Hewlett Packard Enterprise

veeam Ready Appliance Hardened

Solution guide

HPE ProLiant DL380 Gen11 Server

Contents

Recommended configuration

Readers are strongly encouraged to review the following links to configure the HPE ProLiant DL380 Gen11 Server in preparation to be a Veeam Hardened Repository appliance. In addition to these links, relevant screenshots and steps have also been included in this document.

Veeam Backup & Replication on HPE Alletra Storage Server 4120/4140 and HPE ProLiant DL380 Gen11 Server

HPE iLO 6 Security Technology Brief

Expand each section to see screenshots and documentation

How to perform firmware upgrade?

Firmware updates are mandatory for running a Veeam Hardened Repository on an HPE ProLiant DL380 Gen11 Server system. As the update process can change over time, follow the instructions in the HPE Firmware upgrade guide from the vendor.

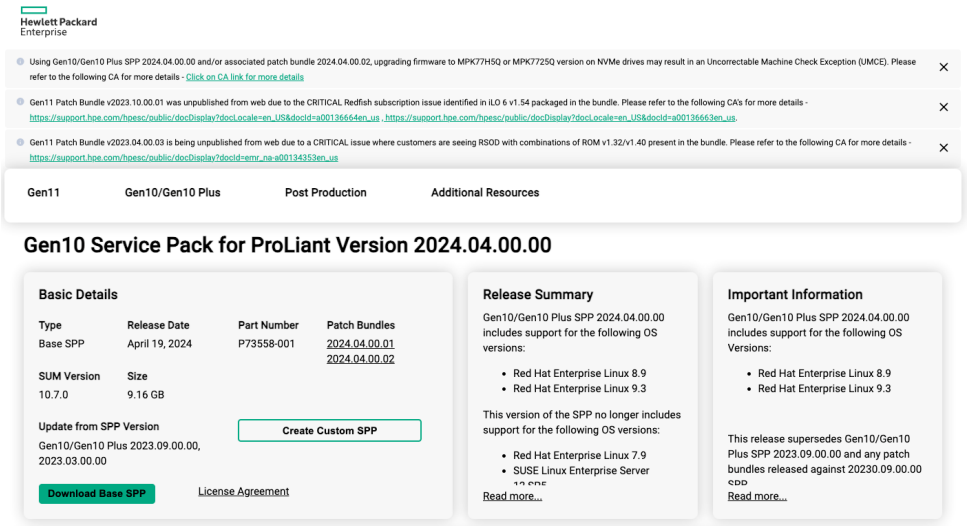
Access the latest release notes with installation instructions

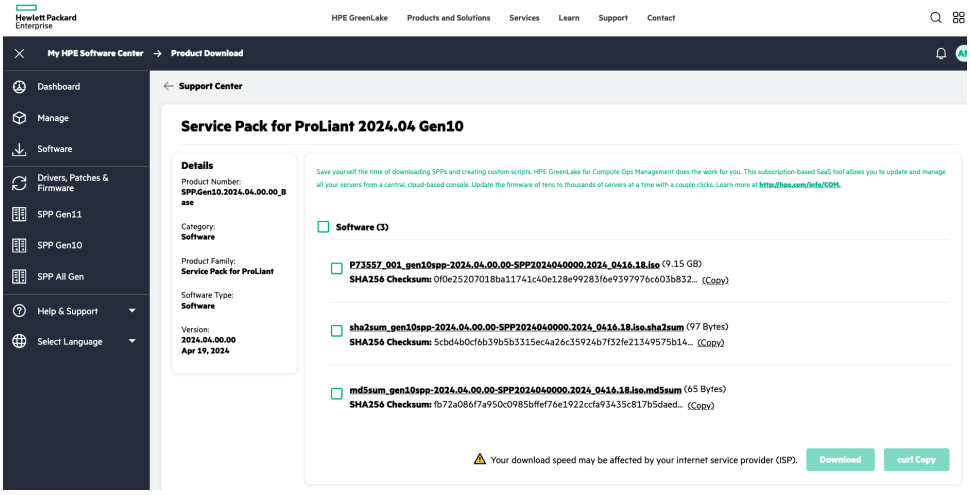
The following steps will update BIOS, firmware, and the HPE iLO management software. To complete this activity, download the most recent SPP, and using the HPE iLO remote console, boot the system directly from the SPP ISO image, select **Automatic Firmware Update**..., and follow the prompts:

1. Download the latest HPE SPP support bundle.

   Be sure to select the specific hardware generation for your hardware. The downloaded file is a bootable ISO.

   Always select the latest support bundle version.

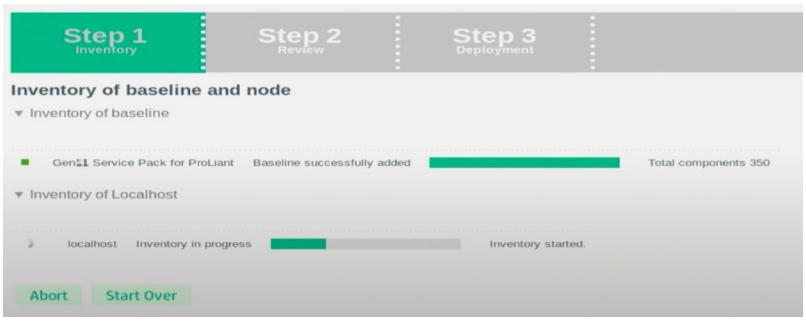




2. Create a bootable USB stick out of the ISO and boot directly on the server or through the remote management (HPE iLO).

An USB stick can be created out of the ISO with the Rufus tool.

3. When the SPP tool is booted, select **Automatic Firmware Update**

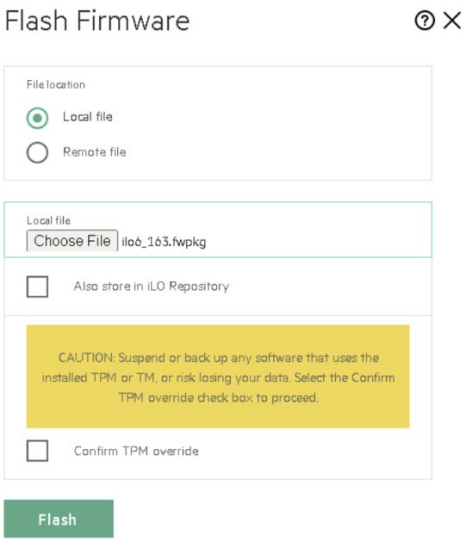


4. Reboot the server

Optional method

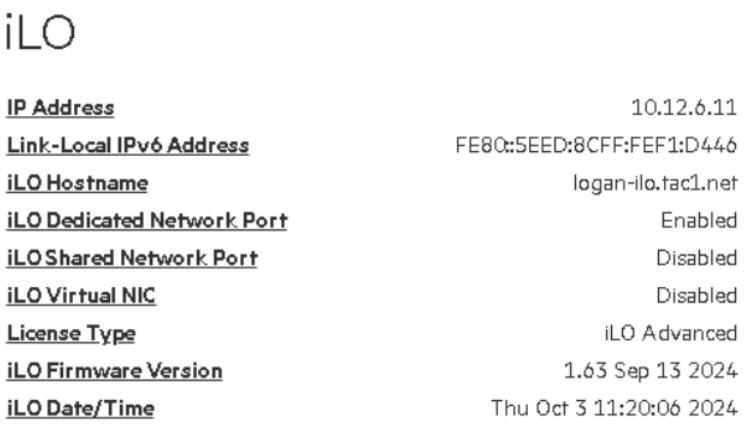
An alternative to booting from the HPE ProLiant Support Pack would be updating firmware through the HPE iLO. In this case, you would download the latest HPE iLO 6 package, click **Firmware & OS Software** in the HPE iLO 6 home page, and follow the prompts to update firmware:

1. Download the latest HPE iLO 6 package from support.hpe.com
2. Click **Firmware & OS Software** in the HPE iLO 6 home page. There, you will see an **Update Firmware** option to click.
3. Choose your local file you just downloaded, check the box next to **Confirm TPM override**, and click **Flash**.



