileges: Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands
  - **Operator** — Privileges: Login to iDRAC, Configure iDRAC, Configure Users, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands
  - **User** — Privileges: Login to iDRAC
  - **No Access** — No assigned privileges
- **Smart Card Authentication** — Enables or disables Smart Card Authentication for iDRAC log in. If enabled, a Smart Card must be installed to access the iDRAC.
  - **Enabled** — Enabling Smart Card login disables all command-line out-of-band interfaces including SSM, Telnet, Serial, remote RACADM, and IPMI over LAN.
  - **Disabled** — On subsequent logins from the graphical user interface (GUI), the regular login page displays. All command-line out-of-band interfaces—including Secure Shell (SSH), Telnet, Serial, and RACADM—are set to their default states.
  - **Enabled with RACADM** — Enabling smart card login with RACADM disables all command-line out-of-band interfaces— including SSM, Telnet, Serial, remote RACADM, and IPMI over LAN—while still allowing RACADM access.

Click **Next** to proceed to **Step 7: Confirmation**.

Step 7: Confirmation

Confirm the changes you made by viewing the **Summary** screen. You can apply the changes, or cancel all changes and exit the iDRAC Configuration Wizard. If you apply the changes, a `Please Wait` message displays while your changes are saved. When the operation is complete, a final **Confirmation** screen displays indicating whether the changes were applied successfully, left unchanged, or failed.

Click **Finish** to save your settings and return to the main wizards screen.

RAID Configuration

If your system has one or more supported PERC RAID controller(s) with PERC 6.1 firmware or greater or SAS RAID controller(s), you have the option of using the RAID Configuration wizard to configure a virtual disk as the boot device.

To launch the RAID Configuration Wizard:

1 Click **Hardware Configuration** in the left pane.

2 Click **Configuration Wizards** in the right pane.

3 Click **RAID Configuration** to launch the wizard.

The following steps will walk you through the RAID Configuration wizard:

- Step 1: View Current Configuration
- Step 2: Select RAID Controller
- Step 2 (Continued): Foreign Configuration Found
- Step 3: Select the Express or Advanced Wizard
- Step 4: Select Basic Settings
- Step 4 (Continued): Express Wizard Only - Assign a Hot Spare
- Step 5: Express Wizard Only - Review Summary
- Step 6: Advanced Wizard Only - Select Physical Disks
- Step 7: Advanced Wizard Only - Additional Settings
- Step 8: Advanced Wizard Only - Review Summary

Step 1: View Current Configuration

The **View Current Configuration** screen displays the attributes of any virtual disks already configured on the supported RAID controllers attached to the system. You have two options:

- Accept the existing virtual disks without making changes. To select this option, click **Back**.

  NOTE: If you intend to install the operating system on an existing virtual disk, ensure that the virtual disk size and RAID level are appropriate.

- Delete all existing virtual disks and use the RAID configuration wizard to create a single, new virtual disk to be used as the new boot device. To select this option, click **Next**.

  NOTE: RAID 0 does not provide data redundancy. Other RAID levels do provide data redundancy and may enable you to reconstruct data in the event of a disk failure.

Step 2: Select RAID Controller

The **Select RAID Controller** screen displays all supported RAID controllers attached to the system. Select the RAID controller on which you want to create the virtual disk, and then click **Next**.

Step 2 (Continued): Foreign Configuration Found

The **Foreign Configuration Found** screen displays only if a foreign configuration resides on the selected RAID controller.

A foreign configuration is a set of physical disks containing a RAID configuration that has been introduced to the system but is not yet managed by the RAID controller to which it is attached. You may have a foreign configuration if physical disks have been moved from a RAID controller on another system to a RAID controller on the current system.

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

- If the foreign configuration contains data that you want to keep, select **Ignore Foreign Configuration**. If you select this option, the disk space containing the foreign configuration is not available for use in a new virtual disk.

- To delete all data on the physical disks containing the foreign configuration, select **Clear Foreign Configuration**. This option frees the disk space containing the foreign configuration and makes it available for use in a new virtual disk.

Click **Next** after making your selection.

Step 3: Select the Express or Advanced Wizard

Create a virtual disk using either the **Express Wizard** or the **Advanced Wizard**.

- The **Express Wizard** enables you to select the RAID level only. The Express Wizard then selects a virtual disk configuration for the user which implements the selected RAID level and optionally enables you to assign a hot spare. Select **Express Wizard** to quickly create a virtual disk using recommended settings.

  NOTE: Express Wizard is not available on all controllers.

  NOTE: If the available physical disks are using both Serial Attached SCSI (SAS) and Serial ATA (SATA) protocols, Dell recommends that you use the Advanced Wizard.

- The **Advanced Wizard** enables you to specify which protocol is used when creating the disk pool for the virtual disks. A disk pool is a logical grouping of disks attached to a RAID controller on which one or more virtual disks can be created. In addition to the RAID level, the Advanced Wizard allows more flexibility with physical disk selection, span configuration, cache policy, and other virtual disk attributes. Select **Advanced Wizard** to specify all virtual disk settings.

  NOTE: Dell recommends a good knowledge of RAID and your hardware configuration to use the Advanced Wizard.

Click **Next** after making your selection.

