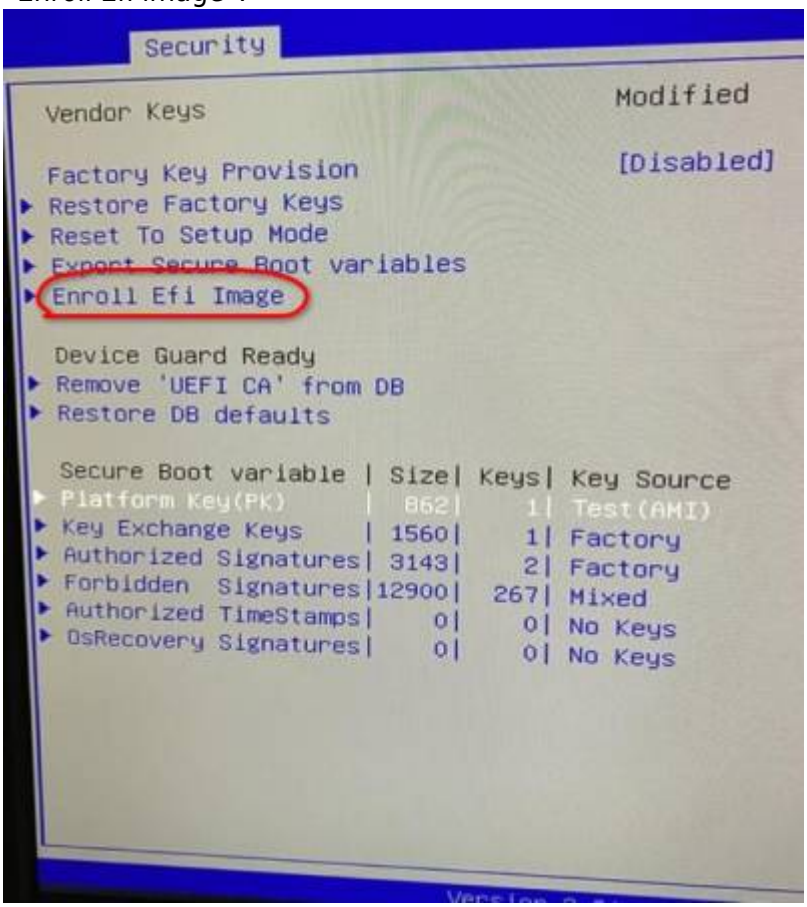
Secure Boot

For Batocera v38 and lower

Batocera **v38** and lower has minimal Secure Boot support, and only if the UEFI BIOS will allow direct enrollment of an EFI loader hash. This usually can be done from the security options of the BIOS. Search for an option which allows you to “Add keys”, “Generate keys from EFI file” or “Enroll Efi image”:



For Batocera **v39** and higher on x86_64 systems, streamlined support for Secure Boot is present. This makes it easier to boot Batocera on PCs which have poor secure boot key management in the native UEFI BIOS. The process detailed below will install Batocera's security certificate into the machine's “Machine Owner Keys” (MOK) into the PC's UEFI variable store. This will allow the machine to execute Batocera's bootloader, which has been digitally signed with Batocera's certificate, even when Secure Boot is enabled in the BIOS.

Modifying Secure Boot and related settings may trip a “tamper switch” (Platform Configuration Register, PCR) in the system's Trusted Platform Module (TPM). Once the switch has been tripped, it cannot be reset without providing a recovery key. If BitLocker Disk Encryption is enabled, Windows will detect the tampering and will ask for the BitLocker recovery key before allowing Windows to boot.

If the system is managed by someone else (such as your employer), recovery may require assistance from an authorized system administrator. Act responsibly, and only install Batocera on systems you own and manage.

