

# EFIシェルを使用してセキュアマルウェア分析アプライアンスを回復モードで起動し、回復モードをブートオプションに追加する方法

## 内容

[概要](#)

[問題](#)

[解決方法](#)

[EFIシェル](#)

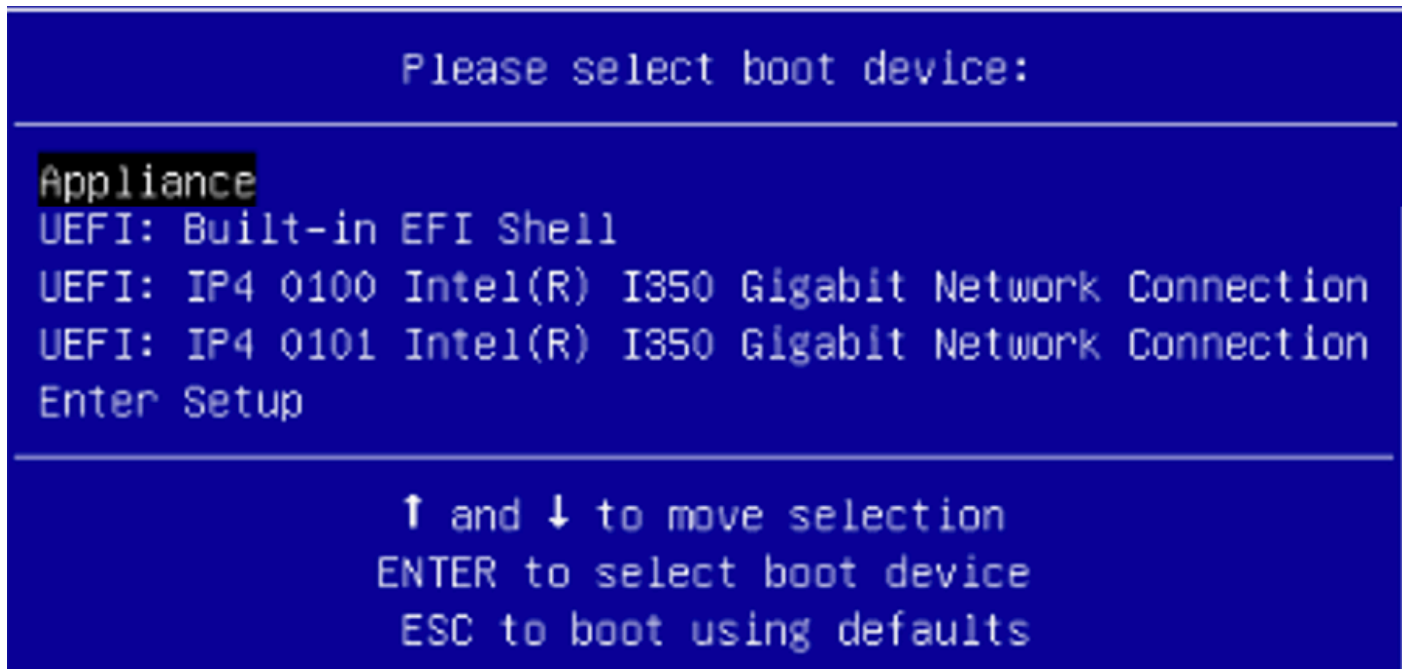
[ブートオプションへの回復モードの追加](#)

## 概要

このドキュメントでは、EFIシェルを使用してSecure Malware Analytics®アプライアンスをリカバリモードで起動し、回復モードをブートオプションに追加する手順について説明します。

