# 如何使用EFI外壳将安全恶意软件分析设备引导到恢复模式并向引导选项添加恢复模式

## 目录

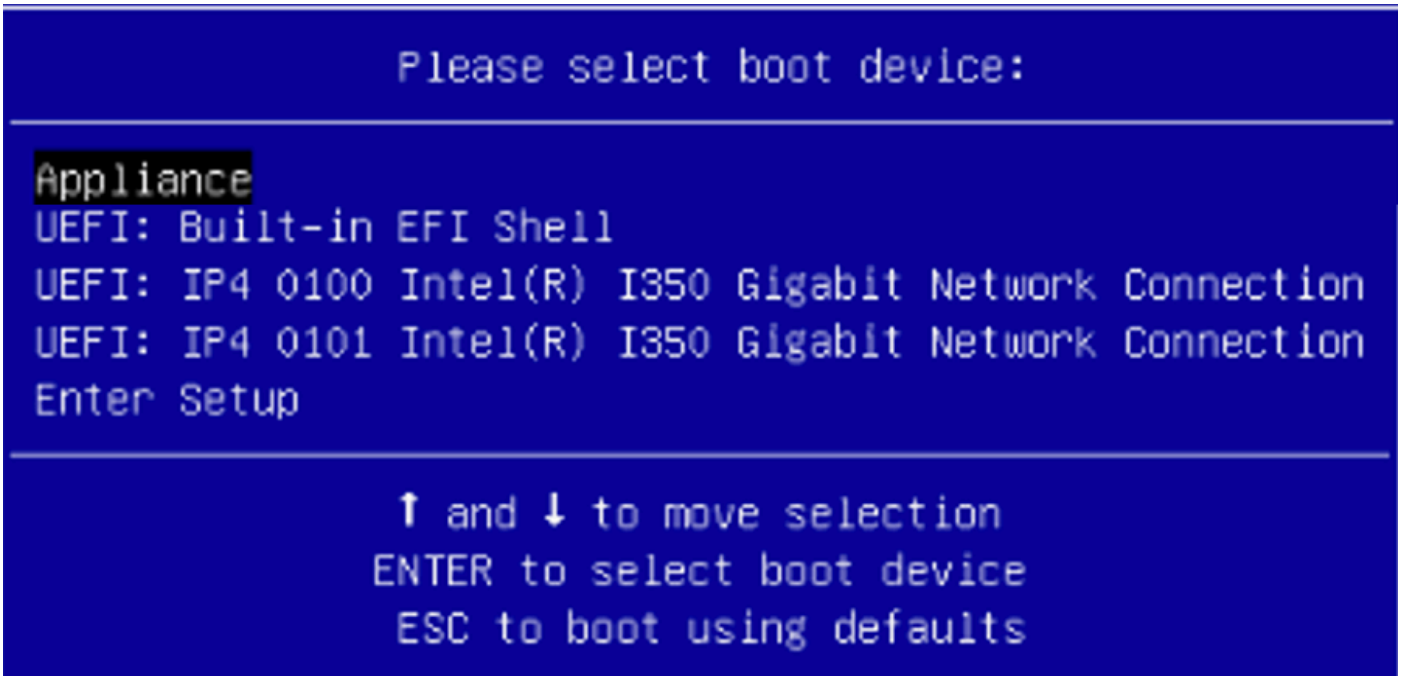


## 简介

本文档介绍如何使用EFI外壳将安全恶意软件分析®设备引导到恢复模式以及将恢复模式添加到引导选项的步骤。

## 问题

您将能够看到，如图所示，BIOS窗口中未显示恢复模式：




要在此场景中引导到恢复模式，我们必须使用下一节中介绍的步骤。

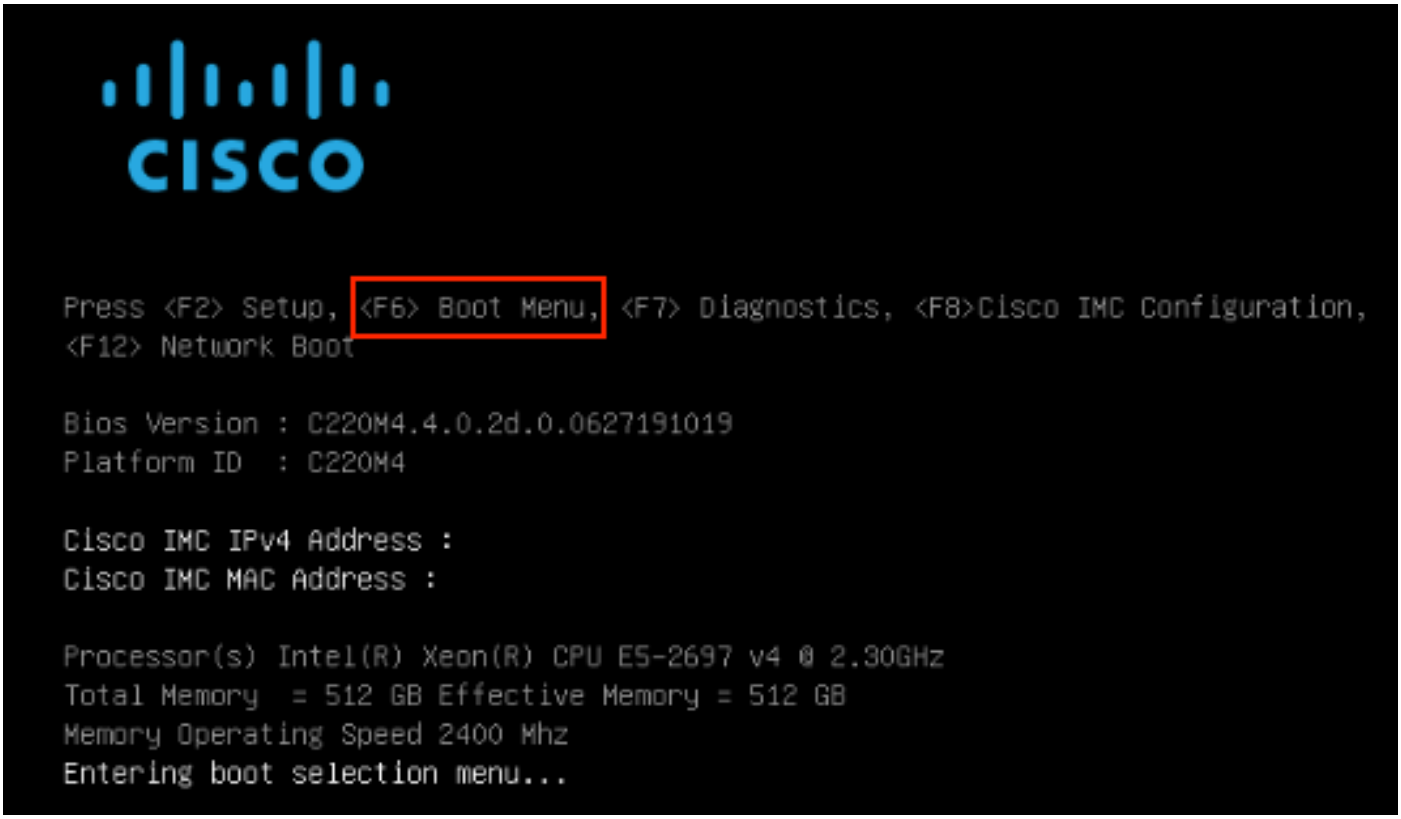
## 解决方案

### EFI外壳

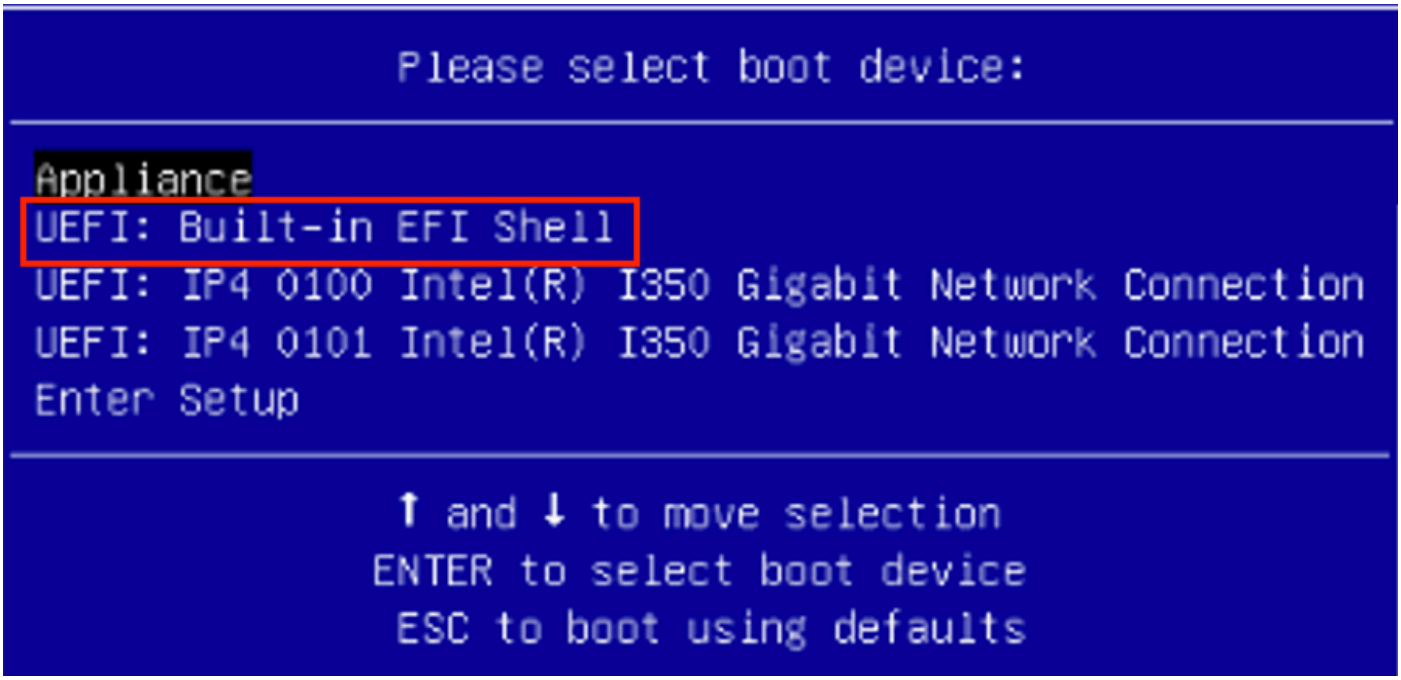
步骤1.将KVM适配器连接到外部显示器和键盘，并将其插入位于设备前面的KVM端口。如果CIMC可用且已配置，则可以使用远程KVM。

步骤2.重新启动设备。

步骤3.在BIOS窗口中按F6，查看可能的引导目标列表。




步骤4.选择UEFI:内置EFI外壳。




步骤5.在启动脚本完成之后，按ESC键进入EFI Shell。

步骤6.可用文件系统的列表。

```
UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x00050008). Revision 1.02
Mapping table
      fs0: Alias(s):HD29a0b::blk1:
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(1,GPT,7303FEC6-7E81-4D88-961C-AE562681960F,0x800,0x4
00000)
      fs1: Alias(s):HD29b0b::blk5:
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(1,GPT,C65AF6B6-C149-4184-B744-EB15CD038D5B,0x800,0x4
00000)
     blk0: Alias(s):
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)
     blk4: Alias(s):
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)
     blk2: Alias(s):
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(2,GPT,900A83C7-D4F4-44C3-B6D3-35D2DCC6249F,0x400800,
0x400000)
     blk3: Alias(s):
