



UEFI Menu

Table of contents

Accessing the UEFI Menu

Front Page

Device Manager

Secure Boot Configuration

Network Device List

System Configuration

RAM Disk Configuration

iSCSI Configuration

Tls Auth Configuration

Unified Extensible Firmware Interface (UEFI) is low-level firmware that is part of the NVIDIA® BlueField® bootloader stack. UEFI acts as an interface between the BlueField's Arm-trusted firmware (ATF) bootloader and the OS.

Info

The UEFI specification is available at [UEFI.org](https://uefi.org).

UEFI provides a menu which supports certain configuration options. This section lists and describes configurations supported from the UEFI Device Manager menu.

Info

For more complete information beyond the Device Manager menu option, please refer to the [NVIDIA Networking Server-Side Documentation of Flexboot & UEFI > User Manual > User Interface > HII \(UEFI\) System Settings Configuration Options](#).

Info

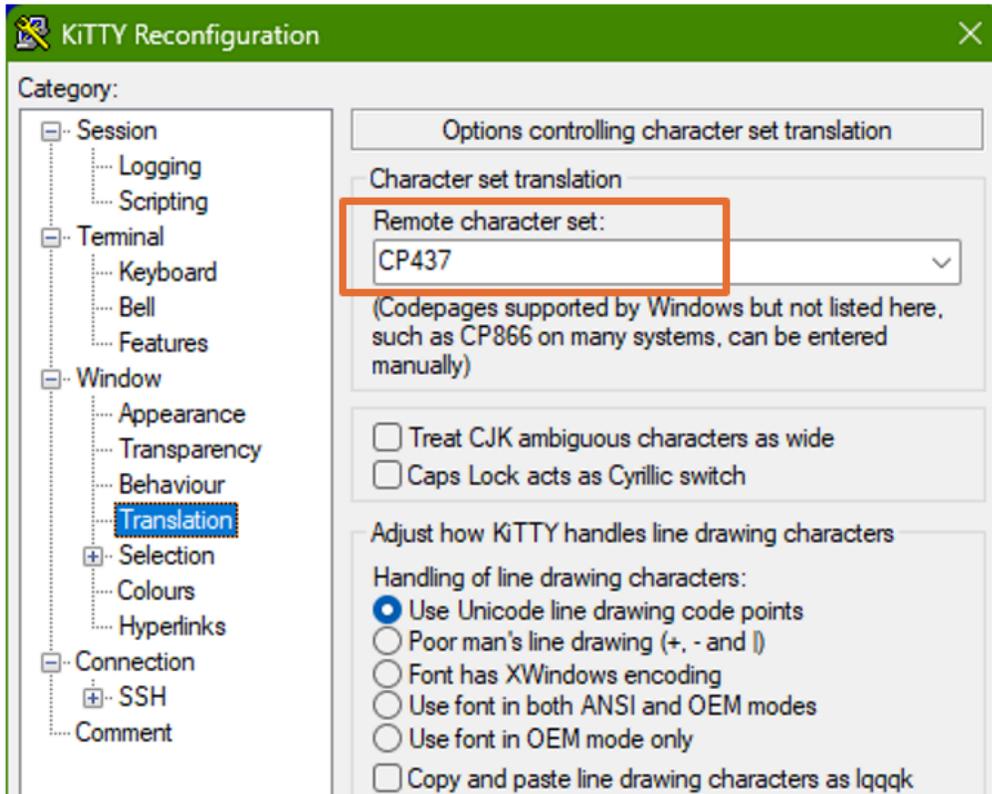
Most of these menu items are also configurable via [Redfish](#) (when enabled).

Accessing the UEFI Menu

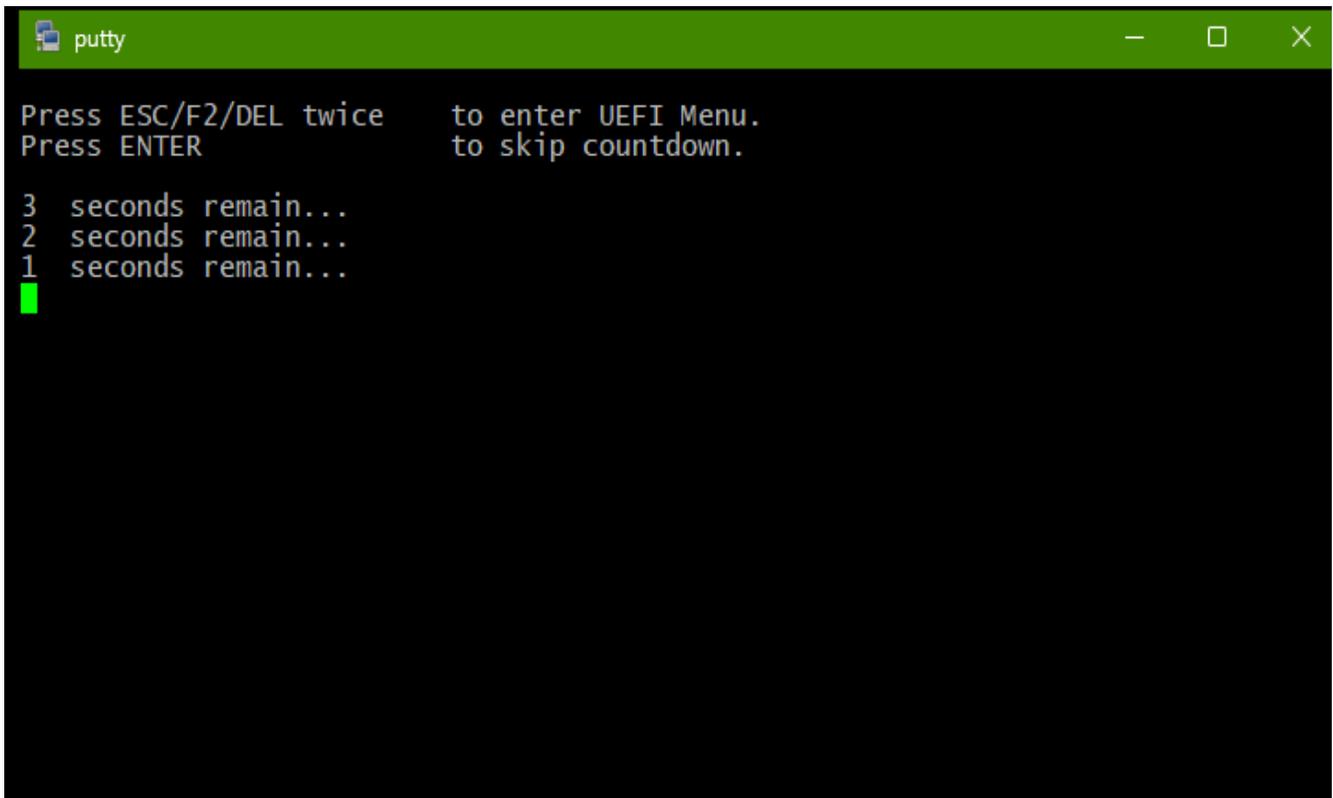
To access the UEFI menu, users must have a connection to the BlueField console either through a UART serial port or the virtual RShim console device. The console should be configured to 115200 8N1. The UEFI's UI window size is 80 columns and 25 rows. Configure your terminal size accordingly.

