Overview

HPE ProLiant Compute Gen12 Embedded Security

Experience unparalleled security benefits when you choose the HPE ProLiant Compute Gen12 servers for your infrastructure needs. These servers have cutting-edge embedded security features, ensuring robust protection for your critical data and applications. With a focus on adaptability and scalability, these servers offer top-notch performance while maintaining the highest level of security. Backed by a comprehensive warranty, they provide peace of mind and a reliable foundation for your security server infrastructure. Make a confident choice and elevate your security posture with the unbeatable security advantages of HPE ProLiant Compute Gen12 servers.

Physical Security Options

- **System maintenance switch**
- **USB security**
- **Rack and power security**
- **Bezel lock**
- **Chassis intrusion detection switch**

HPE Integrated Lights-Out (HPE iLO 7)

Enhance your server security with the advanced embedded security features of HPE iLO 7, allowing you to monitor ongoing management, service alerting, reporting, and remote management with confidence.

Secure Enclave with FIPS 140-3 Level 3 support enhances Silicon Root of Trust using Advanced Key Management

Learn more at iLO Security Implementation Guide **https://www.hpe.com/info/iLO.**

Server Data Security

The available Gen12 controller and drive security highlights are depicted below.

Encryption and key management

Remote Key Management

iLO manages the key exchange between the key manager and the other products. iLO uses a unique user account based on its MAC address to communicate with the key manager. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the key manager with administrator privileges. For more information about the deployment of the user account, see the key manager documentation.

The following key managers are supported.

- ESKM/KMIP Supported Formats
- Utimaco ESKM
- Thales ChiperTrust

For version information, see the iLO user guide: **http://www.hpe.com/support/ilo7-ug-en**

Local Key Management

The server securely stores local encryption keys in iLO's secure enclave which is in process for FIPS 140-3 Level 3 validation. The encryption keys can be managed through the UEFI BIOS interface, the iLO GUI, and Redfish APIs.

Overview

Self-encrypting drives (SED)

For storage devices that support the Opal Storage Specification, security is enhanced by making the storage device self-encrypting (SED). Self-encrypting drives encrypt stored data so that an unauthorized user cannot read it. The encryption keys are protected by a local master key (LMK) or through the use of a random master key (RMK).

For more information about self-encrypting drives, see **Self-encrypting drives.**

To view the HPE self-encrypting drive offerings, see the HPE ProLiant Compute SSD Selector Tool: **https://ssd.hpe.com/**

SED is the ideal choice for data-at-rest encryption. It is an HDD or SSD that contains an Advanced Encryption Standard (AES) hardware encryption engine, which encrypts data at line rate as it is written to the storage media and provides access control by locking the drive when power is lost. The media encryption key (MEK) encrypts all the user data on the drive. It is stored encrypted on the drive, and the user cannot access it. The MEK is encrypted with a user password, also called a key encrypting key (KEK), which is used to unlock the drive. The KEK can be stored and managed by Host key management (HKM), Local key management (LKM), and Remote key management (RKM).

SED is ideal for customers who need their data protected with encryption. SEDs provide data-at-rest protection, which means that when power is lost (for example, when the server is turned off), the drive is locked. If someone steals a drive from a server, they cannot read any of the data from that drive. SED performs at line rate, so it does not impact overall server performance, which is critical for customers in the financial service industry (FSI), healthcare, and the U.S. government sectors.

For more information, see the HPE Storage controllers and server: data encryption overview at the following website: **https://www.hpe.com/info/SCEO.**

HPE Compute MR Controllers

HPE Compute MR controllers support Self-Encrypting Drives (SED) that secure the drive data from unauthorized access or modification. Because the data on the drive is encrypted, it cannot be accessed without appropriate security authorization, even if an SED drive is removed from the storage system.

