# 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

Java iKVM Viewer v1.69.35 [172.31.33.137] - Resolution 800 X 600 - FPS 29		
Virtual Media Record Macro Options User List Capture Power Control Exit		
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Main <mark>Advanced</mark> Event Logs IPMI Security Boot Save & Exit		
<ul> <li>Boot Feature</li> <li>CPU Configuration</li> <li>Chipset Configuration</li> <li>SATA Configuration</li> <li>SSATA Configuration</li> <li>Server ME Configuration</li> <li>PCIE/PCI/PNP Configuration</li> <li>Super IO Configuration</li> <li>Serial Port Console Redirection</li> <li>ACPI Settings</li> <li>CSM Configuration</li> <li>Trusted Computing</li> </ul>	Trusted Computing Settings	
▶ iSCSI Configuration	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>	
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.		

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

🛃 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		
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Advanced		
Configuration Security Device Support [Enabled] TPM State [Enabled] Pending Operation [None] Device Select [Auto]	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.	
Current Status Information TPM Enabled Status [Enabled] TPM Active Status [Activated] TPM Owner Status [Unowned] Intel TXT(LT-SX) Configuration TXT Support [Disabled]		
	++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.		

### 4. Save changes and reboot

🛃 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	
Aptio Setup Utility – Copyright (C) 2017 American Main Advanced Event Logs IPMI Security Boot <mark>Save &amp; Exit</mark>	Megatrends, Inc.
Discard Changes and Exit Save Changes and Reset	Reset the system after saving the changes.
Save Options Save Changes Discard Changes Restore Optimized Defaults Save as User Defaults Restore User Defaults	
Boot Override UEFI: Built-in EFI Shell IBA GE Slot 0200 v1572	
	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.	



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

# 6. Boot into USB flash drive: type "FS0:" 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 blk0 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

🔮 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 blk0 PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x09164049,0x3F,0x7AFFC1) blk0 :Removable HardDisk - Alias hd32a0c0b fs0 PaiPcat(0x0)/Pai/(0x1A,0x0)/USB(0x0,0x0)/UPF(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 <mark>startup.nsh</mark> , any other key to continue. Shell≻ fsO:
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 hd32aOcOb blkO		
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 ske 340 \*\*\* 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 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

🛃 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	
Aptio Setup Utility – Copyright (C) 2017 American Main Advanced Event Logs IPMI Security Boot <mark>Save &amp; Exit</mark>	Megatrends, Inc.
Discard Changes and Exit Save Changes and Reset	Reset the system after saving the changes.
Save Options Save Changes Discard Changes	
Restore Optimized Defaults Save as User Defaults Restore User Defaults	
Boot Override UEFI: Built-in EFI Shell IBA GE Slot 0200 v1572	
	t↓: Select Item Enter: Select +/-: Change Opt. F1: General Help
	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.	

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		
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Advanced		
Configuration Security Device Support TPM State Pending Operation Device Select	[Enabled] [Disabled] [None] [Auto]	Enable/Disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
Current Status Information TPM Enabled Status TPM Active Status TPM Owner Status Intel TXT(LT–SX) Configuration TXT Support	[Disabled] [Deactivated] TPM State Disabled Enabled	
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.		

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

## 2. Save changes and reboot

🛃 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	
Aptio Setup Utility – Copyright (C) 2017 American Main Advanced Event Logs IPMI Security Boot <mark>Save &amp; Exit</mark>	Megatrends, Inc.
Discard Changes and Exit Save Changes and Reset	Reset the system after saving the changes.
Save Options Save Changes Discard Changes Restore Optimized Defaults Save as User Defaults Restore User Defaults Boot Override UEFI: Built-in EFI Shell IBA GE Slot 0200 v1572	
	++: Select Screen fJ: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.	