Prerequisites for Heads

13-16 minutes

▼ Table of contents

Required equipment

To install Heads on a physical device, you will need:

- Supported motherboard or laptop (see below)
- A heads compatible USB security dongle (see below)
- A heads compatible storage device for your public GPG key (USB flash drive)

If your device requires external flashing (see below), you will also need:

- SPI Programmer: green pcb ch341a programmer or raspberry pi or bus pirate (green ch341a is recommended for new users and can be found almost anywhere with preassembled clip as a kit.
    - Beware that black ch341a are known to not provide 3.3V as most NOR chips requires and should me manually fixed. If you intend to use a ch341a for initial flashing and occasional unbricking, this is perfectly fine without modification. Otherwise, you should look into other programmers or do the fix yourself. A lot of people suggest against using ch341a unless modified.
- Wires and a clip SOIC8 to connect your programmer of choice to the board's SPI flash chip(s).
    - The Pomona 5250 is suggested as it is high quality and easier to make contact with the pins.
- A second computer to flash from (Try to use a recommended operating system: Qubes or Debian 9 or Fedora 30)

Supported devices

Please see the current heads source for up-to-date supported board configurations.

Note repeatedly untested boards from willing to test board owners were moved to unmaintained_boards directory and aren't built by CircleCI anymore

If *you have an external programmer* and *are techsavvy enough to bring their support back yourself*, read the Community page and reach out. I will gladly assist in your quest :)

USB Security Dongles (aka security token aka smartcard)

NOTE - Heads does **NOT** support FIDO2 or U2F authentication. Be careful when purchasing to buy a compatible key.

NOTE - HOTP remote attestation is supported from Librem platforms by default, Otherwise HOTP is explicitely supported by board configurations having `hotp` in their board names.

NOTE - The NitroKey 3 comes in three sizes: USB A, A-mini and C. Nk3a mini (USB A-mini) is the one most shipped with novacustom and nitropads.

- ThinkPads have USB A ports, not C. After that, it's users preferences for the form factor desired.

Legacy vs Maximized boards

Some history first on the historical x230-flash and x230 boards that initially created the Heads project.

Heads was initially developped on the x230 board (first xx30 board supported).

At that time, ME cleaning/neutering was not a thing. Then me_cleaner facilitated the task. The X230 board, as all xx30 family boards do not have a single SPI flash, but two. On the bottom SPI flash chip lies the Intel Flash Descriptor (IFD), Intel Management Enging (ME), Intel Gigabit Configuration (GBE) and some BIOS available space spanning from 4MB chip. On the top SPI flash is the original BIOS region which spans to BIOS region on the 8MB chip.

Original work done on Heads without ME cleaning led to the creation of a two phase flashing of the board. It required an original external flashing of the x230-flash ROM to the 4MB top chip, which permitted to boot into a minimal BIOS recovery shell from which the x230 board 12MB ROM could be internally flashed through flashrom and Linux, fitting into the 4MB SPI flash from x230-flash ROM. Booting into x230-flash launches a recovery shell which made possible to flash only the BIOS region from the x230 created ROM. This ROM image is incomplete, and flashing the whole 12MB image would create a brick. A script made available through x230-flash was taking care of only flashing the BIOS region defined under untouched IFD region, which permitted to flash the 7MB defined BIOS region inside of the IFD descriptor, without touching ME, GBE or the IFD itself.

Then me_cleaner came to life, which permitted to clean ME in different ways. me_cleaner project grew mature, and eventually permitted, for xx20 and xx30 families, to not only clean ME, but neuter it. Neutering here means that not only ME was asked to deactivate itself, but most of the modules inside of it could be removed. For the xx20 family, it eventually meant that only Platform Bring UP (BUP) was required for the computer to maintain its functions, while for the xx30, BUP and ROM byPass (ROMP) are necessary. This also meant that the space used by the ME kernel and libraries being deleted could be reused for other purposes. But that space being freed could never be took for granted. Unless the IFD descriptor was modified to reduce ME region to match freed space, coreboot CBFS region maximized to match freed ME available space. Doing so permitted the BIOS region (coreboot + Heads) to jump from a 7MB available BIOS region in IFD descriptor to 11.5MB on the x230 and the whole xx30 family boards. But no board configuration permitted to take advantage of that for numerous reasons, most of which being legal matters, with blobs being non redistributable.

The consequence of that is the appearance of Maximized boards the multiple xx20 and xx30 boards now lying under Heads repository, and the complexity for newcomers to build and use Heads for the first time.

In short, legacy boards will produce ROMs that are incomplete by themselves; they do not contain a valid IFD descriptor and require internal and manual flashrom program invocation with proper parameters from a script to inform flashrom to use the actual IFD defined BIOS region and flash that area only. Otherwise a non-booting system would result. A brick.

The maximized boards were created to produce fully valid and complete images for those boards. Blobs download/cleaning scripts were created for xx20 and xx30 platforms, which download ME blobs from the manufacturer, remove all the nasty bits reducing ME used space to the minimal and put resulting blob where it is needed from coreboot configuration to be integrated in the final produced ROM. A valid IFD descriptor is provided under the blob directory to match reduced ME size, giving the freed space to the BIOS region. A generated GBE blob is also provided in tree, required to have a functional e1000e ethernet interface, with an important limitation to be known from Heads users: the MAC address of maximized boards is fixed to DE:AD:C0:FF:EE. That is not so important for the majority of us connecting through wifi nowadays. But if a lot of Heads machines are living on the same LAN, or if privacy is needed through Ethernet connection, NetworkManager or other manual configuration will need to be applied to randomize/fixate Ethernet MAC address to desired value prior of connecting to a network.

