Secure Boot tools for ArcaOS (Sboot v1.0)

Copyright 2022 Bankai Software

Licensed for use under the GPL v2

Development coordinated by OS2Voice.org

Table of content

Getting Support & Disclaimer

SBoot is for UEFI systems only and *will not run* if your system boots OS/2 in CSM/BIOS mode. It has been tested on a limited number of computers and performed as expected on each. This software will only work on ArcaOS version 5.1.0. and higher.

If you encounter an issue or have a question, please send an email to helpdesk@os2voice.org. In your email provide a clear description of the issue you encountered and any error message you got. Emails will be answered on a best effort basis.

Before running this software, please shut down all programs under ArcaOS.

If you want to support the Dutch OS/2 VOICE please consider making a donation via our donation website: https://donation.os2voice.org.

Note that each machine is different: there is *no guarantee* that it will work properly on yours. This software is provided as-is and its use is entirely *at your own risk!* Bankai Software B.V. and the Dutch OS/2 VOICE foundation cannot be held liable for any damages resulting using the Sboot software.

The Sboot software is published under the GPL 2 license, the software sources can be found in in the directory sources\efitools.zip.

How secure boot works and how to enable it with ArcaOS.

When Secure Boot is enabled, the UEFI firmware will not load a binary (i.e. a UEFI program or driver) unless it has a cryptographic signature that can be decrypted using one of the keys in its database.

Given that several of Microsoft's keys are always in the database, one way for a third-party to make its software bootable is to have Microsoft sign its binary. This is what the Linux community has done with their 'Shim' bootloader and 'Machine Owner Key' (MOK) system.

Since we would prefer not to get Microsoft involved, the OS/2 community has taken a different approach. Arca Noae signs its UEFI binaries with its own private key but leaves it up to the user to add its public key to the certificate database on your PC.

The UEFI specification does not allow a program to change the database unless it is signed with a special key that only MS has. Lacking that, the only permitted alternative is to have a user who is sitting in front of the computer manually enter any updates. There are two ways to get the certificate of ArcaOS installed on your PC:

1. Some Desktop systems offer a “Key Maintenance” option to do this. If your system has this feature, you can use it to import AN's key from disk yourself (look in your EFI System Partition for '\EFI\BOOT\OS2\ANdb.crt').

2. The above feature is missing on many Desktop systems and laptops. That's where SBoot comes in. Any machine that supports Secure Boot is required to offer an option to switch the system from the normal “User Mode” to a special “Setup Mode”. Switching to Setup mode deletes *all* keys in the database and leaves the machine completely non-secure. In this state, *any* program can modify the database however it wishes without needing a key. And that is what SBoot does.

   In Step 3, it takes advantage of “Setup Mode” to add Arca Noae's key and restore the original keys saved in Step 1. When you reboot, the firmware sees that the database has all the required keys and switches the system back to secured “User Mode”.

Overview

SBoot allows you to boot ArcaOS 5.1 when your UEFI-based computer's **Secure Boot** feature is enabled. Use it if you plan to run Windows 10 or 11 on this system, or if you simply want to be ready in case you enable Secure Boot someday.

SBoot guides you through the 3 steps needed to install Arca Noae's public encryption key in your firmware's Secure Boot database.

- Step **1**: backs up the database
- Step **2**: boots into your system's firmware so you can switch to “Setup Mode”
- Step **3**: runs after you boot back into ArcaOS to add Arca Noae's key and restore the database

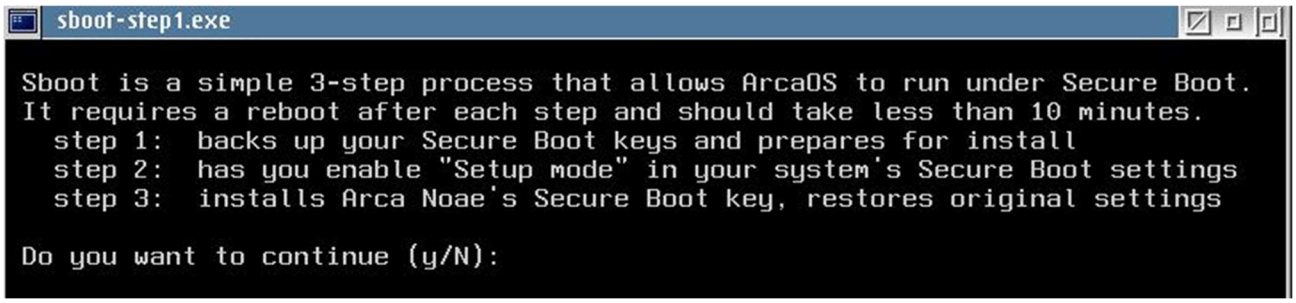
When complete, the database will be identical to the original except that it will have one new key for ArcaOS. After a successful run, you can delete the SBoot package because you should never need to run it again on your PC. If you try, SBoot will advise you that AN's key is already installed and will exit.

