Hewlett Packard
Enterprise

HPE UEFI System Utilities User Guide for HPE ProLiant Gen9 Servers

Abstract

This guide details how to access and use the Unified Extensible Firmware Interface (UEFI) that is embedded in the system ROM of all UEFI-based ProLiant Gen9 servers. It details how to access and use both UEFI and Legacy BIOS options provided in BIOS/Platform Configuration menus that were formerly known as the ROM-Based Setup Utility (RBSU). All options and available responses are defined. This document is for the person who installs, administers, and troubleshoots servers and storage systems.

Part Number: 794200-005
Published: April 2016
Edition: 1

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Acknowledgments

Linux® is a U.S. registered trademark of Linus Torvalds.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.


® is a registered trademark of the UEFI Forum, Inc.

Contents

Part I Getting started

This part introduces the UEFI System Utilities menu-driven interface and its configuration options.

1 Introduction

The UEFI System Utilities is embedded in the system ROM. The UEFI System Utilities enable you to perform a wide range of configuration activities, including:

- Configuring system devices and installed options.
- Enabling and disabling system features.
- Displaying system information.
- Selecting the primary boot controller or partition.
- Configuring memory options.
- Launching other pre-boot environments, such as the Embedded UEFI Shell and Intelligent Provisioning.

HPE ProLiant Gen9 servers that are configured for UEFI Boot Mode can provide:

- Support for boot partitions larger than 2.2 TB. Such configurations could previously only be used for boot drives when using RAID solutions such as Smart Array.
- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.
- An Embedded UEFI Shell that provides a pre-boot environment for running scripts and tools.
- Operating system specific functionality, such as Microsoft Windows 2012, which supports several features only when installed in UEFI mode.
- Boot support for option cards that only support a UEFI option ROM.

What is UEFI?

Unified Extensible Firmware Interface (UEFI) defines the interface between the operating system and platform firmware during the boot, or start-up process. Compared to BIOS, UEFI supports advanced pre-boot user interfaces. The UEFI network stack enables implementation on a richer network-based OS deployment environment while still supporting traditional PXE deployments. UEFI supports both IPv4 and IPv6 networks. In addition, features such as Secure Boot enable platform vendors to implement an OS-agnostic approach to securing systems in the pre-boot environment.

The ROM-Based Setup Utility (RBSU) functionality is available from the UEFI interface along with additional configuration options.

2 UEFI System Utilities overview

Launching the System Utilities

1. Optional: If you access the server remotely, start an iLO remote console session.
   a. Open a browser and enter `https://<iLO host name or IP address>` to log on to the iLO web interface.
   b. On the login page, do one of the following:
      - Enter a directory or local user account name and password, and click **Log In**.
      - Click the **HPE Zero Sign In** button.

        This button is displayed when iLO is configured for Kerberos network authentication.
2. Navigate to the **Remote Console→Remote Console** page.
3. Verify that your system meets the requirements for using the remote console application you want to use.
4. Click the launch button for your selected application.

   Alternatively, you can click an Integrated Remote Console link on the **Overview** page.
5. Restart or power on the server.

   The server restarts and the ProLiant POST screen appears.
6. Press **F9**.

   The **System Utilities** screen appears.
7. Continue Navigating the System Utilities .

Navigating the System Utilities

1. Launch the System Utilities and do one of the following.
   - To navigate through the screens and modify settings, press any of the navigational keys. Key functions are shown at the bottom of every System Utilities screen.
   - To access the *HPE UEFI System Utilities and Shell Command Mobile Help for HPE ProLiant Gen9 Servers*, scan the QR code on the bottom of the System Utilities screen with your mobile device.
2. To exit the System Utilities screen and reboot the server, press **Esc** until the main menu is displayed, and then select one of the following options:
   - Exit and resume system boot—Exits the system and continues the normal boot process. The system continues through the boot order list and launches the first bootable option in the system.
   - Reboot the System—Exits the system and reboots the system without continuing the normal boot process.

   The screen displays the booting process, and the ProLiant POST screen appears. Toward the end of the boot process, the boot options screen is displayed. It is visible for several seconds before the system attempts to boot from a supported boot device. .

System Utilities key functions

- Up or down arrow—Selects a menu option. When selected, the color of a menu option changes from white to yellow text.
- **Enter**—Selects an entry. A selected option changes color from white to yellow. When a submenu is available, the submenu appears.
- **Esc**—Returns to the previous screen.

- **F1**—Displays online help about a selection.
- **F7**—Loads default UEFI configuration settings and prompts you to:
  - Press **Enter** to apply defaults.
  - Press **Esc** to cancel.
- **F10**—Prompts you to save changed settings.
  - Press **Y** to save (apply) settings.
  - Press **N** to discard settings.
  - Press **Esc** to exit the confirmation prompt without saving or discarding settings.

When a reboot is required

For certain configuration changes to take effect, a reboot might be required. In such cases, a prompt appears on the applicable System Utilities screen that tells you to do so.

System Utilities menu overview

NOTE: UEFI system configuration options vary by Gen9 platform. Therefore, you might not see some of the options that are documented here.

The System Utilities screen is the main screen in the UEFI menu-driven interface. It displays menu options for the following configuration tasks:

- System Configuration—Displays options for viewing and configuring:
  - BIOS/Platform Configuration (RBSU)
  - Using the iLO 4 Configuration Utility
  - Other system-specific devices, such as installed PCIe cards, NICs and Smart Arrays. For example, **Embedded FlexibleLOM Port 1**.

    NOTE: Throughout the menus, the interface attempts to display the proper marketing name for installed PCI devices. If the interface does not recognize a device, it assigns a generic label to the device, such as a `non-HPE name`. This generic labeling does not affect the functionality or operation of the device. Devices vary based on your system.
- One-Time Boot Menu—Displays options for selecting a boot override option and running a UEFI application from a file system.
- Embedded Applications—Displays options for viewing and configuring:
  - Embedded UEFI Shell
  - Integrated Management Log (IML)
  - Active Health System Log (AHS)
  - Firmware Update
  - Embedded Diagnostics
  - Intelligent Provisioning

- System Information—Displays options for viewing the server name and generation, serial number, product ID, BIOS version and date, power management controller, backup BIOS version and date, system memory, and processors.
- System Health—Displays options for viewing the current health status of all devices in the system.
- Exit and resume system boot—Exits the system and continues the normal booting process.
- Reboot the system—Exits the system and reboots it by going through the **UEFI Boot Order** list and launching the first bootable option in the system. For example, you can launch the UEFI Shell, if enabled and listed as the first bootable option in the list.
- Select Language—Enables you to select a language to use in the user interface. English is the default language.

Common setup and configuration FAQs

1. **How do I access the UEFI System Utilities?**
   See “Launching the System Utilities ” (page 13).
2. **How do I update the firmware or system ROM?**
   See “Updating firmware or system ROM” (page 16).
3. **How do I use the Firmware Update application to upgrade the system ROM to the version included on the USB key already inserted into the server?**
   See “Updating firmware or system ROM” (page 16).
4. **How do I transition from RBSU settings to UEFI settings?**
   The BIOS/Platform Configuration (RBSU) menu replaces the ROM-Based Setup Utility (RBSU) on ProLiant Gen9 servers. Use this menu to access and use both UEFI and Legacy BIOS options. See “BIOS/Platform Configuration (RBSU)” (page 19).
5. **When would I want to choose Legacy BIOS Mode rather than UEFI Mode as my boot mode, and vice versa?**
   Certain situations might require that you operate in Legacy BIOS Mode, such as booting custom OS images that were installed using legacy boot mode or created using a legacy BIOS system.
   UEFI Mode is enabled by default and is required for certain options, including:
   - Secure Boot, UEFI Optimized Boot, Generic USB Boot, IPv6 PXE Boot, iSCSI Boot, and Boot from URL
   - Fibre Channel/FCoE Scan Policy
   - Booting to a hard disk drive larger than 2.2 TB
   - Booting the Embedded User Partition.
6. **How do I select between Legacy BIOS and UEFI Mode?**
   See “Selecting the boot mode” (page 45).
7. **How do I determine if a server has UEFI boot options?**
   See “Boot Options” (page 45).
8. **How do I select a boot device?**
   To access the One-Time Boot Menu where you can select an option for a one-time boot override, do one of following:
   - Press **F11** during server POST.
   - On the **System Utilities** screen, select **One-Time Boot Menu**. See One-Time Boot Menu options.

   To modify the boot order for all boots, see Changing the UEFI boot order, or Changing the Legacy BIOS boot order.

9 **How do I enable or disable Intel Hyperthreading?**
By default, Intel Hyperthreading is enabled. To disable or re-enable this setting, see “Enabling or disabling Intel Hyperthreading” (page 39).

10 **How do I configure the Minimum Processor Idle Power Package State to No Package State?**
By default, this is set to Package C6 (retention) State, the lowest processor idle power state. To change this setting, see “Minimum Processor Idle Power Package C-State” (page 63).

11 **How do I configure the time zone?**
See “Date and Time” (page 101).

12 **How do I save my configuration changes and reboot the system?**
1. When you are done making changes, if you do not see the prompt `Changes are pending. Do you want to save changes and exit?`, press **F10** to display it.
2. Press **Y** to save your changes.
   A `Change saved` confirmation prompt appears.
3. Select a reboot option and press **Enter**:
   - Exit and resume system boot—Exits the system and continues the normal boot process. The system continues through the boot order list and launches the first bootable option in the system.
   - Reboot the System—Exits the system and reboots the system without continuing the normal boot process.

13 **How do I enter the Embedded UEFI Shell?**
See “Launching the Embedded UEFI Shell” (page 28).

14 **How do I view the health status of all installed options and devices?**
See “Viewing System Health” (page 32).

15 **How do I use CONREP to replicate UEFI settings?**
See “Configuration Replication Utility (CONREP)” (page 104).

Updating firmware or system ROM

To update firmware or system ROM, use any of the following methods:

- The **Firmware Update** option in the System Utilities. See “Updating firmware from the System Utilities” (page 16).
- The `fwupdate` command in the **Embedded UEFI Shell**.
- Service Pack for ProLiant (SPP)
- HPE online flash components

Updating firmware from the System Utilities

Use this option to update firmware components in the system, including the system BIOS, NICs, and storage cards. Your system can be set to either Legacy BIOS Mode or UEFI Mode.

1. Access the System ROM Flash Binary component for your server from the Hewlett Packard Enterprise Support Center (**http://www.hpe.com/support/hpesc**). When searching for the component, always select **Cross operating system** to locate the binary file.
2. Copy the binary file to a USB media or iLO virtual media.
3. Attach the media to the server.
4. Launch the **System Utilities**, select **Embedded Applications→Firmware Update**, and press **Enter**.

5. Select a device and press **Enter**.

   The **Firmware Updates** screen lists details about your selected device, including the current firmware version in use.
6. Select **Select Firmware File** and press **Enter**.
7. Select the flash file in the **File Explorer** list and press **Enter**.

   The firmware file is loaded and the **Firmware Updates** screen lists details of the file in the **Selected firmware file** field.
8. Select **Image Description** and press **Enter**, then select a firmware image and press **Enter** again. A device can have multiple firmware images.
9. Select **Start firmware update** to update the firmware components in the system.

Part II System Utilities main menu options

The System Utilities main menu is your starting point for:

- System Configuration
- One-Time Boot Menu
- Embedded Applications
- System Information
- System Health
- Exit and resume system boot
- Reboot the System
- Select Language

3 System Configuration

System Configuration menu options

- BIOS/Platform Configuration (RBSU)
- iLO 4 Configuration Utility
- Embedded device information

BIOS/Platform Configuration (RBSU)

The **BIOS/Platform Configuration (RBSU)** menu replaces the ROM-Based Setup Utility (RBSU) on ProLiant Gen9 servers. This menu contains many of the nested options for accessing both UEFI and Legacy BIOS options, including:

- System Options
- Boot Options
- Network Options
- Embedded UEFI Shell options
- Power Management options
- Performance Options
- Server Security options
- PCI Device Enable/Disable
- Server Availability options
- BIOS Serial Console and EMS options
- Server Asset Information options
- Advanced Options
- Date and Time
- System Default Options

Using the iLO 4 Configuration Utility

iLO 4 Configuration Utility options

You can access the iLO 4 Configuration Utility from the physical system console, or by using an iLO 4 remote console session. The utility has the following options:

- Network Options
- Advanced Network Options
- User Management
- Setting Options
- Set to Factory Defaults
- Reset iLO (active connections)
- About

Network Options

- **MAC Address** (read-only)—The MAC address of the selected iLO network interface.
- **Network Interface Adapter**—Specifies the iLO network interface adapter to use.
  - **ON**—Uses the iLO Dedicated Network Port.
  - **Shared Network Port**—Uses the Shared Network Port. This option is only available on supported servers.
  - **OFF**—Disables all network interfaces to iLO.
- **Transceiver Speed Autoselect** (iLO Dedicated Network Port only)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network. This option is only available when **Network Interface Adapter** is set to **ON**.
- **Transceiver Speed Manual Setting** (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface. This option is only available when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
- **Transceiver Duplex Setting** (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface. This option is only available when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
- **VLAN Enable** (Shared Network Port only)—Enables the VLAN feature.

  When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.
- **VLAN ID** (Shared Network Port only)—When a VLAN is enabled, specifies a VLAN tag. All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.
- **DHCP Enable**—Configures iLO to obtain its IP address (and many other settings) from a DHCP server.
- **DNS Name**—Sets the DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`).

  This name can only be used if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.
- **IP Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- **Gateway IP Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.

Configuring Network Options

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Network Options**, and press **Enter**.
2. Select any of the Network Options and press **Enter**, then select a setting or enter a value for that option and press **Enter** again.
3. Press **F10**.

Advanced Network Options

- **Gateway from DHCP**—Specifies whether iLO uses a DHCP server-supplied gateway.
- **Gateway #1**, **Gateway #2**, and **Gateway #3**—If **Gateway from DHCP** is disabled, specifies up to three iLO gateway IP addresses.
- **DHCP Routes**—Specifies whether iLO uses the DHCP server-supplied static routes.
- **Route 1**, **Route 2**, and **Route 3**—If **DHCP Routes** is disabled, specifies the iLO static route destination, mask, and gateway addresses.
- **DNS from DHCP**—Specifies whether iLO uses the DHCP server-supplied DNS server list.
- **DNS Server 1**, **DNS Server 2**, **DNS Server 3**—If **DNS from DHCP** is disabled, specifies the primary, secondary, and tertiary DNS servers.
- **WINS from DHCP**—Specifies whether iLO uses the DHCP server-supplied WINS server list.
- **Register with WINS Server**—Specifies whether iLO registers its name with a WINS server.
- **WINS Server #1** and **WINS Server #2**—If **WINS from DHCP** is disabled, specifies the primary and secondary WINS servers.
- **Domain Name**—The iLO domain name. If DHCP is not used, specifies a domain name.

Configuring Advanced Network Options

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Advanced Network Options**, and press **Enter**.
2. Select any of the Advanced Network Options and press **Enter**, then select a setting or enter a value for that option and press **Enter** again.
3. Press **F10**.

User Management

- Add User
- Edit/Remove User

Add User

Use this option to add new local iLO user accounts, including:

New User iLO 4 Privileges

- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.
- **Remote Console Access**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
- **Configure Settings**—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration.

New User Information

- **New User Name**—Specifies the name that appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The user name must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each login name.
- **Login Name**—Specifies the name that must be used when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in iLO logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.
- **Password** and **Password Confirm**—Sets and confirms the password that is used for logging in to iLO. The maximum length for a password is 39 characters. Enter the password twice for verification.

Adding new user accounts

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→User Management→Add User**, and press **Enter**.
2. Select any of the New User iLO 4 Privileges and press **Enter**.
3. For each option, select one of the following settings and press **Enter** again.
   - **YES** (default)—Enables the privilege for this user.
   - **NO**—Disables the privilege for this user.
4. Select a New User Information entry and press **Enter**.
5. Complete each entry for the new user, and press **Enter**.
6. Create as many user accounts as needed, and then press **F10**.

Edit/Remove User

Use this option to edit iLO user account settings, or to delete user accounts.

Editing or removing user accounts

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→User Management→Edit/Remove User**, and press **Enter**.
2. Select the **Action** menu for the user name you want to edit or delete, and press **Enter**.
3. Select one of the following, and press **Enter**.
   - **No Change**—Returns you to the main menu.
   - **Delete**—Deletes this user.
   - **Edit**—Edits the user.
4. Depending on your selection in Step 3Step 6, do one of the following:
   - If you selected **No Change**, no further action is needed.
   - If you selected **Delete**, the user name is marked to be deleted when you save the changes on this page.
   - If you selected **Edit**, update the login name, password, or user permissions.
5. Update as many user accounts as needed, and then press **F10**.

Setting Options

Use this menu to view and configure iLO access settings.

- **iLO 4 Functionality**—Enables or disables the iLO 4 features. The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled.

  NOTE: The iLO functionality cannot be disabled on blade servers.

