Server Configuration Lock User Guide for HPE ProLiant Compute servers and HPE Synergy

Part Number: 30-E6DC65C0-006
Published: August 2026
Edition: 6

Server Configuration Lock User Guide for HPE ProLiant Compute servers and HPE Synergy

Abstract

This document describes how to configure and use the Server Configuration Lock feature on Hewlett Packard Enterprise servers and compute modules with HPE iLO 5, HPE iLO 6, and HPE iLO 7. This document is for individuals who are responsible for the secure configuration and operation of HPE servers.

Part Number: 30-E6DC65C0-006
Published: August 2026
Edition: 6

© Copyright 2021–2026 Hewlett Packard Enterprise Development LP

Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for the information outside the Hewlett Packard Enterprise website.

Revision history

Part number	Publication date	Edition	Summary of changes
30-E6DC65C0-006	August 2026	6	Modified the Lost or forgotten Server Configuration Lock password troubleshooting topic.
30-E6DC65C0-005	June 2025	5	Updated for Gen12 server support.

Part number	Publication date	Edition	Summary of changes
30-E6DC65C0-004	July 2024	4	Added instructions for recovering a server that is in halt status with Server Configuration Lock enabled.
30-E6DC65C0-003	November 2022	3	• Updated to include Gen11 products. • Added information about the HPE Server Security Optimized Service for HPE ProLiant.

Table of contents

Server Configuration Lock....5
Server Configuration Lock system requirements....6
Server Configuration Lock and remote management....7
Disabling Server Configuration Lock in-transit status with the UEFI System Utilities....7
Configuring Server Configuration Lock with the UEFI System Utilities....9
Configuring Server Configuration Lock by using a REST client....14
Server Configuration Lock settings....16
Viewing Server Configuration Lock status in the iLO web interface....18
Server Configuration Lock errors and troubleshooting....20
Lost or forgotten Server Configuration Lock password....20
Unable to edit selected server settings....20
Unable to edit Server Configuration Lock settings....21
A server is stuck in halt status with Server Configuration Lock enabled....22
HPE Trusted Supply Chain....23
HPE Trusted Supply Chain server configuration....24
HPE Server Security Optimized Service for HPE ProLiant....25
Security resources....26
Support and other resources....28
Accessing Hewlett Packard Enterprise Support....28
HPE product registration....29
Accessing updates....29
Remote support....30
Warranty information....30
Regulatory information....31
Documentation feedback....31

Server Configuration Lock

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.

HPE Trusted Supply Chain servers ship with this feature enabled and the server is set to `in-transit` status. HPE creates the Server Configuration Lock password and it is securely transmitted to the customer. On first boot, the customer enters the password to disable the `in-transit` status. At this time, they can disable or modify the feature configuration.

Server Configuration Lock creates a digital fingerprint of the server configuration. The digital fingerprint is a securely stored log file on the server TPM 2.0 (if supported) or in the server nonvolatile memory.

Server Configuration Lock monitors the server for:

- DIMM changes
- CPU changes
- PCIe device changes
- Security configuration changes
- System firmware revisions
- Server Configuration Lock password authentication failures

If a configuration change is detected during POST, an administrator must enter the Server Configuration Lock password to review the issue and continue the startup process. The configuration change is recorded in the Integrated Management Log (IML). A count of the detected issues is available in the Server Configuration Lock detection log in the UEFI System Utilities.

You can configure Server Configuration Lock in the UEFI System Utilities or by using the iLO RESTful API.

> **IMPORTANT**
> When you use Server Configuration Lock, remember to record the password securely. By design, this security feature prevents bypassing or resetting the password when it is lost or forgotten.

Subtopics

Server Configuration Lock system requirements
Server Configuration Lock and remote management

Disabling Server Configuration Lock in-transit status with the UEFI System Utilities
Configuring Server Configuration Lock with the UEFI System Utilities
Configuring Server Configuration Lock by using a REST client
Server Configuration Lock settings
Viewing Server Configuration Lock status in the iLO web interface
Server Configuration Lock errors and troubleshooting

More information

HPE Trusted Supply Chain
Lost or forgotten Server Configuration Lock password

Server Configuration Lock system requirements

- The installed System ROM/BIOS firmware supports the Server Configuration Lock feature.
  - **Gen10 and Gen10 Plus servers**: Version 2.00 is required for Intel-based servers, and version 1.40 is required for AMD-based servers.
  - **Gen11 servers**: All versions.
  - **Gen12 servers**: All versions.

  NOTE

  The Server Configuration Lock feature is not available on HPE Gen11 and Gen12 servers that use Ampere processors.

- The server is configured to use **UEFI Boot Mode** and **UEFI Optimized Boot** is enabled.

  Server Configuration Lock is not supported in Legacy Boot Mode.
- For iLO 5 only: The server was rebooted after upgrading to iLO 5 1.40 or later.
- For iLO 5 and iLO 6 only: The server was rebooted after the security state was changed from Production to a higher security state.
- An iLO Advanced license is installed.

Server Configuration Lock and remote management

Performing automated configuration and management tasks on servers and compute modules with remote management tools such as HPE OneView and the iLO RESTful API is not supported when Server Configuration Lock is enabled. When a change to the digital fingerprint is detected, the Server Configuration Lock password is required during POST, which prevents the completion of automated tasks.

More information

Configuring Server Configuration Lock by using a REST client
Configuring Server Configuration Lock with the UEFI System Utilities
Disabling Server Configuration Lock in-transit status with the UEFI System Utilities

Disabling Server Configuration Lock in-transit status with the UEFI System Utilities

Prerequisites

The server is set to `in-transit` status.

