UEFI Menu

Table of contents

Unified Extensible Firmware Interface (UEFI) is l ow-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.

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).

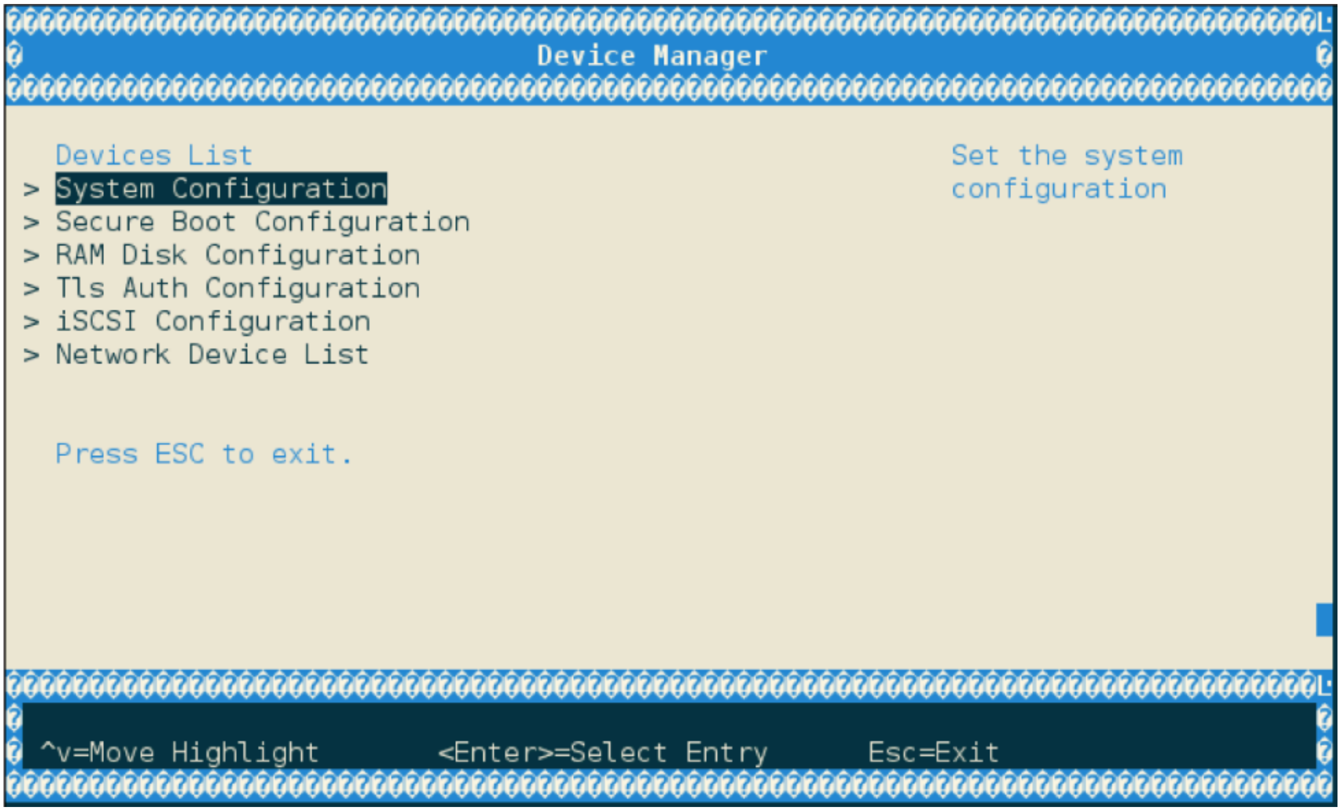
To access the UEFI menu, users must have a connection to the BlueField console either through a UART serial port or the virtual RShim console device. To enter the UEFI menu, hit the Esc key twice during the normal boot sequence.

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.