Before proceeding, make a copy of the required BitLocker recovery keys. Documentation on locating the keys can be found at https://support.microsoft.com/en-us/windows/where-to-look-for-your-bitlocker-recovery-key-fd2b3501-a4b9-61e9-f5e6-2a545ad77b3e

Technical references:

https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/switch-pcr-banks-on-tpm-2-0-devices

https://www.dell.com/support/kbdoc/en-us/000124361/bitlocker-is-prompting-for-a-recovery-key-and-you-cannot-locate-the-key

Prerequisites

- The system must be an Intel/AMD system that supports booting in 64-bit UEFI mode, with the standard Microsoft signing key certificates.
- Secure Boot must be enabled during the setup process. If offered the option to select the mode of Secure Boot to use, the “Standard” mode is recommended. Other modes are untested.
- The UEFI BIOS firmware must support booting from the desired installation media type, and it must be possible to select which drive to boot while using UEFI.
- A keyboard is required to navigate the MOK management procedure detailed below.

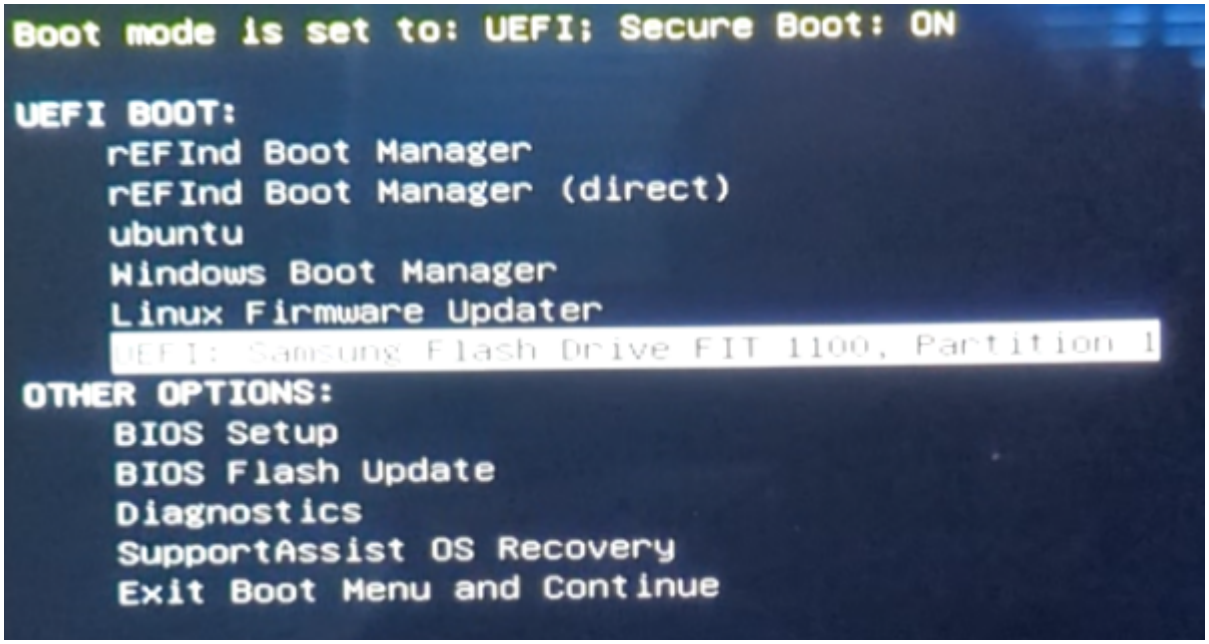
As some of this configuration is vendor-specific, consult the manual for the machine before getting started.

Preparation

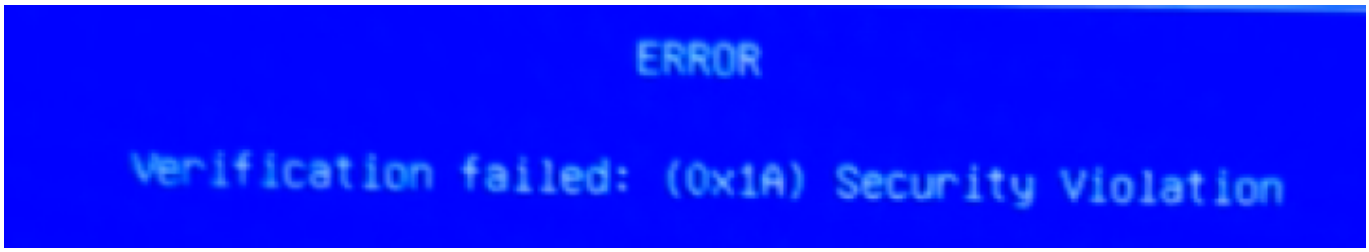
Flash Batocera on a drive, or upgrade an existing installation to **v38** or higher. Attach the drive to your computer.

