Verify Support for UEFI Secure Boot

For supported software information, click here.

UEFI secure boot is a verification mechanism for ensuring that a Versa Operating System™ (VOS™) device boots only software components that are trusted. The UEFI secure boot verifies the software components sequentially, starting with verifying the signature of the boot loader.

You can use UEFI secure boot on devices with UEFI firmware that supports secure boot, which include Versa CSG300 and CSG700 series appliances running Ubuntu18.04 (Bionic). To ensure that you receive CSG300 and CSG700 series appliances from the factory that support UEFI secure boot and on which Ubuntu 18.04 is installed, include the SECURE-BOOT-CSG300-700 SKU when you place your order. Otherwise, the appliances are shipped with Ubuntu 14.04 (Trusty) for backwards compatibility reasons.

When the appliance on which secure boot is enabled starts, the firmware checks the signature of each portion of the boot software, including low-level drivers and the operating system. If the signatures are valid, the appliance boots and the firmware turns control over to the operating system. Providing a secure handoff allows the secure boot to act as an interface between the VOS software and the firmware.

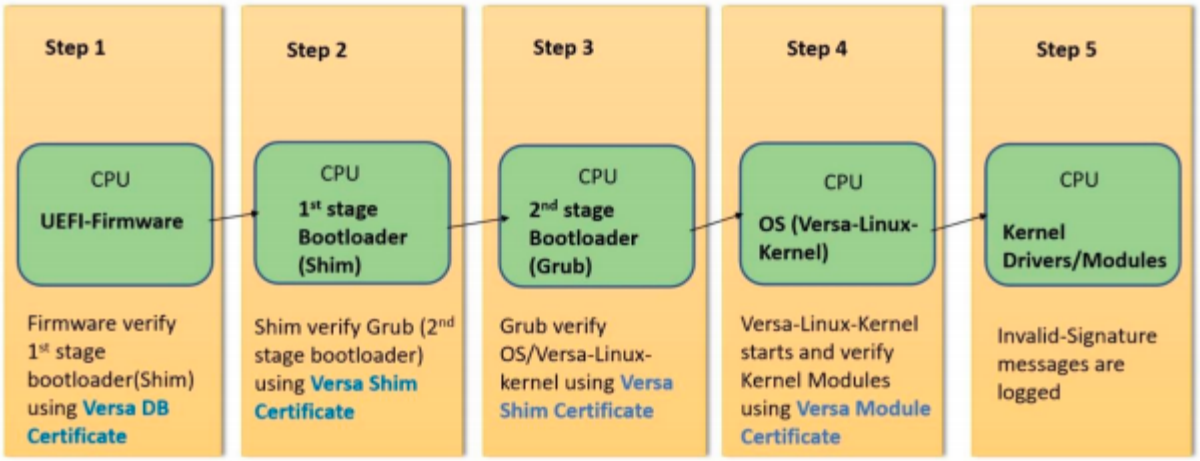
Versa appliances that support UEFI secure boot provide UEFI firmware-based root-of-trust, chain-of-trust, and other protections against bootkits, kernel-mode rootkits, and driver rootkits when the appliance is booting by verifying the signatures of signed boot loaders, operating system kernels, and kernel drivers.

The root of trust is based on a root Versa certificate that is present in the UEFI firmware. The chain of trust is based on a chain of Versa certificates that depends on the previous certificate. The keys used for root of trust and chain of trust are based on public-key cryptography. All the Versa private keys used for signing secure boot images are securely stored by Versa Networks.

Note: Legacy devices with legacy BIOS do not support UEFI secure boot. Only legacy devices that has UEFI secure boot firmware or BIOS can install the VOS in UEFI mode by using a bootable USB and enabling secure boot.

Versa UEFI Secure Boot Sequence

The following figure illustrates the Versa UEFI secure boot sequence, which performs the steps necessary to verify all the software components involved in the boot-up process.



