Hewlett Packard Enterprise

UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy

Abstract

This guide details how to access and use the Unified Extensible Firmware Interface (UEFI) that is embedded in the system ROM of all ProLiant Gen10 servers and HPE Synergy compute modules. 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: 881334-001a
Published: July 2017
Edition: 2

Notices

Acknowledgments

Contents

Getting started

UEFI System Utilities

The UEFI System Utilities is embedded in the system ROM. Its features 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 preboot environments.

HPE servers with UEFI 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.
- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.
- UEFI Graphical User Interface (GUI)
- An Embedded UEFI Shell that provides a preboot environment for running scripts and tools.
- 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.

UEFI System Utilities overview

Launching the System Utilities

Procedure

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, enter a directory or local user account name and password, and click **Log In**.
   c. Select **Remote Console & Media** in the iLO navigation tree.

      The Launch tab is displayed.
   d. Verify that your system meets the requirements for using the remote console application you want to use.
   e. Click the launch button for your selected application.

      You can also launch an iLO remote Console session by: Integrated Remote Console link on the **Information - iLO Overview** page.

      - Selecting Integrated Remote Console link on the **Information - iLO Overview** page.
      - Select the Console thumbnail in the low left corner of the iLO web interface then choose the application type to launch.
2. Restart or power on the server.

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

   The **System Utilities** screen appears.

Navigating the System Utilities

Procedure

1. Launch the System Utilities and do one of the following.
   - To navigate through the screens and modify settings, use your pointing device or press any of the navigational keys. Key functions are shown at the bottom of every System Utilities screen.

     TIP:

     When **Setup Browser Selection** is set to **Auto** (the default setting) or **GUI**, you can use your pointing device to navigate the System Utilities screens. When **Setup Browser Selection** is set to **Text**, you must use the navigational keys.
   - To access the mobile online help, scan the QR code on the bottom left 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 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.

Navigating the System Utilities in GUI mode

System Utilities GUI that allows you to navigate using either your pointing device or navigational keys. In GUI mode, selected menu items turn green.

NOTE:

GUI mode is not supported when you access the System Utilities using a serial console.

To set the browser mode to GUI:

Prerequisites

- The System Utilities is accessed through Integrated Remote Console or a physical terminal.
- **Setup Browser Selection** is set to **Auto** or **GUI**.

Procedure

1. From the **System Utilities** screen, select **Setup Browser Selection.**.
2. Select **Auto** or **GUI**.
3. Save the setting.
4. Reboot the system.

UEFI System Utilities GUI

HPE ProLiant Gen10 and HPE Synergy compute modules support a GUI UEFI System Utilities. Both mouse and keyboard devices are supported on the UEFI System Utilities GUI.

Regions

The System Utilities GUI has the following regions:

1. Caption Bar — This region shows the UEFI form title and the system buttons. The Form title shows the name of the form that you are currently navigating.
2. Navigation History — This region shows the forms to which you navigated previously. A Navigation History node is added to the navigation history each time you visit a new system utility form.
3. Server Information — This region shows server information and function key information.
4. System Utilities Form — This region shows the menu options of the current form.
5. Activity Bar — This region shows the system wide functions, such as function keys and the system status indicator.

Keyboard support in the GUI

The GUI has support for basic keys to navigate the system utilities form. The TAB key is used to change the focus on the different regions of the form. Supported keys include:

- Up and Down arrows
- Enter
- Function keys
- Esc key

Navigation History region and keyboard support

Navigation History shows system utility forms which user navigated previously. A Navigation History node is added to the Navigation History each time you visit a new form. You can Click a Navigation History node to return to the utility form that you previously visited.

If there are too many Navigation History nodes to fit on the Navigation History bar, the Home node is collapsed. To view a pop-up list of the navigation history node that you visited, you can select the Home node. To return to a previously accessed form, you can Click a Navigation History node from the list.

To move through the Navigation History region, you use the:

- Tab key to change focus in the Navigation History region.
- Enter key to get in to the Navigation History node selection mode and to select a node.
- Arrow keys to move to the node you want to select.
- Esc key to exit the Navigation History node selection mode.

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 in text browser mode, or to green in GUI mode.
- **Enter**—Selects an entry. A selected option changes color from white to yellow in text browser mode, or to green in GUI mode. When a submenu is available, the submenu appears.
- **Esc**—Returns to the previous screen.
- **F1**—Displays online help about a selection in text mode.

  NOTE:

  To display online help in GUI mode, click the **?** icon on the upper right corner of the System Utilities main screen.

- **F7**—Loads default UEFI BIOS configuration settings.

  NOTE:

  Pressing **F7** only resets the BIOS configuration. It does not reset other entities, such as option cards or iLO.

- **F10**—Prompts you to save changed settings.
- **F12**—Prompts you to save changed settings, and then exits the System Utilities.
- **Reboot Required** (radio button)—Is selected and turns red when changes require that you reboot the server.
- **Changes Pending** (radio button)—Is selected and turns red when changes are pending that must be saved to take effect.

When a reboot is required

For certain configuration changes to take effect, a reboot might be required. In such cases, one of the following occurs depending on your **Setup Browser Selection** that prompts you to do so.

- In GUI mode, the **Reboot Required** (radio button) is selected and turns red when changes require that you reboot the server.
- In text mode, a prompt appears on the applicable System Utilities screen.

System Utilities menu overview

NOTE:

UEFI system configuration options vary by server 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)**
- **iLO 5 Configuration Utility**
- Other system-specific devices, such as installed Smart Array devices, PCIe cards, and NICs. 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**
  - **Firmware Update**
  - **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 boot 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**.
2. **How do I transition from RBSU settings to UEFI settings?**

   The BIOS/Platform Configuration (RBSU) menu replaced the ROM-Based Setup Utility (RBSU). Use this menu to access and use UEFI options. See **BIOS/Platform Configuration (RBSU)**.
3. **How do I update the firmware or system ROM?**

   See **Updating firmware or system ROM**.
4. **How do I select a boot device?**

   See **Launching the System Utilities**. 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 Options**.

   To modify the boot order for all boots, see **Changing UEFI boot order**.
5. **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**.
6. **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**.

7. **How do I configure the time zone?**

   See **Setting the Date and Time**.

8. **How do I save my configuration changes and reboot the system?**

   a. 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.

   b. Press Y to save your changes.

      A `Change saved` confirmation prompt appears.

   c. 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.

9. **How do I enter the Embedded UEFI Shell?**

   See **Launching the Embedded UEFI Shell**.

10. **How do I view the health status of all installed options and devices?**

    See **Viewing System Health**.

11. **How do I use CONREP to replicate UEFI settings?**

    See **Configuration Replication Utility (CONREP)**.

12. **How do I set Jitter Control?**

    See **Configuring Advanced Performance Tuning options**.

13. **How do I tune performance with Workload Profiles?**

    See **Workload Profiles and performance options**.

14. **How do I use the RESTful Interface Tool or API to replicate the UEFI settings?**

    See the RESTful Interface Tool documentation on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/redfish**).

15. **How do I change the security settings on my server, such as Secure Boot or TPM?**

    See **Server Security Options**. Also see *HPE Gen10 Servers Intelligent System Tuning at* **http://www.hpe.com/support/gen10-intelligent-system-tuning-en**.

16. **What is HPE Intelligent System Tuning and how do I use it?**

    HPE Intelligent System Tuning (IST) includes modulate frequency control (jitter smoothing) and server tuning with workload profiles. See **Configuring Advanced Performance Tuning Options** and **Workload Profiles and performance options**.

Updating firmware or system ROM

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

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

Updating firmware from the System Utilities

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

Procedure

1. Access the System ROM Flash Binary component for your server from the Hewlett Packard Enterprise Support Center.
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**, and select **Embedded Applications** > **Firmware Update**.
5. Select a device.

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

   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 then select a firmware image.

   A device can have multiple firmware images.
9. Select **Start firmware update**.

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

System Configuration

System Configuration menu options

- BIOS/Platform Configuration (RBSU)
- iLO 5 Configuration Utility
- Other system-specific devices, such as installed PCIe cards, NICs, and Smart Arrays. For example, Embedded FlexibleLOM Port 1.

BIOS/Platform Configuration (RBSU)

The **BIOS/Platform Configuration (RBSU)** menu contains many of the nested options for accessing UEFI options, including:

- Workload Profile
- System Options
- Memory Options
- Virtualization Options
- Boot Options
- Network Options
- Storage Options
- Power and Performance Options
- Embedded UEFI Shell Options
- Power Management Options
- Server Security Options
- PCI Device Configuration Options
- Server Availability Options
- Advanced Options
- Date and Time
- System Default Options

Using the iLO 5 Configuration Utility

iLO 5 Configuration Utility options

You can access the iLO 5 Configuration Utility from the physical system console, or by using an iLO 5 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)—Specifies 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**—Specifies 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**—Specifies 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**—Specifies 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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **Network Options**.
2. Select any of the **Network Options**, and then select a setting or enter a value for that option.
3. Save your settings.

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **Advanced Network Options**.
2. Select any of the **Advanced Network Options**, and then select a setting or enter a value for that option.
3. Save your settings.

User Management

- **Add User**
- **Edit/Remove User**

Add User

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

New User iLO 5 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. After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the iLO 5 Configuration Utility, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- Host BIOS—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.

- Host NIC—Enables a user to configure the host NIC settings.
- Host Storage—Enables a user to configure the host storage settings.

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

Procedure

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

Edit/Remove User

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

Editing or removing user accounts

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **User Management** > **Edit/Remove User**.
2. Select the **Action** menu for the user name you want to edit or delete.
3. Select one of the following.
   - **Delete**—Deletes the user name.
   - **Edit**—Enables you to edit the user login name, password or user permissions.
4. Update as many user accounts as needed, and then save your settings.

Setting Options

Use this menu to view and configure iLO access settings.

- **iLO 5 Functionality**—Specifies whether iLO functionality is available. When this setting is enabled (default), the iLO network is available and communications with operating system drivers are active. When this setting is disabled, the iLO network and communications with operating system drivers are terminated.

  The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled.

NOTE:

For ProLiant blade servers, the iLO functionality cannot be disabled on blade servers.

- **iLO 5 Configuration Utility**—Enables or disables the iLO 5 Configuration Utility.

  If this option is set to **Disabled**, the iLO 5 Configuration Utility menu item is not available when you access the UEFI System Utilities.
- **Require Login for iLO 5 Configuration**—Determines whether a user-credential prompt is displayed when a user accesses the iLO 5 Configuration Utility.

  If this setting is **Enabled**, a login dialog box opens when you access the iLO 5 Configuration Utility.
- **Show iLO 5 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. Settings are:
  - **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. Settings (in bits per second) are:
  - **9600**
  - **19200**
  - **57600**
  - **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 5 Configuration Utility.
- **iLO Web Interface**—Specifies whether the iLO web interface can be used to communicate with iLO. This setting is enabled by default.

Configuring access settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **Setting Options**.
2. Update user access **Setting Options**.
3. Save your settings.

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 5 Configuration Utility until after the next system reboot. If you are managing iLO remotely, the remote console session is automatically ended.

If the server has a factory installed license key, the license key is retained.

Resetting iLO to the factory default settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **Set to factory defaults**.

   The iLO 5 Configuration Utility prompts you to select **YES** or **NO**.
2. Select **YES**.
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 5 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 5 Configuration Utility is not available again until the next reboot.

Resetting iLO active connections

Prerequisite

Configure iLO Settings privilege

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **Reset iLO**.

   The iLO 5 Configuration Utility prompts you to select **YES** or **NO**.
2. Select **YES**.
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 server complex programmable logic device version.
- **Serial Number**—The iLO serial number.
- **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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **iLO 5 Configuration Utility** > **About**.
2. View information **about** iLO components.

Viewing and configuring embedded device information

Viewing controller information

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Controller Information**.
2. In the Controller Information screen, view the information.

Configure controller settings

Modifying controller settings

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Configure Controller Settings** > **Modify Controller Settings**.
2. In the Modify Controller Settings screen, modify any of the following settings:

Setting	Description
Transformation priority	Rate at which requests from the operating system are processed: • High: Completes as fast as possible at the expense of normal I/O. • Medium: Completes with some impact on normal I/O. • Low: Performs when normal I/O is not occurring.
Rebuild priority	Determines the urgency with which the controller treats an internal command to rebuild a failed logical drive. • Low: Normal system operations take priority over a rebuild. • Medium: Rebuilding occurs for half of the time, and normal system operations occur for the rest of the time. • Medium high: Rebuilding is given a higher priority over normal system operations. • High: The rebuild takes precedence over all other system operations.
Surface Scan Analysis Priority	Modifies the amount of delay/idle time of the controller before surface scan analysis is resumed. • 0: Disabled • 1-30: Idle with delay • 31: High
Current parallel surface scan count	Controls how many controller surface scans can operate in parallel: • 1: Disabled • 16: Maximum
Physical Drive Write Cache State	On controllers and drives that support physical drive write cache, enable or disable the write cache for all drives that are part of a configured logical drive on the controller.
Spare Activation Mode	Predictive Spare Activation mode activates a spare drive any time a member drive within an array reports a predictive failure. Failure Spare Activation mode activates a spare drive when a member drive within an array fails using fault tolerance methods to regenerate the data.