Configuration Steps

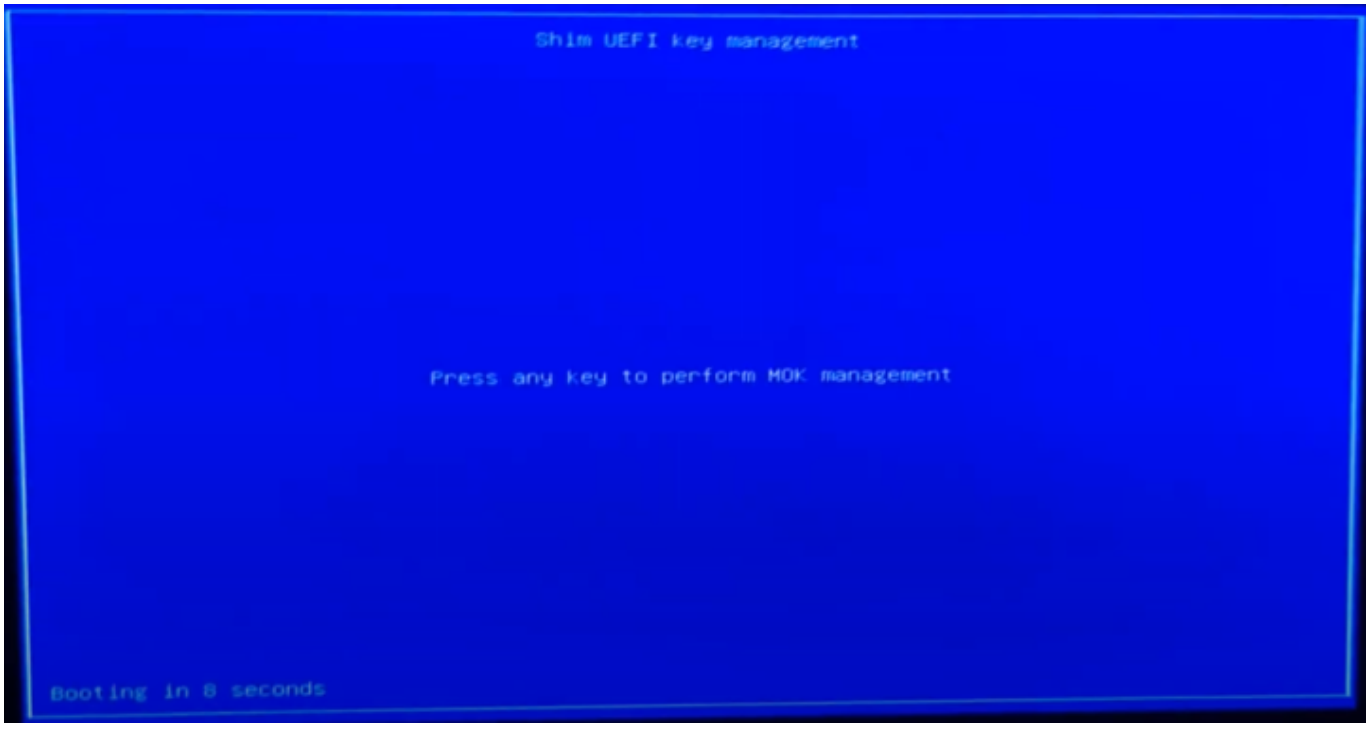
Power on the computer and enter its BIOS setup or boot manager. Set the UEFI boot to the drive Batocera is installed on. The details of how to do this vary by manufacturer. On some systems there is a “boot manager” accessible by a keystroke at boot; on others the “boot order” bust be configured with the Batocera drive set first. Tom's Hardware has a good guide on How to Enter the BIOS on Any PC. For my demonstration run on my Dell laptop, I pressed [F12] at startup to enter the boot menu, used the arrow keys to navigate to the USB media, and hit [ENTER] to boot.