The following key management types are supported:

- **Host Key Management (HKM)**—Manage SEDs by using third-party key management such as SEDutil. SED monitoring is available in HPE MR Storage Administrator, the Storage Command Line Interface (StorCLI) tool, and the UEFI System Utilities.
- **Local Key Management (LKM)**—Enable SED drive security for local key management by using HPE MR Storage Administrator, the StorCLI tool, or the UEFI System Utilities. During setup, you provide a security key identifier and security key. At startup, the security key stored in the controller unlocks the drive. When the drive is powered off, the security-enabled drive data encryption key is locked.
- **Remote Key Management (RKM)**—The UEFI System Utilities works with the iLO key manager configuration to create the security key identifier and security key in the remote key manager server. When the drive is powered off, the security-enabled drive data encryption key is locked. At startup, the security key is retrieved from the remote key manager server to unlock the drive.

To view the controllers a server or compute module supports, see the QuickSpecs document at the following website: **https://www.hpe.com/info/quickspecs**.

Overview

Authentication and Trust of Server Components - SPDM

HPE ProLiant Compute Gen12 servers with iLO 7 use SPDM (Security Protocol and Data Model) to verify the integrity of components and authenticate supported option cards. This allows extending the HPE Silicon Root of Trust to additional components and their firmware in the system. Examples of supported hardware include PCIe option cards, such as storage controllers and network adapters, direct-attached NVMe drives, power supplies, storage backplanes, and riser cards.

This feature uses open DMTF standards to enable a zero-trust configuration between the server management software and the supported server options.

The policy on how the server reacts when a component cannot be authenticated is configurable via iLO 7 settings.

One Button Secure Erase

If you want to decommission a server or prepare it for a different use, you can use the One-button secure erase feature to securely erase user data from the server.

One-button secure erase follows the NIST Special Publication 800-88 Revision 1 in the *Guidelines for Media Sanitization* guide. The appendix recommends minimum sanitization levels for media, ensuring that it is not possible for even a determined malicious party to re-create the data which had been stored on the media. For more information about the specification, see Section 2.5 **Guidelines for Media Sanitization**.

One-button secure erase implements the NIST SP 800-88 Revision 1 Sanitization Recommendations and returns the server and support components to the default state. This feature automates many of the tasks you follow in the **Statement of Volatility** document for a server.

One-button secure erase for DevIDs and System IAK

iLO LDevID, System LDevID, and System LAK certificates are removed during the One-button secure erase process. IDevIDs and IAKs are read-only from the factory in Gen 12 and thus are not removed.

When you use the One-button secure erase process, Hewlett Packard Enterprise recommends performing a manual iLO backup to minimize the impact of losing the iLO LDevID, System LDevID, and LAK certificates. iLO includes all the certificates in its backup service and you can restore the certificates from the backup file.

For More information: **One-button secure erase FAQ**

Standard Features

Industry Security Compliance

- FIPS 140-3
  - iLO 140-3 Level 1 & 3
  - SED 140-3 Level 1
- Secure Digital 4.0
- TPM 2.0 Support
  Notes: Since Gen11, the TPM is integrated by default. Placement of the TPM and the routing of electrical signals to the TPM are optimized for protection against physical attacks. Customers can view the current Trusted Platform Module (**TPM**) configuration and update the settings with the UEFI System Utilities. By default, the TPM 2.0 device is enabled. Performing operations such as disabling the TPM or Clearing its contents can be performed in the UEFI System Utilities.
- NIST
  - NIST SP 800-53: This publication provides a comprehensive set of security controls for federal information systems and organizations and covers a wide range of security areas, including access control, audit and accountability, risk assessment, and system and information integrity.
  - NIST SP 800-171: This standard outlines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations. HPE ProLiant Compute servers comply with the security controls specified in NIST SP 800-171 to ensure the protection of CUI when used in government environments.
  - NIST SP 800-88: This publication provides guidelines for media sanitization, ensuring that sensitive data is securely erased from storage media before disposal or reuse. HPE ProLiant Compute servers adhere to the media sanitization guidelines outlined in NIST SP 800-88 to prevent data breaches during the decommissioning process.
  - NIST SP 800-147B: This publication provides guidelines for securely protecting the BIOS in servers systems against attacks. This includes protection against software attacks which could modify the contents of the BIOS storage part as well as ensuring that flash update operations are performed securely and that images are authenticated prior to being committed to the BIOS storage part.
  - NIST SP 800-193: This publication provides guidelines for protecting the numerous firmware and critical data in a compute system from unauthorized modification and attack. Similar to NIST 800-147B which was focused on the BIOS, this specification extends the protections to other firmware in the system, including the base management controller (BMC) firmware, option card, such as network and storage controllers, firmware, drive firmware, and other firmware. In addition, the specification provides guidelines to protect critical data, such as security settings, against attacks which could compromise the security posture of the system.
- Advanced Encryption Standard (AES)
- LMS
- RSA and ECDSA
- TLS 1.3
- Open SSL 3.xx
- CNSA 1.0
- Common Criteria EAL4+
- Tamper-free updates – components digitally signed and verified. Validate you are using genuine HPE products here: **https://www.hpe.com/us/en/validate.html**