- **iLO 4 Configuration Utility**—Enables or disables the iLO 4 Configuration Utility. If this option is set to **Disabled**, the iLO 4 Configuration Utility menu item is not available when you access the UEFI System Utilities.
- **Require Login for iLO 4 Configuration**—Determines whether a user-credential prompt is displayed when a user accesses the iLO 4 Configuration Utility. If this setting is **Enabled**, a login dialog box opens when you access the iLO 4 Configuration Utility.
- **Show iLO 4 IP Address during POST**—Enables the display of the iLO network IP address during host server POST.
- **Local Users**—Enables or disables local user account access.
- **Serial CLI Status**—Specifies the login model of the CLI feature through the serial port. The following settings are valid:
  - **Enabled-Authentication Required**—Enables access to the iLO CLP from a terminal connected to the host serial port. Valid iLO user credentials are required.
  - **Enabled-No Authentication Required**—Enables access to the iLO CLP from a terminal connected to the host serial port. iLO user credentials are not required.
  - **Disabled**—Disables access to the iLO CLP from the host serial port. Use this option if you are planning to use physical serial devices.
- **Serial CLI Speed (bits/second)**—Specifies the speed of the serial port for the CLI feature. The following speeds (in bits per second) are valid: **9600**, **19200**, **57600**, and **115200**. For correct operation, set the serial port configuration to no parity, 8 data bits, and 1 stop bit (N/8/1).

  NOTE: The 38400 speed is supported in the iLO web interface, but is not currently supported by the iLO 4 Configuration Utility.

Configuring access settings

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Setting Options**, and press **Enter**.
2. View or update user access Setting Options.
3. Press **F10**.

Set to factory defaults

CAUTION: This operation clears all user and license data.

Use this option to reset iLO to the factory default settings. When you do so, you cannot access the iLO 4 Configuration Utility until after the next system reboot. If you are managing iLO remotely, the remote console session is automatically ended.

NOTE: If a server has an installed iLO Advanced license when you perform this procedure, the iLO Advanced icon might be selected when the server boot process finishes. The icon will be set correctly after POST completes, or after the server is shut down, powered off, and then powered on again.

Resetting iLO to the factory default settings

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Set to factory defaults**, and press **Enter**.

   The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.
2. Select **YES**, and press **Enter**.
3. When prompted to confirm the reset, press **Enter**.

   iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended.
4. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The iLO 4 Configuration Utility screen is still open from the previous session.
   b. Press **Esc** until the main menu is displayed.
   c. Select **Exit and Resume Boot** in the main menu, and press **Enter**.
   d. When prompted to confirm the request, press **Enter** to exit the screen and resume the boot process.

Reset iLO

If iLO is slow to respond, you can use this option to perform a reset.

Resetting iLO with this method does not make any configuration changes, but it ends all active connections to iLO. When you reset iLO, the iLO 4 Configuration Utility is not available again until the next reboot.

Resetting iLO active connections

Prerequisite

Configure iLO Settings privilege

To reset iLO active connections:

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Reset iLO**.

   The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.
2. Select **YES**, and press **Enter**.
3. When prompted to confirm the reset, press **Enter**.

   Active iLO connections are reset. If you are managing iLO remotely, the remote console session is automatically ended.

4. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The UEFI System Utilities are still open from the previous session.
   b. Press **Esc** until the main menu is displayed.
   c. Select **Exit and Resume Boot** in the main menu, and press **Enter**.
   d. When prompted to confirm the request, press **Enter** to exit the utility and resume the normal boot process.

About

Use this menu to view information about the following iLO components.

- **Firmware Date**—The iLO firmware revision date.
- **Firmware Version**—The iLO firmware version.
- **iLO CPLD Version**—The iLO complex programmable logic device version.
- **Host CPLD Version**—The ProLiant server complex programmable logic device version.
- **Serial Number**—The iLO serial number.
- **RBSU Date**—The iLO 4 Configuration Utility revision date.
- **PCI BUS**—The PCI bus to which the iLO processer is attached.
- **Device**—The device number assigned to iLO in the PCI bus.

Viewing information about iLO

1. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→About**, and press **Enter**.
2. View information about iLO components.

Embedded device information

Smart Array Controller information

The **System Configuration** screens show device information about installed Smart Array Controllers. HPE 12 Gb/s capable SAS Smart Array controllers (for example, the Smart Array P44ar controller) support UEFI-based servers.

NOTE: Install only Smart Array Controllers that are listed as supported for your server and that are running the latest versions of Smart Array Controller firmware. Other Smart Array controllers are not supported and might not function properly in this server. Before installing the operating system, use the latest SPP in Offline mode to upgrade the firmware to the latest version. Supported controllers not using the proper firmware display as an unknown device in the system configuration.

Viewing and configuring Smart Array Controller information

1. From the **System Utilities** screen, select **System Configuration** and press **Enter**.
2. Select a Smart Array controller and press **Enter**.

   The **System Configuration** screen displays information about the embedded device.

3. Select an option and press **Enter**. Options include:
   - **Device Information**—Lists firmware version, firmware release date, UEFI driver version, PCI device ID, and PCI slot number.
   - **Exit and launch HP Smart Storage Administrator (HPSSA)**—Accesses options for HPSSA, including configuring and monitoring the status of Smart Array controllers.
   - **HPE Shared Memory features**—Enables or disables the use of reserved memory regions to allow direct assignment of devices to guest virtual machines.

NIC and FCoE information

The **System Configuration** screens show information about and configure installed system devices, such as embedded NICs and FCoEs. Devices listed and configuration options available vary by system.

Viewing and configuring NIC and FCoE settings

1. From the **System Utilities** screen, select **System Configuration** and press **Enter**.
2. Select an **Embedded FlexibleLOM** and press **Enter**.

   The **System Configuration** screen displays information about the embedded device.

NPAR configuration

NPAR (NIC Partitioning multi-function mode) enables you to partition a NIC into multiple virtual NICs with multiple PCI physical functions per port. Each PCI function is associated with a different virtual NIC. To the OS and the network, each physical function appears as a separate NIC port.

Enabling NPAR on a NIC

NOTE: The following procedure shows how to enable NPAR on an **Embedded FlexibleLOM** card. NIC options vary by system.

To enable NPAR:

1. From the **System Configuration** screen, select an **Embedded FlexibleLOM** and press **Enter**.

   Information and configuration options related to the embedded device appear.
2. Select **Multi-Function Mode** and press **Enter**.
3. Select **NPAR1.5** and press **Enter**.
4. Press **F10**.

   Up to eight virtual NICs for this device are now available.

4 One-Time Boot Menu

One-Time Boot Menu options

Use the **One-Time Boot Menu** to select a UEFI boot option for a one-time boot override. The option you select does not modify your predefined boot order settings. If you use a USB key or virtual media through the iLO 4 Remote Console, exit and re-enter the System Utilities to refresh this menu so that the devices appear.

Boot options include:

- OS boot manager, such as **Windows Boot Manager**—Lists the boot manager for your installed OS.
- **Generic USB Boot**—Provides a place holder for any USB device that is bootable in UEFI. You can set the boot priority of this option, and retain this priority for use with USB devices you might install in the future. Setting this priority does not affect priorities set for individual USB devices in the **UEFI Boot Order** list.

  NOTE: This option is only available in UEFI Mode. The system attempts to boot all UEFI bootable USB devices in the order you specify in the **Generic USB Boot** entry, even if installed individual USB devices are configured lower in the boot order.

- Embedded Flexible LOMs
- Embedded UEFI Shell
- Embedded SATA Port
- **Run a UEFI Application from a file system**—Enables you to select a UEFI application to run from a file system. You can browse all FAT file systems that are available in the system. You can also select an x64 UEFI application (with a .EFI extension) to execute (can be an OS boot loader or any other UEFI application).
- **Legacy BIOS One-Time Boot Menu**—Exits and launches the **Legacy BIOS One-Time Boot Menu**, where you can select a specific override option for this boot only. This option does not modify your boot order mode settings.

Selecting an option for a one-time boot

1. From the **System Utilities** screen, select **One-Time Boot Menu** and press **Enter**.
2. Select an option and press **Enter**.
3. Reboot the server.

5 Embedded Applications

Embedded Applications options

- Embedded UEFI Shell
- Integrated Management Log (IML)
- Active Health System Log
- Firmware Update
- Embedded Diagnostics
- Intelligent Provisioning

Embedded UEFI Shell

Use this option to launch the Embedded UEFI Shell. The Embedded UEFI Shell is a pre-boot command line environment for scripting and running UEFI applications, including UEFIboot loaders. The Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS.

Launching the Embedded UEFI Shell

Prerequisites

- Boot Mode is set to **UEFI Mode**.
- Embedded UEFI Shell is enabled.
- **Embedded UEFI Shell** is set to enabled (the default setting).

To launch the Embedded UEFI Shell:

1. From the **System Utilities** screen, select **Embedded Applications→Embedded UEFI Shell** and press **Enter**.

   The **Embedded UEFI Shell** screen appears.
2. Press any key to acknowledge that you are physically present.

   This step ensures that certain features, such as disabling **Secure Boot** or managing the **Secure Boot** certificates using third-party UEFI tools, are not restricted.
3. If an administrator password is set, enter it at the prompt and press **Enter**.

   The `Shell>` prompt appears.
4. Enter the commands required to complete your task.
5. Enter the `exit` command to exit the Shell.

More information

HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers

Integrated Management Log (IML)

Use this option to view or clear the IML. The IML provides a record of historical events that have occurred on the server. Entries in the IML can help you diagnose issues or identify potential issues. The IML timestamps each event with one-minute granularity.

Viewing or clearing the IML

1. From the **System Utilities** screen, select **Embedded Applications→Integrated Management Log** and press **Enter**.
2. Select an option and press **Enter**.
   - **View IML**—Displays the Integrated Management Log records.
   - **Clear IML**—Clears all entries in the Integrated Management Log.

Active Health System Log

Use this option to download an AHS log. By default, the system downloads logs from the previous seven days if you do not use the **Range Start Date** and **Range End Date** fields to specify a different time period. When requested by Hewlett Packard Enterprise Support, you can copy your stored `.ahs` file, and email it to your customer support representative.

Downloading an AHS log

1. From the **System Utilities** screen, select **Embedded Applications→Active Health System Log** and press **Enter**.
2. Select **Download Active Health System Log** and press **Enter**.
3. Complete the following and press **Enter** after each selection or data entry.
   - **Download Entire Log**—Unless you are advised by support personnel to download AHS records for the life of the server, leave this disabled (not selected). The default setting is disabled.
   - **Range Start Date**—Enter a starting date for log collection.
   - **Range End Date**—Enter an ending date for log collection.
   - **Select File Location**—Select this to open a File Explorer screen and select the FAT16 FAT32 partition on local or virtual writable media on which to download the AHS log.

     NOTE: Hewlett Packard Enterprise recommends storing AHS logs on USB or HDD media. Storing logs on SD cards is not supported.

   - Optional: Add your customer information, including support case number, and contact information.
4. Select **Start Download** and press **Enter**.

   The UEFI firmware communicates with iLO to download the requested AHS log files and package them into one `.ahs` file.
5. When requested by Hewlett Packard Enterprise Support, copy your stored `.ahs` file, and email it to your customer support representative.

NOTE: You can also download AHS log files by selecting **System Utilities→System Health→Download Active Health System Log**.

Firmware Update

Use this option to update firmware components in the system, including the system BIOS, NICs, and storage cards.

More information

Updating firmware from the System Utilities

Embedded Diagnostics

Use this option to launch the ProLiant Hardware Diagnostics menu. From there, you can view health summary status, run system tests and component tests, and view test logs.

Launching Embedded Diagnostics

1. From the **System Utilities** screen, select **Embedded Applications→Embedded Diagnostics** and press **Enter**.

   The ProLiant Hardware Diagnostics screen appears.
2. Select an option and press **Enter**.
   - **System Health**—Lists a Health Summary (status for BIOS hardware, fans, temperature, battery, memory, network, and storage), Fans (zone, label, status, and speed), Temperature (label, location, status, current reading, and cautions), Power Supplies (power supply summary and smart storage battery), Processors, Memory, NIC Information, Storage, and Firmware Information
   - **System Tests**—Lists information and gives you options for checking hardware subsystems to ensure they are working properly. The Quick Test option performs a 10-minute check of the hardware. The Extensive Test option performs a full check of the hardware and can take two or more hours to complete.
   - **Component Tests**—Lists information and gives you options for checking Processor, Memory, Hard Drive, Keyboard, Mouse, Network, Optical Drive, System Board, USB Port, and Video tests.
   - **Test Logs**—Displays test logs, which contain information about test type and results, including failures.
   - **IML Log**—Displays all IML log files, which include information about the severity, class, initial time, and update time.
   - **Language**—Selects your language for the Embedded Diagnostics.
   - **Exit**—Exits the **Embedded Diagnostics** menu and returns you to the **System Utilities** screen.

Intelligent Provisioning

Use this option to launch Intelligent Provisioning. Intelligent Provisioning is a single-server deployment tool embedded in ProLiant Gen9 servers that simplifies ProLiant server setup, providing a reliable and consistent way to deploy ProLiant server configurations. This option lets you select the Intelligent Provisioning host override option for this boot only. It does not modify the normal boot order or boot mode settings. For more information, see the *HPE Intelligent Provisioning User Guide for HPE ProLiant Gen9 Servers* on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/intelligentprovisioning/docs**).

Launching Intelligent Provisioning

1. From the **System Utilities** screen, select **Embedded Applications** and press **Enter**.
2. Select **Intelligent Provisioning** and press **Enter**.
3. Reboot the server to return to the **System Utilities** menu.

6 System Information and System Health

System Information

Use this option to view:

- **Summary**—Shows a summary of system settings, including:
  - **System Name**
  - **Serial Number**
  - **Product ID**
  - **BIOS Version** and **Backup BIOS Version**
  - **Power Management Controller FW Version**
  - **User Defaults**
  - **Boot Mode**
  - **System Memory**
  - Processor types
  - iLO IPv4 and IPv6 IP addresses
  - Embedded **Network Devices**
- **Processor**—Shows detailed processor information. including:
  - **CPU** number, **Socket** number and **Socket Locator** label
  - Whether the CPU socket is **Populated** with a CPU package
  - A brief CPU **Manufacturer Description** and a list of **Characteristics** that the CPU supports
  - The **Core Count**, the number of enabled cores, and **Thread Count** (number of logical cores) in the CPU package
  - The **Rated Speed** and **External Clock Speed** of the CPU
  - The **Voltage** of the CPU package
  - A list of **Microcode Patches** being installed by the BIOS
  - L1, L2, and L2 cache size and speed
- **Memory Information**—Shows detailed memory information, including
  - **Total System Memory**
  - **Total Memory Slots**
  - Operating frequency and voltage
  - The **Number of Slots** connected to the CPU
  - The number of **Installed Modules** that are directly connected to the CPU

- **PCI Device Information**—Shows detailed information about each PCI device.
- **Firmware Information**—Shows detailed firmware information, including:
  - **System ROM** and **Redundant System ROM**
  - **Power Management Controller Firmware** and boot loader
  - Hardware PAL/CPLD, SPS, and APML firmware
  - **Smart Storage Battery Firmware**
  - Smart Array and NIC firmware

Viewing System Information

1. From the **System Utilities** screen, select **System Information** and press **Enter**.
2. Select an option to display related information, and press **Enter**.

NOTE: You can also view firmware information using the RESTful Interface Tool. See the RESTful Interface Tool documentation at: **http://www.hpe.com/info/restfulinterface/docs**.

System Health

Use this screen to check the health status of all devices in the system. This screen shows, for example, the presence of any unsupported devices found during the boot process. You can also use this screen to collect AHS logs, which enable you to better address system issues.

Viewing System Health

1. From the **System Utilities** screen, select **System Health** and press **Enter**.
2. Select **View System Health** and press **Enter**.
3. From the **System Utilities** screen, select **System Health** and press **Enter**.
4. (Optional) To download an AHS log from this screen:
   a. Select **Download Active Health System Log** and press **Enter**.

      The Active Health System Log screen appears. This is the same screen that appears when you select **System Utilities→Embedded Applications→Active Health System Log**.

   b. Follow steps 3 through 5 in Downloading an AHS log.

7 Rebooting the system and selecting a language

Rebooting the system

Exit and resume system boot

Use this option to exit the system and continue the normal boot process. The system continues through the boot order list and launches the first bootable option in the system. For example, you can launch the UEFI Embedded Shell, if it is enabled and selected as first bootable option in the **UEFI Boot Order** list.

Exiting and resuming system boot

1. From the **System Utilities** screen, select **Exit and resume system boot** and press **Enter**.

   A confirmation message appears.
2. Press **Enter** to exit and resume normal boot.

Reboot the System

Use this option to exit the system and reboot the system without continuing with the normal boot process.

Rebooting the system

1. From the **System Utilities** screen, select **Reboot the System** and press **Enter**.

   A confirmation message appears.
2. Press **Enter** to reboot the system.

Selecting a language

Select Language

Use this option to select a one of the following languages for the system.

- **English**
- **Japanese**
- **Simplified Chinese**

Selecting a system language

1. From the **System Utilities** screen, select **Select Language** and press **Enter**.
2. Select an option and press **Enter**.
3. Press **F10**.

Part III BIOS/Platform Configuration options

The **System Utilities→BIOS/Platform Configuration (RBSU)** menu is your starting point for:

- System Options
- Boot Options
- Network Options
- Storage Options
- Server Security
- PCI Device Enable/Disable
- Server Availability
- BIOS Serial Console and EMS
- Server Asset Information
- Advanced Options
- Date and Time
- System Default Options

8 Configuring System Options

System Options

Serial Port Options

Embedded Serial Port

Use this option to assign a logical COM port address and associated default resources to a selected physical serial port.

NOTE: The operating system can overwrite this setting.

Assigning an Embedded Serial Port

Prerequisite

For proper screen resolution, set the console resolution in the terminal software to **100x31**.

