

# 如何使用EFI Shell將安全惡意軟體分析裝置引導至恢復模式並將恢復模式新增到引導選項

## 目錄

[簡介](#)

[問題](#)

[解決方案](#)

[EFI外殼](#)

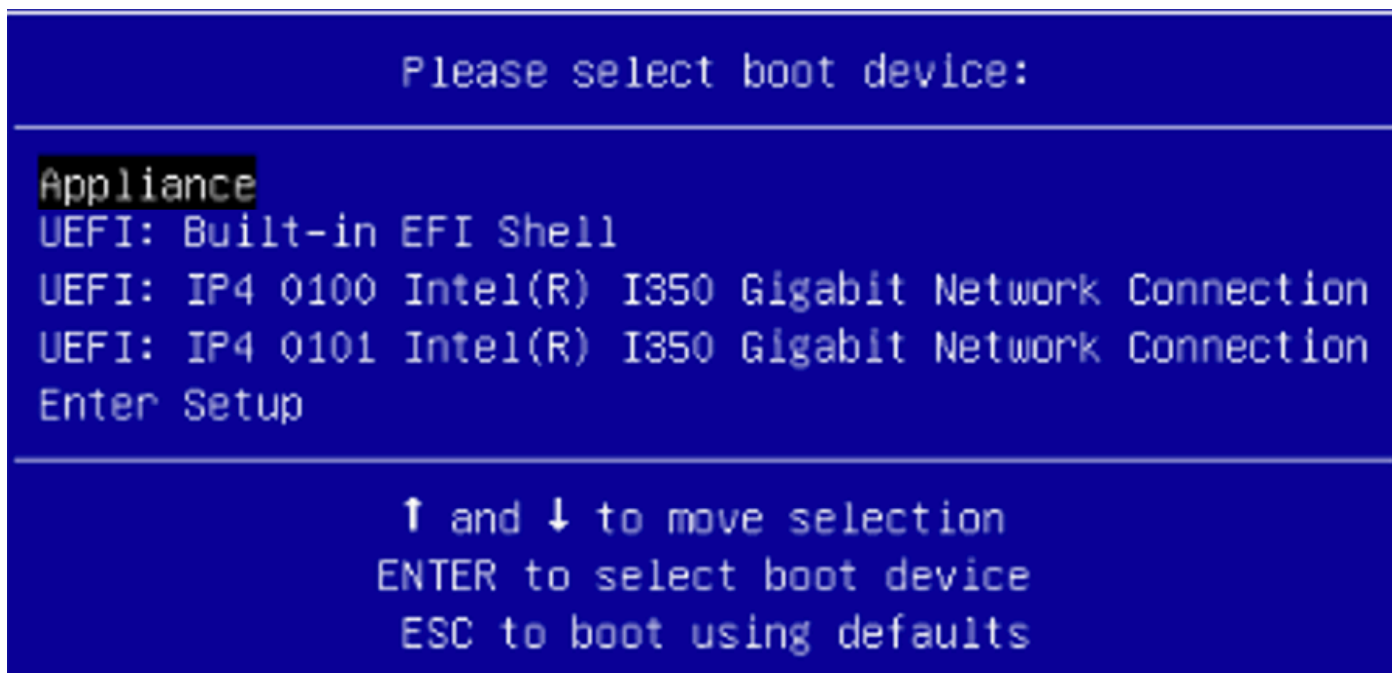
[將恢復模式新增到引導選項](#)

