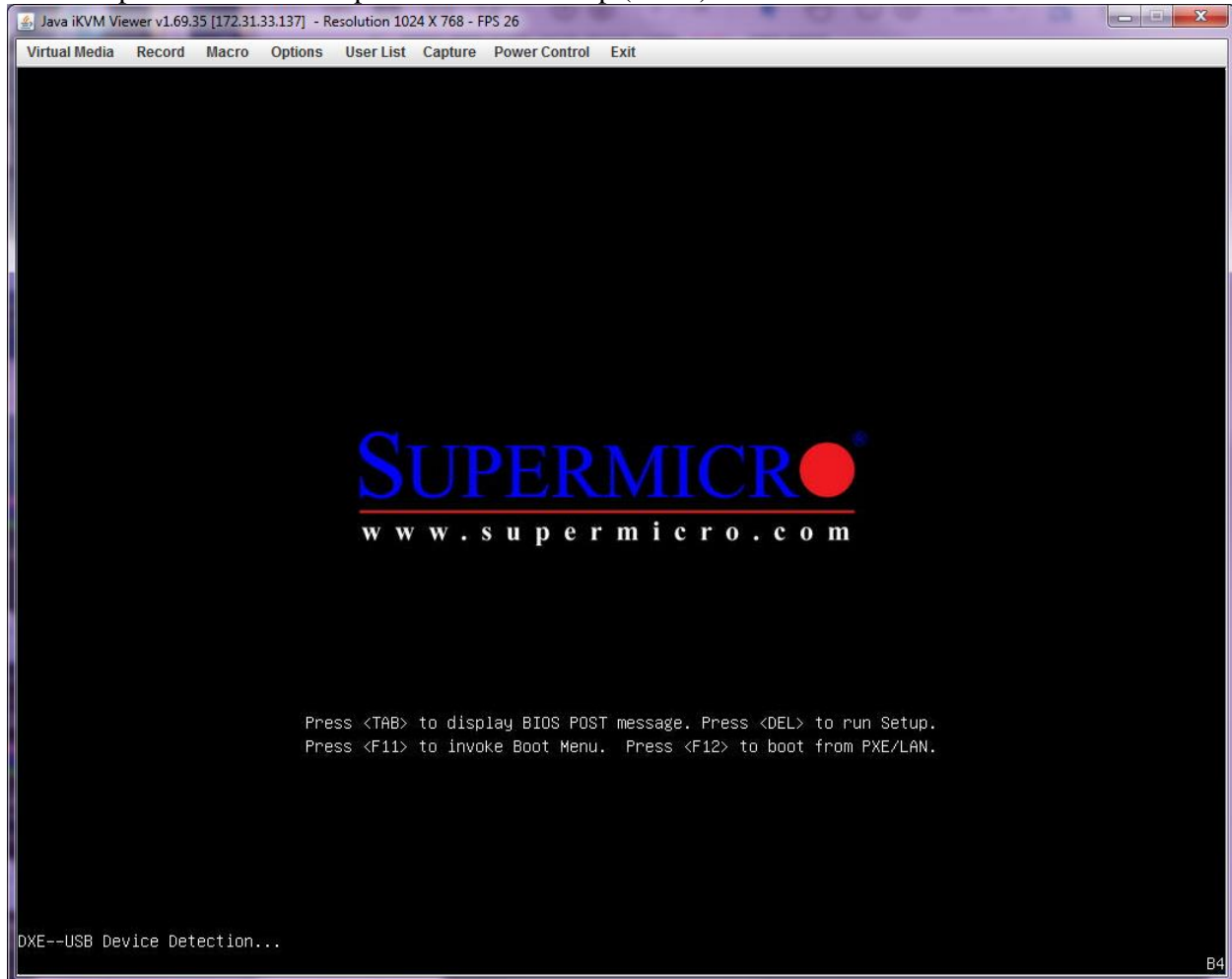


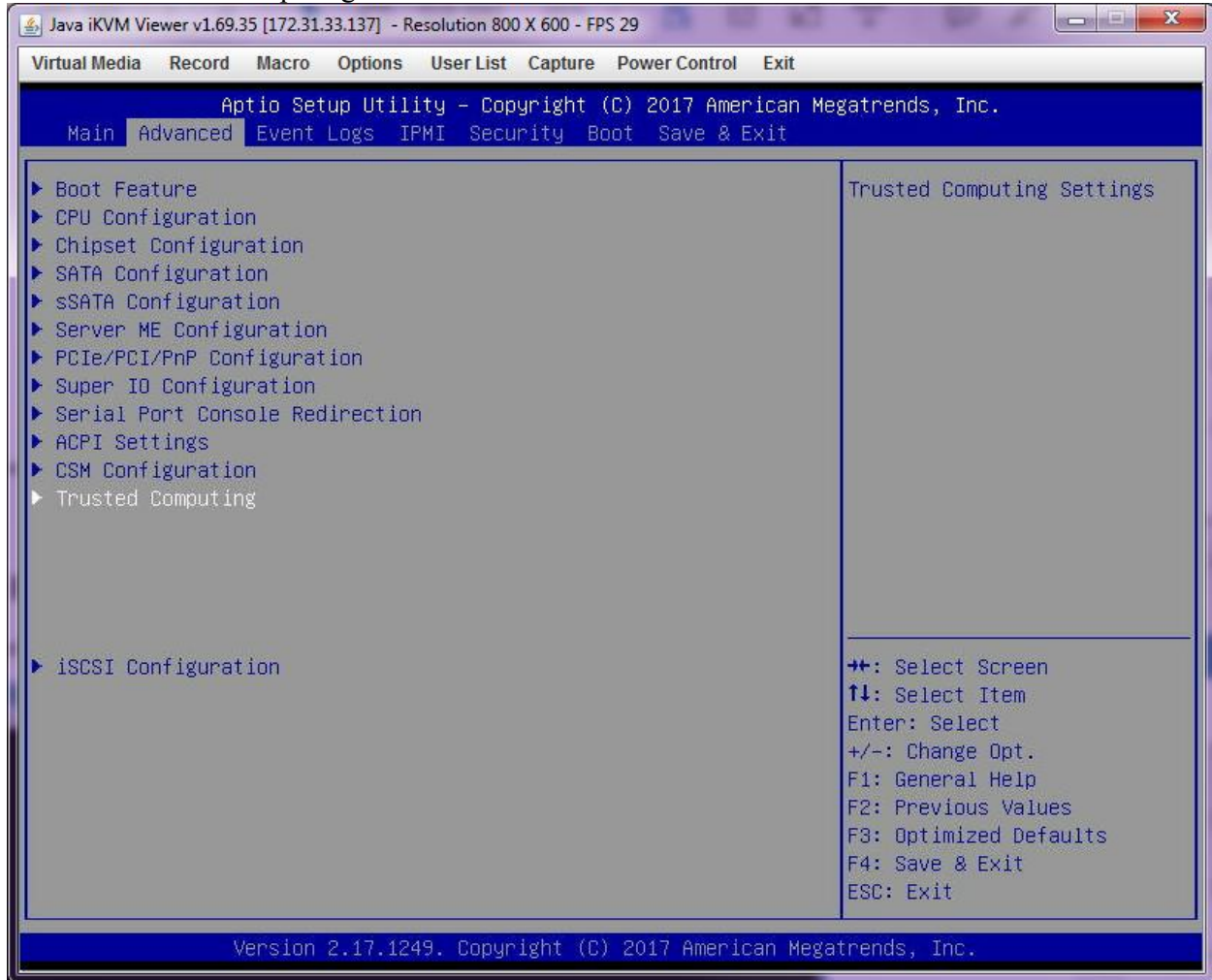
AOM-TPM-9655V/AOM-TPM-9655H
AOM-TPM-9655V/AOM-TPM-9655H
Firmware Change