To assign an embedded serial port:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Serial Port Options→Embedded Serial Port** and press **Enter**.
2. Select a setting and press **Enter**.
   - **COM 1: IRQ4: I/0: 3F8h-3FFh** (default)
   - **COM 2: IRQ3: I/0: 2F8h-2FFh**
   - **Disabled**
3. Press **F10**.

Virtual Serial Port

Use this option to assign a logical COM port address and the associated default resources used by the Virtual Serial Port (VSP). VSP enables the iLO Management Controller to appear as a physical serial port to support the BIOS Serial Console and the operating system serial console.

Assigning a Virtual Serial Port

Prerequisite

For proper screen resolution, set the console resolution in the terminal software to **100x31**.

To assign a virtual serial port:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Serial Port Options→Virtual Serial Port** and press **Enter**.
2. Select a setting and press **Enter**.
   - **COM 1: IRQ4: I/0: 3F8h-3FFh**
   - **COM 2: IRQ3: I/0: 2F8h-2FFh** (default)
   - **Disabled**
3. Press **F10**.

USB Options

USB Control

Use this option to configure how USB ports and embedded devices operate at startup.

Setting USB Control

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→USB Control** and press **Enter**.
2. Select a setting and press **Enter**.
   - **USB Enabled** (default)—Enables all USB ports and embedded devices.
   - **External USB Port Disabled**—Disables external USB ports while maintaining full support for embedded USB devices managed by the ROM and operating system.
3. Press **F10**.

USB Boot Support

Set this option to disabled to prevent the system from booting any USB devices connected to the server. This includes preventing boot to virtual media devices and the embedded SD or SD card slot, if supported.

Setting USB Boot Support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→USB Boot Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—The system can boot from USB devices connected to the server.
   - **Disabled**—The system cannot boot from USB devices connected to the server.
3. Press **F10**.

Removable Flash Media Boot Sequence

Use this option to select which USB or SD Card devices to search first when enumerating boot devices. You can select whether the system attempts to boot external USB drive keys, internal USB drive keys, or the internal SD Card slot first. The **Removable Flash Media Boot Sequence** does not override the device boot order in the Standard Boot Order (IPL) option. Configure this option when Boot Mode is set to Legacy BIOS Mode because UEFI Boot Mode enables you to boot from an USB device available in the boot list. See “Boot Mode” (page 45). Settings are:

Selecting the Removable Flash Media Boot Sequence

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→Removable Flash Media Boot Sequence** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Internal SD Card First**—Boots using the internal SD card slot.
   - **Internal Drive Keys First**—Boots using the internal USB drive keys.
   - **External Drive Keys First** (default)—Boots using external USB drive keys.
3. Press **F10**.

Virtual Install Disk

Use this option to enable or disable the virtual install disk. The virtual install disk contains drivers specific to the server that an operating system can use during installation. When this option is enabled, Microsoft Windows Server automatically locates required drivers and installs them, eliminating the need for user intervention and the requirement that a driver be present on external media during operating system installation. In some cases, the virtual install disk remains visible from the installed operating system as a read-only drive. During manual installations using Intelligent Provisioning, this option is disabled automatically.

Enabling or disabling the Virtual Install Disk

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→Virtual Install Disk** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—The Virtual Install Disk appears as a drive in the operating system.
   - **Disabled** (default)—The Virtual Install Disk does not appear as a drive in the operating system.
3. Press **F10**.

Embedded User Partition

Use this option to enable or disable the general purpose disk partition on non-volatile flash memory that is embedded on the system board.

You can also configure the Embedded User Partition using the RESTful Interface Tool. See the RESTful Interface Tool documentation at: **http://www.hpe.com/info/restfulinterface/docs**.

Enabling or disabling the Embedded User Partition

Prerequisite

Boot Mode is set to **UEFI Mode**.

To enable or disable the Embedded User Partition:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→Embedded User Partition** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—When the partition is formatted, enables the server to have read and write access to the Embedded User Partition.

     NOTE: After you enable the Embedded User Partition, you must format it using the server operating system software.

   - **Disabled** (default)—The server does not have access to the embedded user partition.
3. Press **F10**.

Internal SD Card Slot

Use this option to enable or disable the internal SD (Secure Digital) card slot. The slot holds an SD non-volatile flash memory card that is embedded on the system board.

Enabling or disabling the Internal SD Card Slot

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→Internal SD Card Slot** and press **Enter**.
2. Select a setting and press **Enter**:
   - **Enabled** (default)—The server can access the internal SD card slot.
   - **Disabled**—The server cannot access the internal SD card slot.
3. Press **F10**.

USB 3.0 Mode

Use this option to set the mode in which USB 3.0-capable devices operate.

- **Auto** (default)—USB 3.0-capable devices operate at USB 2.0 speeds in the pre-boot environment and during boot. When a USB 3.0 capable OS USB driver loads, USB 3.0 devices transition to USB 3.0 speeds. This mode is compatible with operating systems that do not support USB 3.0 while still allowing USB 3.0 devices to operate at USB 3.0 speeds with modern operating systems.
- **Enabled**—USB 3.0-capable devices operate at USB 3.0 speeds at all times (including the pre-boot environment) when in UEFI Boot Mode. Do not use this mode with operating systems that do not support USB 3.0. When operating in Legacy BIOS Boot Mode, the USB 3.0 ports do not function in the pre-boot environment and are not bootable.
- **Disabled**—USB 3.0-capable devices function at USB 2.0 speeds at all times.

Setting the USB 3.0 Mode

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→USB 3.0 Mode** and press **Enter**.
2. Select a setting and press **Enter**.
3. Press **F10**.

Processor Options

- Intel (R) Hyperthreading Options
- Processor Core Disable
- Processor x2APIC Support

NOTE: Options that appear on this menu vary by server model.

Intel (R) Hyperthreading Options

Use this option to disable or enable the logical processor cores on processors supporting Intel Hyperthreading technology. Intel Hyperthreading improves overall performance for applications that benefit from a higher processor core count.

NOTE: Hyperthreading is not supported on all processors. For more information, see the documentation for your processor model.

Enabling or disabling Intel Hyperthreading

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Processor Options→Intel (R) Hyperthreading Options** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables the logical processor cores on processors supporting Intel Hyperthreading technology.
   - **Disabled**—Disables the logical processor cores on processors supporting Intel Hyperthreading technology.
3. Press **F10**.

Processor Core Disable

Use this option to specify the number of cores to enable per processor socket, in multiples of four. Unused cores are disabled. Setting this option can:

- Reduce processor power usage
- Improve overall performance for applications that benefit from higher performance cores rather than more processing cores
- Solve issues with software that is licensed on a per-core basis

Setting the number of enabled processor cores

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Processor Options→Processor Core Disable** and press **Enter**.
2. Enter the number of cores to enable per processor socket and press **Enter**.
   - If you enter an incorrect value, all cores are enabled.
   - If you enter **0**, all cores are enabled.
3. Press **F10**.

Processor x2APIC Support

Use this option to enable or disable x2APIC support. When enabled (the default setting), processor x2APIC support helps operating systems run more efficiently on high core count configurations and optimizes interrupt distribution in virtualized environments. Enabled mode does not enable

x2APIC hardware, but provides the support necessary to the operating system. Unless you are using an older hypervisor or operating system that is not compatible with x2APIC support, leave this option enabled.

Enabling or disabling Processor x2APIC Support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Processor Options→Processor x2APIC Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Generates the ACPI x2APIC control structures, and adds the option of enabling x2APIC support to the operating system when it loads.
   - **Disabled**—Disables x2APIC support.
3. Press **F10**.

SATA Controller Options

- Embedded SATA Configuration
- SATA Secure Erase

Embedded SATA Configuration

Use this option to enable embedded chipset SATA (Serial Advanced Technology Attachment) controller support. You can select ACHI or HPE Dynamic Smart Array RAID support. Make sure that you are using the correct operating system drivers for your selected option.

△ **CAUTION:** Dynamic Smart Array is not supported when the boot mode is configured to Legacy BIOS Mode. Enabling Dynamic Smart Array RAID results in data loss or data corruption on existing SATA drives. Back up all drives before enabling this option.

See your operating system documentation before enabling SATA AHCI support to ensure your base media drivers support this feature.

Enabling embedded chipset SATA controller support

Prerequisites

- The correct operating system drivers for your selected option
- Boot Mode is set to **UEFI Mode**.

To enable SATA controller support:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→SATA Controller Options→Embedded SATA Configuration** and press **Enter**.
2. Ensure that you are using the correct ACHI or RAID system drivers for your SATA option.
3. Select a setting and press **Enter**.
   - **Enable SATA AHCI Support**—Enables the embedded chipset SATA controller for AHCI.
   - **Enable Dynamic Smart Array RAID Support**—Enables the embedded chipset SATA controller for Dynamic Smart Array RAID.
4. Press **F10**.

SATA Secure Erase

Use this option to control whether SATA Secure Erase functionality is supported. This function prevents the Secure Freeze Lock command from being sent to SATA hard drives.

Enabling SATA Secure Erase

Prerequisites

- The SATA controller on the hard drive is in ACHI mode.
- The hard drive supports the Secure Erase command.

To enable SATA Secure Erase:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→SATA Controller Options→SATA Secure Erase** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—The Security Freeze Lock command is not sent to supported SATA hard drives, enabling Secure Erase to function.
   - **Disabled** (default)—Disables Secure Erase.
3. Press **F10**.

Virtualization Options

Virtualization Technology

Use this option to enable or disable Intel Virtualization Technology on a Virtual Machine Manager (VMM). When enabled (the default setting) a VMM supporting Virtualization Technology can use hardware capabilities provided by UEFI Intel processors.

NOTE: You do not need to disable **Virtualization Technology** if you are using a VMM or an operating system that does not support AMD-V virtualization.

Enabling or disabling Virtualization Technology

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Virtualization Options→Virtualization Technology** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables a VMM supporting this option to use hardware capabilities provided by UEFI Intel processors.
   - **Disabled**—Does not enable a VMM to use hardware capabilities provided by UEFI Intel processors.
3. Press **F10**.

Intel (R) VT-d

Use this option to enable or disable Intel Virtualization Technology for Directed I/O (VT-d) on a Virtual Machine Manager (VMM).

NOTE: If you are not using a hypervisor or an operating system that supports this feature, it is not necessary to set the Intel (R) VT-d option to disabled. You can leave it enabled.

Enabling or disabling Intel VT-d

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Virtualization Options→Intel (R) VT-d** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables a hypervisor or operating system supporting this option to use hardware capabilities provided by Intel's Virtualization Technology for directed I/O.
   - **Disabled**—Does not enable a hypervisor or operating system supporting this option to use hardware capabilities provided by Intel's Virtualization Technology for directed I/O.
3. Press **F10**.

SR-IOV

The SR-IOV (Single Root I/O Virtualization) interface is an extension to the PCI express (PCIe) specification. It enables the BIOS to allocate more PCI resources to PCIe devices. Enable this option for a PCIe device or operating system that supports SR-IOV. Leave it enabled when using a hypervisor.

Enabling or disabling SR-IOV

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Virtualization Options→SR-IOV** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables a hypervisor to create virtual instances of a PCIe device, potentially increasing performance.
   - **Disabled**—Does not enable a hypervisor to create virtual instances of a PCIe device.
3. Press **F10**.

Boot Time Optimization

- Dynamic Power Capping Functionality
- Extended Memory Test
- Memory Fast Training

Dynamic Power Capping Functionality

Use this option to configure when the system ROM executes power calibration during the boot process.

Setting Dynamic Power Capping Functionality

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Boot Time Optimization→Dynamic Power Capping Functionality** and press **Enter**.

2. Select a setting and press **Enter**.
   - **Auto**—Power calibration runs the first time the server is booted and is only run again when the hardware configuration settings of the server change.
   - **Enabled** (default)—Power calibration runs on every system boot.
   - **Disabled**—Power calibration does not run, and Dynamic Power Capping is not supported.
3. Press **F10**.

Extended Memory Test

Use this option to configure whether the system validates memory during the memory initialization process. When enabled (the default) and uncorrectable memory errors are detected, the memory is mapped out, and the failed DIMMs are logged to the IML.

NOTE: When enabled, this setting might significantly increase system boot time.

Enabling or disabling Extended Memory Test

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Boot Time Optimization→Extended Memory Test** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables **Extended Memory Test**.
   - **Disabled**—Disables **Extended Memory Test**.
3. Press **F10**.

Memory Fast Training

Use this option to configure memory training on server reboots. When enabled (the default), the platform uses the previously saved memory training parameters determined from the last cold boot of the server, which improves server boot time.

NOTE: When enabled, this setting might significantly increase system boot time.

Enabling or disabling Memory Fast Training

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Boot Time Optimization→Memory Fast Training** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables Memory Fast Training, enabling the server to use previously saved memory training parameters.
   - **Disabled**—The platform performs a full memory training on every server reboot.
3. Press **F10**.

Memory Operations—Advanced Memory Protection

Use this option to configure additional memory protection with Error Checking and Correcting (ECC). **Advanced ECC Support**, the default setting, provides the largest memory capacity to the operating system.

Configuring Advanced Memory Protection

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Memory Operations→Advanced Memory Protection** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Advanced ECC Support** (default)—Provides the largest memory capacity to the operating system while protecting the system against all single-bit failures and some multi-bit failures.
   - **Online Spare with Advanced ECC Support**—Enables the system to automatically map out a group of memory that is receiving excessive correctable memory errors. This memory is replaced by a spare group of memory.
   - **Mirrored Memory with Advanced ECC Support**—Provides the maximum protection against uncorrected memory errors that might otherwise result in a system failure. You must install additional memory to provide mirrored memory to the operating system.
3. Press **F10**.

9 Configuring Boot Options

Boot Options

Boot Mode

Use this option to set the boot mode for the system. ProLiant Gen9 servers provide two boot mode configurations: UEFI Mode and Legacy BIOS Mode. Certain boot options require that you select a specific boot mode.

By default, the boot mode is set to **UEFI Mode**. The system must boot in **UEFI Mode** to use the following options:

- Secure Boot, UEFI Optimized Boot, Generic USB Boot, IPv6 PXE Boot, iSCSI Boot, and Boot from URL
- Fibre Channel/FCoE Scan Policy
- Embedded User Partition
- BL140i Smart Array SW RAID controller

NOTE: The boot mode you use must match the operating system installation. If not, changing the boot mode can impact the ability of the server to boot to the installed operating system.

Selecting the boot mode

Prerequisite

When booting to **UEFI Mode**, leave **UEFI Optimized Boot** enabled so that the system to use native UEFI graphic drivers.

To select the Boot Mode:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→Boot Mode** and press **Enter**.
2. Select a setting and press **Enter**.
   - **UEFI Mode** (default)—Configures the system to boot to a UEFI compatible operating system.
   - **Legacy BIOS Mode**—Configures the system to boot to a traditional operating system in Legacy BIOS compatibility mode.
3. Press **F10**.
4. Reboot the server.

UEFI Optimized Boot

Use this option to control whether the system BIOS boots using native UEFI graphic drivers. Leave it enabled for compatibility with VMware ESXi on a system configured for UEFI Boot Mode, and to enable and use **Secure Boot Mode**.

Before changing this setting, consider the following:

- If you are running Microsoft Windows 2008 or Windows 2008 R2 operating systems, and the system is configured for UEFI Boot Mode, this option must be set to disabled. Legacy BIOS Mode components are needed for video operations in Windows.
- **Boot Mode** must be set to **UEFI Mode** when this option is enabled. See “Boot Mode” (page 45).
- This option must be enabled to:
  - Enable and use **Secure Boot**. See “Secure Boot” (page 78).
  - Operate VMware ESXi.

Enabling or disabling UEFI Optimized Boot

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→UEFI Optimized Boot** and press **Enter**.
2. Select an option and press **Enter**.
   - **Enabled** (default)—Configures the system BIOS to boot using native UEFI graphic drivers. Select this setting for compatibility with VMware ESXi on a system configured for UEFI Boot Mode, and to enable and use **Secure Boot Mode**.
   - **Disabled**—Configures the system BIOS to boot using INT10 legacy video expansion ROM. Select this setting to boot Windows Server 2008 R2 in UEFI Boot Mode.
3. Press **F10**.

Boot Order Policy

Use this option to control the system behavior when attempting to boot devices per the **UEFI Boot Order** list and no bootable device is found.

Setting the boot order policy

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→Boot Order Policy** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Retry Boot Order Indefinitely** (default)—Configures the system to continuously attempt the boot order until a bootable device is found.
   - **Attempt Boot Order Once**—Configures the system to attempt to execute all items in the boot menu once, and halts the system.
   - **Reset After Failed Boot Attempt**—Configures the system to attempt to execute all items once, and reboots the system.
3. Press **F10**.

UEFI Boot Order

Use this option to change the order in which entries in the **UEFI Boot Order** list boot.

You can also configure the **UEFI Boot Order** list using the RESTful Interface Tool. See the RESTful Interface Tool documentation at: **http://www.hpe.com/info/restfulinterface/docs**.

Changing the UEFI boot order

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→UEFI Boot Order** and press **Enter**.
2. Use the arrow keys to navigate within the boot order list.

3. Press the **+** key to move an entry higher in the boot list.
4. Press the **-** key to move an entry lower in the list.
5. Press **F10**.

Advanced UEFI Boot Maintenance

- Add Boot Option
- Delete Boot Option

Add Boot Option

Use this option to select an x64 UEFI application with an .EFI extension, such as an OS boot loader or other UEFI application, to add as a new UEFI boot option.

The new boot option is appended to the UEFI Boot Order list. When you select a file, you are prompted to enter the boot option description (which is then displayed in the boot menu), as well as any optional data to be passed to an .EFI application.