## 簡介

本文檔介紹如何使用EFI Shell將Secure Malware Analytics®裝置引導至恢復模式並將恢復模式新增到引導選項的步驟。

## 問題

您可以看到如下圖所示，BIOS視窗中未顯示恢復模式：



在此案例中，為了能夠引導進入恢復模式，必須使用下一節中介紹的步驟。

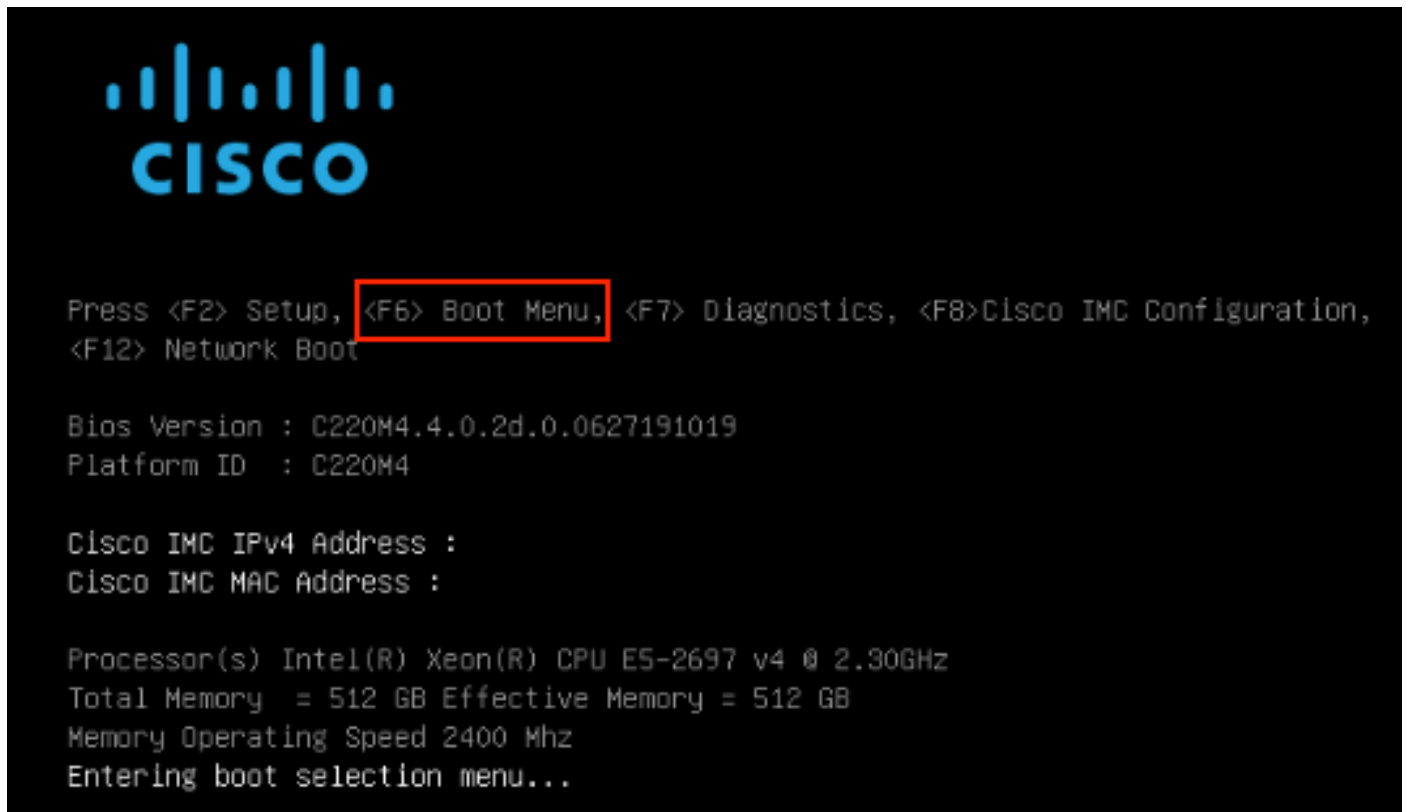
## 解決方案

### EFI外殼

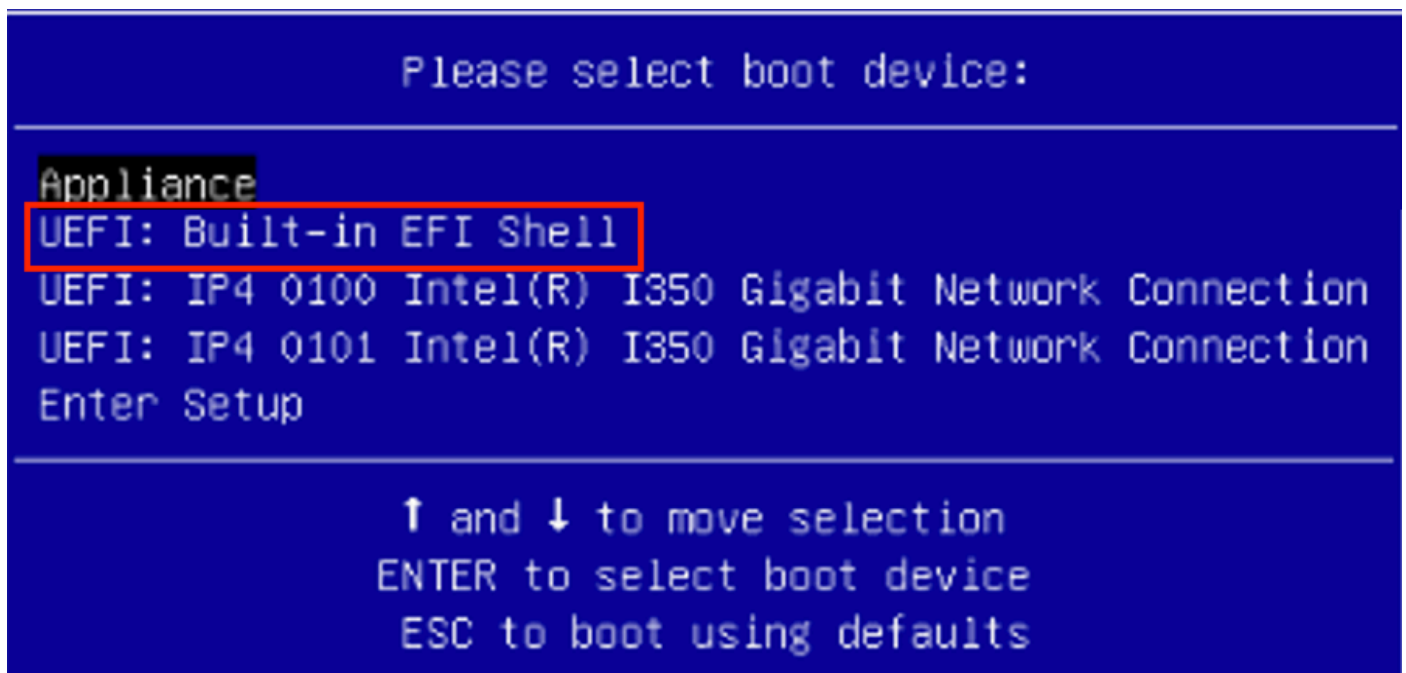
步驟1.將KVM介面卡連線到外部顯示器和鍵盤，並將其插入裝置前面的KVM埠。如果CIMC可用且已配置，則可以使用遠端KVM。

步驟2.重新啟動裝置。

步驟3.在BIOS視窗中按F6獲取可能的引導目標清單。



步驟4.選擇UEFI:內建EFI外殼。



步驟5.在此之後，請在啟動指令碼完成之前按ESC以移入EFI Shell。

## 步驟6. 可用檔案系統的清單。

```
UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x0005000B). 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,7303FEC6-7E81-4D8B-961C-AE562681960F,0x800,0x400000)
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-EB15CD03805B,0x800,0x400000)
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,0x400800,0x4000000)
blk3: Alias(s):
  PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,GPT,D5A6A81E-85F9-464B-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> _
```

## 步驟7. 此時，您需要找到位於其中一個檔案系統中的Recovery目錄。

## 步驟8. 導航到該目錄。

```
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)
```

## 步驟9. 執行命令fs1:\efi\Recovery\boot.efi

步驟10.裝置啟動至恢復模式。


```
>>
>>
>> help
COMMANDS:
  configure -- show|set: View or modify configuration variables
  comms     -- 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|address|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 -- single|with-reinstall: Nondestructively rerun configuration in single-user mode, with or without preceding 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
>>
```