About this task

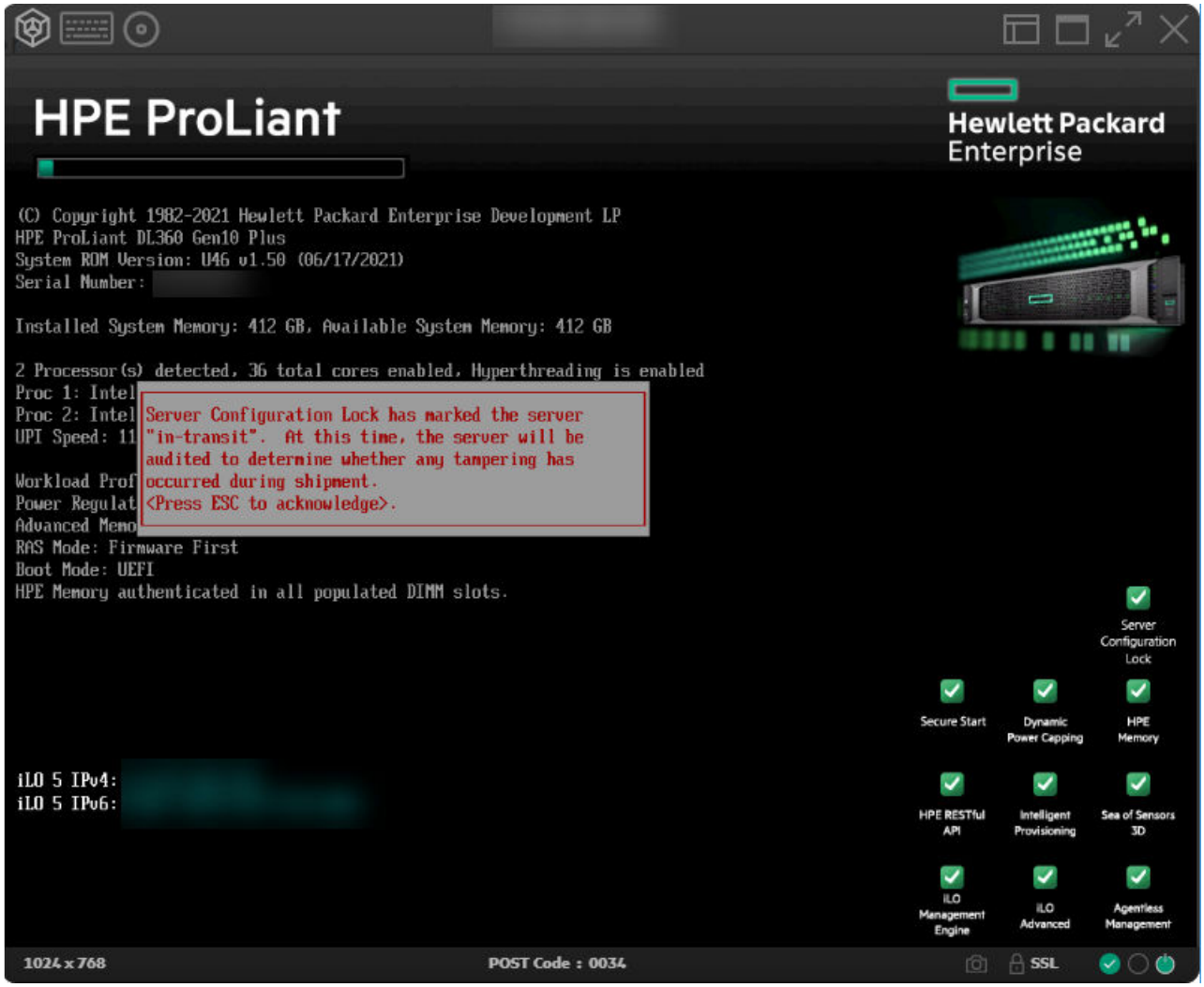
When you power on a server that is configured with Server Configuration Lock `in-transit` status, complete the following steps to continue the startup process.

Procedure

1. Power on the server and observe the POST process.

   To observe the POST process, start the server locally or use the iLO remote console.

   During POST, the following message appears:



2. Press `ESC` to acknowledge the message.

   The server prompts you for the Server Configuration Lock password.

   If you are starting an HPE Trusted Supply Chain server for the first time, the password was securely transmitted to you or your administrator by Hewlett Packard Enterprise. If it is not an HPE Trusted Supply Chain server, the password was set by the administrator who configured the Server Configuration Lock feature.

3. Enter the Server Configuration Lock password, and then press `Enter`.

   The startup process resumes.

4. (Optional) Press **F9** to start the UEFI System Utilities.

5. (Optional) Edit the Server Configuration Lock settings.

More information

Configuring Server Configuration Lock with the UEFI System Utilities

Configuring Server Configuration Lock with the UEFI System Utilities

Prerequisites

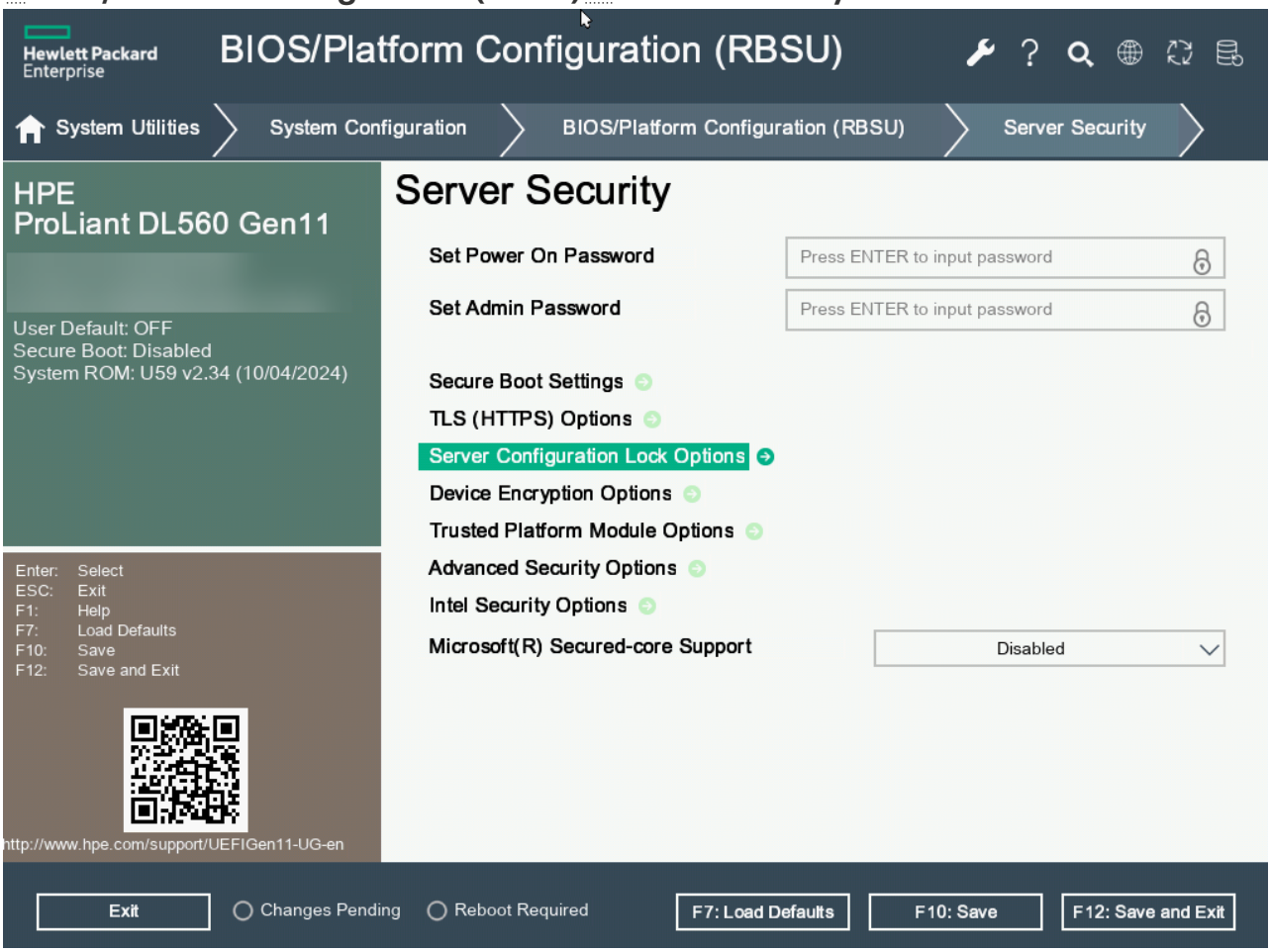
A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/hpeilodocs-quicklinks**.

