

, Intel Management Engine (Intel ME)

- Intel ME
- Intel ME



:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12



Intel Management Engine (Intel ME)

— , Intel 2008 .
Intel ME , . (), . Intel , ME . , , , . Intel ME .

Intel ME

, Intel ME, , .

:

```
rmmod mei_wdt
rmmod mei_me
rmmod mei
```

"", /etc/modprobe.d/ , , /etc/modprobe.d/mei.conf, :



```
blacklist mei_wdt
blacklist mei_me
blacklist mei
```

Intel ME

Intel ME intelmetool: <https://github.com/zamaudio/intelmetool>

Intel ME:

Bad news, you have a `Q67 Express Chipset LPC Controller` so you have ME hardware on board and it is very difficult to remove, continuing...

RCBA at 0xfed1c000

MEI not hidden on PCI, checking if visible

MEI found: [8086:1c3a] 6 Series/C200 Series Chipset Family MEI Controller #1

ME Status : 0x1e000245

ME Status 2 : 0x60000006

ME: FW Partition Table : OK

ME: Bringup Loader Failure : NO

ME: Firmware Init Complete : YES

ME: Manufacturing Mode : NO

ME: Boot Options Present : NO

ME: Update In Progress : NO

ME: Current Working State : Normal

ME: Current Operation State : M0 with UMA

ME: Current Operation Mode : Normal

ME: Error Code : No Error

ME: Progress Phase : Host Communication

ME: Power Management Event : Clean Mof->Mx wake

ME: Progress Phase State : Host communication established

PCI READ [bc] : 0x000000bc
ME: Extend SHA-256: 193f2d686de7ecee80a98a140b2084bd084b33b06e05640f39f5c0d62d36bb69

ME seems okay on this board
WRITE [00] : CB: 0x80040007
WRITE [00] : CB: 0x000002ff
ME: timeout waiting for data: expected 8, available 6
ME: GET FW VERSION message failed
WRITE [00] : CB: 0x80080007
WRITE [00] : CB: 0x00000203
WRITE [00] : CB: 0x00000000
READ [08] : CB: 0x800d0007
READ [08] : CB: 0x00008203
READ [08] : CB: 0x00000000
READ [08] : CB: 0xde5c4704
READ [08] : CB: 0x0007000d
ME Capability: Full Network manageability : ON
ME Capability: Regular Network manageability : ON
ME Capability: Manageability : ON
ME Capability: Small business technology : OFF
ME Capability: Level III manageability : OFF
ME Capability: IntelR Anti-Theft (AT) : OFF
ME Capability: IntelR Capability Licensing Service (CLS) : ON
ME Capability: IntelR Power Sharing Technology (MPC) : ON
ME Capability: ICC Over Clocking : ON
ME Capability: Protected Audio Video Path (PAVP) : ON
ME Capability: IPV6 : ON
ME Capability: KVM Remote Control (KVM) : ON
ME Capability: Outbreak Containment Heuristic (OCH) : ON
ME Capability: Virtual LAN (VLAN) : ON
ME Capability: TLS : OFF
ME Capability: Wireless LAN (WLAN) : ON
exiting