## 問題

図に示すように、BIOSウィンドウにリカバリモードが表示されません。



このシナリオでリカバリモードで起動するには、次のセクションで説明する手順を使用する必要があります。

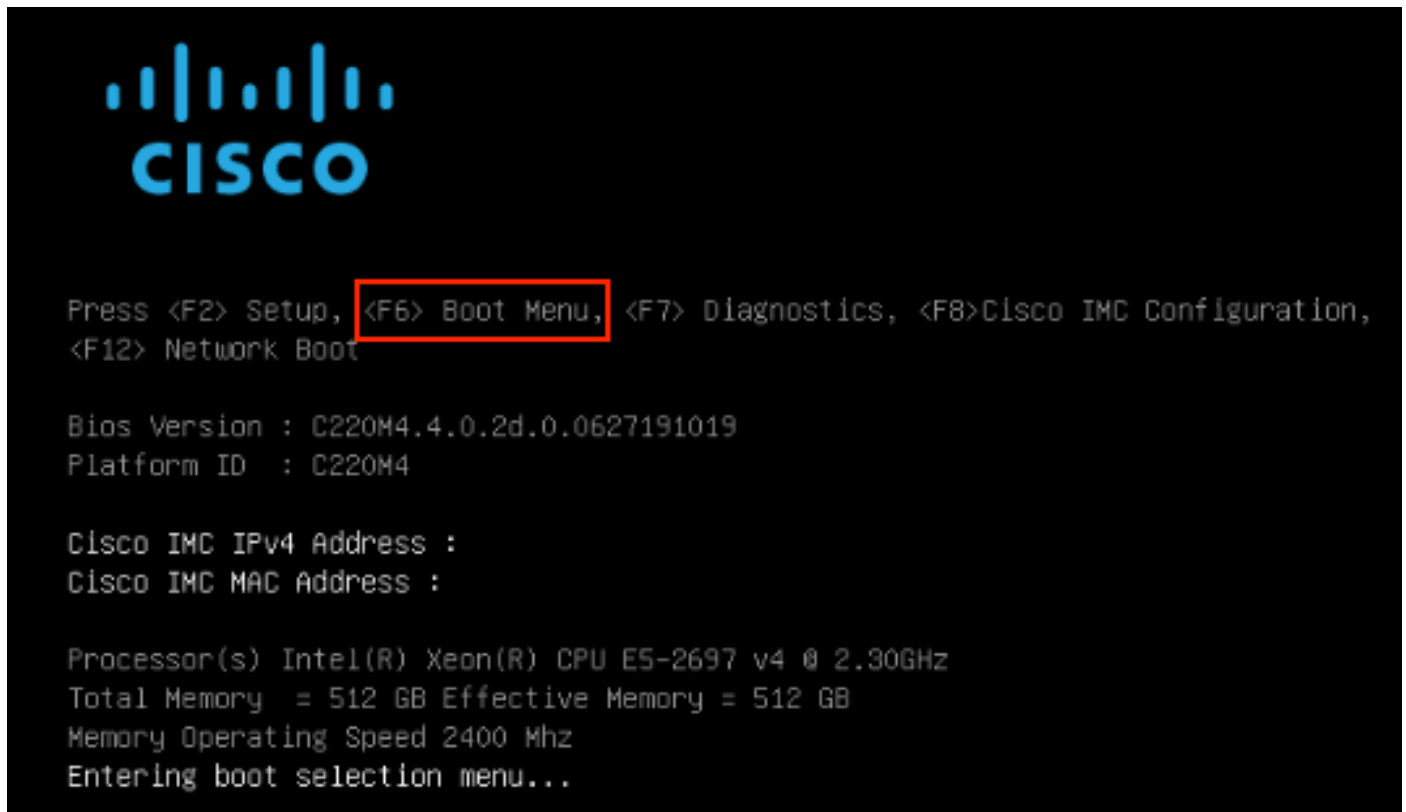
## 解決方法

### EFIシェル

ステップ1:KVMアダプタを外部モニタとキーボードに接続し、デバイスの前面にあるKVMポートに接続します。CIMCが使用可能で設定されている場合は、リモートKVMを使用できます。

