(ATA Security FDE/SED TCG OPAL)

(" "), .

, , , .

, "", , " ".

- ""
-
- TA Security
  -
  -
  -
  -
  -
  -
- TCG OPAL
  -
  -
  - (PBA)
  -
  - PBA
  -
  -
    -
    -
    - OPAL
-
  - " "
  -

:

- 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

, , (, ,) , (S1, S2, S3 («Suspend to RAM» (STR) BIOS, « » («Standby»)), , . , S4 («Suspend to disk» (STD)), , .

""

(" ", Full-Drive Encription (FDE) Self-Encrypting Drive (SED),) , , , . " ", .
:

- AES 128 / AES 256 ;
- ;
- "" , ;

, , .

, , . :

- ATA Security - / , ATA.
  , , ;
- TCG OPAL - , , , , , . , "" (shadow) , . OPAL , .

ATA Security TCG OPAL . , , , , SATA ( ) , , , . .

TA Security

ATA Security .

hdparm, hdparm. / Astra Linux.
(. synaptic)

```
sudo apt install hdparm
```

(/dev/sda):

```
sudo hdparm -I /dev/sda
```

:

```
$ sudo hdparm -I /dev/sda

/dev/sda:

ATA device, with non-removable media
        Model Number: TOSHIBA HDWD110
        Serial Number: X7HW1XWFS
        Firmware Revision: MS2OA8J0
        Transport: Serial, ATA8-AST, SATA 1.0a, SATA II Extensions, SATA Rev 2.5, SATA Rev 2.6, SATA Rev 3.0;
Revision: ATA8-AST T13 Project D1697 Revision 0b
Standards:
        Used: unknown (minor revision code 0x0029)
        Supported: 8 7 6 5
        Likely used: 8
Configuration:
        Logical max current
        cylinders 16383 16383
        heads 16 16
        sectors/track 63 63
        --
        CHS current addressable sectors: 16514064
        LBA user addressable sectors: 268435455
        LBA48 user addressable sectors: 1953525168
        Logical Sector size: 512 bytes
        Physical Sector size: 4096 bytes
        Logical Sector-0 offset: 0 bytes
        device size with M = 1024*1024: 953869 MBytes
        device size with M = 1000*1000: 1000204 MBytes (1000 GB)
        cache/buffer size = unknown
        Form Factor: 3.5 inch
        Nominal Media Rotation Rate: 7200
Capabilities:
        LBA, IORDY(can be disabled)
        Queue depth: 32
        Standby timer values: spec'd by Standard, no device specific minimum
        R/W multiple sector transfer: Max = 16 Current = 16
        Advanced power management level: disabled
        DMA: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 udma5 *udma6
        Cycle time: min=120ns recommended=120ns
        PIO: pio0 pio1 pio2 pio3 pio4
        Cycle time: no flow control=120ns IORDY flow control=120ns
Commands/features:
        Enabled Supported:
                * SMART feature set
                  Security Mode feature set
                * Power Management feature set
                * Write cache
                * Look-ahead
                * Host Protected Area feature set
                * WRITE_BUFFER command
                * READ_BUFFER command
                * NOP cmd
                * DOWNLOAD_MICROCODE
```

```
                  Advanced Power Management feature set
                  Power-Up In Standby feature set
                * SET_FEATURES required to spinup after power up
                  SET_MAX security extension
                * 48-bit Address feature set
                * Device Configuration Overlay feature set
                * Mandatory FLUSH_CACHE
                * FLUSH_CACHE_EXT
                * SMART error logging
                * SMART self-test
                  Media Card Pass-Through
                * General Purpose Logging feature set
                * WRITE_{DMA|MULTIPLE}_FUA_EXT
                * 64-bit World wide name
                * URG for READ_STREAM[_DMA]_EXT
                * URG for WRITE_STREAM[_DMA]_EXT
                * WRITE_UNCORRECTABLE_EXT command
                * {READ,WRITE}_DMA_EXT_GPL commands
                * Segmented DOWNLOAD_MICROCODE
                  unknown 119[7]
                * Gen1 signaling speed (1.5Gb/s)
                * Gen2 signaling speed (3.0Gb/s)
                * Gen3 signaling speed (6.0Gb/s)
                * Native Command Queueing (NCQ)
                * Host-initiated interface power management
                * Phy event counters
                * NCQ priority information
                  Non-Zero buffer offsets in DMA Setup FIS
                * DMA Setup Auto-Activate optimization
                  Device-initiated interface power management
                 In-order data delivery
                * Software settings preservation
                * SMART Command Transport (SCT) feature set
                * SCT Write Same (AC2)
                * SCT Error Recovery Control (AC3)
                * SCT Features Control (AC4)
                * SCT Data Tables (AC5)
Security:
        Master password revision code = 65534
                supported
              not enabled
              not locked
                  frozen
              not expired: security count
              not supported: enhanced erase
              156min for SECURITY ERASE UNIT.
Logical Unit WWN Device Identifier: 5000039fd3cc4d45
        NAA : 5
        IEEE OUI : 000039
        Unique ID : fd3cc4d45
Checksum: correct
```