3. Click **Submit changes**.

Modifying advanced controller settings

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Configure Controller Settings** > **Advanced Controller Settings**.
2. In the Advanced Controller Settings screen, modify any of the following settings:

Setting	Description
Degraded Mode Performance Optimization	Used to tune controller performance for video applications and requires the installation of a valid license key. Options are Enabled or Disabled.
Physical Drive Request Elevator Sort	Controls the behavior of the controller cache write Elevator sort algorithm. This option is used to tune controller performance for video applications and requires the installation of a valid license key. Options are Enabled or Disabled.
Alternate Inconsistency Repair Policy	Controls the behavior of the controller inconsistency repair Policy. This option is used to tune the controller performance for Video applications and requires the installation of a valid license key. Options are Enable or Disable.
Maximum drive Request Queue Depth	Controls the maximum number of physical drive requests that the firmware will submit to a drive at any given time. This option is used to tune controller performance for video applications. Options are 2, 4, 8, 16, 32, or Automatic.
Monitor and Performance Analysis Delay	Controls the behavior of the controller Monitor and Performance Analysis Delay and is expressed in values ranging from 0 to 60. This option is primarily used to tune controller performance for video applications and requires the installation of a valid license key.
HDD Flexible Latency Optimization	Reduces the maximum observed latency from a host request.

3. Click **Submit changes**.

Clearing the controller configuration

Clearing the controller configuration destroys the controller metadata, including array configurations and partition information.

CAUTION:

When you clear the controller configuration, all data on the attached media is no longer accessible and cannot be recovered.

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Configure Controller Settings** > **Clear Configuration**.
2. In the Clear Configuration screen, select one or both of the following: .
   - **Delete All Array Configurations** - deletes all the arrays in the controller. All the data in the arrays is also deleted.
   - **Delete RIS on All Physical Drives**- deletes RAID metadata on the drives that are not part of the array

Viewing the backup power source status

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Configure Controller Settings**
2. In the Backup Power Source screen, view the status of the backup power.

Managing power settings

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Configure Controller Settings** > **Manage Power Settings**.
2. In the Manage Power Settings screen, update any of the following settings.

Setting	Description
Power Mode	Options are: • Maximum performance (default)-- Power savings options that affect performance are disabled. • Balanced-- Use this setting to save power with minimal effects on performance. • Minimum power-- When settings are selected without regard to system performance, maximum power savings is achieved. Hewlett Packard Enterprise recommends the minimum power setting for specific applications, but it is not appropriate for most customers. Most applications will suffer significant performance reduction.
Survival Mode	Allows controller to throttle back dynamic power settings to minimum when temperature exceeds the threshold. This minimum setting allows the server to run in most situations, but performance may decrease.

3. Click **Submit changes**.

Configure arrays

Creating an array

When you create an array, you can select drives, specify RAID level, and configure array settings, including strip size and logical drive size.

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Create Array**.
2. In the Create Array screen, select each drive that you want to include in the array and click **Proceed to next Form**.

   NOTE:

   - Select drives of the same type, all SATA, or all SAS, for instance. Do not mix drive types.
   - If you use Smart Array S100i SW RAID, SAS drives are not supported.

3. In the Set RAID Level screen, select the RAID Level from the drop-down menu and click **Proceed to next Form**.
4. In the Set Logical Drive Configuration screen, specify the configuration settings or use the default selection.

Setting	Description
Logical Drive Label	Use the default selection for the drive label or enter a new label. The characters in the label can be alphanumeric or spaces.
Strip Size/Full Stripe Size	Strip size is the amount of data that is stored on each physical drive in the array. The full stripe size is the amount of data that the controller can read or write simultaneously on all the drives in the array. For RAID levels that support fault tolerance through parity, the parity information is calculated one full strip size at a time. You can specify from 8KiB to 1024KiB, depending on the number of disks and RAID level. The default value is all available space. If you use Smart Array S100i SW RAID, the minimum size is 16KiB and the maximum size is 256KiB.
Sectors Per Track	Number of sectors per track presented to the operating system as part of the legacy disk geometry (C/H/S) information.
Size	Values in decimal; minimum RAID size is 16 MiB.
Unit Size	Logical drive unit size (MiB/GiB/TiB)
Acceleration Method	Logical drive acceleration method (controller cache or none)

5. Click **Submit Changes**.

For the array creation to complete, a reboot is required.

Managing an array

Viewing logical drive properties

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **List Logical Drives** > ***logical drive*** > **Logical Drive Details**.
2. In the Logical Drive Details screen, view the details.

Creating a logical drive

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **Create Logical Drive**
2. In the Create Logical Drive screen, select the RAID level, and click **Proceed to next Form**.
3. In the Set Logical Drive Configuration screen, use the default values for the configuration or specify different values.

Setting	Description
Logical Drive Label	Use the default selection for the drive label or enter a new label. The characters in the label can be alphanumeric or spaces.
Strip Size/Full Stripe Size	Strip size is the amount of data that is stored on each physical drive in the array. The full stripe size is the amount of data that the controller can read or write simultaneously on all the drives in the array. For RAID levels that support fault tolerance through parity, the parity information is calculated one full strip size at a time. You can specify from 8KiB to 1024KiB, depending on the number of disks and RAID level. The default value is all available space. If you use Smart Array S100i SW RAID, the minimum size is 16KiB, and the maximum size is 256KiB.
Sectors Per Track	Number of sectors per track presented to the operating system as part of the legacy disk geometry (C/H/S) information.
Size	Values in decimal; minimum RAID size is 16 MiB.
Unit Size	Logical drive unit size (MiB/GiB/TiB)
Acceleration Method	Logical drive acceleration method (controller cache or none)

4. Click **Submit Changes**.

Assigning spare drives

A spare is a drive that automatically replaces a failed drive in a logical drive.

Prerequisites

A spare drive must meet the following criteria.

- It must be an unassigned drive or a spare drive for another array.
- It must be the same type as existing drives in the array (for example, SATA or SAS).
- The drive capacity must be greater than or equal to the smallest drive in the array.

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **Manage Spare Drives**.
2. In the Manage Spare Drives screen, select the spare activation type:
   - **Assign Dedicated Spare**
   - **Assign Auto Replace Spare**
3. Select the drive that you want to assign as a spare.

NOTE:

Only drives that meet the criteria listed in the prerequisites are displayed.

Deleting a spare drive

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **Manage Spare Drives** > **Delete Spare Drives**.
2. From the Delete Spare Drives screen, select the spare that you want to delete, and click **Delete Spare Drives**.

Identifying a device

Use the UEFI System Utilities to identify a drive by blinking its LED.

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **Identify Device**.
2. In the Identify Device screen, specify the duration (in seconds) that you want the LED to blink, select the drive configuration type, and click **Start**.

To stop blinking the LED, click **Stop**.

Deleting an array

This procedure deletes:

- All the logical drives on the array.
- All data on the logical drives that are part of the array.

If the deleted array is the only one on the controller, the controller settings are erased, and the default configuration is restored.

To delete an individual logical drive, see "Deleting a logical drive."

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **Delete Array**.
2. In the Delete Array screen, click **Submit Changes**.

Editing a logical drive

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **List Logical Drives** > ***logical drive*** > **Edit Logical Drive**.
2. In the Edit Logical Drive screen, edit any of the following settings.

Setting	Description
Acceleration method	Acceleration method can increase database performance by writing data to the cache memory instead of directly to the logical drives. Options are: • Controller cache--writes data to the cache memory. • None--disables caching to reserve the cache module for other logical drives on the array.
Logical drive label	This label value appears in the Logical Drive Details screen. The label can contain alphanumeric characters and spaces only.

3. Click **Submit Changes**.

Deleting a logical drive

Use this procedure to delete an individual logical drive. To delete all logical drives in an array, see "Deleting an array."

IMPORTANT:

If you delete the logical drive, any data on the logical drive is deleted as well. If the logical drive that you are deleting is the only logical drive in the array, the array is also deleted.

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Array Configuration** > **Manage Arrays** > ***array*** > **List Logical Drives** > ***logical drive*** > **Delete Logical Drive**.
2. In the Delete Logical Drive screen, click **Submit Changes**.

Disk Utilities

Viewing disk device information

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Disk Utilities** > ***disk*** > **Device Information**.
2. In the Device Information screen, view the information.

Identifying a disk device

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Disk Utilities** > ***disk*** > **Identify Device**.
2. In the Identify Device screen, specify the duration (in seconds) that you want the LED to blink, select the drive configuration type, and click **Start**.

To stop blinking the LED, click **Stop**.

Setting bootable devices for Legacy Boot Mode

Setting the primary and secondary bootable devices (Legacy Boot Mode)

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Set Bootable Device(s) for Legacy Boot Mode** > **Select Bootable Logical Drive** > ***logical drive***.
2. In the *Logical Drive* screen, select either of the following:
   - **Set as Primary Bootable Device**
   - **Set as Secondary Bootable Device**

Setting the number of OS bootable drives (Legacy Boot Mode)

Procedure

1. From the System Utilities screen, select **System Configuration** > ***controller*** > **Set Bootable Device(s) for Legacy Boot Mode** > **Number of OS bootable drives**.
2. In the Number of OS bootable drives screen, specify the number of OS bootable drives.
3. Click **Submit Changes**.

Viewing and configuring NIC and FCoE settings

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

Procedure

1. From the **System Utilities** screen, select **System Configuration**.
2. Select a device.

   A **System Configuration** screen displays information about the embedded device.
3. View, select, or enter settings.
4. Save your settings.

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 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.

- Internal SD Card
- 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

Procedure

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

Embedded Applications

Launching the Embedded UEFI Shell

Use the **Embedded UEFI Shell** 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 UEFI boot loaders. The Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS.

Prerequisites

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

Procedure

1. From the **System Utilities** screen, select **Embedded Applications** > **Embedded UEFI Shell**.

   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.

Viewing or clearing the Integrated Management Log

Use the **Integrated Management Log** (IML) option to view or clear the 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 time stamps each event with one-minute granularity.

Procedure

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

Logging in to Active Health System Viewer

Procedure

1. To access the AHSV web page, go to **http://www.hpe.com/servers/ahsv** in a supported browser. Supported browsers include:
   - Internet Explorer 11
   - Chrome 51 or later
   - Firefox 46 or later
2. Enter your **User ID** (email address) and **Password** and click **Sign In**.

NOTE:

To log in using an HPE Passport account, or to create an HPE Passport account, go to **http://www.hpe.com/info/insightonline**. In most cases, your HPE Passport account is the same as the email address you used during the HPE Passport account registration process. If you changed your user ID in the Hewlett Packard Enterprise Support Center, be sure to log in with your user ID and not your email address.

NOTE:

To have the system remember your log in credentials, select **Remember Me** before clicking **Sign In**.

Downloading Active System Health data

HPE Support used the Active Health System (AHS) log file for problem resolution. The high level steps for submitting a case are:

Procedure

1. Download an AHS Log from the server experiencing a support issue. See **Downloading an Active Health System Log**
2. Upload the AHS Log to the Active Health System Viewer (http://www.hpe.com/servers/AHSV). See **Uploading an AHS log to AHSV**
3. Review the Fault Detection Analytics for any self-repair actions/recommendations. See the *AHSV User Guide* for more information.
4. Create a support case using the AHSV Navigation menu. See the *AHSV User Guide* for more information.

Downloading an Active Health System Log

By default, the system downloads an **Active Health System Log** 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.

Procedure

1. From the **System Utilities** screen, select **Embedded Applications** > **Active Health System Log**.
2. Select **Download Active Health System Log**.
3. Select or enter the following.
   - **Download Entire Log**—Unless you a support representative advises you 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 option 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**.

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 or use the **Uploading an AHS log to AHSV** task.

NOTE:

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

Uploading an AHS log to AHSV

The maximum file size limit is 250 MB. For logs that are larger than 250 MB, contact the HPE Support Center for assistance.

This task in done from the AHSV, not from System Utilties.

Prerequisites

IMPORTANT:
The server from which the AHS log was created must have a valid warranty. If the server is out of warranty, an error message is displayed: "Server is not Entitled. Check these options for renewing your license." The options include:

- Buy more licenses.
- Find partner for license purchase.
- Contact HPE Support.

Procedure

1. Select **Upload AHS Log**.
2. Navigate to your log file and click **Open**.

   A window is displayed that shows parsing and log loading states. As the AHS log loads, the screen displays the estimated time of completion.

   TIP:

   This window also displays videos for different platforms. You can search and play different videos while you are waiting for the log file to load.

   To cancel the load process, click **Cancel**.

Launching Intelligent Provisioning

Intelligent Provisioning is an embedded, single-server deployment tool that simplifies server setup, providing a reliable and consistent way to deploy server configurations. The **Intelligent Provisioning** 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 Intelligent Provisioning user guide on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/intelligentprovisioning/docs**).

Procedure

1. From the **System Utilities** screen, select **Embedded Applications** > **Intelligent Provisioning**.
2. To return to the **System Utilities** menu, reboot the server.

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**
  - **Power Management Controller FW Version**
  - **User Defaults**
  - **Boot Mode**
  - **System Memory**
  - Processor types
  - **iLO Firmware Version**
  - Embedded **Network Devices**
- **Processor Information**—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** 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.
- **Export System Information to file**—Opens a screen where you can:

  1. **Select file location**—Select or specify a new file for the exported information.
  2. Select which type of system information to export.
     - Summary
     - Processor
     - Memory
     - PCI device
     - Firmware
  3. To export the information, save your selections and exit the System Utilities.

Viewing System Information

Procedure

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

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**.

Viewing System Health

Use the **System Health** option 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.

Procedure

1. From the **System Utilities** screen, select **System Health**.
2. Select **View System Health**.
3. (Optional) Download an AHS log. See **Downloading an Active Health System Log** .

Rebooting the system, selecting a language, and setting the browser mode

Rebooting the system

Exiting and resuming system boot

Use the **Exit and resume system boot** 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.

Procedure

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

   A confirmation message appears.
2. Click **OK** or press **Enter**.

Rebooting the system

Use the **Reboot the System** option to exit the system and reboot without continuing with the normal boot process.