UEFI's UI uses a legacy character encoding, CP437 (code page 437), to ensure most compatibility. Configure your terminal to use this code page to show the table borders properly.

The following is an example for how to configure this properly in putty:



To enter the UEFI menu, hit the Esc key twice when prompted during the normal boot sequence:

A screenshot of a Putty terminal window with a green title bar. The terminal text reads: "Press ESC/F2/DEL twice to enter UEFI Menu. Press ENTER to skip countdown." followed by a 3-second countdown: "3 seconds remain...", "2 seconds remain...", "1 seconds remain...". A green cursor is visible on the line "1 seconds remain...".

```
putty
Press ESC/F2/DEL twice to enter UEFI Menu.
Press ENTER to skip countdown.
3 seconds remain...
2 seconds remain...
1 seconds remain...
█
```

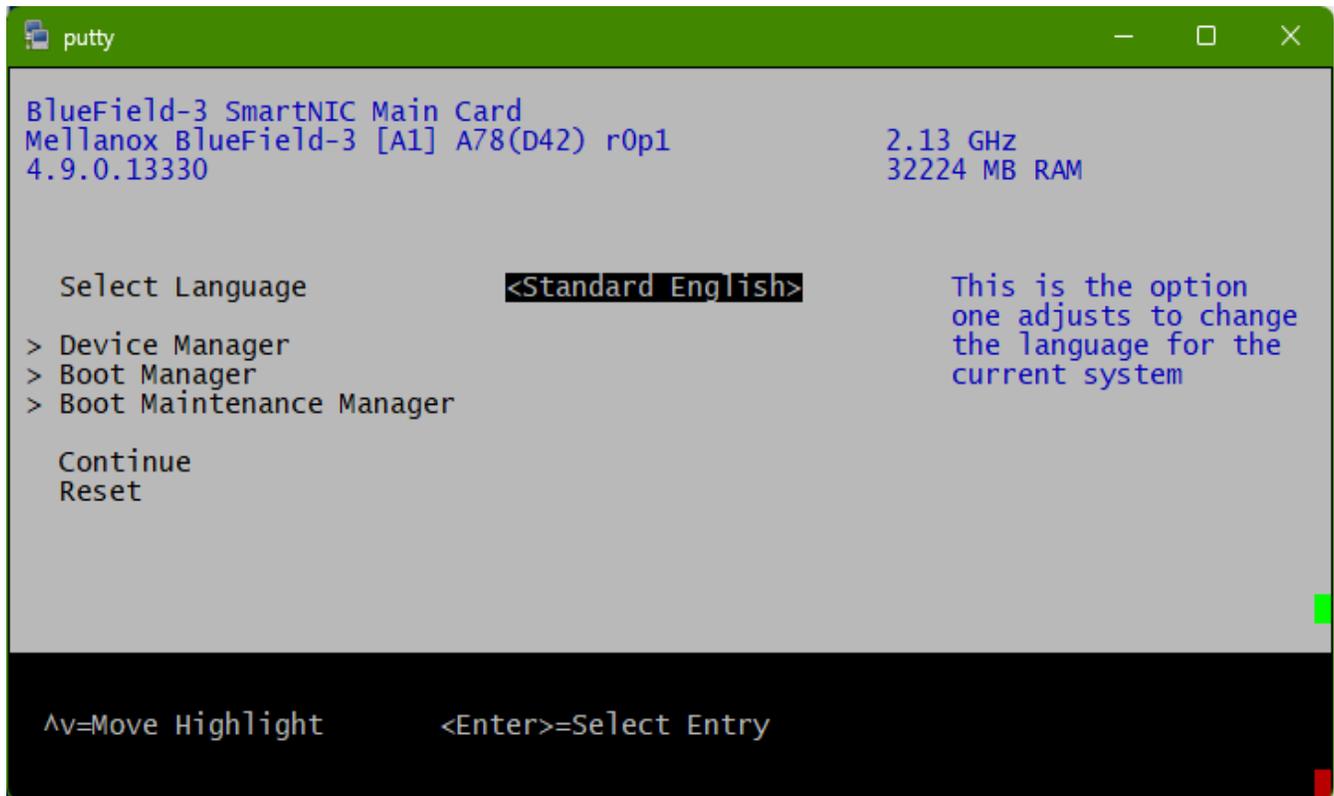
Note

All BlueField platforms ship with a default UEFI menu password, `bluefield`. If the password is set to `bluefield` when you enter the UEFI menu, users are prompted to change it.

Tip

NVIDIA strongly recommends all DPUs have their UEFI password set to a non-default value. This can be done using the UEFI menu or Redfish.