The following paragraphs describe the steps in the Versa UEFI secure boot sequence:

1. The UEFI firmware verifies the signature of the shim boot loader using the public key from the Versa database certificate. (Note that this certificate must have already been uploaded to the UEFI firmware database variable or database.) After verification, control is transferred to the shim boot loader.
2. The shim boot loader verifies the signature of the Grub boot loader using the public key from the built-in Versa shim certificate. After verification, control is transferred to the Grub boot loader. This transfer forms a chain of trust.
3. The Grub boot loader verifies the signature of the Versa-customized Linux kernel using the public key from the Versa shim certificate. After verification, control is transferred to the Linux kernel. This transfer forms an extended chain of trust.
4. The customized Linux kernel verifies the signature of all the kernel modules (.ko files) using the public key from the Versa module certificate, which is embedded in the customized Linux kernel. This step forms an extended chain of trust.
5. Error messages for all invalid signature and kernel modules with no signature are logged.

Check VOS Secure Boot Status

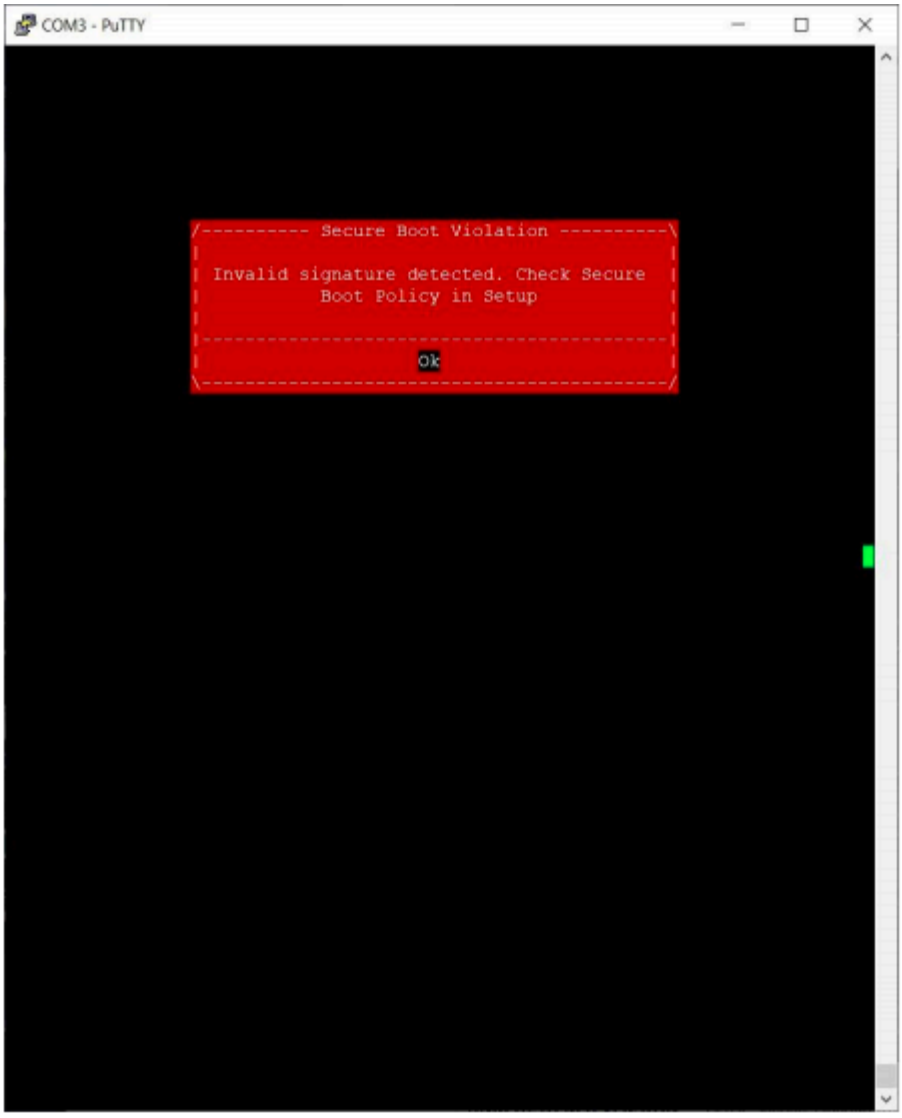
To check when UEFI secure boot is enabled on a Versa appliance, issue the **mokutil --sb-state** command:

```
[admin@versa-flexvnf: ~] $ mokutil --sb-state
SecureBoot enabled
```