## 將恢復模式新增到引導選項

步驟1.將KVM介面卡連線到外部顯示器和鍵盤，並將其插入裝置前面的KVM埠。如果CIMC可用且已配置，則可以使用遠端KVM。

步驟2.重新啟動裝置。

步驟3.在BIOS視窗中按F6獲取可能的引導目標清單。



```
CISCO

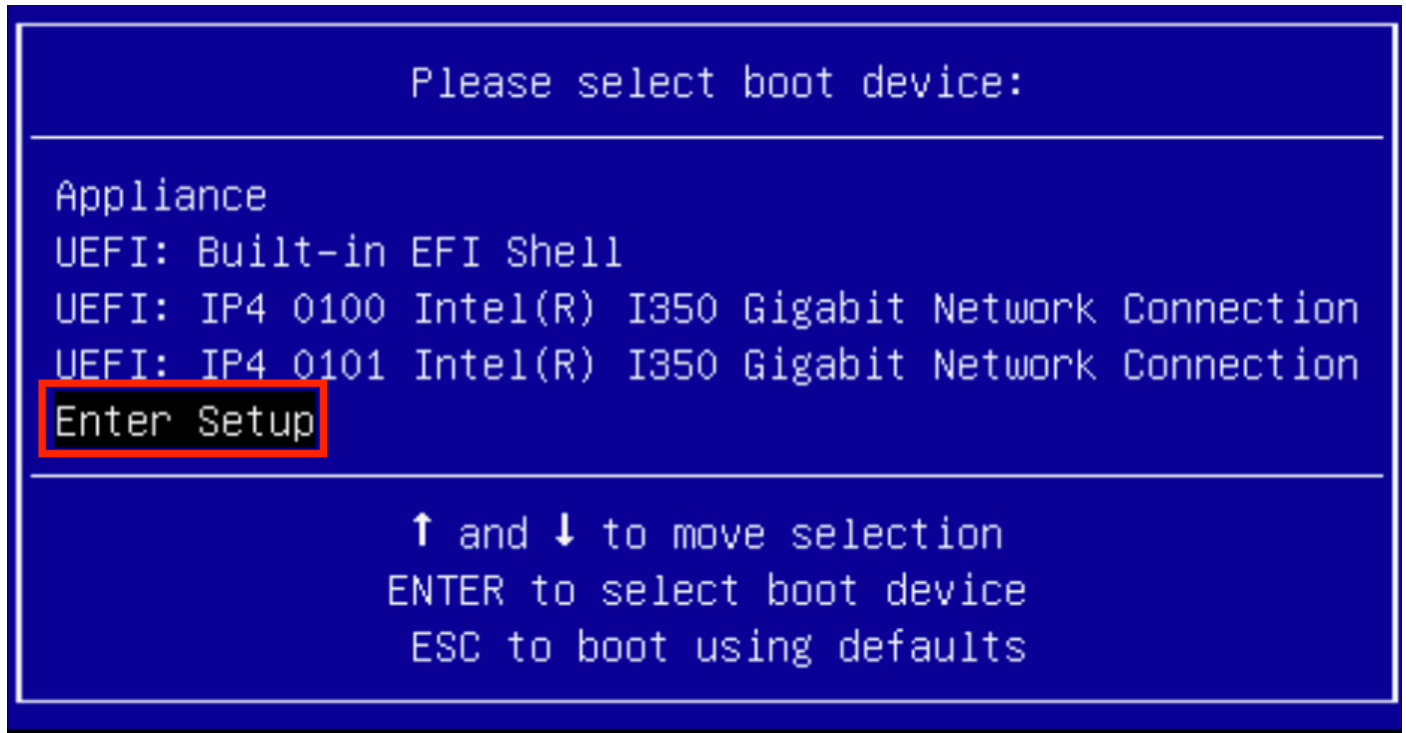
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M4.4.0.2d.0.0627191019
Platform ID  : C220M4

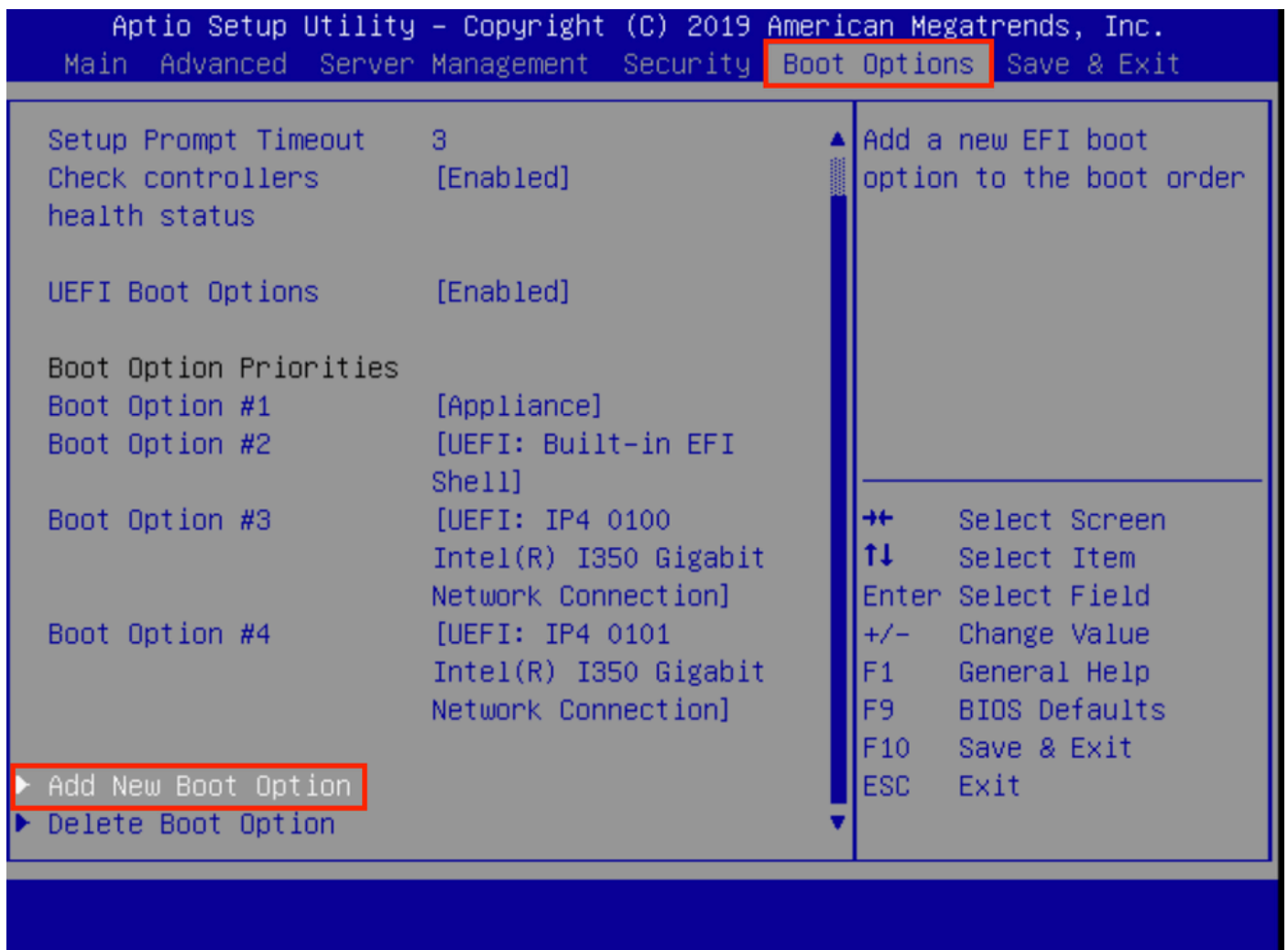
Cisco IMC IPv4 Address :
Cisco IMC MAC Address :

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz
Total Memory = 512 GB Effective Memory = 512 GB
Memory Operating Speed 2400 Mhz
Entering boot selection menu...
```

