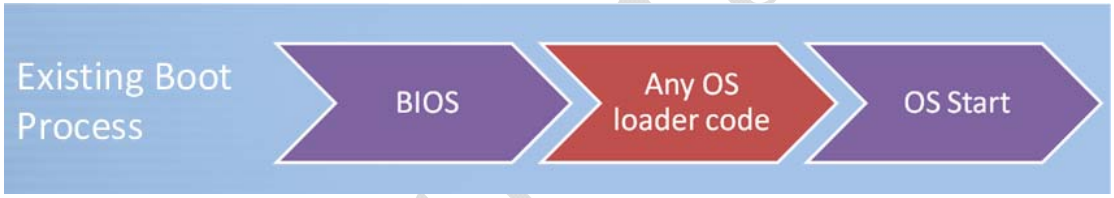
Lanner's Secure Boot and Secure Flash

Overview

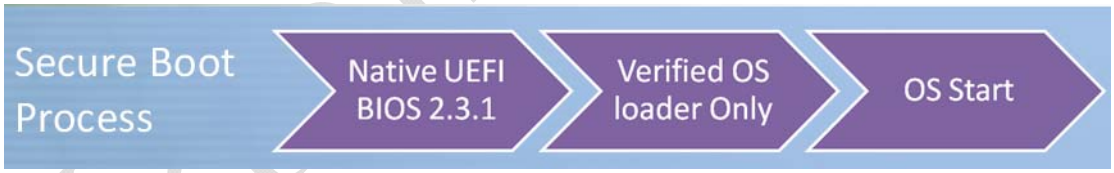
Secure Boot is a form of verified booting technology which ensures boot path validations. As defined in UEFI (Unified Extensible Firmware Interface) specifications, this BIOS-based technology assures that the system firmware checks if the boot loader is signed with a cryptographic key contained in the database in the firmware. In other words, Secure Boot is a firmware-based boot path validation mechanism that contains cryptographic key and it will check if the boot loader is protected by the key. Only the ones with proper digital signature verification in the next-stage boot loaders, kernels or user space can access the system. This will prevent the execution of codes that are not signed with the cryptographic key programmed in the system firmware.

Differences Between Existing Boot Process and Secure Boot Process:

In the "Existing Boot Process", the BIOS will run any OS boot loader, even if it is a malware.



In the "Secure Boot Process", the UEFI BIOS will only launch a verified OS boot loader. Malware cannot replace the boot loader.

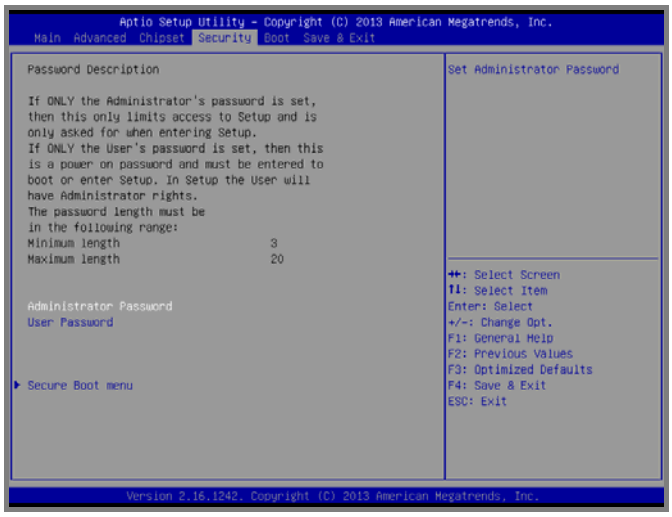


Device Operations

Lanner's network appliances are compatible with Secure Boot to prevent unsigned execution of codes from tampering the boot path or boot media. Once the console-to-serial connection is properly established, the administrator can run a test on a terminal PC with compatible software emulator, such as Tera Term or Hyper Terminal Utility, as long as VT100/ANSI modes are set. Regarding operating systems, Secure Boot is supported in Linux, Windows 8 or above, and FreeBSD 10.1.

There is no specific hardware requirement and is BIOS-based; just a non-volatile storage that can be switched to read-only mode during the system boot-up. As soon as

Lanner network appliances are booting up, simply enter the BIOS menu. Then go to “Security” and select “Secure Boot” to enable it.



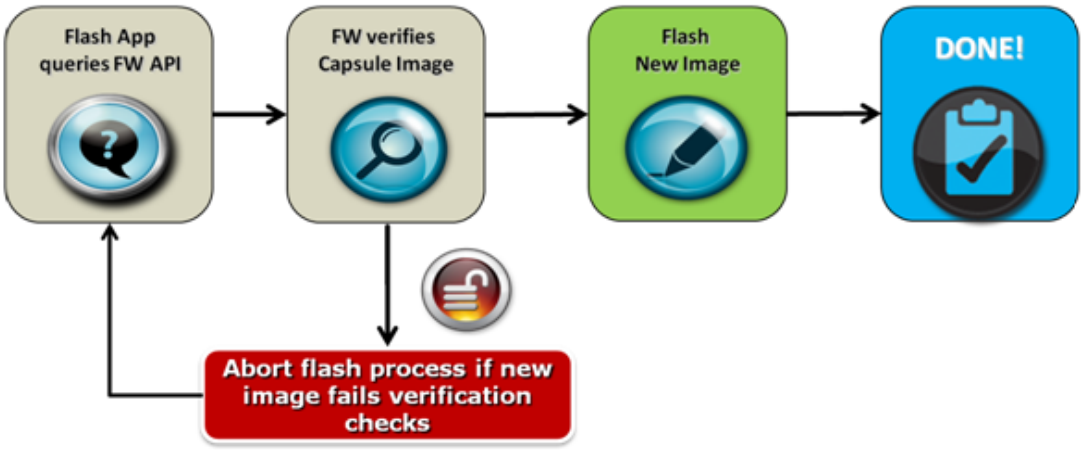
Once the status of Secure Boot is “active”, the system will be secured from being tampered by executions of unvalidated codes to attack your boot path or boot media.

Lanner’s Secure Flash for BIOS Protection

Lanner also releases an enhanced version of Secure Boot, named “Secure Flash”. The software technology verifies and performs updates, as well as enforces write protect to block unauthorized code execution to your BIOS. When executing BIOS updates, a signed key which is contained in the database in the system firmware is required. In other words, the digital signature is added in the binary file and only legitimate BIOS images are allowed to be read from the disk and updated.

Secure Flash provides three types of BIOS updates: runtime update, recovery update and capsule update, all protected by secure flash keys.

- Runtime update – as defined by its term, BIOS will be updated during the runtime.
- Recovery update – BIOS images will be read from the disk during the execution of recovery and the updates will be carried out simultaneously.
- Capsule update – when the system enters S3 (Suspend-to-RAM) state and then resumes, BIOS will be updated.



For Lanner network appliances, certain flash utility programs are required and some commands must be issued depending on the update modes: runtime, recovery or capsule. For more details, please consult with Lanner representatives for user guides.

Lanner's Verified Models

FW-7573
FW-8771

Lanner's Compatible Models

Compatible models include Lanner's hardware platforms driven by Intel Rangeley CPU/C226 PCH, which require BIOS customization to make Secure Boot available.

FW-7525
FW-7526
NCA-7551
FW-7571
FW-7585
FW-8759