Procedure

1. From the **System Utilities** screen, select **Reboot the System**.

   A confirmation message appears.
2. Click **Yes, Reboot**, or press **Enter**.

Selecting a language and browser mode

Selecting a system language

Procedure

1. From the **System Utilities** screen, select **Select Language**.
2. Select a language.
   - **English**
   - **Japanese**
   - **Simplified Chinese**
3. Save your setting.

Selecting a browser mode

Procedure

1. From the **System Utilities** screen, select **Setup Browser Selection.**.
2. Select a setting.

- **GUI**—Opens a GUI-based browser when you access the System Utilities using the Integrated Remote Console or a physical terminal.
- **Text**—Opens a text-based browser when you access the System Utilities using a serial console.
- **Auto**—Depending on how you access the System Utilities, opens either a text-based browser, or a GUI-based browser.

3. Save the setting.

For more information, see **Navigating the System Utilities in GUI mode**.

BIOS/Platform Configuration options

Selecting a Workload Profile

Workload Profiles and performance options

Workload Profiles are a configuration option to deploy BIOS settings based on the workload customer intends to run on the server. Workload Profiles are a configuration option to deploy BIOS settings to accommodate the intended application of the server.

Workload Profiles is one of the HPE Intelligent System Tuning (IST) features.

System provided Workload Profiles

The system provides these Workload Profiles:

General Power Efficient Compute

This profile is the default profile for most ProLiant servers and HPE Synergy compute modules.

This profile applies the most common performance settings that benefit most application workloads while also enabling power management settings that have minimal impact to overall performance. The settings that are applied heavily favor a balanced approach between general application performances versus power efficiency.

This profile is recommended for customers that do not typically tune their BIOS for their workload.

General Peak Frequency Compute

This profile is intended for workloads that generally benefit from processors or memory that must achieve the maximum frequency possible, for any individual core, at any time. Power management settings are applied when they ensure that any component frequency upside can be readily achieved. Processing speed is favored over any latencies that might occur. This profile is a general-purpose profile, so optimizations are done generically to increase processor core and memory speed.

This profile benefits workloads that typically benefit from faster compute time.

General Throughput Compute

This profile is intended to be used for workloads where the total maximum sustained workload throughput is needed. Increased throughput does not always occur when the processor runs at the highest individual core speed. Increased throughput can occur when the processor is able to perform sustained work across all available cores during maximum utilization. Power management settings are disabled when they are known to have impact on maximum achievable bandwidth.

Best throughput is achieved when the workload is also (Non-uniformed Memory Access) NUMA aware and optimized so settings that benefit NUMA awareness are applied.

Virtualization - Power Efficient

This profile is intended to be used for virtualization environments. The profile ensures that all available virtualization options are enabled. Certain virtualization technologies can have possible performance impacts to nonvirtualized environments and can be disabled in other profiles. Power management settings can have an impact on performance when running virtualization operating systems and this profile applies power management settings that are virtualization friendly.

Virtualization - Max Performance

This profile is intended to be used for virtualization environments. The profile ensures that all available virtualization options are enabled. Power management settings are disabled in favor of delivering maximum performance.

Low Latency

This profile is intended to be used by customers who desire the least amount of computational latency for their workloads. This profile follows the most common best practices that are documented in the HPE Low Latency Whitepaper. Maximum speed and throughput are often sacrificed to lower overall computational latency. Power management and other management features that might introduce computational latency are also disabled.

The profile benefits customers running Real-Time Operating Systems (RTOS) or other transactional latency sensitive workloads.

Mission Critical

This profile is intended to be used by customers who trade off performance for server reliability above the basic server defaults. The profile enables advanced memory reliability, availability, and serviceability (RAS) features that are known to have more than a measurable impact to computational performance. Enabling this profile will have an impact to maximum memory bandwidth and will increase memory latency.

Transactional Application Processing

This profile is intended to be used for business processing environments, such as online transaction processing (OLTP) applications that require a database back-end. For example, workloads typically comprised of a high number of user-based, transactional applications running on a single server with cohosted database component. The profile balances the requirement of managing both peak frequency and throughput.

High Performance Compute (HPC)

This profile is intended for customers running in a traditional HPC environment. Typically, these environments are clustered environments where each node performs at maximum utilization for extended periods of time to solve large-scale scientific and engineering workloads. The default for our Apollo series servers, power management is typically disabled in favor of sustained available bandwidth and processor compute capacity. This profile is similar to the Low Latency profile except that some latency is accepted to achieve maximum throughput.

Decision Support

This profile is intended for Enterprise Business Database (Business Intelligence) workloads that are focused on operating and/or accessing data warehouses, such as data mining or online analytical processing (OLAP).

Graphic Processing

This profile is intended for workloads that are run on server configurations which utilize Graphics Processing Units (GPUs.) GPUs typically depend on maximum bandwidth between I/O and Memory. Power management features that have impact on the links between I/O and memory are disabled. Peer to Peer traffic is also critical and therefore virtualization is also disabled.

I/O Throughput

This profile is intended to be used for configurations that depend on maximum throughput between I/O and memory. Processor utilization driven power management features that have performance impact to the links between I/O and memory are disabled.

Custom

This option on the Workload Profiles menu disables Workload Profiles. Use this option if you want to set specific BIOS options for your deployment manually. When you select Custom, all the settings for the previously selected profile are carried forward. You can edit all or some of the options.

Custom is not a profile and settings that you specify are not saved as a template.

Default profiles for servers

Workload Profile options support a variety of power and performance requirements. For most HPE ProLiant Gen10 servers and HPE Synergy compute modules, Workload Profile is set to **General Power Efficient Compute** by default. This Workload Profile provides common performance and power settings suitable for most application workloads. For ProLiant XL servers in an HPE Apollo system, the Workload Profile is set to **HighPerformance Compute** by default.

Selecting a Workload Profile other than the Custom profile affects other setting options. For example, selecting the **General Peak Frequency Compute** profile automatically sets **Power Regulator** mode to **Static High Performance**. This setting cannot be changed and is grayed out.

Workload Profiles dependencies

Dependencies

There are multiple options that are available for BIOS configuration. Not all profiles set the same options to specific settings. Each profile is designed to obtain specific performance results and sets different options to meet those results. The options that a profile sets are called dependencies. All other options are unaffected by the Workload Profile and are referred to as nondependent settings.

Dependencies and switching profiles

When you change a profile, only the dependent settings for that profile are changed. Nondependent settings remain what they were before you changed your profile.

For example:

1. Select the General Power Efficient Compute profile, which has the Energy Performance Bias set to Balanced Performance.
2. Select the General Peak Frequency Compute profile, which has no dependency on Energy Performance Bias. The Energy Performance option is set to Balanced Performance because that setting is carried forward from the General Power Efficient Compute profile.
3. Select the General Throughput Compute profile, which has the Energy Performance Bias set to Maximum Performance.
4. Select the General Peak Frequency Compute profile which has no dependency on Energy Performance Bias. Energy Performance Bias is set to Maximum Performance because that setting is carried forward from the General Throughput Compute profile.

There is no way to revert to a previous profile and dependencies. Once you change to a new profile, the new dependencies are applied. The only way to revert to older profiles, is to exit without saving your changes. Exiting without saving reverts to where you were when you entered RBSU. Once you save a profile, you cannot revert from that profile to any intermediate dependencies.

Dependencies and options matrix

The following tables show the Workload Profiles and their dependencies. The Workload Profiles are listed in the order that they are listed on the user interface. In the table, "X" means that the option setting has no requirement for the profile and can be edited. Dependencies cannot be edited.

NOTE:

Not all the options listed are adjustable on all servers. However, even if you do not have the option of adjusting some of these settings, they default to the values shown here.

Table 1: Workload Profiles General Power Efficient Compute — Low Latency

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency
SR-IOV	X	X	X	Enabled	Enabled	Disabled
VT-D	X	X	X	Enabled	Enabled	Disabled
VT-x	X	X	X	Enabled	Enabled	Disabled
Power Regulator	Dynamic Power Savings	Static High Performance	Static High Performance	OS Control	Static High Performance	Static High Performance
Minimum Processor Idle Power Core C-state	C6	X	X	C6	No C-states	No C-states
Minimum Processor Idle Power Package C-state	Package C6 Retention	Package C6 Retention	Package C6 Retention	Package C6 Retention	No C-states	No C-states
Energy Performance Bias	Balanced Performance	X	Max Performance	Balanced Performance	Max Performance	Max Performance
Collaborative Power Control	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	Enabled	Enabled	Enabled	X	Enabled	Disabled
Intel NIC DMA Channels (IOAT)	Enabled	X	X	X	X	X
HW Prefetcher	Enabled	Enabled	Enabled	X	X	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	X	X	Enabled
DCU Stream Prefetcher	Enabled	Enabled	Enabled	X	X	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	X	X	Enabled
NUMA Group Size Optimization	Flat	Clustered	Clustered	Clustered	Clustered	Clustered

Table Continued

Memory Patrol Scrubbing	X	X	X	X	X	Disabled
Memory Refresh Rate	X	1X	1X	X	X	1X
UPI Link Power Management	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Sub-NUMA Clustering	Disabled	X	Enabled	Disable	Enabled	X
Energy-Efficient Turbo	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Uncore Frequency Shifting	Auto	Max	X	Auto	Max	Max
x2APIC	X	X	X	X	X	Disabled
Channel Interleaving	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Memory Bus Frequency	X	X	X	X	X	X
A3DC	X	X	X	X	X	Disabled

Table 2: Workload Profiles Mission Critical — I/O Throughput

	Mission Critical	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput
SR-IOV	X	X	Disabled	X	Disabled	X
VT-D	X	X	Disabled	X	Disabled	X
VT-x	X	X	Disabled	X	Disabled	X
Power Regulator	X	Static High Performance	Static High Performance	X	X	X
Minimum Processor Idle Power Core C-state	X	No C-states	No C-states	X	X	X
Minimum Processor Idle Power Package C-state	X	No C-states	No C-states	X	X	X
Energy Performance Bias	X	Max Performance	Max Performance	X	Max Performance	Max Performance

Table Continued

Collaborative Power Control	X	X	Disabled	X	X	X
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	X	Enabled	Enabled	X	X	X
Intel NIC DMA Channels (IOAT)	X	Enabled	Enabled	X	X	Enabled
HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
DCU Stream Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
NUMA Group Size Optimization	X	Clustered	Clustered	Clustered	Clustered	Clustered
Memory Refresh Rate	2X	X	1X	X	X	X
UPI Link Power Management	X	Disabled	Disabled	X	X	X
Sub-NUMA Clustering	X	X	X		X	X
Energy-Efficient Turbo	X	X	Disabled	X	X	X
Uncore Frequency Shifting	X	X	Max	X	Max	Max
x2APIC	X	X	Disabled	X	Disabled	X
Channel Interleaving	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Memory Bus Frequency	X	X	X	X	X	X
A3DC	Enabled	X	Disabled	X	X	X

Applying a Workload Profile

You apply a Workload Profile to have the system manage your workload according to predefined settings provided with the system. Dependent options cannot be changed and are grayed out. You can change any nondependent options in a profile.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Workload Profile**.
2. Select a **Workload Profile**.
3. Optional: Change any nondependent options that you want to change.
4. Save and reboot to apply your Workload Profile.

Changing dependent options after applying a profile

There may be one or more dependent options that you want to change in your Workload Profile. Dependent options cannot be changed for a predefined profile. You can change the dependent options in Custom mode. When you are in Custom mode, your deployment is no longer in profile mode and you can manually adjust option settings. When you enter Custom mode, all the settings from the previously applied profile are shown.

The easiest way to change dependent settings is to modify an applied profile. First apply a Workload Profile that has most of the settings that you want to use then change to Custom mode. Then change only the settings you want to have new values.

Prerequisites

Apply a Workload Profile before you do this task.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Workload Profile**.
2. Select the Custom profile option.

   All of the settings from the previously applied Workload Profile are shown. All options are editable.
3. Change the options that you want to have new values.
4. Save and reboot to apply the changes.

Configuring System Options

Configuring Boot Time Optimizations

Setting Dynamic Power Capping Functionality

Use the **Setting Dynamic Power Capping Functionality** option to configure when the system ROM executes power calibration during the boot process.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Boot Time Optimizations** > **Dynamic Power Capping Functionality**.
2. Select a setting.
   - **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**—Power calibration runs on every system boot.
   - **Disabled**—Power calibration does not run, and Dynamic Power Capping is not supported.
3. Save your setting.

Enabling or disabling Extended Memory Test

Use the **Extended Memory Test** option to configure whether the system validates memory during the memory initialization process. When enabled, and uncorrectable memory errors are detected, the memory is mapped out, and the failed DIMMs are logged to the IML.

NOTE:

Enabling this option might significantly increase boot time.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Boot Time Optimizations** > **Extended Memory Test**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling Memory Fast Training

Use the **Memory Fast Training** option to configure memory training on server reboots. When enabled, the platform uses the previously saved memory training parameters determined from the last cold boot of the server, which improves server boot time. When installed on your server, and this setting is enabled, NVDIMM-N Memory contents are left undisturbed during warm resets. If Memory Fast Training is disabled, each warm reset is upgraded to a cold reset and results in an NVDIMM-N backup and restore. Hewlett Packard Enterprise recommends that you leave Memory Fast Training enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Boot Time Optimizations** > **Memory Fast Training**.
2. Select a setting.

- **Enabled**—Enables the server to use previously saved memory training parameters.
- **Disabled**—The platform performs a full memory training on every server reboot.

3. Save your setting.

Setting the UEFI POST Discovery Mode

Use the **UEFI POST Discovery Mode** option to control how the system loads UEFI device drivers.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Boot Time Optimizations** > **UEFI POST Discovery Mode**.
2. Select a setting.
   - **Auto**—The system only loads the UEFI device drivers that are required for booting the devices in the UEFI Boot Order list.
   - **Force Full Discovery**—The system loads the UEFI drivers for all devices, making all boot targets available.