Step 4: Select Basic Settings

Select the RAID type for the virtual disk from the **RAID Level** drop-down menu:

- **RAID 0** — Stripes data across the physical disks. RAID 0 does not maintain redundant data. When a physical disk fails in a RAID 0 virtual disk, there is no method for rebuilding the data. RAID 0 offers good read and write performance with 0 data redundancy.

- **RAID 1** — Mirrors or duplicates data from one physical disk to another. If a physical disk fails, data can be rebuilt using the data from the other side of the mirror. RAID 1 offers good read performance and average write performance with good data redundancy.

- **RAID 5** — Stripes data across the physical disks, and uses parity information to maintain redundant data. If a physical disk fails, the data can be rebuilt using the parity information. RAID 5 offers good read performance and slower write performance with good data redundancy.

- **RAID 6** — Stripes data across the physical disks, and uses two sets of parity information for additional data redundancy. If one or two physical disks fail, the data can be rebuilt using the parity information. RAID 6 offers better data redundancy and read performance but slower write performance with very good data redundancy.

- **RAID 10** — Combines mirrored physical disks with data striping. If a physical disk fails, data can be rebuilt using the mirrored data. RAID 10 offers good read and write performance with good data redundancy.

NOTE: For PERC controllers, RAID 50 and RAID 60 virtual disks cannot be created when using the RAID Configuration Wizard in USC. If you want to create RAID 50 and RAID 60 virtual disks, use the controller utilities such as <Ctrl><R> or *Systems Build and Update Utility*.

NOTE: The virtual disk size is automatically calculated and displayed in the **Size** field. You cannot change the virtual disk size.

If you are using the Express Wizard, proceed to "Step 4 (Continued): Express Wizard Only - Assign a Hot Spare."

If you are using the Advanced Wizard, click **Next** and proceed to "Step 6: Advanced Wizard Only - Select Physical Disks."

Step 4 (Continued): Express Wizard Only - Assign a Hot Spare

To assign a hot spare to the virtual disk, select the **Assign a Hot Spare Disk** check box; otherwise, leave the check box clear.

NOTE: A hot spare is an unused backup physical disk that can be used to rebuild data from a redundant virtual disk. A hot spare can be used only with a redundant RAID level. Hot spares also have requirements for physical disk size. The hot spare must be as big as or bigger than the smallest physical disk included in the virtual disk. If the RAID level and physical disk availability do not meet these requirements, a hot spare will not be assigned.

Click **Next** to continue with "Step 5: Express Wizard Only - Review Summary."

Step 5: Express Wizard Only - Review Summary

Review the virtual disk attributes you selected before creating a virtual disk.

CAUTION: Clicking the Finish button deletes all existing virtual disks except for any foreign configurations that you specified should be kept. All data residing on the deleted virtual disks will be lost.

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

OR

To return to a previous screen to review or change selections, click **Back**. To exit the Wizard without making changes, click **Cancel**.

NOTE: For more control over the virtual disk attributes, click Cancel and use the Advanced Wizard to create the virtual disk.

Step 6: Advanced Wizard Only - Select Physical Disks

Use the **Select Physical Disks** screen to select the physical disks to be used for the virtual disk. The number of physical disks required for the virtual disk varies depending on the RAID level. The minimum and maximum numbers of physical disks required for the RAID level are displayed on the screen.

- Select the protocol for the disk pool from the **Protocol** drop-down menu: **Serial Attached SCSI (SAS)** or **Serial ATA (SATA)**. SAS drives are used for high performance, and SATA drives provide a more cost-effective solution.

  NOTE: A disk pool is a logical grouping of physical disks on which one or more virtual disks can be created. The protocol is the type of technology used to implement RAID.

- Select the media type for the disk pool from the **Media Type** drop-down menu: **Hard Disk Drives (HDD)** or **Solid State Disks (SSD)**. HDDs use traditional rotational magnetic media for data storage, and SSDs implement flash memory for data storage.

- Select the span length from the **Select Span Length** drop-down menu. The span length value refers to the number of physical disks included in each span.

  NOTE: Span length applies only to RAID 10. The **Select Span Length** drop-down menu is active only if the user has selected RAID-10.

- Select the physical disks using the check boxes at the bottom of the screen. Your physical disk selection must meet the requirements of the RAID level and span length. To select all of the physical disks, click **Select All**.

Click **Next** after making your selections.

Step 7: Advanced Wizard Only - Additional Settings

Use the **Additional Settings** screen to specify cache policies and stripe element size. You can also assign a hot spare to the virtual disk.

📝 **NOTE:** The virtual disk size is automatically calculated and displayed in the **Size** field. The user cannot change the virtual disk size.

- Select the stripe element size from the **Stripe Element Size** drop-down menu. The stripe element size is the amount of disk space a stripe consumes on each physical disk in the stripe.

  📝 **NOTE:** The **Stripe Element Size** drop-down menu may contain more options than initially displayed on the screen. Use the up-arrow and down-arrow keys to display all options.

- Select the read policy from the **Read Policy** drop-down menu.

  - **Read Ahead** — The controller reads sequential sectors of the virtual disk when seeking data. The Read Ahead policy may improve system performance if the data is written to sequential sectors of the virtual disk.

  - **No Read Ahead** — The controller does not use the Read Ahead policy. The No Read Ahead policy may improve system performance if the data is random and not written to sequential sectors.