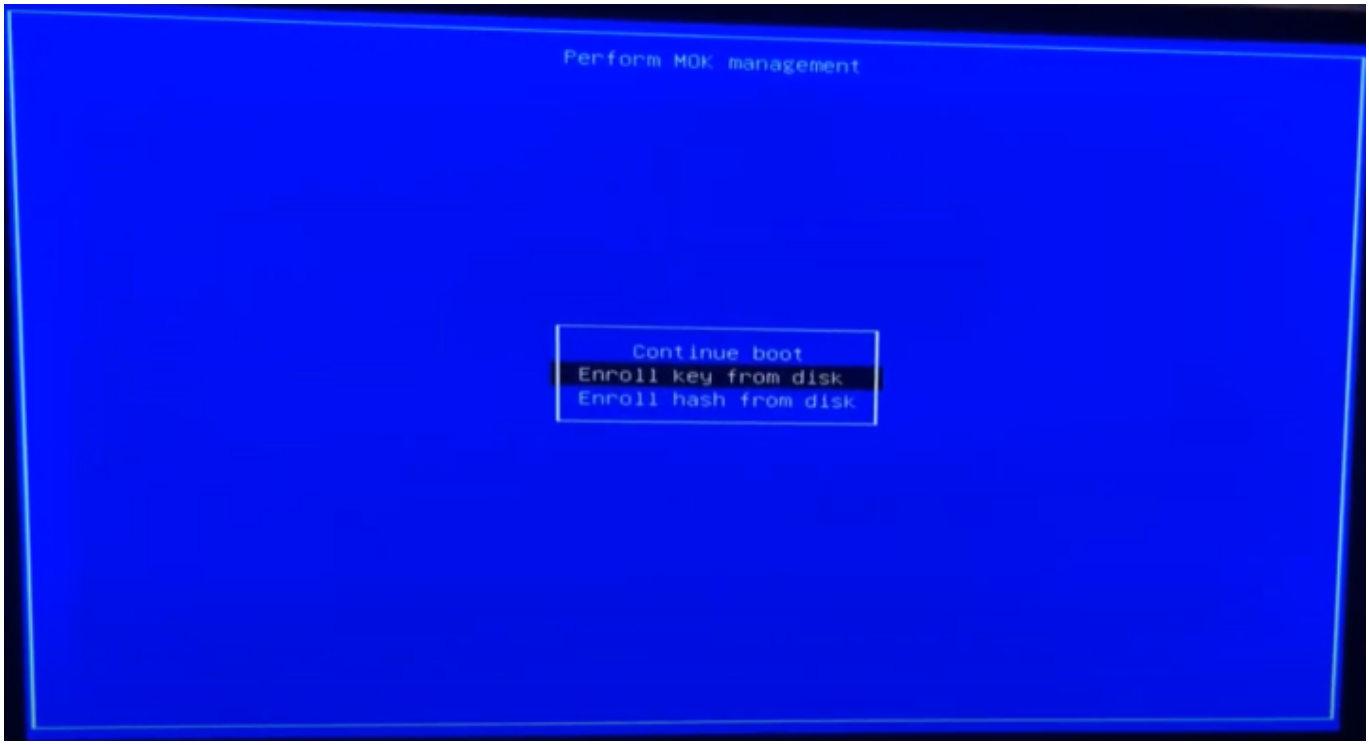
A blue screen will appear with a message **Error Verification Failed (0x1A) Security Violation**. Hit [ENTER] on the keyboard to continue.