     NOTE:

     This setting might significantly increase boot time.
3. Save your setting.

Enabling or disabling Memory Clear on Warm Reset

Use the **Memory Clear on Warm Reset** option to configure when memory is cleared on warm resets. Disabling this option can save boot time by skipping the clearing of memory on warm resets.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Boot Time Optimizations** > **Memory Clear on Warm Reset**.
2. Select a setting.
   - **Enabled**—Memory is cleared on all reboots.
   - **Disabled**—Memory is only cleared on a warm reset when requested by the operating system.
3. Save your setting.

Configuring Serial Port Options

Assigning an Embedded Serial Port

Use the **Embedded Serial Port** option to assign a logical COM port address and associated default resources to a selected physical serial port.

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Serial Port Options** > **Embedded Serial Port**.
2. Select a setting.

- **COM 1: IRQ4: I/0: 3F8h-3FFh**
- **COM 2: IRQ3: I/0: 2F8h-2FFh**
- **Disabled**

3. Save your setting.

Assigning a Virtual Serial Port

Use the **Virtual Serial Port** 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.

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Serial Port Options** > **Virtual Serial Port**.
2. Select a setting.
   - **COM 1**
   - **COM 2**
   - **Disabled**
3. Save your setting.

Configuring USB Options

Setting USB Control

Use the **USB Options** option to configure how USB ports and embedded devices operate at startup.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** > **USB Control**.
2. Select a setting.
   - **All USB Ports Enabled**—Enables all USB ports and embedded devices.
   - **All USB Ports Disabled**—Disables all USB ports and embedded devices.
   - **External USB Ports Disabled**—Disables external USB ports.
   - **Internal USB Ports Disabled**—Disables internal USB ports.
3. Save your setting.

Enabling or disabling USB Boot Support

Use the **USB Boot Support** option to control whether the system can boot from connected USB devices, such as virtual media devices, and the embedded SD card slot, if supported.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** > **USB Boot Support**.
2. Select a setting.

- **Enabled** —The system can boot from USB devices connected to the server.
- **Disabled**—The system cannot boot from USB devices connected to the server.

3. Save your setting.

Selecting the Removable Flash Media Boot Sequence

Use the **Removable Flash Media Boot Sequence** option to select which USB or SD card devices to search first when enumerating boot devices.

Prerequisites

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** > **Removable Flash Media Boot Sequence**.
2. Select a setting.
   - **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**—Boots using external USB drive keys.
3. Save your setting.

Enabling or disabling 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 is 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** > **Virtual Install Disk**.
2. Select a setting.
   - **Enabled**—Virtual Install Disk appears as a drive in the operating system.
   - **Disabled**—Virtual Install Disk does not appear as a drive in the operating system.
3. Save you setting.

Enabling or disabling the Internal SD Card Slot

Use the **SD Card Slot** option to control whether the server can access the SD (Secure Digital) nonvolatile flash memory card that is embedded on the system board.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** > **Internal SD Card Slot**.
2. Select a setting.
   - **Enabled**—The server can access the internal SD card slot.
   - **Disabled**—The server cannot access the internal SD card slot.
3. Save your setting.

Configuring Server Availability

Enabling or disabling ASR

Prerequisite

The System Management driver is loaded.

Use the **ASR Status** option to enable or disable Automatic Server Recovery, which automatically reboots the server if the server locks up.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **ASR Status**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Setting the ASR timeout

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **ASR Timeout**.
2. Select a wait time.
   - **5 Minutes**
   - **10 Minutes**
   - **15 Minutes**
   - **20 Minutes**
   - **30 Minutes**
3. Save your setting.

Enabling or disabling Wake-On LAN

Use the **Wake-On LAN** option to enable or disable the ability of the server to power on remotely using a WOL-capable NIC.

Prerequisite

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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **Wake-On LAN**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Setting the POST F1 prompt delay

Use the **POST F1 Prompt** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **POST F1 Prompt**.
2. Select a setting.
   - **Delayed 20 seconds**—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. Save your setting.

Enabling or disabling momentary power button functionality

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **Power Button Mode**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Setting the automatic power-on state

Use the **Automatic Power-On** option to configure how the server automatically powers on when AC power is applied. By default, the system returns to its previous power state when AC power is restored after an AC power loss.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **Automatic Power-On**.
2. Select a setting.
   - **Always Power On**—The system automatically returns to a power on state, even if it was in the “off” state when power was lost.
   - **Always Power Off**—The system automatically returns to a power off state.
   - **Restore Last Power State**—The system automatically returns to its previous power off state.
3. Save your setting.

Setting the power-on delay

Use the **Power-On Delay** option to set whether to delay the server from turning on for a specified time. This option enables staggering when the server powers 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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** > **Power-On Delay**.
2. Select a setting.
   - **No Delay**
   - **Random Delay**
   - **15 Second Delay**
   - **30 Second Delay**
   - **45 Second Delay**
   - **60 Second Delay**
3. Save your setting.

Viewing and entering server asset information

Entering server information

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information** > **Server Information**.
2. Select and complete entries.
   - **Server Name**—Enter a server name.
   - **Server Asset Tag**—Enter a server asset number.

- **Asset Tag Protection**—Select a setting:
  - **Unlocked**
  - **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**—Displays the logo during system boot.
  - **Disabled**—Does not display the logo during system boot. This setting does not affect system boot times.

3. Save your settings.

Entering administrator information

Use the **Administrator Information** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information** > **Administrator Information**.
2. Select and complete entries.
   - **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. Save your settings.

Entering service contact information

Use the **Service Contact Information** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information** > **Service Contact Information**.
2. Select and complete entries.
   - **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. Save your settings.

Entering a custom POST message

Use the **Custom POST Message** option to display a custom message on the server POST screen.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information** > **Custom POST Message**.
2. Enter a message of up to 60 characters.
3. Save your setting.

Configuring Processor Options

Enabling or disabling Intel Hyperthreading

Use the **Intel (R) Hyperthreading Options** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Processor Options** > **Intel (R) Hyperthreading Options**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Setting the number of enabled processor cores

Use the **Enabled Cores per Processor** option to specify the number of cores to enable per processor socket using Intel's Core Multi-Processing (CMP) Technology. 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Processor Options** > **Enabled Cores per Processor**.
2. Enter the number of cores to enable.

   If you enter **0**, or a value that is not supported by the processor, all cores are enabled.
3. Save your setting.

Enabling or disabling Processor x2APIC Support

When enabled, **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. Some hypervisors and operating systems cannot use X2APIC unless **Processor x2APIC Support** is set to **Force Enabled** prior to booting.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Processor Options** > **Processor x2APIC Support**.
2. Select a setting.

- **Enabled**—Generates the ACPI x2APIC control structures, and adds the option of enabling x2APIC support to the operating system when it loads.
- **Force Enabled**—For certain processors, enables x2APIC support to the operating system when it loads.
- **Disabled**—Disables x2APIC support.

3. Save your setting.

Configuring Memory Options

Configuring Advanced Memory Protection

Use the **Advanced Memory Protection** option to configure additional memory protection with Error Checking and Correcting (ECC). **Advanced ECC Support** provides the largest memory capacity to the operating system, and is the required setting when NVDIMMs are installed on your server. Other options are not supported when NVDIMMs are installed. Selecting one of the unsupported options when NVDIMMs are installed generates messages that are displayed in the IML, and the NVDIMMs are disabled until the configuration is set to Advanced ECC Support. When **Advanced Memory Protection** is set to **Advanced ECC Support**, the Advanced Memory Protection option is hidden (greyed out) in the menu.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Advanced Memory Protection**.
2. Select a setting.
   - **HPE Fast Fault Tolerant (ADDDC)**—Enables the system to correct memory errors and continue to operate in cases of multiple DRAM device failures on a DIMM. Provides protection against uncorrectable memory errors beyond what is available with Advanced ECC.
   - **Advanced ECC Support**—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. Save your settings.

Configuring the Memory Refresh Rate

The **Memory Refresh Rate** option controls the refresh rate of the memory controller and might affect the performance and resiliency of the server memory. It is recommended that you leave this setting in the default state unless indicated in other documentation for this server.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Memory Refresh Rate**.
2. Select a setting.
   - **1x Refresh**
   - **2x Refresh**
3. Save your setting.

Enabling or disabling channel interleaving

Use the **Channel Interleaving** 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.

When you are enabling NVDIMM-N Memory Interleaving, you must also enable **Channel interleaving**.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Channel Interleaving**.
2. Select a setting.
   - **Enabled**—Enables the highest level of interleaving for which the system memory is configured.
   - **Disabled**—Does not enable memory interleaving.
3. Save your setting.

Setting the maximum memory bus frequency

Use the **Maximum Memory Bus Frequency** option to configure the system to run memory at a lower maximum speed than that supported by the installed processor and DIMM configuration.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Maximum Memory Bus Frequency**.
2. Select a setting.
   - **Auto**—Memory runs at the maximum speed supported by the system configuration.
   - **1333 MHz**
   - **1600 MHz**
   - **1867 MHz**
   - **2133 MHz**
3. Save your setting.

Enabling or disabling Memory Patrol Scrubbing

When enabled, **Memory Patrol Scrubbing** corrects memory soft errors so that, over the length of the system runtime, the risk of producing multi-bit and uncorrectable errors is reduced..

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Memory Patrol Scrubbing**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling node interleaving

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Node Interleaving**.
2. Select a setting.
   - **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**—Disables node interleaving, providing optimum performance in most environments.
3. Save your setting.

Configuring the memory mirroring mode

Use the **Memory Mirroring** option to configure how much of the total available system memory is reserved for mirroring.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Memory Mirroring Mode**.
2. Select a setting.
   - **Full Mirror**—Reserves 50% of the total available memory for mirroring.
   - **Partial Mirror (20% above 4GB)**—Reserves 20% of the total available memory above 4 GB for mirroring.
   - **Partial Mirror (10% above 4GB)**—Reserves 10% of the total available memory above 4 GB for mirroring.
   - **Partial Mirror (Memory below 4GB)**—Depending on the memory configuration, reserves 2 GB or 3 GB of lower memory below 4 GB for mirroring.
   - **Partial Mirror (OS Configured)**—Enables the operating system to configure partial memory mirroring.
3. Save your setting.

Configuring memory remapping

Use the **Memory Remap** option to remap system memory that might be disabled due to a failure event, such as an uncorrectable memory error.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Memory Remap**.
2. Select a setting.
   - **Remap All Memory**—Makes all memory in the system available again on the next boot.
   - **No Action**—Leaves any affected memory unavailable to the system.
3. Save your setting.

Configuring Virtualization Options

Enabling or disabling Virtualization Technology

Use the **Intel(R) Virtualization Technology (Intel VT)** to control whether a Virtual Machine Manager (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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Virtualization Options** > **Intel(R) Virtualization Technology (Intel VT)**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling Intel VT-d

Use the **Intel (R) VT-d** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Virtualization Options** > **Intel (R) VT-d**.
2. Select a setting.
   - **Enabled**—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. Save your setting.

Enabling or disabling 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Virtualization Options** > **SR-IOV**.
2. Select a setting.

- **Enabled**—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. Save your setting.

Configuring Boot Options

Selecting the boot mode

This server provides 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 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

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.

Prerequisite

When booting to **UEFI Mode**, leave **UEFI Optimized Boot** enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **Boot Mode**.
2. Select a setting.
   - **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. Save your setting.
4. Reboot the server.

Enabling or disabling UEFI Optimized Boot

Use **UEFI Optimized Boot** to control whether the system BIOS boots using native UEFI graphic drivers.

Prerequisites:

- When **UEFI Optimized Boot** is enabled, Boot Mode must be set to UEFI Mode.
- **UEFI Optimized Boot** must be enabled to:
  - Enable and use Secure Boot.
  - Operate VMware ESXi.

Prerequisites

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **UEFI Optimized Boot**.
2. Select an option.
   - **Enabled**—When set to UEFI Mode, configures the system BIOS to boot using native UEFI graphic drivers.
   - **Disabled**—Configures the system BIOS to boot using INT10 legacy video expansion ROM. This setting is required if you are using Microsoft Windows 7 as your operating system.

3. Save your setting.
4. Reboot the server.

Setting the boot order policy

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

Procedure

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

Changing the UEFI Boot Order list

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **UEFI Boot Settings** > **UEFI Boot Settings** > **UEFI Boot Order**.
2. To navigate within the boot order list, use your pointing device or the arrow keys.
3. Select an entry and change its order in the list:
   - To move an entry higher in the boot list, press the **+** key, or drag and drop the entry.
   - To move an entry lower in the boot list, press the **-** key, or drag and drop the entry.
4. Save your changes.

Controlling the UEFI boot order

Use the UEFI Boot Order Control option to enable or disable individual UEFI boot options. Enabled items are selected (checked). Disabled items remain in their location in the UEFI Boot Order list , but are not attempted during the boot process.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **UEFI Boot Settings** > **UEFI Boot Settings** > **UEFI Boot Order Control**.
2. Do the following:
   - To enable an option, select the corresponding check box.
   - To disable an option, select the corresponding check box.
3. Save your changes.

Adding a boot option to the UEFI Boot Order list

Use **Add Boot 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.

Procedure

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** > **UEFI Boot Settings** > **Add Boot Option**.
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**.

Deleting boot options from the UEFI Boot Order list

NOTE:

If a deleted option points to a standard boot location, such as a network PXE boot or a removable media device, the system BIOS adds the option on the next reboot.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **UEFI Boot Settings** > **Delete Boot Option**.
2. Select one or more options from the list.
3. Select **Commit Changes and Exit**.