  - **Adaptive Read Ahead** — The controller initiates the Read Ahead policy only if the most recent read requests accessed sequential sectors of the disk. If the recent read requests accessed random sectors of the disk, then the controller uses the No Read Ahead policy.

- Select the write policy from the **Write Policy** drop-down menu.

  – **Write Through** — The controller sends a write-request completion signal only after the data is written to the disk. The Write Through policy provides better data security than the Write Back policy since the system assumes the data is available only after it has been written to the disk.

  – **Write Back** — The controller sends a write-request completion signal as soon as the data is in the controller cache but has not yet been written to disk. The Write Back policy may provide faster write performance, but it also provides less data security since a system failure could prevent the data from being written to disk.

  – **Force Write Back** — The write cache is enabled regardless of whether the controller has an operational battery. If the controller does not have an operational battery, data loss may occur in the event of a power failure.

- To assign a hot spare to the virtual disk, select the **Assign a Hot Spare Disk** check box. A hot spare is an unused backup physical disk that can be used to rebuild data from a redundant virtual disk.

- Select the physical disk to be used as the hot spare from the **Hot Spare Disk** drop-down menu.

  > **NOTE:** A hot spare can be used only with a redundant RAID level. Hot spares also have requirements for physical disk size. The hot spare cannot be smaller than the smallest physical disk included in the virtual disk. If the RAID level and physical disk availability do not meet these requirements, the **Assign a Hot Spare Disk** check box is disabled.

Click **Next** after making your selection.

Step 8: Advanced Wizard Only - Review Summary

The Summary step displays the virtual disk attributes based on your selections.

> ⚠ **CAUTION: Clicking the Finish button deletes all existing virtual disks except for any foreign configurations that you specified should be kept. All data residing on the deleted virtual disks will be lost.**

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

OR

To return to a previous screen to review or change selections, click **Back**. To exit the Wizard without making changes, click **Cancel**.

Advanced Configuration

Use Advanced Configuration to modify advanced settings.

1 Select **Hardware Configuration** from the left menu

2 Click **Advanced Configuration** in the right panel.

3 Select the device you want to configure.

USC Hardware Configuration allows you to configure other devices through Human Interface Infrastructure (HII). HII is a UEFI-standard method for viewing and setting a device's configuration. You can utilize a single utility to configure multiple devices that had different pre-boot configuration utilities in the past. HII also provides localization, meaning that utilities that were previously English-only, such as the BIOS <F2> setup, may now have a localized HII equivalent.

As of the current release of USC, your server's default configuration contains setups for two device types that are supported in the Hardware Configuration Advanced Configuration: the system **BIOS** and **NIC**.

- The **BIOS** setup is very similar to the current setup utility (accessible by pressing the <F2> key during system startup); however, HII can access only a subset of the utilities available in system startup.

- The **NIC** setup reflects various NIC attributes, some of which were visible in the controller option read-only memory (ROM). However, many of these attributes were previously only modifiable in Operating System utilities.

NOTE: Integrated Broadcom NICs are controlled both by the BIOS and by settings stored on the device itself. As a result, the **Boot Protocol** field in the HII of integrated NICs has no effect; this setting is instead controlled by the BIOS on the **Integrated Devices** screen. To set integrated NICs to an iSCSI or PXE boot mode, select **System BIOS Settings**, then select **Integrated Devices**. On this screen, you will see a list of each embedded NIC—select the appropriate value: **Enabled** for no boot capability, **Enabled with PXE** to use the NIC for PXE boot, or **Enabled with iSCSI** to use the NIC to boot from an iSCSI target.

Depending on your system configuration, other device types may also appear in Advanced Configuration, if they support the HII configuration standard.

5

Deploying the Operating System

The OS Deployment wizard assists you in installing an operating system on the current system.

Unified Server Configurator (USC) provides drivers that may be required for operating system installation, depending on which operating system you are installing. The OS Deployment wizard extracts these drivers and copies them to a staging directory. For supported Microsoft® Windows® operating systems, these extracted drivers are installed during the operating system installation. For supported Linux operating systems, you must manually install the extracted drivers after the operating system installation is complete. See "Deploy the Operating System" for more information.

NOTE: Although USC comes with embedded drivers that are factory installed, there may be more current drivers available. You should run the Platform Update wizard to ensure that you have the most current drivers before installing the operating system.

Before installing the operating system, the OS Deployment wizard detects if a boot device is available. A boot device is a physical disk, virtual disk, or other storage device on which the operating system can be installed.

If your system has a RAID controller, you can configure a virtual disk and choose to use the virtual disk as the boot device.

If your system does not have a RAID controller or if you choose to bypass the optional RAID configuration, the OS Deployment wizard installs the operating system to a default location, which is typically the disk identified as Disk 0 in the BIOS utility.

Launch the Operating System Deployment Wizard

1   Start USC by booting the system and pressing the <F10> key within 10 seconds of the Dell logo being displayed.

2   Click **OS Deployment** in the left pane.

3   Click **Deploy OS** in the right pane.

If your system has a RAID controller, continue with "Optional RAID Configuration." If your system does not have a RAID controller, continue with "Step 1: Select an Operating System."

Optional RAID Configuration

If your system has a RAID controller, you have the option of launching the RAID Configuration wizard and configuring a virtual disk as the boot device.

