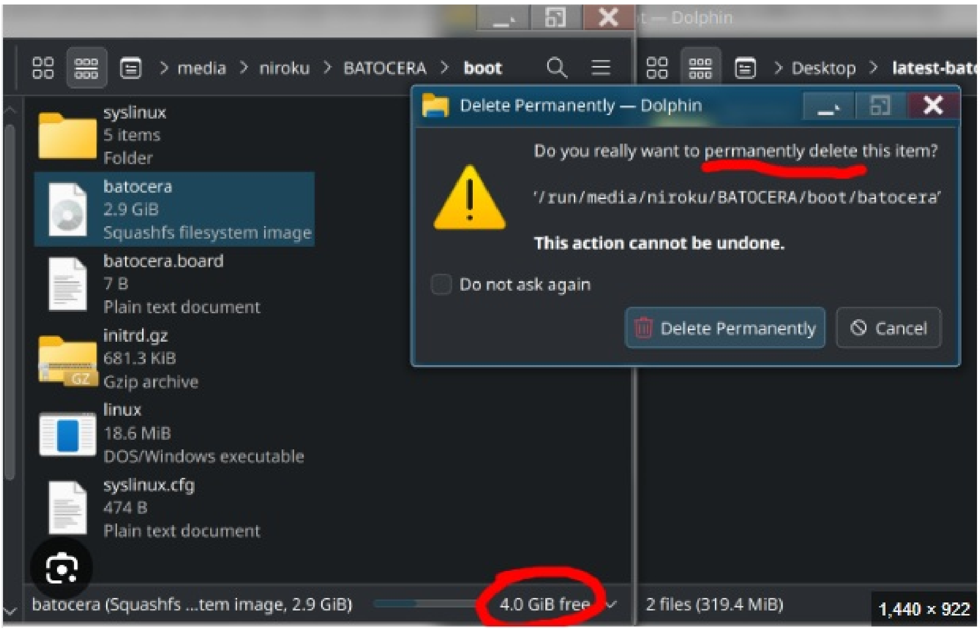
Home » BATOCERA » **BATOCERA Upgrading and Downgrading with Secure Boot User Guide**

Contents [hide]

BATOCERA

BATOCERA Upgrading and Downgrading with Secure Boot



syslinux
5 items
Folder

batocera
2.9 GiB
Squashfs filesystem image

batocera.board
7 B
Plain text document

initrd.gz
681.3 KiB
Gzip archive

linux
18.6 MiB
DOS/Windows executable

syslinux.cfg
474 B
Plain text document

Do you really want to permanently delete this item?

'/run/media/niroku/BATOCERA/boot/batocera'

This action cannot be undone.

□ Do not ask again

batocera (Squashfs ...tem image, 2.9 GiB) 4.0 GiB free

2 files (319.4 MiB)

Specifications

- Compatibility: x86_64 systems with Batocera v39 and higher
- Feature: Secure Boot support
- Certification: Batocera's encryption certificate

Product Usage Instructions

Preparation:

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

Configuration Steps:

1. A blue screen will appear with a message “Error Verification Failed (0x1A) Security Violation.” Hit [ENTER] on the keyboard to continue.
2. On the Shim UEFI key management screen, hit any key before the ten-second timer expires.
3. On the Perform MOK management screen, navigate to Enroll key from disk and hit [ENTER].
4. Navigate to the BATOCERA partition on the Select Key screen and hit [ENTER].
5. Navigate to the ENROLL_THIS_KEY_IN_MOKMANAGER_batocera.cer certificate file on the second Select Key screen and hit [ENTER].
6. Navigate to the Continue menu item on the Enroll MOK screen and hit [ENTER].
7. Navigate to the Yes menu item on the Enroll the key(s)? screen and hit [ENTER].
8. Hit [ENTER] on the second Perform MOK management screen to reboot the system.