Changing the Legacy BIOS Boot Order list

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **Legacy BIOS Boot Order**.
2. To navigate within the boot order list, use your pointing device or the arrow keys.
3. Select an entry and change its order in the list:
   - To move an entry higher in the boot list, press the **+** key, or drag and drop the entry.
   - To move an entry lower in the boot list, press the **-** key, or drag and drop the entry.
4. Save your changes.
5. Reboot the server.

Configuring Network Options

Network Boot Options

- Pre-Boot Network Environment Policy
- IPv6 DHCP Unique Identifier
- Network Boot Retry Support
- Network Interface Cards (NICs)
- PCIe Slot Network Boot
- HTTP Support
- UEFI iSCSI Policy

Setting the Pre-Boot Network Environment

Use the Pre-Boot Network Environment option to set a preference for how your network boot targets appear in the **UEFI Boot Order** list. This option also controls the Pre-Boot network operations from Embedded UEFI Shell.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **Pre-boot Network Environment**.
2. Select a setting.
   - **Auto**—All network operations initiated in the pre-boot environment occur over IPv4 or IPv6. The order of the existing network boot targets in the **UEFI Boot Order** list is not modified. New network boot targets are added to the end of the list using the default policy of the system BIOS.
   - **IPv4**—All network operations initiated in the pre-boot environment only occur over 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**—All network operations initiated in the pre-boot environment only occur over 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.
3. Save your changes.

Setting the IPv6 DHCP Unique Identifier method

Use the IPv6 DHCP Unique Identifier option to control how the IPv6 DHCP Unique Identifier (DUID is set.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **IPv6 DHCP Unique Identifier**.
2. Select a setting.
   - **Auto**—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. Save your changes.

Enabling or disabling Network Boot Retry Support

Use the Network Boot Retry Support option to enable or disable the network boot retry function. When enabled, the system BIOS attempts to boot the network device up to the number of times set in the Network

Boot Retry Count option before attempting to boot the next network device. This setting only takes effect when attempting to boot a network device from the **F12** function key and one-time boot options.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **Network Boot Retry Support**.
2. Select a setting.
   - **Enabled**—Enables network boot retry.
   - **Disabled**—Disables network boot retry.
3. Save your changes.

Enabling or disabling network boot for a NIC

Use the Network Interface Cards (NICs) option to enable or disable network boot 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options**.
2. Select a NIC.
3. Select a setting.
   - **Network Boot**—Enables network boot.
   - **Disabled**—Disables network boot.
4. Save your changes.
5. If you selected **Network Boot**, reboot the server so that the NIC boot option appears in the boot order list.

Enabling or disabling PCIe Slot Network Boot

Use the PCIe Slot Network Boot option to enable or disable UEFI network boot for NIC cards in PCIe slots.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **PCIe Slot Network Boot**.
2. Select a PCIe slot entry.
3. Select a setting.
   - **Enabled**—Enables UEFI network boot for NIC cards in PCIe slots.
   - **Disabled**—Disables UEFI network boot for NIC cards in PCIe slots.
4. Save your changes.

Setting HTTP support

Prerequisites

Use this option to control the UEFI HTTP(s) boot support when in UEFI Mode and using the **Embedded UEFI Shell** > **Discover Shell Auto-Start Script using DHCP** setting.

To enable HTTPS boot, either by selecting **Auto** or **HTTPS only**, you must enroll the respective TLS certificate of the HTTPS server under **Server Security** > **TLS (HTTPS) Options**

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **HTTP Support**.
2. Select a setting.
   - **Auto**—Automatically adds HTTP(S) boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTP or HTTPS URLs provided by the DHCP server. Any other URLs provided by the DHCP server are ignored.
   - **HTTP only**—Automatically adds HTTP boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTP URLs provided by the DHCP server, and to ignore any HTTPS or other URLs that are provided.
   - **HTTPs only**—Automatically adds HTTPS boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTPS URLs provided by the DHCP server, and to ignore any HTTP or other URLs that are provided.
3. Save your changes.

Setting the iSCSI policy

Use the iSCSI Policy option to control which initiator is used for iSCSI boot on configured NIC ports.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **iSCSI Policy**.
2. Select a setting.
   - **Software Initiator**—Enables the UEFI iSCSI software initiator.
   - **Adapter Initiator**—Disables the UEFI iSCSI software initiator and only uses the adapter specific iSCSI initiator.

     NOTE: To enable iSCSI boot from the adapter initiator, you must enable iSCSI in the adapter firmware and configure it.
3. Save your changes.

Configuring Pre-Boot Network Settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Pre-Boot Network Settings**.
2. Select any of the **Pre-boot Network Settings** options.
3. Select additional settings or enter additional values for that option.
4. Save your changes.

Pre-Boot Network Settings

Use this option to configure a preboot network interface and related settings.

IMPORTANT:

If you plan to run `webclient` or `ftp` over the same interface, you do not need to use the Embedded UEFI Shell `ifconfig` command on a network interface. The **Pre-Boot Network Settings** configured in the System Utilities automatically selects these interface.

If the interface used by `ftp` and `webclient` are configured by `ifconfig`, that setting is erased. 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 preboot network connections.
  - **Auto** (default)—The system uses the first available port with a network connection.
  - **Select Specific Port** — The system uses the selected NIC port.
- **DCHPv4** — Enables or disables obtaining the preboot network IPv4 configuration from a DHCP server for Network operations from the Embedded UEFI Shell.
  - **Enabled** — Enables DHCPv4 network address configuration. Individual settings are not available.
  - **Disabled** — Disables DHCPv4 address configuration, requiring you to configure the following static IP address settings manually.
    - **IPv4 Address**
    - **IPv4 Subnet Mask**
    - **IPv4 Gateway**
    - **IPv4 Primary DNS**
    - **IPv4 Secondary DNS**
- **Preboot Network Proxy**—Specifies a preboot network proxy. When set, network operations for the Pre-Boot Network Interface are attempted through the configured proxy. The proxy must be in an HTTP URL format, and can be specified as `http://IPv4_address:port`, `http://[IPv6_address]:port` or `http://FQDN:port`.
- **IPv6 Config Policy**
  - **Automatic**—Enables preboot network IPv6 configuration to be automatically obtained for Network operations from the Embedded UEFI Shell. Individual settings are not available.
  - **Manual**—Enables you to configure static IP address settings individually.
- **Boot from URL 1, 2, 3 or 4**—Specifies a network URL to a bootable ISO or EFI file. Enter a URL in either HTTP or HTTPS format, using either an IPv4 or IPv6 server address or host name. For example, the URLs can be in any of the following formats: `http://192.168.0.1/file/image.iso`, `http://example.com/file/image.efi`, `https://example.com/file/image.efi`, `http://[1234::1000]/image.iso`. 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:

  Boot from URL does not depend on the "DHCPv4" and "IPv6 Config Policy" settings.

  Booting from an ISO file can involve only booting a preliminary OS environment image, such as WinPE or a mini Linux, or a complete OS install image if the OS supports the HTTP Boot feature (Old OS versions may not support booting from an ISO file or OS install image). Please check your OS documentation for the HTTP Boot feature support.

Prerequisites for Boot from URL

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

- Leave the boot mode set to **UEFI Mode**.
- A DHCP server must be available for the **Boot from URL** to work.

iSCSI Boot Configuration

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**.

Adding an iSCSI initiator name

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

Procedure

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

   This setting is saved automatically.

Adding an iSCSI boot attempt

Procedure

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

   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 connection.
4. Complete the configuration settings.
   - **iSCSI Attempt Name**—Enter a name.
   - **iSCSI Boot Control**—Select **Enabled**. (The default setting is **Disabled**).
   - **IP Address Type**—Select an address type.
   - **Connection Retry Count**—Enter a value from 0 to 16. Default is 3 retries.
   - **Connection Timeout**—Enter a value in ms from 100 to 20000. Default is 20000 (20 seconds).
   - **Initiator DHCP**—This is the default setting. If you must configure static IP addresses for the Initiator, clear this option. The target name, IP address, port, and boot LUN must also be configured manually (disable Target DHCP Config) if you configure static addresses for the Initiator.
   - **Target DHCP Config**—This is the default setting. If you must configure the target settings manually, clear this check box) and enter a target name, IP address, port, and boot LUN.
   - Optional: **Authentication Type**—Default is NONE. If required, select **CHAP** and complete the CHAP entries.
5. Select **Save Changes**.

Deleting iSCSI boot attempts

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **iSCSI Boot Configuration** > **Delete iSCSI Boot Attempts**.
2. Select one or more iSCSI boot attempt entries.
3. Select **Commit Changes and Exit**.

Viewing and modifying iSCSI boot attempt details

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **iSCSI Boot Configuration** > **iSCSI Attempts**.
2. Select an entry from the list.
3. View or modify the details about the boot attempt.

Configuring VLAN Configuration

Use the VLAN Configuration option to configure global VLAN settings for all enabled network interfaces. The configuration includes interfaces used in PXE boot, iSCSI boot, and HTTP/HTTPS boot, and for all preboot network access from the Embedded UEFI Shell.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **VLAN Configuration**.
2. Complete the following.
   a. **VLAN Control**—Select **Enabled** to enable VLAN tagging on all enabled network interfaces. This setting is disabled by default.
   b. **VLAN ID**—When **VLAN Control** is enabled, enter a VLAN ID between 1 and 4094.
   c. **VLAN Priority**—When **VLAN Control** is enabled, enter a priority value of 0 to 7 for VLAN tagged frames.
3. Save your changes.

Configuring Storage Options

Enabling embedded chipset SATA controller support

Use the **Embedded SATA Configuration** option to enable embedded chipset SATA (Serial Advanced Technology Attachment) controller support. You can select AHCI or HPE Smart Array S100i SR Gen10 SW 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.

Prerequisites

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **SATA Controller Options** > **Embedded SATA Configuration**.
2. Ensure that you are using the correct ACHI or RAID system drivers for your SATA option.
3. Select a setting.
   - **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. Save your setting.

Enabling SATA Secure Erase

Use the **SATA Secure Erase** 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.

Prerequisites

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

Procedure

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

Setting the embedded storage boot policy

Use the **Embedded Storage Boot Policy** 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.

Prerequisites

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **Embedded Storage Boot Policy**.
2. Select a storage controller.
3. Select a setting.
   - **Boot All Targets** —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. Save your setting.

Setting the PCIe storage boot policy

Prerequisite

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

Use the **PCIe Storage Boot Policy** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **PCIe Storage Boot Policy**.
2. Select a storage controller.
3. Select a boot target.
4. Save your setting.

Changing the default Fibre Channel/FCoE scanning policy

Prerequisite

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

Use the **Fibre Channel/FCoE Scan Policy** 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. For Fibre Channel controllers in PCIe slots, this setting is overridden by the PCIe Storage Boot Policy setting.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **Fibre Channel/FCoE Scan Policy**.
2. Select a setting.
   - **Scan All Targets**—Each installed FC/FCoE adapter scans all available targets.
   - **Scan Configured Targets Only**—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. Save your setting.

Enabling or disabling Embedded NVM Express Option ROM

Use the **Embedded NVM Express Option ROM** option to control how the NVM Express Option ROM is loaded.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **NVM Express Options** > **Embedded NVM Express Option ROM**.
2. Select a setting.
   - **Enabled**—The system loads the NVM Express Option ROM provided by the system BIOS.
   - **Disabled**—The system loads the NVM Express Option ROM provided by the adapter.
3. Save your setting.

Configuring Power and Performance Options

Setting the Power Regulator mode

Use **Power Regulator** settings to help increase server efficiency and manage power consumption.

NOTE:

Certain processors only support one power state and operate at their initialized frequency, regardless of the selected power regulator mode.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Power Regulator**.
2. Select a setting.
   - **Dynamic Power Savings Mode**—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. Save your setting.

Setting the minimum processor idle power core C-State

Use the **Minimum Processor Idle Power Core C-State** 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.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Minimum Processor Idle Power Core C-State**.
2. Select a setting.
   - **C6 State** (default—lowest)
   - **C3 State**
   - **C1E State**
   - **No C-states**
3. Save your setting.

Setting the Minimum Processor Idle Power Package C-State

Use the **Minimum Processor Idle Power Package C-State** option to configure the lowest processor idle power state (C-State). The processor automatically transitions into package C-States based on the 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.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Minimum Processor Idle Power Package C-State**.
2. Select a setting.
   - **Package C6 (retention) State** (default—lowest)
   - **Package C6 (non-retention) State**
   - **No Package State**
3. Save your setting.

Enabling or disabling Intel Turbo Boost Technology

Intel Turbo Boost 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Intel(R) Turbo Boost Technology**.
2. Select a setting.
   - **Enabled**—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. Save your setting.

Setting the Energy/Performance Bias

Use the **Energy/Performance Bias** option to configure several processor subsystems to optimize the processor’s performance and power usage.

NOTE:

Options vary by installed processors.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Energy/Performance Bias**.
2. Select a setting.

- **Maximum Performance**—Provides the highest performance and lowest latency. Use this setting for environments that are not sensitive to power consumption.
- **Balanced Performance**—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. Save your setting.

Enabling or disabling collaborative power control

For operating systems that support the Processor Clocking Control (PCC) interface, enabling **Collaborative Power Control** 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.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Collaborative Power Control**.
2. Select a setting.
   - **Enabled**—The operating system requests processor frequency changes.
   - **Disabled**—The operating system does not request processor frequency changes.
3. Save your setting.

Setting Intel DMI Link Frequency

Use the **Intel DMI Link Frequency** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Intel DMI Link Frequency**.
2. Select a setting.
   - **Gen 1 Speed**
   - **Gen 2 Speed**
3. Save your setting.