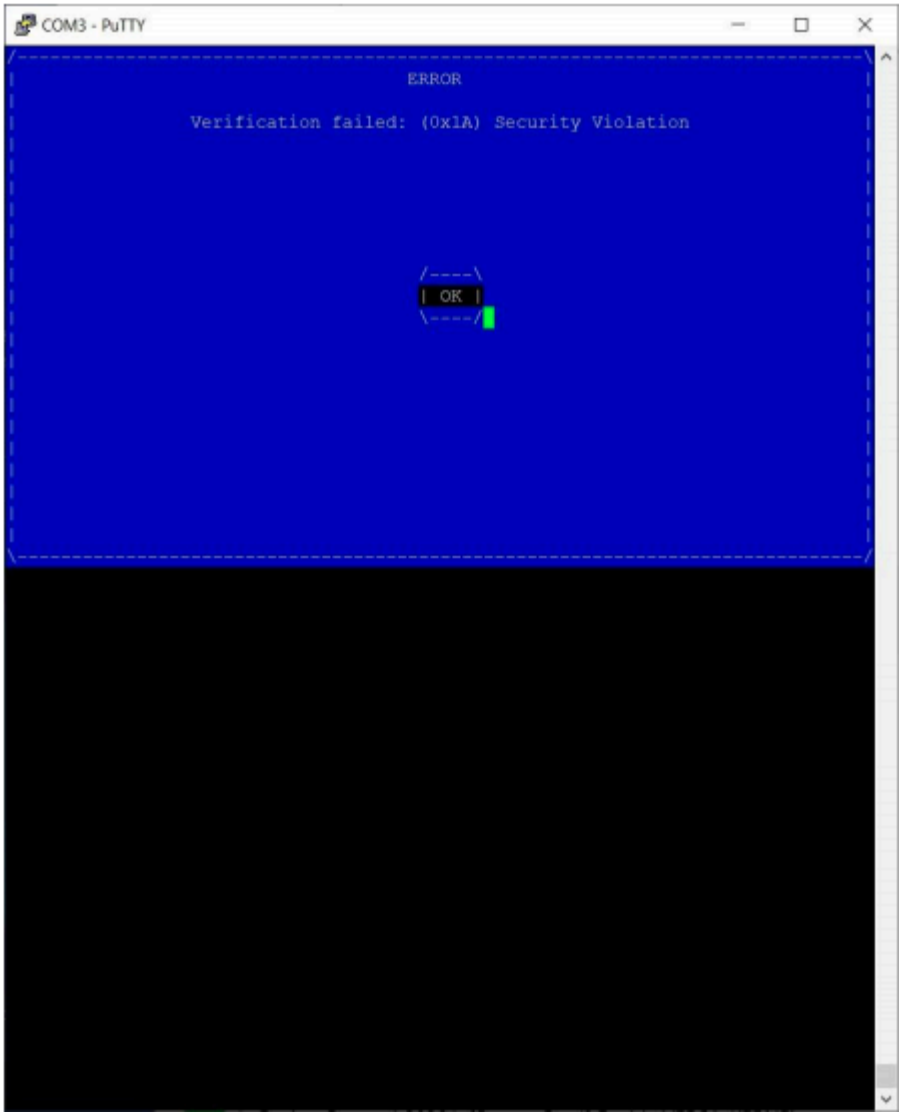
To check which GUID partition table (GPT) partition is used in UEFI mode, issue the **parted –i** command. The following example output shows that Partition 1 is used.