ATA Security "Security":

```
...

    Security:
            Master password revision code = 65534
                    supported
                  not enabled
                  not locked
                      frozen
                  not expired: security count
                  not supported: enhanced erase
                  156min for SECURITY ERASE UNIT.

    ....
```

, ("Master password ... supported"), ("not enabled").
, ("frozen"). BIOS- / , , .

, :

- , USB, ;
- BIOS- / , ( ).
  / "" ;

(- 12345678 /dev/sdb) :

```
sudo hdparm --user-master u --security-set-pass 12345678 /dev/sdb
```

.
, , , (sdb):

```
sudo -i
echo 1 >/sys/block/sdb/device/delete
exit
```

SATA . , .
:

```
sudo -i
echo "- - -" > /sys/class/scsi_host/hostX/scan
exit
```

hostX - (/sys/class/scsi_host/host3/scan), .

, .
( ) (12345678):

```
sudo hdparm --user-master u --security-unlock 12345678 /dev/sdb
```

:

```
sudo hdparm -z /dev/sdb
```

:

```
sudo hdparm --user-master u --security-disable 12345678 /dev/sdb
```

, :

```
sudo hdparm -z /dev/sdb
```

TCG OPAL

, OPAL

TCG Opal , Astra Linux.

ATA (TPM), (, libata). , libata,

"... " " . libata.allow_tpm = 1, ...".

Wki Archlinux .

, us_english. .
, , , .

, , .
(,), .

/ ATA TPM
C https://github.com/Drive-Trust-Alliance/sedutil/wiki/Executable-Distributions.

ATA TPM:

1. allow_tpm = 1 /etc/default/grub:

   GRUB_CMDLINE_LINUX_DEFAULT="quiet splash libata.allow_tpm=1"

2. :

   ```
   sudo update-grub
   ```

3. .

: BIOS 64bit UEFI.

```
wget -O RESCUE32.img.gz https://github.com/Drive-Trust-Alliance/exec/blob
/master/RESCUE32.img.gz?raw=true
```

```
wget -O RESCUE64.img.gz https://github.com/Drive-Trust-Alliance/exec/blob
/master/RESCUE64.img.gz?raw=true
```

UEFI Secure Boot.

:

```
gunzip RESCUE32.img.gz
```

```
gunzip RESCUE64.img.gz
```

USB- , :

.

```
dd if=RESCUE32.img of=/dev/sd?
```

```
dd if=RESCUE64.img of=/dev/sd?
```

.

Login "root" .

sedutil-cli --scan

:

```
#sedutil-cli --scan
Scanning for Opal compliant disks
/dev/nvme0 2 Samsung SSD 960 EVO 250GB 2B7QCXE7
/dev/sda 2 Crucial_CT250MX200SSD1 MU04
/dev/sdb 12 Samsung SSD 850 EVO 500GB EMT01B6Q
/dev/sdc 2 ST500LT025-1DH142 0001SDM7
/dev/sdd 12 Samsung SSD 850 EVO 250GB EMT01B6Q
No more disks present ending scan
```

2 , OPAL 2, .