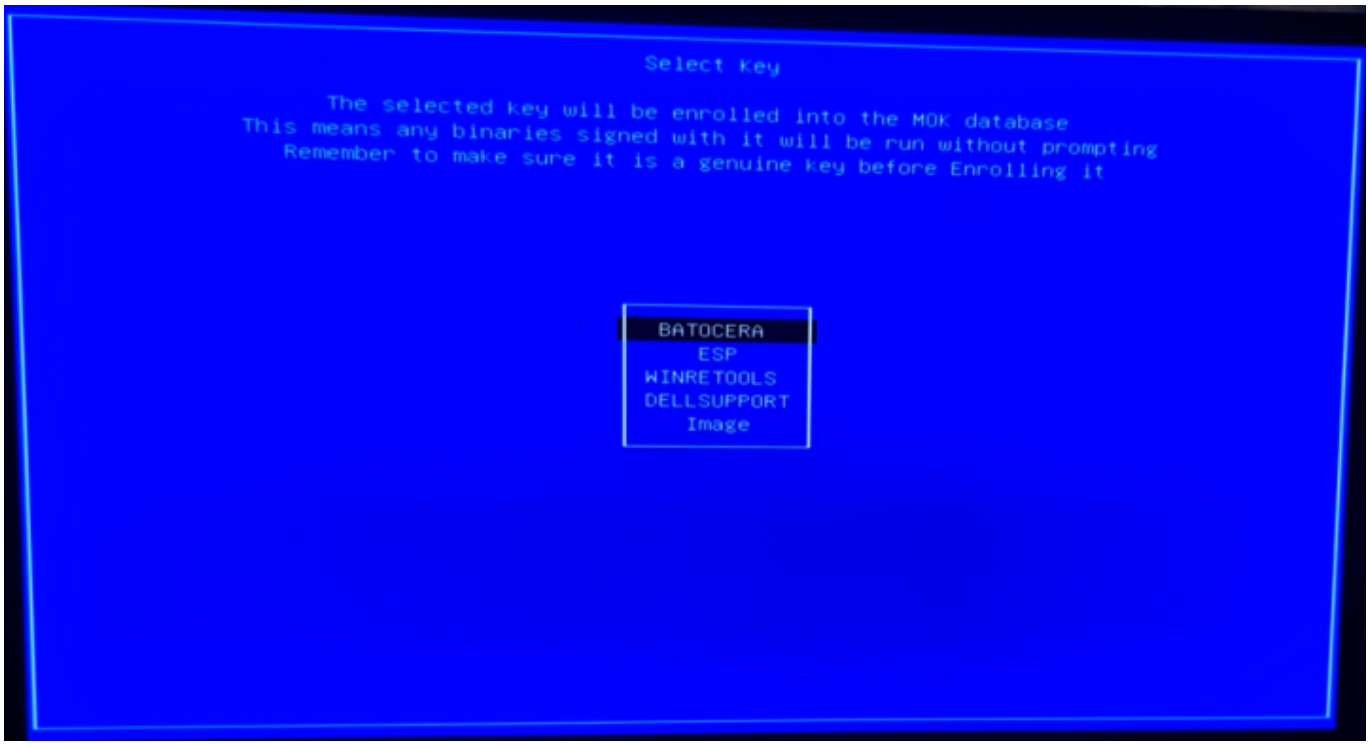
On the **Shim UEFI key management** screen, hit any key before the ten-second timer expires.