4. You will see a progress bar tick up to 100% a couple of times, and then the HPE iLO will restart. The restart may take a few minutes, so don't be alarmed if you lose connection with the HPE iLO. The page should return on its own.

5. Once the HPE iLO returns, verify the new HPE iLO version in **Information** on the HPE iLO home page.



RAID controller configuration

Operating system boot devices

- **RAID card description:** This is HPE NS204i-u Gen11 NVMe Hot Plug Optimized Storage Device, which is the dedicated and preconfigured hardware RAID 1 OS boot device. It includes two HPE enterprise-class 480 GB NVMe M.2 SSDs on a single HPE Synergy add-in card. It auto-creates a RAID 1 volume during boot and therefore does not require configuration. Boot devices enable the deployed OS to be mirrored through a dedicated hardware RAID 1.

Backup storage drives

- **Cache policy:** 8 GB flash-backed write cache (10% read / 90% write)
- **Strip size used:** 256K
- **Data protection method:** RAID 6 (13+2, 1 hot spare)

Considerations for LUN configuration

- Default initialization method—Full. Use this method, otherwise, the initialization will complete slowly and in background, impacting performance for days.
- Assign only 10% of the controller cache to read.
- **Number of logical volumes**

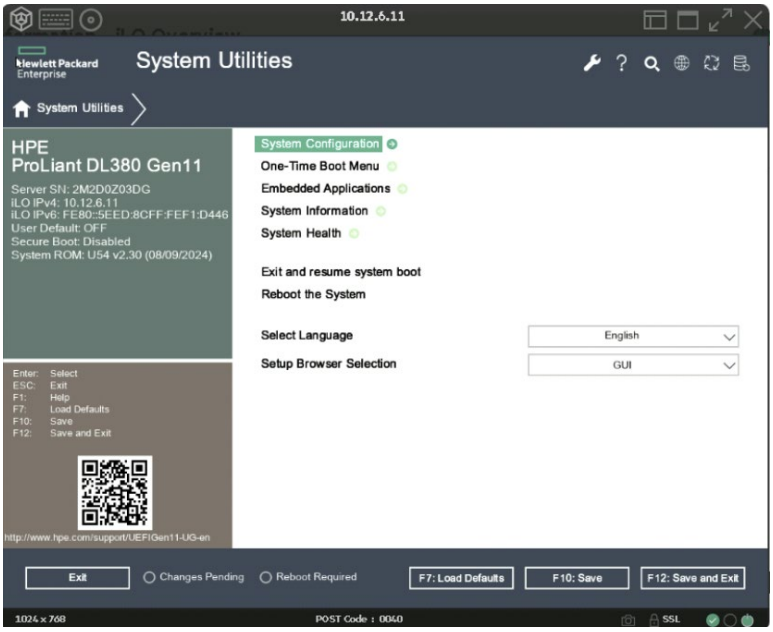
  If you have a dedicated boot device, such as the HPE NS204i-u Gen11 NVMe Hot Plug Boot Optimized Storage Device, Hewlett Packard Enterprise recommends using the entire array capacity for a single logical volume.

  If, instead, you plan to boot from this array, HPE recommends creating two volumes: a smaller ~250 GB one to be used as a boot volume and a second larger volume with all the remaining capacity to be used by the Veeam backup repositories.