SBoot is as automated as possible but it still requires your involvement. The UEFI specifications demand that a user sitting in front of the computer - not a program - make these firmware changes. The only alternative is to get Microsoft involved, something we'd prefer not to do.

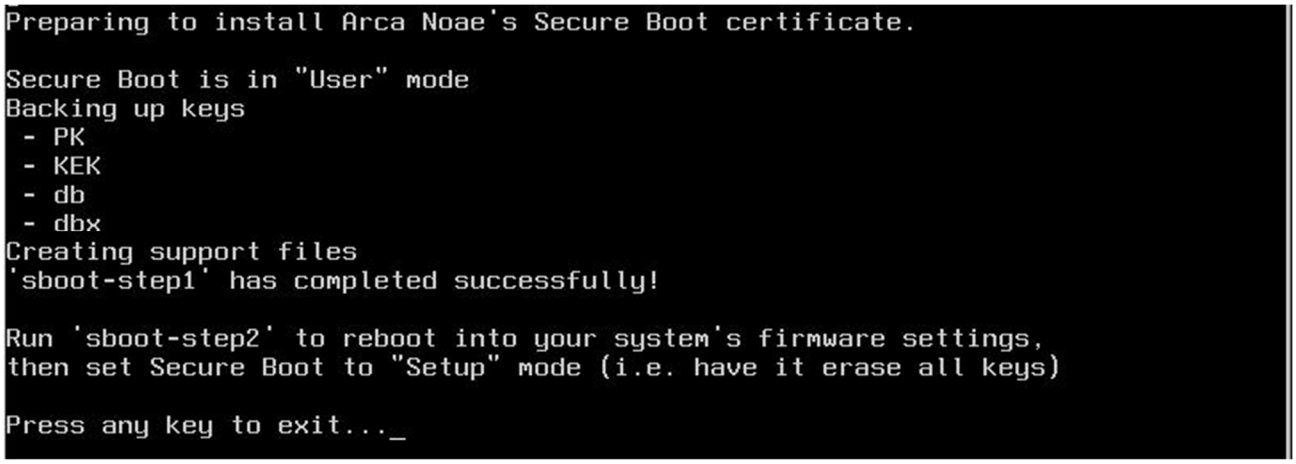
Step 1 Running SBoot

SBoot is a completely self-contained package that requires *no additional files* and *no user configuration*. The top level of the SBoot folder contains the 3 programs you will use. Run them by doubleclicking on their icons - no need to use a commandline. There are also two subfolders for SBoot's internal use; please do not modify them in any way.

Doubleclick on 'sboot-step1.exe'. You should see:



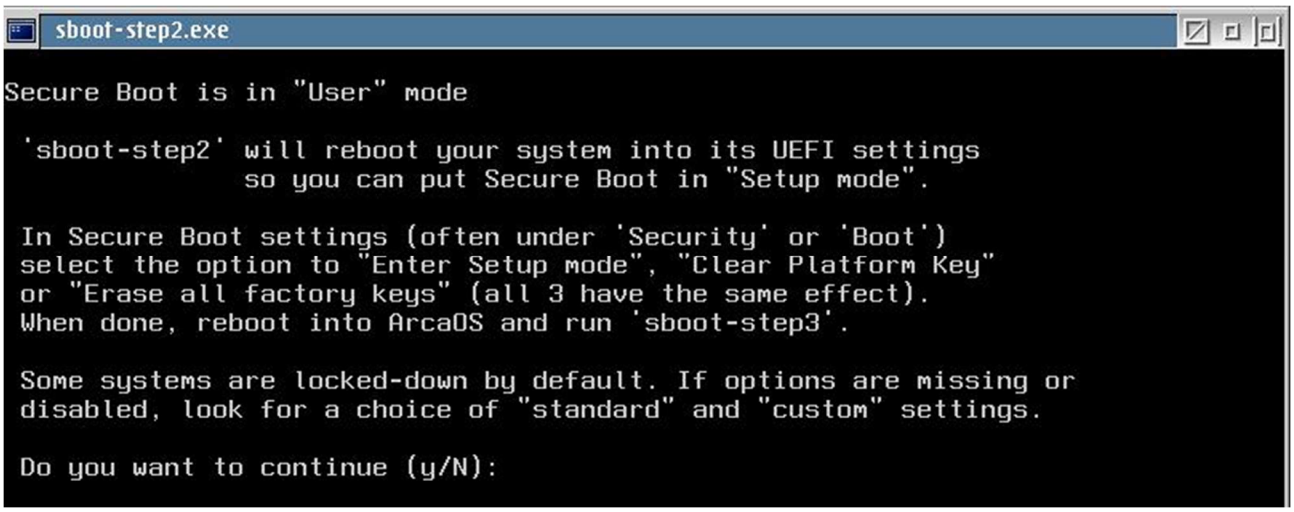
When you press 'Y' to continue, this will be displayed:



Press any key to finish Step 1.

Step 2

Doubleclick on 'sboot-step2.exe'. You should see:



When you press 'Y' to continue, your system will reboot to your firmware (BIOS) setup screens.

Your goal here is to locate the screen(s) that contain Secure Boot options. Somewhere in these screens is an option to "Enter Setup mode" or "Clear Platform Key" or "Erase all factory keys". Regardless of the name, the effect is the same: it erases all keys (which is why we backed them up in Step 1).

When you find the option, select it and confirm your choice.

Notes:

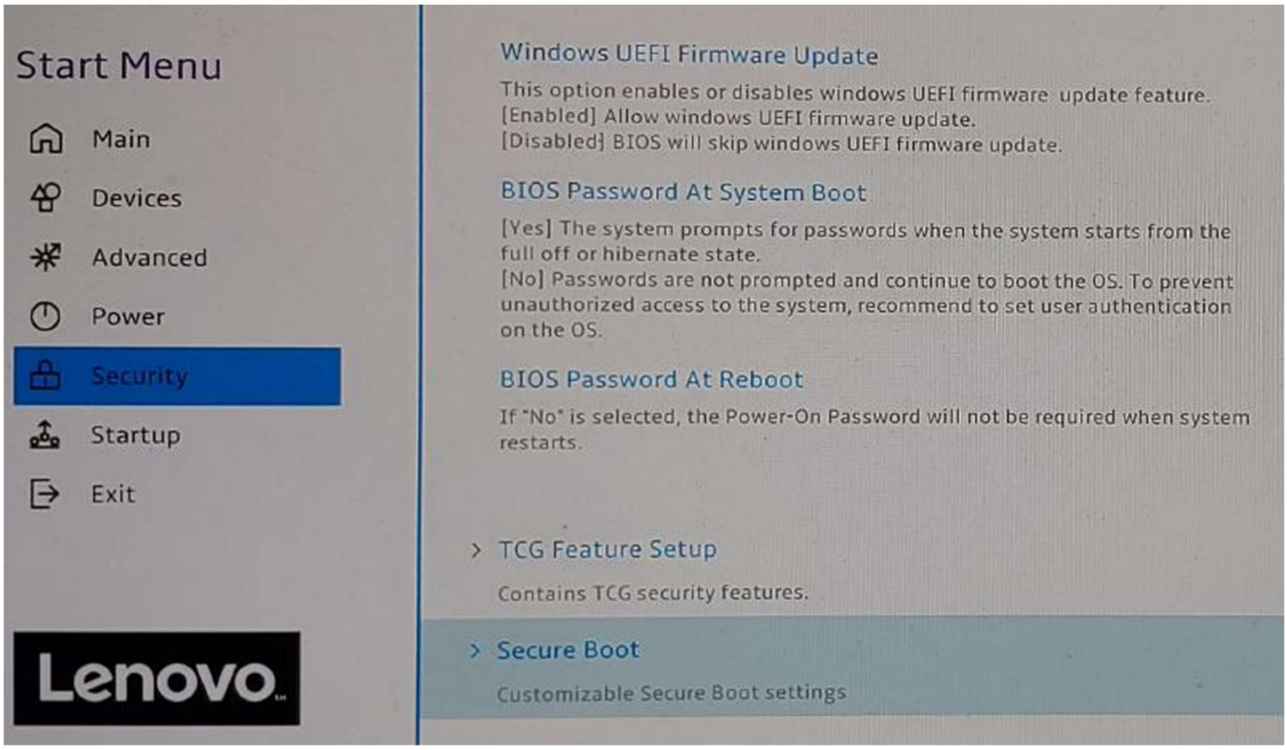
- Any machine that lets you delete the security keys also has an option to restore the factory-supplied default keys, so you can always restore the machine to its original state.