For Use with UEFI

9655 (TPM1.2) Firmware Update

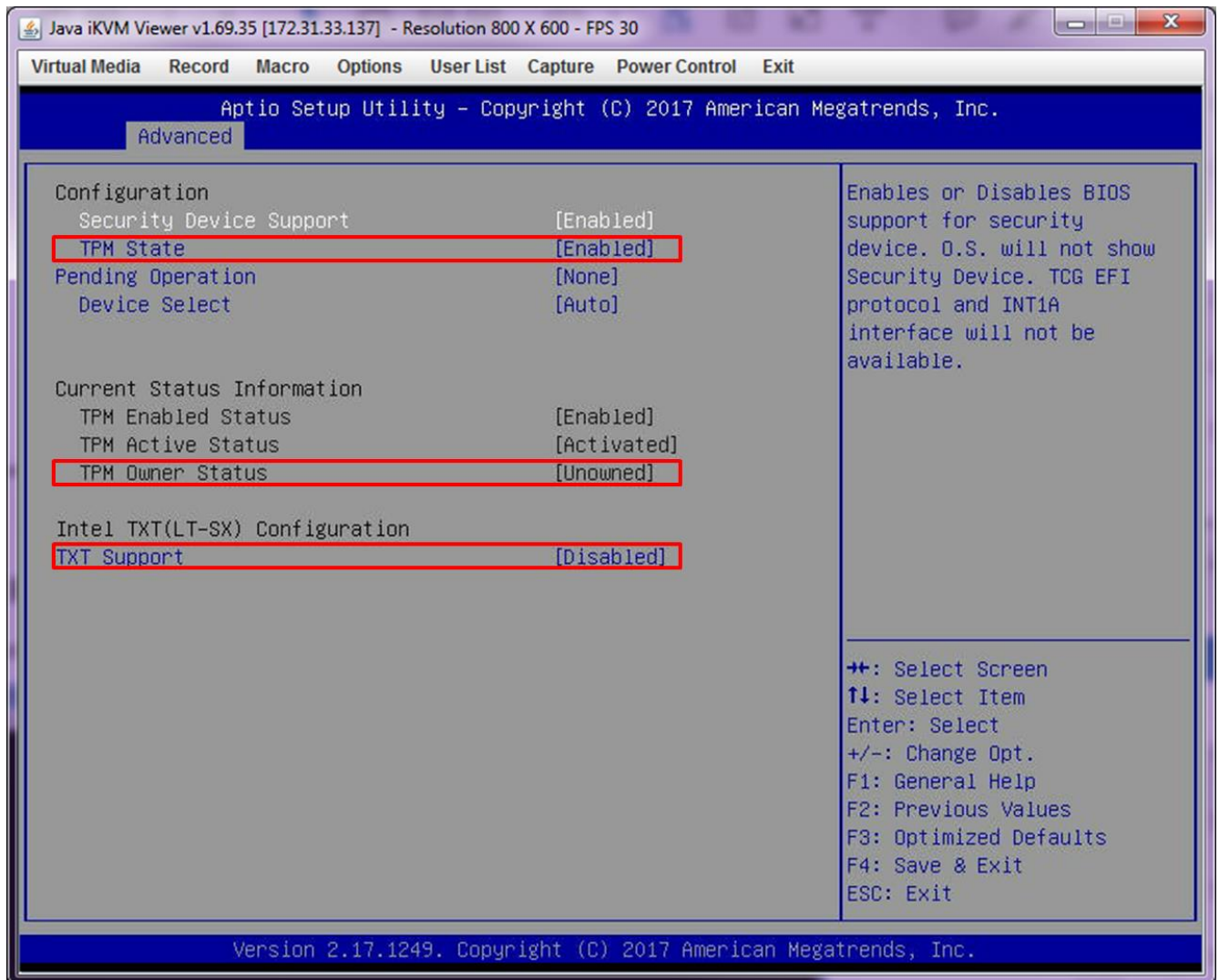
1. Boot up motherboard and press DEL into Setup (BIOS)