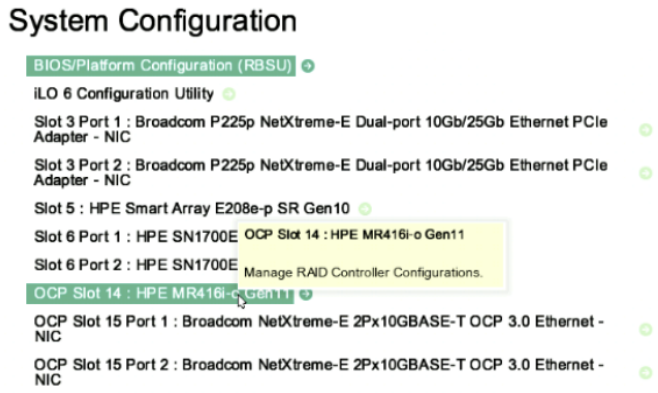
Backup storage drive configuration

Create one RAID 6 volume consisting of 15 drives plus 1 hot spare. This will be a total of 16 data drives. The RAID 6 volume is entirely managed by a single HPE MR416i-p smart array controller card in the HPE ProLiant DL380 Gen11 Server and is thus offloaded from the OS.

Press **F9** on boot to enter System Utilities, and then choose **System Configuration**