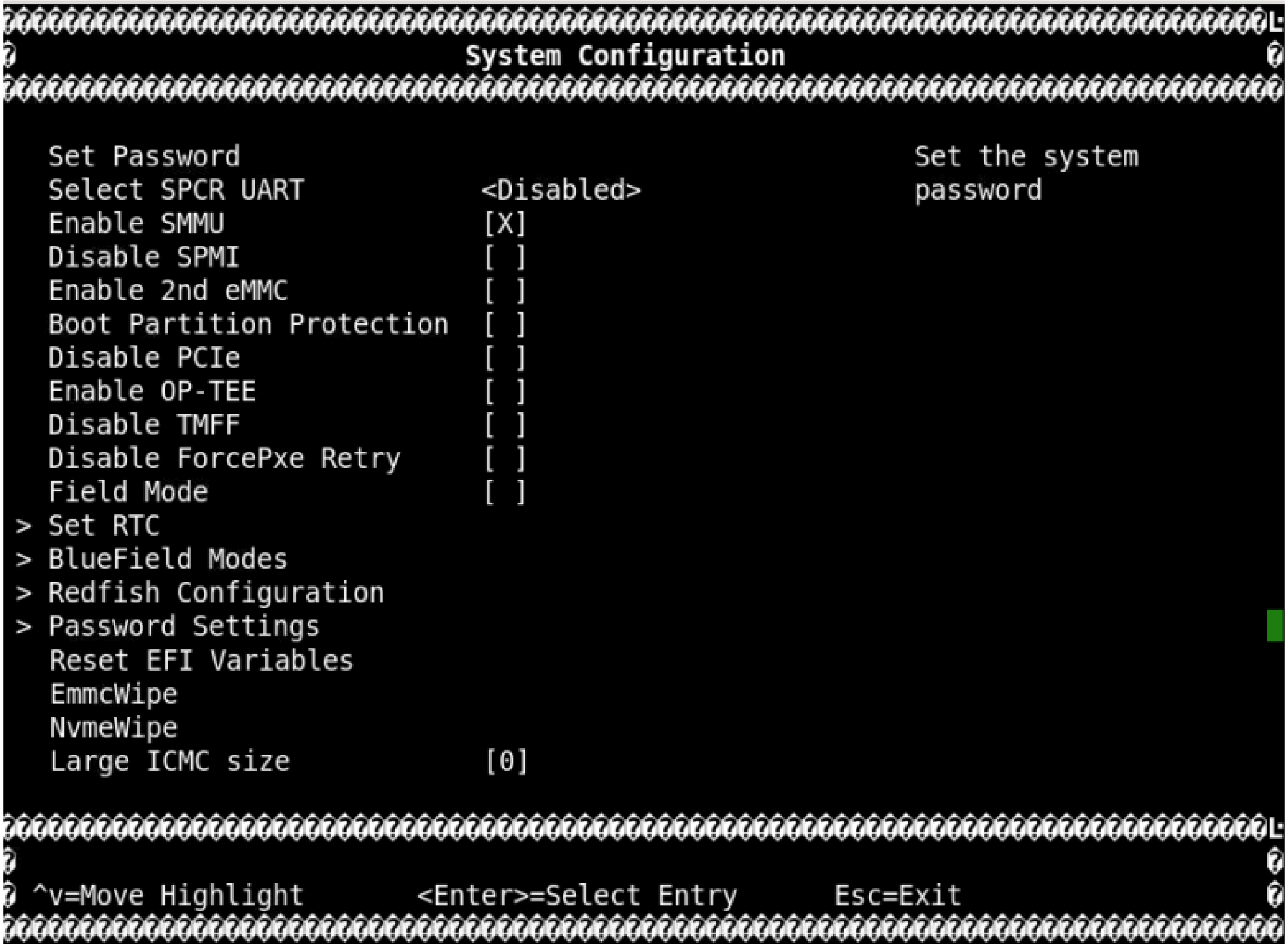
```
                              Device Manager

  Devices List                                        Set the system
> System Configuration                                configuration
> Secure Boot Configuration
> RAM Disk Configuration
> Tls Auth Configuration
> iSCSI Configuration
> Network Device List


  Press ESC to exit.


 ^v=Move Highlight      <Enter>=Select Entry      Esc=Exit
```

System Configuration

Lists different system configuration options.

Note

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



```
                              System Configuration

   Set Password                                        Set the system
   Select SPCR UART           <Disabled>               password
   Enable SMMU                [X]
   Disable SPMI               [ ]
   Enable 2nd eMMC            [ ]
   Boot Partition Protection  [ ]
   Disable PCIe               [ ]
   Enable OP-TEE              [ ]
   Disable TMFF               [ ]
   Disable ForcePxe Retry     [ ]
   Field Mode                 [ ]
 > Set RTC
 > BlueField Modes
 > Redfish Configuration
 > Password Settings
   Reset EFI Variables
   EmmcWipe
   NvmeWipe
   Large ICMC size            [0]

  ^v=Move Highlight       <Enter>=Select Entry      Esc=Exit
```

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, 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.
Select SPCR UART	Choose UART for serial port console redirection [<Disabled>|<UART Port 0> | <UART Port 1>]. 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. ⚠ **Warning** Leave this attribute to its default if you are not certain how to configure it, or you may destabilize your system.

Enable SMMU	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. ⚠ **Warning** Leave this attribute to its default if you do not certain how to configure it.
Disable SPMI	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. ⚠ **Warning** Leave this attribute to its default if you do not certain how to configure it.

Enable 2nd eMMC	Enable/disable the second eMMC. Some legacy BlueField systems have 2 eMMC devices. This feature has been discontinued. ⚠ **Warning** Leave this attribute to its default (disabled) if you do not certain how to configure it, or your system will not boot correctly.
Boot Partition Protection	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. ⓘ **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. ⓘ **Info** If secure boot is enabled, these partitions are write-protected by default.