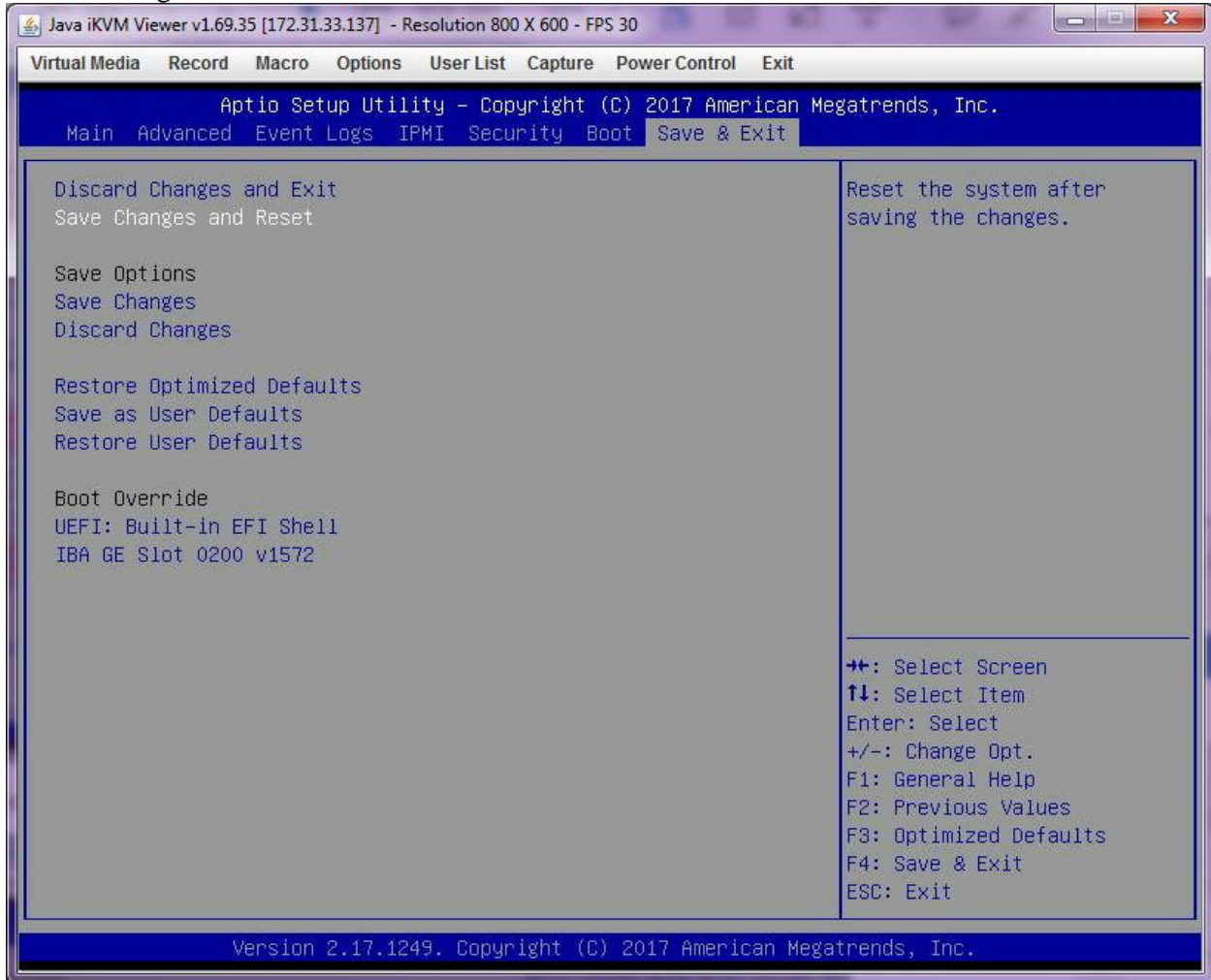
2. Go to “Trusted Computing” under Advanced