Procedure

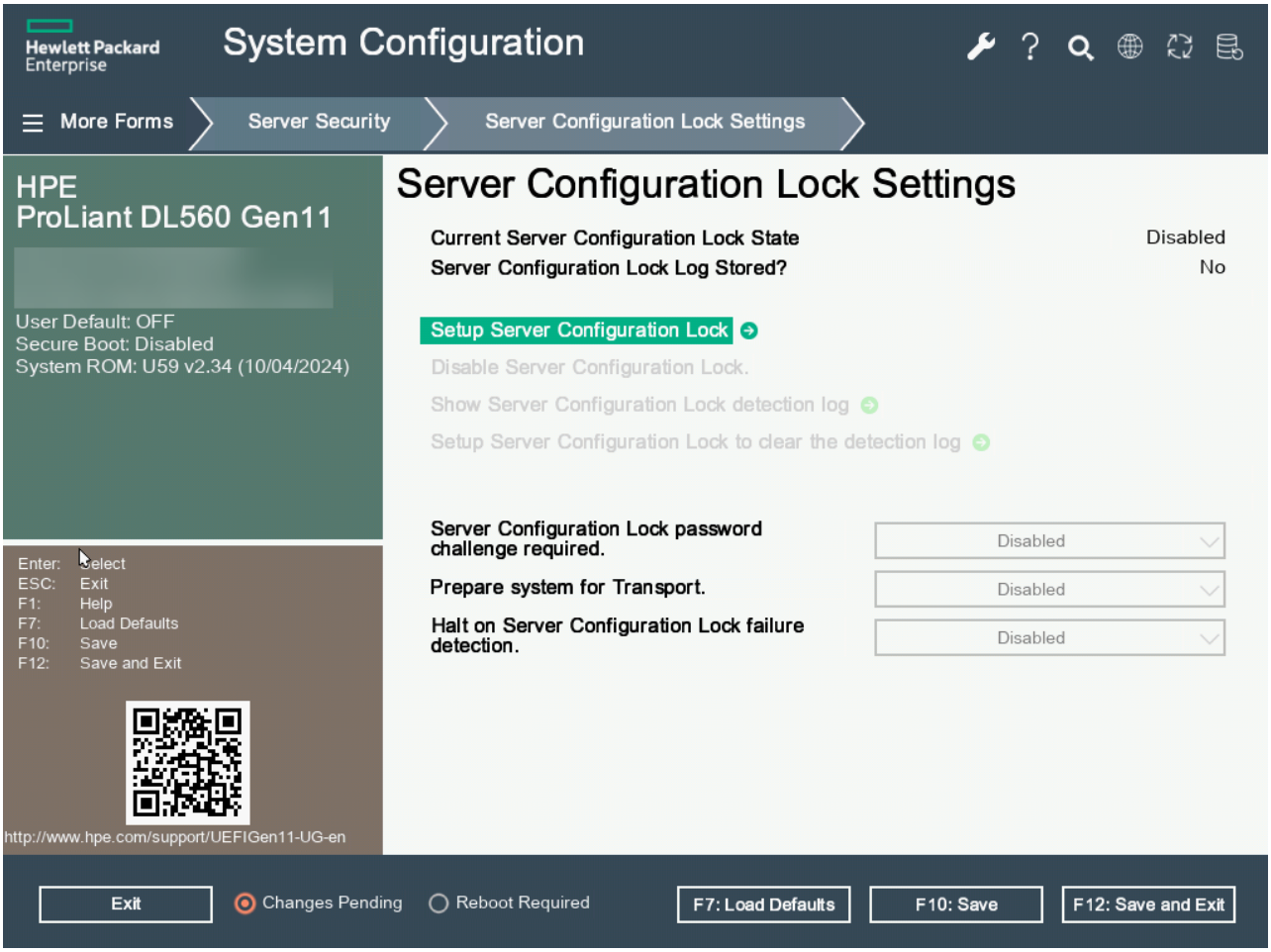
1. Start the UEFI System Utilities.
   a. (Optional) If you access the server remotely, start an iLO remote console session.
   b. Restart or power on the server.
   c. Press **F9** in the server POST screen.

   The UEFI System Utilities start.