	Note This menu option is not currently supported for BlueField-3.
Disable PCIe	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. **Note** This attribute is used for diagnostic purposes and should not be modified.
Enable OP-TEE	Enable/disable support for trusted execution environment. **Warning** Do not enable this feature. More information will be provided in future releases.
Disable TMFF	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. **Warning**

	Leave this attribute to its default if you do not certain how to configure it.
Disable Force Pxe Retry	If enabled, PXE boot option entries are attempted only once instead of retrying them in a loop when "ForcePxe" is requested via IPMI interface
Field Mode	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. ⚠ **Warning** Leave this attribute to its default unless you are certain you wish to enable field mode on the NIC BMC. Consult the DPU BMC user manual for more information on field mode.
Set RTC	Allows users to set the time and date for the real-time clock.
BlueField Modes	• Internal CPU Model: [<Separated>|<Embedded>] • Host Privilege Level: [<Restricted>|<Privileged>] • NIC Mode – sets the BlueField to operate in either NIC mode or DPU mode ⓘ **Note** Any change to this attribute requires device reset to take effect.

Redfish Configuration	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. The RTCSync option syncs RTC time with Redfish time under the Manager schema.
Password Settings	• 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.
Reset EFI Variables	This action clears all EFI variables to factory default state. Reset the device to take effect. ⚠ **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.
Emmc Wipe	Clears the eMMC disk. The action is immutable and all data on eMMC is lost after it is performed.
Nvme Wipe	Clears the NVMe SSD. This action is immutable and all data on NVMe SSD is lost after it is performed.
Large ICMC size	Set the large ICMC size in Hex and MB. Valid value: 0-100000h in 80h increments. ⓘ **Info**

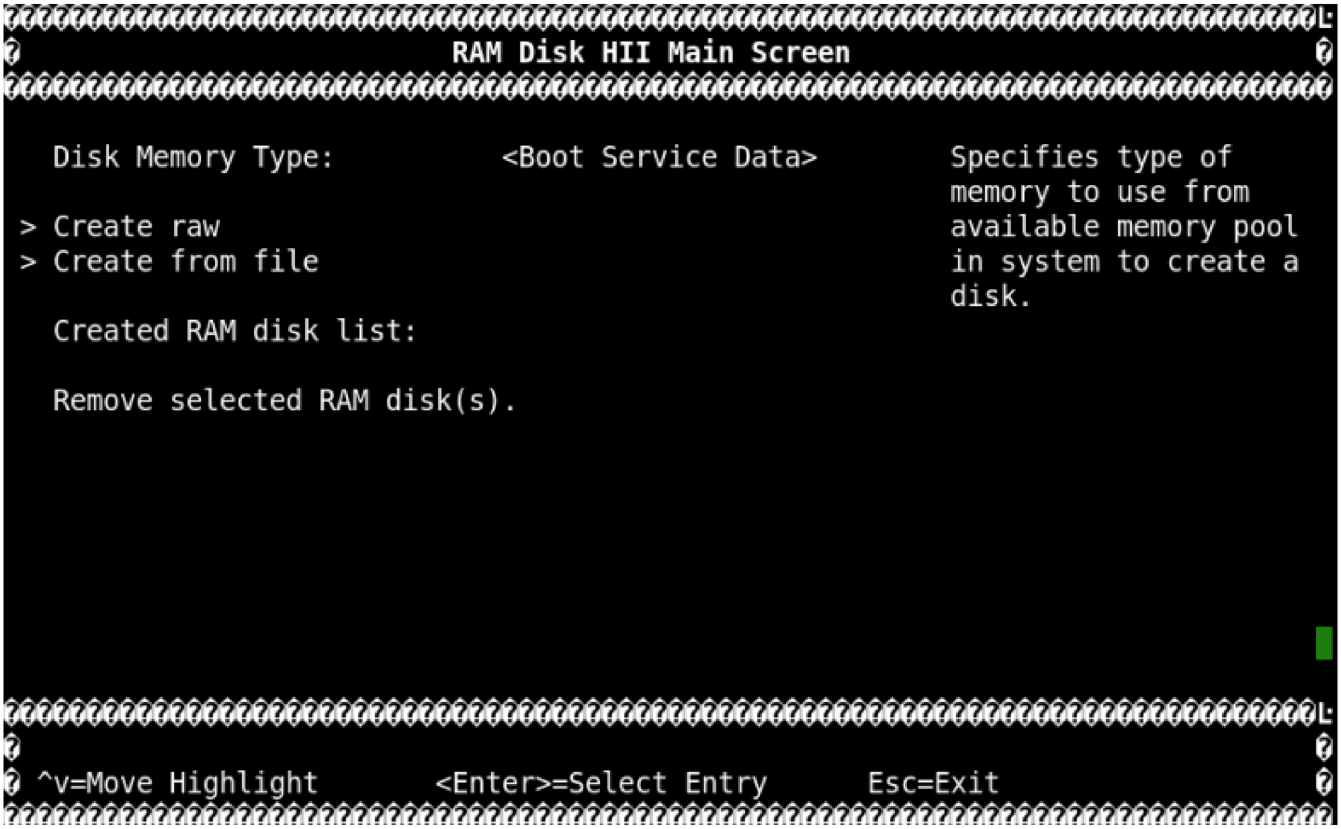
	This menu option is only relevant for BlueField-3 platforms.