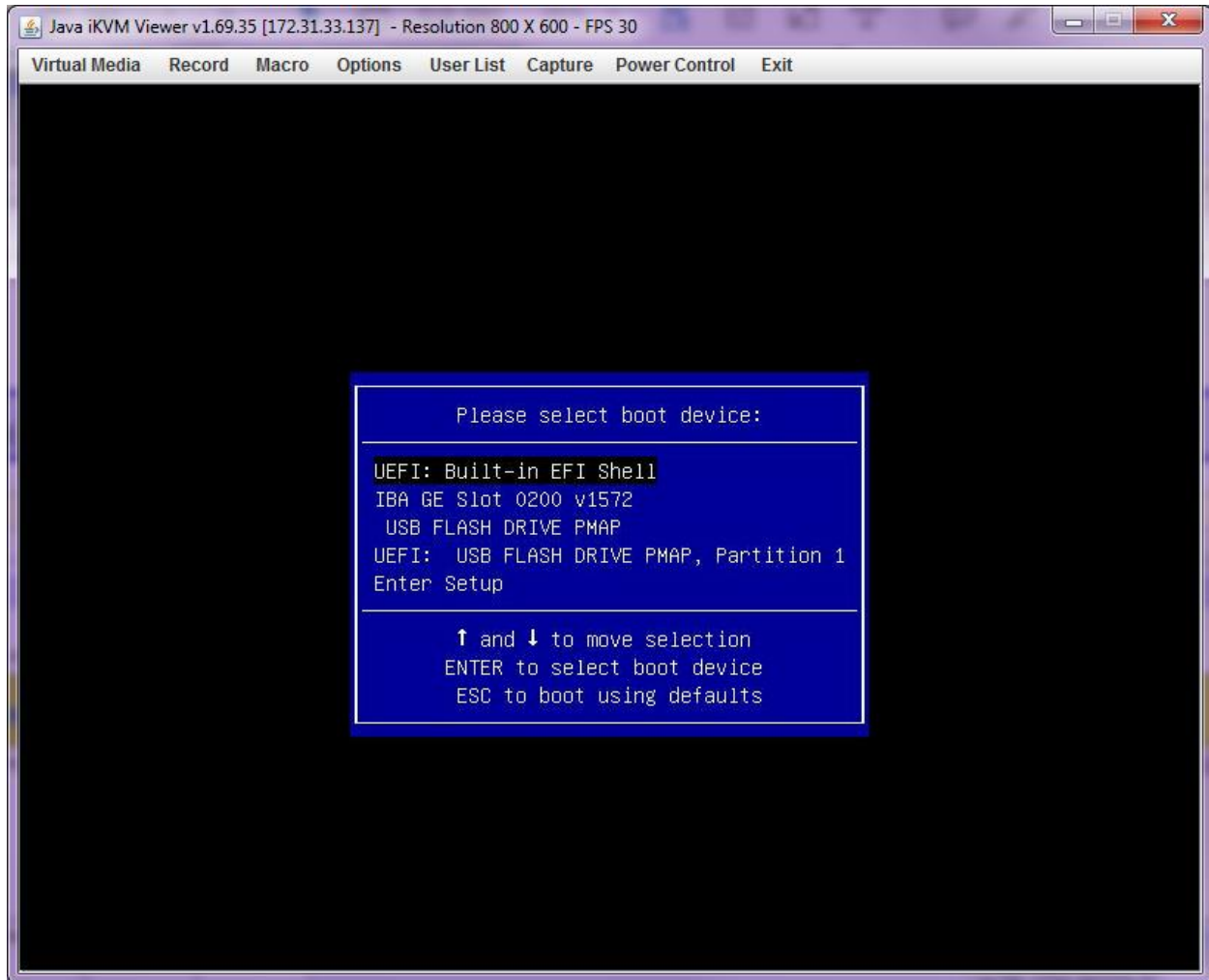
3. Make sure “TPM State” is enable, “TPM Owner Status” is “Unowned” and “TXT Support” is disable.