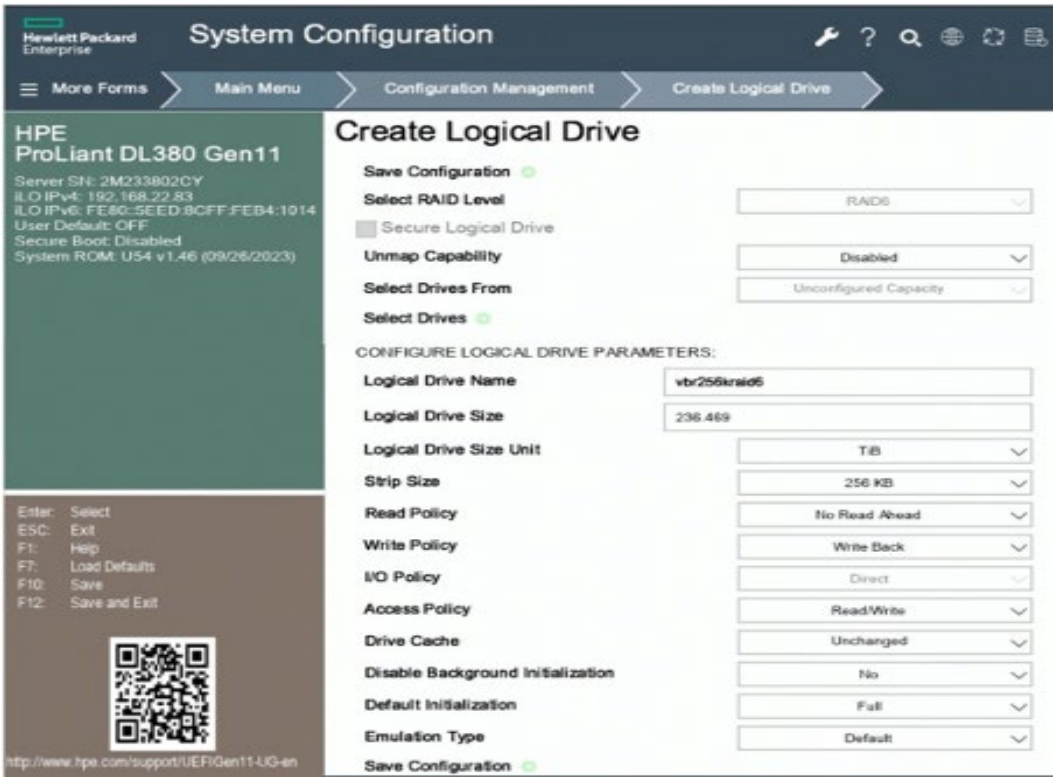
Choose the **MR RAID** card



On the next screen, choose **Configure** in the **ACTIONS** section

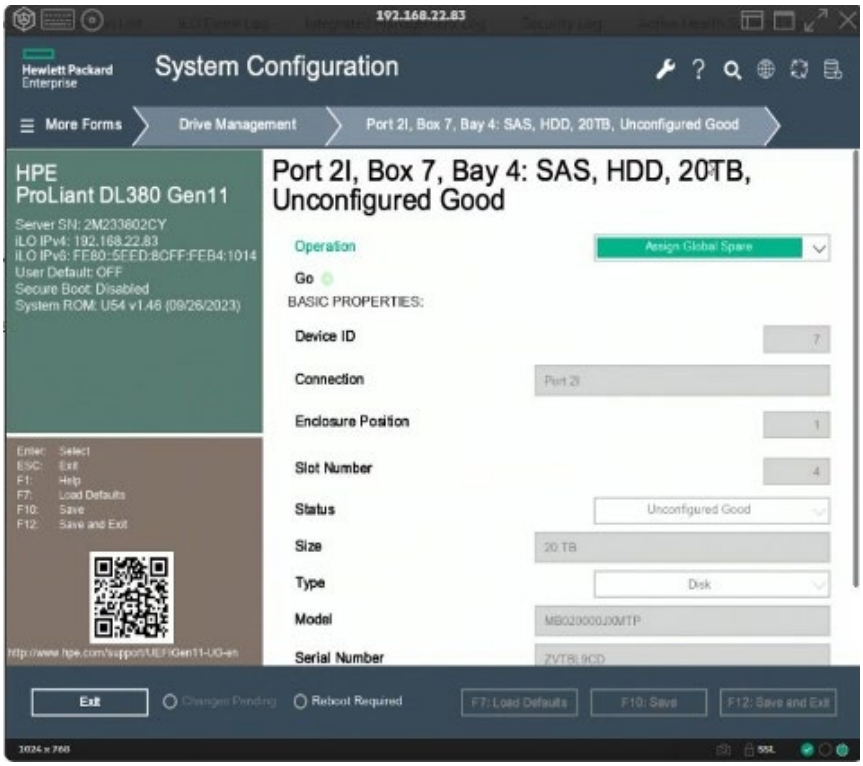
Choose **Create Logical Drive**

Create the logical drive by choosing the various options and click **Save Configuration**.

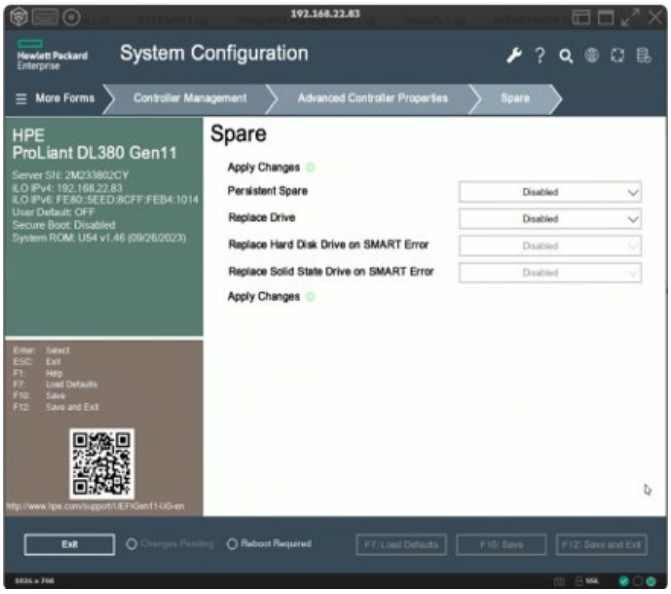


Configuration of spare disks on HPE ProLiant DL380 Gen11 Server

The HPE MR416i-p Gen11 Storage Controller used on the HPE ProLiant DL380 Gen11 Server provides two options for configuring the spare drives: Dedicated spare and global spare. A dedicated spare is dedicated to one array with a specific RAID configuration and a global spare replaces a failed drive in any type of RAID array. **To assign a drive as a global spare, from the UEFI System Utilities of the server, select System Configuration → HPE MR416 Gen11 → Main Menu → Drive Management**. In **Drive Management**, select a drive of your choice, and in the drive screen, select **Assign Global Spare Drive** from the **Operation** drop-down list.