ステップ2 : デバイスをリブートします。

ステップ3:BIOSウィンドウでF6キーを押して、可能なブートターゲットのリストを表示します。



```

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

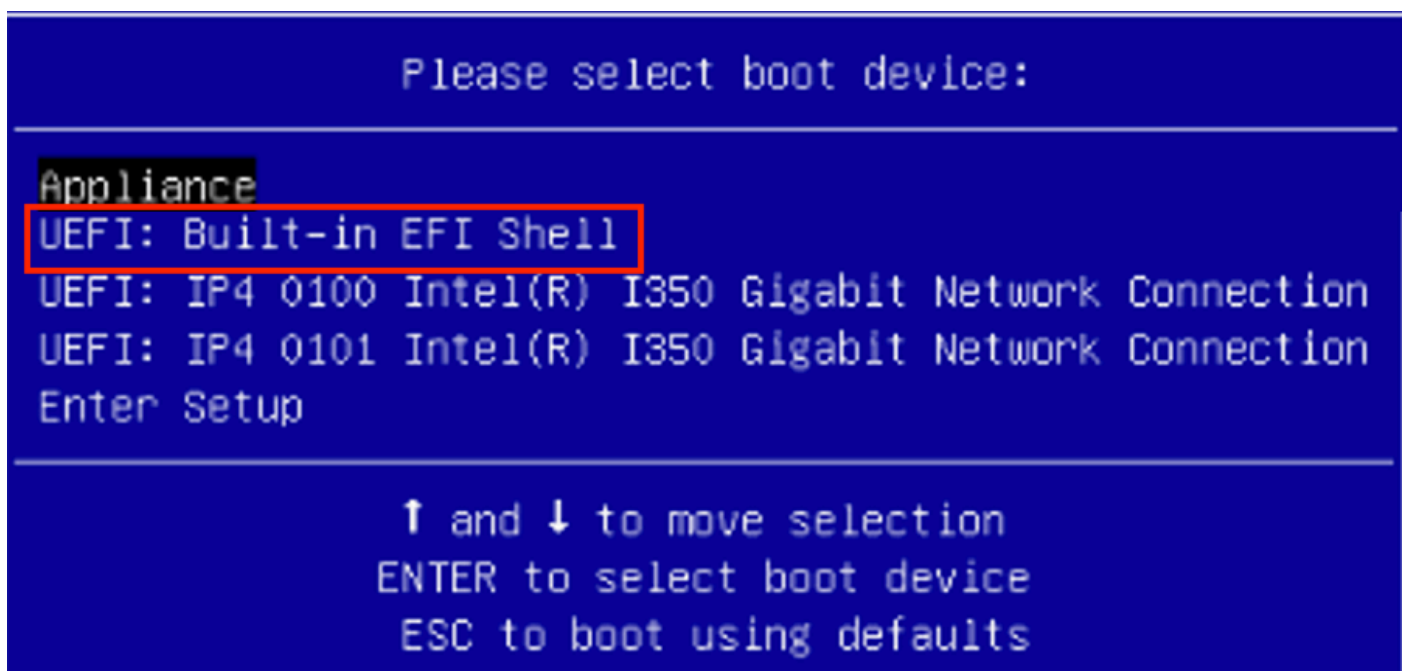
Bios Version : C220M4.4.0.2d.0.0627191019
Platform ID : C220M4

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...

```

ステップ4:[UEFI:組み込みのEFIシェル。



```

Please select boot device:

Appliance
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

```

ステップ5：直後に、起動スクリプトが終了する前にEscキーを押して、EFIシェルに移動します。

ステップ6：使用可能なファイルシステムのリスト。

```
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-AE5626B1960F,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-EB15CD038D5B,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,900A83C7-04F4-44C3-B603-35D2DCC6249F,0x400800,0x400000)
blk3: Alias(s):
  PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,GPT,D5A6A81E-85F9-464B-9277-3E4A89B43D65,0x800800,0x05A6FDF)
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>
```

ステップ7：この時点で、ファイル・システムの1つに含まれるRecoveryディレクトリを見つける必要があります。

ステップ8：そのディレクトリに移動します。

```
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)
```

ステップ9 : コマンドfs1:\efi\Recovery\boot.efiを実行します

ステップ10 : デバイスが回復モードで起動します。

```
>>
>>
>> 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|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
>>
```

## ブートオプションへの回復モードの追加

ステップ1:KVMアダプタを外部モニタとキーボードに接続し、デバイスの前面にあるKVMポートに接続します。CIMCが使用可能で設定されている場合は、リモートKVMを使用できます。