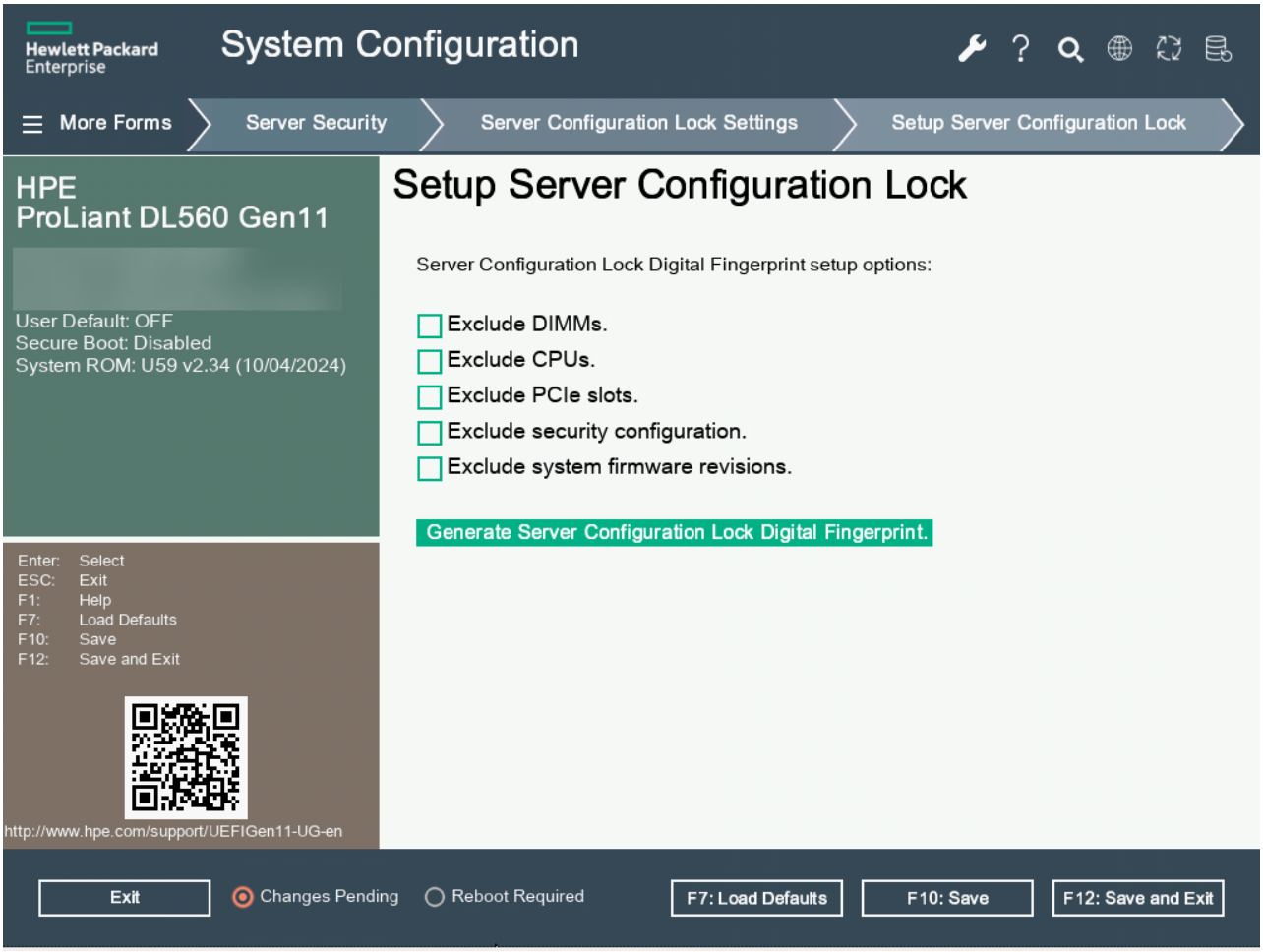
2. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security**.



3. Select **Server Configuration Lock Options**.



4. Click **Setup Server Configuration Lock**.

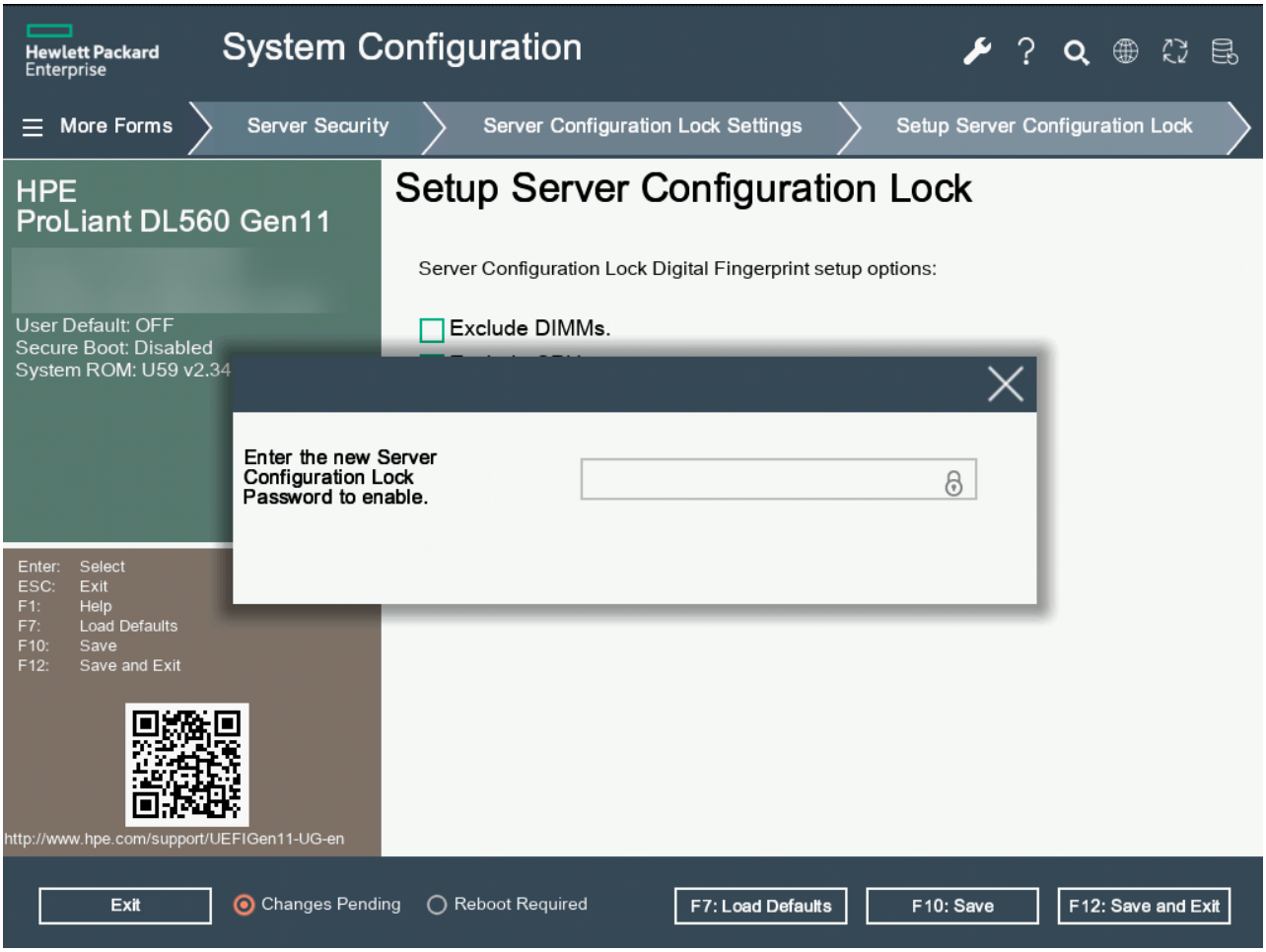


5. (Optional) Select or clear check boxes for the components that you want to exclude from the Server Configuration Lock digital fingerprint.