Secure Boot Configuration

Please refer to section "UEFI Secure Boot" for more information.

RAM Disk Configuration

Provides option to create/delete RAM disks.



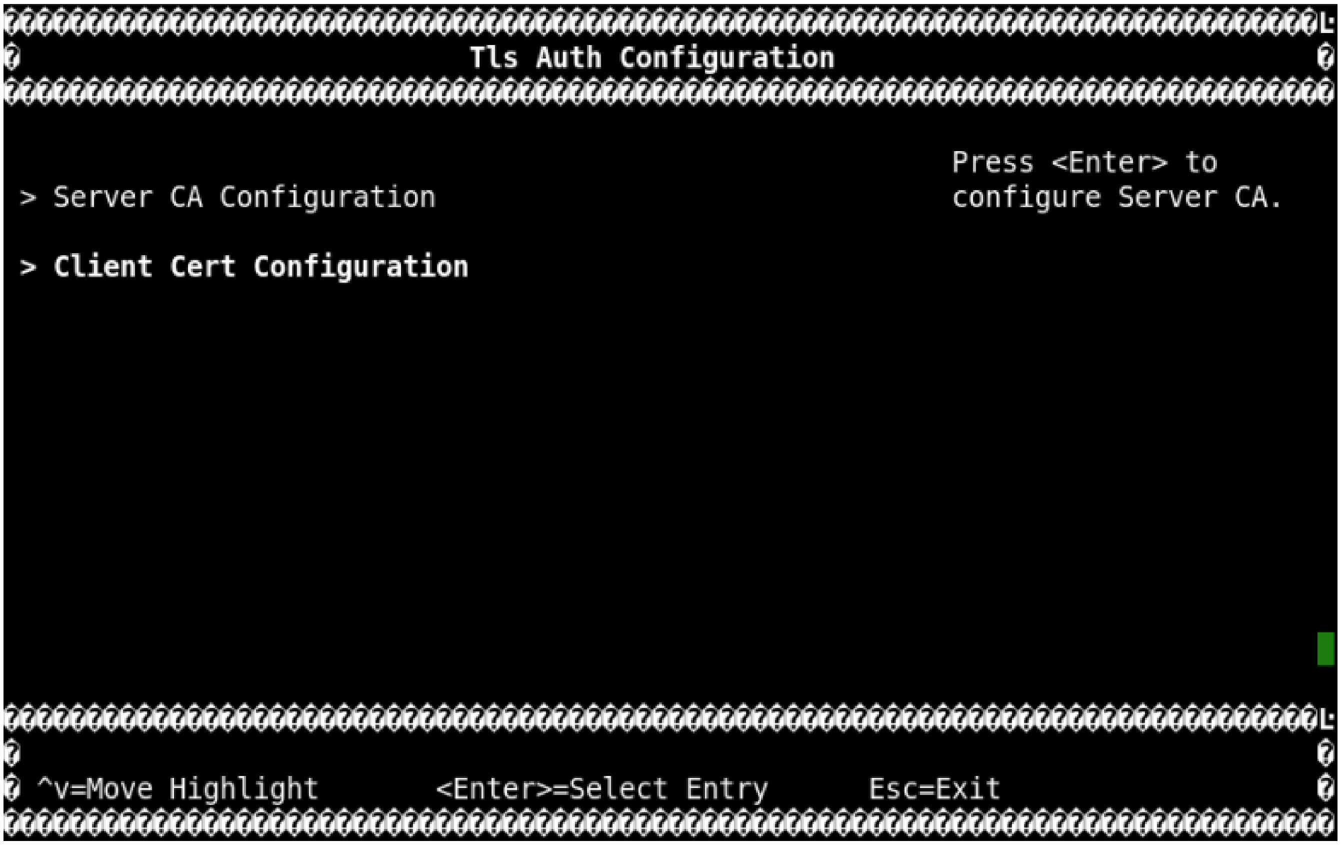
```
                          RAM Disk HII Main Screen

  Disk Memory Type:          <Boot Service Data>       Specifies type of
                                                       memory to use from
> Create raw                                           available memory pool
> Create from file                                     in system to create a
                                                       disk.
  Created RAM disk list:

  Remove selected RAM disk(s).



 ^v=Move Highlight       <Enter>=Select Entry      Esc=Exit
```