> [admin@versa-flexvnf: ~] $ **sudo parted -i**
> [sudo] password for admin:
> Model: ATA M.2 (S42) 3ME4 (scsi)
> Disk/dev/sda: 64.0gb
> Sector size (logical/physical): 512B/512B
> Partition Table:gpt
> Disk Flags:
> Number Start End Size File system Name Flags
> 1 1049kB 538MB 537MB fat32 EFI System Partition boot, esp
> 2 538MB 64.0GB 63.5GB ext4

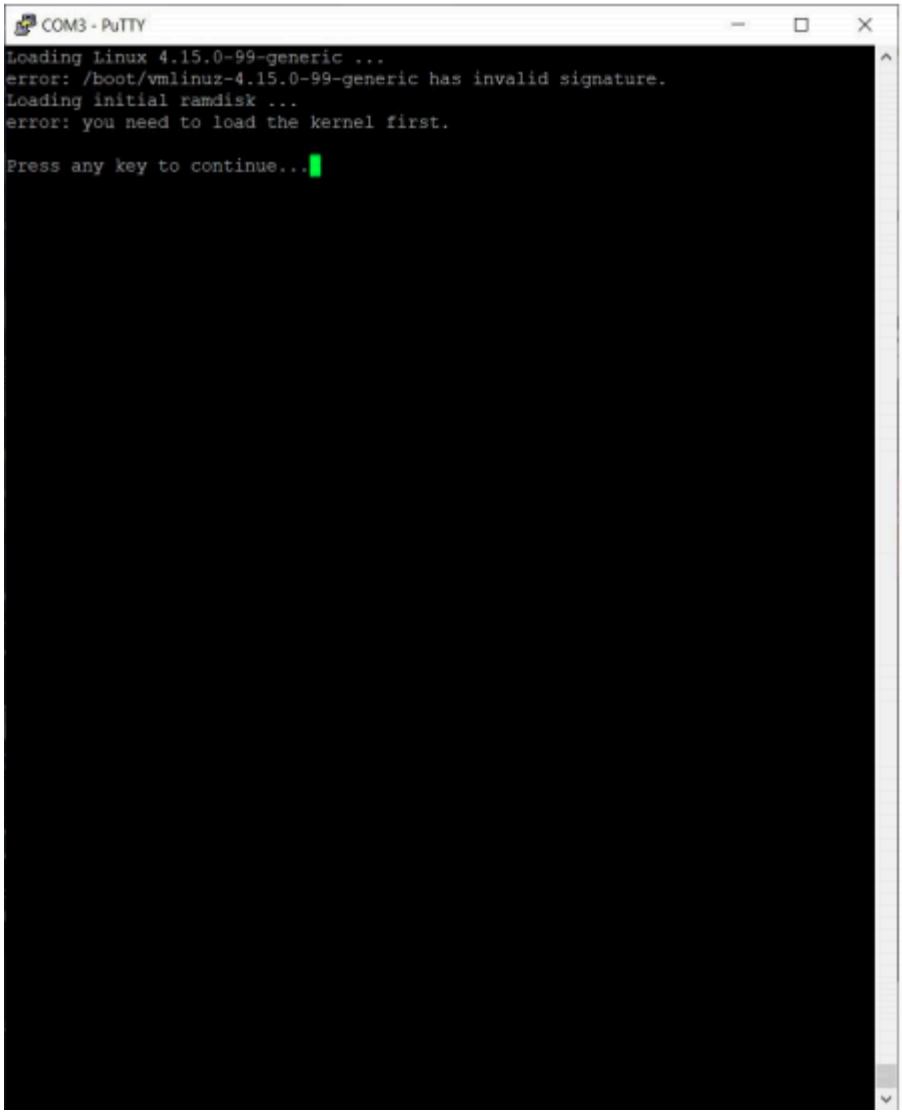
When a secure boot fails in the shim boot loader, the UEFI firmware stops the bootup process and displays a message indicating that the signature is invalid:



When a secure boot fails in the Grub boot loader, the shim boot loader displays a message indicating that verification has failed and stops the bootup process when it detects an invalid signature or no signature in the Grub boot loader file:



When a secure boot fails in the Linux kernel, the GRUB boot loader displays a message indicating that the signature is invalid and stops the boot process when it detects an invalid signature or no signature in the Linux kernel file:



When the Linux kernel module signature verification fails, the Linux kernel verifies the signature of all kernel modules and logs an error message with the specific kernel module name. For example:

Supported Software Information

Releases 21.2.1 and later, running with Ubuntu 18.04 (Bionic), support all content described in this article.