Secure Boot

- 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

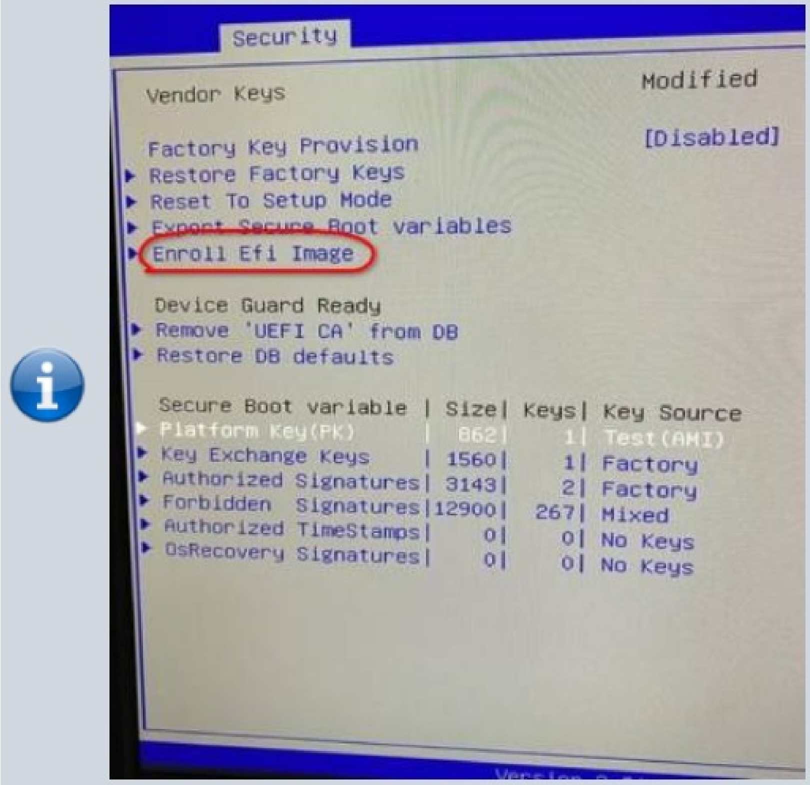
for the BitLocker recovery key before allowing Windows to boot.

- 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

For Batocera **v38** and lower, the keys must be enrolled by the BIOS itself (if available, otherwise just use legacy/CSM boot). 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”. The file to be selected, if asked, is `EFI/boot/bootx64.efi`.



```
   Security

 Vendor Keys                                      Modified

 Factory Key Provision                            [Disabled]
▸ Restore Factory Keys
▸ Reset To Setup Mode
▸ Export Secure Boot variables
▸ Enroll Efi Image

 Device Guard Ready
▸ Remove 'UEFI CA' from DB
▸ Restore DB defaults

 Secure Boot variable | Size| Keys| Key Source
▸ Platform Key(PK)     |  862|    1| Test(AMI)
▸ Key Exchange Keys    | 1560|    1| Factory
▸ Authorized Signatures| 3143|    2| Factory
▸ Forbidden  Signatures|12900|  267| Mixed
▸ Authorized TimeStamps|    0|    0| No Keys
▸ OsRecovery Signatures|    0|    0| No Keys
```

This method can be used instead of using the MOK management tool as explained below. Batocera **v38** and lower does not have the MOK management tool installed.

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.

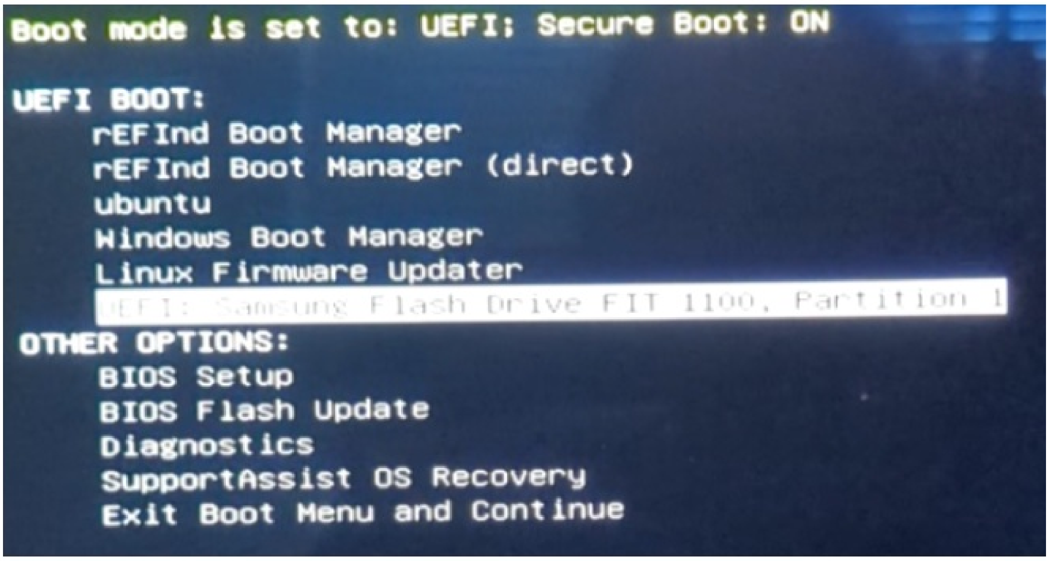
As some of this configuration is vendor-specific, consult the manual for the machine before getting started.