ステップ2 : デバイスをリブートします。

ステップ3:BIOSウィンドウでF6キーを押して、可能なブートターゲットのリストを表示します。



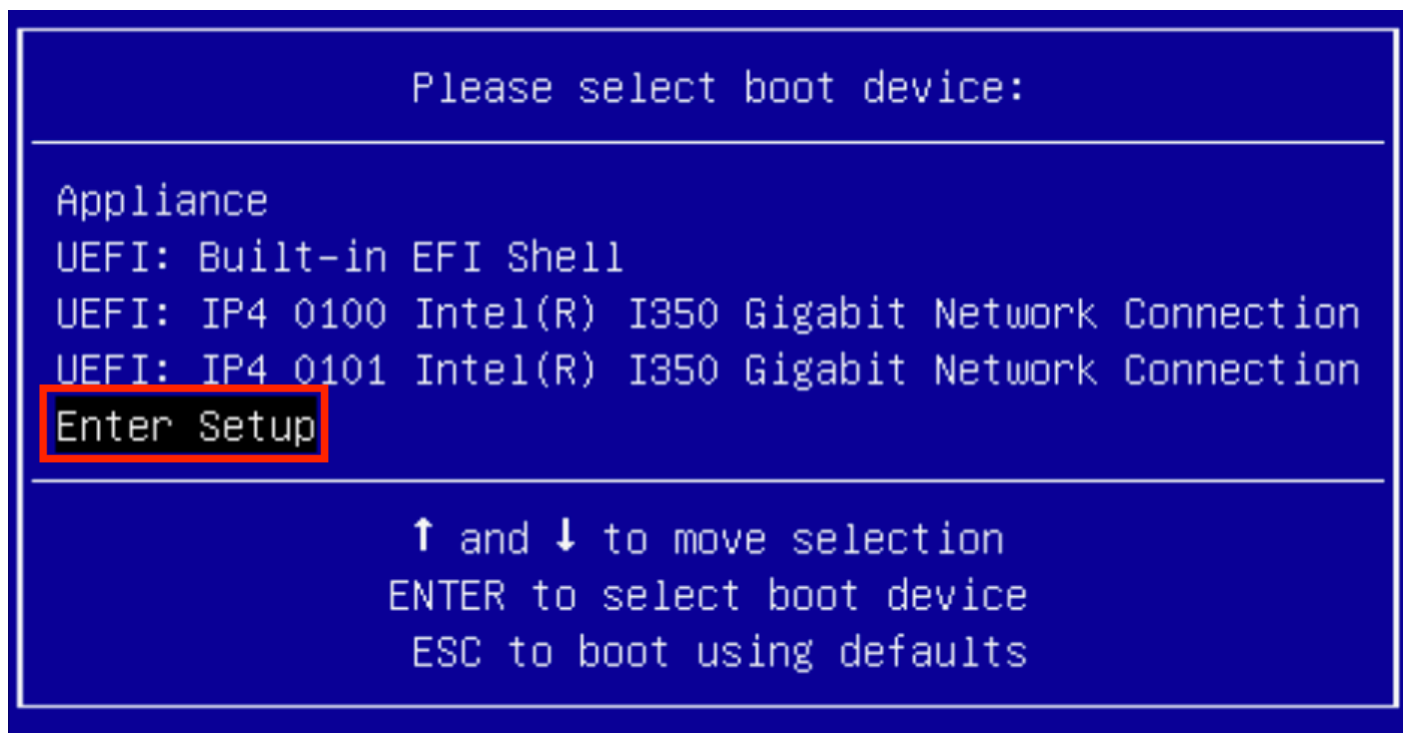
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,  
<F12> Network Boot