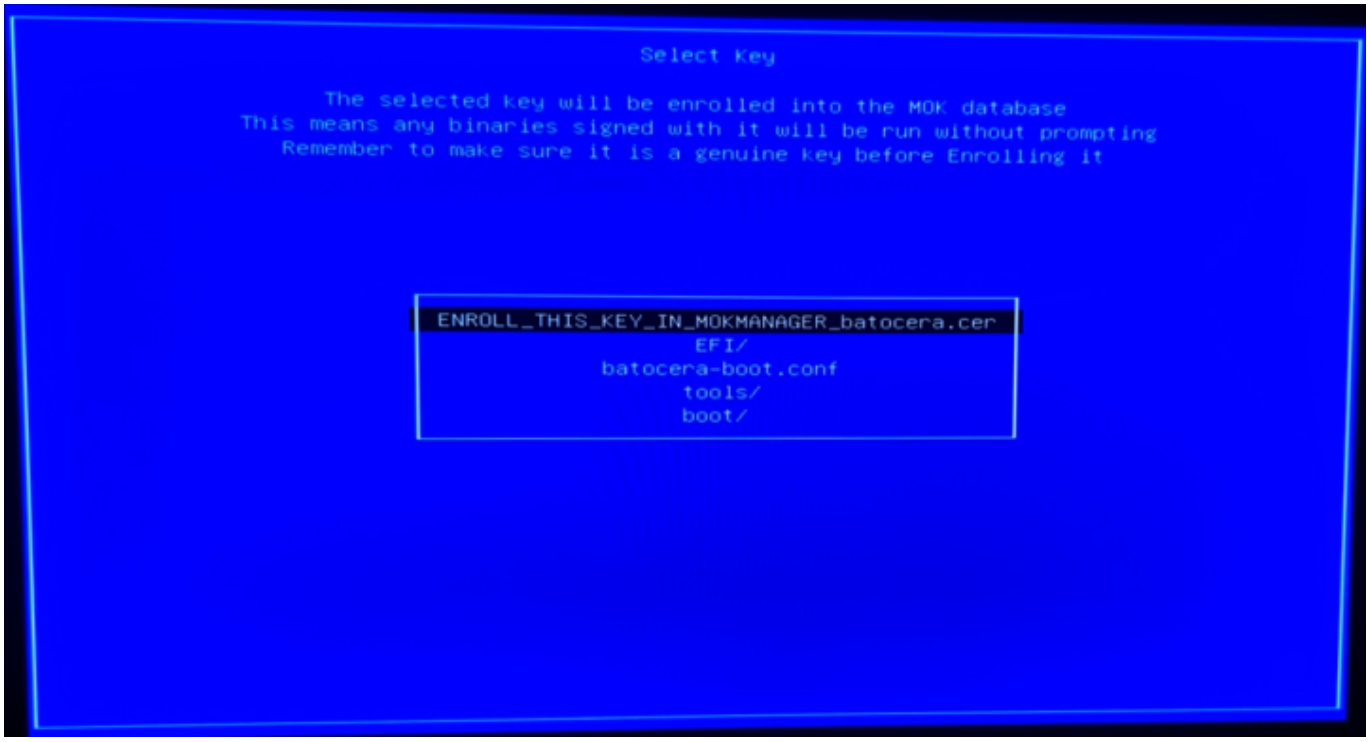
On the **Perform MOK management** screen, use the arrow keys to navigate to **Enroll key from disk**, and hit [ENTER].



On the **Select Key** screen, navigate to the **BATOCERA** partition and hit [ENTER].