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,GPT,D5A6A81E-85F9-4648-9277-3E4A89B43D65,0x800800,
0xD5A6FDF)
     blk6: Alias(s):
          PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(2,GPT,ED9A0467-38FD-4DCF-A409-057CEC64FA1E,0x400800,
0x2B9A8CFDF)
Press ESC in 5 seconds to skip startup.nsh or any other key to continue.
Shell> _
```

步骤7.此时，您需要找到位于其中一个文**件系**统中的“恢复”目录。

步骤8.导航到该目录。

```
Shell> fs1:
fs1:\> dir
Directory of: fs1:\
03/16/2022  17:12              31,736  meta_contents.tar.xz
10/26/2020  11:29                 149  startup.nsh
12/21/2016  23:42 <DIR>         4,096  efi
04/30/2021  08:28         836,030,464  recovery.rosfs
          3 File(s)  836,062,349 bytes
          1 Dir(s)
fs1:\> cd efi
fs1:\efi\> dir
Directory of: fs1:\efi\
12/21/2016  23:42 <DIR>         4,096  .
12/21/2016  23:42 <DIR>             0  ..
04/30/2021  08:28 <DIR>         4,096  Recovery
          0 File(s)              0 bytes
          3 Dir(s)
fs1:\efi\> cd Recovery
fs1:\efi\Recovery\> dir
Directory of: fs1:\efi\Recovery\
12/21/2016  23:42 <DIR>         4,096  .
12/21/2016  23:42 <DIR>         4,096  ..
04/30/2021  08:28          18,255,144  boot.efi
          1 File(s)  18,255,144 bytes
          2 Dir(s)
```