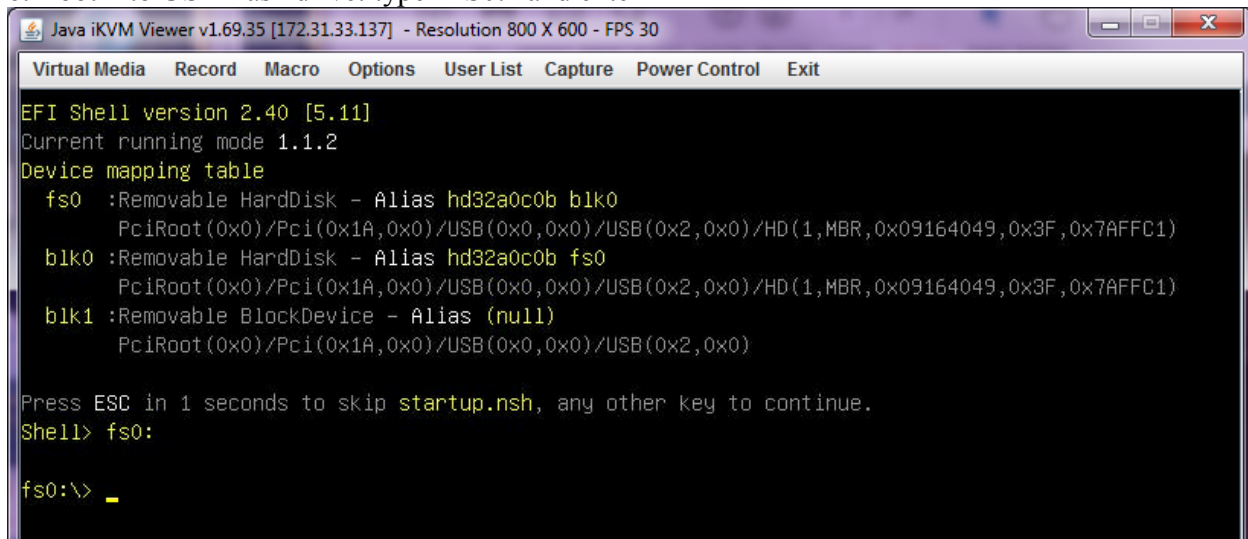
4. Save changes and reboot



5. Press F11 into Boot Menu and select “UEFI: Built-in EFI Shell”



6. Boot into USB flash drive: type “FS0:” and enter



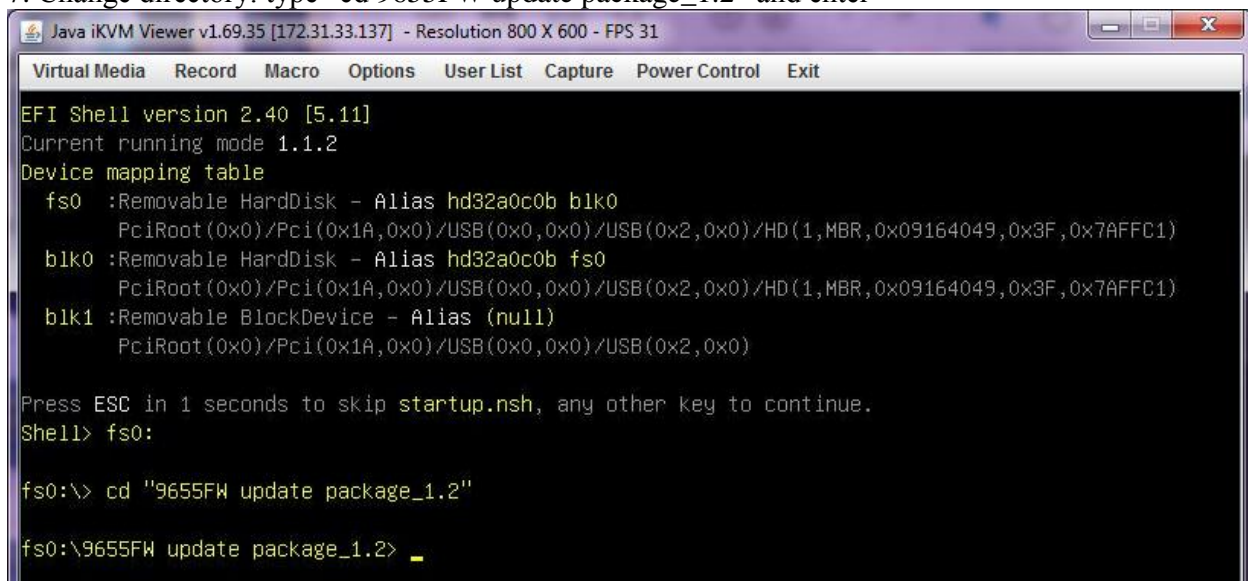
The screenshot shows a Java iKVM Viewer window with a terminal interface. The terminal displays the EFI Shell version 2.40 [5.11] and the current running mode 1.1.2. A device mapping table is shown, listing three devices: fs0 (Removable HardDisk - Alias hd32a0c0b b1k0), blk0 (Removable HardDisk - Alias hd32a0c0b fs0), and blk1 (Removable BlockDevice - Alias (null)). The user is prompted to press ESC to skip startup.nsh. The user enters 'fs0:' at the Shell prompt, and the prompt changes to 'fs0:\> _'.

```
Java iKVM Viewer v1.69.35 [172.31.33.137] - Resolution 800 X 600 - FPS 30
Virtual Media Record Macro Options User List Capture Power Control Exit
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
  fs0 :Removable HardDisk - Alias hd32a0c0b b1k0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk0 :Removable HardDisk - Alias hd32a0c0b fs0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk1 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> _
```