Preparation

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

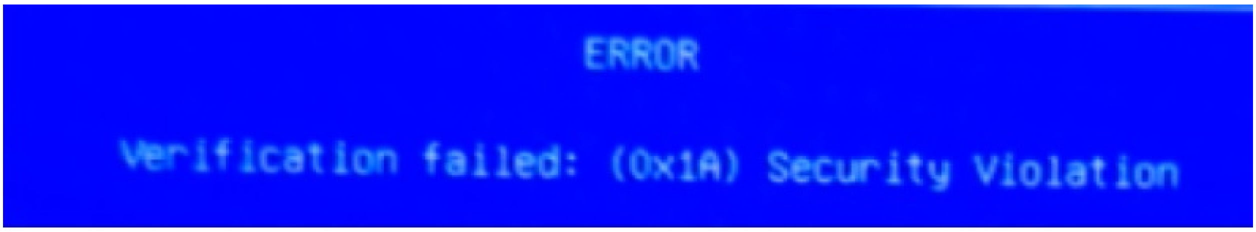
Configuration Steps

- 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.



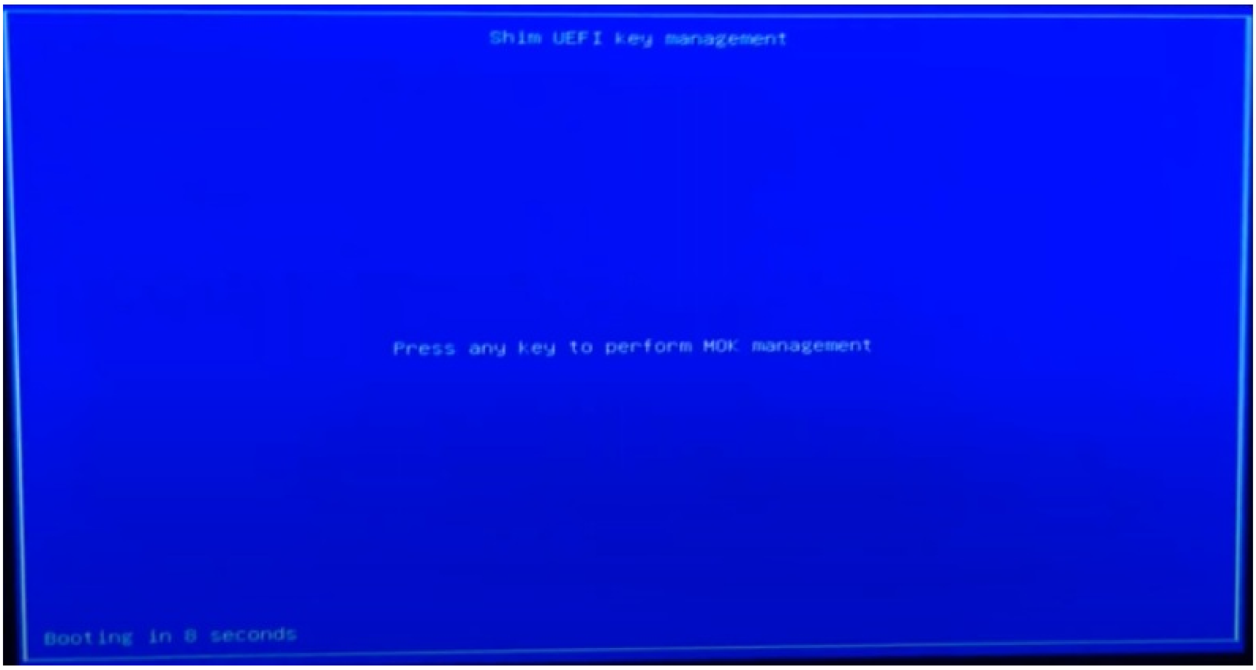
```
Boot mode is set to: UEFI; Secure Boot: ON

UEFI BOOT:
    rEFInd Boot Manager
    rEFInd Boot Manager (direct)
    ubuntu
    Windows Boot Manager
    Linux Firmware Updater
    UEFI: Samsung Flash Drive FIT 1100, Partition 1
OTHER OPTIONS:
    BIOS Setup
    BIOS Flash Update
    Diagnostics
    SupportAssist OS Recovery
    Exit Boot Menu and Continue
```