Setting NUMA Group Size Optimization

Use the **NUMA Group Size Optimization** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **NUMA Group Size Optimization**.
2. Select a setting.
   - **Clustered**—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. Save your setting.

Enabling or disabling Intel Performance Monitoring Support

Intel processors include performance counters that software can use to measure DRAM performance (including NVDIMM-N performance). This option is a monitoring tool, and does not impact performance. For example, the Intel Performance Counter Monitor (PCM) tools can report per-channel bandwidth.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Intel Performance Monitoring Support**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Configuring Uncore Frequency Scaling

Use the **Uncore Frequency Scaling** option to control the frequency scaling of the processor's internal busses (the uncore.)

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Uncore Frequency Scaling**.
2. Select a setting.
   - **Auto**—Enables the processor to dynamically change frequencies based on workload.
   - **Maximum or minimum frequency**—Enables tuning for latency or power consumption.
3. Save your setting.

Enabling or disabling Sub-NUMA Clustering

Sub-NUMA Clustering divides the cores, cache, and memory of the processor into multiple NUMA domains. Enabling this option can increase performance for workloads that are NUMA aware and optimized.

NOTE:

Up to 1 GB of system memory might become unavailable when Sub-NUMA Clustering is enabled.

Prerequisite

To enable this option, enable **XPT Prefetcher**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Sub-NUMA Clustering**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling the Energy Efficient Turbo option

Use the **Energy Efficient Turbo** option to control whether the processor uses an energy-efficiency based policy.

Prerequisite

Intel(R) Turbo Boost Technology is enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Energy Efficient Turbo**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Setting a Local/Remote Threshold

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Local/Remote Threshold**.
2. Select a setting.
   - **Disabled**
   - **Low**
   - **Medium**
   - **High**
3. Save your setting.

Disabling Processor Prefetcher Options

By default, **Processor Prefetcher Options** are enabled to provide optimal performance for most environments. In some cases, disabling these options can improve performance.

IMPORTANT:

To verify that you can improve performance in your environment, perform application bench marking before you disable a processor prefetcher option.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Processor Prefetcher Options**.
2. Select a setting.

- **HW Prefetcher**
- **Adjacent Sector Prefetcher**
- **DCU Stream Prefetcher**
- **DCU IP Prefetcher**
- **XPT Prefetcher**

  NOTE:

  This setting must be enabled when **Sub-NUMA Clustering** is enabled.

3. Select **Disabled**.
4. Save your changes.

Enabling or disabling I/O Options

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **I/O Options**.
2. Select an option.
   - **ACPI SLIT**—Enables or disables the Advanced Configuration and Power Interface System Locality Information Table (ACPI SLIT). ACPI SLIT 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.
   - **Intel NIC DMA Channels (IOAT)**—Enables or disables DMA acceleration on Intel NICs. If your server does not have Intel NICs, leave this setting disabled.
   - **Memory Proximity Reporting for I/O**—Enables or disables 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.
3. Select **Enabled** or **Disabled**.
4. Save your changes.

Configuring Advanced Performance Tuning Options

Use Advanced Performance Tuning to control frequency changes that cause jitters and affect latency. You can manage Jitter Control manually or automatically. You can also specify a frequency to use, regardless of whether the processor frequency changes. For more information about Jitter Control, see *HPE Gen10 Servers Intelligent System Tuning* at **www.hpe.com/suppport/gen10-intelligent-system-tuning-en**

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Advanced Performance Tuning Options**.
2. Configure settings.
   - **Processor Jitter Control**—Manages processor frequency variance due to technologies, such as Turbo, that varies the frequency based on power, thermals, and active cores. Select an option:

- **Auto-tuned**—Monitors frequency variance, and automatically adjusts the frequency to minimize variance over time.
- **Manual-tuned**—Operates the processor at a fixed frequency, and enables you to select lower or higher frequencies statically.
- **Disabled**—Disables Processor Jitter Control.

- **Processor Jitter Control Frequency**—Do one of the following:
  - If you selected **Auto-tuned**, enter a starting frequency unit in MHz.
  - If you selected **Manual-tuned**, enter a frequency unit in MHz.

    NOTE: If your specified frequency is not supported, the system firmware adjusts the frequency to the nearest higher intermediate frequency supported by the processor.

3. Save your changes.

Setting the redundant power supply mode

Use the **Redundant Power Supply Mode** 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** shares the power delivery equally between all installed power supplies.

Prerequisite

Workload Profile is set to **Custom**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Advanced Power Options** > **Redundant Power Supply Mode**.
2. Select a setting.
   - **Balanced Mode**—The system 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 semirandom 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. Save your setting.

Configuring the Embedded UEFI Shell

Enabling or disabling the Embedded UEFI Shell

Use the **Embedded UEFI Shell** option to enable or disable the 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 Embedded UEFI Shell is added to the UEFI Boot Order list.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Embedded UEFI Shell**.
2. Select a setting.
   - **Enabled**—Enables you to launch the **Embedded UEFI Shell** from the pre-boot environment and add it to the **UEFI Boot Order** list.
   - **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. Save your setting.

Adding the Embedded UEFI Shell to the UEFI Boot Order list

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Add Embedded UEFI Shell to Boot Order**.
2. Select a setting.
   - **Enabled**—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. Save your setting.

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

Use the **UEFI Shell Script Auto-Start** 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.
- 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 a network location first, followed by any locally attached FAT16, or FAT32-formatted media.
- It is recommended that you have only one `startup.nsh` file on one file system.

Prerequisites

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

Procedure

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

Enabling or disabling Shell script verification

Prerequisites

- **Boot Mode** is set to **UEFI Mode**.
- **Embedded UEFI Shell** is enabled.
- **Secure Boot** is enabled.
- Shell scripts are enrolled in the Secure Boot database.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Shell Script Verification**.
2. Select a setting.
   - **Enabled**—Enables Shell script verification.
   - **Disabled**—(Default) Does not enable Shell script verification.
3. Save your setting.

Setting the Embedded UEFI Shell startup script location

Use the **Shell Auto-Start Script Location** 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.

Prerequisites

- **Embedded UEFI Shell** is enabled.
- **UEFI Shell Script Auto-Start** is enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Shell Auto-Start Script Location**.
2. Select a setting.

- **Auto**—The Shell attempts to retrieve the startup script from the network location first, followed by locally attached media.
- **File Systems on Attached Media**—The Shell looks for the `startup.nsh` script file on a UEFI-accessible local file system, such as a FAT32 partition on a USB disk or HDD.
- **Network Location**—The Shell looks for a `.nsh` script at an HTTP/HTTPS or FTP location accessible to the system.

3. Save your setting.

Enabling or disabling discovery of the Shell auto-start script using DHCP

Use the **Discover Shell Auto-Start using DHCP** option to let the Shell discover the startup script URL using DHCP. When enabled, the Shell sends DHCP requests with the DHCP `User Class` option set to the string `UEFIShell`.

Prerequisites

- **Embedded UEFI Shell** is enabled.
- **UEFI Shell Script Auto-Start** is enabled.
- **HTTP Support** policy is enabled, and the URL provided by the DHCP server matches the HTTP Support policy setting.
- **Shell Auto-Start Script Location** is set to **Network Location** or **Auto**.
- The DHCP server is configured to provide HTTP/HTTPS or FTP URLs.
- The DHCP server is configured to respond to the `User Class` option set to `UEFIShell`. When using DHCP over IPv4, the User Class option is Option 77, and Option 15 when using DHCP over IPv6.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Discover Shell Auto-Start using DHCP**.
2. Select a setting.
   - **Enabled**—The Shell uses DHCP to discover the startup script URL.
   - **Disabled**—The Shell does not send DHCP requests to discover the startup script URL.
3. Save your setting.

Setting the network location for the Shell auto-start script

Prerequisites

- **Embedded UEFI Shell** is enabled.
- **Shell Auto-Start Script Location** is set to **Network Location** or **Auto**.
- **Shell Auto-Start Script Discovery using DHCP** is disabled.
- When specifying and HTTPS URL, the TLS certificate of the HTTPS server is configured using **Server Security** > **TLS (HTTPS) Options**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** > **Network Location for Shell Script-Auto Start**.
2. Enter the network location of the `.nsh` file. Valid values are:

- An HTTP/HTTPS URL for either an IPv4 or IPv6 server address or host name.
- An FTP URL for either an IPv4 or IPv6 server address or host name.

  Examples:

  - `http://192.168.0.1/file/file.nsh`
  - `http://example.com/file/file.nsh`
  - `https://example.com/file/file.nsh`
  - `http://[1234::1000]/file.nsh`

3. Save your setting.

Configuring Server Security

Server Security options

- Set Power On Password
- Set Admin Password
- Secure Boot Settings
- TLS (HTTPS) Options
- Trusted Platform Module options
- Intel (R) TXT Support
- One-Time Boot Menu (F11 Prompt)
- Processor AES-NI Support
- System Intrusion Detection
- Backup ROM Image Authentication

Setting the power-on password

Use the **Set Power On Password** option to set a password for accessing the server during the boot process. When you are 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Set Power On Password**.
2. Enter your password.

   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. Save your changes.
5. Reboot the server.

Setting an administrator password

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Set Admin Password**.
2. Enter the password.

   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. Save your changes.
5. Reboot the server.

Secure Boot

Secure Boot is a server security feature that is 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
- Preboot 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 **http://www.hpe.com/servers/ossupport**.

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 Remote Console.

You can configure Secure Boot:

- Using the **System Utilities** options described in the following sections.
- Using the iLO RESTful API to clear and restore certificates. For more information, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/redfish**).
- Using the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Enabling or disabling Secure Boot

Prerequisite

To enable this option:

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

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Attempt Secure Boot**.
2. Select a setting.
   - **Enabled**—Enables Secure Boot.
   - **Disabled**—Disables Secure Boot.
3. Save your changes.
4. Reboot the server.

Advanced Secure Boot Options

- **PK - Platform Key**—Establishes a trust relationship between the platform owner and the platform firmware.
- **KEK - 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.
- **DB - Allowed Signatures Database**—Maintains a secure boot allowed signature database of signatures that are authorized to run on the platform.
- **DBX - Forbidden Signatures Database**—Maintains a secure boot blacklist signature database of signatures that are not authorized to run on the platform
- **DBT - Timestamp Signatures Database**—Maintains signatures of codes in the timestamp signatures database.
- Delete all keys
- Export all keys
- Reset all keys to platform defaults

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.

Viewing Advanced Secure Boot Options settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Select the **View** entry for the exchange key or signatures database option.
4. Select the entry for the option you want to view.

Example: Viewing HPE UEFI Secure Boot 2016 PK Key details

From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options** > **PK - Platform Key** > **View PK entry** > **HPE UEFI Secure Boot 2016 PK Key**.

Enrolling a Secure Boot certificate key or database signature

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Select **Enroll <*option name*>**.
4. Select **Enroll <*option name*> using file**.

   The File Explorer screen shows attached media devices.
5. Select the attached media device where the certificate file is located and press **Enter**.
6. Continue selecting the menu path for the certificate file. Press **Enter** after each selection.
7. (Optional) Select a **Signature Owner GUID**.
8. (Optional) If you selected **Other** for the signature owner GUID, enter a **Signature GUID**.

   Use the following 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`

9. Select **Commit changes and exit**.

Example: Enrolling 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** > **KEK - Key Exchange Key** > **Enroll KEK entry**.
2. Select **Enroll KEK using file**.
3. Select the location of the certificate file from an attached media device.
4. (Optional) Select a **Signature Owner GUID**.
5. (Optional) If you selected **Other** for the signature owner GUID, enter a **Signature GUID**.
6. Select **Commit changes and exit**.

Deleting a Secure Boot certificate key or database signature

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Do one of the following.
   - If there is one option available for deletion:
     a. Select the **Delete <*option name*>** check box.
     b. Click **Yes**.
   - If there is more than one option available for deletion:
     a. Select **Delete <*option name*>**.
     b. Select the check box for the option you want to delete.
     c. Click **Yes**.

Example: 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** > **KEK - Key Exchange Key** > **Delete KEK entry**.
2. Select the check box for the entry you want to delete.
3. Click **Yes**.

Deleting all keys

The **Delete all keys** option deletes all keys in the system, including the Platform Key.

IMPORTANT:

After you delete all keys, the system is forced to immediately disable Secure Boot. Secure Boot remains disabled upon system reboot until valid secure boot keys are restored.

Procedure

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**.
2. Press **Enter** to delete all keys.
3. Confirm the deletion.

Exporting a Secure Boot certificate key or database signature

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Select **Export <*option name*>**.
4. Select the entry you want to export.

   A File Explorer screen shows attached media devices.
5. Do one of the following.
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press **Enter** after each selection.
   - To export to a new file, press **+**, and enter a file name.

Example: Exporting an Allowed Signatures Database signature

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options** > **DB - Allowed Signatures Database** > **Export Signature** > **HPE UEFI Secure Boot 2016 DB Key**.
2. Select the entry you want to export.

   A File Explorer screen shows attached media devices.
3. Do one of the following.
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press **Enter** after each selection.
   - To export to a new file, press **+**, and enter a file name.

Exporting all Secure Boot certificate keys

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options** > **Export all keys**.

   A File Explorer screen shows attached media devices.
2. Do one of the following.
   - Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press **Enter** after each selection.
   - To export to a new file, press **+**, and enter a file name.

Resetting a Secure Boot certificate key or database signature to platform defaults

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Select **Reset to platform defaults**.
4. Click **Yes**.

Resetting all Secure Boot certificate keys to platform defaults

Procedure

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**.
2. Click **Yes**.