步骤9.执行命**令fs1:\efi\Recovery\boot.efi**

步骤10.设备引导到恢复模式。

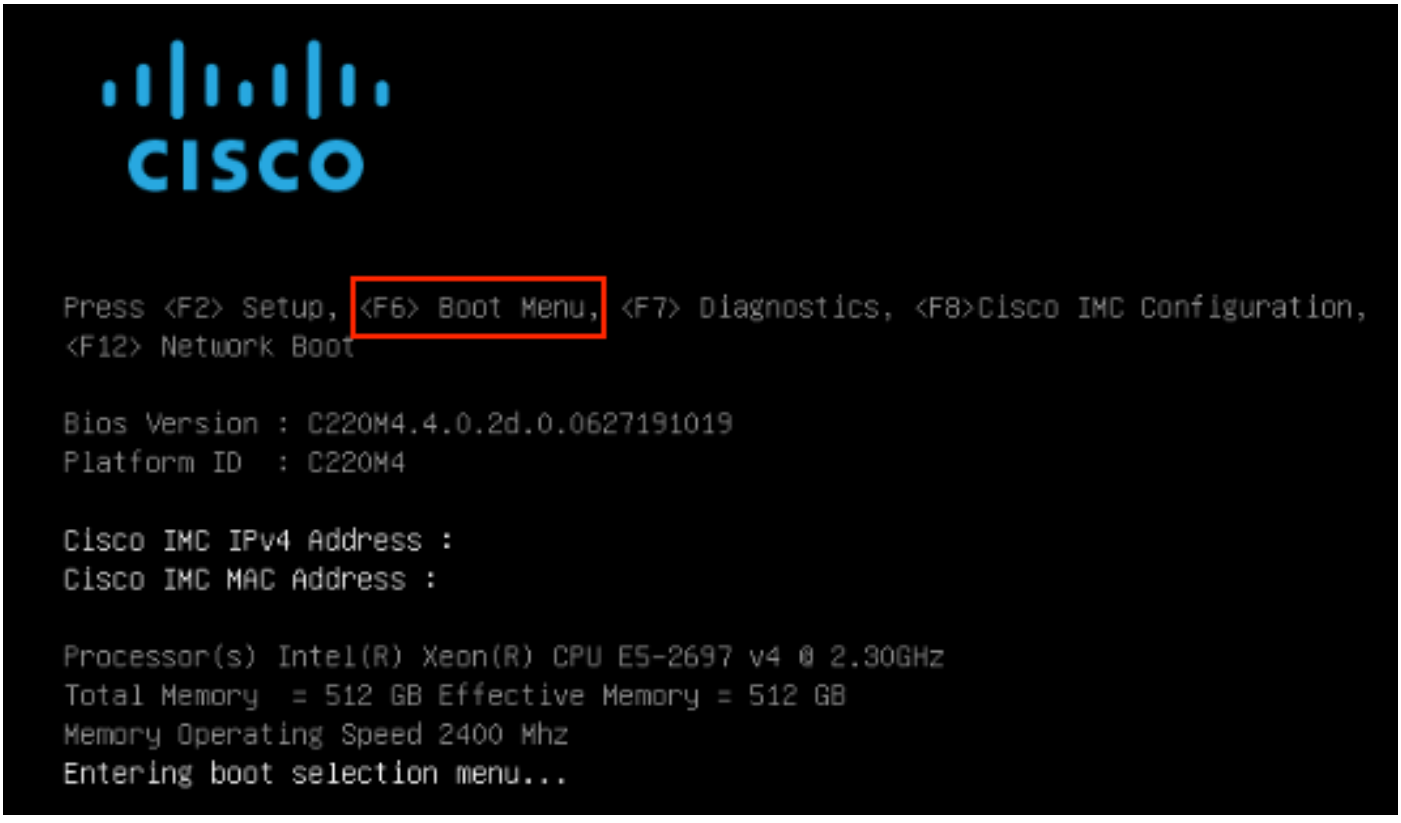
```
>>
>>
>> help
   COMMANDS:
          configure -- show|set: View or modify configuration variables
              conns -- listening|open|all: Show open connections
       destroy-data -- Reset appliance to be a target for the restore process
               exit -- Exit tgsh.
            graphql -- Following content until the next empty line is treated as a GraphQL query to run
               halt -- Halt appliance
               help -- List available commands, or 'help COMMAND' for details.
          netconfig -- Update configured network settings
    netconfig-apply -- Modify active network configuration to match saved settings
             netinfo -- routes|firewall|addrs|stats: Show network configuration and status
             opadmin -- import|check: Sync from, or validate, new configuration format
              passwd -- Change password for this account
                ping -- ping [-c count] [-I interface] host: ping a remote host
            poweroff -- Power off appliance
              reboot -- Reboot appliance
         reconfigure -- simple|with-reinstall: Nondestructively rerun configuration in single-user mode, with or without precedin
g reinstall
             service -- {status|start|stop|restart} [svc-name]: Toggle ThreatGRID services
       support-mode -- status|start|stop: Toggle support mode
          traceroute -- Determine the path used to a network location
             version -- Shows appliance version
>>
```

## 将恢复模式添加到引导选项

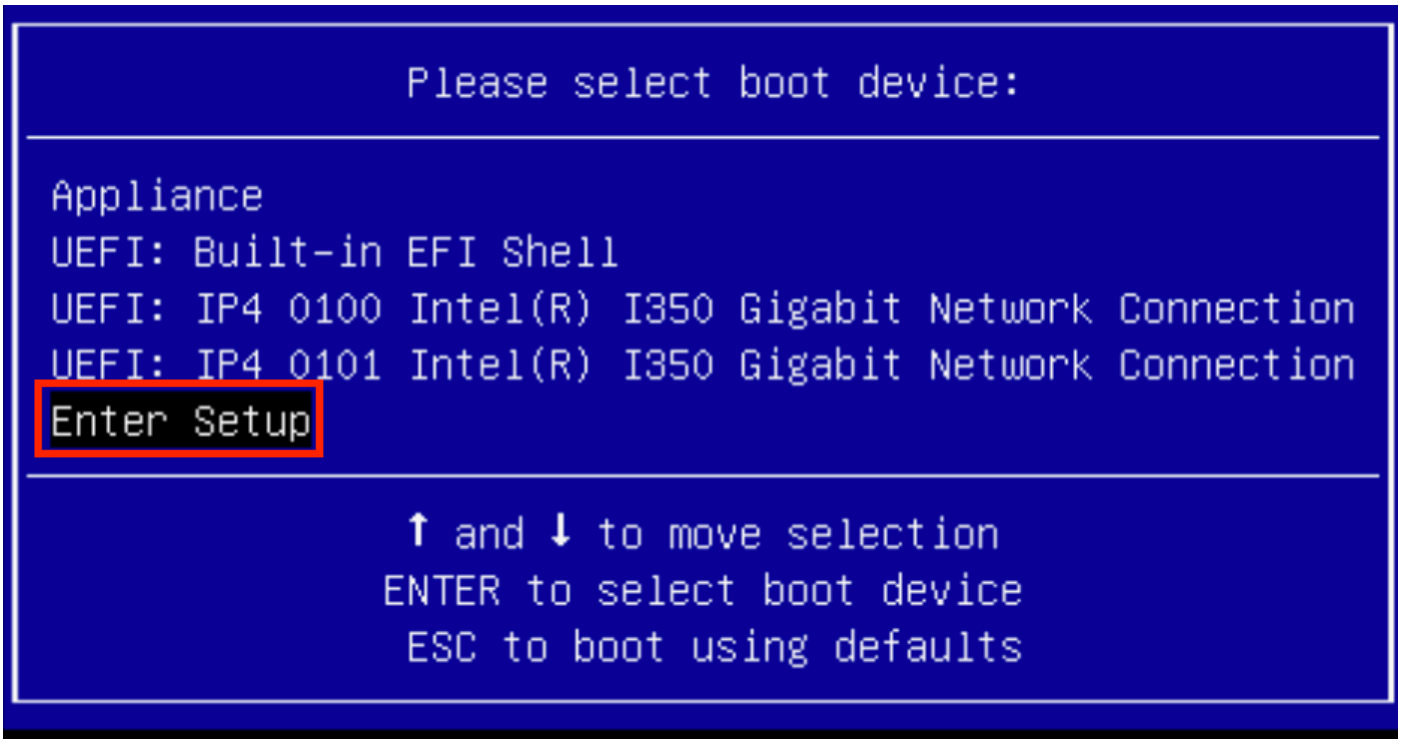
步骤1.将KVM适配器连接到外部显示器和键盘，并将其插入位于设备前面的KVM端口。如果CIMC可用且已配置，则可以使用远程KVM。