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

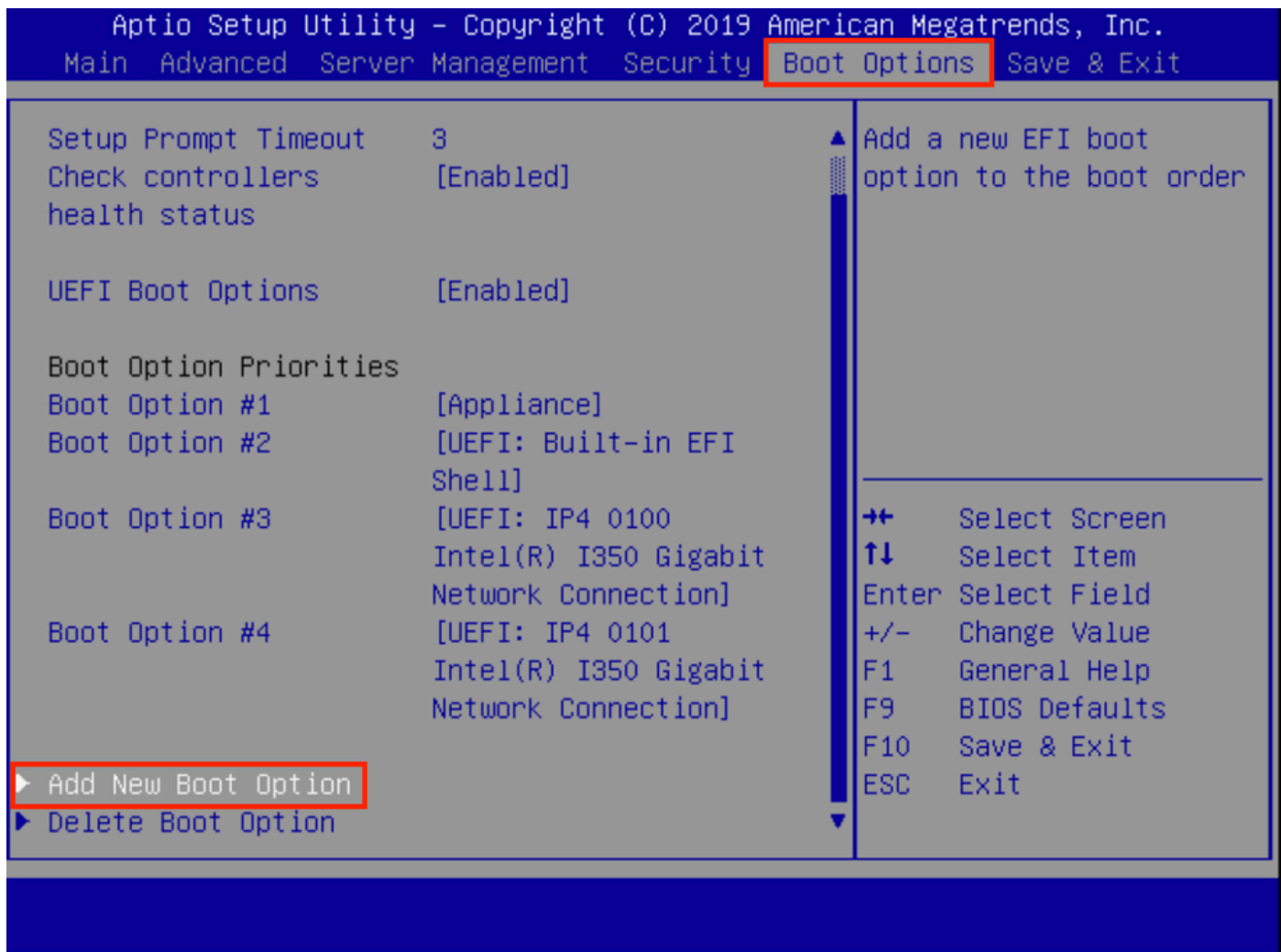
Cisco IMC IPv4 Address :  
Cisco IMC MAC Address :

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...

ステップ4:[Enter Setup]を選択します。



ステップ5:[Boot Options]に移動し、下にスクロールして、[Add New Boot Option]を選択します。



ステップ6:[Add boot]オプションを選択し、Recoveryと入力します。

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

ステップ7:[Path for boot]オプションを選択し、適切なファイル・システムを選択します。

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

ステップ8:<efi>、<Recovery>および<boot.efi>を選択します。

Select a File to Boot

&lt;efi&gt;