Front Page

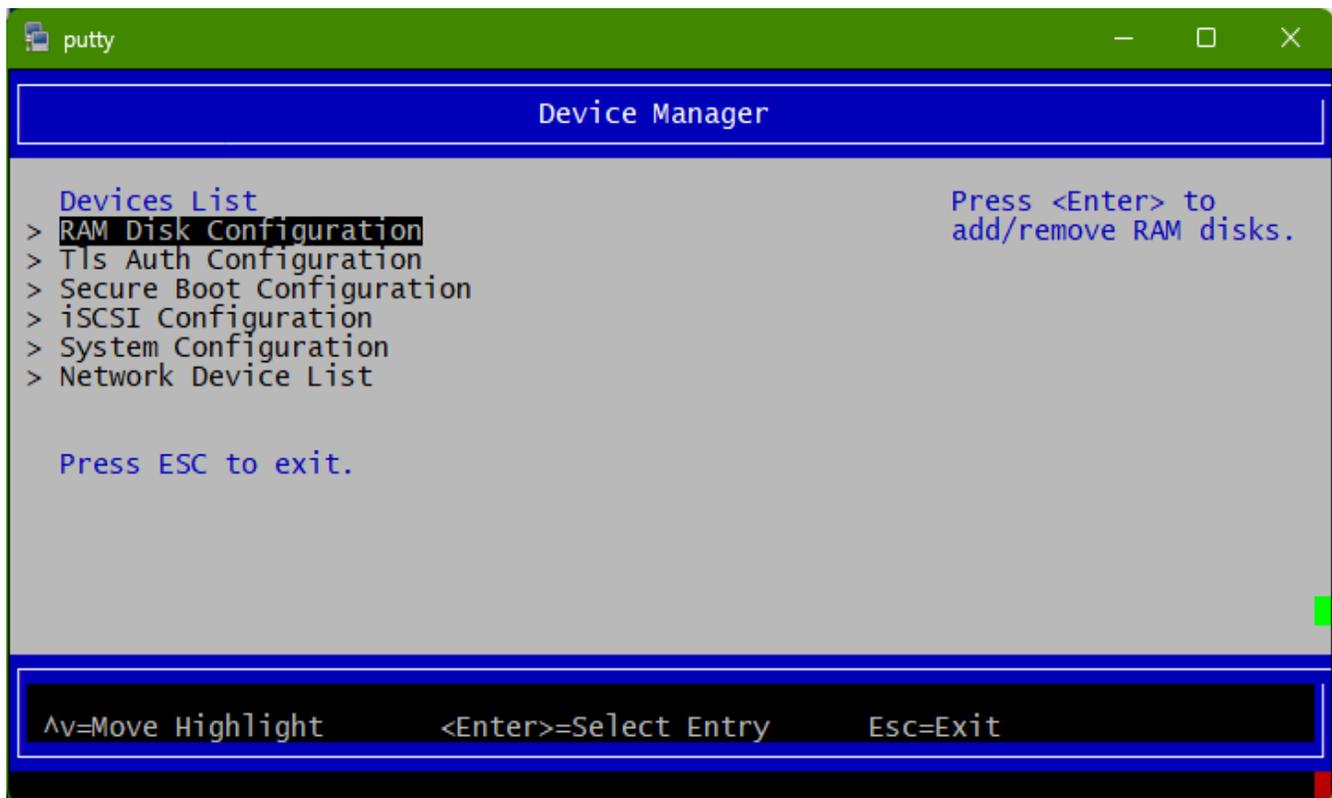


There are three main menu items in the front page:

- Device Manager
- Boot Manager
- Boot Maintenance Manager

The rest of this page focuses on Device Manager.

Device Manager

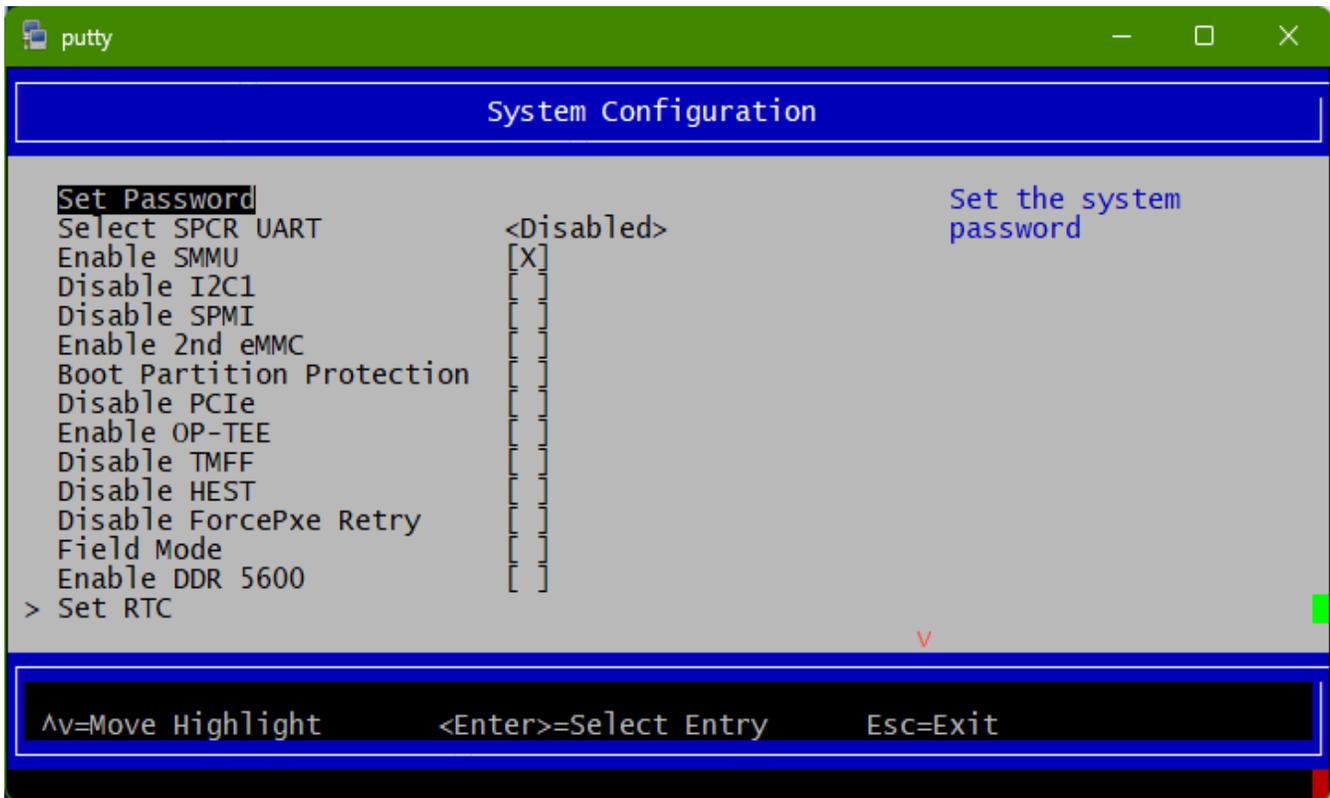


System Configuration

Lists different system configuration options.

Note

Some configuration options may require a system reset to take effect.



i Info

To change the configuration of any of these BIOS attributes using Redfish, refer to section "[Changing BIOS Attributes Value](#)" in the BMC Software User Manual.

Menu Option	Description
Set Password	Set the system password. Set the UEFI password. All BlueField Platforms ship with a default UEFI menu password, <code>bluefield</code> . If the password is set to <code>bluefield</code> when you enter the UEFI menu, users are prompted to change it. <p style="text-align: center;">Tip</p>

Menu Option	Description
	<p>NVIDIA strongly recommends all DPUs have their UEFI password set to a non-default value. This can be done using the UEFI menu or Redfish.</p>
<p>Select SPCR UART</p>	<p>Choose UART for serial port console redirection [<Disabled> <UART Port 0> <UART Port 1>].</p> <p>Users may set the SPCR table (ACPI) to point to UART0, UART1, or disable the feature. The OS can reference this table to steer serial output. For example, Linux uses this table for its earlycon feature.</p> <div data-bbox="402 730 1463 993" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to its default if you are not certain how to configure it, or you may destabilize your system.</p> </div>
<p>Enable SMMU</p>	<p>Enable/disable the SMMU. BlueField Platforms have an integrated SMMU on the SoC. Users may enable or disable this unit. Enabling it can make the system more secure but, with certain network flows, the enabled SMMU could cause performance issues.</p> <div data-bbox="402 1335 1463 1556" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to its default if you do not certain how to configure it.</p> </div>
<p>Disable SPMI</p>	<p>Enable/disable ACPI server platform management interface table. Allows users to enable/disable the ACPI SPMI table. This table instructs the OS on what interface/device to use for the IPMI SSIF.</p> <div data-bbox="402 1812 1463 1944" style="background-color: #f8d7da; padding: 10px;"> <p> Warning</p> </div>