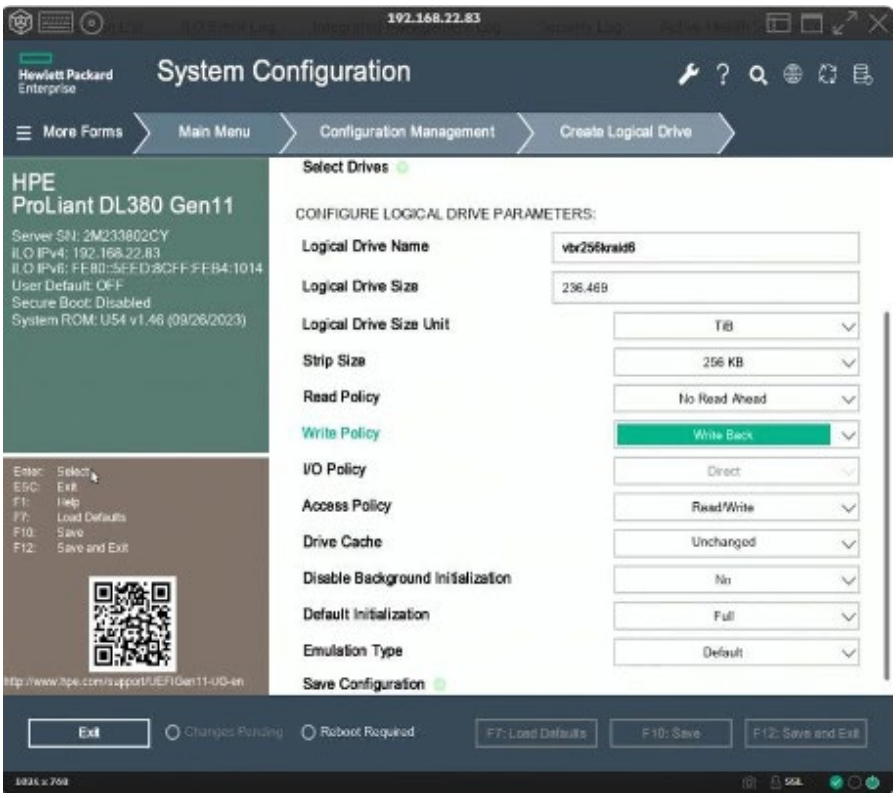


By default, the HPE MR416i-p Storage Controller allocates the configured spare drive as a persistent spare, which means that replacing a spare drive in the same slot will automatically configure the new drive as spare. Also, the **Replace Drive** option that allows copying all the data from a spare drive to a data drive is enabled. Both these options need to be disabled to avoid overhead on the system during the data copy process and enable any replacement drive to be configured as a spare drive. To perform these settings, launch **System Utilities System Configuration → HPE MR416 Gen11 → Main Menu → Controller Management → Advanced Controller Properties → Spare**.



Configuration of smart array internal cache on HPE ProLiant DL380 Gen11 Server

The HPE MR416i-p Gen11 Controller used on the HPE ProLiant DL380 Gen11 Server is built with 8 GB of persistent cache. The cache read/write policy for the backup repository volume can be selected during the creation of the logical drive. The **Write Policy** should be set to **Write Back**. In this mode, the controller sends a data transfer completion signal to the host when the controller cache has received all the data in a transaction. This option provides a good balance between data protection and performance as the controller switches between write back and write through depending on the controller status. The **Read Policy** is set to No Read Ahead (default option).