Legacy boards advocates that unlocking IFD regions and ME could permit ME to be modified. While it is true, the non-removable parts of ME (BUP and/or ROMP) are signed together and verified per ME coproocessor prior of permitting the platform to boot. Consequently, removing the nasty parts of ME and providing an unlocked IFD and baked GBE was the chosen path for *Maximized* boards. It is still possible for advanced users to decide to relock the IFD regions prior of flashing maximized boards, while this path would be manual and complexify future internal upgrades. Actually provided Maximized boards take into consideration that the whole SPI flash chip is internally flashable, which would result in flashrom complaining on next internal upgrades. It is still also possible for advanced users to override Heads internally kept configuration to replace the *FLASHROM_OPTIONS* statement to specify manually the IFD defined specific sections to flash : `--ifd --image bios --image ME` etc

Current Legacy boards

xx30-flash: 4MB ROM images to be flashed internally through 1vyrain or Skulls. Unlocking IFD and cleaning/neutering ME still highly recommended prior of doing initial flash. 1vyrain deactivates ME internally. But if one leaves 1vyrain and chooses another ROM, 1vyrain applied hacks to deactivate ME will not be applied anymore. Note that Skulls permits to unlock IFD as an option prior of initial flash. So if it was not applied at that step, then the end user can only upgrade to Legacy boards produced ROMs in the future, the IFD and ME not being flashable internally and requiring an external flash to go with Maximized boards.

xx30: Baked 12MB ROM images to be flashed internally through xxxx-flash flashed ROMs. Those ROMs can only be internally flashed from/to legacy boards configuration. Flashing a legacy ROM from a Maximized ROM will result in a brick, since Maximized boards produced ROMs will flash the whole combined opaque 12MB ROM internally, overwriting IFD, ME and GBE with empty content. Resulting into a brick.

xx20: Those ports (t420 and x220 at time of writing) landed on Heads later in time and were historically produced by making required blobs available by applying scripts on SPI backups to extract required blobs. Consequently, those boards do not suffer from feature reduction as of now; they always took for granted that ME was neutered and IFD was unlocked. They still only flash internally the BIOS region, which was maximized to take advantage of 7.5MB available SPI space for BIOS region, while not reflashing the whole SPI.

xxxx-hotp-verification: Legacy, reduced versions of their HOTP maximized counterpart. At the time of writing

this, those board configuration will normally loose dropbear support, while xx30 versions will not have FBWhiptail anymore. That means that there is no framebuffer enforced graphical interface under Heads with background color cues notifying the end user of warning (yellow) or errors (red) contextual, graphical menus.

Current Maximized boards

xx30-maximized: Those board configuration produce 3 ROM images: One full 12MB image containing reduced ME, maximized IFD BIOS region and GBE to be flashed internally, and two splitted out ROM images from the full image named bottom (8MB) and top images (4MB), aimed to be externally flashed to their physical SPI counterparts If built locally, the builder has the option of extracting blobs from a backup image which will put GBE, ME and IFD binaries at the right location in the blobs directory which will be included into coreboot created full ROM image, including Heads payload. There is a risk that ME will be bigger/smaller since backuped blobs might be of sifferent size. In the case ME is bigger then expected, there is a chance that the flashed system will result in a brick. This is why Cleaning ME instructions in this website strongly advises into upgrading to Lenovo 2.76 version of the firmware prior of backuping the bottom SPI ROM, unlocking IFD and clean that specific version of proprietary firmware. This is also why it is suggested to only backup your GBE to keep your MAC address for Ethernet and use the download script under blobs/xx30 to download and neuter verified version of Lenovo ME downloaded straight from their website. Those do not enforce HOTP firmware verification (see hotp-maximized counterparts) against supported USB Security dongles and rely solely on TOTP to manually verify firmware integrity prior of each boot, that is: launching OTP application on smartphone to manually verify that the TOTP codes generated on both screens of smartphone and laptop matches from smartphone generated and scanned Qr code after first boot of Heads new firmware.

xxxx-hotp-maximized: Those board configurations are the same as prior maximized board configuration, but produce ROM images enforcing TOTP+HOTP for firmware verification on supported, already bought and received prior of flashing USB Security dongles to be bounded with Heads.

Legacy to Maximized boards upgrade path

It is possible to upgrade from Legacy to Maximized boards under certain conditions.

If you come from 1vyrain, this is impossible. 1vyrain does not unlock neither IFD nor ME regions of the SPI. Consequently, flashing internally anything else then Legacy boards produced ROMs will result in a brick.

If coming from Skulls, *if and only optional unlocking step has been followed*, you can upgrade internally through a manual flashrom call, just like if you were coming from Heads Legacy boards while having followed the me_cleaning page instructions prior of initial flash.

If coming from Skulls or Heads Legacy board configurations while having unlocked IFD initially, you can flash from the recovery shell manually. **IF UNSURE, PLEASE VERIFY FIRST**

Having a full xxxx-hotp-maximized or xxxx-maximized board config produced ROM available on a USB stick, alongside with your USB Security dongle's matching exported public key, do the following:

```
mount-usb
flashrom -p internal -w /media/PathToMaximizedRom.rom
```

On next reboot, Heads will guide you into factory resetting your USB Security dongle or import your

previously generated public key matching your USB Security dongle's private key.

It will then regenerate a TOTP/HOTP secret and sign /boot content. You will then have to define a new default boot and optionally renew/change your Disk Unlock Key to be released to to OS to unlock your encrypted OS installation to move forward.

In the case nothing is found installed on your disk, Heads will propose you to boot from USB to install a new Operating System, prior of being able to do the above steps prior of booting into your system.

Emulated devices

For further information, see Emulating Heads