Menu Option	Description
	<p>Leave this attribute to its default if you do not certain how to configure it.</p>
<p>Enable 2nd eMMC</p>	<p>Enable/disable the second eMMC. Some legacy BlueField systems have 2 eMMC devices. This feature has been discontinued.</p> <div data-bbox="402 604 1463 863" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to its default (disabled) if you do not certain how to configure it, or your system will not boot correctly.</p> </div>
<p>Boot Partition Protection</p>	<p>Enable/disable the eMMC boot partition protection. Takes effect after reboot. There are 2 logical "boot partitions" on the eMMC device used to store ATF/UEFI code. These are referred to as the primary/secondary boot partitions. Users can write-protect these partitions using this attribute.</p> <div data-bbox="402 1203 1463 1623" style="background-color: #fff3cd; padding: 10px;"> <p> Info These are separate devices from the flash storage used by the OS (for file systems). They do not contain file systems and are only used for storing binary boot code on raw flash. Do not confuse an eMMC boot partition with an EFI System Partition (ESP) used to store boot loaders and OS images on a FAT32 file system.</p> </div> <div data-bbox="402 1686 1463 1902" style="background-color: #fff3cd; padding: 10px;"> <p> Info If secure boot is enabled, these partitions are write-protected by default.</p> </div>

Menu Option	Description
	<p> Note This menu option is not currently supported for BlueField-3.</p>
Disable PCIe	<p>Enable/disable PCIe root complex. Normally, UEFI enumerates the PCIe bus during the boot process and reports this information to the OS via the ACPI SSDT table. If this attribute is disabled, UEFI does not populate the SSDT with the PCIe root complex information, so the OS does not have visibility to devices on the PCIe bus.</p> <p> Note This attribute is used for diagnostic purposes and should not be modified.</p>
Enable OP-TEE	<p>Enable/disable support for trusted execution environment.</p> <p> Warning Do not enable this feature. More information will be provided in future releases.</p>

Menu Option	Description
Disable TMFF	<p>Enable/disable the BlueField-specific ACPI TMFIFO table. This can be used by some OSes to perform console/debugging over the BlueField TMFIFO interface. It can override the SPCR table.</p> <div data-bbox="402 401 1463 621" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to its default if you are not certain how to configure it.</p> </div>
Disable HEST	<p>Disable OS error handling via HEST (hardware error source table). HEST is a mechanism for reporting hardware errors (e.g., CPU errors, memory errors, PCIe errors) to the OS. By default, this option is disabled (i.e., HEST is enabled) so the OS can handle hardware errors more gracefully by either logging them or taking corrective action. When this option is checked and HEST is disabled, the BIOS (ATF/UEFI) is immediately involved when hardware errors happen, potentially preventing undesired error propagation.</p> <div data-bbox="402 1121 1463 1299" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to default if you are not certain.</p> </div>
Disable ForcePxe Retry	<p>If enabled, PXE boot option entries are attempted only once instead of retrying them in a loop when "ForcePxe" is requested via IPMI interface</p>
Field Mode	<p>Disable/enable NIC BMC field mode. Allows users to enable/disable NIC BMC field mode. When the NIC BMC has field mode enabled, most of its functionality is disabled (beyond the serial console). The BlueField Platform's OOB interface will also not be functional if field mode is enabled.</p> <div data-bbox="402 1782 1463 1944" style="background-color: #f8d7da; padding: 10px;"> <p> Warning Leave this attribute to its default unless you are certain you wish to enable field mode on the NIC</p> </div>

Menu Option	Description
	<p>BMC. Consult the DPU BMC user manual for more information on field mode.</p>
Set RTC	<p>Allows users to set the time and date for the real-time clock.</p>
BlueField Modes	<ul style="list-style-type: none"> • Internal CPU Model: [<Separated> <Embedded>] • Host Privilege Level: [<Restricted> <Privileged>] • NIC Mode – sets the BlueField to operate in either NIC mode or DPU mode <div style="background-color: #ffffcc; padding: 10px; margin-top: 10px;"> <p>Note Any change to this attribute requires device reset to take effect.</p> </div>
Redfish Configuration	<p>Enable/disable Redfish support. If UEFI is unable to discover a Redfish server, it reverts to using the defined UEFI boot options (i.e., the "normal" UEFI boot sequence). Disabling Redfish helps improve boot time as the Redfish server discovery process is skipped.</p> <p>Disabling Redfish in the UEFI menu disables the Redfish client in UEFI. However, users can still interact with BMC Redfish server. Any request sent to the BMC Redfish server when the UEFI Redfish client is disabled would be cached by the BMC server until the UEFI Redfish client is re-enabled to process the pending requests.</p> <p>BMC Redfish server clears the pending cached request if BMC is factory reset or power cycled.</p> <p>The <code>RTCSync</code> option syncs RTC time with Redfish time under the Manager schema.</p>
Password Settings	<ul style="list-style-type: none"> • Default Password Policy – mandates the password being set adheres to the new policy of 12 characters minimum and 64 characters maximum. The last 5 passwords cannot be reused. • Set Legacy Password – set password with legacy password policy to accommodate a UEFI firmware downgrade. The new password policy (default) is not compatible with older versions of UEFI firmware.

Menu Option	Description
Reset EFI Variables	<p>This action clears all EFI variables to factory default state. Reset the device to take effect.</p> <div data-bbox="402 359 1463 699" style="background-color: #f0d0d0; padding: 10px;"> <p> Warning Only reset the EFI variable store under the advice of NVIDIA Enterprise Support. Resetting the EFI variable store deletes all UEFI variables including the boot options and the system may not boot without setting new boot options.</p> </div>
EmmcWipe	<p>Clears the eMMC disk. The action is immutable and all data on eMMC is lost after it is performed.</p> <div data-bbox="402 919 1463 1102" style="background-color: #ffffcc; padding: 10px;"> <p> Info This action is logged in the RShim log.</p> </div>
NvmeWipe	<p>Clears the NVMe SSD. This action is immutable and all data on NVMe SSD is lost after it is performed.</p> <div data-bbox="402 1318 1463 1501" style="background-color: #ffffcc; padding: 10px;"> <p> Info This action is logged in the RShim log.</p> </div>