Adding a boot option to the UEFI Boot Order list

1. Attach media with a FAT16 or FAT32 partition on it.
2. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→Advanced UEFI Boot Maintenance→Add Boot Option** and press **Enter**.
3. Browse for an .EFI application from the list and press **Enter**.
4. If necessary, continue to press **Enter** to drill-down through the menu options.
5. Enter a boot option description and optional data and press **Enter**.

   The new boot option appears in the **UEFI Boot Order** list.
6. Select **Commit changes and exit** to save your selection.

Delete Boot Option

Use this option to delete one or more applications from the **UEFI Boot Order** list.

Deleting boot options from the UEFI Boot Order list

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→Advanced UEFI Boot Maintenance→Delete Boot Option** and press **Enter**.
2. Select one or more options from the list. Press **Enter** after each selection.
3. Select an option and press **Enter**,
   - **Commit Changes and Exit**
   - **Discard Changes and Exit**

Legacy BIOS Boot Order

When your server is configured in Legacy BIOS Mode, you can use this setting to change the order in which the server looks for OS boot firmware within the **Legacy BIOS Boot Order** list.

Changing the Legacy BIOS boot order

Prerequisite

Boot Mode is set to **Legacy BIOS Mode**.

To change the Legacy BIOS boot order:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→Legacy BIOS Boot Order** and press **Enter**.
2. Use the arrow keys to navigate within the boot order list.
3. Press the **+** key to move an entry higher in the boot list.
4. Press the **-** key to move an entry lower in the list.
5. Press **F10**.

10 Configuring Network Options

Network Options

- Network Boot Options
- Pre-Boot Network Settings
- iSCSI Boot Configuration
- VLAN Configuration

Network Boot Options

- UEFI PXE Boot Policy
- IPv6 DHCP Unique Identifier
- Network Boot Retry Support
- Network Interface Cards (NICs)
- PCIe Slot Network Boot

UEFI PXE Boot Policy

Use this option to set the order of network boot targets in the **UEFI Boot Order** list. When set to Auto (the default setting) new network boot targets are added to the end of the list according to the default policy of the system ROM.

NOTE: When both IPv4 and IPv6 are enabled, each network boot target appears twice in the **UEFI Boot Order** list (one for IPv4 and the other for IPv6).

Setting the UEFI PXE Boot Policy

Prerequisite

Boot Mode is set to **UEFI Mode**.

To set the UEFI PXE Boot Policy:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Network Boot Options→UEFI PXE Boot Policy** and press **Enter**.
2. Select a setting and press **Enter**.
   - **IPv4 then IPv6**—Modifies the **UEFI Boot Order** list to include all existing IPv4 targets before any existing IPv6 targets. New network IPv4 boot targets are added before IPv6 targets.
   - **IPv4**—Removes all existing IPv6 network boot targets in the **UEFI Boot Order** list. New IPv6 network boot targets are not added to the list.
   - **IPv6**—Removes all existing IPv4 network boot targets in the **UEFI Boot Order** list. New IPv4 network boot targets are not added to the list.
   - **IPv6 then IPv4**—Modifies the **UEFI Boot Order** list to include all existing IPv4 targets before any existing IPv6 targets. New network IPv6 boot targets are added before IPv4 targets.
   - **Auto** (default)—Modifies the order of the existing network boot targets in the **UEFI Boot Order** list. New network boot targets are added to the end of the list using the system ROM's default policy.

3. Press **F10**.

IPv6 DHCP Unique Identifier

Use this option to control how the IPv6 DHCP Unique Identifier (DUID is set. **Auto**, the default setting, sets the DUID using the Universal Unique Identifier (UUID) of the server or, if the server is not available, the Link-Layer Address Plus Time (DUID-LLT) method. When set to DUID-LLT, the DUID is set based on the Link-Layer Address Plus Time (DUID-LLT) method.

Setting the IPv6 DHCP Unique Identifier method

Prerequisite

Boot Mode is set to **UEFI Mode**.

To set the IPv6 DHCP Unique Identifier method:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Network Boot Options→IPv6 DHCP Unique Identifier** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)—Sets the DUID using the Universal Unique Identifier (UUID) of the server or, if the server is not available, the Link-Layer Address Plus Time (DUID-LLT) method
   - **DUID-LLT**—Sets the DUID using the Link-Layer Address Plus Time (DUID-LLT) method.
3. Press **F10**.

Network Boot Retry Support

Use this option to enable or disable the network boot retry function. By default, the system BIOS attempts to boot the network device, such as a PXE device, up to 20 times before attempting to boot the next Initial Program Load (IPL) device.

Enabling or disabling Network Boot Retry Support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Network Boot Options →Network Boot Retry Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables network boot retry.
   - **Disabled**—Disables network boot retry.
3. Press **F10**.

Network Interface Cards (NICs)

Use this option to enable or disable network boot (PXE or FCoE) for an installed NIC. Devices listed vary from system to system and can include, for example:

- **Embedded LOM 1 Port 1**
- **Embedded FlexibleLOM 1 Port 1**

NOTE: You might need to configure the NIC firmware to activate the boot option.

Enabling or disabling network boot for a NIC

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Network Boot Options** and press **Enter**.
2. Select a NIC and press **Enter**.

3. Select a setting and press **Enter**.
   - **Network Boot** (default)—Enables network boot.
   - **Disabled**—Disables network boot
4. Press **F10**.
5. If you selected **Network Boot**, reboot the server so that the NIC boot option appears in the **UEFI Boot Order** list or the **Legacy BIOS Boot Mode** list.

PCIe Slot Network Boot

Use this option to enable or disable UEFI PXE boot for NIC cards in PCIe slots. Devices listed vary from system to system and can include, for example:

- **Slot 3 NIC Port 1 Boot**
- **Slot 3 NIC Port 2 Boot**

Enabling or disabling PCIe Slot Network Boot

Prerequisite

Boot Mode is set to **UEFI Mode**.

To enable or disable PCIe Slot Network Boot:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Network Boot Options →PCIe Slot Network Boot** and press **Enter**.
2. Select a PCIe slot entry and press **Enter**.
3. Select a setting and press **Enter**.
   - **PXE Boot** (default)—Enables PXE boot.
   - **Disabled**—Disables PXE boot.
4. Press **F10**.

Pre-Boot Network Settings

Use this option to configure a pre-boot network interface and related settings.

IMPORTANT: You do not need to use the Embedded UEFI Shell `ifconfig` command on a network interface if you plan to run `webclient` or `ftp` over the same interface because these interface and IP address settings are automatically selected by the **Pre-Boot Network Settings** configured in the System Utilities.

If the interface used by `ftp` and `webclient` happens to be configured by `ifconfig`, that setting is erased and, instead, the System Utilities **Pre-Boot Network Settings** menu is applied on the interface when the commands are run.

- **Pre-Boot Network Interface**—Specifies the network interface used for pre-boot network connections.
  - **Auto** (default)—The system uses the first available port with a network connection.
  - **Embedded NIC**—The system uses the selected NIC. If the selected NIC has more than one port, the system only uses the first available port with a network connection.
- **DHCPv4**—Enables or disables obtaining the pre-boot network IPv4 configuration from a DHCP server.
  - **Enabled** (default)—Enables DHCPv4 IPv4 network address configuration.

NOTE: This setting makes IPv4 address, subnet mask, gateway, and DNS settings unavailable because values are supplied automatically.

- **Disabled**—Disables DHCPv4 address configuration, requiring you to manually configure the following static IP address settings.
  - **IPv4 Address**
  - **IPv4 Subnet Mask**
  - **IPv4 Gateway**
  - **IPv4 Primary DNS**
  - **IPv4 Secondary DNS**

- **Boot from URL**—Specifies a network URL to a bootable ISO or EFI file. Enter a URL in either HTTP or FTP format, using either an IPv4 server address or host name. IPv6 addresses are not supported. When configured, this URL is listed as a boot option in the UEFI Boot menu. Then you can select this option from the boot menu to download the specified file to the system memory and enable the system to boot from the file.

  NOTE: To use this setting:

  - Configure the pre-boot network settings to access the URL location.
  - Leave the boot mode set to UEFI Boot Mode.

  When booting from an ISO file, use a file that the system can use to boot a preliminary operating system environment, such as WinPE, mini-Linux, or VMware ESX installer. Doing so enables further installation to proceed over an OS network connection. ISO files that contain the full OS installation media are not supported.

Configuring Pre-Boot Network Settings

Prerequisites

When using the **Boot from URL** setting:

- Configure the pre-boot network settings to access the URL location.
- Leave the boot mode set to **UEFI Mode**.
- When booting from an ISO file, use a file that the system can use to boot a preliminary operating system environment, such as WinPE, mini-Linux, or VMware ESX installer.

To configure Pre-Boot Network Settings:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→Pre-Boot Network Settings** and press **Enter**.
2. Select any of the Pre-Boot Network Settings options and press **Enter**, then select a setting or enter a value for that option and press **Enter** again.

iSCSI Boot Configuration

- iSCSI Initiator Name
- Add an iSCSI Boot Attempt
- Delete iSCSI Boot Attempts
- iSCSI Attempts

NOTE: You can also configure iSCSI Boot settings using the RESTful Interface Tool. See the RESTful Interface Tool documentation at: **http://www.hpe.com/info/restfulinterface/docs**.

iSCSI Initiator Name

Use this option to set a name for the iSCSI initiator using iSCSI Qualified Name (IQN) format. EUI format is not supported. This option overrides the default name set for the initiator.

Adding an iSCSI initiator name

Prerequisite

Boot Mode is set to **UEFI Mode**.

To add an iSCSI initiator name:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→iSCSI Boot Configuration→iSCSI Initiator Name** and press **Enter**.
2. Enter a unique name for the iSCSI initiator using iSCSI Qualified Name (IQN) format. For example: `iqn.2001-04.com.example:uefi-13021088`.
3. Press **Enter**.

Add an iSCSI Boot Attempt

Use this option to configure an iSCSI boot target.

Adding an iSCSI boot attempt

Prerequisite

- Boot Mode is set to **UEFI Mode**.

To add an iSCSI boot attempt:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→iSCSI Boot Configuration→Add an iSCSI Boot Attempt** and press **Enter**.

   A message appears stating that this boot attempt will not be in effect until the next server reboot.
2. Press **Enter**.
3. Select a port on which to attempt iSCSI boot and press **Enter**.
4. Complete the configuration settings and press **Enter** to save each setting.
   - **iSCSI Attempt Name**—Enter a name.
   - **iSCSI Boot Control**—Select **Enabled**. (The default setting is **Disabled**).
   - **IP Address Type**—Select **IPv4**.
   - **Connection Retry Count**—Enter a value from 0 to 16. Default is 0 (no retries).
   - **Connection Timeout**—Enter a value in milliseconds from 100 to 20000. Default is 1000.
   - **Initiator DHCP**—Press **Enter** to enable configuring the iSCSI initiator address from DHCP.

- **Target DHCP Config**—Disable this option (clear the check box), and enter a target name, IP address, port and boot LUN. This option is enabled by default.
- Optional: **Authentication Type**—If required, select **CHAP** and complete the CHAP entries.

5. Select **Save Changes**.

Delete iSCSI Boot Attempts

Use this option to delete one or more iSCSI boot targets.

Deleting iSCSI boot attempts

Prerequisite

Boot Mode is set to **UEFI Mode**.

To delete an iSCSI boot attempt:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→iSCSI Boot Configuration→Delete iSCSI Boot Attempts** and press **Enter**.
2. Select an iSCSI boot target entry and press **Enter**.
3. Select **Commit Changes and Exit**.

iSCSI Attempts

Use this option to view or modify the details of iSCSI boot attempts.

Viewing and modifying iSCSI boot attempt details

Prerequisite

Boot Mode is set to **UEFI Mode**.

To view and modify iSCI boot attempt details:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→iSCSI Boot Configuration→iSCSI Attempts** and press **Enter**.
2. Select an entry from the list and press **Enter** to view or modify the details about the boot attempt.

VLAN Configuration

Use this option to set the global VLAN configuration for all enabled network interfaces, including those used in PXE boot, iSCSI boot, and HTTP boot, and for all pre-boot network access from the Embedded UEFI Shell.

Configuring VLAN Configuration

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Network Options→VLAN Configuration** and press **Enter**.

2. Complete the following and press **Enter** after each selection or data entry.
    - **VLAN Control**—Select **Enabled** to enable VLAN tagging on all enabled network interfaces. This setting is disabled by default.
    - **VLAN ID**—When **VLAN Control** is enabled, enter a global VLAN ID of 0 to 4094 for all enabled network interfaces.
    - **VLAN Priority**—When **VLAN Control** is enabled, enter a priority value of 0 to 7 for VLAN tagged frames.
3. Press **F10**.

11 Configuring Storage Options

Storage Options

- Fibre Channel/FCoE Scan Policy
- Embedded Storage Boot Policy
- PCIe Storage Boot Policy

Fibre Channel/FCoE Scan Policy

Use this option to change the default policy for scanning for valid FC/FCoE (or boot from SAN) boot targets. By default, each installed FC/FCoE adapter only scans targets that are preconfigured in the device settings.

NOTE: This setting is only available in UEFI Boot Mode. For Fibre Channel controllers in PCIe slots, this setting is overridden by the PCIe Storage Boot Policy setting.

Changing the default Fibre Channel/FCoE scanning policy

Prerequisite

Boot Mode is set to **UEFI Mode**.

To change the scanning policy:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Storage Options→Fibre Channel/FCoE Scan Policy** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Scan All Targets**—Each installed FC/FCoE adapter scans all available targets.
   - **Scan Configured Targets Only** (default)—Each installed FC/FCoE adapter only scans targets that are preconfigured in the device settings. This setting overrides any individual device settings configured in the device-specific setup.
3. Press **F10**.

Embedded Storage Boot Policy

Use this option to select the UEFI BIOS boot targets for embedded storage controllers. By default, all valid boot targets attached to the storage controller are available to the **UEFI Boot Order** list.

Setting the embedded storage boot policy

Prerequisite

Boot Mode is set to **UEFI Mode**.

To set the embedded storage boot policy

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Storage Options→Embedded Storage Boot Policy** and press **Enter**.
2. Select a storage controller and press **Enter**.

3. Select a setting and press **Enter**.
   - **Boot All Targets** (default)—All valid boot targets attached to the storage controller are available to the **UEFI Boot Order** list.
   - **Boot Limit to 3 Targets**—A maximum of three boot targets attached to the storage controller are available to the **UEFI Boot Order** list.
   - **Boot No Targets**—No boot targets attached to the storage controller are available to the **UEFI Boot Order** list.
4. Press **F10**.

PCIe Storage Boot Policy

Use this option to select the UEFI BIOS boot targets for storage controllers in PCIe slots.

NOTE: This setting overrides the Fibre Channel/FCoE Scan Policy setting for Fibre Channel controllers in PCIe slots.

Setting the PCIe storage boot policy

Prerequisite

Boot Mode is set to **UEFI Mode**.

To set the embedded storage boot policy

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Storage Options→PCIe Storage Boot Policy** and press **Enter**.
2. Select a storage controller and press **Enter**.
3. Select a setting and press **Enter**.
4. Press **F10**.

12 Configuring the Embedded UEFI Shell

Embedded UEFI Shell options

- Embedded UEFI Shell
- Add Embedded UEFI Shell to Boot Order
- UEFI Shell Script Auto-Start
- Shell Auto-Start Script Location
- Network Location for Shell Auto-Start Script

More information

HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers

Embedded UEFI Shell

Use this option to enable or disable the **Embedded UEFI Shell**, a pre-boot command line environment for scripting and running UEFI applications, including UEFI boot loaders. The **Embedded UEFI Shell** also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS. When enabled, and Add Embedded UEFI Shell to Boot Order is enabled (the default settings) the **Embedded UEFI Shell** is added to the **UEFI Boot Order** list.

See the *HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers* for details on running Shell scripts.

Enabling or disabling the Embedded UEFI Shell

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Embedded UEFI Shell→Embedded UEFI Shell** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables you to launch the **Embedded UEFI Shell** from the pre-boot environment and add it to the **UEFI Boot Order** list. See Add Embedded UEFI Shell to Boot Order.
   - **Disabled**—The **Embedded UEFI Shell** is not available in the pre-boot environment and you cannot add it to the **UEFI Boot Order** list.
3. Press **F10**.

Add Embedded UEFI Shell to Boot Order

Use this option to add the **Embedded UEFI Shell** as an entry in the **UEFI Boot Order** list on the next reboot of the server.

Adding the Embedded UEFI Shell to the UEFI Boot Order list

Prerequisite

Boot Mode is set to **UEFI Mode**.

To add the Embedded UEFI Shell to the boot order list:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Embedded UEFI Shell→Add Embedded UEFI Shell to Boot Order** and press **Enter**.

2. Select a setting and press **Enter**.
   - **Enabled** (default)—Adds the embedded UEFI Shell to the boot order list on the next reboot.
   - **Disabled**—The embedded UEFI Shell is not added to the boot order list.
3. Press **F10**.

UEFI Shell Script Auto-Start

Use this option to enable or disable automatic execution of the Embedded UEFI Shell startup script during Shell startup.

- You can use the startup script to create a RAM disk, download files from the network, collect data, upload results back to network, and then boot to the OS without rebooting the system.
- You can store the script file on local media, or access it from a network location.
- You must name the script file `startup.nsh` and place it on local media or a network location accessible to the server.
- When auto-start is enabled, and the **Shell Auto-Start Script Location** option is set to **Auto**, the Shell looks for the script file in any of the FAT16 or FAT32 file systems available.
- It is recommended that you have only one `startup.nsh` file on one file system. See “Boot Mode” (page 45), and the *HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers*.