Tls Auth Configuration

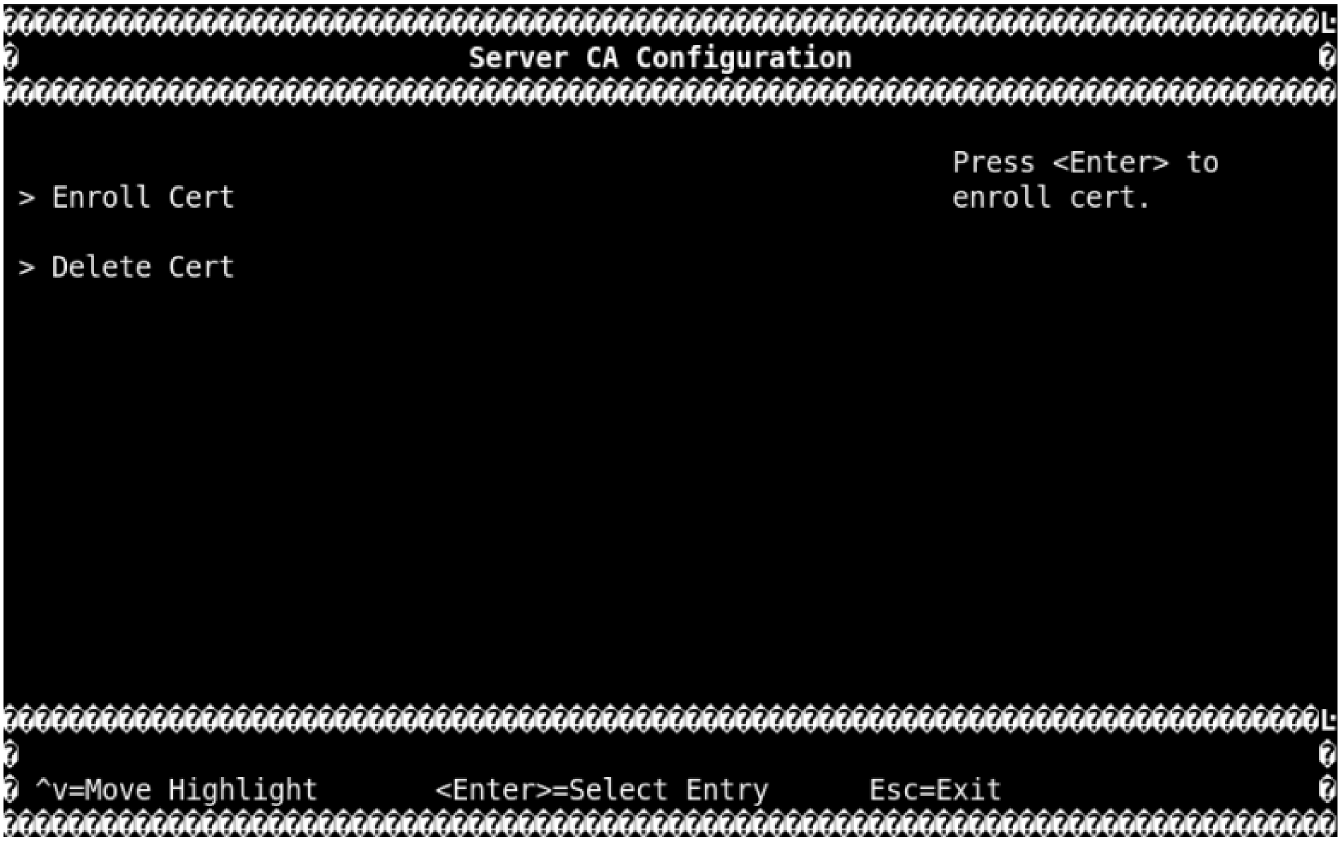
Provides configuration (enroll/delete) of TLS auth certificates for HTTPS traffic in UEFI.

ⓘ **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.