   For more information, see Server Configuration Lock settings.

6. Click **Generate Server Configuration Lock Digital Fingerprint**.

   A Server Configuration Lock password prompt is displayed.



7. Enter a Server Configuration Lock password, and then press **Enter**.

   The Server Configuration Lock password is case-sensitive. It can be 16–31 characters long.

   The software prompts you to re-enter the password.

8. Re-enter the password, and then press **Enter**.

   The software confirms that the password was updated.

9. Click **OK**.

0. (Optional) To update additional Server Configuration Lock settings, click **Server Configuration Lock Options**.

   You can disable the feature or update the following settings:

   - **Server Configuration Lock Challenge required**.
   - **Prepare system for Transport**.
   - **Halt on Server Configuration Lock failure detection**.

For more information, see Server Configuration Lock settings.

1. To save the changes and exit, press **F12**.
2. When prompted to confirm the request, click **Yes - Save Changes**.

   The UEFI System Utilities notify you that a system reboot is required.
3. Click **Reboot**.

More information

Server Configuration Lock settings
Server Configuration Lock system requirements

Configuring Server Configuration Lock by using a REST client

Prerequisites

- iLO user account with the Host BIOS privilege.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/hpeilodocs-quicklinks**.

Procedure

1. Set up a REST client to log in to iLO.

   For example, in Postman, select the **Basic Auth** authorization type and enter your iLO credentials.
2. (Optional) To view the current settings, enter a command similar to the following:

   For Gen10:

   ```
   Get iLO hostname or IP address/redfish/v1/systems/1/bios/
   serverconfiglock/
   settings/
   ```

   For Gen10 Plus, Gen11, and Gen12:

   ```
   Get iLO hostname or IP address/redfish/v1/systems/1/bios/oem/hpe/
   serverconfiglock/settings/
   ```

   The output is similar to the following Gen10 Plus server example:

```
{
  "@odata.context": "/
redfish/v1/$metadata#HpeServerConfigLock.HpeServerConfigLock",
  "@odata.etag": "W/\"49261F237D999393939CACCDA535394E\"",
  "@odata.id": "/redfish/v1/systems/1/bios/oem/hpe/serverconfiglock/
settings/",
  "@odata.type": "#HpeServerConfigLock.v1_0_0.HpeServerConfigLock",
  "Id": "settings",
  "Name": "Server Configuration Lock Pending Settings",
  "NewServerConfigLockPassword": null,
  "ServerConfigLockChallenge": "Disabled",
  "ServerConfigLockDisable": "False",
  "ServerConfigLockExcludeCpus": "False",
  "ServerConfigLockExcludeDimms": "False",
  "ServerConfigLockExcludeFwRevs": "False",
  "ServerConfigLockExcludePciSlots": "False",
  "ServerConfigLockExcludeSecurity": "False",
  "ServerConfigLockLogStored": "False",
  "ServerConfigLockPassword": null,
  "ServerConfigLockState": "Enabled",
  "ServerConfigLockTamperHalt": "Disabled",
  "ServerConfigLockTransport": "Disabled"
}
```


3. Use a `patch` command to modify the settings.

   For example:

   ```
   {
   "ServerConfigLockPassword": "config_lock_password",
   "ServerConfigLockChallenge": "Enabled"
   }
   ```

   Ensure that you select raw and JSON in your REST client. The Server Configuration Lock password is required.

   The REST client notifies you that a reboot is required for the changes to take effect. For example:

   ```
   "MessageId": "iLO.2.14.SystemResetRequired"
   ```

4. Reboot the server.

More information

Server Configuration Lock settings
Server Configuration Lock system requirements

Server Configuration Lock settings

The UEFI System Utilities **Server Configuration Lock Settings** page shows the following values and options:

Current Server Configuration Lock State

This read-only value indicates feature status (enabled or disabled).

This value is called `ServerConfigLockState` in the iLO RESTful API.

Server Configuration Lock Log Stored?

This read-only value indicates whether a saved Server Configuration Lock detection log is available. A saved log is available after a discrepancy is detected.

This value is called `ServerConfigLockLogStored` in the iLO RESTful API.

Setup Server Configuration Lock

Use this option to configure the Server Configuration Lock feature.

This value is called `ServerConfigLockPassword` in the iLO RESTful API.

Disable Server Configuration Lock

Use this option to disable the Server Configuration Lock feature.

This value is called `ServerConfigLockDisable` in the iLO RESTful API. When you update this setting with the iLO RESTful API, the Server Configuration Lock password is required.

Show Server Configuration Lock detection log

Use this option to view a saved log. If there is no saved log, this value is unavailable.

There is no equivalent value in the iLO RESTful API.

Setup Server Configuration Lock to clear the detection log

Use this option to update the Server Configuration Lock settings. This action clears a saved detection log. If there is no saved log, this value is unavailable.

The iLO RESTful API equivalent is to use `NewServerConfigLockPassword` and `ServerConfigLockPassword` to clear the log and create a new digital fingerprint.

Server Configuration Lock password challenge required

When enabled, the Server Configuration Lock password is required at startup.

This value is called `ServerConfigLockChallenge` in the iLO RESTful API. When you update this setting with the iLO RESTful API, the Server Configuration Lock password is required.

Prepare system for Transport

When enabled, the Server Configuration Lock password is required at the first boot to disable the `in-transit` status.

This value is called `ServerConfigLockTransport` in the iLO RESTful API. When you update this setting with the iLO RESTful API, the Server Configuration Lock password is required.

Halt on Server Configuration Lock failure detection

When enabled, the Server Configuration Lock will halt on a configuration change detection. This feature is useful with servers that are managed remotely through the iLO RESTful API, without a keyboard or video option.

This value is called `ServerConfigLockTamperHalt` in the iLO RESTful API. When you update this setting with the iLO RESTful API, the Server Configuration Lock password is required.

Server Configuration Lock options

The following options are available when you set up Server Configuration Lock.

Password

The Server Configuration Lock password is case-sensitive. It can be 16–31 characters long.

Digital Fingerprint options

To customize the information included in the Server Configuration Lock Digital Fingerprint, select or clear the following check boxes:

- **Exclude DIMMs**

  Excludes DIMMs from the digital fingerprint.