TLS (HTTPS) Options

Viewing TLS certificate details

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **View Certificates**.
2. Select a certificate.

Enrolling a TLS certificate

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Enroll Certificate**.
2. Select **Enroll certificate using File Explorer**.

   The File Explorer screen shows attached media devices.
3. Select the attached media device where the certificate file is located and press **Enter**.
4. Continue selecting the menu path for the certificate file. Press **Enter** after each selection.
5. Select **Commit changes and exit**.

Deleting a TLS certificate

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Delete Certificate**.
2. From the list of certificates, select the certificates you want to delete.
3. Select **Commit changes and exit**.

Deleting all TLS certificates

The **Delete all Certificates** option deletes all certificates in the system.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Delete all Certificates**.
2. Press **Enter**.
3. Confirm the deletion.

Exporting a TLS certificate

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Export Certificate**.
2. Select a file format for the exported certificate.

   A File Explorer screen shows attached media devices.
3. Do one of the following.
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press **Enter** after each selection.
   - To export to a new file, press **+**, and enter a file name.

Exporting all TLS certificates

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Export all Certificates**.

   A File Explorer screen shows attached media devices.
2. Do one of the following.
   - Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press **Enter** after each selection.
   - To export to a new file, press **+**, and enter a file name.

Resetting all TLS settings to platform defaults

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Reset all settings to platform defaults**.
2. Click **OK**.

Configuring advanced TLS security settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Advanced Security Settings**.
2. Configure options.
   - To configure which cipher suites are allowed for TLS connections:
     a. Select **Cipher suites allowed for TLS connections**.
     b. Select one of the following:

- Individual check boxes for the cipher suites you want to allow.
- **Select Platform Default Cipher suites**

c. Select **Commit changes and exit**.

- To configure the certificate validation process for every TLS connection:

  a. Select **Certificate validation process for every TLS connection**.

  b. Select a setting:

  - **PEER** (recommended)—The certificate presented by the peer is validated for secure communication.
  - **NONE**—Does not validate the certificate.

- To enable or disable strict host name checking:

  a. Select **Strict Hostname checking**.

  b. Select a setting:

  - **ENABLE**—The host name of the connected server is validated with the host name in the certificate supplied by the server.
  - **DISABLE**—The host name of the connected server is not validated with the host name in the certificate supplied by the server.

- To specify which protocol version to use for TLS connections:

  a. Select **TLS Protocol Version Support**.

  b. Select a setting:

  - **AUTO**—Negotiates the highest protocol version that is supported by both the TLS server and the client.
  - **1.0**—Uses TLS protocol version 1.0.
  - **1.1**—Uses TLS protocol version 1.1.
  - **1.2**—Uses TLS protocol version 1.2.

3. Save your changes.

Configuring Trusted Platform Module options

Trusted Platform Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to make sure that the platform remains trustworthy. For servers configured with a Trusted Platform Module, TPM enables the firmware and operating system to take measurements of all phases of the boot process. For information on installing and enabling the TPM module option, see the user documentation for your server model.

When enabling the Trusted Platform module, observe the following guidelines:

- By default, the Trusted Platform Module is enabled as TPM 2.0 when the server is powered on after installing it.
- In UEFI Mode, the Trusted Platform Module can be configured to operate as TPM 2.0 or TPM 1.2.
- In Legacy Boot Mode, the Trusted Platform Module configuration can be changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module options**.
2. Select an option. On servers configured with an optional TPM, you can set the following:
   - **TPM 2.0 Operation**—Sets the operation of TPM 2.0 to execute after a reboot. Options are:
     - **No Action**—There is no TPM configured.
     - **Clear**—TPM is cleared during reboot, and **TPM 2.0 Operation** is set to **No Action**.
   - **TPM Mode Switch**—Sets the TPM mode to execute after a reboot. Options are:
     - **No Action**
     - **TPM 1.2**
     - **TPM 1.2, FIPS**
     - **TPM 2.0**
   - **TPM 2.0 Visibility**—Sets whether TPM is hidden form the operating system. Options are:
     - **Visible**
     - **Hidden**—Hides TPM from the operating system. Use this setting to remove TPM options from the system without having to remove the actual hardware.
   - **TPM UEFI Option ROM Measurement**—Enables or disables (skips) measuring UEFI PCI operation ROMs. Options are:
     - **Enabled**
     - **Disabled**
   - **Chipset-TPM**—This option is visible only when there is no physical TPM chip installed. This option sets the state of a virtual TPM, for example the Intel PTT. Options are:
     - **Enabled**
     - **Disabled**
3. Save your changes.
4. Reboot the system.

   After the system reboots, you can view the **Current TPM Type** and **Current TPM State** settings.
5. Verify that your new **Current TPM Type** and **Current TPM State** settings appear at the top of the screen.

Enabling or disabling Intel TXT support

Use the Intel TXT Support option to enable or disable Intel TXT (Trusted Execution Technology) support for servers with Intel processors.

Prerequisites

Before you can enable Intel (R) TXT support, you must enable:

- All Intel processor cores
- Hyperthreading
- VT-d
- TPM

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

NOTE:

A physical TPM is always enabled, discoverable, and working by default. A virtual TPM is not on by default and must be enabled manually.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Intel (R) TXT Support**.
2. Select a setting.
   - **Enabled**—Enables TXT support
   - **Disabled**—Disables TXT support.
3. Save your changes.

Enabling or disabling the 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. When this option is enabled, you can boot directly into the One-Time Boot Menu in the System Utilities by pressing F11 in the POST screen after a server reboot.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **One-Time Boot Menu (F11 Prompt)**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your changes.

Enabling or disabling the Intelligent Provisioning F10 prompt

Use the **Intelligent Provisioning (F10 Prompt)** option to control whether you can press the F10 key to access Intelligent Provisioning from the POST screen.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Intelligent Provisioning (F10 Prompt)**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling processor AES-NI support

Use the Processor AES-NI option to enable or disable the Advanced Encryption Standard Instruction Set in the processor.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Processor AES-NI Support**.
2. Select a setting.

- **Enabled**—Enables AES-NI support.
- **Disabled**—Disables AES-NI support.

3. Save your changes.

Enabling or disabling backup ROM image authentication

Use the Backup ROM Image Authentication option to enable or disable cryptographic authentication of the backup ROM image on startup.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Backup ROM Image Authentication**.
2. Select a setting.
   - **Enabled**—The backup ROM image is authenticated on startup.
   - **Disabled**—The backup ROM image is not authenticated on startup. Only the primary image is authenticated.
3. Save your changes.

Enabling or disabling system intrusion detection

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **System Intrusion Detection**.
2. Select a setting.
   - **Enabled**—Intrusion detection is enabled.
   - **Disabled**—Intrusion detection is not enabled.
3. Save your changes.

Configuring PCIe devices

Selecting advanced PCIe device settings

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration** > **Advanced PCIe Configuration.**
2. Select settings.
   - **NVMe PCIe Resource Padding**—Configures PCIe resources to support PCIe hot-add for NVMe drives.
     - **Normal**—Only allocates PCIe resources to devices installed at boot time. PCIe hot-add is not supported.
     - **Medium**—Allocates additional PCIe resources for each PCIe root port, which might enable a PCIe hot-add event to work without requiring a system reboot to enumerate the device.
     - **High**—Allocates a maximum amount of PCIe resources to allow for the best chance of supporting a PCIe hot-add event.
   - **Maximum PCI Express Speed**—When **Workload Profile** is set to **Custom**, sets the maximum speed at which the server allows PCI Express devices to operate.
     - **Per Port Control**
     - **PCIe Generation 1.0**
3. Save your settings.

Configuring specific PCIe devices

Use the **PCIe Device Configuration** options to enable or disable, and select configuration settings for embedded and added-in PCI devices. Disabling devices reallocates the resources (memory, I/O, and ROM space and power) that are normally allocated to the device. By default, all devices are enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration**.
2. Select a device from the list.
3. Select settings. Depending on the device, options include:
   - **Device Disable**
     - **Auto**—The device is automatically enabled at server boot.
     - **Disabled**—The device is not automatically enabled.
   - **PCIe Link Speed**
     - **Auto**—Sets the link speed to the maximum supported speed of the PCIe link.
     - **PCIe Generation 1.0**—Sets the link speed to a maximum speed of PCIe Generation 1.0.
     - **PCIe Generation 2.0**—Sets the link speed to a maximum speed of PCIe Generation 2.0.
     - **PCIe Power Management (ASPM)**

        - **Auto**
        - **Disabled**
        - **L1 Enabled**—The device's link enters a lower power standby state at the expense of a longer exit latency.
    - **PCIe Option ROM**
        - **Enabled**—The platform optimally loads PCIe Option ROMs to save boot time.
        - **Disabled**—The platform disables all PCIe Option ROM optimizations, which might be required for older PCIe devices.
4. Save your settings.

Configuring advanced platform configuration options

Selecting a ROM image

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

Procedure

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

Configuring an embedded video connection

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Embedded Video Connection**.
2. Select a setting.
   - **Auto**—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. Save your setting.

Enabling or disabling Consistent Device Naming

On supported operating systems, use the **Consistent Device Naming** option to control 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Consistent Device Naming**.
2. Select a setting.

- **CDN Support for LOMs and Slots**—Names all NIC ports on the system.
- **CDN Support for LOMs Only**—Names Embedded NICs and FlexibleLOMs, but no other NIC ports.
- **Disabled**—Disables consistent device naming.

3. Save your setting.

Enabling or disabling mixed power supply reporting

Use the **Mixed Power Supply Reporting** option to set whether the server logs messages when a mixed supply configuration is present.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Mixed Power Supply Reporting**.
2. Select a setting.
   - **Enabled**
   - **Disabled**
3. Save your setting.

Enabling or disabling High Precision Event Timer (HPET) ACPI Support

Use the **High Precision Event Timer (HPET) ACPI Support** option to enable or disable the High Precision Event Timer (HPET) table and device object in ACPI.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **High Precision Event Timer (HPET) ACPI Support**.
2. Select a setting.
   - **Enabled**—The HPET is available to an operating system that supports it using the industry standard ACPI name space.
   - **Disabled**—The HPET is not available to an operating system that supports it using the industry standard ACPI name space.
3. Save your setting.

Setting TPM FIPS Mode Switch Operation

Use the **TPM FIPS Mode Switch Operation** option to set whether TPM operates using the Federal Information Processing Standard.

Prerequisites

- Your operating system supports TPM 1.2 FIPS mode.
- Trusted Platform Module **TPM Mode Switch** setting is set to **1.2, FIPS**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **TPM FIPS Mode Switch Operation**.
2. Select a setting.

- **No Action**—No mode is set.
- **Regular mode**—TPM does not operate in FIPS mode.
- **FIPS mode**—TPM operates using the Federal Information Processing Standard.

3. Save your setting.

Setting the thermal configuration

Use the **Thermal Configuration** 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**.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Fan and Thermal Options** > **Thermal Configuration**.
2. Select a setting.
   - **Optimal Cooling**—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. Save your setting.

Enabling or disabling thermal shutdown

Use the **Thermal Shutdown** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Fan and Thermal Options** > **Thermal Shutdown**.
2. Select a setting.
   - **Enabled**—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. Save your setting.

Setting fan installation requirements messaging

Use the **Fan Installation Requirements** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Fan and Thermal Options** > **Fan Installation Requirements**.
2. Select a setting.

- **Enable Messaging**—The server displays messages and log events to the IML when required fans are not installed. The server can still boot and operate. This setting 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.

3. Save your setting.

Setting the fan failure policy

Use the **Fan Failure Policy** 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.

Procedure

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

Enabling or disabling higher ambient temperature support

Use the **Extended Ambient Temperature Support** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Fan and Thermal Options** > **Extended Ambient Temperature Support**.
2. Select a setting.
   - **Disabled**
   - **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 servers support both 40c Ambient (ASHRAE 3) and 45c Ambient (ASHRAE 4).

3. Save your setting.

Re-entering a serial number

Use the **Serial Number** option to re-enter the server serial number after replacing the system board. This value must match the serial number sticker located on the back of the chassis.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Service Options** > **Serial Number**.
2. Enter the serial number and press **Enter**.
3. Save the setting.

Re-entering a product ID

Use the **Product ID** option to re-enter the product ID after replacing the system board. This value must match the product ID sticker located on the back of the chassis.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Service Options** > **Product ID**.
2. Enter the product ID and press **Enter**.
3. Save your setting.

Configuring advanced debug options

Prerequisites

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

Use **Advanced Debug Options** to control the output level of debug and POST boot progress messages.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Debug Options**.
2. Select settings.
   - **UEFI Serial Debug Message Level**—Sets the level of debug messages output to the serial console.
     - **Disabled**
     - **Errors Only**
     - **Medium**
     - **Network**
     - **Verbose**

       NOTE:

       This setting can significantly increase boot time.
     - **Custom**
   - **POST Verbose Boot Progress**—Enables detailed messaging that might be helpful in determining why a server became unresponsive during the boot process.

- **Disabled**
- **Serial Only**—Detailed messages are output to the serial console.
- **All**—Detailed messages are output to the POST screen and serial console.