Menu Option	Description														
Large ICMC size	<p>Set the large ICMC size in hex and MB. Valid value: 0-100000h in 80h increments.</p> <div data-bbox="402 359 1463 579" style="background-color: #ffffcc; padding: 10px;"> <p>i Info This menu option is only relevant for BlueField-3 platforms.</p> </div>														
Enable DDR 5600	<p>Enable/disable DDR max speed of 5600 MT/s.</p> <div data-bbox="402 762 1463 1182" style="background-color: #ffffcc; padding: 10px;"> <p>i Info This menu option is only relevant for B3220 BlueField-3 devices which have a default speed of 5200 MT/s. This speed can be increased to 5600 MT/s provided the hardware can support it, which is indicated via the fuse bits. Other BlueField SKUs are automatically fixed at 5600 MT/s irrespective of this setting and cannot be reduced to 5200 MT/s.</p> </div>														
L3 Cache Partition	<p>Set the L3 cache partition level to allocate part of the L3 cache for the NIC and others for the BlueField-3 Arm core. The customer-selectable L3 cache partition to be allocated for the NIC can be selected from the following percentage levels:</p> <table border="1" data-bbox="402 1461 1130 1892"> <thead> <tr> <th>L3 Cache Level #</th> <th>L3 Cache Percentage for NIC</th> </tr> </thead> <tbody> <tr> <td>0 (default)</td> <td>0% (default)</td> </tr> <tr> <td>1</td> <td>12.5%</td> </tr> <tr> <td>2</td> <td>25%</td> </tr> <tr> <td>3</td> <td>37.5%</td> </tr> <tr> <td>4</td> <td>50%</td> </tr> <tr> <td>5</td> <td>62.5%</td> </tr> </tbody> </table>	L3 Cache Level #	L3 Cache Percentage for NIC	0 (default)	0% (default)	1	12.5%	2	25%	3	37.5%	4	50%	5	62.5%
L3 Cache Level #	L3 Cache Percentage for NIC														
0 (default)	0% (default)														
1	12.5%														
2	25%														
3	37.5%														
4	50%														
5	62.5%														

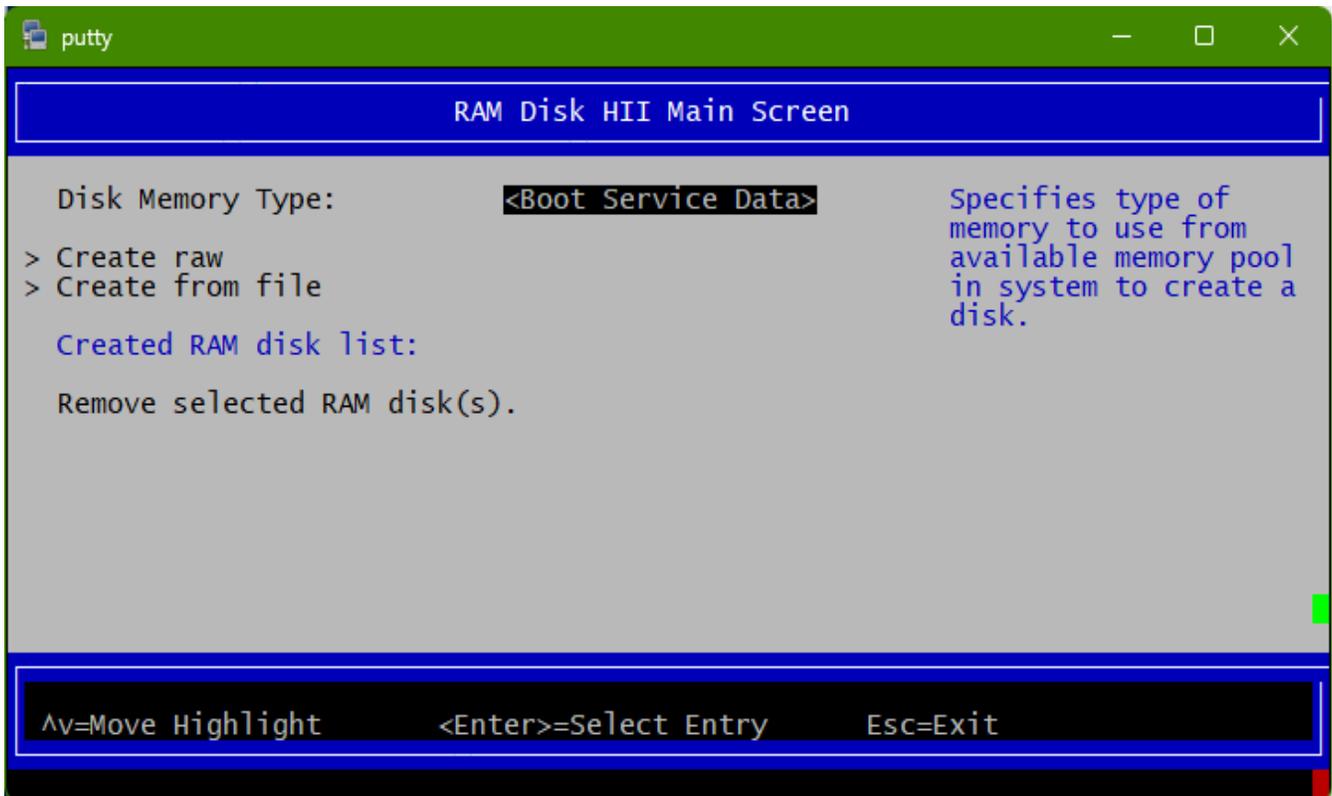
Menu Option	Description	
	L3 Cache Level #	L3 Cache Percentage for NIC
	6	75%
	7	87.5%
	 Warning Do not enable this feature. More information will be provided in future software releases.	

Secure Boot Configuration

Please refer to section "[Arm OS Secure Boot \(Configured from UEFI\)](#)" for more information.

RAM Disk Configuration

Provides option to create/delete RAM disks.