, OPAL2, .

(PBA)

linuxpba debug.

.

:

#linuxpba
DTA LINUX Pre Boot Authorization
Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 Samsung SSD 960 EVO 250GB is OPAL NOT LOCKED
Drive /dev/sda Crucial_CT250MX200SSD1 is OPAL NOT LOCKED
Drive /dev/sdb Samsung SSD 850 EVO 500GB is OPAL NOT LOCKED
Drive /dev/sdc ST500LT025-1DH142 is OPAL NOT LOCKED
Drive /dev/sdd Samsung SSD 850 EVO 250GB is OPAL NOT LOCKED

, "is OPAL".

OPAL. " "

/dev/sdc /usr/sedutil/UEFI64-1.15.img.gz ( ).
/dev/sd? .

.
:

```
#
gunzip /usr/sedutil/UEFI64-n.nn.img.gz
```

(debug,):

```
sedutil-cli --initialsetup debug /dev/sdc
#
sedutil-cli --loadPBAimage debug /usr/sedutil/UEFI64-n.nn.img /dev/sdc
sedutil-cli --setMBREnable on debug /dev/sdc
```

:

```
sedutil-cli --enableLockingRange 0 password drive
```

PBA

, .
debug. :

#linuxpba

DTA LINUX Pre Boot Authorization
Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 Samsung SSD 960 EVO 250GB is OPAL NOT LOCKED
Drive /dev/sda Crucial_CT250MX200SSD1 is OPAL NOT LOCKED
Drive /dev/sdb Samsung SSD 850 EVO 500GB is OPAL NOT LOCKED
Drive /dev/sdc ST500LT025-1DH142 is OPAL Unlocked <---!!!
Drive /dev/sdd Samsung SSD 850 EVO 250GB is OPAL NOT LOCKED

, ("is OPAL Unlocked").
, OPAL.

SID Admin1, .
:

```
sedutil-cli --setsidpassword debug yourrealpassword /dev/sdc
sedutil-cli --setadmin1pwd debug yourrealpassword /dev/sdc
```

:

```
#sedutil-cli --setsidpassword debug yourrealpassword /dev/sdc
#sedutil-cli --setadmin1pwd debug yourrealpassword /dev/sdc
- 14:20:53.352 INFO: Admin1 password changed
```

:

```
sedutil-cli --setmbrdone on yourrealpassword /dev/sdc
```

```
#sedutil-cli --setmbrdone on yourrealpassword /dev/sdc
- 14:22:21.590 INFO: MBRDone set on Your drive in now using OPAL locking.
```

.

(PBA) .

BIOS PBE .

OPAL .

```
sedutil-cli --disableLockingRange 0 <password> <drive>
sedutil-cli --setMBREnable off <password> <drive>
```

:

```
#sedutil-cli --disablelockingrange 0 debug /dev/sdc
- 14:07:24.914 INFO: LockingRange0 disabled
#sedutil-cli --setmbrenable off debug /dev/sdc
- 14:08:21.999 INFO: MBREnable set off
```

```
sedutil-cli --enableLockingRange 0 <password> <drive>
sedutil-cli --setMBREnable on <password> <drive>
```

:

```
#sedutil-cli --enablelockingrange 0 debug /dev/sdc
- 14:07:24.914 INFO: LockingRange0 enabled ReadLocking,WriteLocking
#sedutil-cli --setmbrenable on debug /dev/sdc
- 14:08:21.999 INFO: MBREnable set on
```

OPAL

OPAL , .
, .

```
sedutil-cli --revertnoerase <password> <drive>
sedutil-cli --reverttper <password> <drive>
```

:

#sedutil-cli --revertnoerase debug /dev/sdc
- 14:22:47.060 INFO: Revert LockingSP complete
#sedutil-cli --reverttper debug /dev/sdc
- 14:23:13.968 INFO: revertTper completed successfully
#

" "

, , . , , , ., , , .

, , .
. .