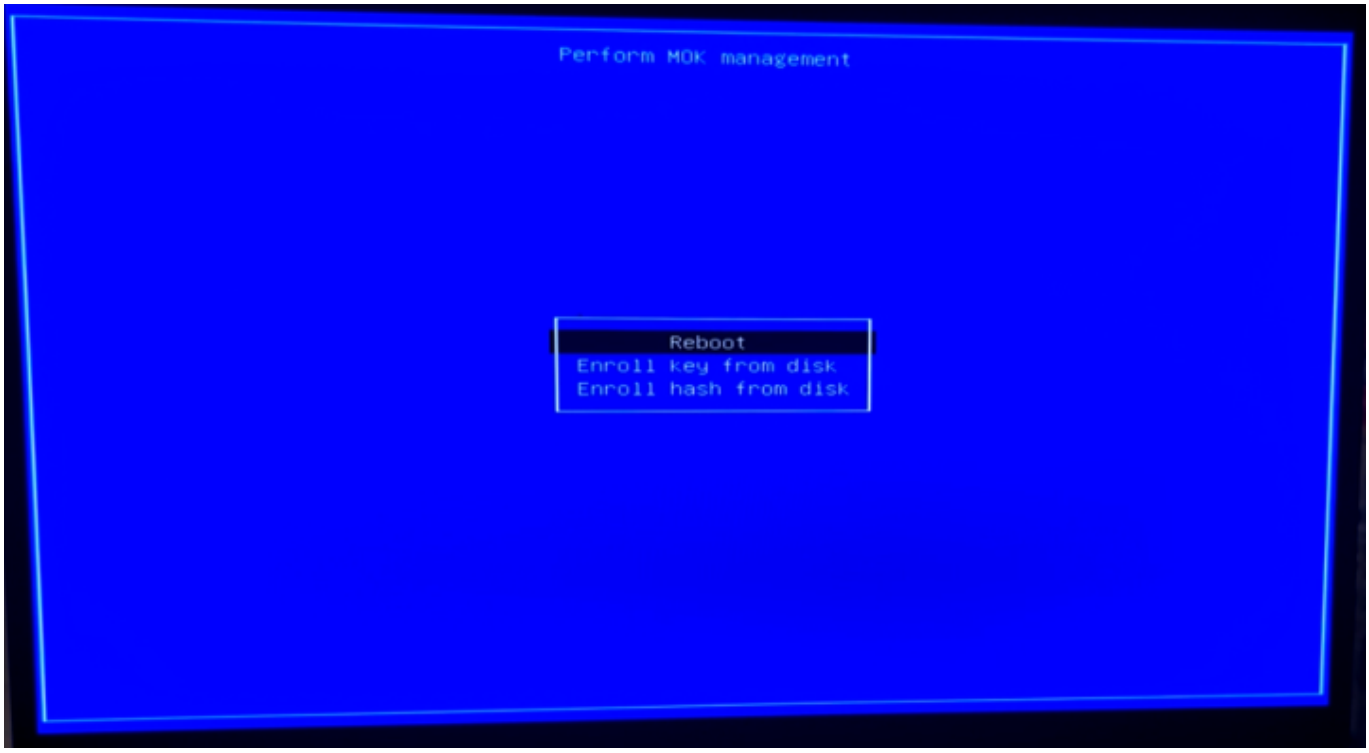
On the second **Select Key** screen, navigate to the **ENROLL_THIS_KEY_IN_MOKMANAGER_batocera.cer** certificate file, and hit [ENTER].



On the **Enroll MOK** screen, navigate to the **Continue** menu item, and hit [ENTER].

On the **Enroll the key(s)?** screen, navigate to the **Yes** menu item, and hit [ENTER].

On the second **Perform MOK management** screen, hit `[ENTER]` to reboot the system.



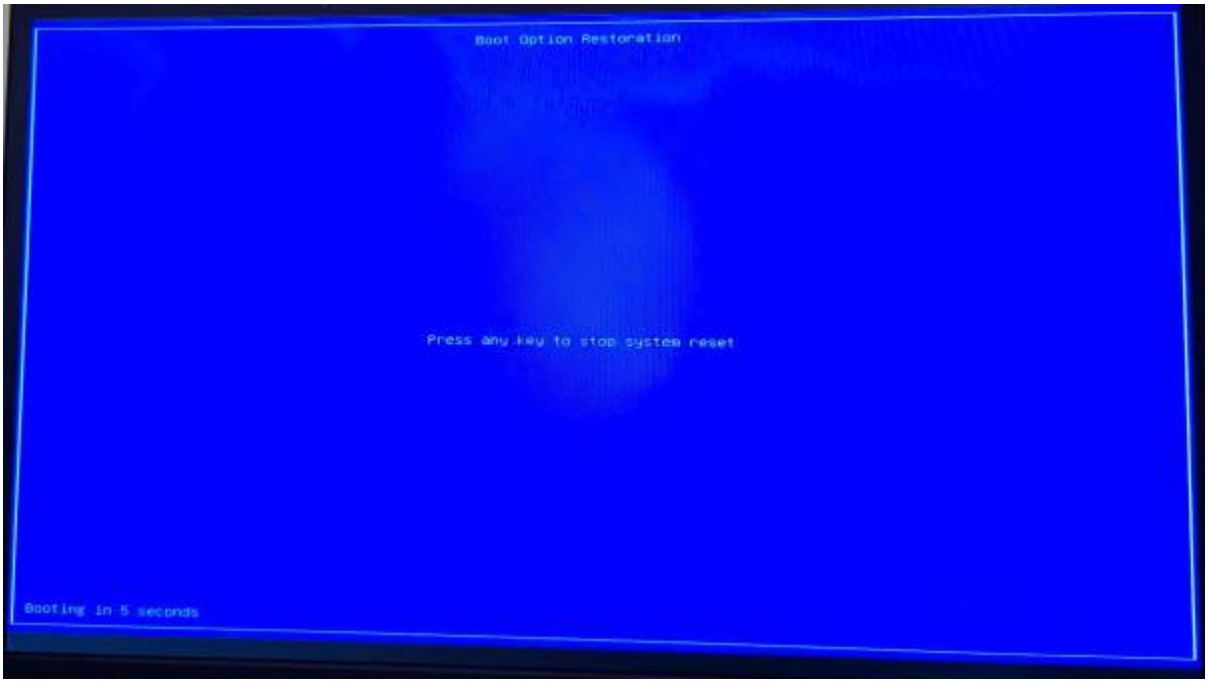
The system will reboot. If the system's TPM is enabled, proceed to the next section, otherwise it should automatically launch Batocera with Secure Boot enabled.