Enabling or disabling automatic execution of the Embedded UEFI Shell startup script

Prerequisites

- Boot Mode is set to **UEFI Mode**.
- Embedded UEFI Shell is enabled.

To enable or disable auto-start:

To enable or disable **UEFI Shell Script Auto-Start**:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Embedded UEFI Shell→UEFI Shell Script Auto-Start** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—The UEFI Shell startup script executes during Shell startup.
   - **Disabled** (default)—The UEFI Shell startup script does not execute during Shell startup.
3. Press **F10**.

Shell Auto-Start Script Location

Use this option to select the location of the Embedded UEFI Shell startup script. When **UEFI Shell Script Auto-Start** is enabled, this setting specifies where the Shell looks for the `startup.nsh` file. When set to **Auto**, the default setting, the Shell looks for the script file in any of the FAT16 or FAT32 file systems available.

Setting the Embedded UEFI Shell startup script location

Prerequisites

- Boot Mode is set to **UEFI Mode**.
- Embedded UEFI Shell is enabled.
- UEFI Shell Script Auto-Start is enabled.

To set the Embedded UEFI Shell startup script location:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Embedded UEFI Shell→Shell Auto-Start Script Location** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)—The Shell looks for the script file in any of the FAT16 or FAT32 file systems available.
   - **File Systems on Attached Media**—The Shell looks for the script file in a specific FAT16 or FAT32 file system.
   - **Network Location**—The Shell looks for the script file at a specific URL.
3. Press **F10**.

Network Location for Shell Auto-Start Script

Use this option to set the network URL location of the UEFI Shell startup script.

- You can specify a URL in HTTP or FTP format using either an IPv4 server address or host name.
- The script file at the location must end with a `.nsh` file extension.
- When **UEFI Shell Script Auto-Start** is enabled, and the **Shell Auto-Start Script Location** is set to **Network Location**, the Shell attempts to load and execute the startup script from the network location pointed to by the specified URL.

NOTE: IPv6 server addresses are not supported.

Setting the network location for the Shell auto-start script

Prerequisites

- Boot Mode is set to **UEFI Mode**.
- Embedded UEFI Shell is enabled.
- Shell Auto-Start Script Location is set to **Network Location**.

To set the network location for the Shell auto-start script:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Embedded UEFI Shell→Network Location for Shell Script-Auto Start** and press **Enter**.
2. Enter a network location and press **Enter**. Use HTTP or FTP format and an IPv4 server address or host name.
3. Press **F10**.

13 Configuring Power Management

Power Management options

- Power Profile
- Power Regulator
- Minimum Processor Idle Power Core C-State
- Minimum Processor Idle Power Package C-State
- Advanced Power Options

Power Profile

Use this option to select a power profile based on power and performance characteristics. **Balanced Power and Performance**, the default setting, provides optimum settings to maximize power savings with minimal impact to performance for most operating systems and applications.

Setting a power profile

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Power Profile** and press **Enter**.
2. Select a setting and **Enter**.
   - **Balanced Power and Performance** (default)—Provides optimum settings to maximize power savings with minimal impact to performance for most operating systems and applications.
   - **Minimum Power Usage**—Enables power reduction mechanisms that can negatively affect performance. This mode guarantees a lower maximum power usage by the system.
   - **Maximum Performance**—Disables all power management options that can affect negatively affect performance.
   - **Custom**—Enables you to configure settings for your environment.
3. Press **F10**.

Power Regulator

When **Power Profile** is set to **Custom**, use this option to set the power regulator mode for ProLiant support. Power regulator settings can help you increase server efficiency and manage power consumption. **Dynamic Power Savings Mode**, the default setting, automatically varies processor speed and power usage based on processor utilization.

NOTE: Certain processors support only one power state and operate at their initialized frequency, regardless of the selected **Power Regulator** mode.

Setting the Power Regulator mode

Prerequisite

Power Profile is set to **Custom**.

To select a Power Regulator mode:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Power Regulator** and press **Enter**.

2. Select a setting and press **Enter**.
   - **Dynamic Power Savings Mode** (default)—Automatically varies processor speed and power usage based on processor utilization. This mode uses an ROM-based algorithm to monitor processor activity. It can reduce overall power consumption with little or no impact to performance, and does not require OS support.
   - **Static Low Power Mode**—Reduces processor speed and power usage. Guarantees a lower maximum power usage for the system. This mode is useful in environments where power availability is constrained and it is critical to lower the maximum power use of the system.
   - **Static High Performance Mode**—Processors run in the maximum power and performance state, regardless of the OS power management policy. This mode is useful in environments where performance is critical and power consumption is less important.
   - **OS Control Mode**—Processors run in their maximum power and performance state at all times, unless the OS enables a power management policy.
3. Press **F10**.

Minimum Processor Idle Power Core C-State

When the **Power Profile** is set to **Custom**, use this option to select the lowest idle power (C-State) of the processor that the operating system uses. The higher the C-State, the lower the power usage of that idle state. By default, C-State is set to C6, the lowest setting.

Setting the minimum processor idle power core C-State

Prerequisite

Power Profile is set to **Custom**.

To select a minimum processor idle power core C-State setting:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Minimum Processor Idle Power Core C-State** and press **Enter**.
2. Select a setting and press **Enter**.
   - **C6 State** (default—lowest)
   - **C3 State**
   - **C1E State**
   - **No C-states**
3. Press **F10**.

Minimum Processor Idle Power Package C-State

When the **Power Profile** is set to **Custom**, use this option to configure the lowest processor idle power state (C-State). The processor automatically transitions into package C-States based on the Core C-States in which cores on the processor have transitioned. The higher the package C-State, the lower the power usage of that idle package state. The default setting, Package C6 (non-retention), is the lowest power idle package state supported by the processor.

NOTE: This option is available on servers with Intel processors.

Minimum Processor Idle Power Package C-State

Prerequisite

Power Profile is set to **Custom**.

To select a minimum processor idle power package C-State setting:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Minimum Processor Idle Power Package C-State** and press **Enter**.
2. Select an option and press **Enter**.
   - **Package C6 (retention) State** (default—lowest)
   - **Package C6 (non-retention) State**
   - **No Package State**
3. Press **F10**.

Advanced Power Options

- Intel QPI Link Power Management
- Intel QPI Link Frequency
- Energy/Performance Bias
- Maximum Memory Bus Frequency
- Channel Interleaving
- Maximum PCI Express Speed
- Dynamic Power Savings Mode Response
- Collaborative Power Control`
- Redundant Power Supply Mode
- Intel DMI Link Frequency

Intel QPI Link Power Management

Use this option to enable or disable power management for QPI (Quick Path Interconnect) links. When enabled, the default setting, QPI links are put into a low power state when the links are not being used. This lowers power usage with minimal performance effect.

NOTE: This option is available on servers with multiple Intel processors. You can configure it on systems with two or more CPUs.

Enabling or disabling Intel QPI Link Power Management

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Intel QPI Link Power Management** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables power management on QPI links.
   - **Disabled**—Disables power management on QPI links.
3. Press **F10**.

Intel QPI Link Frequency

Use this option to set the QPI link frequency to a low speed. Doing so can reduce power consumption, but can also impact system performance.

NOTE: You can configure this option on systems with two or more CPUs.

Setting the Intel QPI link frequency

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Intel QPI Link Frequency** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)
   - **Min QPI Speed**—Sets QPI link frequency to a low speed.
3. Press **F10**.

Energy/Performance Bias

When **Power Profile** is set to **Custom**, use this option to configure several processor subsystems to optimize the processor's performance and power usage. **Balanced Performance**, the default setting, provides optimum power efficiency and is recommended for most environments.

NOTE: Options vary by installed processors.

Setting the Energy/Performance Bias

Prerequisite

Power Profile is set to **Custom**.

To select an Energy/Performance Bias setting:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Energy/Performance Bias** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Maximum Performance**—Provides the highest performance and lowest latency. Use this setting for environments that are not sensitive to power consumption.
   - **Balanced Performance** (default)—Provides optimum power efficiency and is recommended for most environments.
   - **Balanced Power**—Provides optimum power efficiency based on server utilization.
   - **Power Savings Mode**—Provides power savings for environments that are power sensitive and can accept reduced performance.
3. Press **F10**.

Maximum Memory Bus Frequency

When **Power Profile** is set to **Custom**, use this option to configure the system to run memory at a lower maximum speed than that supported by the installed processor and DIMM configuration. **Auto**, the default setting, enables memory to run at the maximum speed supported by the system configuration.

Setting the maximum memory bus frequency

Prerequisite

Power Profile is set to **Custom**.

To select a maximum memory bus frequency setting:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Maximum Memory Bus Frequency** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)—Memory runs at the maximum speed supported by the system configuration.
   - **1333MHz**
   - **1066MHz**
   - **800MHz**
3. Press **F10**.

Channel Interleaving

When **Power Profile** is set to **Custom**, use this option to enable or disable a higher level of memory interleaving. Typically, higher levels of memory interleaving result in maximum performance. However, reducing the level of interleaving can result in power savings. The default setting of **Enabled** enables the highest level of interleaving for which the system memory is configured.

Enabling or disabling channel interleaving

Prerequisite

Power Profile is set to **Custom**.

To enable or disable channel interleaving:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Channel Interleaving** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables the highest level of interleaving for which the system memory is configured.
   - **Disabled**—Does not enable memory interleaving.
3. Press **F10**.

Maximum PCI Express Speed

When **Power Profile** is set to **Custom**, use this option to lower the maximum PCI-express speed at which the server enables PCI-express devices to operate. Doing so can resolve issues with problematic PCI-express devices. **Maximum Supported**, the default setting, enables the platform to run at the maximum speed supported by the platform or the PCIe device (whichever is lower.)

NOTE: Changing this setting from the default of **Maximum Supported** might affect the performance of high-end cards, such as 10GbE NIC cards and I/O accelerators.

Setting the maximum PCI-express speed

Prerequisite

Power Profile is set to **Custom**.

To set the maximum PCI-express speed:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Maximum PCI Express Speed** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Maximum Supported** (default)—Configures the platform to run at the maximum speed supported by the platform or the PCIe device (whichever is lower.)
   - **PCIe Generation 1.0**—Configures the platform to run at PCIe Generation 1.0, the lowest speed possible in the PCIe links.
3. Press **F10**.

Dynamic Power Savings Mode Response

When **Power Profile** is set to **Custom**, use this option to enable the system ROM to control processor performance and power state depending on the processor workload. The default setting of **Fast** enables a fast response time, and is optimal for most workloads where low latency response to an increase in processor demand is a requirement.

NOTE: Depending on your processor workload, changing this option from the default setting of **Fast** can negatively affect performance.

Setting the dynamic power savings mode response speed

Prerequisite

Power Profile is set to **Custom**.

To set dynamic power savings mode response speed:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Dynamic Power Savings Mode Response** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Fast** (default)—Sets a fast response time. This setting is optimal for most workloads where low latency response to an increase in processor demand is a requirement.
   - **Slow**—Sets a slow response time. This setting is optimal for workloads where a longer latency response to an increase in processing demand is an acceptable trade-off for reduced power consumption.
3. Press **F10**.

Collaborative Power Control

When **Power Profile** is set to **Custom**, use this option to enable or disable collaborative power control. For operating systems that support the Processor Clocking Control (PCC) interface, enabling collaborative power control (the default setting) configures the operating system to request processor frequency changes, even when the **Power Regulator** option is set to **Dynamic Power Savings Mode** on the server. For operating systems that do not support the PCC Interface, or when the **Power Regulator** mode is not configured for **Dynamic Power Savings Mode**, this option has no impact on system operation.

Enabling or disabling collaborative power control

Prerequisite

Power Profile is set to **Custom**.

To enable or disable collaborative power control:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Collaborative Power Control** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—The operating system requests processor frequency changes.
   - **Disabled**—The operating system does not request processor frequency changes.
3. Press **F10**.

Redundant Power Supply Mode

When **Power Profile** is set to **Custom**, use this option to set how the system handles redundant power supply configurations. All High Efficiency Mode settings provide the most power efficient operation when you are using redundant power supplies by keeping half of the power standby mode at lower power usage levels. **Balanced Mode**, the default setting, shares the power delivery equally between all installed power supplies.

Setting the redundant power supply mode

Prerequisite

Power Profile is set to **Custom**.

To set the redundant power supply mode:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Redundant Power Supply Mode** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Balanced Mode** (default)—Shares the power delivery equally between all installed power supplies.
   - **High Efficiency Mode (Auto)**—The system selects between the odd or even power supply based on a semi-random distribution within a group of systems.
   - **High Efficiency Mode (Odd Supply Standby)**—The system places the odd power supply in standby.
   - **High Efficiency Mode (Even Supply Standby)**—The system places the even power supply in standby.
3. Press **F10**.

Intel DMI Link Frequency

Use this option to force the link speed between the processor and south bridge to run at slower speeds. Doing so can reduce power consumption, but can also impact system performance.

NOTE: You can configure this option on systems with two or more CPUs.

Intel DMI Link Frequency

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Power Management→Advanced Power Options→Intel DMI Link Frequency** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)
   - **Min QPI Speed**
3. Press **F10** .

14 Configuring Performance Options

Performance Options

- Intel (R) Turbo Boost Technology
- ACPI SLIT Preferences
- Advanced Performance Tuning Options

Accessing Performance Options

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options** and press **Enter**.
2. Select any of the Performance Options and press **Enter**.

Intel (R) Turbo Boost Technology

Use this option to enable or disable Intel Turbo Boost Technology. The technology controls whether the processor transitions to a higher frequency than the processor's rated speed if the processor has available power and is within temperature specifications.

Enabling or disabling Intel Turbo Boost Technology

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Intel (R) Turbo Boost Technology** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables the logical processor cores on processors supporting hyperthreading technology.
   - **Disabled**—Reduces power usage and also reduces the system’s maximum achievable performance under some workloads.
3. Press **F10**.

ACPI SLIT Preferences

Use this option to enable or disable the Advanced Configuration and Power Interface System Locality Information Table (ACPI SLIT). It defines the relative access times between processors, memory subsystems, and I/O subsystems. Operating systems that support the SLIT can use this information to improve performance by allocating resources and workloads more efficiently.

Enabling or disabling ACPI SLIT preferences

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→ACPI SLIT Preferences** and press **Enter.**
2. Select a setting and press **Enter**.
   - **Enabled**—Enables ACPI SLIT.
   - **Disabled** (default)—Does not enable ACPI SLIT.
3. Press **F10**.

Advanced Performance Tuning Options

- Node Interleaving
- Intel NIC DMA Channels (IOAT)
- HW Prefetcher

- Adjacent Sector Prefetcher
- DCU Stream Prefetcher
- DCU IP Prefetcher
- QPI Snoop Configuration
- QPI Bandwidth Optimization (RTID)
- Memory Proximity Reporting for I/O
- I/O Non-posted Prefetching
- NUMA Group Size Optimization
- Intel Performance Monitoring Support

Node Interleaving

Use this option to enable or disable NUMA node interleaving. Typically, you can obtain optimum performance on NUMA nodes by leaving this option disabled (the default setting). When this option is enabled, memory addresses are interleaved across the memory installed for each processor and some workloads might experience improved performance.

Enabling or disabling node interleaving

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→ Node Interleaving** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled—**Memory addresses are interleaved across the memory installed for each processor. All nodes must be of equal memory size. System performance might be impacted.
   - **Disabled** (default)—Disables node interleaving, providing optimum performance in most environments.
3. Press **F10**.

Intel NIC DMA Channels (IOAT)

Use this option to enable or disable DMA acceleration on Intel NICs. If your server does not have Intel NICs, leave this setting disabled.

Enabling or disabling DMA acceleration on Intel NICs

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→Intel NIC DMA Channels (IOAT)** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**
   - **Disabled** (default)
3. Press **F10**.

HW Prefetcher

Use this option to disable or enable the processor prefetch function. In most environments, leave it enabled for optimal performance. With certain workloads, disabling this option might provide a performance benefit. Do so only after performing application benchmarking to verify improved performance in a particular environment.

NOTE: This option is available on servers with Intel processors. Disabling this option is not recommended because it can degrade system performance.

Enabling or disabling the Intel prefetch function

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→HW Prefetcher** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Adjacent Sector Prefetcher

Use this option to disable or enable the adjacent sector prefetch function. In most environments, leave the option enabled for optimal performance. With certain workloads, disabling it might provide a performance benefit. Do so only after performing application benchmarking to verify improved performance in a particular environment.

IMPORTANT: Disabling this option is not recommended because it typically degrades system performance.

Enabling or disabling the adjacent sector prefetch function

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→Adjacent Sector Prefetch** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

DCU Stream Prefetcher

Use this option to enable or disable the DCU stream prefetch function. In most environments, leave the option enabled for optimal performance. With certain workloads, disabling it might provide a performance benefit. Do so only after performing application benchmarking to verify improved performance in a particular environment.

Enabling or disabling the DCU stream prefetch function

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→DCU Stream Prefetcher** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

DCU IP Prefetcher

Use this option to enable or disable the DCU IP stream prefetch function. In most environments, leave the option enabled for optimal performance. With certain workloads, disabling it might provide a performance benefit. Do so only after performing application benchmarking to verify improved performance in a particular environment.

Enabling or disabling the DCU IP stream prefetch function

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→DCU IP Prefetcher** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

QPI Snoop Configuration

Use this option to choose the snoop mode used by the processor and QPI bus. Changing this option can impact memory performance.