Select a File to Boot

---

<...>

<Recovery>

Select a File to Boot

---

<...>

boot.efi

ステップ9:[Create]を選択します。

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

ステップ10 : 新しいブートオプションが作成されます。

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

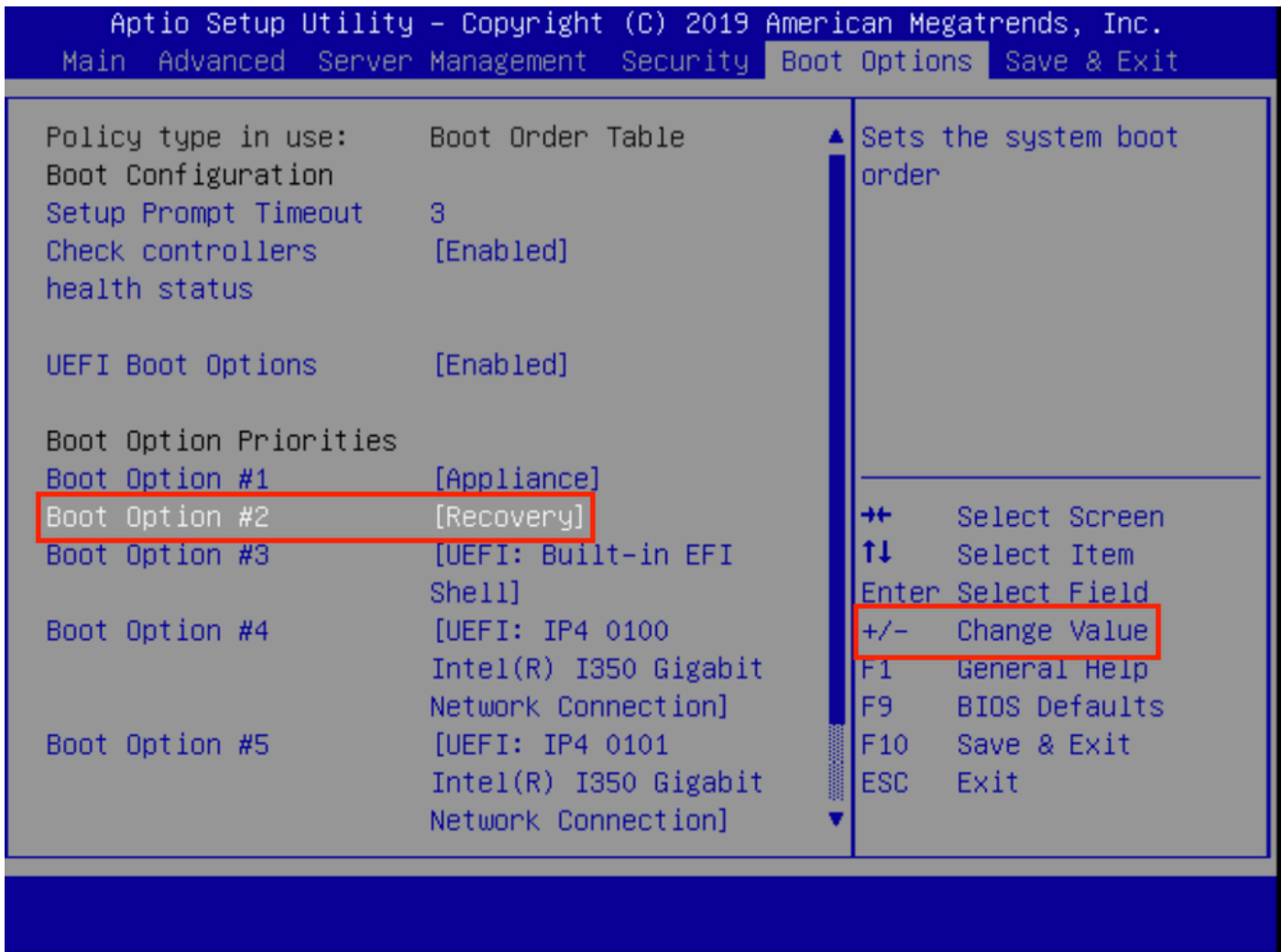
F1     General Help

F9     BIOS Defaults

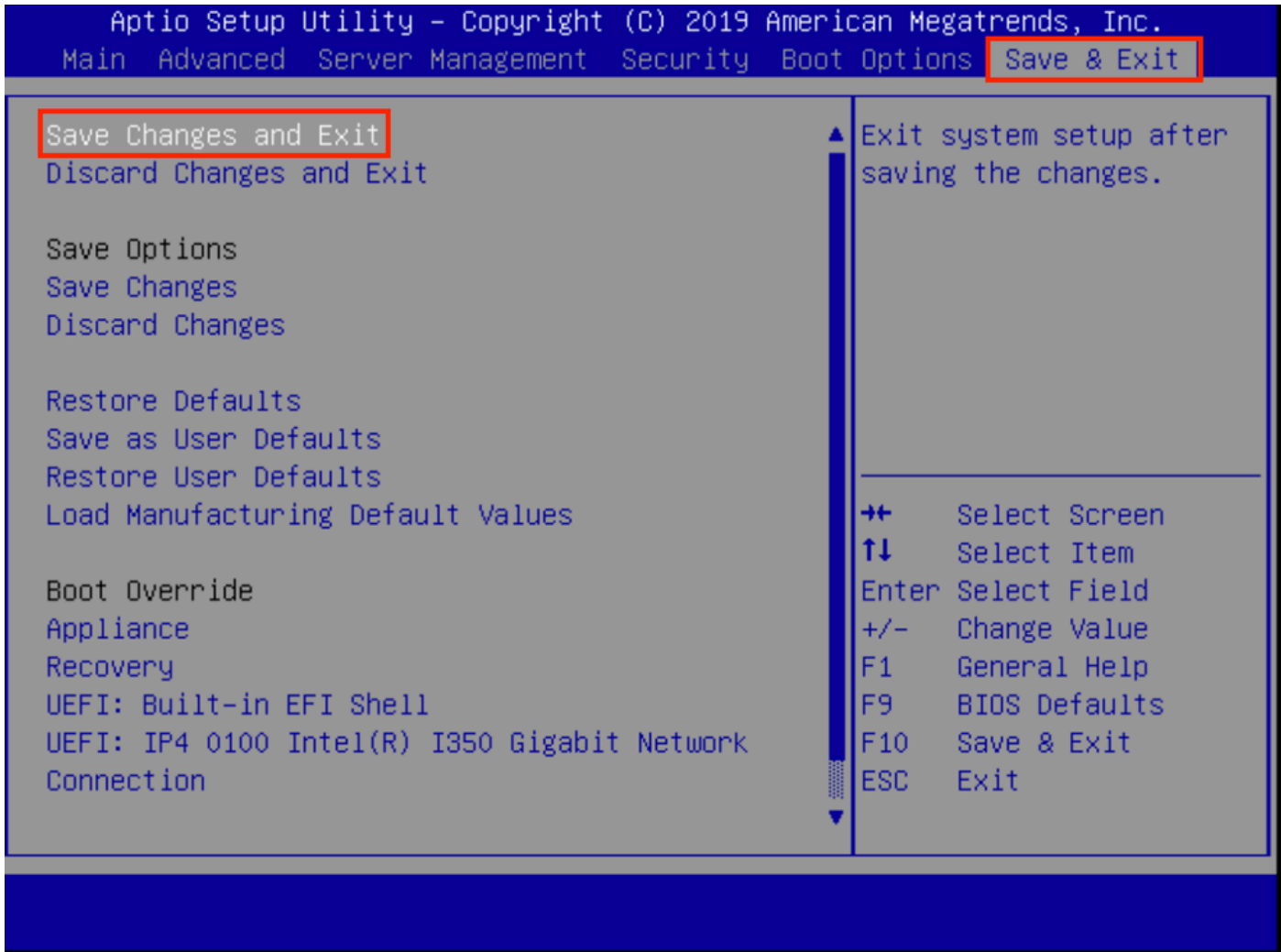
F10    Save &amp; Exit

ESC    Exit

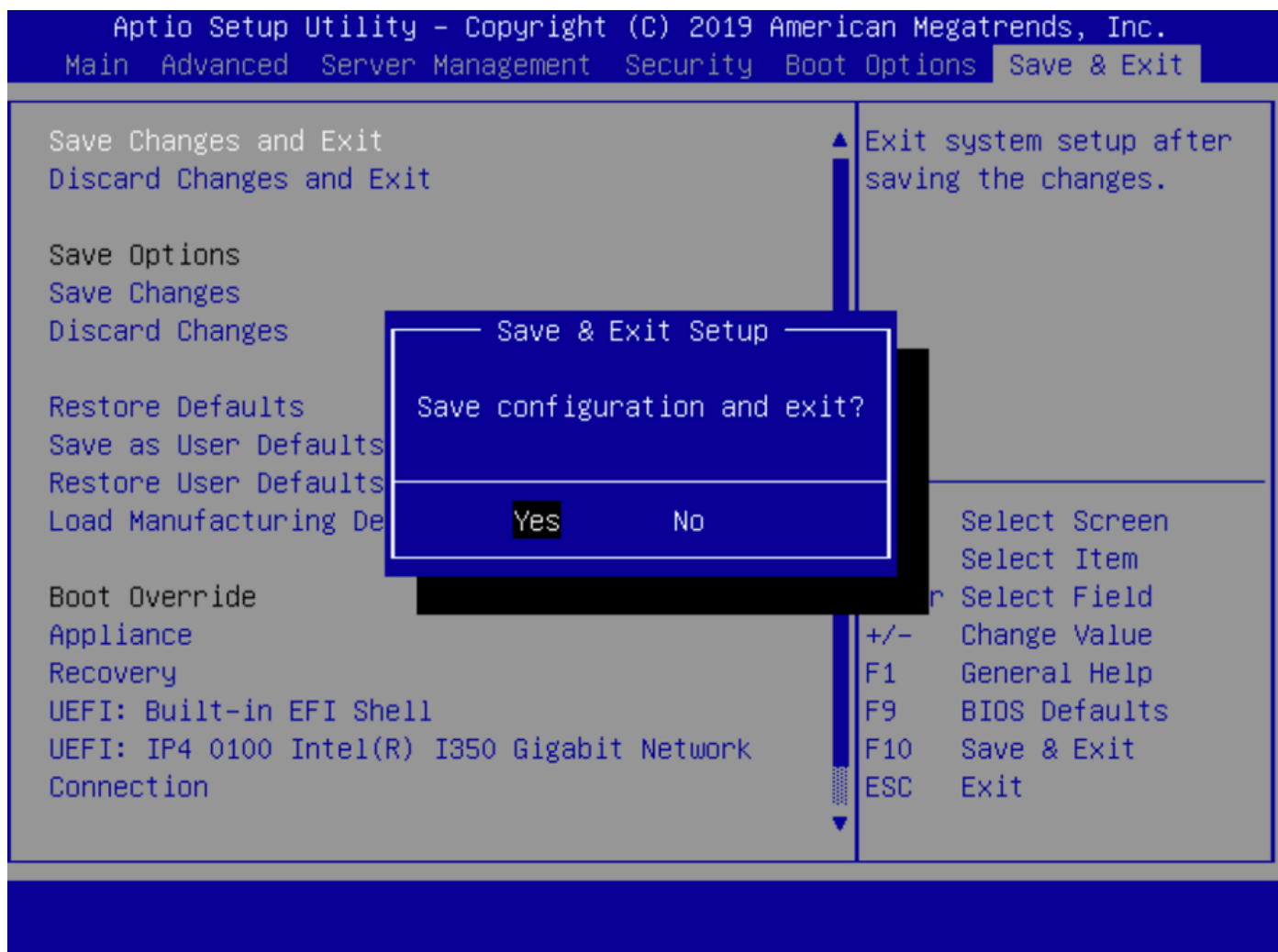
ステップ12:+/- ボタンを使用して、#2の場所にリカバリオプションを配置します。



ステップ13:[Save & Exit]に移動し、[Save Changes and Exit]を選択します。



ステップ14 : 変更を確認します。



ステップ15 : デバイスが正常にブートします。

詳細については、『[Secure Malware Analytics Appliance Administration Guide](#)』を[参照してください](#)。  
[さい](#)。