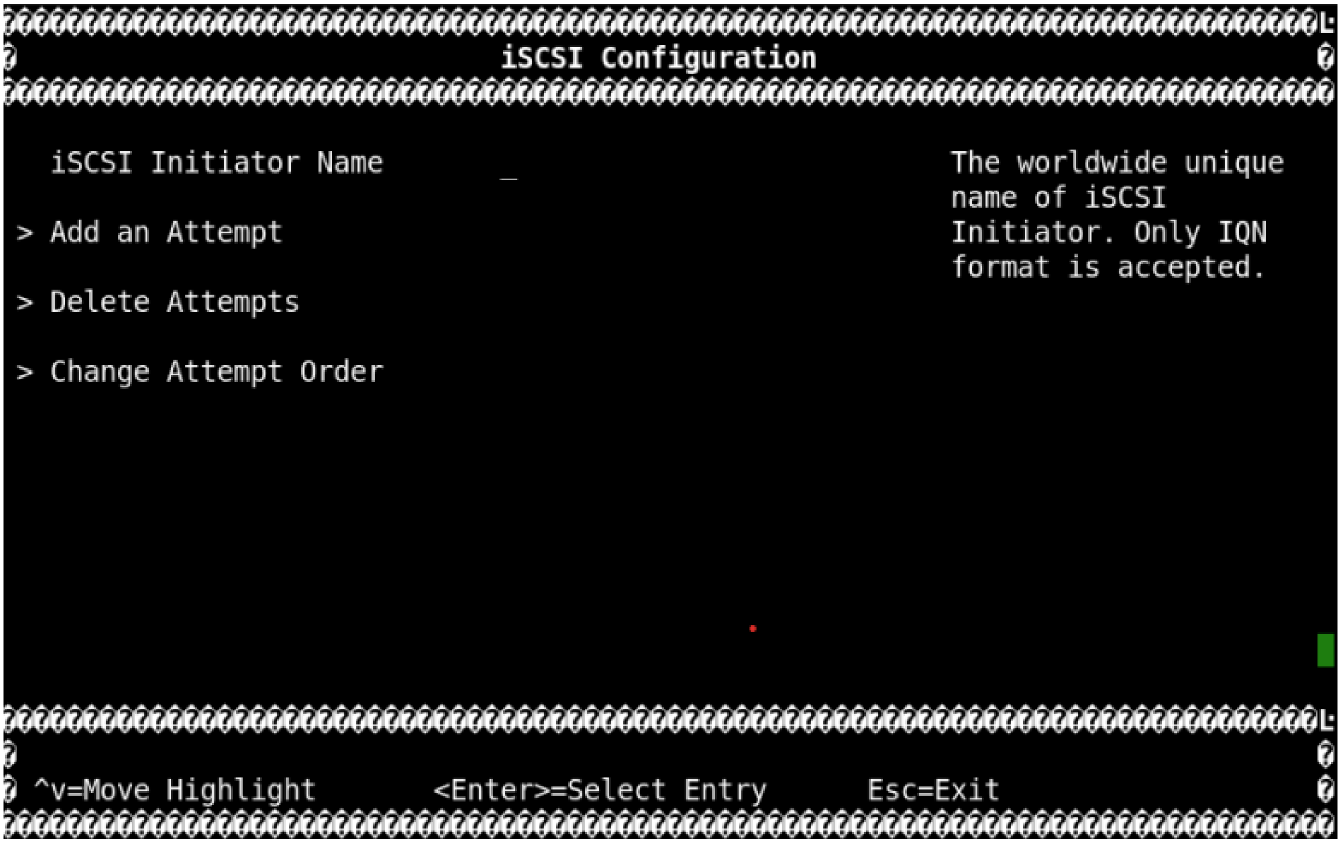
```
                          Tls Auth Configuration

                                                     Press <Enter> to
> Server CA Configuration                            configure Server CA.

> Client Cert Configuration



 ^v=Move Highlight      <Enter>=Select Entry      Esc=Exit
```



```
                    Server CA Configuration

                                               Press <Enter> to
> Enroll Cert                                  enroll cert.

> Delete Cert


 ^v=Move Highlight     <Enter>=Select Entry     Esc=Exit
```

iSCSI Configuration

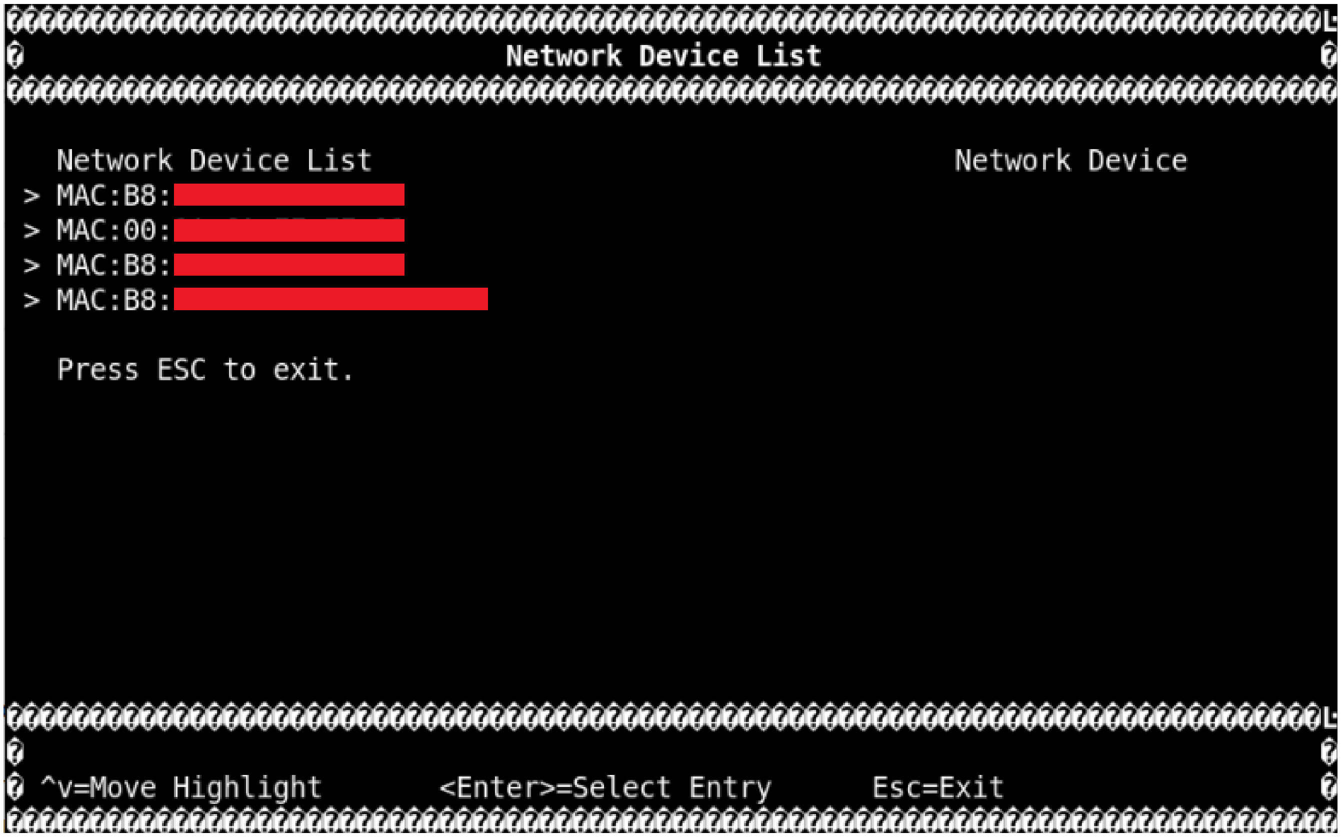
Provides configuration options for iSCSI.



```
                              iSCSI Configuration

  iSCSI Initiator Name          _                         The worldwide unique
                                                          name of iSCSI
> Add an Attempt                                          Initiator. Only IQN
                                                          format is accepted.
> Delete Attempts

> Change Attempt Order



  ^v=Move Highlight      <Enter>=Select Entry      Esc=Exit
```