Standard Features

Embedded Security

HPE Server UEFI

Unified Extensible Firmware Interface (UEFI) is an industry standard that provides better manageability and more secured configuration than the legacy ROM while interacting with your server at boot time. HPE ProLiant Compute Gen12 servers have a UEFI Class 3 implementation to support UEFI Mode. This means that HPE ProLiant Compute Gen12 severs only support UEFI Boot mode and do NOT support Legacy Boot Mode.

UEFI enables numerous capabilities specific for HPE ProLiant servers such as:

- UEFI Secure Boot and Secure Start enable enhanced security as part of the ProLiant Silicon Root of Trust.
- Embedded UEFI Shell
- Server Configuration Lock

Notes: The UEFI System Utilities tool is analogous to the HPE ROM-Based Setup Utility (RBSU) of legacy BIOS. For more information, please visit **https://www.hpe.com/servers/uefi**. Server Configuration Lock protects a server against tampering or compromise to the server composition. You can enable this feature when a server is in transit or use it all the time to monitor for configuration changes. Please visit:
https://support.hpe.com/hpesc/public/docDisplay?docId=a00117189en_us&page=GUID-1AD22221-A36A-48A8-8E0D-445164A9A2E4.html

HPE Compute Ops Management

Unlock unparalleled security advantages across your fleet of iLO enabled servers with HPE Compute Ops Management. HPE is revolutionizing compute management by providing an intuitive cloud operating experience on the HPE GreenLake platform, ensuring streamlined and highly secure operations from the edge to the cloud. Benefit from automated key lifecycle tasks, including onboarding, updating, managing, and monitoring HPE servers, to achieve enhanced security and efficiency. Manage single locations or multiple distributed sites with ease, while leveraging batch policy controls and automated updates to keep tens to thousands of servers secure. Elevate your security posture and gain peace of mind with the comprehensive security features offered by HPE Compute Ops Management.

For more information, visit the HPE Compute Ops Management Security Best Practices:
https://www.hpe.com/psnow/doc/a50004263enw

Standard Features

Secure Supply Chain Services

HPE supply chain security innovation: Enhancing trust and resilience from edge to cloud hyperlink to **https://www.hpe.com/psnow/doc/a00134892enw?jumpid=in_pdfviewer-psnow**

At HPE, we have designed a high-performing and trusted supply chain ecosystem with our partners, suppliers, customers, and employees to provide a foundational line of defense against cybersecurity risk against cybercriminals. HPE is committed to providing a highly secure supply chain as an important step toward reducing cybersecurity risks for our customers as they modernize their hybrid cloud environments from edge to cloud.

For Hardened Servers from HPE Global Factory Network, consider one of these specialized services:

- **HPE Trusted Supply Chain** (P36394-B21) is an optional security upgrade intended for agencies and regulated industries needing enhanced security and compliance needs. Applying this option to a DL3XX Gen12 CTO server ensures it has a country of origin of the USA in a secured facility by vetted HPE personnel assigned to the manufacturing processes. Many checkpoints/inspections for malicious microcode and counterfeit parts are performed throughout the server build, and additional safeguards are put in place against cyber-exploits throughout the server lifecycle. The HPE ProLiant Compute Gen12 Embedded Security is re-branded as a HPE ProLiant DL3XX Gen12 to denote the HPE Trusted Supply Chain security enhancements. Trusted Supply Chain enabled servers are Trade Agreement Act (TAA) compliant and have a country-of-origin USA. **https://buy.hpe.com/us/en/options/enterprise-security-protection/security-modules/security-chips-modules/hpe-trusted-supply-chain-for-hpe-proliant/p/p36394-b21**
  Notes: HPE offers multiple Trade Agreement Act (TAA) compliant configurations to meet the needs of US Federal Government customers. These products are either manufactured or substantially transformed in a designated country. TAA compliance is only provided when HPE options are included as part of factory-integrated orders (CTO).

- The **Server Security Optimization Service**, available with part number R9S59A, is designed to enhance server security and optimize protection for organizations worldwide with stringent security and compliance requirements. By opting for this service on any Gen12 server, you can ensure that your server is meticulously built in a secure facility by trusted HPE personnel who safeguard the manufacturing processes. Multiple checkpoints and inspections are conducted to detect and mitigate malicious microcode and counterfeit parts during the server build, with added security measures implemented to defend against cyber threats throughout the server's lifecycle. **https://buy.hpe.com/us/en/options/enterprise-security-protection/security-modules/security-chips-modules/hpe-server-security-optimized-service-for-hpe-proliant/p/r9s59a**

Notes: For More Details of overall Compute Security, please visit Compute Security Reference Guide: **https://support.hpe.com/hpesc/public/docDisplay?docId=a00018320en_us**

Service and Support

Consulting Services

No matter where you are in your journey to hybrid cloud, experts can help you map out your next steps. From determining what workloads should live where, to handling governance and compliance, to managing costs, our experts can help you optimize your operations.

https://www.hpe.com/services/consulting

HPE Managed Services

HPE runs your IT operations, providing services that monitor, operate, and optimize your infrastructure and applications, delivered consistently and globally to give you unified control and let you focus on innovation.

HPE Managed Services | HPE

Operational services

Optimize your entire IT environment and drive innovation. Manage day-to-day IT operational tasks while freeing up valuable time and resources. Meet service-level targets and business objectives with features designed to drive better business outcomes.

https://www.hpe.com/services/operational

HPE Lifecycle Services

HPE Lifecycle Services provide a variety of options to help maintain your HPE systems and solutions at all stages of the product lifecycle. A few popular examples include:

- Lifecycle Install and Startup Services: Various levels for physical installation and power on, remote access setup, installation and startup, and enhanced installation services with the operating system.
- HPE Firmware Update Analysis Service: Recommendations for firmware revision levels for selected HPE products, taking into account the relevant revision dependencies within your IT environment.
- HPE Firmware Update Implementation Service: Implementation of firmware updates for selected HPE server, storage, and solution products, taking into account the relevant revision dependencies within your IT environment.
- Implementation assistance services: Highly trained technical service specialists to assist you with a variety of activities, ranging from design, implementation, and platform deployment to consolidation, migration, project management, and onsite technical forums.
- HPE Service Credits: Access to prepaid services for flexibility to choose from a variety of specialized service activities, including assessments, performance maintenance reviews, firmware management, professional services, and operational best practices.

Notes: To review the list of Lifecycle Services available for your product, go to:

https://www.hpe.com/services/lifecycle

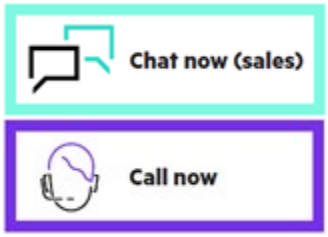
For a list of the most frequently purchased services using service credits, see the **HPE Service Credits Menu**

Summary of Changes

Date	Version History	Action	Description of Change
05-May-2025	Version 2	Changed	Overview and Standard Features sections were updated.
24-Feb-2025	Version 1	New	New QuickSpecs

Copyright

Make the right purchase decision.
Contact our presales specialists.



Get updates

a50009218enw - 17250 - Worldwide - V2 - 05-May-2025

Hewlett Packard Enterprise