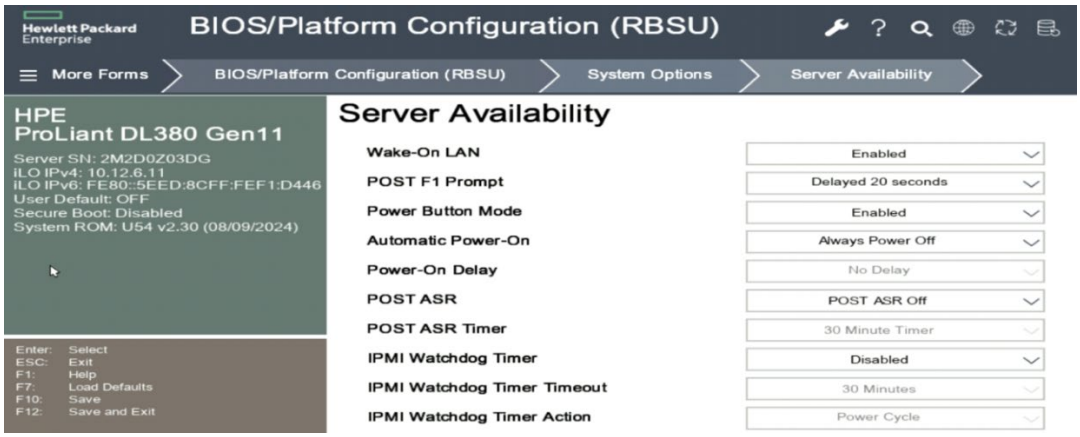


BIOS UEFI settings

Step-by-step installation instructions

1. From the HPE iLO interface, click **Administration**
2. Click the **Boot Order** tab
3. Scroll to the bottom, then click the **Boot to System Setup Utilities** button
4. Power on or restart the server
5. Disable USB support
   a. Select **System Configuration**
   b. Select **BIOS/Platform Configuration** (RBSU)
   c. Select **System Options**
   d. Select **USB Options**
   e. Select **USB Boot Support**

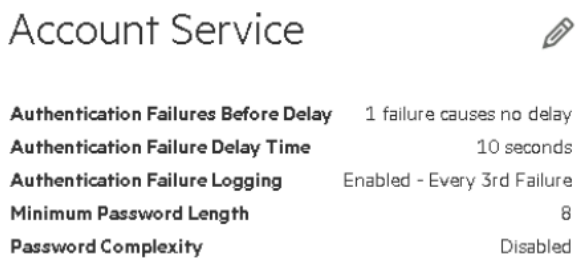
   f. Select **Disabled** to disable USB Boot Support
   g. Press **F10** to save your options and then click the **System Options** menu
6. Set Power Button Mode to **Always Power On**
   a. Back in the **System Options** menu, select **Server Availability**. If you were navigating to this from the **System Utilities** main menu after pressing F9 during POST, the path would be **BIOS/Platform Configuration-->System Options-->Server Availability**
   b. Select **Automatic Power-On** and set it to **Always Power On**
   c. Select **POST ASR** and set it to **POST ASR On**
   d. Press **F10** to save and then click the **Main Menu**



7. Configure password complexity
   a. **Security-->Access Settings-->Account Service**

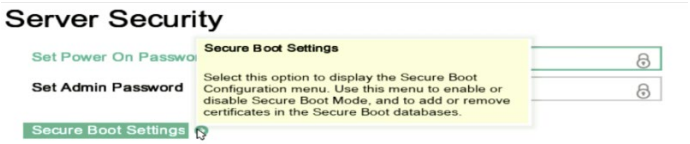
      You can set these features to your requirements. Enabling password complexity enforces the following on passwords:

   b. At least one uppercase ASCII character
   c. At least one lowercase ASCII character
   d. At least one ASCII digit
   e. At least one other type of character (for example, a symbol, a special character, or a punctuation)