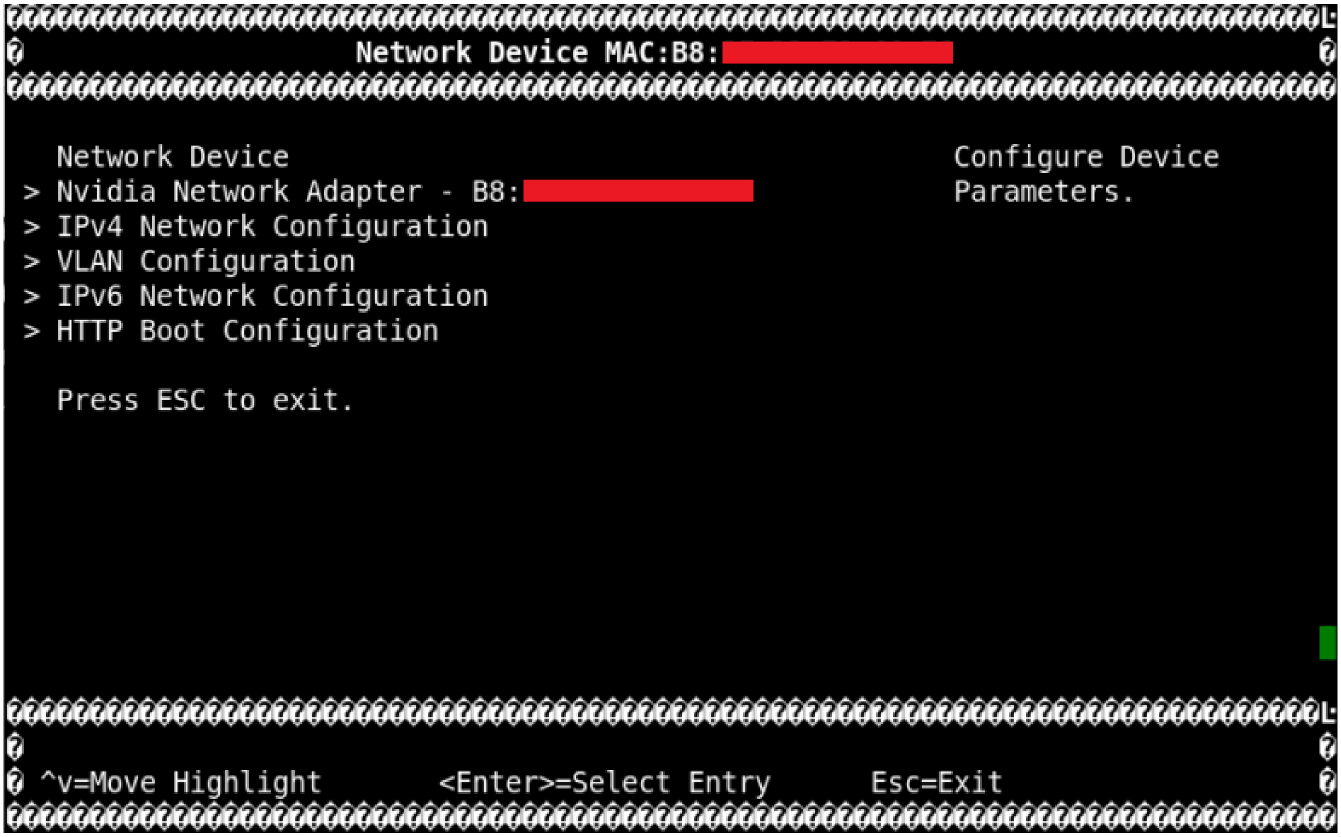
Network Device List

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



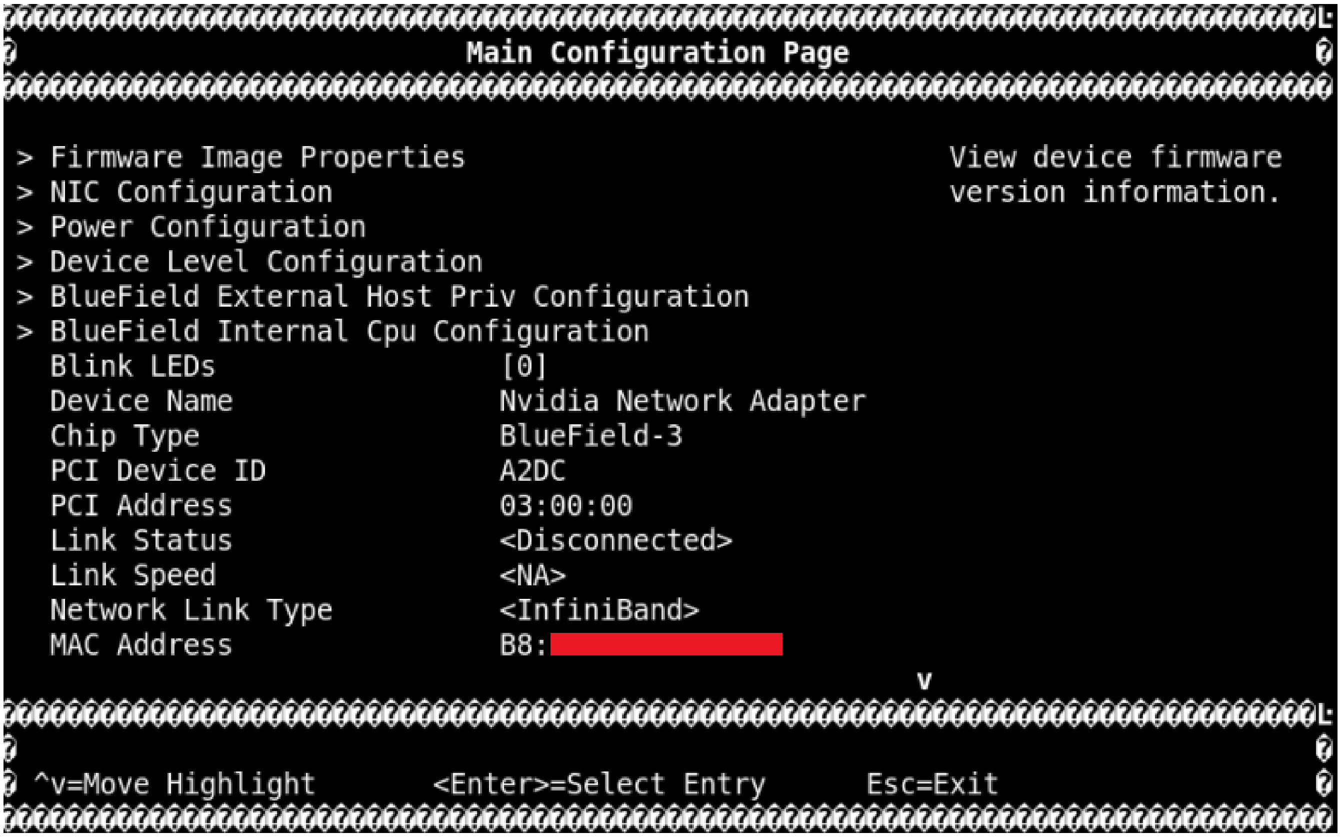
```
                              Network Device List

  Network Device List                                    Network Device
> MAC:B8:[redacted]
> MAC:00:[redacted]
> MAC:B8:[redacted]
> MAC:B8:[redacted]

  Press ESC to exit.

 ^v=Move Highlight       <Enter>=Select Entry      Esc=Exit
```

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.



```
                    Network Device MAC:B8:[redacted]

   Network Device                                        Configure Device
 > Nvidia Network Adapter - B8:[redacted]                Parameters.
 > IPv4 Network Configuration
 > VLAN Configuration
 > IPv6 Network Configuration
 > HTTP Boot Configuration

   Press ESC to exit.



  ^v=Move Highlight       <Enter>=Select Entry      Esc=Exit
```

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



```
                         Main Configuration Page

> Firmware Image Properties                          View device firmware
> NIC Configuration                                  version information.
> Power Configuration
> Device Level Configuration
> BlueField External Host Priv Configuration
> BlueField Internal Cpu Configuration
  Blink LEDs                [0]
  Device Name               Nvidia Network Adapter
  Chip Type                 BlueField-3
  PCI Device ID             A2DC
  PCI Address               03:00:00
  Link Status               <Disconnected>
  Link Speed                <NA>
  Network Link Type         <InfiniBand>
  MAC Address               B8:[redacted]
                                                 v

 ^v=Move Highlight      <Enter>=Select Entry      Esc=Exit
```