7. Change directory: type “cd 9655FW update package_1.2” and enter



The screenshot shows the same Java iKVM Viewer window as above. The terminal displays the same EFI Shell version 2.40 [5.11] and device mapping table. The user is prompted to press ESC to skip startup.nsh. The user enters 'fs0:' at the Shell prompt, and the prompt changes to 'fs0:\> _'. The user then enters 'cd "9655FW update package_1.2"' at the fs0:\> prompt, and the prompt changes to 'fs0:\9655FW update package_1.2> _'.

```
Java iKVM Viewer v1.69.35 [172.31.33.137] - Resolution 800 X 600 - FPS 31
Virtual Media Record Macro Options User List Capture Power Control Exit
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
  fs0 :Removable HardDisk - Alias hd32a0c0b b1k0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk0 :Removable HardDisk - Alias hd32a0c0b fs0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk1 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> cd "9655FW update package_1.2"

fs0:\9655FW update package_1.2> _
```

8. Run script to update TPM1.2 firmware: type "9655.nsh" and enter

```
Java iKVM Viewer v1.69.35 [172.31.33.137] - Resolution 800 X 600 - FPS 30
Virtual Media Record Macro Options User List Capture Power Control Exit
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
  fs0  :Removable HardDisk - Alias hd32a0c0b b1k0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk0 :Removable HardDisk - Alias hd32a0c0b fs0
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1)
  blk1 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> cd "9655FW update package_1.2"

fs0:\9655FW update package_1.2> 9655.nsh_
```

```
fs0:\TPM_updateFW\9655FW_update> 9655.nsh
9655.nsh> cd Firmware
9655.nsh> TPMFactoryUpd.efi -update config-file -config TPM12_latest.cfg
*****
* Infineon Technologies AG TPMFactoryUpd Ver 01.01.2212.00 *
*****

TPM update information:
-----
Firmware valid           : Yes
TPM family               : 1.2
TPM enabled              : Yes
TPM activated            : Yes
TPM owner set            : No
TPM deferred physical presence : No (Not settable)
TPM firmware version     : 4.32.879.0
Remaining updates        : 64
New firmware valid for TPM : Yes
TPM family after update  : 1.2
TPM firmware version after update : 4.34.1010.2
```



```
Selected firmware image:  
TPM12_4.32.879.0_to_TPM12_4.34.1010.2.BIN
```

```
Preparation steps:  
TPM1.2 Ownership preparation was successful.
```

DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

```
Updating the TPM firmware ...  
Completion: 100 %  
TPM Firmware Update completed successfully.
```

```
9655.nsh> TPMFactoryUpd.efi -info
```

```
*****  
* Infineon Technologies AG TPMFactoryUpd Ver 01.01.2212.00 *  
*****
```

```
TPM information:
```

```
-----
```

```
Firmware valid           : Yes  
TPM family               : 1.2  
TPM firmware version    : 4.34.1010.2  
TPM enabled              : Yes  
TPM activated           : No  
TPM owner set           : Yes  
TPM deferred physical presence : No (Settable)  
Remaining updates       : 63
```