Setting the QPI snoop configuration

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→QPI Snoop Configuration** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Home Snoop** (default)—Provides high memory bandwidth in an average NUMA environment.
   - **Early Snoop**—Decreases memory latency, but might also result in lower overall bandwidth as compared to the other modes.
   - **Cluster on Die**—Provides increased memory bandwidth in highly optimized NUMA workloads.
3. Press **F10**.

QPI Bandwidth Optimization (RTID)

Use this option to configure the QPI link between two processors for optimal performance.

NOTE: Changing this option from the default setting of **Balanced Performance** can have a negative impact on memory and system performance.

Setting QPI Bandwidth Optimization (RTID)

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→QPI Bandwidth Optimization (RTID)** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Balanced Performance** (default)—Provides the best performance for most applications and benchmarks.
   - **Optimized for I/O (Alternate RTID)**—Increases bandwidth from I/O devices, such as GPUs, that rely on direct access to system memory.

     NOTE: This setting is available on systems with two or more CPUs.

3. Press **F10**.

Memory Proximity Reporting for I/O

Use this option to set whether the system ROM reports the proximity relationship between I/O devices and system memory to the operating system. Most operating systems can use this information to efficiently assign memory resources for devices, such as network controllers and storage devices.

NOTE: Certain I/O devices might not be able to take advantage of I/O handling benefits if their OS drivers are not properly optimized to support this feature. For more information, see your operating system and I/O device documentation.

Enabling or disabling Memory Proximity Reporting for I/O

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→Memory Proximity Reporting for I/O** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

I/O Non-posted Prefetching

Use this option to enable or disable the I/O non-posted prefetch function. In most environments, leave the option enabled for optimal performance. With certain workloads, disabling it might provide a performance benefit. Do so only after performing application benchmarking to verify improved performance in a particular environment.

Enabling or disabling I/O Non-posted Prefetching

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→I/O Non-posted Prefetching** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

NUMA Group Size Optimization

Use this option to configure how the system ROM reports the number of logical processors in a NUMA (Non-Uniform Memory Access) node. The resulting information helps the operating system group processors for application use.

Setting NUMA Group Size Optimization

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→NUMA Group Size Optimization** and press **Enter**.

2. Select a setting and press **Enter**.
   - **Clustered** (default)—Optimizes groups along NUMA boundaries, providing better performance.
   - **Flat**—Enables applications that are not optimized to take advantage of processors spanning multiple groups to utilize more logical processors.
3. Press **F10**.

Intel Performance Monitoring Support

Use this option to provide Intel Performance Monitoring Toolkit support to certain chipset devices .This option does not impact system performance.

Enabling or disabling Intel Performance Monitoring Support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Performance Options→Advanced Performance Tuning Options→Intel Performance Monitoring Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—Enables support.
   - **Disabled** (default)—Disables support.
3. Press **F10**.

15 Configuring Server Security

Server Security options

- Set Power On Password
- Set Admin Password
- One-Time Boot Menu (F11 Prompt)
- Intelligent Provisioning (F10 Prompt)
- Embedded Diagnostics
- Embedded Diagnostics Mode
- No-Execute Protection
- Processor AES-NI Support
- Intel (R) TXT Support
- Secure Boot
- Trusted Platform Module options

Set Power On Password

Use this option to set a password for accessing the server during the boot process. When powering-on the server, a prompt appears where you enter the password to continue. To disable or clear the password, enter the password followed by a / (slash) when prompted to enter the password.

NOTE: In the event of an Automatic Server Recovery (ASR) reboot, the power-on password is bypassed and the server boots normally.

Setting the power-on password

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Set Power On Password** and press **Enter**.
2. Enter your password and press **Enter**. A password can be:
   - 31 characters maximum
   - Any combination of numbers, letters, and special characters

   A message appears telling you the password setting is successful.
3. Confirm the password and press **Enter**.

   A message appears confirming that the password is set.
4. Press **F10**.

Set Admin Password

Use this option to set an administrator password to protect the server configuration. If enabled, you are prompted for this password before being allowed to modify the configuration.

Setting an administrator password

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Set Admin Password** and press **Enter**.

2. Enter the password and press **Enter**. A password can be:
   - 31 characters maximum
   - Any combination of numbers, letters, and special characters
3. Confirm the password and press **Enter**.

   A message appears confirming that the password is set.
4. Press **F10**.

One-Time Boot Menu (F11 Prompt)

Use this option to control whether you can press the **F11** key to boot directly to the **One-Time Boot Menu** during the current boot. This option does not modify the normal boot order settings. By default, this option is enabled, and you can boot directly into the **One-Time Boot Menu** in the **System Utilities** by pressing **F11** in the ProLiant main screen after a server reboot. See “One-Time Boot Menu options” (page 27).

Enabling or disabling the One-Time Boot Menu F11 prompt

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→One-Time Boot Menu (F11 Prompt)** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Intelligent Provisioning (F10 Prompt)

Use this option to control whether you can press the **F10** key to access Intelligent Provisioning from the ProLiant POST screen.

Enabling or disabling the Intelligent Provisioning F10 prompt

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Intelligent Provisioning (F10 Prompt)** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Embedded Diagnostics

Use this option to enable or disable UEFI **Embedded Diagnostics** functionality. When enabled (the default setting), you can launch it from the **System Utilities→Embedded Applications→Embedded Diagnostics** menu. See “Embedded Diagnostics” (page 30).

Setting Embedded Diagnostics to launch from the System Utilities

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Embedded Diagnostics** and press **Enter**.

2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables you to launch **Embedded Diagnostics**.
   - **Disabled**—Prevents you from launching **Embedded Diagnostics**.
3. Press **F10**.

Embedded Diagnostics Mode

Use this option select whether to view **Embedded Diagnostics** in auto or text console mode. See “Embedded Diagnostics” (page 30).

NOTE: If you connect to the server using a BIOS serial console, you must view **Embedded Diagnostics** in text mode and not in auto (graphical) mode.

Setting the Embedded Diagnostics viewing mode

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Embedded Diagnostics Mode** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)—Displays **Embedded Diagnostics** in graphical mode.
   - **Text Mode**—Displays **Embedded Diagnostics** in text mode. Select this if you connect to the server using a BIOS serial console.
3. Press **F10**.

No-Execute Protection

Use this option to enable or disable protection against malicious code and viruses on your system. When enabled, memory is marked as non-executable unless the location contains executable code. If viruses attempt to insert and execute code from non-executable memory locations, these viruses are intercepted and an exception is generated. This option is enabled by default.

NOTE: Enable this option if you are using a Virtual Machine Manager, such as VMware ESX/ESXi and Windows Hyper-V.

Enabling or disabling no-execute virus protection

Prerequisites

Your operating system must support this option for you to enable it.

To enable or disable no-execute virus protection:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→Server Security→No-Execute Protection** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Processor AES-NI Support

Use this option to enable or disable the Advanced Encryption Standard Instruction Set in the processor.

Enabling or disabling processor AES-NI support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Processor AES-NI Support** and press **Enter**.
2. elect a setting and press **Enter**.
   - **Enabled** (default)—Enables AES-NI support.
   - **Disabled**—Disables AES-NI support.
3. Press **F10**.

Intel (R) TXT Support

Use this option to enable or disable Intel TXT (Trusted Execution Technology) support for servers with Intel processors. Enabling the TXT support option automatically enables:

- All Intel processor cores
- Hyperthreading. See “Intel (R) Hyperthreading Options” (page 39).
- VT-d. See “Intel (R) VT-d” (page 41).
- TPM. See “Trusted Platform Module options” (page 84).

Disabling any of these features while TXT is enabled can prevent TXT from working properly.

Enabling or disabling Intel TXT support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Intel (R) TXT Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—Enables TXT support.
   - **Disabled** (default)—Disables TXT support.
3. Press **F10**.

Secure Boot

Secure Boot is a server security feature that is completely implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Pre-boot UEFI shell applications
- OS UEFI boot loaders

When Secure Boot is enabled:

- Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.
- Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot.

  For more information about supported operating systems, see the *UEFI System Utilities and Shell Release Notes for ProLiant Gen9 Servers* on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/ProLiantUEFI/docs**).

You can customize the certificates embedded in the UEFI BIOS by adding or removing your own certificates, either from a management console directly attached to the server, or by remotely connecting to the server using the iLO 4 Remote Console.

You can configure Secure Boot using:

- The **System Utilities** options described in the following sections.
- The RESTful API. For more information, see the Hewlett Packard Enterprise website **http://www.hpe.com/support/restfulinterface/docs**.

You can use the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Before you enable Secure Boot, make sure you:

- Select **UEFI Boot Mode**. See "Boot Mode" (page 45).
- Enable **UEFI Optimized Boot**. See "UEFI Optimized Boot" (page 45).

Secure Boot Settings

Secure Boot Enforcement

Use this setting to enable or disable Secure Boot.

Enabling or disabling Secure Boot

Prerequisite

To enable this option:

- Set Boot Mode to **UEFI Mode**.
- Enable UEFI Optimized Boot.

To enable or disable Secure Boot:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Secure Boot Enforcement** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**—Enables Secure Boot.
   - **Disabled** (default)—Disables Secure Boot.

Advanced Secure Boot Options

NOTE: Changing the default security certificates can cause the system to fail booting from some devices. It can also cause the system to fail launching certain system software such as Intelligent Provisioning.

Platform Key (PK) Options

- Enroll PK
- Delete Platform Key (PK)

Enroll PK

Use this option to enroll a PK certificate. A Platform Key protects the next key from uncontrolled modification.

Enrolling a PK certificate

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Platform Key (PK) Options→Enroll PK** and press **Enter**.
2. Select **Enroll PK Using File** and press **Enter**.
3. Enter the name of a file on an attached media device. Supported formats include .der, .cer, and .crt.
4. (Optional) To apply a signature GUID to this key:
   a. Select **Signature GUID (optional)** and press **Enter**.
   b. Enter an ID and press **Enter**. Use the following GUID format (36 characters): `11111111-2222-3333-4444-1234567890ab`.
      - For Hewlett Packard Enterprise certificates, enter `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
      - For Microsoft certificates, enter `77fa9abd-0359-4d32-bd60-28f4e78f784b`
      - For SUSE certificates, enter `2879c886-57ee-45cc-b126-f92f24f906b9`
5. Select **Commit changes and exit**.

Delete Platform Key (PK)

Use this option to delete a PK certificate.

NOTE: Deleting the Platform Key forces Secure Boot to be disabled until you enroll a new PK.

Deleting a PK certificate

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Platform Key (PK) Options→Delete Platform Key (PK)** and press **Enter**.
2. Select a key from the list and press **Enter**.
3. Press **Enter** to delete the key.

Key Exchange Key (KEK) Options

- Enroll KEK Entry
- Delete KEK Entry

Enroll KEK Entry

Use this option to enroll a Key Exchange Key certificate. The Key Exchange Key protects the signature database from unauthorized modifications. No changes can be made to the signature database without the private portion of this key.

Enrolling a KEK certificate

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Key Exchange Key (KEK) Options→Enroll KEK Entry** and press **Enter**.
2. Select **Enroll KEK using File** and press **Enter**.
3. Enter the name of a file on an attached media device. Supported formats include .der, .cer, and .crt.
4. (Optional) To apply a signature GUID to this key:
   a. Select **Signature GUID (optional)** and press **Enter**.
   b. Enter an ID and press **Enter**. Use the following GUID format (36 characters): `11111111-2222-3333-4444-1234567890ab`.
      - For Hewlett Packard Enterprise certificates, enter `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
      - For Microsoft certificates, enter `77fa9abd-0359-4d32-bd60-28f4e78f784b`
      - For SUSE certificates, enter `2879c886-57ee-45cc-b126-f92f24f906b9`
5. Select **Commit changes and exit**.

Delete KEK Entry

Use this option to delete a Key Exchange Key.

Deleting a KEK entry

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Platform Key (PK) Options→Delete KEK Entry** and press **Enter**.
2. Select a key from the list and press **Enter**.
3. Press **Enter** to delete the key.

Allowed Signatures Database (DB) Options

The Allowed Signatures Database maintains signatures of codes that are authorized to run on the platform. This menu displays the following options:

- Enroll Signature (Allowed DB)
- Delete Signature (Allowed DB)

Enroll Signature (Allowed DB)

Use this option to enroll a signature in the Allowed Signatures Database. This database maintains signatures of codes that are authorized to run on the platform.

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Allowed Signatures Database (DB) Options→Enroll Signature** and press **Enter**.
2. Select **Enroll Signature Using File** and press **Enter**.
3. Enter the name of a file on an attached media device. Supported formats include .der, .cer, and .crt.

4. (Optional) To apply a signature GUID to this signature:
   a. Select **Signature GUID (optional)** and press **Enter**.
   b. Enter an ID and press **Enter**. Use the following GUID format (36 characters): `11111111-2222-3333-4444-1234567890ab`.
      - For Hewlett Packard Enterprise certificates, enter `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
      - For Microsoft certificates, enter `77fa9abd-0359-4d32-bd60-28f4e78f784b`
      - For SUSE certificates, enter `2879c886-57ee-45cc-b126-f92f24f906b9`
5. Select **Commit changes and exit**.

Enrolling a signature in the Allowed Signatures Database

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Allowed Signatures Database (DB) Options→Enroll Signature** and press **Enter**.
2. Select **Enroll Signature Using File** and press **Enter**.
3. Enter the name of a file on an attached media device. Supported formats include .der, .cer, and .crt.
4. (Optional) To apply a signature GUID to this signature:
   a. Select **Signature GUID (optional)** and press **Enter**.
   b. Enter an ID and press **Enter**. Use the following GUID format (36 characters): `11111111-2222-3333-4444-1234567890ab`.
      - For Hewlett Packard Enterprise certificates, enter `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
      - For Microsoft certificates, enter `77fa9abd-0359-4d32-bd60-28f4e78f784b`
      - For SUSE certificates, enter `2879c886-57ee-45cc-b126-f92f24f906b9`
5. Select **Commit changes and exit**.

Delete Signature (Allowed DB)

Use this option to delete a signature from the Allowed Signatures Database.

Deleting a signature from the Allowed Signatures Database

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Allowed Signatures Database (DB) Options→Delete Signature** and press **Enter**.
2. Select a signature from the list and press **Enter**.
3. Press **Enter** to delete the signature.

Forbidden Signatures Database (DBX) Options

- Enroll Signature (Forbidden DB)
- Delete Signature (Forbidden DB)

Enroll Signature (Forbidden DB)

Use this option to enroll a signature in the Forbidden Signatures Database. The Forbidden Signatures Database maintains signatures of codes that are not authorized to run on the platform.

Enrolling a signature in the Forbidden Signatures Database

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Forbidden Signatures Database (DBX) Options→Enroll Signature** and press **Enter**.
2. Select **Enroll Signature Using File** and press **Enter**.
3. Enter the name of a file on an attached media device. Supported formats include .der, .cer, and .crt.
4. (Optional) To apply a signature GUID to this signature:
   a. Select **Signature GUID (optional)** and press **Enter**.
   b. Enter an ID and press **Enter**. Use the following GUID format (36 characters): `11111111-2222-3333-4444-1234567890ab`.
      - For Hewlett Packard Enterprise certificates, enter `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
      - For Microsoft certificates, enter `77fa9abd-0359-4d32-bd60-28f4e78f784b`
      - For SUSE certificates, enter `2879c886-57ee-45cc-b126-f92f24f906b9`
5. Select **Commit changes and exit**.

Delete Signature (Forbidden DB)

Use this option to delete a signature from the Forbidden Signatures Database.

Deleting a signature from the Forbidden Signatures Database

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Forbidden Signatures Database (DBX) Options→Delete Signature** and press **Enter**.
2. Select a signature from the list and press **Enter**.
3. Press **Enter** to delete the signature.

Delete all keys (PK, KEK, DB, DBX)

Use this option to delete all keys in the system, including the Platform Key.

NOTE: Changing the default security certificates can cause the system to fail booting from some devices, or to fail launching certain software such as Intelligent Provisioning.

Deleting all keys

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Delete all keys (PK, KEK, DB, DBX)** and press **Enter**.
2. Press **Enter** to delete all keys.

Reset all keys to platform defaults

Use this option to reset all keys to platform defaults.

Resetting all keys to platform defaults

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Secure Boot Settings→Advanced Secure Boot Options→Reset all keys to platform defaults** and press **Enter**.
2. Press **Enter** to reset all keys.

Trusted Platform Module options

Use this menu to access Trusted Platform Module (TPM) options for servers configured with a TPM. TPM enables the firmware and operating system to take measurements of all phases of the booting process. For information on installing and enabling the TPM module option, see the user documentation for your server model.

△ **CAUTION:** A TPM locks all data access if you do not follow proper procedures for modifying the server, including updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings.

Configuring Trusted Platform Module options

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Trusted Platform Module options** and press **Enter**.
2. Select an option and press **Enter**, then select a setting for that option and press **Enter** again. On servers configured with an optional TPM, you can set the following:
   - **TPM 2.0 Operation**—Sets the operational state of TPM 2.0. Options are:
     - **No Action** (default)—There is no TPM configured.
     - **Enabled**—TPM and **Secure Boot** (when enabled) are fully functional.
     - **Disabled**—TPM is visible but functionality is limited. This option also resets TPM to factory settings, clearing assigned passwords, keys, or ownership data.