📝 **NOTE:** If your system does not have a RAID controller, the OS Deployment wizard bypasses the RAID configuration option and goes directly to "Step 1: Select an Operating System."

To configure RAID:

- Select **Configure RAID Now** and click **Next**. This option launches the RAID Configuration wizard. After RAID configuration is complete, you will return to the OS Deployment wizard. See "RAID Configuration" for more information on launching and using the RAID Configuration wizard.

To bypass RAID configuration:

- Select **Go Directly to OS Deployment** and click **Next**. This option launches the OS Deployment wizard. If you select this option, the operating system will be installed on the default boot device identified in the BIOS utility. Continue with "Step 1: Select an Operating System."

Deploy the Operating System

USC provides drivers that may be required by the operating system being installed or that are recommended for updating your system after installation. These drivers are extracted to a temporary location and then deleted after an 18-hour period or when pressing the <F10> key to either cancel operating system installation or re-enter USC after rebooting.

📝 **NOTE:** During the 18-hour period when the drivers are extracted to the temporary location, you cannot update the USC, drivers, or diagnostics using a DUP after the operating system is installed, or the DUP will display a message that another session is open.

📝 **NOTE:** You should run the Platform Update wizard to ensure that you have the most current drivers before installing the operating system.

Step 1: Select an Operating System

Select the operating system you want to install and click **Next**.

USC extracts the drivers required by the operating system you selected. The drivers are extracted to an internal USB drive named `OEMDRV`.

NOTE: For Red Hat® Enterprise Linux® 4.*x* server and Red Hat Enterprise Linux 5.*x* server, the drivers are extracted to `OEMDRV` under `/oemdrv/*.rpm`. For SUSE® Linux Enterprise Server 10 SP2, the drivers are extracted under `/linux/suse/x86_64-sles10/install/*.rpm`.

NOTE: The process for extracting the drivers may take several minutes.

NOTE: All drivers copied by the OS Deployment wizard are removed after 18 hours. You must complete the operating system installation within 18 hours for the copied drivers to be available. To remove the drivers before the 18-hour period is over, reboot the system and press the <F10> key to re-enter USC. Using the <F10> key to cancel the operating system installation or to re-enter USC upon reboot removes the drivers during the 18-hour period.

After the drivers are extracted, USC prompts you to insert the operating system installation media.

NOTE: When installing the Microsoft Windows operating system, the extracted drivers are automatically installed during the operating system installation. When installing the Linux operating system, the operating system installation uses native drivers. After the Linux installation is complete, you need to manually install the drivers extracted by USC. See "Step 4: Update Drivers for Linux Systems Only" for more information.

Step 2: Insert the Operating System Media

Insert the operating system installation media when prompted and click **Next**.

NOTE: USC supports internal SATA optical drives, USB optical drives, and virtual media devices. If the installation media is corrupt or not readable, then USC may be unable to detect the presence of a supported optical drive. In this case, you may receive an error message stating that no optical drive is available. If the media is not valid (if it is the incorrect CD or DVD, for example), a message displays requesting that you insert the correct installation media.

NOTE: Virtual media is supported through iDRAC. For more information on setting up virtual media through iDRAC, see the *User Guide* for your system's iDRAC device.

Step 3: Reboot the System

Click **Finish** to reboot the system and continue with the operating system installation. Upon reboot, the system boots to the operating system installation media.

⚠ **CAUTION: During Red Hat 5.x installation, you will receive a warning that a read-only file system was detected; Linux has detected the temporary storage area of USC that stores updates for your system. Click OK, and a second warning will appear indicating that the read-only file system has a loop partition layout and that it needs to be formatted. Click the Ignore drive button. You may see both warnings several times during the course of Red Hat 5.x installation.**

⚠ **CAUTION: During the beginning of Windows 2003 installation, the installer will automatically detect and possibly assign the default drive letter C to the USC temporary storage device OEMDRV. Creating a new Windows-bootable system partition on the hard drive will assign the partition to a drive letter other than C; this is standard Windows installer behavior. To assign the new partition to C, see "Assign a Windows-Bootable System Partition to the C: Drive" for more information.**

✍ **NOTE:** When the system reboots after you click Finish, you may be prompted to press a key before booting to the operating system installation media. If you do not press a key, the system boots to the hard drive and not the operating system installation media.

✍ **NOTE:** In the event that the operating system installation is interrupted and the system reboots before installation completes, you may be prompted to press a key in order to boot from the operating system installation media.

✍ **NOTE:** You can cancel the operating system installation by pressing the <F10> key. Be aware that pressing the <F10> key at any point during the installation process or while rebooting causes any drivers provided by the OS Deployment wizard to be removed.

✍ **NOTE:** Windows 2008 UEFI operating system installations are not currently supported.

Step 4: Update Drivers for Linux Systems Only

On the following operating systems, Dell recommends that you update your system with the extracted drivers after installation. The drivers are extracted to a drive (or device) named OEMDRV.