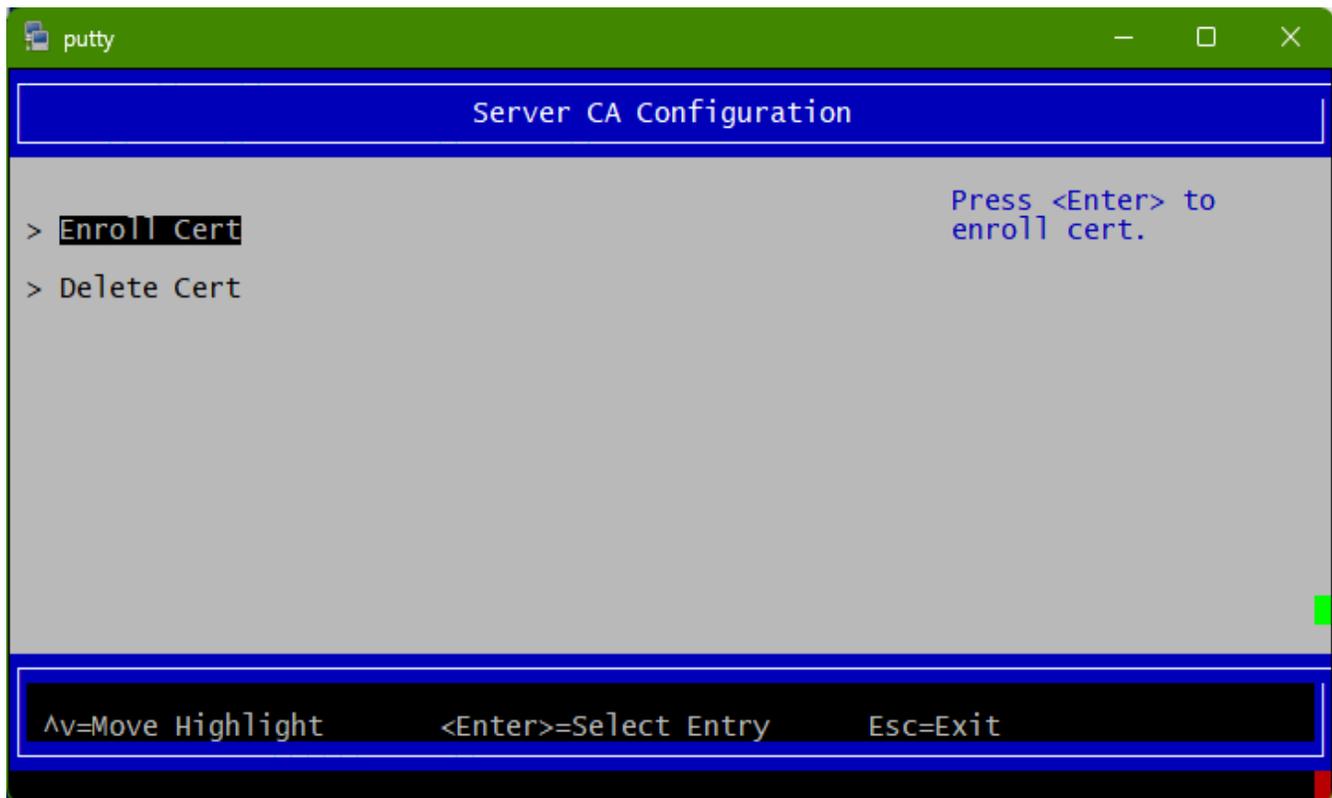
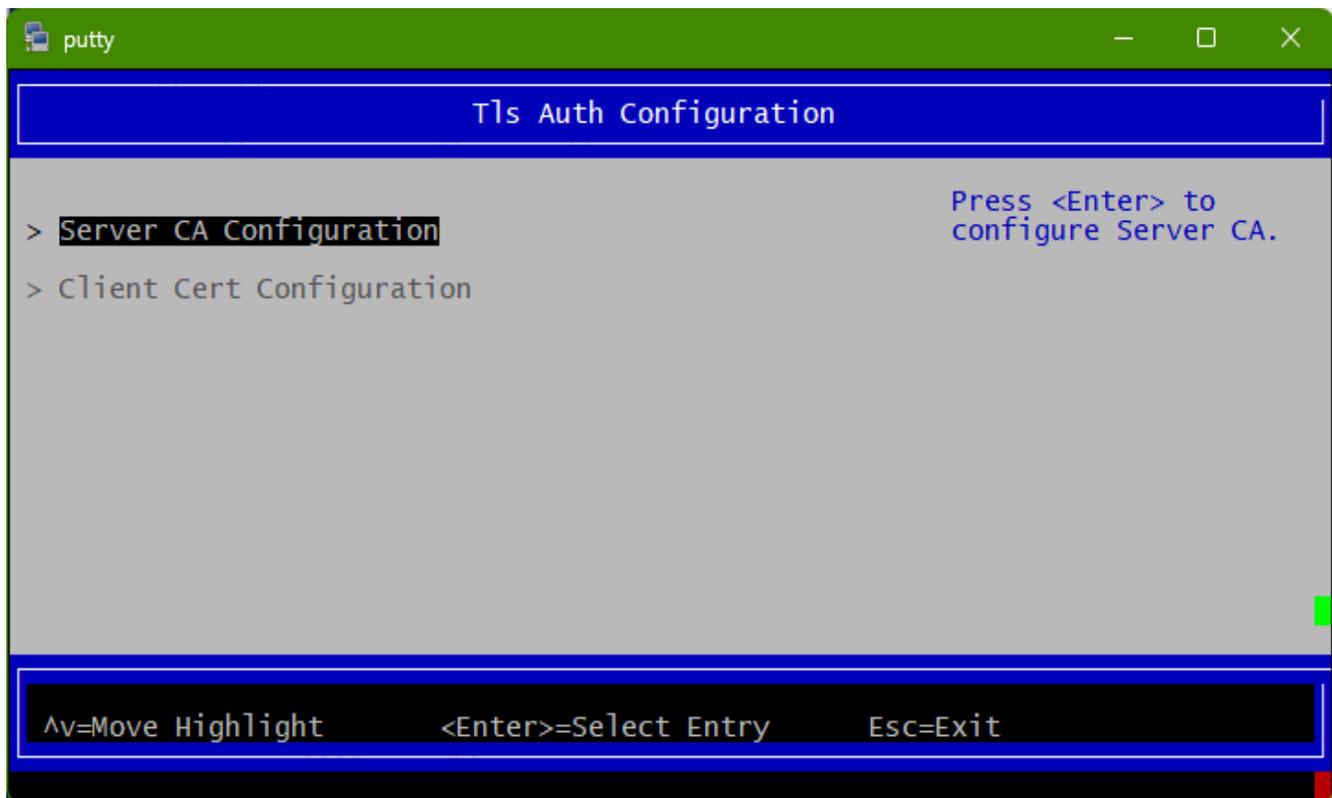


Tls Auth Configuration

Provides configuration (enroll/delete) of TLS auth certificates for HTTPS traffic in UEFI.