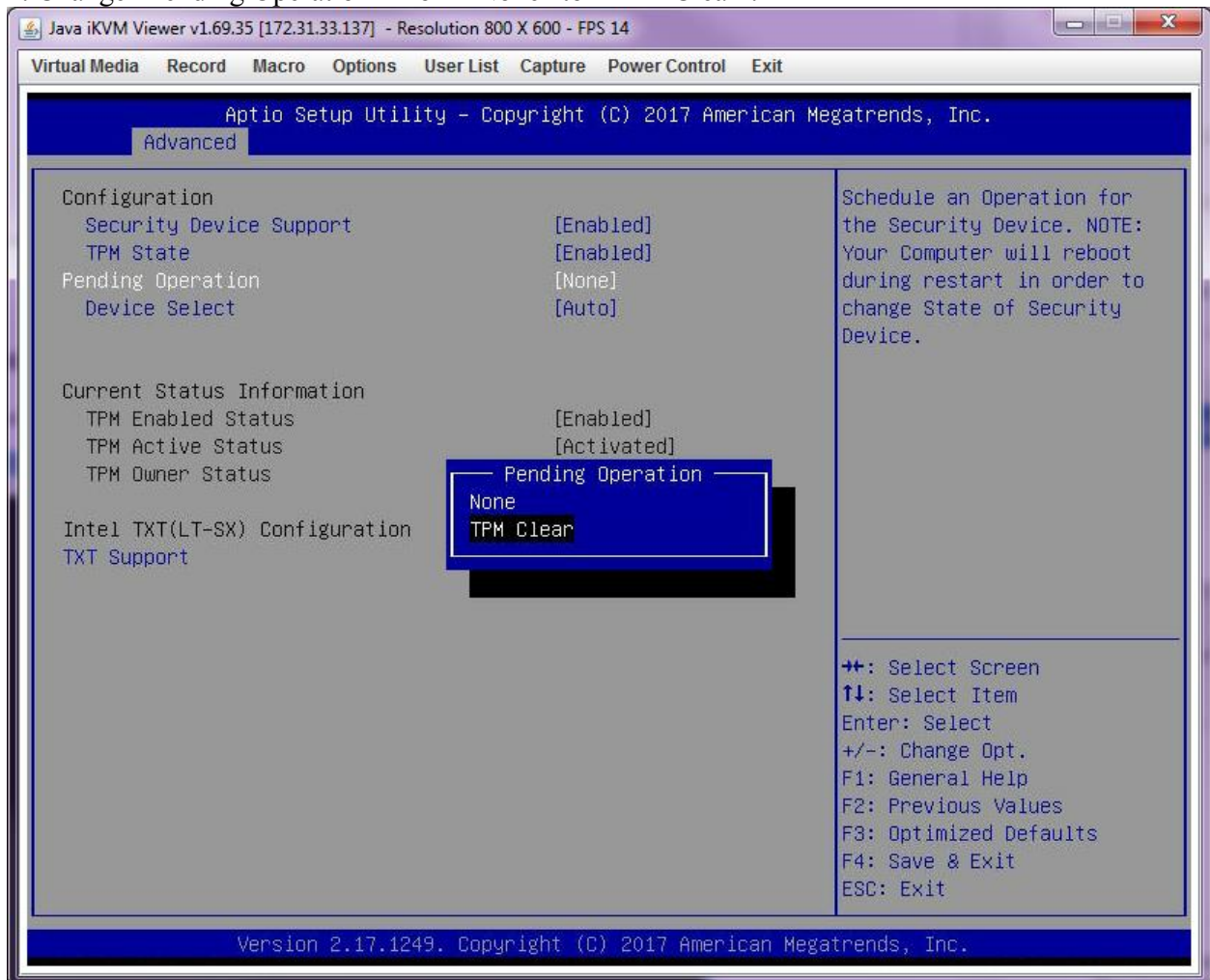
```
9655.nsh> cd ..
```

Appendix

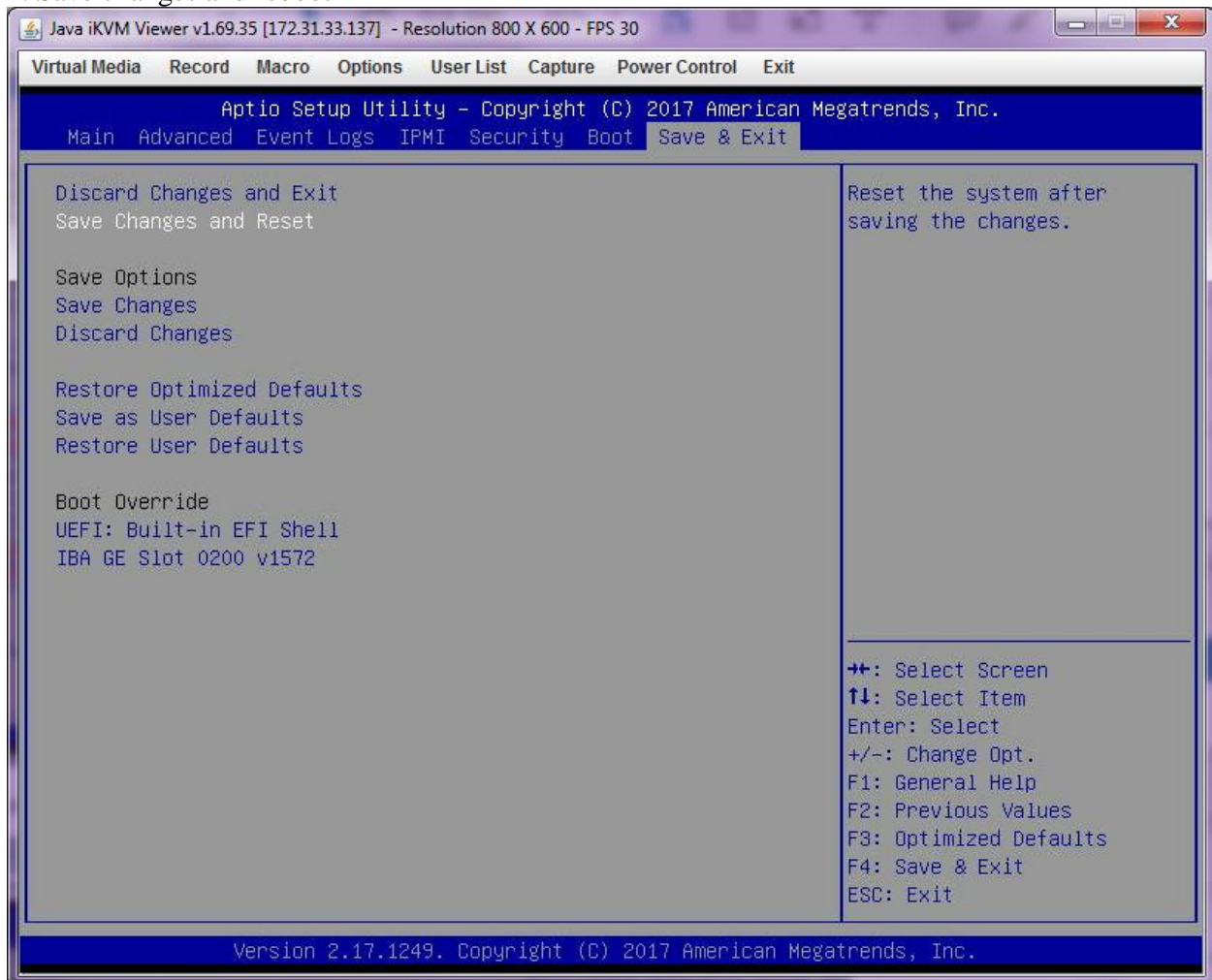
Make the “TPM Owner Status” from “Owned” to “Unowned”.



