Unified Extensible Firmware Interface (UEFI)

What's new

- Secure Start enabled for enhanced security
- HTTP/HTTPS boot and NVMe drive boot options now supported
- HPE Smart Array initial configuration available on UEFI pre boot environment and
  iLO RESTful API
- Workload Profiles for performance optimization
- RAS enhancements - HPE Fast Fault Tolerance Memory Support

Overview

Wondering how to get your HPE ProLiant Server up and running with improved security using industry standard interfaces?

Each HPE ProLiant Gen9 and Gen10 Server supports Unified Extensible Firmware Interface (UEFI). This industry standard is a set of interfaces between the system firmware, the operating system, and various components of the system firmware that deliver enhanced security benefits for the HPE Servers.

The HPE ProLiant system BIOS is a UEFI solution based on the latest UEFI Specification revisions. In addition, most HPE ProLiant Gen9 and Gen10 Server are UEFI Class 2 solution, supporting both Legacy BIOS boot and UEFI boot modes,

providing users the flexibility to switch between modes. UEFI supports iLO RESTful API and is Redfish API conformant.

Features

Increase Server Security with combined UEFI Secure Boot and Secure Start

UEFI provides a higher level of security by protecting against unauthorized operating systems and malware rootkit attacks, validating that only authenticated ROMs, pre-boot applications, and OS boot loaders that have been digitally signed are run.

Secure Start Hardware Root of Trust.

All UEFI drivers, OS boot loaders, and UEFI applications are digitally signed and binaries are verified using a set of embedded trusted keys. Only validated and authorized components are executed.

Performs safety checks to prevent inadvertently disabling Secure Boot in failure modes and logging security violations for auditing purposes.

HPE ProLiant Gen10 Servers support the optional Trusted Platform Module (TPM). TPM 2.0 is supported when the platform is in UEFI boot mode and can be used by the operating system to enhance system security.

Improved deployment performance available on UEFI System Utilities

Take advantage of Workload Profiles for simplifying performance optimization for customer workload matching.

Intelligent System Tuning enables Processor Jitter Control to avoid processor frequency changes (including Turbo Mode transitions) that introduce latency. Jitter reduction algorithm finds the frequency that allows the workload most upside with no jitter.

HPE Smart Array for Gen10 Servers configuration now available on the UEFI System Utilities and iLO RESTful API.

Increased Memory Resiliency with RAS (Reliability, Availability, and Serviceability). RAS enables memory error detection and correction features (such as Address-based Memory Mirroring, HPE Fast Fault Tolerance Memory, and POST Package Repair) to prevent data corruption and avoid system disruptions.

Take Advantage of Embedded UEFI Shell and iLO RESTful API - Redfish API Conformant for scalability

UEFI includes the UEFI Shell, a command line interface (CLI) application that allows scripting, file manipulation, obtaining system information, and running other UEFI applications plus more than ten HPE specific commands for easier configuration.

UEFI Shell is based on the UEFI Shell Specification 2.1, with improvements for server configuration, hardware inventory, firmware updates, deployment, and Secure Boot key management

UEFI supports iLO RESTful API and is Redfish API conformant. You can create your own UEFI applications, or configure UEFI with the scripting RESTful Interface Tool to manage BIOS and HPE Smart Array Attribute Registry resources and match the latest BIOS/Platform Configuration options.

Configure UEFI with Standard Boot Methods for an Enhanced and Flexible Network

UEFI supports PXE boot for IPv6 networks allowing a unified network stack to PXE boot from any network controller while maintaining backward compatibility and continuing to support IPv4 PXE.

Supports PXE Multicast boot for image deployment to multiple servers at the

same time.

UEFI Extended Network Stack for IPv4 enhancements overcome the limitations of PXE and TFTP by using more reliable TCP connections instead of UDP.

Modern booting from HTTP or HTTPS (New on HPE ProLiant Gen10) with a URL boot option that can be an EFI boot loader or a deployment ISO image.

New System Utilities BIOS/Platform Configuration (RBSU) IPv6 DHCP Unique Identifier menu that allows users to select how the UEFI BIOS will use the DHCP Unique Identifier (DUID) for IPv6 PXE Boot.

For additional technical information, available models and options, please reference the QuickSpecs

Make the right purchase decision.
Contact our presales specialists.

Download

Chat now (sales)

Share now

Get updates

Parts and Materials: HPE will provide HPE-supported replacement parts and materials required to maintain the covered hardware.

Parts and components that have reached their maximum supported lifetime and/or the maximum usage limitations as set forth in the manufacturer's operating manual, product quick-specs, or the technical product data sheet will not be provided, repaired, or replaced as part of these services.

Image may differ from the actual product

PSN6935826WWEN, May, 2024.

Hewlett Packard Enterprise