步骤2.重新启动设备。

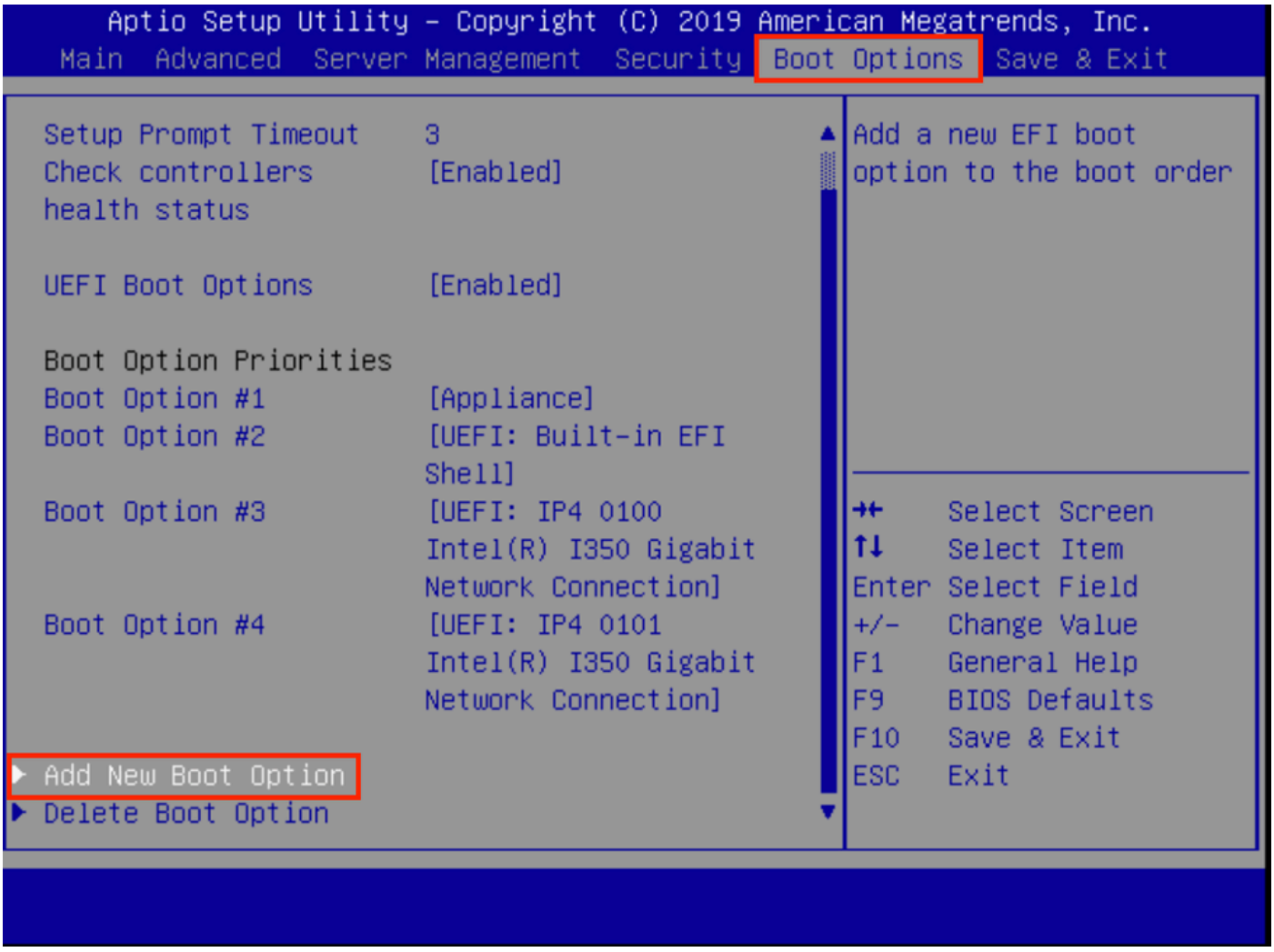
步骤3.在BIOS**窗口**中按F6，查看可能的引导目标列表。



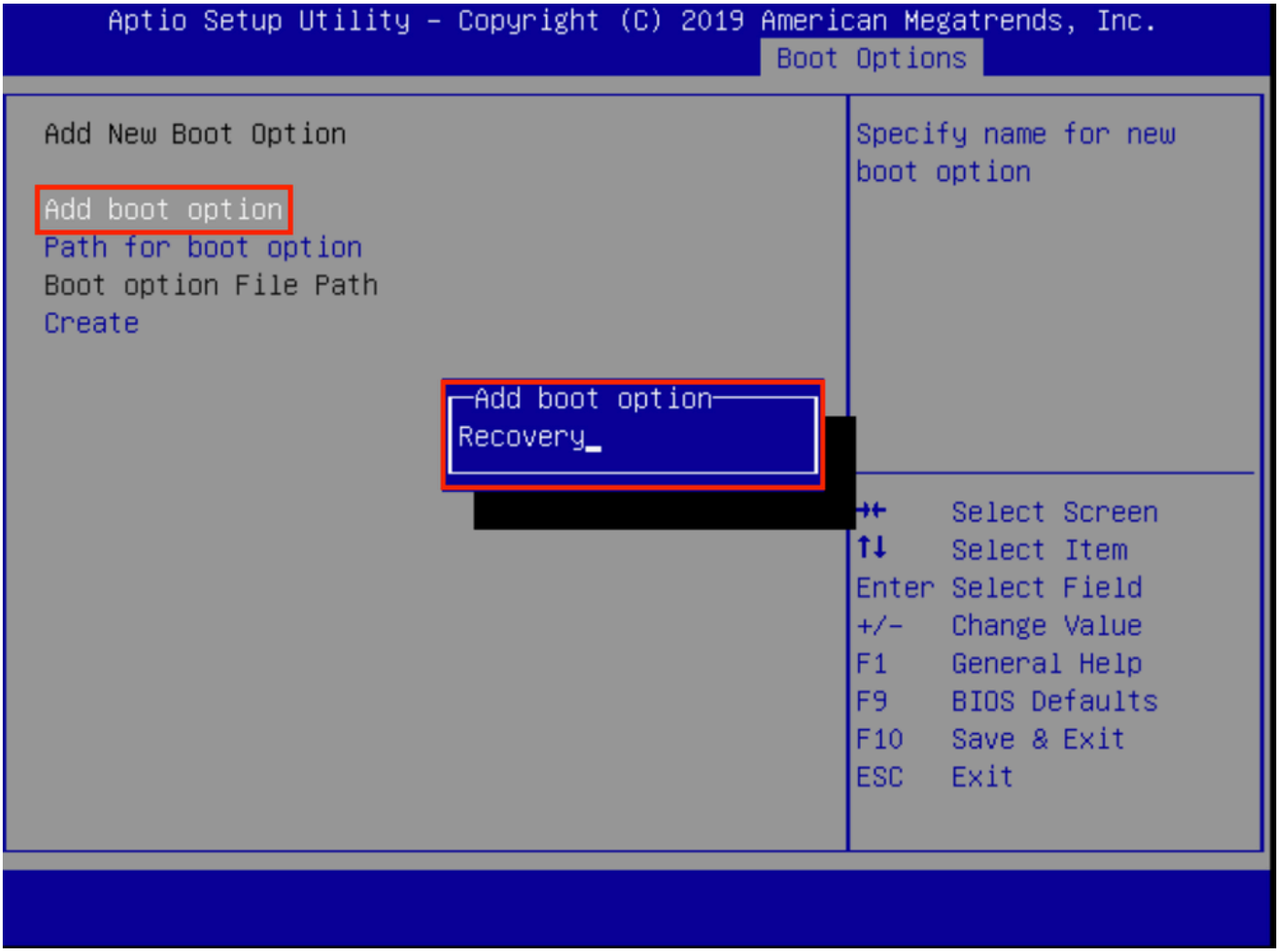
步骤4.选择“**输入设置**”。



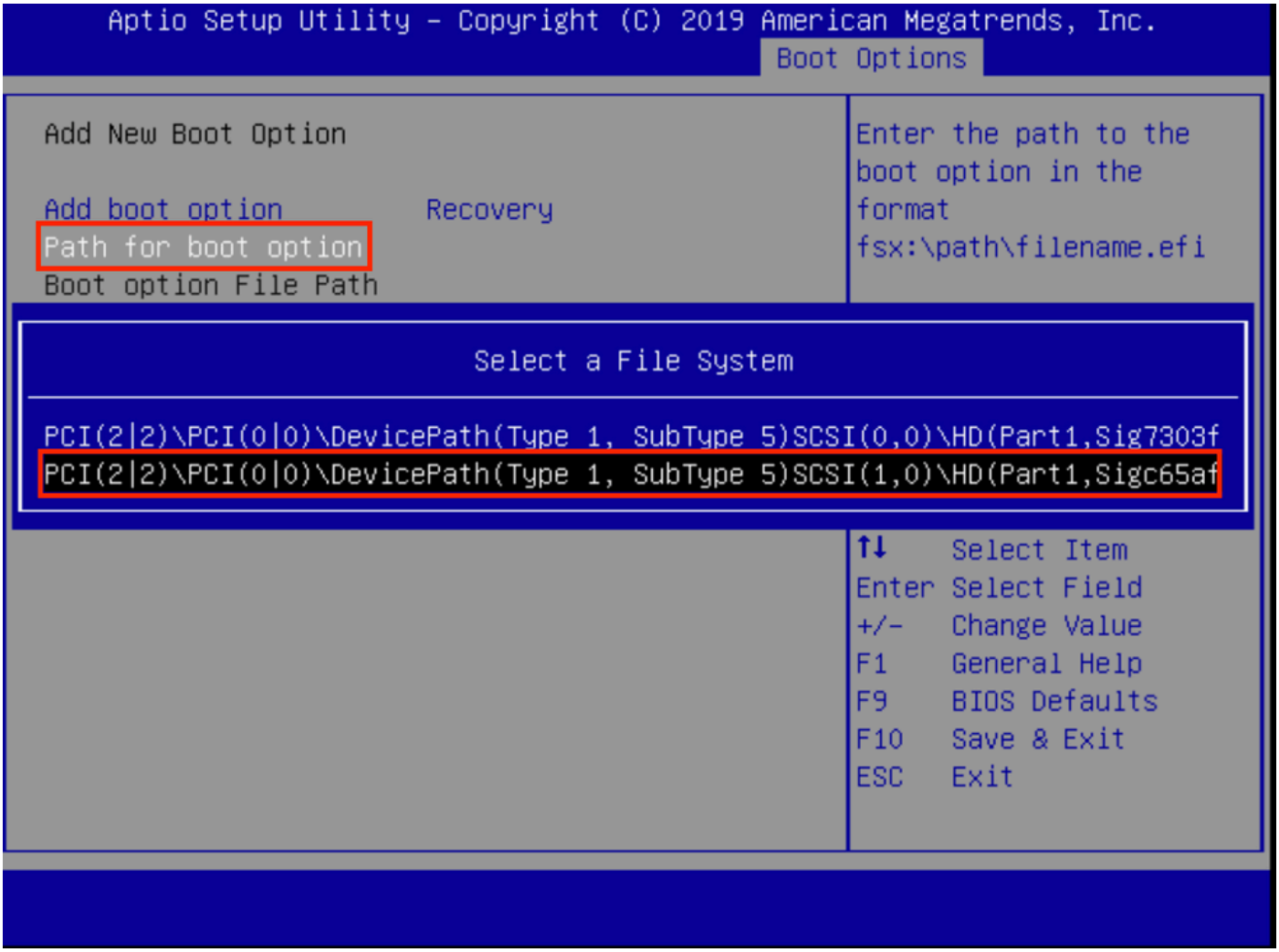

步骤5.导航至“**引导选**项”，滚动到底部，然后选择“添**加新引导选项”**。



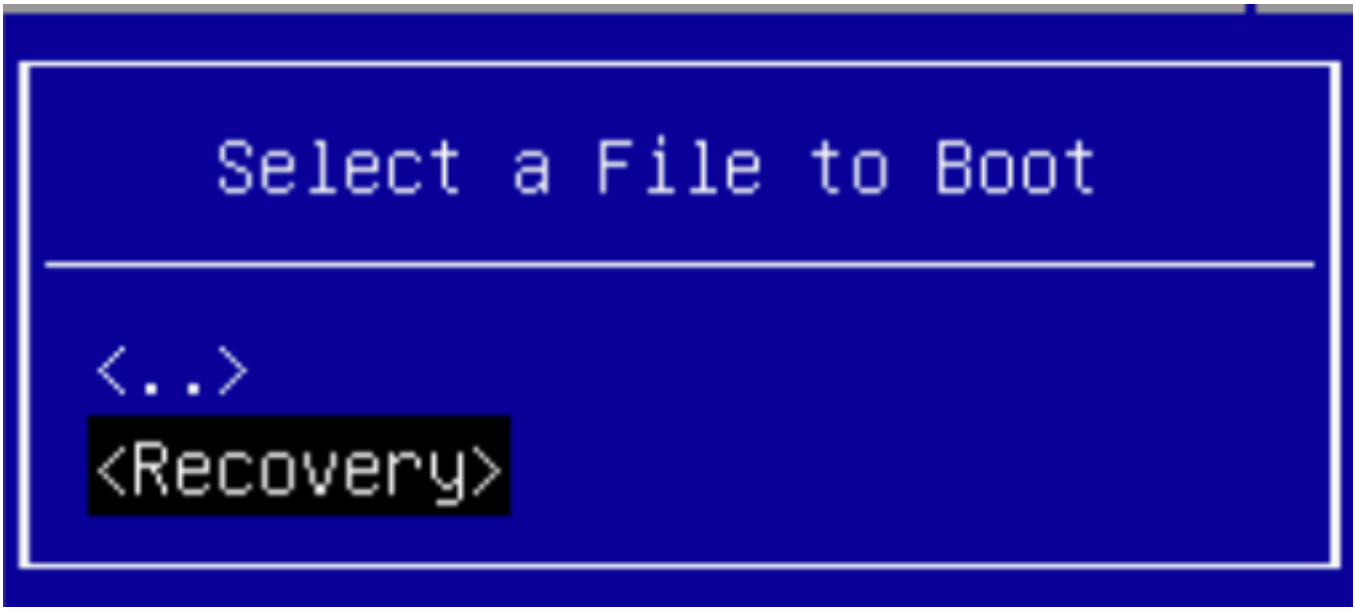