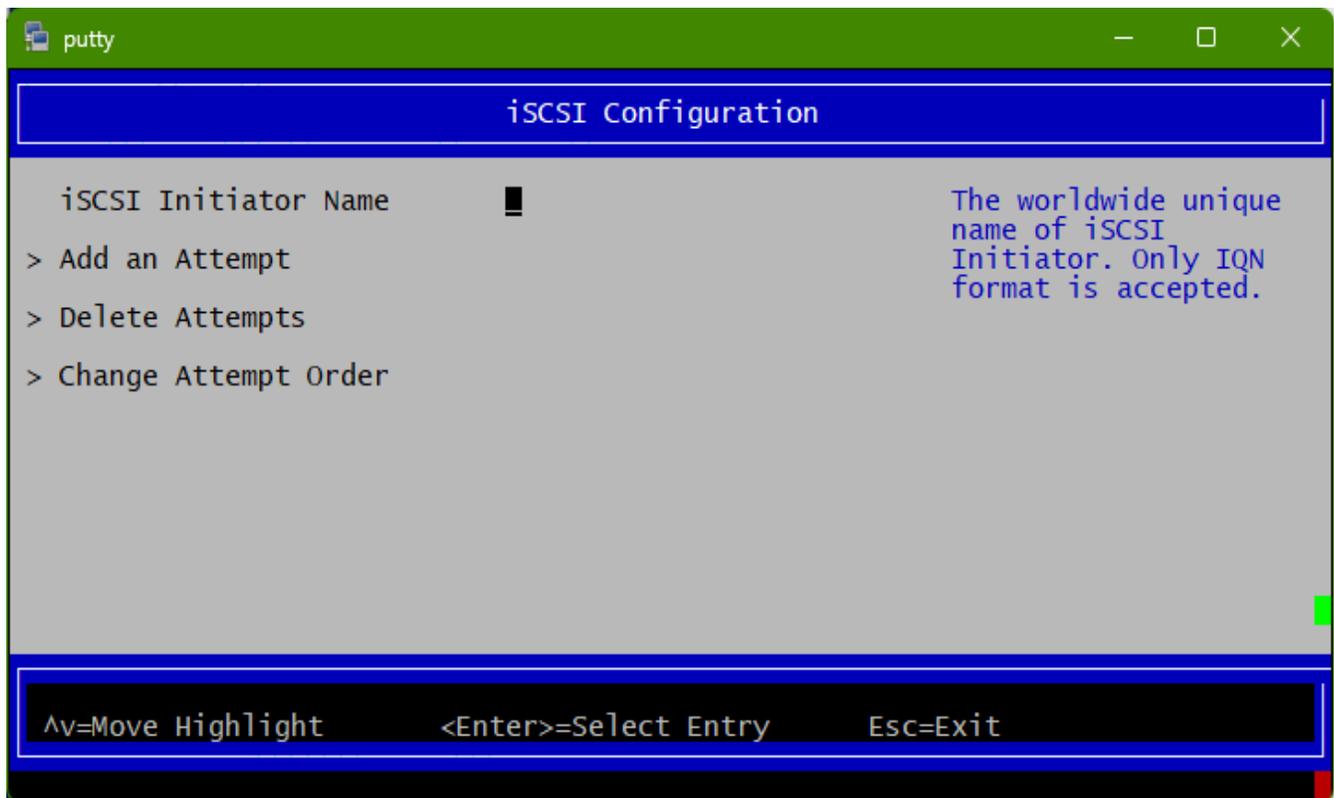
Note

If TLS Auth certificate is configured then all HTTPS traffic on all network interfaces will be verified. UEFI only supports Server CA configuration, Client CA configuration is currently not supported.



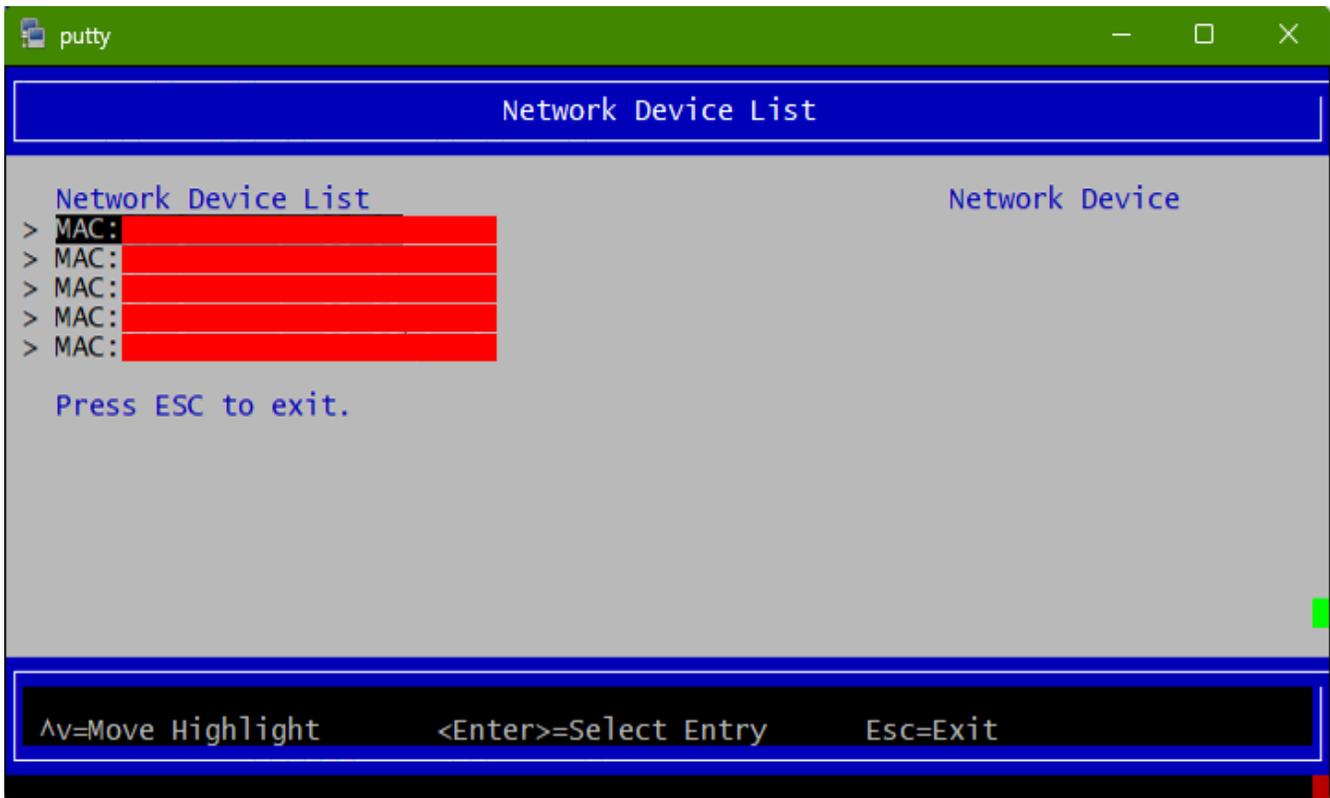
iSCSI Configuration

Provides configuration options for iSCSI.