- If "Enter Setup mode" is disabled or missing, the machine may be in “Deployed Mode” which prevents manual changes. Look for an option to "Enter User mode" to re-enable changes. Alternately, the machine may offer a choice of “Standard” and “Custom” settings. If so, choose “Custom”.

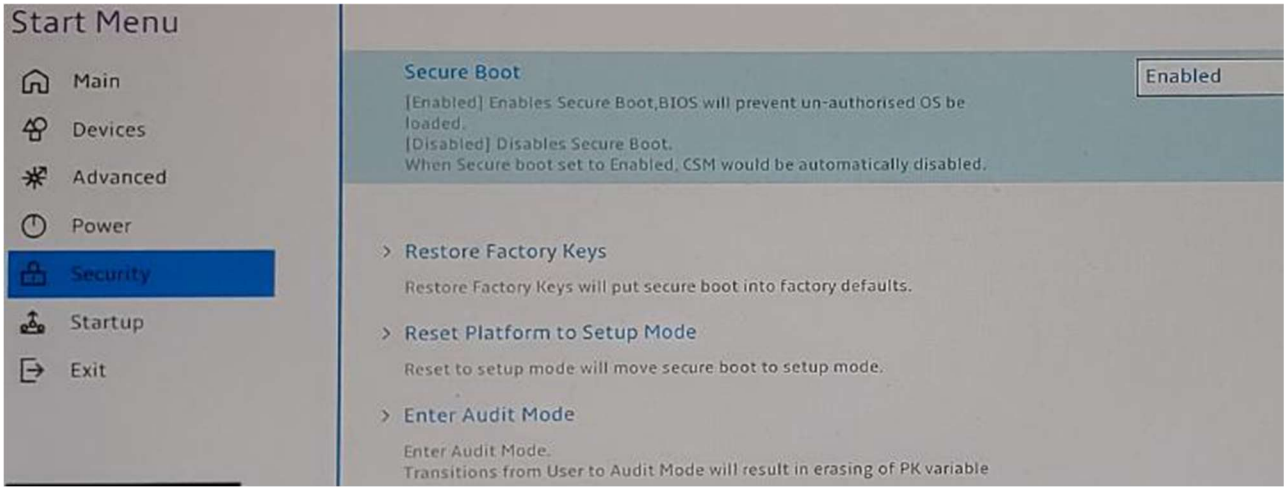
- Every computer manufacturer uses different screens and different terms, but any machine that supports Secure Boot has these options because the UEFI spec requires them. The following are screenshots from a Lenovo desktop system:

Step 2 *(continued)*

This is firmware's top-level 'Security' screen and links to the 'Secure Boot' options:

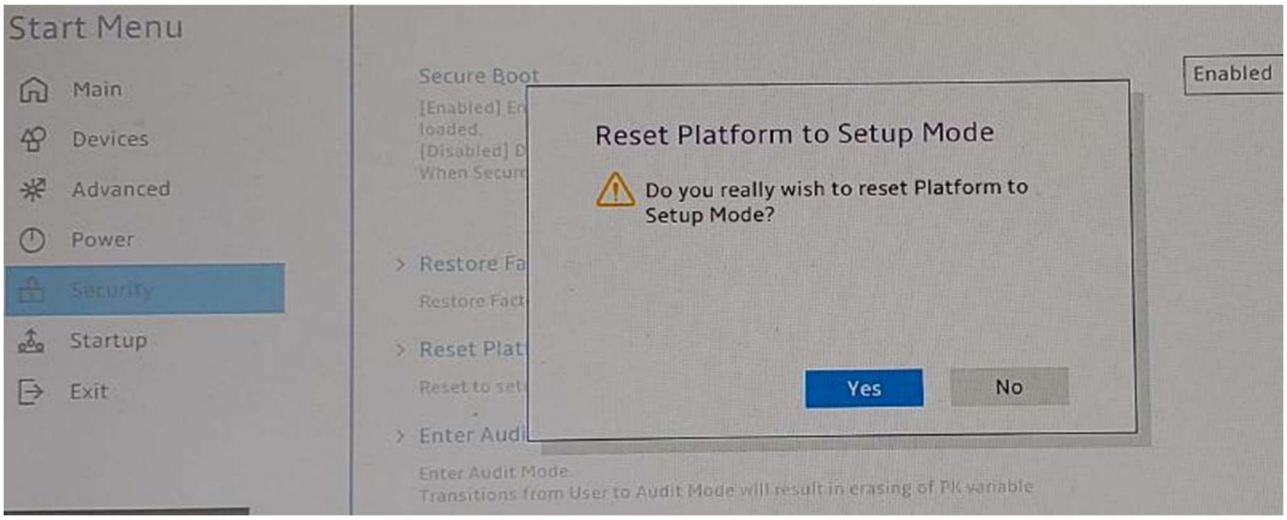


This screen has the option we're looking for, 'Reset Platform to Setup Mode':



Step 2 *(continued)*

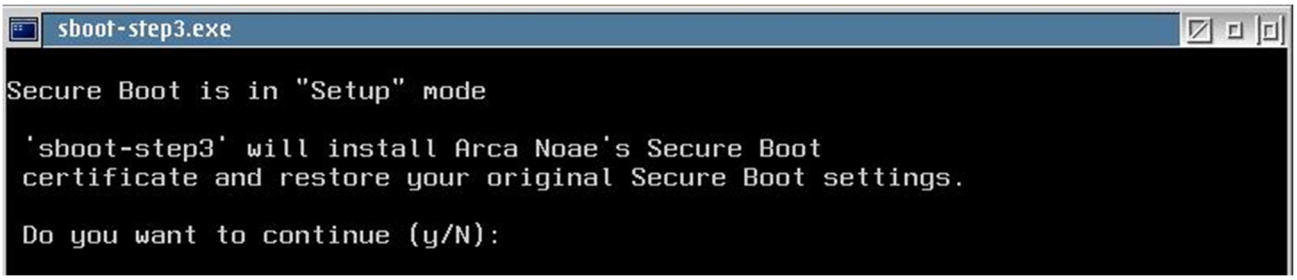
After selecting 'Reset Platform to Setup Mode', a confirmation dialog appears:



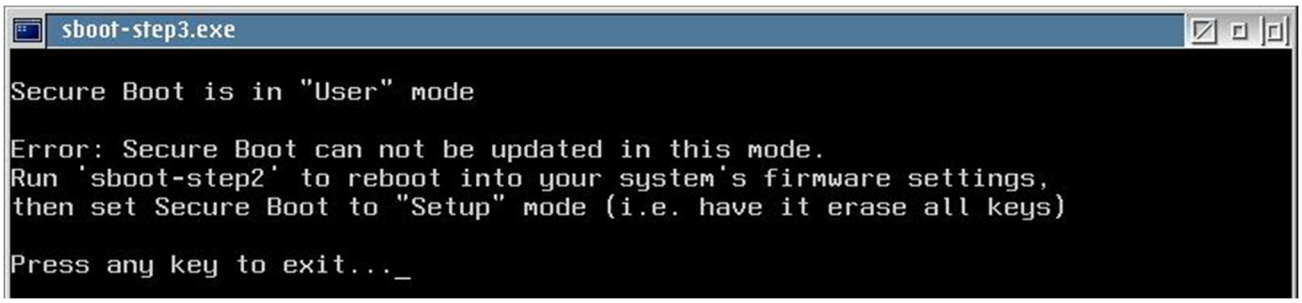
Once you've found the option and selected it, save your changes, exit firmware setup, and reboot ArcaOS.

Step 3

Doubleclick on 'sboot-step3.exe'. You should see:



Important: note that SBoot reports your machine is now in **Setup** mode, indicating that Step 2 was successful, and you are ready to finish the process. If Step 2 failed, you will see this instead:



If Step 2 was successful, press 'Y' to continue. This will be displayed:

Press any key to finish Step 3, then reboot.

You can now enable Secure boot in your UEFI setup.