步驟4.選擇輸入設定。



步驟5.導覽至Boot Options，滾動至底部，然後選擇Add New Boot Option。



步驟6.選擇Add boot option，然後鍵入Recovery。

Add New Boot Option

Add boot option

Path for boot option

Boot option File Path

Create

Specify name for new boot option

Add boot option  
Recovery\_

→+ Select Screen  
↑↓ Select Item  
Enter Select Field  
+/- Change Value  
F1 General Help  
F9 BIOS Defaults  
F10 Save & Exit  
ESC Exit

步驟7.選擇Path for boot選項並選擇正確的File System。

Add New Boot Option

Add boot option

Recovery

Path for boot option

Boot option File Path

Enter the path to the  
boot option in the  
format

fsx:\path\filename.efi

Select a File System

PCI(2|2)\PCI(0|0)\DevicePath(Type 1, SubType 5)SCSI(0,0)\HD(Part1,Sig7303f

PCI(2|2)\PCI(0|0)\DevicePath(Type 1, SubType 5)SCSI(1,0)\HD(Part1,Sigc65af

↑↓ Select Item  
Enter Select Field  
+/- Change Value  
F1 General Help  
F9 BIOS Defaults  
F10 Save & Exit  
ESC Exit

步驟8.選擇<efi>、<Recovery>和<boot.efi>。

Select a File to Boot

&lt;efi&gt;

Select a File to Boot

---

<...>

<Recovery>

Select a File to Boot

---

<...>

boot.efi

步驟9.選擇Create。



Add New Boot Option

Creates the newly  
formed boot option

Add boot option

Recovery

Path for boot option

Boot option File Path

\efi\Recovery\boot.efi

**Create**

---

←→ Select Screen  
↑↓ Select Item  
Enter Select Field  
+/- Change Value  
F1 General Help  
F9 BIOS Defaults  
F10 Save & Exit  
ESC Exit

