# Enabling VNF Secure Boot

Secure boot is part of the Unified Extensible Firmware Interface (**UEFI**) standard which ensures that a device boots only using a software that is trusted by the Original Equipment Manufacturer (OEM). The UEFI (Unified Extensible Firmware Interface) specification defines a secure boot methodology that prevents loading software which is not signed with an acceptable digital signature. When the device starts, the firmware checks the signature of the boot software and the operating system. If the signatures are valid, the device boots, and the firmware gives the control to the operating system.

The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the system during the system startup process. If you enable the secure boot feature, only the authorized software applications boots up from the device. This feature ensures that the software applications that boot up on the device are certified by Cisco. A secure compute system ensures that the intended software on the system runs without malware or tampered software.

To display the system boot mode and the bootloader version, run the **show platform software system boot** command.

```
Router#show platform software system boot
Boot mode: EFI
Bootloader version: 2.0
```

### Restrictions

- The following secure boot environments are supported:
  - ESXi version 6.5 or higher
  - KVM RHEL 7.5 using open stack license
  - NFVIS release 3.11 or later
- Only EFI firmware modes support the secure boot
- GRUB2 and new disk partition layout is available

**Note** Each hypervisor has a unique process to enable secure boot for the guest VMs. To enable secure boot, see the hypervisor specific documentation.

A set of high-level hypervisor specific steps to enable secure boot are mentioned below:

### ESXi Secure Boot Setup

- Create VM using ESXi 6.5 or later version using VM version 13 or greater. To choose the EFI firmware mode, navigate through **VM Options** > **Boot Options** > **Firmware** > **EFI**.
- Power down the VM after the initial boot and the IOS prompt is complete.
- Enable the EFI secure boot in **Edit Settings** > **VM Options** > **Boot Options** > **Secure Boot**.
- Power up the VM and the VNF boots up securely.

**Important** You cannot modify the firmware mode (from BIOS to EFI or vice versa) after you create the VM.

### KVM Secure Boot Setup

- Create the VM.
- Power down the VM after the VM is created and the VNF IOS prompt is complete.
- Install the PK, KEK, and db certificates from the **EFI Firmware** menu and reset.

  To create the custom keys, see Custom Keys for Secure boot. For db certificates, see MicCorUEFCA2011_2011-06-27.crt and MicWinProPCA2011_2011-10-19.crt.
- Secure boot the VM.

### NFVIS Secure Boot Setup

- Upgrade to NFVIS 3.11 release or later.
- Register an Cisco Catalyst 8000V EFI tarball with the NFVIS repository.
- Create a VM using the registered EFI image.
- Secure boot the VM.