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



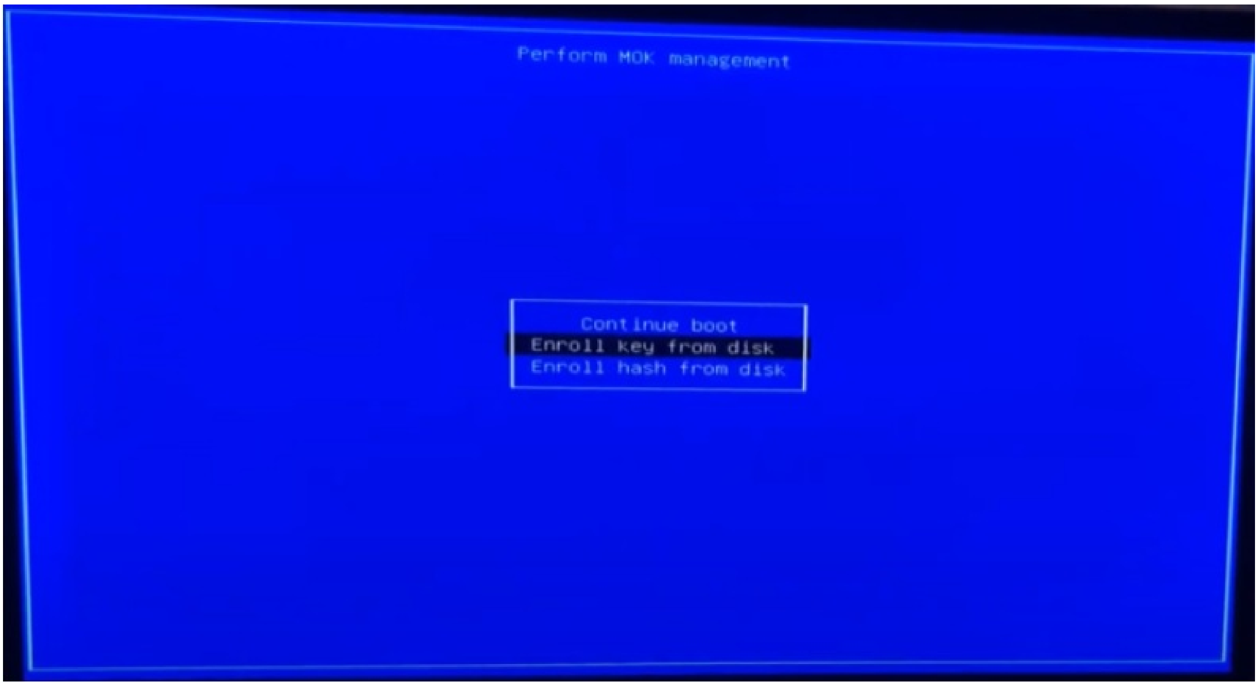
```
                    ERROR

Verification failed: (0x1A) Security Violation
```

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



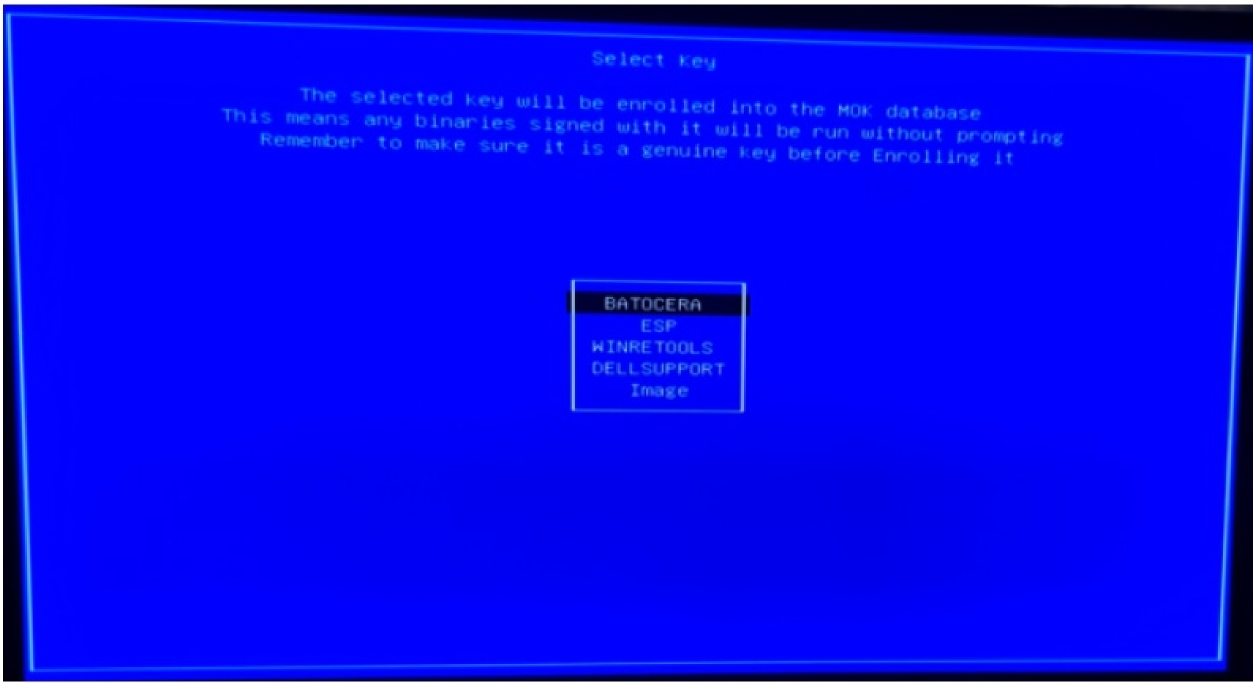
```
                 Shim UEFI key management



       Press any key to perform MOK management



Booting in 8 seconds
```