步驟10. 建立新引導選項。

Add New Boot Option

Creates the newly  
formed boot option

Add boot option            Recovery

Path for boot option

Boot option File Path    \efi\Recovery\boot.efi

Create

SUCCESS

Boot Option Created Successfully

OK

Select Screen

Select Item

Select Field

+/-    Change Value

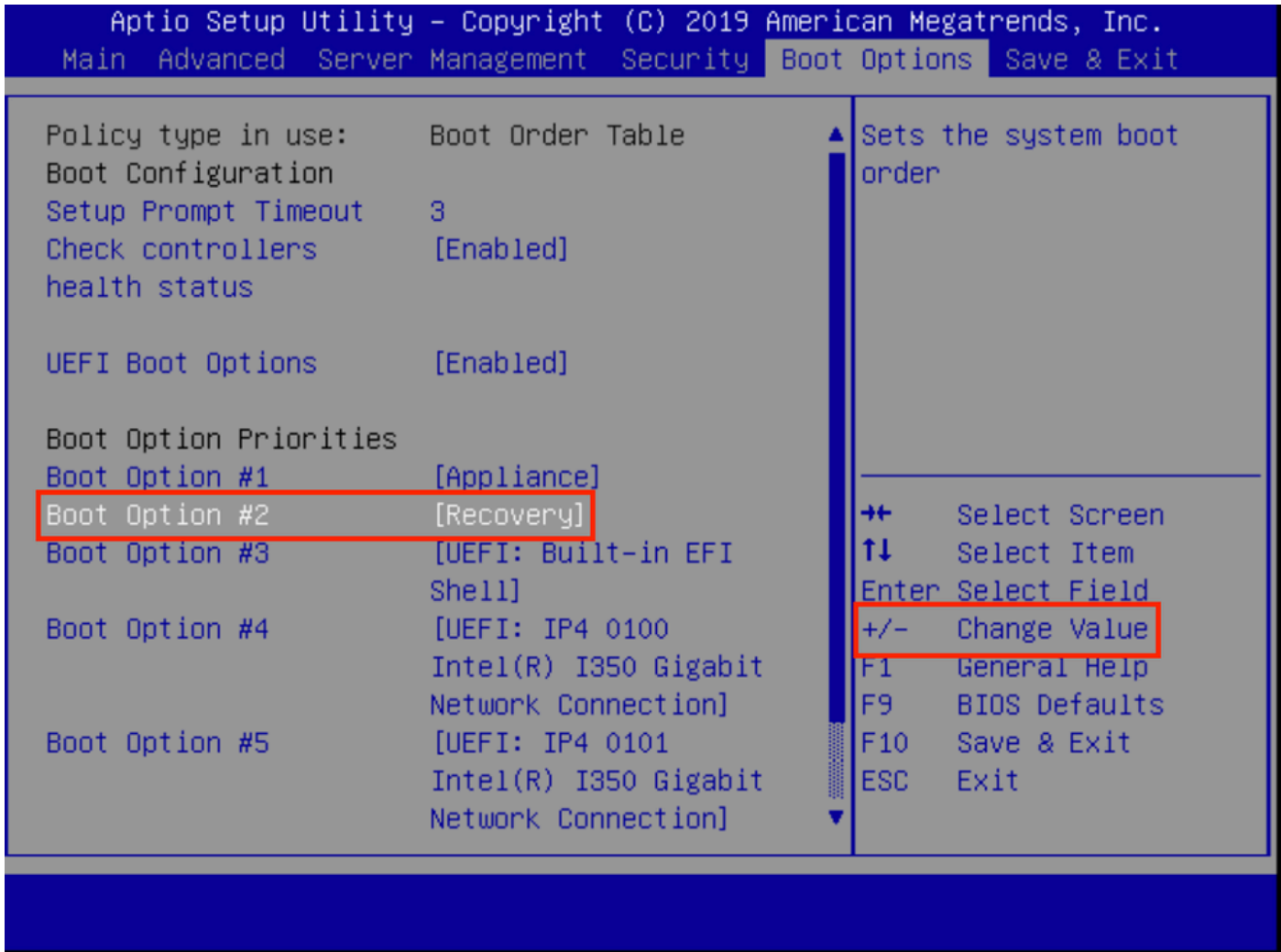
F1     General Help

F9     BIOS Defaults

F10    Save &amp; Exit

ESC    Exit

步驟12.使用+/- — 按#2將**Recovery**選項放在適當的位置。



步驟13.導覽至Save & Exit，然後選擇Save Changes and 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