- Red Hat Enterprise Linux 4.7 server — The location of the drivers on the OEMDRV drive after installation is:

  `/oemdrv/*.rpm`

- Red Hat Enterprise Linux 5.2 server — The location of the drivers on the OEMDRV drive after installation is:

  `/oemdrv/*.rpm`

- SUSE Linux Enterprise Server 10 with Service Pack 2 — The location of the drivers on the OEMDRV drive after installation is:

  `/linux/suse/x86_64-sles10/install/*.rpm`

Use the following command to install the drivers:

`rpm -Uvh *.rpm`

Assign a Windows-Bootable System Partition to the C: Drive

After you have completed the USC portion of Windows 2003 Server installation, your server will reboot and begin the text-mode portion of the installation. During this phase, you may need to perform the following steps to ensure Windows installs to your C: drive.

NOTE: Follow these instructions after Windows 2003 Server Setup presents you with a list of existing drive partitions and/or unpartitioned space available on your computer.

1 Select the unpartitioned space, and then press <c> to create a hard-disk partition. Follow the on-screen instructions to create a partition.

2 Select the newly-created partition, and then press <d> to delete the partition. Follow the on-screen instructions to delete the partition.

3 Select the unpartitioned space again, and then press <c> to create a primary hard-disk partition. Follow the on-screen instructions to create a partition. Windows will now install on the C: drive.

For more information on assigning the Windows-bootable system partition to the C: drive, see **http://support.microsoft.com/kb/896536**.

6

Running Diagnostics

The **Diagnostics** utility enables you to run a diagnostics utility from Unified Server Configurator (USC).

When to Run Diagnostics

Dell recommends that you run diagnostics as part of a regular maintenance regimen to validate that the system and attached hardware are functioning properly. Because the diagnostics utility has a physical (as opposed to logical) view of attached hardware, this utility may be able to identify hardware problems that the operating system and other online tools cannot. You can use the diagnostics utility to validate the memory, I/O devices, CPU, physical disks, and other peripherals.

Performing Diagnostics

To start the diagnostics utility, click **Diagnostics** in the left pane and click **Launch Diagnostics** in the right pane. When the diagnostics utility launches, follow the prompts on the screen.

NOTE: You must reboot your system to exit the Diagnostics utility and re-enter USC.

The results of the diagnostics tests are displayed on the screen when the tests complete. The test results describe the problems found. You can use this information to search the Dell Support website at **support.dell.com** for details on resolving the problem.

If you want to exit the diagnostics utility, press the <Esc> key. Pressing the <Esc> key causes the system to reboot.

Updating the Diagnostics Utility

Use the Platform Update wizard to update the diagnostics utility. See "Updating the Platform" for more information.

7

Configuring a Local USB Device for Platform Updates

If your organization's users are on a private network that cannot access external sites like **ftp.dell.com**, you can provide platform updates from a locally-configured USB device.

NOTE: The USB device you use as a platform update repository must be able to hold at least 3 GB of content.

NOTE: A USB device is not required for users that have access to **ftp.dell.com** through a proxy server.

NOTE: For the latest platform updates, download the most recent *Server Update Utility* ISO for your system from the Dell Support website at **support.dell.com**.

Creating the Local USB Repository

To create a platform update repository on a local USB device:

1 Download the *Server Update Utility* ISO for your system from **support.dell.com**, and burn it to a DVD.

2 Copy all files in the **repository** folder of the DVD you just created to the root directory of the USB device.

3 Create a folder named **catalog** in the root directory of the USB device. Move the files **catalog.xml.gz** and **catalog.xml.gz.sign** from the root directory of the USB device to the **catalog** folder you just created.

4 Communicate the requirements and steps for accessing the local USB device to your users. See "Accessing Updates on a USB Device."

Accessing Updates on a USB Device

When the Platform Update wizard prompts the user to specify the online repository, the user should select the **USB Device** check box and then select the appropriate USB device from the **USB Device** drop-down menu.

📝 **NOTE:** The user should connect the USB device to the system before the system boots into USC. If the USB device is not connected before launching USC, USC will not be able to access the updates.

8

USC Repair

The Unified Server Configurator (USC) repair package restores embedded tools and utilities in the event of a hardware failure or flash memory corruption. Such failures can occur for many reasons, including power loss or interruption of an update process.

When to Run USC Repair

If the message System Services update required appears when you boot up, the embedded device that stores USC may contain corrupted data. To resolve the issue, you must first attempt to update USC by executing the USC Dell Update Package (DUP); see the *Dell Update Packages User Guide* available at **support.dell.com/manuals** for more information. If executing the DUP does not solve the problem, you must use the USC repair package.

Performing a USC Repair

1 Go to **ftp.dell.com** and download the file named "Unified Server Configurator - Lifecycle Controller Enabled Repair Package" to a temporary location.

2 Connect to iDRAC on your system using the iDRAC Web interface.

   For more information on iDRAC, see the *User Guide* for your system's iDRAC device.

3 From the iDRAC Web interface, click **Remote Access**.

4 Select **iDRAC**.

5 Select the **Update** tab, and then browse to the USC Repair Package you downloaded from **ftp.dell.com**.

6 Click **Next**, and then click **OK** to confirm the upload.

   Allow the process to complete before you continue to step 7.

7 Reboot your system, and then press the <F10> key to enter USC.

8 Complete the installation of all recommended updates. See "Updating the Platform" for more information.

When updates are complete, your system automatically reboots.

9 While the system reboots, press the <F10> key again to enter USC.

If a warning message appears on the initial USC screen, you must repeat step 8 until the server is in a fully-recovered state.