步骤6.选择“添**加引导选项**”并键入**“恢复”**。

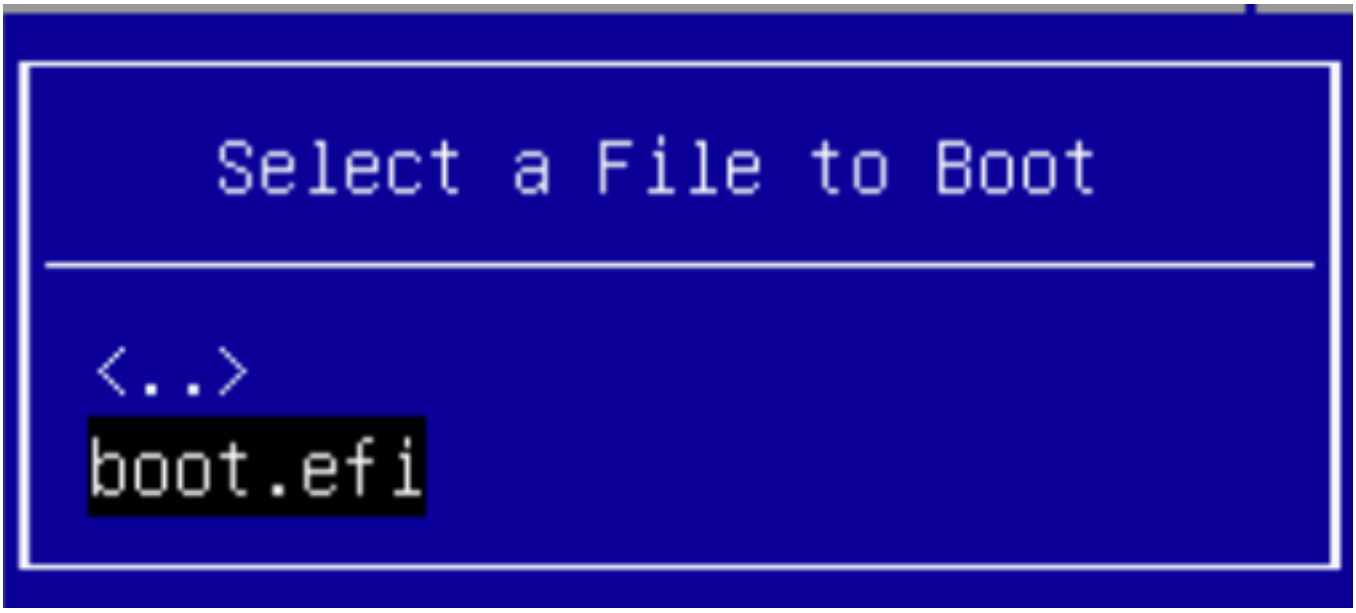



步骤7.选择Path for boot**选项，然后选**择适当的**File System**。

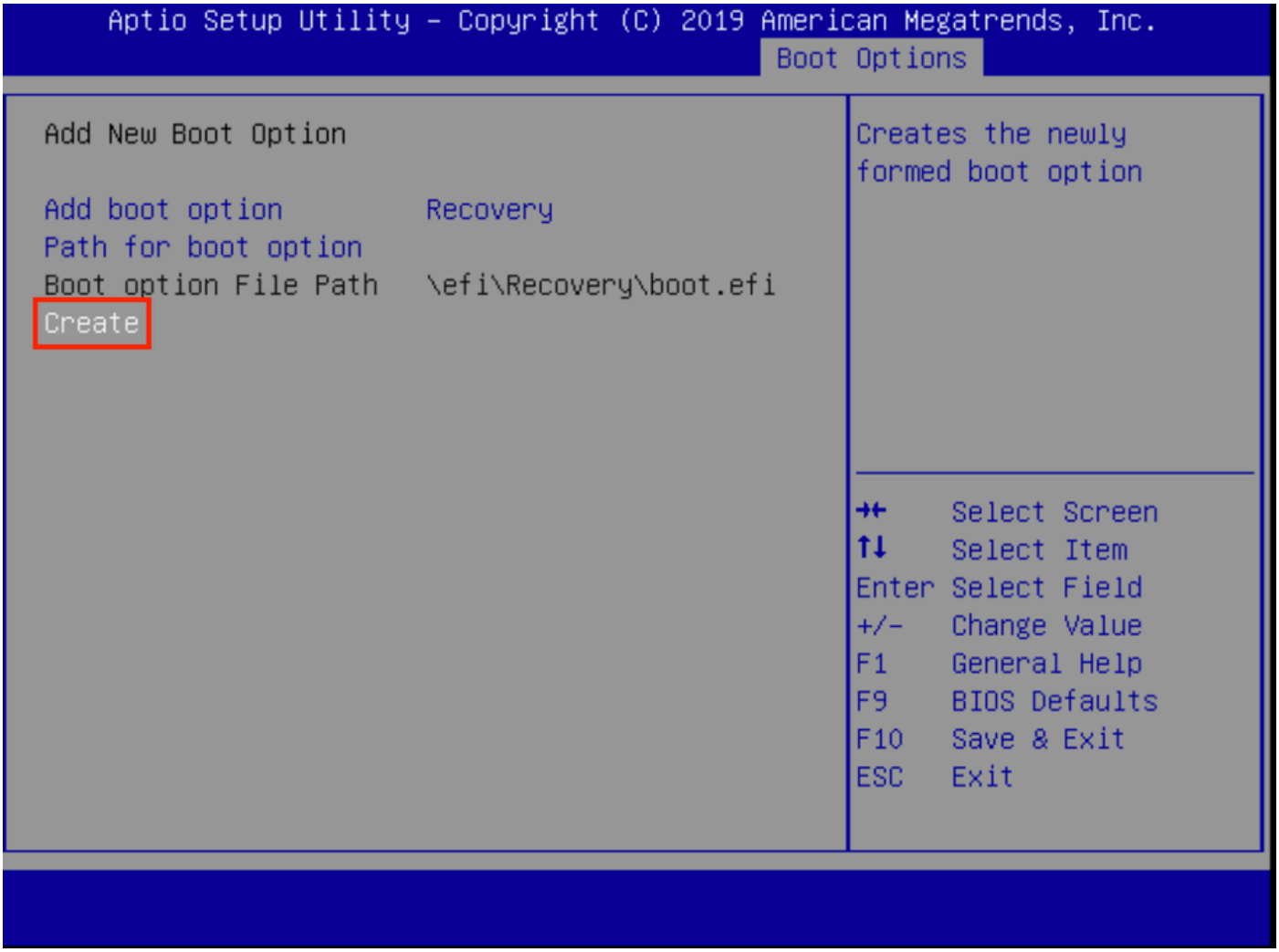



步骤8.选择<efi>、<Recovery>和<boot.efi>。

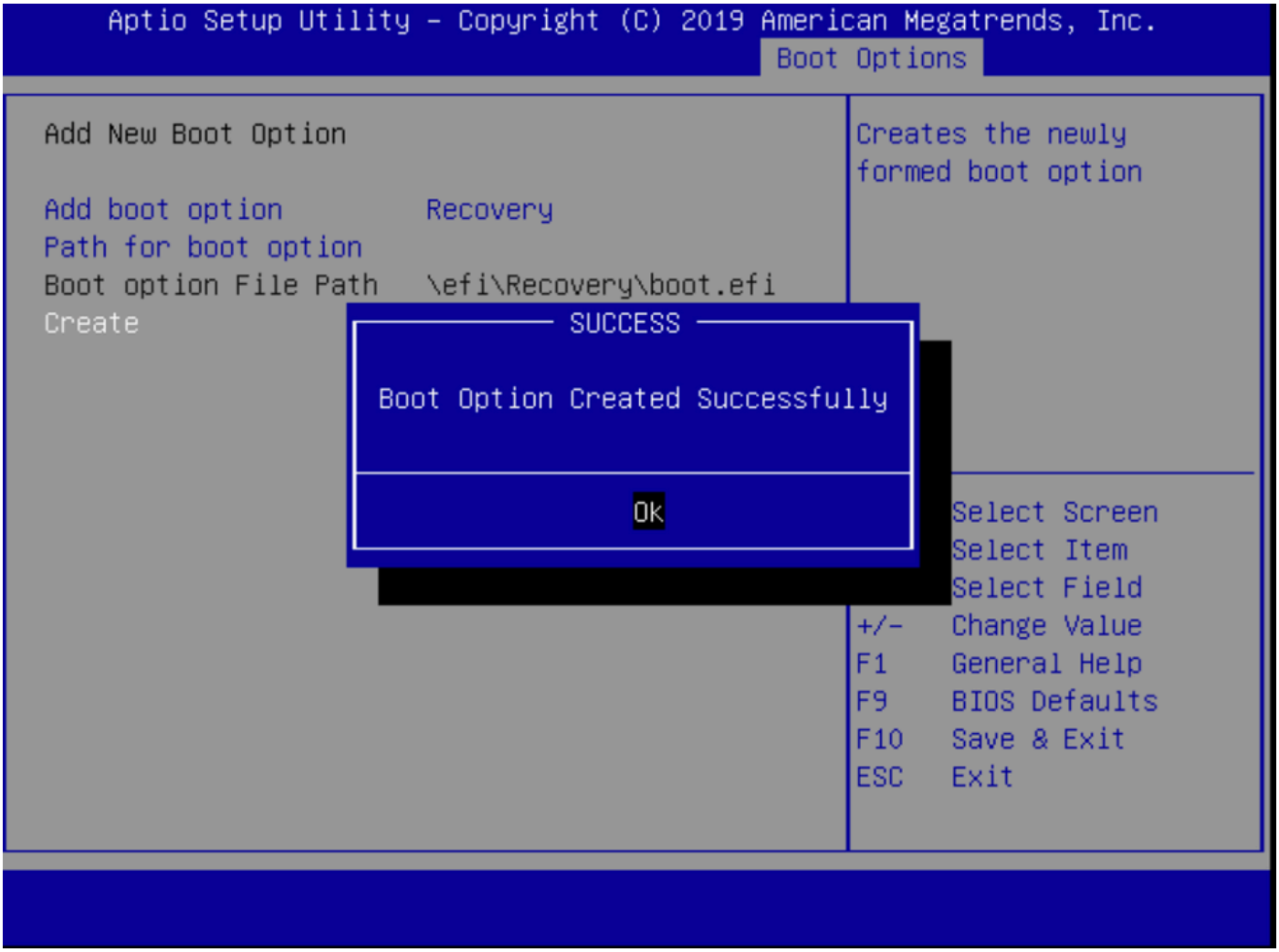


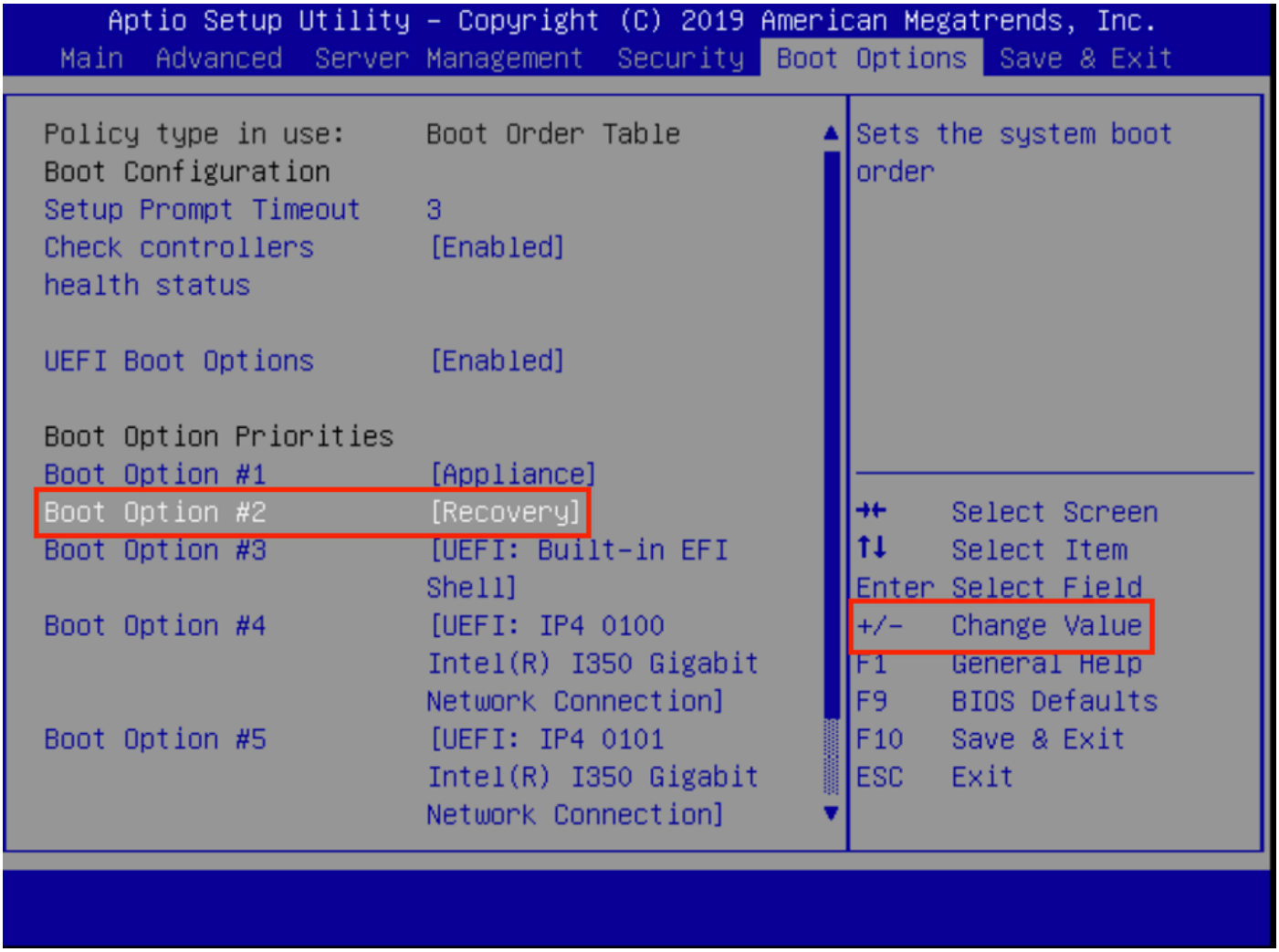