       NOTE: Disabling TPM can prevent the server from booting to the TPM-aware operating system if the OS uses TPM measurements.
   - **TPM 2.0 Visibility** (default)—Sets whether TPM is hidden form the operating system. Options are:
     - **Visible** (default)
     - **Hidden**—Hides TPM from the operating system. **Secure Boot** is disabled and TPM does not respond to any commands. Use this setting to remove TPM options from the system without having to remove the actual hardware.
   - **TPM Binding**—Sets whether data is encrypted using a TPM bind key, which is a unique RSA key. Options are:
     - **Enabled**
     - **Disabled** (default)
   - **TPM UEFI Option ROM Measurement**—Enables or disables (skips) measuring UEFI PCI operation ROMs. Options are:
     - **Enabled** (default)
     - **Disabled**
3. Verify that your new **Current TPM Type** and **Current TPM State** settings appear at the top of the screen.
4. Press **F10**.

16 Configuring PCI devices

PCI Device Enable/Disable

Use this option to enable or disable embedded and added-in PCI devices. Disabling devices re-allocates the resources (memory, I/O, and ROM space and power) that are normally allocated to the device. By default, all devices are enabled.

Enabling or disabling a PCI device

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→PCI Device Enabled/Disable** and press **Enter**.
2. Select a device on the system from the list and press **Enter**.
3. Select **Enable** or **Disable** and press **Enter**.
4. Press **F10**.

17 Configuring Server Availability

Server Availability options

- ASR Status
- ASR Timeout
- Wake-On LAN
- POST F1 Prompt
- Power Button Mode
- Automatic Power-On
- Power-On Delay

ASR Status

Use the option to enable or disable ASR (Automatic Server Recovery). When enabled, the system automatically reboots if the server locks up. ASR is enabled by default.

Enabling or disabling ASR

Prerequisite

The System Management driver is loaded.

To enable or disable ASR

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→ASR Status** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**—Disables all ASR functionality.
3. Press **F10**.

ASR Timeout

When **ASR Status** is enabled, use this option to set the time to wait before rebooting the server in the event of an operating system crash or server lockup. When the server has not responded in the selected amount of time, the server automatically reboots.

Setting the ASR timeout

Prerequisite

ASR Status is enabled.

To set the ASR timeout:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→ASR Timeout** and press **Enter**.
2. Select a setting and press **Enter**.
   - **5 Minutes**
   - **10 Minutes** (default)
   - **15 Minutes**

- **20 Minutes**
- **30 Minutes**

3. Press **F10**.

Wake-On LAN

Use this option to enable or disable the ability of the server to power on remotely when it receives a special packet. When enabled, **Wake-On LAN** powers up the system remotely using a WOL-capable NIC. This option requires a WOL-capable NIC, NIC driver, and operating system.

NOTE: If you enable this option, remove all power cords before adding or removing any adapters. Some adapters can cause the system to power on when added or removed.

Enabling or disabling Wake-On LAN

Prerequisite

A WOL-capable NIC, NIC driver, and operating system

To enable or disable Wake-On LAN:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→Wake-On LAN** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled**
   - **Disabled** (default)
3. Press **F10**.

POST F1 Prompt

Use this option to configure how the system displays the `F1` key in the server POST screen. When enabled and an error occurs, you can press the `F1` key to continue with the server power up sequence.

A series of system tests execute during POST and:

- If failures occur that allow the system to continue operating, the system continues to boot and then posts a message.
- If critical components fail or are missing, the server attempts to boot. If it can boot, it posts a message and, when enabled, an `F1` prompt.
- If the system cannot run with the missing or failed components, it halts until those components are replaced.

Setting the POST F1 prompt delay

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→POST F1 Prompt** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Delayed 20 seconds** (default)—If an error occurs, the system pauses for 20 seconds at the `F1` prompt, and then continues to boot the OS.
   - **Delayed 2 seconds**—If an error occurs, the system pauses for two seconds at the `F1` prompt, and then continues to boot the OS.
   - **Disabled**—If an error occurs, the system bypasses the `F1` prompt and continues to boot.

3. Press **F10**.

Power Button Mode

Use this option to enable or disable momentary power button functionality. Power Button Mode does not affect the four-second power button override or the remote power control functionality.

Enabling or disabling momentary power button functionality

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→Power Button Mode** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—Enables the momentary power button functionality.
   - **Disabled**—Disables the momentary power button functionality.
3. Press **F10**.

Automatic Power-On

Use this option to configure how the server automatically powers on when AC power is applied to the system. By default, the system returns to its previous power state when AC power is restored after an AC power loss. The **Always Power On** option sets the system to always return to the “on” state, even if it was in the “off” state when power was lost.

Setting the automatic power-on state

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→Automatic Power-On** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Always Power On**—The system automatically returns to a power on state.
   - **Always Power Off**—The system automatically returns to a power off state.
   - **Restore Last Power State** (default)—The system automatically returns to its previous power off state.
3. Press **F10**.

Power-On Delay

Use this option to set whether or not to delay the server from turning on for a specified time. This enables staggering when servers power up after a power loss, which can prevent power usage spikes.

NOTE: These events override the **Power-On Delay** setting and immediately power on the server:

- Pressing the power button using the iLO Virtual Power Button
- **Wake-ON LAN** events
- RTC (Real-Time Clock) wake-up events

Setting the power-on delay

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Availability→Power-On Delay** and press **Enter**.

2. Select a setting and press **Enter**.
   - **No Delay** (default)
   - **Random Delay**
   - **15 Second Delay**
   - **30 Second Delay**
   - **45 Second Delay**
   - **60 Second Delay**
3. Press **F10**.

18 Configuring BIOS serial console and EMS options

BIOS Serial Console and EMS options

BIOS serial console and EMS console redirection enable you to view POST error messages and run RBSU remotely through a serial connection to the server COM port or iLO Virtual Serial port. To do so, you do not need a keyboard or mouse. This menu includes:

- BIOS Serial Console Port
- BIOS Serial Console Emulation Mode
- BIOS Serial Console Baud Rate
- EMS Console

NOTE: Some languages or characters might require that you use a specific emulation mode.

BIOS Serial Console Port

Use this option to configure how to redirect video and keystrokes through the serial port. When set, this option can interfere with non-terminal devices attached to the serial port. If this occurs, set it to disabled.

IMPORTANT: This option is not supported on Japanese or Simplified Chinese systems.

Configuring the BIOS serial console port

Prerequisites

To set (enable) the option, you must use:

- Terminal software with a Unicode character set (for example: UTF-8)
- A supported language other than Japanese or Simplified Chinese

To configure the BIOS serial console port:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→BIOS Serial Console and EMS→BIOS Serial Console Port** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)
   - **Disabled**
   - **Physical Serial Port**
   - **Virtual Serial Port**
3. Press **F10**.
4. If you enabled a BIOS serial console port, connect a null modem cable to the serial port/COM port on which it is enabled.

BIOS Serial Console Emulation Mode

Use this option to select a serial console emulation mode type. Your selection depends on the emulation you want to use in your serial terminal program (for example, Hyper Terminal or PuTTY). The BIOS emulation mode must match the selected mode in the terminal program. When you select ANSI mode, some special characters are displayed in the serial console (for example, a degree symbol °).

BIOS Serial Console Emulation Mode

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→BIOS Serial Console and EMS→BIOS Serial Console Emulation Mode** and press **Enter**.
2. Select a setting and press **Enter**.
   - **VT100** (default)
   - **ANSI**
   - **VT100+**
3. Press **F10**.

BIOS Serial Console Baud Rate

Use this option to set the transfer rate at which data is transmitted through the serial port.

Setting the BIOS serial console baud rate

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→BIOS Serial Console and EMS→BIOS Serial Console Baud Rate** and press **Enter**.
2. Select a setting and press **Enter**.
   - **9600**
   - **19200**
   - **38400**
   - **57600**
   - **115200** (default)
3. Press **F10**.

EMS Console

Use this option to configure the ACPI serial port settings for redirecting the Windows Server Emergency Management (EMS) console.

When setting this option for redirecting EMS through a network connection, do the following:

- If you are using iLO 4, select the value (COM1 or COM2) that corresponds to the resources assigned to the **Virtual Serial Port** in the **System Options→Serial Port Options** menu.
- If you are redirecting EMS through a physical serial port, select the value (COM1 or COM2) that corresponds to the resources assigned to the **Embedded Serial Port** in the **System Options→Serial Port Options** menu.

EMS Console in Windows Server 2008 and 2012

EMS provides input and output support for all Microsoft Windows kernel components, including the loader, setup, recovery console, OS kernel, blue screens, and the Special Administration Console. The Special Administration Console is a text mode management console that is available after Windows Server 2008 or 2012 OS is initialized.

Microsoft enables EMS in the OS, and you must also enable EMS in the ROM. When enabled, EMS assumes the serial port for redirection and can cause interference with other devices attached to the serial port. To avoid interference, EMS is disabled in the system ROM by default on ProLiant ML and DL servers. If EMS is disabled in Windows Server 2008 or 2012, configure the EMS console on a COM port, and reboot the server to update the `boot.ini` file.

Configuring the EMS console

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→BIOS Serial Console and EMS→EMS Console** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Disabled** (default)
   - **COM1**—Enables the EMS console on the COM1 port.
   - **COM2**—Enables the EMS console on the COM2 port.
3. Press **F10**.

19 Configuring Server Asset Information

Server Asset Information options

- Server Information
- Administrator Information
- Service Contact Information
- Custom POST Message

Selecting Server Asset Information options

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Asset Information** and press **Enter**.
2. Select an option and press **Enter**.

Server Information

Use this option to enter reference information for the server administrator. For text settings, enter a maximum of 14 characters. By default, all values are blank.

Entering server information

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Asset Information→Server Information** and press **Enter**.
2. Select a setting and press **Enter**, then complete or select an entry and press **Enter** again.
   - **Server Name**—Enter a server name.
   - **Server Asset Tag**—Enter a server asset number.
   - **Asset Tag Protection**—Select a setting:
     - **Unlocked**(default)
     - **Locked**—Locks asset tag information. The asset tag is not erased if you restore default system settings.
   - **Server Primary OS**—Enter a description of the primary OS of the server.
   - **Server Other Information**—Enter additional text describing the server.
   - **Power-On Logo**—Select a setting:
     - **Enabled** (default)—Displays the logo during system boot.
     - **Disabled**—Does not display the logo during system boot. This setting does not affect system boot times.
3. Press **F10**.

Administrator Information

Use this option to enter contact information for the server administrator. The number of characters allowed for each entry varies by server model. By default, all values are blank.

Entering administrator information

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Asset Information→Administrator Information** and press **Enter**.

2. Select a setting and press **Enter**, then complete an entry and press **Enter** again.
   - **Administrator Name**—Enter the server administrator's name.
   - **Administrator Phone Number**—Enter the server administrator's phone number.
   - **Administrator E-mail Address**—Enter the server administrator's e-mail address.
   - **Administrator Other Information**—Enter additional text relating to the server administrator.
3. Press **F10**.

Service Contact Information

Use this option to enter service contact information for the server administrator. The number of characters allowed for each entry varies by server model. By default, all values are blank.

Entering service contact information

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Asset Information→Service Contact Information** and press **Enter**.
2. Select a setting and press **Enter**, then complete an entry and press **Enter** again:
   - **Service Contact Name**—Enter the service contact's name.
   - **Service Phone Number**—Enter the service contact's phone number.
   - **Service Contact E-mail Address**—Enter the service contact's e-mail address.
   - **Service Contact Other Information**—Enter additional text relating to the service contact.
3. Press **F10**.

Custom POST Message

Use this option to enter a custom message of up to 60 characters to display during server POST on the ProLiant POST screen.

Entering a custom POST message

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Asset Information→Custom POST Message** and press **Enter**.
2. Enter a message of up to 60 characters and press **Enter**.
3. Press **F10**.

20 Configuring advanced platform configuration options

Advanced Options

ROM Selection

On a server with redundant ROMs, use this option to revert the server to a previous BIOS ROM image.

Selecting a ROM image

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→ROM Selection** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Use Current ROM** (default)
   - **Switch to Backup ROM**—Reverts to the image in use before the last flash event.
3. Press **F10**.

Video Options

Use this option to configure the video display. By default, the system BIOS disables the embedded video controller when an optional video controller is installed in the system. You can use this option to leave the embedded video controller enabled so that the iLO remote video functions properly and also provides dual-head video support. Early system startup video is always displayed to the embedded video controller.

NOTE:

- The ability to support dual-head video between the embedded and a stand-up device depends on support from the operating system. For more information, see your operating system documentation.
- When multiple optional video cards are installed, the card that is selected as primary is based on PCI enumeration, which varies by platform. You might have to remove and reinstall the cards in a different order to control which card is the primary controller.

Configuring the video display

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Video Options** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Add-in Video Enabled, Embedded Video Disabled** (default)—The system only displays video to the first discovered add-in video controller.
   - **Both Add-in and Embedded Video Enabled**—The system displays video to the embedded and the first discovered add-in video controller.
3. Press **F10**.

Embedded Video Connection

Use this option to configure an external video connection to the embedded video connection. By default, the external video connection to the embedded video controller is automatically disabled to save power when a monitor is not attached. It is enabled automatically when a monitor is attached (including when the server is operating).

Configuring an embedded video connection

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Embedded Video Connection** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Auto** (default)—The external video connection to the embedded video controller is automatically disabled to save power when a monitor is not attached. It is enabled automatically when a monitor is attached (including when the server is operating).
   - **Always Disabled**—The external video connection to the embedded video controller is disabled and a monitor connected to this port does not display except during system boot.
   - **Always Enabled**—The external video connection to the embedded video controller is always enabled. This option is only required if a monitor is attached with a monitor detection that does not function, causing Auto mode to not work properly.
3. Press **F10**.

Fan and Thermal Options

- Thermal Configuration
- Thermal Shutdown
- Fan Installation Requirements
- Fan Failure Policy
- Extended Ambient Temperature Support

Thermal Configuration

Use this option to select the fan cooling method for the system. Modifying this option is only advised for configurations that differ from typical Hewlett Packard Enterprise-supported configurations that cannot be cooled adequately via **Optimal Cooling**, the default setting.

Setting the thermal configuration

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Fan and Thermal Options→Thermal Configuration** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Optimal Cooling** (default)—Provides the most efficient solution by configuring fan speeds to the minimum required to provide adequate cooling.
   - **Increased Cooling**—Operates fans at a higher speed.
   - **Maximum Cooling**—Provides the maximum cooling available for the system.
3. Press **F10**.

Thermal Shutdown

Use this option to configure the system to shut down when a fan failure occurs in non-redundant fan mode. A shutdown is initiated due to non-redundant fan failures or temperature increases beyond the pre-set threshold. If disabled, the System Management Driver ignores thermal events and the system immediately powers off in data-destructive situations.

Enabling or disabling thermal shutdown

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Fan and Thermal Options→Thermal Shutdown** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)—The server automatically shuts down when the internal server temperature reaches within five degrees of the critical level.
   - **Disabled**—The server does not automatically shut down when the internal server temperature reaches within five degrees of the critical level. Shutdown occurs when the temperature reaches the critical level.
3. Press **F10**.

Fan Installation Requirements

Use this option to configure how the server reacts when all required fans are not installed. Operating the server without the required fans can result in damage to the hardware components. By default, the server displays messages and log events to the IML when required fans are not installed. The server can still boot and operate.

Setting fan installation requirements messaging

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Fan and Thermal Options→Fan Installation Requirements** and press **Enter**.

   Select a setting and press **Enter**.
   - **Enable Messaging** (default)—The server displays messages and log events to the IML when required fans are not installed. The server can still boot and operate. This is the recommended setting.
   - **Disable Messaging**—The server does not display message and log events when required fans are not installed. All indications that the server is operating without required fans are removed.
2. Press **F10**.

Fan Failure Policy

Use this option to configure how the server reacts when fans fail, resulting in the server not having required fans in operation.

NOTE: Operating a server without the required fans installed and operating is not recommended and can impact the ability for the system to cool components properly. It can also result in damage to hardware components.

Setting the fan failure policy

Use this option to configure how the server reacts when fans fail, resulting in the server not having required fans in operation. By default, the server cannot boot or operate if it does not have required fans operating due to one or more fan failures

NOTE: Operating a server without the required fans installed and operating is not recommended and can impact the ability for the system to cool components properly. It can also result in damage to hardware components.

To set the **Fan Failure Policy**:

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Fan and Thermal Options→Fan Failure Policy** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Shutdown/Halt on Critical Fan Failures** (default)—The server cannot boot or operate if it does not have required fans operating due to one or more fan failures. This is the recommended setting.
   - **Allow Operation with Critical Fan Failures**—The server can boot and operate if it does not have required fans operating due to one or more fan failures.

   Press **F10**.

Extended Ambient Temperature Support

Use this option to enable the server to operate at higher ambient temperatures than are normally supported.

NOTE: This option is only supported by specific hardware configurations. See your HPE server documentation before enabling extended ambient temperature support. Improper system operation or damage to hardware components can result from enabling these features in unsupported configurations.

Enabling or disabling higher ambient temperature support

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Fan and Thermal Options→Extended Ambient Temperature Support** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Disabled** (default)
   - **Enabled for 40c Ambient (ASHRAE 3)**—Enables the server to operate in environments with ambient temperatures up to 40 degrees Celsius.
   - **Enabled for 45c Ambient (ASHRAE 4)**—Enables the server to operate in environments with ambient temperatures up to 45 degrees Celsius.

   NOTE: Not all Gen9 servers support both 40c Ambient (ASHRAE 3) and 45c Ambient (ASHRAE 4).
3. Press **F10**.