3. Save your settings.

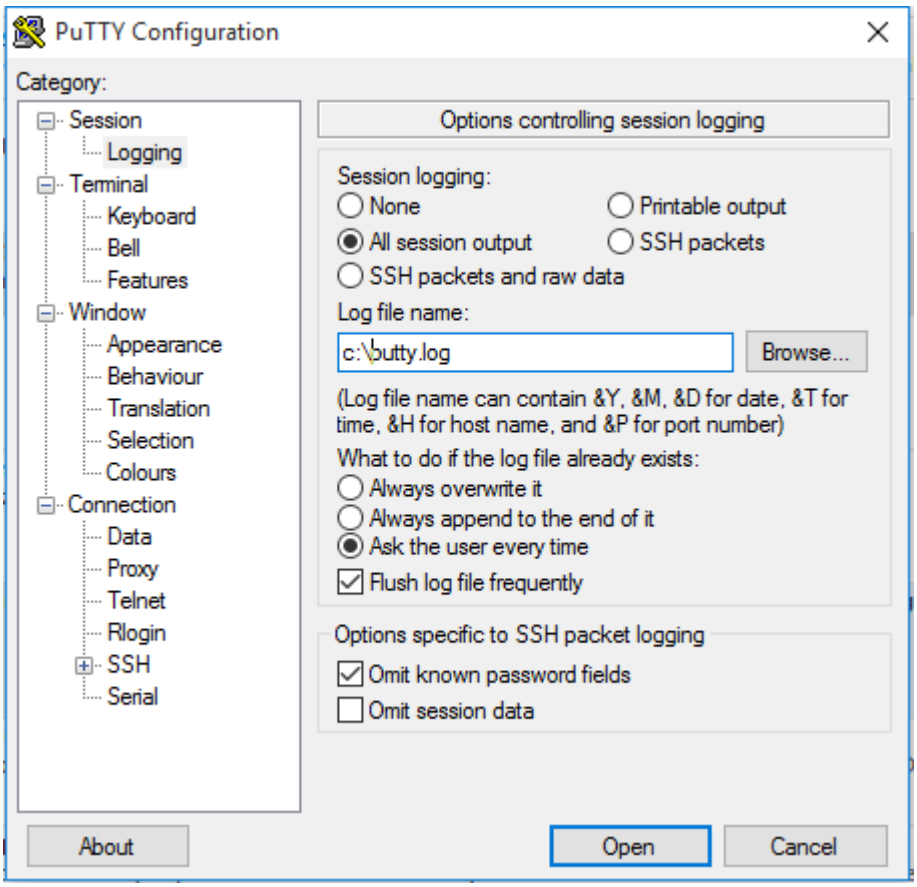
Obtaining UEFI serial output log data with the UEFI System Utilities

Use this task to obtain serial output log data if physical access to the server is not available. If you are using a PCIe Expansion Card, you can enable debug collection from the card.

Procedure

1. During POST press F9 to enter **System Utilities**.
2. From the System Utilities screen, select **System Configurations** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Debug Options**.
3. Set the debug level:
   a. Select **UEFI Serial Debug Level**.
   b. Select **Medium Verbosity**.
4. If you are using an expansion card, enable debug data collection from the expansion card:
   a. Select **POST Verbose Boot Progress**.
   b. Select either **Serial Only** or **All**.
5. Save and exit System Utilities.
6. Open an iLO Virtual Serial Port (VSP) session. See **Launching the System Utilities**.
7. Use a utility, such as PuTTY, to establish the connection and ensure that you enable logging to a file (select **All session output**).

   The following example shows sample PuTTY settings for logging data:


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Options controlling session logging
Session logging:
None
Printable output
All session output
SSH packets
SSH packets and raw data
Log file name:
c:\putty.log
Browse...
(Log file name can contain &Y, &M, &D for date, &T for time, &H for host name, and &P for port number)
What to do if the log file already exists:
Always overwrite it
Always append to the end of it
Ask the user every time
Flush log file frequently
Options specific to SSH packet logging
Omit known password fields
Omit session data
About
Open
Cancel

Configuring the date and time and system defaults

Setting the Date and Time

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Date and Time**.
2. Select a setting, and then complete your entry.
   - **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**—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**—Does not adjust the local time displayed for Daylight Savings Time.
   - **Time Format**
     - **Coordinated Universal Time (UTC)**—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. Save your settings.

Resetting system defaults

Restoring default system settings

Use the **Restore Default System Settings** 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)

  To save a custom default configuration to use during a system restore, use **User Default Options**. Doing so saves settings you might otherwise lose.
- Other entities, such as option cards or iLO, that must be individually reset.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** > **Restore Default System Settings**.
2. Select **Yes, restore the default settings**.
3. Reboot the server.

Restoring default manufacturing settings

Use the **Restore Default Manufacturing Settings** 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**.

To save a custom default configuration to use during a system restore, use **User Default Options**. Doing so saves settings you might otherwise lose.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** > **Restore Default Manufacturing Settings**.
2. Select **Yes, restore the default settings**.
3. Reboot the server.

Changing the default UEFI device priority

Use the **Default UEFI Device Priority** 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 in this option. 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.

Prerequisites

User Default Options are configured and saved.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** > **Default UEFI Device Priority**.
2. Select an entry.
3. Use the **+** key to move the entry higher in the list. Use the **-** key to move it lower in the list. Use your pointing device or the arrow keys to navigate the list.
4. Save your settings.

Saving or erasing user default options

Use **User Default Options** 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.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** > **User Default Options**.
2. Select an option.
   - **Save User Defaults**

- **Yes, Save**—Saves the current settings as the system default settings.
- **No, Cancel**—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 settings manually.
  - **No, Cancel**—Does not erase the current user-defined default settings

3. Save your setting.

Scripted configuration flows

Using scripted configuration flows

Scripted configuration flow

You can use BIOS/Platform Configuration (RBSU) with the RESTful API Tool to create standard server configuration scripts to automate many of the manual steps in the server configuration process.

iLO RESTful API support for UEFI

ProLiant servers and HPE Synergy compute modules include support for configuring UEFI BIOS settings using the RESTful API. The RESTful API Tooi is a management interface that server management tools can use to perform server configuration, inventory, and monitoring. A REST client uses HTTPS operations to configure supported server settings, such as iLO 5 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**).

Configuration Replication Utility (CONREP)

CONREP is included in the STK and is a utility that operates with the BIOS/Platform Configuration (RBSU) to replicate hardware configuration. 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. You can find the STK on the Hewlett Packard Enterprise website (**http://www.hpe.com/servers/stk**). 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**).

HPE Smart Storage Administrator (SSA)

HPE SSA Scripting is a standalone application that is distributed with the HPE SSA CLI application and is used for configuring arrays on Smart Array devices. 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**.

Troubleshooting

Troubleshooting

Cannot boot devices

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

1. 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**.

2. Retry the boot procedure.

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 that your card is supported before you install it. Although third-party option cards might work, they are not optimized for 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

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

Action

1. Use **User Default Options** to save a custom default configuration to use during a system restore.
2. Retry the boot procedure.

Cannot restore system defaults

Symptom

- 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

1. Use the **Restore Default System Settings** option, or the **Restore Default Manufacturing Settings** option to restore your settings.
2. Retry the procedure.

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 URL 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 UEFI Shell user guide.
2. Change your static network connection settings and try to download the file in URL again.

Solution 2

Cause

The DHCP server did not respond.

Action

1. Ensure that 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 that 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 that you have admin privileges on the server.

Action

1. Ensure that the file is present, and 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.
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.
   a. The Embedded UEFI Shell interface is added to the **UEFI Boot Order** list or the **One-Time Boot Menu**.
   b. When added to the **UEFI Boot Order** list, the Embedded UEFI Shell interface is the first boot option in the **UEFI Boot Order** list so that it overrides other boot options to load.
   c. UEFI Shell Script Auto-Start is enabled.
   d. 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.
   e. The `.nsh` script only contains supported commands.
   f. Your system has enough RAM memory to create RAM disks during automated script execution.
   g. Any OS boot loader or diagnostics application launched using the `.nsh script` is supported to run in UEFI the environment.
   h. If the shell script verification is enabled, ensure the script is enrolled in the Secure Boot database and that the script starts with the line #!NSH.
2. Try the deployment again.

Cannot execute Option ROM for one or more devices

Symptom

You cannot execute Option ROM for one or more devices.

Cause

The amount of available Option ROM space has been exceeded.

Action

1. Disable any unnecessary option ROMs (such as PXE).
2. Retry the procedure.

Cannot find a new network or storage device in the Boot Order list

Symptom

You connected a network or storage device, and it does not appear in the Boot Order list.

Cause

Newly-added devices do not appear in the boot order list until you reboot the system.

Action

1. Reboot the system.
2. Verify that your device appears in the Boot Order list.

Intel TXT is not working properly

Cause

One of the prerequisites may not be enabled.

Action

- Verify that the prerequisites are enabled:
  - All Intel processor cores
  - Hyperthreading
  - VT-d
  - TPM

Invalid Server Serial Number and Product ID

Symptom

You see an error message that the Server Serial Number and Product ID are invalid, corrupted, or lost.

Cause

The serial number, product ID, or both, are invalid, corrupted, or lost.

Action

1. Enter the correct values for these fields.
2. Verify that the error message does not appear again.

Invalid time or date

Symptom

You see a message stating that the time and date is not set.

Cause

The time or date in the configuration memory is invalid.

Action

1. Use the Date and Time option to change the settings.
2. Verify that the message does not appear again.

Networking devices are not functioning properly

Cause

Only networking devices on the list of supported server options should be used.

Action

- Hewlett Packard Enterprise recommends that networking devices be updated to the latest version of firmware before they are used in the server. Before installing the operating system, use the latest Service Pack for ProLiant in Offline mode to upgrade the firmware to the latest version.

NOTE:

If the default boot mode settings are different than the user-configured settings, the system might not boot the OS installation when the defaults are restored. To avoid this issue, use the User Default Options feature in UEFI System Utilities to override the factory default settings.

System unresponsive

Cause

There is a mis-configured or malfunctioning PCIe expansion card.

Action

- Enable PCIe debug information collection to identify the problem card. See **Obtaining UEFI serial output log data with the UEFI System Utilities.**

Server will not boot

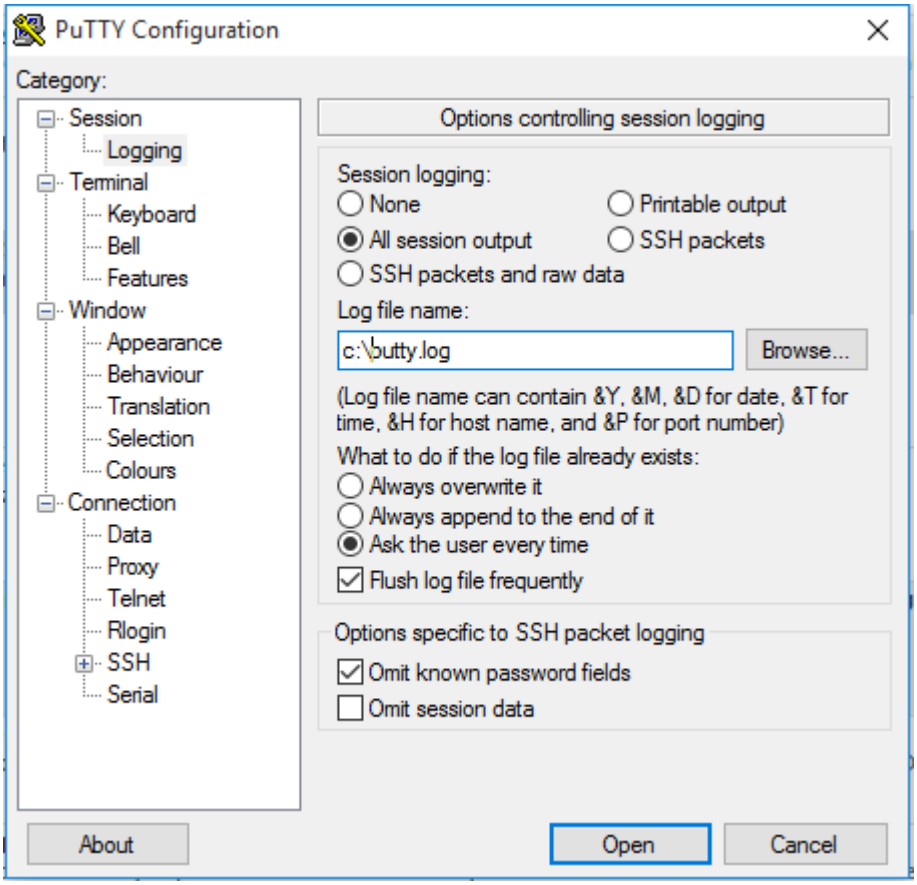
Cause

Enable serial debug with the maintenance switch

Action

1. Power off the server.
2. Locate the Server Maintenance Switch (12 position switch) and set DIP 4 to the ON position. Refer to the chassis hood label for details on the location of the switch.
3. Attach a NULL mode cable to the server serial port or open an iLO Virtual Serial Port (VSP) session.
4. Use a utility, such as PuTTY, to establish the connection and ensure that you enable logging to a file (select **All session output**).

   The following example shows sample PuTTY settings for logging data:



Smart Array controllers are not functioning properly

Cause

Other Smart Array controllers are not supported and will not function properly.

For more information on supported options, see the server QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).

For more information on the latest firmware and driver versions, see the Hewlett Packard Enterprise website (**https://www.hpe.com/support/hpesc**).

Action

- Hewlett Packard Enterprise recommends that Smart Array controllers be updated to the latest version of firmware before they are used in the server. Before installing the operating system, use the latest Service Pack for ProLiant in Offline mode to upgrade the firmware to the latest version.

VMware not booting in UEFI mode

Cause

UEFI Optimized Boot is not enabled.

Action

- Enable UEFI Optimized Boot.

Support

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

UEFI Specification

www.uefi.org/specifications

UEFI Learning Resources

www.uefi.org/learning_center

RESTful API Tool

http://www.hpe.com/info/redfish

Contact Hewlett Packard Enterprise Worldwide

http://www.hpe.com/assistanceenter

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

For additional websites, see **Support and other resources**.

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:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

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

  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 HPE Passport set up with relevant entitlements.

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:

http://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.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

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.