  This value is called `ServerConfigLockExcludeDimms` in the iLO RESTful API.

- **Exclude CPUs**

  Excludes CPUs from the digital fingerprint.

  This value is called `ServerConfigLockExcludeCpus` in the iLO RESTful API.

- **Exclude PCIe slots**

  Excludes PCIe slots from the digital fingerprint

This value is called `ServerConfigLockExcludePciSlots` in the iLO RESTful API.

- **Exclude security configuration**

  Excludes security configuration changes from the digital fingerprint.

  This value is called `ServerConfigLockExcludeSecurity` in the iLO RESTful API.

- **Exclude system firmware revisions**

  Excludes system firmware revisions from the digital fingerprint.

  This value is called `ServerConfigLockExcludeFwRevs` in the iLO RESTful API.

More information

Configuring Server Configuration Lock by using a REST client
Configuring Server Configuration Lock with the UEFI System Utilities

Viewing Server Configuration Lock status in the iLO web interface

Procedure

Depending on your iLO version:

- Click **Information** in the navigation tree, and then click the **Security Dashboard** tab.
- Click **Security** on the left navigation pane.

The configured Server Configuration Lock setting is displayed.

Figure 1. iLO 5 and iLO 6 Security Dashboard

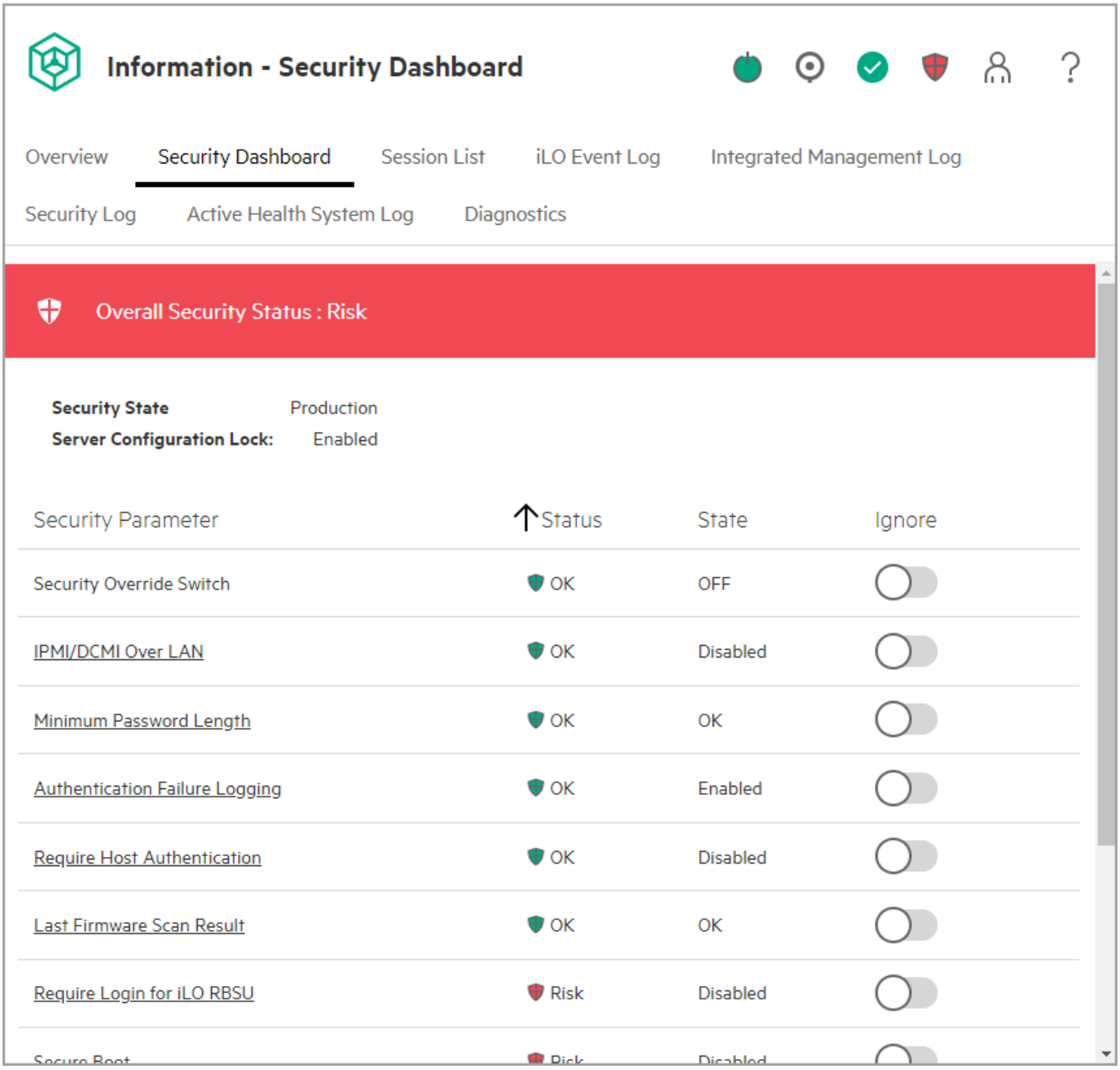
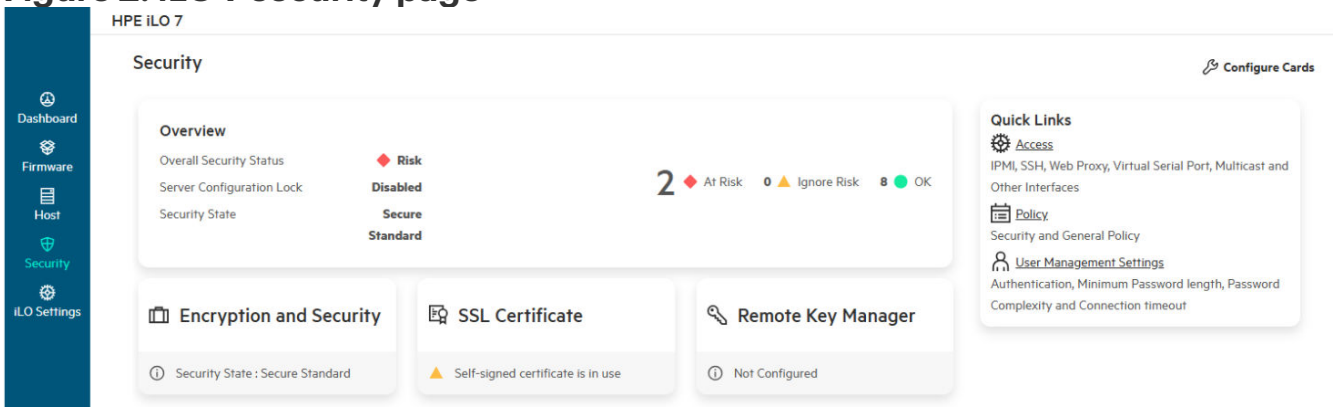


Figure 2. iLO 7 security page



Server Configuration Lock errors and troubleshooting

Subtopics

Lost or forgotten Server Configuration Lock password
Unable to edit selected server settings
Unable to edit Server Configuration Lock settings
A server is stuck in halt status with Server Configuration Lock enabled

Lost or forgotten Server Configuration Lock password

Symptom

Server Configuration Lock is enabled and the password is lost or forgotten.