NOTE: Updates that are required for a complete system recovery are pre-selected by USC. Dell highly recommends running all selected updates on your system.

9

Troubleshooting

This chapter describes the error messages commonly generated by Unified Server Configurator (USC), and provides suggestions for resolving the errors. It also answers questions that are frequently asked by USC users.

Error Messages

Table 9-1.   USC Error Messages

Error Message	Resolution
Drivers pack not found OR Error populating OS list	USC cannot find the drivers required to install the operating system. To resolve this issue, perform a platform update (see "Updating the Platform").
Unable to copy driver files	The drivers required to install the operating system are corrupted. To resolve this issue, perform a platform update (see "Updating the Platform").
Unable to find a boot device on which to install the operating system	USC does not detect a device on which an operating system can be installed. One of the following situations is probably causing the error: • The drives are not properly connected. • There are no recognized storage controllers on the system. • The on-board SATA controller is disabled in the BIOS. To resolve this issue, click **Exit and Reboot** and shut down the system. Then, make sure you have at least one device on which to install an operating system before launching USC again.

Table 9-1. USC Error Messages *(continued)*

Error Message	Resolution
Unable to find a device capable of reading the OS install media	USC cannot detect a device to read the operating system media. One of the following situations is probably causing the error:
	• No optical device is available on the system. Shut down the system and add a SATA optical device or USB optical device.
	• If an optical device is present, it may not be properly connected. Check to ensure the device cables are adequately seated.
	• If an optical device is present, it is disabled in the BIOS. Reboot the system, enter the BIOS setup utility, and enable the SATA ports for the optical device.
	• iDRAC virtual media is disabled. See the *iDRAC User Guide* for your system available at **support.dell.com/manuals**.
The inserted OS media is invalid	The operating system media is damaged or corrupted, or the optical device used to read the media is not functioning correctly.
The repository you selected as a source for the updates has failed an integrity check	This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.
The updates you are trying to apply are not Dell-authorized updates	USC has detected that one or more of the DUPs used to update your system are not Dell authorized. If you are using a local USB device for your update repository and this problem persists, create it again using DUPs from the *Server Update Utility* DVD (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.

Table 9-1.   USC Error Messages *(continued)*

Error Message	Resolution
Decompression of the catalog file failed	The catalog downloaded to compare currently installed versions with the latest available versions cannot be decompressed. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.
File seek of catalog archive failed	The catalog downloaded to compare currently installed versions with the latest available versions is corrupt. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.
FTP download of catalog sign file failed	The catalog downloaded to compare currently installed versions with the latest available versions has failed the digital signature verification check. This error may be caused by temporary network problems; try again later to connect to the update repository. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.
Fatal error launching USC has occurred. The system will reboot.	A fatal error occurred when launching USC. The system will automatically reboot and attempt to enter USC again. If the problem persists after rebooting, see "USC Repair."
Unable to resolve host name	This error is probably caused by one of the following: • You have specified an invalid name for the platform update FTP server. See "Step 2: Select Download Method" in "Updating the Platform." • The Domain Name Server (DNS) specified in the **Network Settings** page is invalid. See "Setting Up USC."

Table 9-1. USC Error Messages *(continued)*

Error Message	Resolution
Network is not configured	Network settings must be configured for USC to work correctly. See "Setting Up USC" for information on configuring USC network settings from the **Network Settings** page.
DUP corrupted	USC has detected that one or more of the DUPs used to update your system is corrupted. If you are using a local USB device for your update repository and this problem persists, create the repository again (see "Configuring a Local USB Device for Platform Updates") or provide an alternate repository.
Invalid Proxy Server	The proxy server specified to access the FTP server is invalid. See "Step 2: Select Download Method" in "Updating the Platform."
Please enter a valid Encryption Key of up to 40 Hex digits	Enter a valid encryption key that contains no more than 40 hex digits. Valid characters are within the ranges of 0–9, a–f, and A–F.
Please enter a valid IPv4 Address for this iDRAC	Enter a valid IPv4 protocol address for iDRAC that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid Subnet Mask	Enter a valid Subnet Mask that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid Default Gateway Address	Enter a valid default gateway address that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid IPv4 DNS Server 1 Address	Enter a valid IPv4 DNS Server1 address that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid IPv4 DNS Server 2 Address	Enter a valid IPv4 DNS Server2 address that is between 0.0.0.0 and 255.255.255.255.
Please enter a valid IPv6 Address for this iDRAC	Enter a valid IPv6 network address for iDRAC. See "Step 4: IPv6 Configuration" in "iDRAC Configuration."
Please specify the IPv6 network address prefix length in the range of 1 to 128	Enter the number of significant bits in the IPv6 address prefix for your network. The prefix length should be between 1 and 128. See "Step 4: IPv6 Configuration" in "iDRAC Configuration."