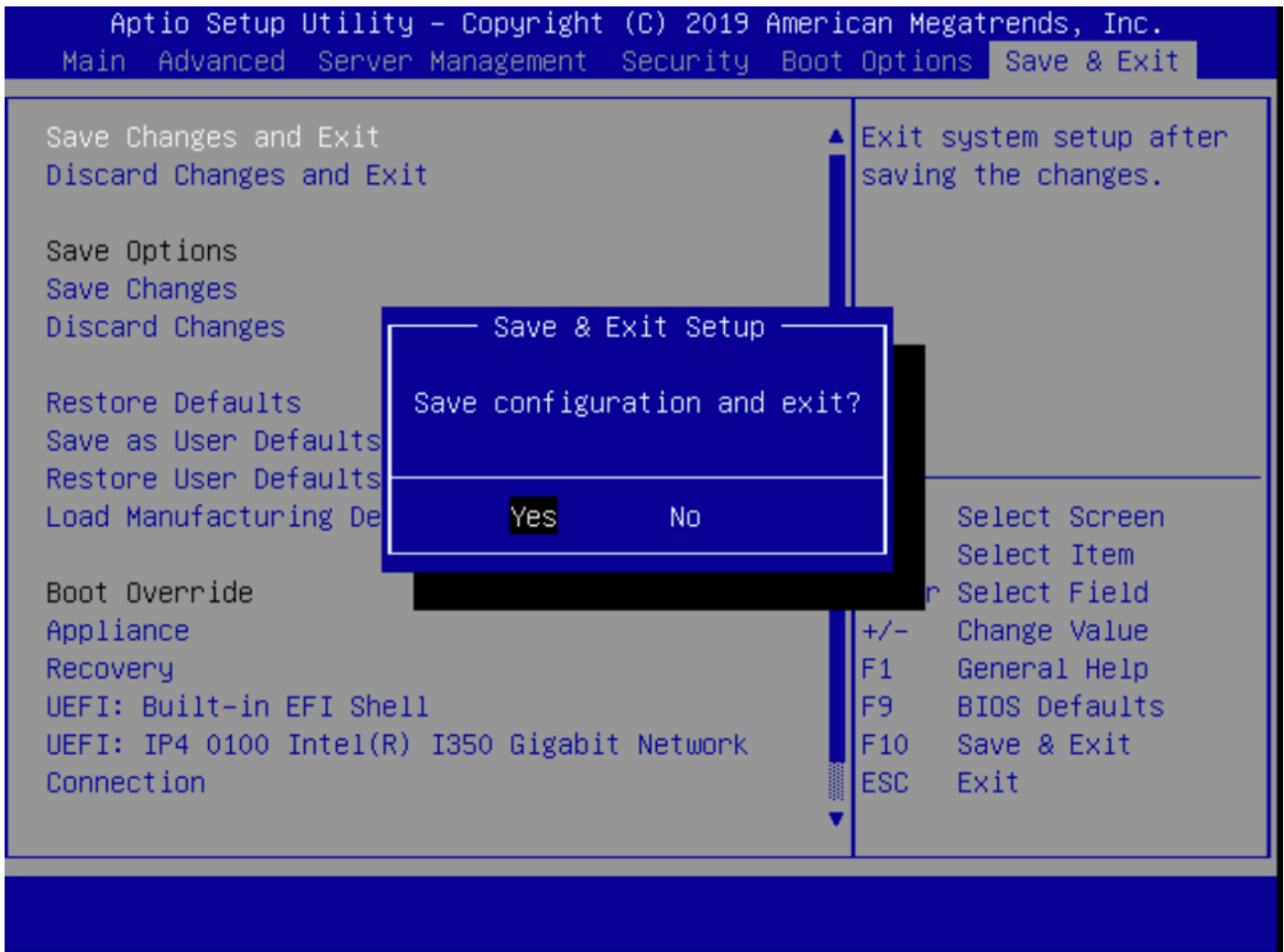
F1 General Help

F9 BIOS Defaults

F10 Save & Exit

ESC Exit

步驟14.確認更改。



步驟15.裝置正常啟動。

有關詳細資訊，請參閱[安全惡意軟體分析裝置管理指南](#)。