Advanced System ROM Options

- NMI Debug Button
- PCI Bus Padding Options
- Consistent Device Naming
- Mixed Power Supply Reporting
- Serial Number
- Product ID

NMI Debug Button

Use this function to enable or disable debug functionality when the system experiences a software lock-up. The button generates a Non-Maskable Interrupt to enable the use of the operating system debugger. When enabled (the default setting), pressing the NMI Debug Button on the system board during normal operation halts the system.

Enabling or disabling the NMI debug button

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→NMI Debug Button** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

PCI Bus Padding Options

Use this option to enable or disable the default PCI Bus padding, which provides each expansion slot with an extra PCI Bus number. By default, the System BIOS pads one PCI bus for each expansion slot to allow expansion cards with PCI-PCI bridges to not affect current bus numbering schemes. Do not disable this option unless you encounter a specific problem with your expansion card.

Enabling or disabling PCI Bus padding

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→PCI Bus Padding Options** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Consistent Device Naming

Use this option to set the level of Consistent Device Naming. On supported operating systems, device naming controls how NIC ports are named based on their locations in the system.

NOTE: Existing NIC connections retain their names until reinstalled under the OS environment.

Enabling Consistent Device Naming

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→Consistent Device Naming** and press **Enter**.
2. Select a setting and press **Enter**.
   - **CDN Support for LOMs only**—Embedded NICs and FlexibleLOM (not NICs installed in expansion slots) are named based on their locations in the system.
   - **Disabled** (default)—All NIC ports are named based on their locations in the system.
3. Press **F10**.

Mixed Power Supply Reporting

Use this option to set whether the server logs messages when a mixed supply configuration is present. This is enabled by default.

Enabling or disabling mixed power supply reporting

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→Mixed Power Supply Reporting** and press **Enter**.
2. Select a setting and press **Enter**.
   - **Enabled** (default)
   - **Disabled**
3. Press **F10**.

Serial Number

Use this option to re-enter the server serial number after replacing the system board. Consult a qualified IT service specialist for assistance in modifying this value. This ID must match the ID located on the chassis.

Re-entering a chassis serial number

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→Serial Number** and press **Enter**.
2. Enter the serial number and press **Enter**.
3. Press **F10**.
4. Press **Enter**.

Product ID

Use this option to re-enter the server product ID after replacing the system board. This ID must match the ID located on the chassis.

Re-entering a product ID

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→Product ID** and press **Enter**.
2. Enter the product ID and press **Enter**.
3. Press **F10**.
4. Press **Enter**.

21 Configuring the date and time and system defaults

Date and Time

Date and Time

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Date and Time** and press **Enter**.
2. Select a setting and press **Enter**, then complete your entry and press **Enter** again.
   - **Date (mm-dd-yyyy)**—Enter the date in a month-day-year (mm-dd-yyyy) format.
   - **Time (hh:mm:ss)**—Enter the time in a 24–hour format (hh:mm:ss) format.
   - **Time Zone**—Use the up and down arrow keys to select your current time zone for the system
   - **Daylight Savings Time**:
     - **Enabled**—Adjusts the local time displayed by one hour for Daylight Savings Time.
     - **Disabled** (default)—Does not adjust the local time displayed for Daylight Savings Time.
   - **Time Format**:
     - **Coordinated Universal Time (UTC)** (default)—Calculates the time stored in the hardware Real Time Clock (RTC) from the associated **Time Zone** setting.
     - **Local Time**—Removes the use of the **Time Zone** setting. This option is useful for addressing interaction issues between Windows operating systems set in Legacy BIOS boot mode.
3. Press **F10**.

Resetting system defaults

System Default Options

- Restore Default System Settings
- Restore Default Manufacturing Settings
- Default UEFI Device Priority
- User Default Options

Restore Default System Settings

Use this option to reset all BIOS configuration settings to their default values and immediately and automatically restart the server.

Selecting this option resets all platform settings except:

- **Secure Boot** BIOS settings
- **Date and Time** settings
- Primary and redundant **ROM Selection** (if supported)

You can save a custom default configuration to use during a system restore. Doing so saves settings you might otherwise lose. See “User Default Options” (page 103).

△ **CAUTION:** When you select use this option to reset configuration settings, any modifications that you have made might be lost.

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Default Options→Restore Default System Settings** and press **Enter**.
2. Select a setting and press **Enter**.
   - **No, cancel the restore procedure.**
   - **Yes, restore the default settings.**
3. Press **Enter** to reboot the server for changes to take effect.

Restoring default system settings

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Default Options→Restore Default System Settings** and press **Enter**.
2. Select a setting and press **Enter**.
   - **No, cancel the restore procedure.**
   - **Yes, restore the default settings.**
3. Press **Enter** to reboot the server for changes to take effect.

Restore Default Manufacturing Settings

Use this option to reset all BIOS configuration settings to their default manufacturing values and delete all UEFI non-volatile variables, such as boot configuration and Secure Boot security keys (if Secure Boot is enabled). Previous changes that you have made might be lost.

The difference between this action and the **Restore Default System Settings** option is that **Restore Default Manufacturing Settings** erases all UEFI variables. An OS can write UEFI variables that store such things as entries in the boot order and key database information for Secure Boot. When you **Restore Default Manufacturing Settings**, this information is cleared, whereas it is retained when you **Restore Default System Settings**.

You can save a custom default configuration to use during a system restore. Doing so saves settings you might otherwise lose. See “User Default Options” (page 103).

Restoring default manufacturing settings

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Default Options→Restore Default Manufacturing Settings** and press **Enter**.
2. Select a setting and press **Enter**.
   - **No, cancel the restore procedure.**
   - **Yes, restore the default settings.**
3. Press **Enter**.

Default UEFI Device Priority

Use this option to change the UEFI device priority that is used when default system settings are restored. The initial **UEFI Boot Order** list is created based on the priorities defined here. Before you change the priority list, you must configure and save user defaults as described in the next section, User Default Options. When the default configuration settings are loaded, the settings from the saved **Default UEFI Device Priority** list are used instead of the system or factory defaults.

Changing the default UEFI device priority

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Default Options→Default UEFI Device Priority** and press **Enter**.
2. Select an entry and press **Enter**.
3. Use the **+** key to move the entry higher in the list. Use the **-** key to move it lower in the list. Use the arrow keys to navigate through the list.
4. Press **F10**.

User Default Options

Use this option to save or erase a configuration as the custom default configuration. Configure the system as necessary and then enable this option to save the configuration as the default configuration. When the system loads the default settings, the custom default settings are used instead of the manufacturing defaults.

Saving or erasing user default options

1. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→System Default Options→User Default Options** and press **Enter**.
2. Select an option and press **Enter**, then select a setting for the option and press **Enter** again.
   - **Save User Defaults**
     - **Yes, Save**—Saves the current settings as the system default settings.
     - **No, Cancel** (default)—Does not save the current settings as the system default settings.
   - **Erase User Defaults**
     - **Yes, erase the current settings**—Erases (deletes) the current user-defined default settings. Once deleted, you can only restore these setting manually.
     - **No, Cancel** (default)—Does not erase the current user-defined default settings
3. Press **F10**.

22 Using scripted configuration flows

Scripted configuration flow

You can use BIOS/Platform Configuration (RBSU) with the Scripting Toolkit (STK) to create standard server configuration scripts to automate many of the manual steps in the server configuration process. You can find the STK on the Hewlett Packard Enterprise website (**http://www.hpe.com/servers/stk**).

The following utilities are provided in the toolkit:

- Configuration Replication Utility (CONREP)
- HPE Smart Storage Administrator (HPE SSA)

Configuration Replication Utility (CONREP)

CONREP with ProLiant Gen9 and other UEFI enabled servers is shipped in the STK and is a utility that operates with the BIOS/Platform Configuration (RBSU) to replicate hardware configuration on ProLiant Gen8 and later servers. This utility is run during State 0, Run Hardware Configuration Utility when performing a scripted server deployment. CONREP reads the state of the system environment variables to determine the configuration and then writes the results to an editable script file. This file can then be deployed across multiple servers with similar hardware and software components. For more information, see the *Scripting Toolkit User Guide* for your operating system environment on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/stk/docs**).

RESTful API support for UEFI

ProLiant Gen9 servers include support for configuring UEFI BIOS settings using the RESTful API, a management interface that server management tools can use to perform configuration, inventory, and monitoring of ProLiant server. A REST client uses HTTPS operations to configure supported server settings, such as iLO 4 and UEFI BIOS settings. For more information about the RESTful API and the RESTful Interface Tool, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/restfulinterface/docs**).

HPE Smart Storage Administrator (HPE SSA)

ProLiant Gen9 servers support Smart Storage Administrator (HPE SSA). HPE SSA Scripting is a standalone application that is distributed with the HPE SSA CLI application. For more information See the *Scripting Toolkit for Windows User Guide* (**http://www.hpe.com/support/STK_Windows_UG_en**), and the HPE SSA guides at: **http://www.hpe.com/info/smartstorage/docs**.

23 Troubleshooting

Basic troubleshooting techniques

The UEFI System Utilities provides basic troubleshooting tools you can use to resolve issues, including:

- Viewing the Integrated Management Log (IML) to see system events time stamped with one-minute granularity.
- Downloading an Active Health System Log (AHS).

  By default, the system downloads logs from the previous seven days if you do not use the **Range Start Date** and **Range End Date** fields to specify a different time period. When requested by Hewlett Packard Enterprise, you can copy your stored `.ahs` file, and email it to your customer support representative.

Cannot boot devices in UEFI Mode

Symptom

You see a message that the option or device you want to boot cannot be found, or it is listed in the system configuration as an unknown device.

Solution 1

Cause

You are attempting to boot to an option that does not have a UEFI Option ROM driver.

Action

Verify that your option card has a UEFI option driver (Option ROM) that supports either x64 or EFI Byte Code for boot functionality.

NOTE:

- UEFI drivers do not display messages on the System Utilities screen or provide function key prompts.
- If you replace the motherboard, UEFI variables are lost.
- You must configure PXE servers with a boot image. For x64 EFI machines, you must also configure the DHCP server to support x64 EFI DHCP boot requests. For more information, see the UEFI Information Library: **http://www.hpe.com/info/ProLiantUEFI/docs**.

Solution 2

Cause

You are attempting to boot to an option that is not supported or is not running the latest firmware.

Action

1. Refer to the Quick Specs or Read This First card for your server to make sure your card is supported before you install it. Although third-party UEFI cards might work, they are not optimized for ProLiant Gen9 servers running UEFI System Utilities.
2. Verify that the correct information is listed in the System Health settings for the option.
3. If necessary, use the latest SPP in offline mode to upgrade the firmware to the latest version.

Solution 3

Cause

You are booting Microsoft Windows 2008 R2, and UEFI Optimized Boot is enabled.

Action

Disable UEFI Optimized Boot.

Solution 4

Cause

You are booting VMware ESXi, and UEFI Optimized Boot is disabled.

Action

Enable UEFI Optimized Boot.

Solution 5

Cause

Your default boot mode settings are different than your user-defined settings.

Action

Save a custom default configuration to use during a system restore. See User Default Options.

Cannot restore system defaults

Symptoms

- After moving a drive from one server to another in Windows, you see an error message that certain settings cannot be found.
- After replacing a motherboard, you lose your configuration settings, such as Secure Boot.

Cause

Moving drives and replacing system hardware can disrupt pointers to previously-configured settings.

Action

Try the following options:

- Restore Default System Settings
- Restore Default Manufacturing Settings

It is a good practice to save a custom default configuration to use during a system restore. Doing so saves settings you might otherwise lose. See User Default Options.

Cannot download the file in the network boot URL

Symptom

You see an error message when you try to download the file in the URL you specified for a network boot.

Solution 1

Cause

The network connection settings you specified during static configuration are incorrect.

Action

1. Use the Embedded UEFI Shell `ping` command to check the network connection. See “Ping” in the *HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers*.
2. Change your static networking connection settings and try to download the file in URL again.

Solution 2

Cause

The DHCP server did not respond.

Action

1. Ensure there is a DHCP server available and it is operational.
2. Try to download the file in the URL again.

Solution 3

Cause

No cable is connected to the selected NIC port.

Action

1. Ensure there is a cable connection.
2. Try to download the URL again.

Solution 4

Cause

The file is incorrect or not present on the server, or it cannot be downloaded due to insufficient privileges. Check the file name and that it exists on the server. Make sure you have admin privileges on the server.

Action

1. Ensure the file is present, that you are using the correct file name and have sufficient privileges to download it.
2. Try to download the file in the URL again.

Solution 5

Cause

The HTTP or FTP server is down or did not respond.

Action

1. Ensure that the HTTP or FTP server you specified is available and that it is operational.
2. Try to download the file in the URL again.

Cannot network boot with the downloaded image file

Symptom

Booting from the image specified in the URL fails.

Solution 1

Cause

The image is not signed and **Secure Boot** is enabled.

Action

1. Ensure that the image is signed and that its Secure Boot settings are correct. See “Secure Boot” in the *HPE UEFI System Utilities User Guide for HPE ProLiant Gen9 Servers*.
2. Try to download the file in the URL again.

Solution 2

Cause

The downloaded file is corrupt.

Action

1. Select a new file.
2. Repeat the URL configuration, specifying the new file.
3. Try to download the new file in the URL.

Cannot deploy from the UEFI Shell script

Symptom

You attempted to deploy an OS using the UEFI Shell script and you see an error message that the deployment failed.

Cause

Configuration settings are not correct.

Action

1. Verify the following.
   - The Embedded UEFI Shell interface is added to the **UEFI Boot Order** list or **One-Time Boot Menu**.
   - When added to the **UEFI Boot Order** list, the Embedded UEFI Shell interface is the first boot option in **UEFI Boot Order** list so that it overrides other boot options to load.
   - UEFI Shell Script Auto-Start is enabled.
   - The correct `startup.nsh` script file location in attached media or a network location is specified. If it is in attached media, the `startup.nsh` script must be either inside the `fs`*`X`*`:\` or the `fs`*`X`*`:\efi\boot\` directory.
   - The `.nsh` script only contains supported commands.
   - Your system has enough RAM memory to create RAM disks during automated script execution.
   - Any OS boot loader or diagnostics application launched using the `.nsh script` is supported to run in UEFI the environment.
2. Try the deployment again.

24 Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    http://www.hpe.com/support/e-updates

  - Software Depot website:

    http://www.hpe.com/support/softwaredepot

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  http://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Related information

The latest documentation for the UEFI System Utilities and Embedded Shell is available at: **http://www.hpe.com/info/ProLiantUEFI/docs**. Available documents include:

- *HPE UEFI Shell User Guide for HPE ProLiant Gen9 Servers*
- *HPE UEFI Shell Quick Reference Card for HPE ProLiant Gen9 Servers*

- *HPE UEFI System Utilities and Shell Release Notes for HPE ProLiant Gen9 Servers*
- *HPE UEFI Deployment Guide for HPE ProLiant Gen9 Servers*

HPE UEFI System Utilities and Shell Command Mobile Help for HPE ProLiant Gen9 Servers is available by scanning the QR code located at the bottom of the System Utilities screen, or at **http://www.hpe.com/qref/ProLiantUEFI/Help**.

Websites

Website	Link
UEFI Specification	**http://www.uefi.org/specifications**
UEFI Learning Resources	**http://www.uefi.org/learning_center**
UEFI EDK2 project on SourceForge (download specifications and code)	**http://sourceforge.net/apps/mediawiki/tianocore**
Hewlett Packard Enterprise Information Library	**http://www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**http://www.hpe.com/support/hpesc**
Contact Hewlett Packard Enterprise Worldwide	**http://www.hpe.com/assistance**
Subscription Service/Support Alerts	**http://www.hpe.com/support/e-updates**
Software Depot	**http://www.hpe.com/support/softwaredepot**
Customer Self Repair	**http://www.hpe.com/support/selfrepair**
Insight Remote Support	**http://www.hpe.com/info/insightremotesupport/docs**

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Glossary

ACHI	Advanced Host Controller Interface
ACR	Array Configuration Replication Utility
ASR	Automatic Server Recovery
CHAP	Challenge-Handshake Authentication Protocol
CNA	Converged Network Adapter
CONREP	Configuration Replication utility
CPLD	Complex Programmable Logic Device. Controls the write access to the secure NVRAM using a write-once register that BIOS programs with a password during boot.
ECP	Extended Capabilities Port Mode
EFI	Extensible Firmware Interface
EMS	Emergency Management Services
EPP	Enhanced Parallel Port Mode
EUI	Extended Unique Identifier
IDE	Integrated Device Electronics
iLO	Integrated Lights-Out
IMD	Integrated Management Display
IML	Integrated Management Log
IOMMU	I/O Memory Management Unit
IPL	Initial Program Load
IRQ	Interrupt Request
iSCSI	Internet Small Computer System Interface
LPT	Local Port
MEMBIST	Memory Built-in Self Test
MPS	Multi-Processor Specification
NMI	Non-Maskable Interrupt
NUMA	Non-Uniform Memory Architecture
NVRAM	Non-Volatile Memory
ORCA	Option ROM Configuration for Arrays
PCC	Processor Clocking Control
PCI	Peripheral Component Interface
PCI-X	Peripheral Component Interconnect Extended
PCIe	Peripheral Component Interconnect Express
POST	Power-On Self-Test
PXE	Pre-Boot Execution Environment
QPI	Intel’s QuickPath Interconnect
RBSU	ROM-Based Setup Utility
ROM	Read-Only Memory
RTC	Real-Time Clock
SATA	Serial Advanced Technology Attachment
SPP	Standard Parallel Port Mode
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
VSP	Virtual Serial Port

Index