Table 9-1.   USC Error Messages *(continued)*

Error Message	Resolution
Please enter the IPv6 Default Gateway address	Enter the IPv6 default gateway address. See "Step 4: IPv6 Configuration" in "iDRAC Configuration."
Please enter a valid IPv6 DNS Server 1 Address	Enter a valid IPv6 DNS Server1 address. See "Step 4: IPv6 Configuration" in "iDRAC Configuration."
Please enter a valid IPv6 DNS Server 2 Address	Enter a valid IPv6 DNS Server2 address. See "Step 4: IPv6 Configuration" in "iDRAC Configuration."
Please enter a valid iDRAC Name of up to 63 characters	Enter a valid iDRAC name that is less than or equal to 63 characters.
Please enter a valid Domain Name of up to 64 characters	Enter a valid domain name that is less than or equal to 64 characters.
Please enter a valid Host Name of up to 62 characters	Enter a valid host name that is less than or equal to 62 characters.
Please enter a value in the range of 1 to 4094	Enter a VLAN ID between 1 and 4094. See "Step 1 (Continued): Advanced LAN Configuration" in "iDRAC Configuration."
Please enter a value in the range of 0 to 7	Enter a VLAN ID priority value between 0 and 7. See "Step 1 (Continued): Advanced LAN Configuration" in "iDRAC Configuration."
Account access change failed. Multiple user accounts required. See help for details.	You must create another user account. Click the **Help** button in the upper-right corner of the screen for more information.
Please enter a valid Username	You must enter a valid user name. To maintain compatibility with other iDRAC configuration tools, Dell recommends using only digits (0–9), alphanumeric characters (a–z, A–Z), and hyphens (–) in the user name string.
Please enter a valid Password	You must enter a valid password. To maintain compatibility with other iDRAC configuration tools, Dell recommends using only digits (0–9), alphanumeric characters (a–z, A–Z), and hyphens (–) in the password string.

Table 9-1. USC Error Messages *(continued)*

Error Message	Resolution
Please enter a valid Confirmation password	You must re-enter the new password and the confirmation password. Be certain that both passwords are exactly the same.
iDRAC communication failure. Please power down, unplug the system, wait 5 seconds, apply power and power on	Communication with iDRAC has failed. To resolve this issue: **1** Turn off the system, and then unplug it. **2** Wait 5 seconds. **3** Plug the system back in, and then turn it on.
iDRAC hard failure. Please power down, unplug the system, wait 5 seconds, apply power and power on	Connection with iDRAC has failed. To resolve this issue: **1** Turn off the system, and then unplug it. **2** Wait 5 seconds. **3** Plug the system back in, and then turn it on.
RAID configuration failed	USC failed when creating the RAID configuration. To resolve this issue: **1** Reboot the system. **2** Re-enter USC by pressing the <F10> key. **3** Try again to create the RAID configuration.
Generic Failure	USC experienced an unidentified error when creating the RAID configuration. To resolve this issue: **1** Reboot the system. **2** Re-enter USC by pressing the <F10> key. **3** Try again to create the RAID configuration.
Sufficient physical disks not available on any supported RAID controller. The wizard will exit.	You do not have a sufficient number of disks to support RAID configuration—you must attach more physical disks and start the RAID Configuration wizard again.
Please select required number of physical disk(s) for current span	The number of physical disks you selected for the current RAID span is incorrect. Review your span selections, and enter the correct number.

Table 9-1.   USC Error Messages *(continued)*

Error Message	Resolution
No physical disk has been selected for this virtual disk	The number of physical disks you selected for the virtual disk is insufficient. Review the minimum number of physical disks required for the current RAID level, and select at least that number of physical disks.
No controller is present in the system	No RAID controller is present in your system. To resolve this issue: **1** Add a supported RAID controller that includes two or more physical disks. **2** Re-enter USC by pressing the <F10> key. **3** Restart the RAID Configuration wizard.
No valid RAID level found	The number of physical disks attached to your system is insufficient for the RAID level you selected. Attach more physical disks and try again.
An error occurred. One or more settings may not be saved.	An error occurred when changing Hardware Advanced Configuration settings. To resolve this issue: **1** Reboot the system. **2** Re-enter USC by pressing the <F10> key. **3** Change the settings again.
An error occurred. One or more settings may not be restored.	An error occurred when restoring Hardware Advanced Configuration settings. To resolve this issue: **1** Reboot the system. **2** Re-enter USC by pressing the <F10> key. **3** Re-open the **Advanced Configuration** screen.
Unable to set new date and time	USC was unable to change the system date and time. To resolve this issue: **1** Reboot the system. **2** Re-enter USC by pressing the <F10> key. **3** Change the date and time settings again.
This feature is not supported in this configuration	Your modular system does not support the feature you selected.

Frequently Asked Questions

When USC downloads updates, where are the files stored?

The files are stored in non-volatile memory, located on the main system board. This memory is not removable and is not accessible through the operating system.

Is a virtual media device or vFlash card required to store data for updates?

No. The files are stored in memory on the main system board.

What is virtual media?

Virtual media is remote media—like CDs, DVDs, and USB keys—that a server identifies as local media.

What is vFlash or virtual flash?

vFlash is a formatted SD (Secure Digital) card that plugs into iDRAC6 Enterprise. vFlash can be formatted and enabled via iDRAC to make it accessible as a USB key for data storage. Virtual flash is a partition on vFlash to which you can remotely write an ISO. See the *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise User Guide* available at **support.dell.com/manuals** for more information.

Can I add my own drivers to use for operating system installation?

No. You cannot add your own drivers for operating system installation. See "Updating the Platform" for more information on updating the drivers that are used for operating system installation.

Can I update the drivers used by an installed operating system through USC?

No. USC only provides drivers that are required for operating system installation. To update the drivers used by an installed operating system, see your operating system's help documentation.