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



Perform MOK management

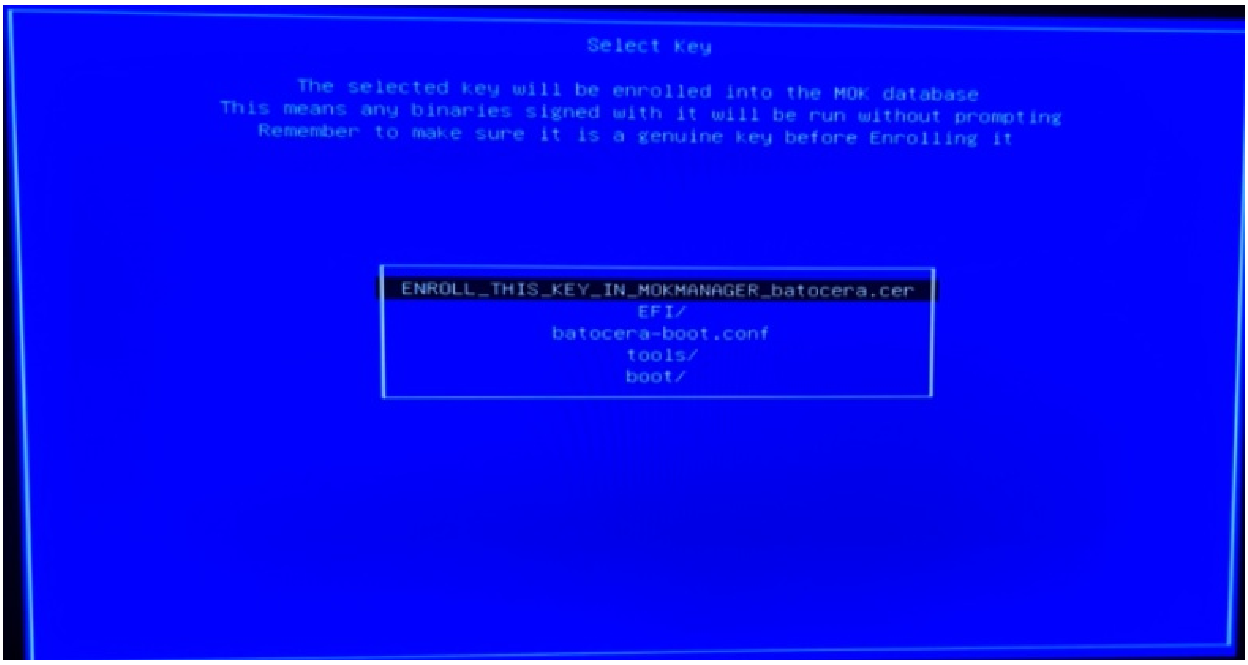
On the Select Key screen, navigate to the BATOCERA partition and hit [ENTER].



Select Key

The selected key will be enrolled into the MOK database
This means any binaries signed with it will be run without prompting
Remember to make sure it is a genuine key before Enrolling it