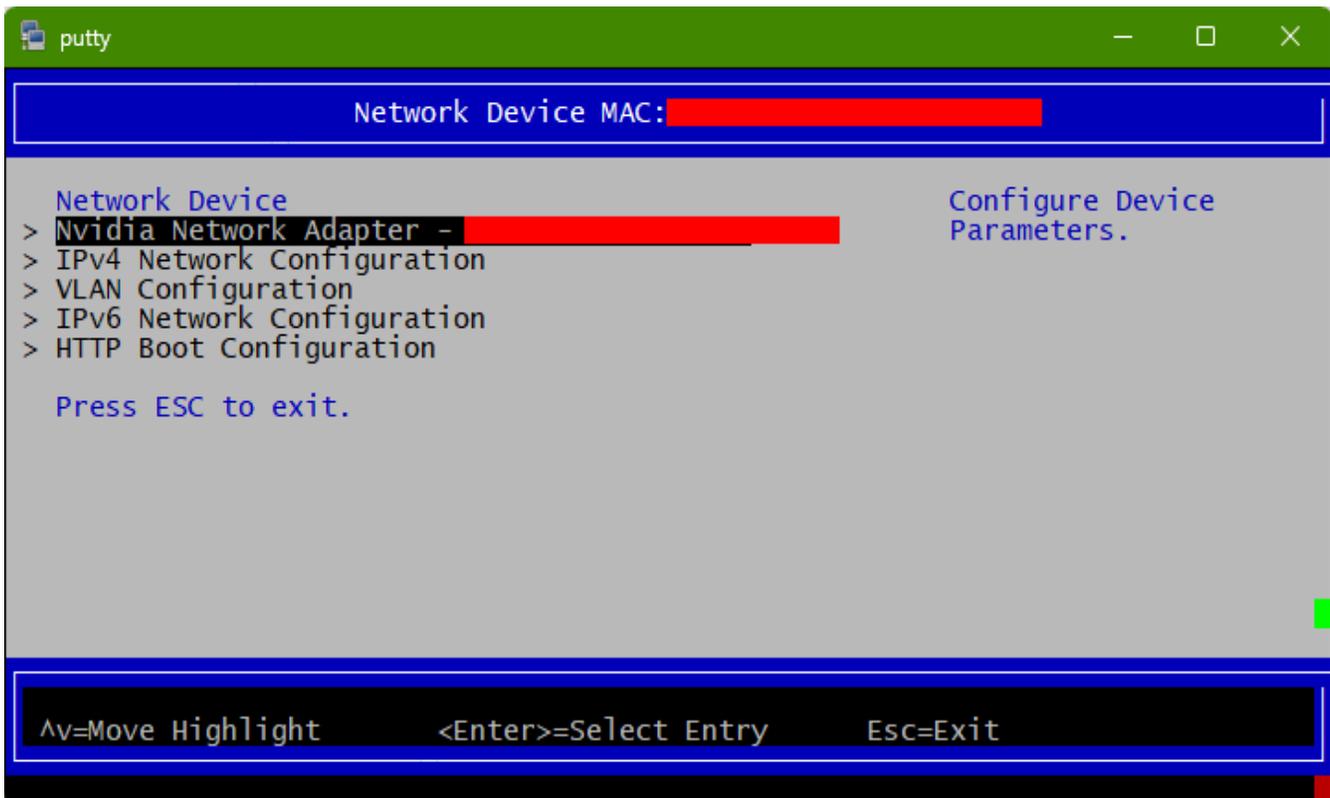


Network Device List

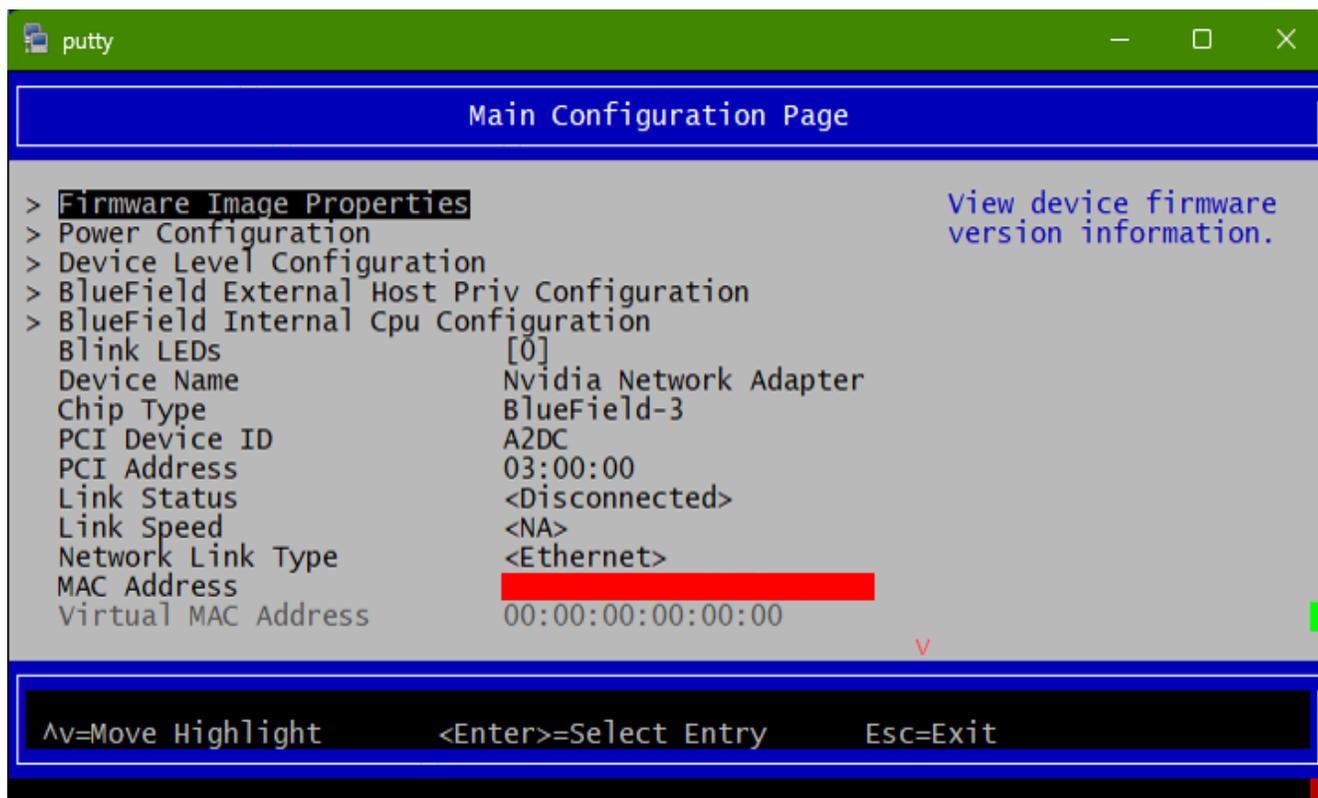
Lists the MAC addresses of the available network interfaces in UEFI.



Users can find more information (Link status, Link speed, PCI ID, Link type, etc.) on each interface upon selection. Users can also configure the interfaces (IPv4, IPv6, VLAN, HTTP BOOT) as needed.



The following menu can be reached by selecting the `Nvidia Network Adapter - <mac-address>` menu options:



Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

© Copyright 2025, NVIDIA. PDF Generated on 12/15/2025