步骤9.选择“创**建**”。



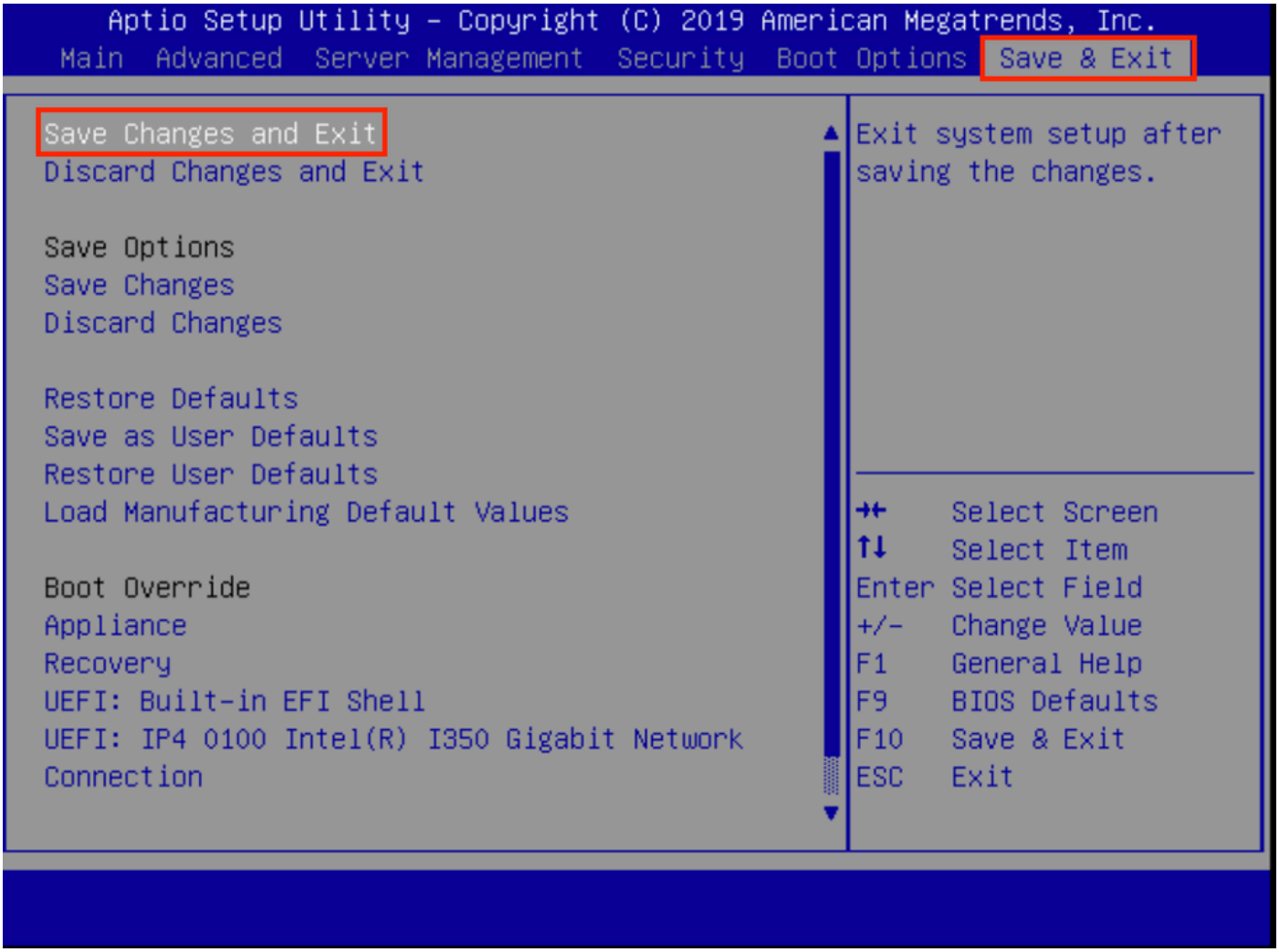

步骤10.创建新的引导选项。



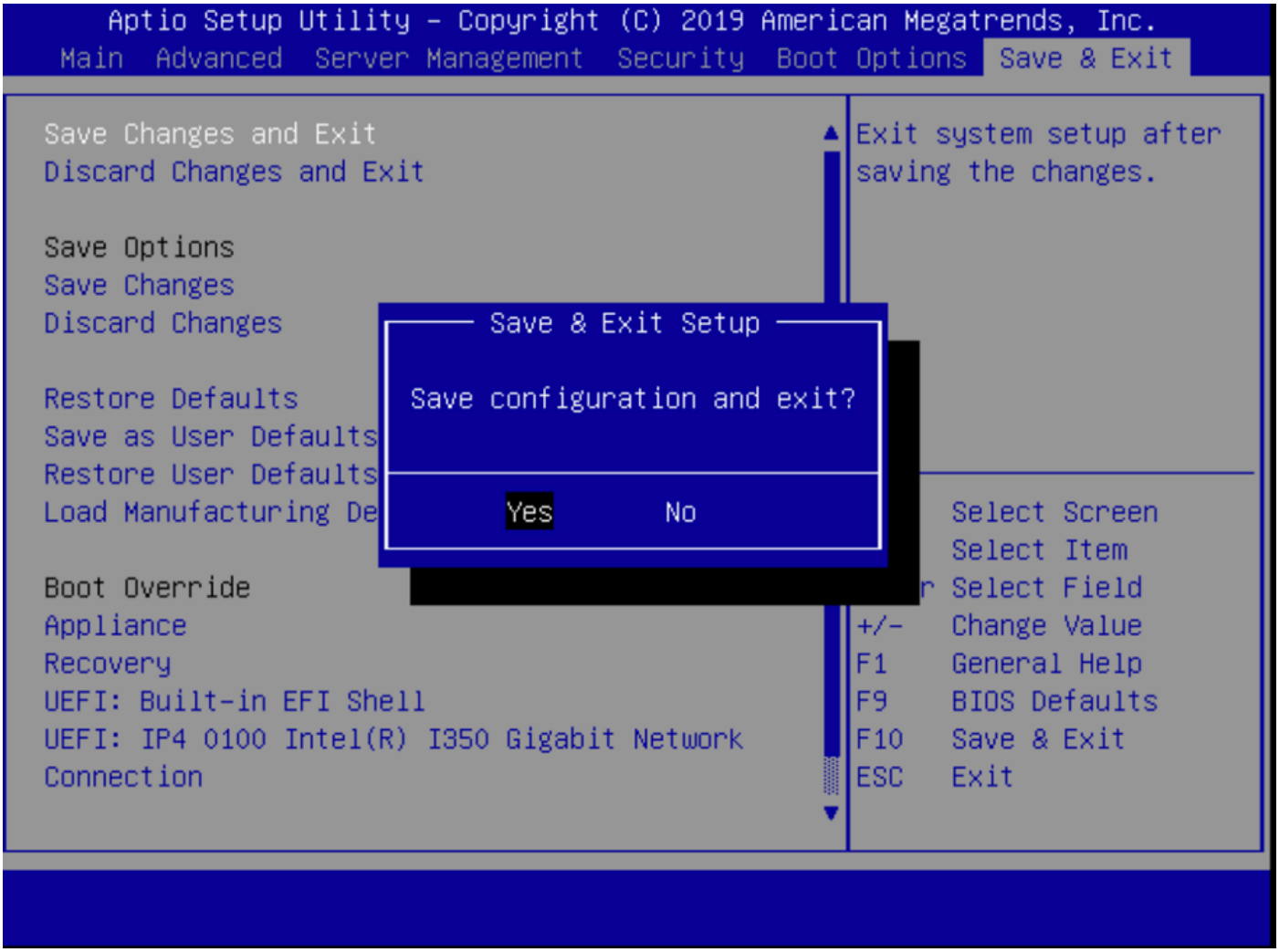

步骤12.将“恢**复**”选项放在#2处，**并带有+/ — 按钮**。




步骤13.导航至“保**存并退出”，**然后选**择“保存更改并退出**”。


Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc.
Main Advanced Server Management Security Boot Options Save & Exit
Save Changes and Exit
Discard Changes and Exit
Save Options
Save Changes
Discard Changes
Restore Defaults
Save as User Defaults
Restore User Defaults
Load Manufacturing Default Values
Boot Override
Appliance
Recovery
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
Exit system setup after saving the changes.
→← Select Screen
↑↓ Select Item
Enter Select Field
+/- Change Value
F1 General Help
F9 BIOS Defaults
F10 Save & Exit
ESC Exit

步骤14.确认更改。




步骤15.设备正常启动。

有关详细信息，请参阅安全恶意软件分析设备管理指南。