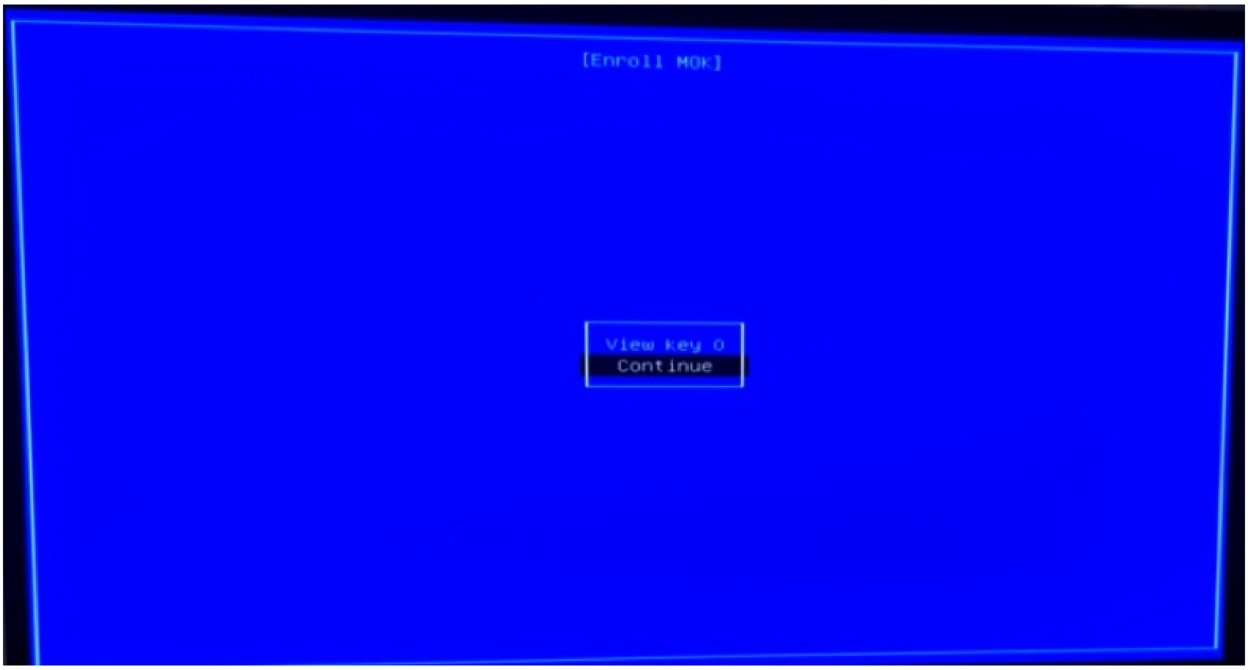
On the second Select Key screen, navigate to the ENROLL_THIS_KEY_IN_MOKMANAGER_batocera.cer certificate file, and hit [ENTER].



Select Key

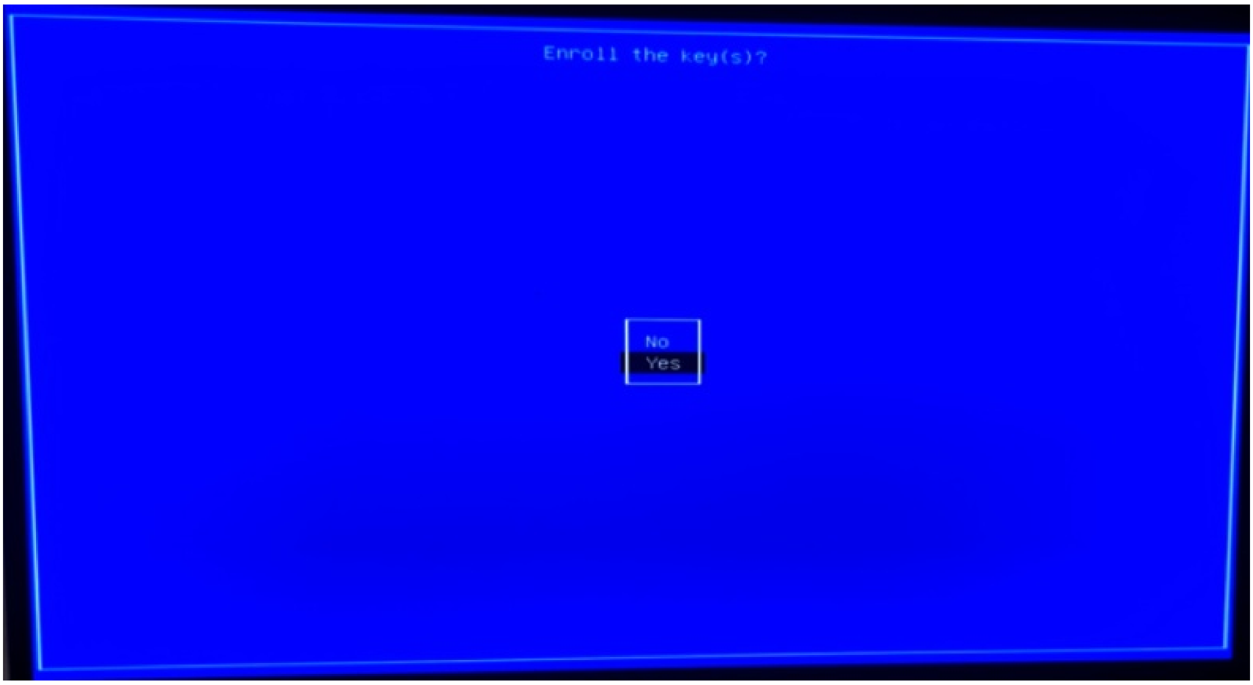
The selected key will be enrolled into the MOK database
This means any binaries signed with it will be run without prompting
Remember to make sure it is a genuine key before Enrolling it