If other operating system disks are attached to the system, they can be selected for boot from your firmware's boot menu. The `efibootmgr` command-line utility in Batocera can also be used to adjust boot order, or to perform a one-time “boot-next” to another UEFI OS. (Fix Me! this commentary needs to move elsewhere)

TPM

Batocera's Secure Boot support requires some interaction between the bootloader and the system's hardware Trusted Platform Module (TPM), **even on systems where Secure Boot is not enabled**.

If the system's TPM is enabled, the first time you boot into the newer Batocera versions, and after completing the Secure Boot MOK management setup (if Secure Boot is enabled), a `Boot Option Restoration` countdown screen will be displayed. If no action is taken, the system will reboot repeatedly into this screen.



Connect a keyboard to the system, and press any key to move on to the next screen.

On the `Boot Options Restored` screen, use the arrow keys to select `Always continue boot` and press `[ENTER]`. The system will then boot into Batocera.

It will be necessary to perform this setup only once, as long as the correct option is selected.

Upgrading and Downgrading with Secure Boot

It is safe to upgrade to later Batocera versions while Secure Boot is enabled. Downgrading to **v39** or higher is also safe. If the newly upgraded/downgraded version was signed with a different signing key certificate which is not already enrolled, the MOK enrollment process may be reappear. It is possible to avoid this by disabling Secure Boot validation in the shim.

If Batocera is downgraded to **v38** or lower, the system may fail to boot in Secure Boot mode from the bootloaders installed by those versions. On systems where Secure Boot can be disabled, disabling it should allow the system to boot again. It is recommended to disable Secure Boot *before* such a downgrade.

After the downgrade, the Secure Boot capable bootloader referenced in the `Batocera` EFI bootloader entry may allow the earlier versions to boot with Secure Boot enabled. Whether this works or not will depend on the system's specific UEFI BIOS behaviors.

Disabling Secure Boot validation in the shim

Once Secure Boot is set up and working, it is possible to leave Secure Boot enabled in the system, while disabling Secure Boot verification in the shim. This is optional, and is riskier than the normal setup allowing only signed bootloader components to run.

To disable Secure Boot verification, SSH into Batocera and run the following:

```
mokutil --disable-validation
```

To re-enable Secure Boot verification:

```
mokutil --enable-validation
```

The `mokutil` command will request a (one-time) password. It is strongly recommended that you use the password 12345678 as the password for the validation state change, reasons for which will be explained below.

Reboot the system, and the MOK Manager will ask to allow changing the verification state. It will then request a few random characters of the password by specifying the position number of the desired character. For example, if it asks for character #2, type 2 and press [ENTER]. Repeat the process until the MOK manager is satisfied, then select the reboot option to restart the system with the new validation state.