Cause

You have an HPE Trusted Supply Chain server, and the Server Configuration Lock password created by Hewlett Packard Enterprise is lost or forgotten.

Action

Contact the License Support Center (**https://myenterpriselicense.hpe.com/cwp-ui/contact-us**) to obtain the Server Configuration Lock password defined by Hewlett Packard Enterprise. Include your HPE order number and applicable serial numbers.

Unable to edit selected server settings

Symptom

You cannot edit selected server settings with the UEFI System Utilities, iLO, or the iLO RESTful API. If you try to edit an affected setting, it might be unavailable, an error might occur, or the value reverts to the previous setting after a reboot.

Some examples of the affected settings follow:

- Boot Mode
- UEFI Optimized Boot
- TPM 2.0 Visibility

- TPM Mode Switch
- Post Screen Mode

Cause

Server Configuration Lock is enabled.

Action

1. Turn off Server Configuration Lock, and then edit the affected settings.
2. (Optional) Re-enable Server Configuration Lock.

More information

Configuring Server Configuration Lock with the UEFI System Utilities
Configuring Server Configuration Lock by using a REST client

Unable to edit Server Configuration Lock settings

Symptom

You cannot edit the Server Configuration Lock settings.

Cause

Certain server settings prevent updates to the Server Configuration Lock configuration. For example, you cannot configure Server Configuration Lock when:

- Legacy Boot Mode is enabled.
- UEFI Optimized Boot is disabled.

Action

Update the server configuration to ensure that it meets the Server Configuration Lock system requirements.

A server is stuck in halt status with Server Configuration Lock enabled

Symptom

A server with Server Configuration Lock enabled needs to be recovered from halt status.

Action

1. Set up a REST client to log in to iLO.

   For example, in Postman, select the **Basic Auth** authorization type and enter your iLO credentials.

2. (Optional) To view the current settings, enter a command similar to the following:

   For Gen10:

   ```
   Get iLO hostname or IP address/redfish/v1/systems/1/bios/
   serverconfiglock/
   settings/
   ```

   For Gen10 Plus and Gen11:

   ```
   Get iLO hostname or IP address/redfish/v1/systems/1/bios/oem/hpe/
   serverconfiglock/settings/
   ```

   The output is similar to the following Gen10 Plus server example:

   ```
   {
     "@odata.context": "/
   redfish/v1/$metadata#HpeServerConfigLock.HpeServerConfigLock",
     "@odata.etag": "W/\"49261F237D999393939CACCDA535394E\"",
     "@odata.id": "/redfish/v1/systems/1/bios/oem/hpe/serverconfiglock/
   settings/",
     "@odata.type": "#HpeServerConfigLock.v1_0_0.HpeServerConfigLock",
     "Id": "settings",
     "Name": "Server Configuration Lock Pending Settings",
     "NewServerConfigLockPassword": null,
     "ServerConfigLockChallenge": "Disabled",
     "ServerConfigLockDisable": "False",
     "ServerConfigLockExcludeCpus": "False",
     "ServerConfigLockExcludeDimms": "False",
     "ServerConfigLockExcludeFwRevs": "False",
     "ServerConfigLockExcludePciSlots": "False",
     "ServerConfigLockExcludeSecurity": "False",
     "ServerConfigLockLogStored": "False",
   ```

```
  "ServerConfigLockPassword": null,
  "ServerConfigLockState": "Enabled",
  "ServerConfigLockTamperHalt": "Disabled",
  "ServerConfigLockTransport": "Disabled"
}
```

3. Use a `patch` command to modify the settings.

   For example:

   ```
   {
        "ServerConfigLockPassword": "config_lock_password",
        "ServerConfigLockDisable": "True",
        "ServerConfigLockTamperHalt": "Disabled"
   }
   ```

   Include the `ServerConfigLockTamperHalt` parameter if this feature is enabled.

   Ensure that you select raw and JSON in your REST client. The Server Configuration Lock password is required.

   The REST client notifies you that a reboot is required for the changes to take effect. For example:

   ```
   {
       "error": {
           "code": "iLO.0.10.ExtendedInfo",
           "message": "See @Message.ExtendedInfo for more information.",
           "@Message.ExtendedInfo": [
               {
                   "MessageId": "iLO.2.27.SystemResetRequired"
               }
           ]
       }
   }
   ```

4. Reboot the server.

HPE Trusted Supply Chain

The HPE Trusted Supply Chain provides a first line of defense against cyber attackers with supported servers built to heightened security standards in secured facilities. HPE Trusted Supply Chain combines security, processes, and people to deliver protection for the most sensitive applications and data even before the server is deployed.

- HPE Trusted Supply Chain server configuration—Add this service to supported servers to ensure that your server is built with the highest security standards in a secured facility in the USA.
- HPE Server Security Optimized Service for HPE ProLiant—Add this service to supported servers to ensure that your server is hardened by turning on advanced safeguards against cyber-exploits throughout the server life cycle.

Subtopics

HPE Trusted Supply Chain server configuration
HPE Server Security Optimized Service for HPE ProLiant

HPE Trusted Supply Chain server configuration

Servers with the HPE Trusted Supply Chain configuration ship with the following characteristics:

Country of origin USA

Built in secure Hewlett Packard Enterprise facilities in the USA, with conformance requirements, each server is inspected and verified to be free from malicious microcode and counterfeit parts, safeguarding it against cyber-exploits throughout its life cycle.

Hardened security built in

HPE Trusted Supply Chain hardens the protections designed into select HPE products with unrivaled supply chain visibility and standards compliance providing a 360° view and mitigation plan for current and emerging cyber threats.

Trusted authenticity

HPE Trusted Supply Chain provides protection with HPE employees assigned to the product build to manage the product manufacturing process that adheres to the strictest sourcing, inspection, and traceability standards.