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

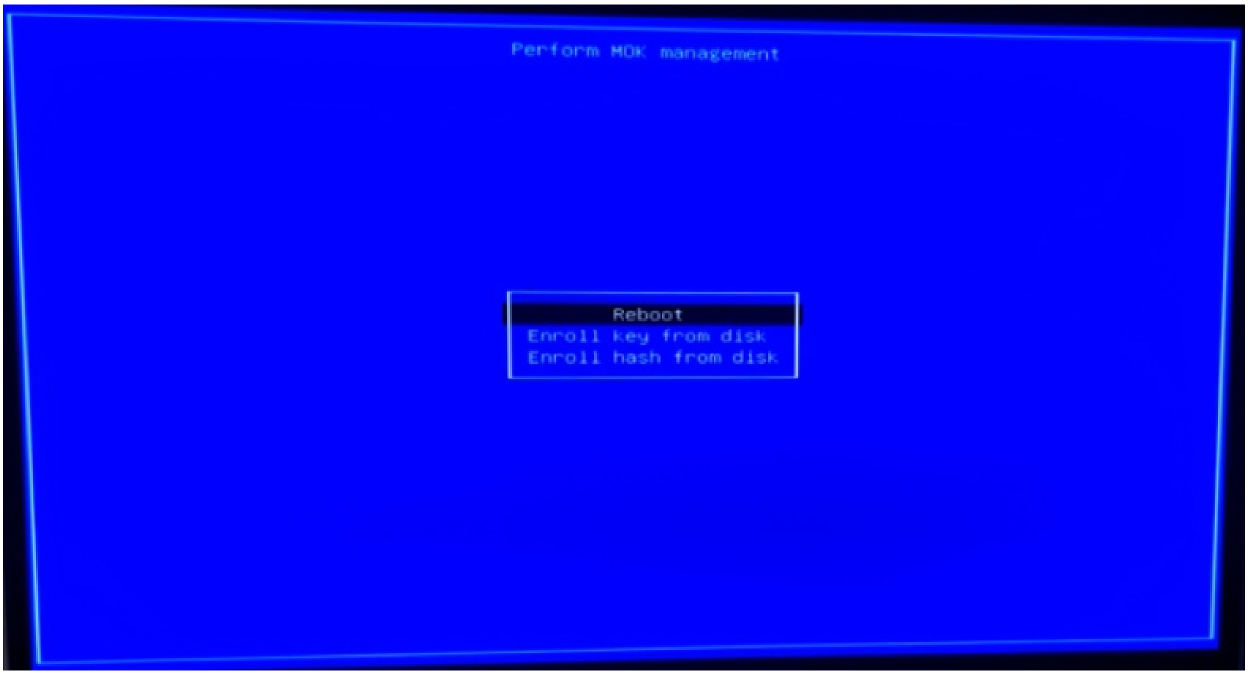


[Enroll MOK]

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



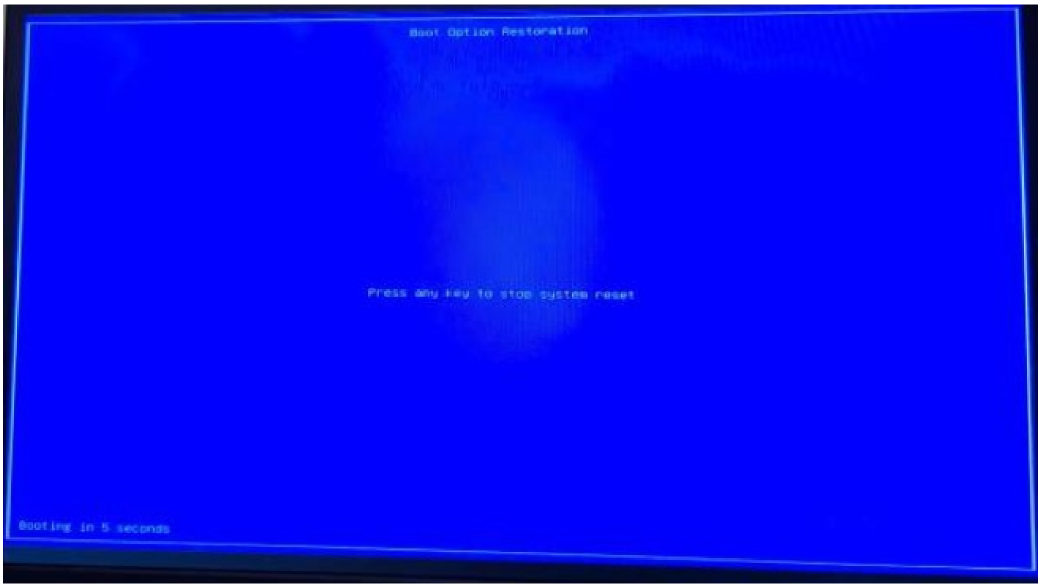
On the second Perform MOK management screen, hit `[ENTER]` to reboot the system.