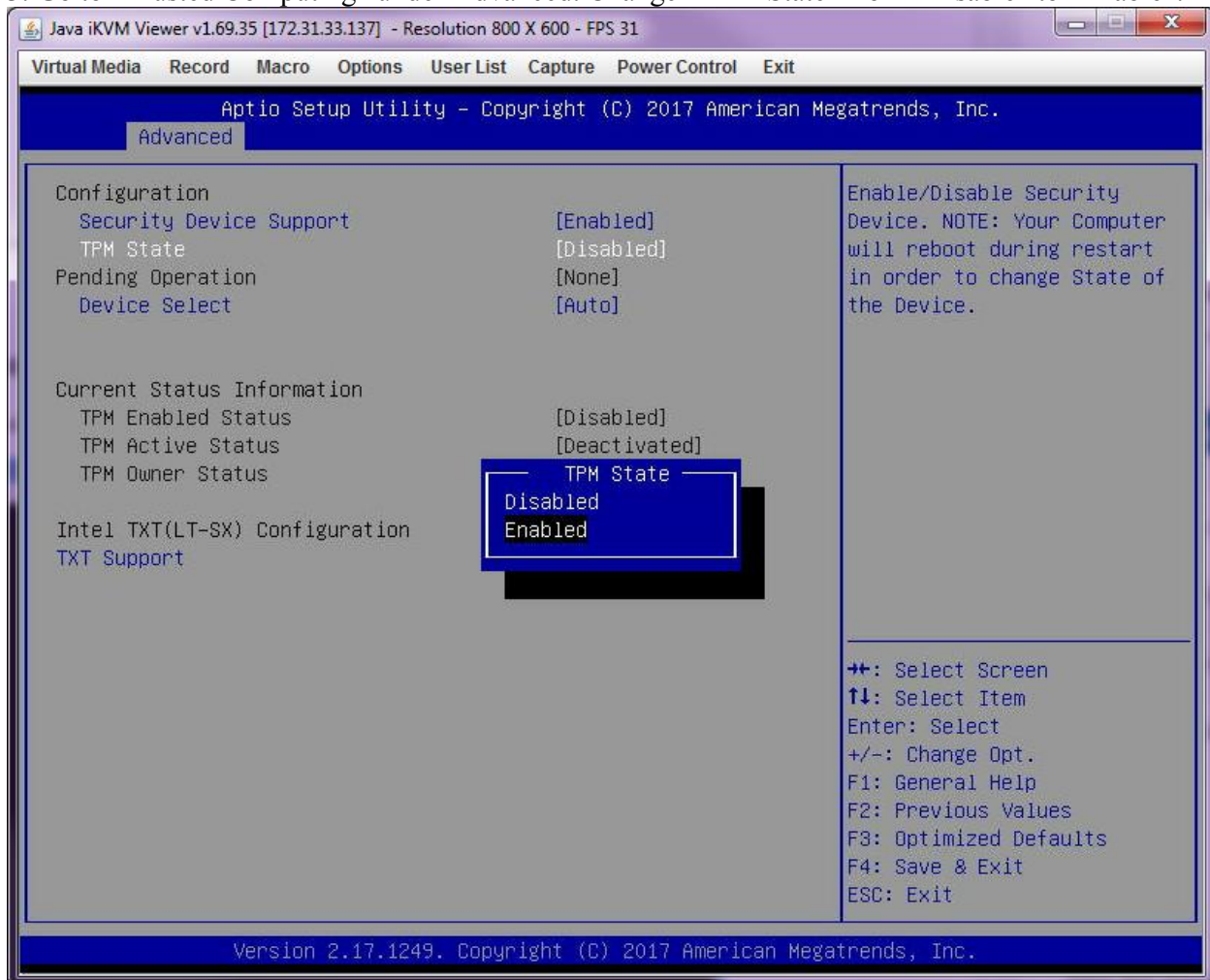
1. Change "Pending Operation" from "None" to "TPM Clear".



2. Save changes and reboot



3. Go to “Trusted Computing” under Advanced. Change “TPM State” from “Disable” to “Enable”.



2. Save changes and reboot