Unique labeling

HPE Trusted Supply Chain products include a **T** in the server model name, for example, HPE ProLiant DL380T. A Trusted Supply Chain sticker is placed on the product hardware.

iLO security state: High Security (iLO 5, iLO 6), Secure Standard (iLO 7)

Configuring iLO to use High Security or Secure Standard mode reduces the attack surface for cyber attackers, making it more difficult to insert compromised code or malware into the server firmware. This security state locks down the host and requires specific authentication through encryption before a user can log into the server.

UEFI Secure Boot feature: Enabled

For customers who ask Hewlett Packard Enterprise to load an OS at the factory, enabling UEFI Secure Boot ensures that each component launched during the boot process is digitally signed. The signature is validated against a set of trusted certificates embedded in the UEFI BIOS. An industry-recognized feature, secure boot ensures that the genuine and authenticated OS is initialized by preventing the loading of unauthenticated BIOS components and OS bootloaders.

If a customer chooses to load the OS on their own, they can configure this feature when the HPE Trusted Supply Chain server is delivered to the end-user location.

HPE Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported HPE Trusted Supply Chain server firmware, hardware components, and options. It creates a digital fingerprint of the server configuration. If any firmware, hardware, or options are altered, an alert is displayed at startup.

Enabling this feature at the factory essentially prevents all tampering or compromise to the server composition, no matter how slight. This feature uses a password, created by Hewlett Packard Enterprise, to lock down the server configuration at the factory. The password is securely transmitted to the customer, who unlocks the server when it arrives.

For customers who need to perform additional configuration steps, perhaps through a reseller or partner, the password can be used to unlock and re-lock the server before it ships to the end-user location.

HPE chassis intrusion detection switch: Enabled

This mechanism protects the HPE Trusted Supply Chain server from physical intrusion. Complementing and reinforcing the protection from the Server Configuration Lock, the chassis intrusion detection switch registers an alert if the top of the server chassis is removed. It logs an event in the iLO firmware, even if the server is powered off. If any cyber attacker or unauthorized personnel open the server chassis, the customer will know that someone might have tampered with the server.

HPE Server Security Optimized Service for HPE ProLiant

Servers with the HPE Server Security Optimized Service for HPE ProLiant option ship with the following characteristics:

iLO security state: High Security (iLO 5, iLO 6), Secure Standard (iLO 7)

Configuring iLO to use High Security or Secure Standard mode reduces the attack surface for cyber attackers, making it more difficult to insert compromised code or malware into the server firmware. This security state locks down the host and

requires specific authentication through encryption before a user can log into the server.

UEFI Secure Boot feature: Enabled

For customers who ask Hewlett Packard Enterprise to load an OS at the factory, enabling UEFI Secure Boot ensures that each component launched during the boot process is digitally signed. The signature is validated against a set of trusted certificates embedded in the UEFI BIOS. An industry-recognized feature, secure boot ensures that the genuine and authenticated OS is initialized by preventing the loading of unauthenticated BIOS components and OS bootloaders.

If a customer chooses to load the OS on their own, they can configure this feature when the HPE Trusted Supply Chain server is delivered to the end-user location.

HPE Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported HPE Trusted Supply Chain server firmware, hardware components, and options. It creates a digital fingerprint of the server configuration. If any firmware, hardware, or options are altered, an alert is displayed at startup.

Enabling this feature at the factory essentially prevents all tampering or compromise to the server composition, no matter how slight. This feature uses a password, created by Hewlett Packard Enterprise, to lock down the server configuration at the factory. The password is securely transmitted to the customer, who unlocks the server when it arrives.

For customers who need to perform additional configuration steps, perhaps through a reseller or partner, the password can be used to unlock and re-lock the server before it ships to the end-user location.

HPE chassis intrusion detection switch: Enabled

If this feature is included in the configuration, it is enabled as part of this service option.

This mechanism protects the HPE Trusted Supply Chain server from physical intrusion. Complementing and reinforcing the protection from the Server Configuration Lock, the chassis intrusion detection switch registers an alert if the top of the server chassis is removed. It logs an event in the iLO firmware, even if the server is powered off. If any cyber attacker or unauthorized personnel open the server chassis, the customer will know that someone might have tampered with the server.

Security resources

Critical product security vulnerability alerts

https://www.hpe.com/info/security-alerts

This website provides detailed information about the latest critical security vulnerability alerts.

Security bulletins

To view the HPE Security Bulletin Library, click **Security Bulletin Library** on the following website: **https://www.hpe.com/support/hpesc**.

To report a security vulnerability, click the **Report a security vulnerability** link on the HPE Security Bulletin Library webpage.

Product alerts

To sign up for email updates, click **Product alerts** and then click **Sign up for Product Alerts** on the following webpage: **https://www.hpe.com/support/hpesc**.

Security overview

- **HPE Security website**
- **360 Degree Security where and when you need it**

Supply chain

- **HPE trusted supply chain expands to worldwide customers**
- **Building Your Organization's Trusted Supply Chain**
- **SiliconANGLE video**
- InfusionPoints report: **How HPE is Leading Supply Chain Security**

Ponemon Institute report

- **The 2025 Global Study on Closing the IT Security Gap**

Moor Insights & Strategy technical paper

Zero Trust - Five Steps For Enterprise IT

HPE and Thales CipherTrust Data Security Platform

HPE servers and storage with Thales CipherTrust Data Security Platform

HPE Compute Ops Management

- **Cloud Security Alliance STAR Registry Listing**
- **HPE Compute Ops Management Security Guide**
- **HPE Compute Ops Management secure gateway** technical paper

Pensando Technology

Distributed Intelligence to the Edge with HPE and Pensando Technology

HPE Resource Library

https://www.hpe.com/us/en/resource-library.html

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support
HPE product registration
Accessing updates
Remote support
Warranty information
Regulatory information
Documentation feedback

Accessing Hewlett Packard Enterprise Support

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

  https://www.hpe.com/info/assistance

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

  https://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

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see **https://www.hpe.com/info/add-products-contracts**.

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

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

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter
- To subscribe to eNewsletters and alerts:

  https://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:

  https://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 Account set up with relevant entitlements.

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 initiates a fast and accurate resolution based on the service level of your product. 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.

HPE Get Connected

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

HPE Tech Care Service

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

HPE Complete Care Service

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

Warranty information

To view the warranty information for your product, see the **warranty check tool**.

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:

https://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:

https://www.hpe.com/info/reach

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

https://www.hpe.com/info/ecodata

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

https://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, use the **Feedback** button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.