- 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. (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 screen with a countdown will be displayed. If no action is taken, the system will reboot repeatedly into this screen.

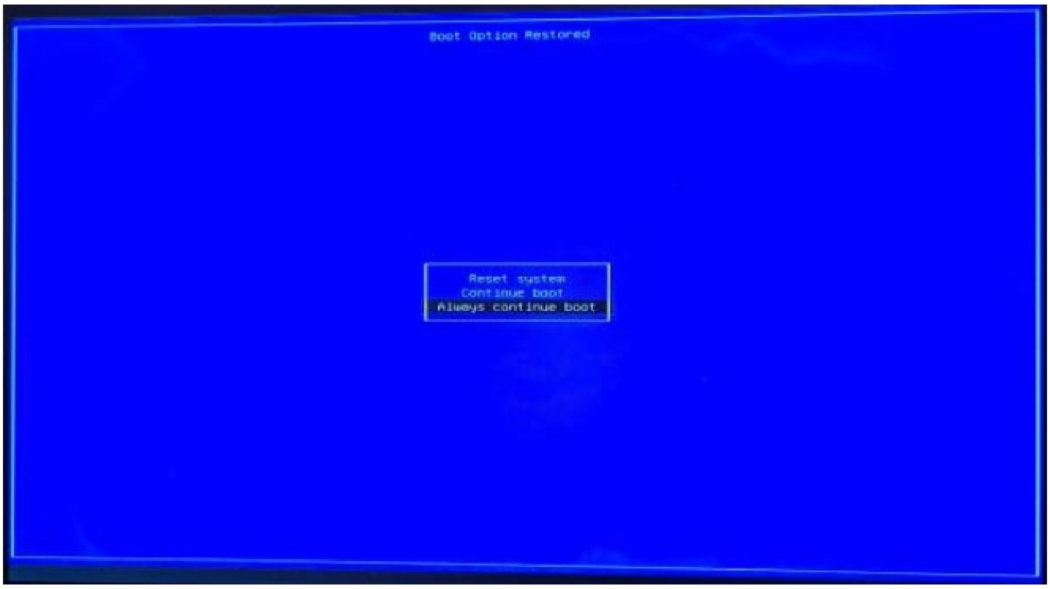


Boot Option Restoration

Press any key to stop system reset

Booting in 5 seconds

- Using a keyboard, 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.



Boot Option Restored

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.

FAQs

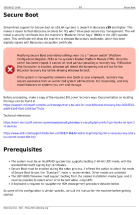
Q: What should I do if I encounter issues during the Secure Boot configuration process?

A: If you encounter any issues during the Secure Boot configuration process, refer to the Batocera.linux Wiki for troubleshooting steps or consult your machine's manual for vendor-specific instructions.

Q: Can Batocera be installed on systems managed by someone else, such as an employer?

A: It is recommended to only install Batocera on systems you own and manage to avoid complications with Secure Boot settings and potential recovery key requirements.

Documents / Resources

 2025/05/27 19:48 1/7 Secure Boot **Secure Boot** Streamlined support for Secure Boot on x86_64 systems is present in Batocera **v39** and higher. This makes it easier to flash Batocera on drives for PCs which have poor secure key management. This will install a security certificate into the machine's "Machine Owner Keys" (MOK) in the UEFI variable store. This certificate will allow the machine to execute Batocera's bootloader, which has been digitally signed with Batocera's encryption certificate. 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. Batocera.linux - Wiki - https://wiki.batocera.org/	BATOCERA Upgrading and Downgrading with Secure Boot [pdf] User Guide Upgrading and Downgrading with Secure Boot, Downgrading with Secure Boot, with Secure Boot, Boot

References

- User Manual

BATOCERA

BATOCERA, Boot, Downgrading with Secure Boot, Upgrading and Downgrading with Secure Boot, with Secure Boot

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

Manuals+ | Upload | Deep Search | Privacy Policy | @manuals.plus | YouTube

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.