Can I add my own drivers and firmware for updating USC to a local USB device?

No. Only drivers and firmware downloaded from the *Server Update Utility* DVD are supported. See "Configuring a Local USB Device for Platform Updates" for more information.

Can I delete USC?

No.

Can I use virtual media for the operating system media source during installation?

Yes. See the *User Guide* for your system's iDRAC device for more information (available at **support.dell.com/manuals**).

Can I use a virtual USB for my update repository?

Yes. See the *User Guide* for your system's iDRAC device for more information (available at **support.dell.com/manuals**).

What is UEFI? With which version does USC comply?

UEFI (Unified Extensible Firmware Interface) is a specification that details an interface for transitioning control from the pre-boot environment to the operating system. USC 1.1 complies with UEFI version 2.1. See **www.uefi.org** for more information.

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

USC offers two ways to configure hardware: *Configuration Wizards* and *Advanced Configuration*.

Configuration Wizards guide you through a sequence of steps to configure your system devices. The Configuration Wizards include iDRAC, RAID, System Date/Time, and Physical Security. See "Hardware Configuration" for more information.

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

Does USC support configuration of all RAID levels and all 11G RAID cards?

USC supports RAID levels 0, 1, 5, 6, and 10 on PERC 6 cards running PERC 6.1 firmware. RAID 0 and 1 are supported on the SAS 6/iR. RAID-50 and RAID-60 currently are not supported through USC; to configure these levels, use controller utilities such as <Ctrl><R> or the Systems Build and Update Utility.

Does USC support rollback of BIOS and firmware?

Yes. See "Rolling Back to Previous BIOS and Firmware Versions" for more information.

Which devices support system updates?

USC currently supports updates to the BIOS, iDRAC firmware, power supply firmware, and certain RAID and NIC controller firmware. See "Updating the Platform" for more information.

Which devices are supported in Advanced Configuration within Hardware Configuration?

Advanced Configuration is available for the BIOS and NIC. Depending on your system configuration, other devices may also appear in Advanced Configuration if they support the HII configuration standard. See "Hardware Configuration" for more information.

What should I do if my system crashes while using USC?

If your system crashes while using USC, a black screen with red text will appear. To resolve this problem, first try rebooting your system and re-entering USC. If that does not resolve the problem, perform the steps in "USC Repair." If that does not resolve the problem, contact Dell for technical assistance.

Glossary

BitLocker — A full disk encryption feature included with the Microsoft® Windows Server® 2008 operating system that encrypts entire volumes.

controller — A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device, such as a disk drive or the keyboard. RAID controllers perform RAID functions, such as striping and mirroring to provide data protection.

disk pool — A logical grouping of disks attached to a RAID controller on which one or more virtual disks can be created.

drive — See *physical disk*.

DUP — Dell Update Package. A self-contained executable in a standard package format. Each Update Package is designed to update a single software component on your system.

hard disk drive — See *physical disk*.

HDD — Hard disk drive. See *physical disk*.

HII — Human Interface Infrastructure. HII is a UEFI-standard method for viewing and setting a device's configuration.

hot spare — A physical disk that is available to aid in recovery of a logical drive.

hard disk — See *physical disk*.

logical drive — See *virtual disk*.

physical disk — A non-volatile, randomly addressable device for storing data. Physical disks are rewritable and commonly referred to as disk drives.

RACADM — A command-line utility that provides a scriptable interface that allows you to locally or remotely configure a remote access controller (RAC).

RAID — Redundant Array of Independent Disks

SAS — Serial Attached SCSI

SATA — Serial ATA

SBUU — System Build and Update Utility. An integrated tool for your Dell systems that enables you to update BIOS and firmware in the pre-operating system environment, apply these settings on the current system or on multiple systems, and install the operating system.

SCSI — Small Computer Systems Interface

SD card — Secure Digital card. A solid-state memory card.

span — A span is a RAID technique used to combine storage space from groups of physical disks into a RAID-10 virtual disk.

SSD — Solid state disk

SSM — System Service Manager. The SSM performs USC functions, such as downloading updates, as a background task.

stripe — See *striping*.

stripe element — A stripe element is the portion of a stripe that resides on a single physical disk. See also *striping*.

stripe element size — The amount of disk space consumed by a stripe element.

stripe size — The total disk space consumed by a stripe, not including a parity disk.

striping — Disk striping writes data across all physical disks in a virtual disk. Each stripe consists of consecutive virtual disk data addresses that are mapped in fixed-size units to each physical disk in the virtual disk using a sequential pattern. For example, if the virtual disk includes five physical disks, the stripe writes data to physical disks one through five without repeating any of the physical disks. The amount of space consumed by a stripe is the same on each physical disk. The portion of a stripe that resides on a physical disk is a stripe element. Striping by itself does not provide data redundancy. Striping in combination with parity does provide data redundancy.

TPM — Trusted Platform Module. TPM is a secure cryptoprocessor that stores cryptographic keys used to protect data.

UEFI — Unified Extensible Firmware Interface. UEFI is a specification that details an interface for transitioning control from the pre-boot environment to the operating system. See **www.uefi.org** for more information.

virtual disk — A virtual disk refers to storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is seen by the operating system as a single disk. Depending on the RAID level used, the virtual disk may retain redundant data in case of a disk failure.

Index

V

W