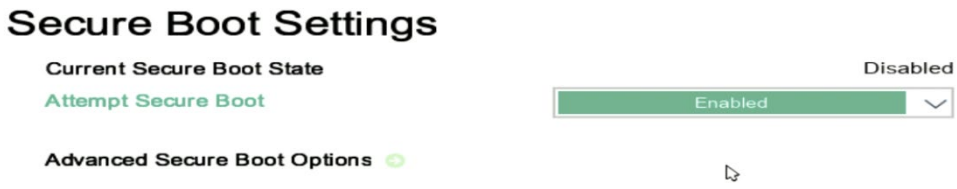


8. Enable Secure Boot, power on password, and admin password
   a. Select **Server Security**. If you were navigating to this from the **System Utilities** main menu after pressing F9 during POST, the path would be **System Configuration**-->**BIOS/Platform Configuration**-->**Server Security**

      In this same screen, you'll be able to set a power on password, an admin password, and enable Secure Boot.



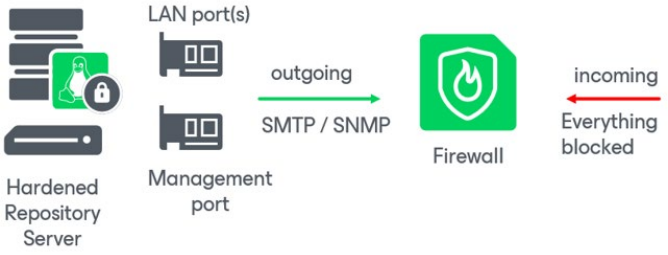
   b. Select **Secure Boot Settings**
   c. Select **Attempt Secure Boot**
   d. A notice will be displayed that a reboot is required. Press the **Enter** keyboard button to continue



   e. Press **F10** to save your configuration and then click the **Server Security** menu
   f. Press the **F12** keyboard button to save and exit.

How to configure HPE iLO remote access?

As HPE iLO remote access and additional management port (Intel®/BMC/. . .) are an attack vector for a ransomware hacker to destroy data on the disk systems of the server, it is recommended to shield the system with firewall or switch port access rules that allow only SMTP/SNMP management to the management system and deactivate any incoming message. If possible, implement hardware management on a completely different infrastructure that does not have any network interaction capability with production. Another option is to disconnect the management ports and monitor the systems manually in the data center.



We also recommend to follow the HPE best practices for HPE iLO hardening:

Threat to be defeated

ISO boot attack is a type of attack frequently attempted by cybercriminals. Be informed, stay protected!

Solutions

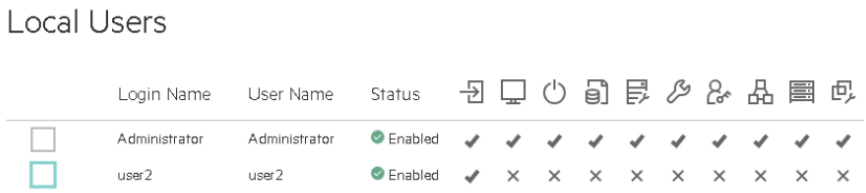
Enable as many of the following security features to protect access to the HPE iLO, even if you disable access. Someone by accident could connect the interface and you need to stay protected.

- Enable Kerberos and multifactor authentication (MFA)
- Enable Smartcard authentication
- Power-on password
- Enable firewall / access port switch rules to let only SMTP/SNMP out and do not let any communication in including management and WebUI (see the previous screenshot).
- Disconnect HPE iLO physically

More details from HPE for security settings: HPE iLO 5 Security Technology Brief and HPE Gen10 and Gen10 Plus Security Reference Guide

Restrict HPE iLO user access

The HPE iLO does have an option to restrict user access. A user could be created with read-only access by going to **Administration-->User Administration** after logging into the HPE iLO. In the image, you'll see that a **user2** was created with only login access.



This user will be able to view all HPE iLO settings, but the user will not be able to launch a remote console, make any configuration changes, or take any disruptive or destructive actions such as power cycling the server or booting from an ISO.

Contact

Web: support.hpe.com

Learn more at

HPE.com/us/en/alliance/Veeam

Chat now (sales)

a50011632ENW

Hewlett Packard Enterprise