# Configuring Secure Boot



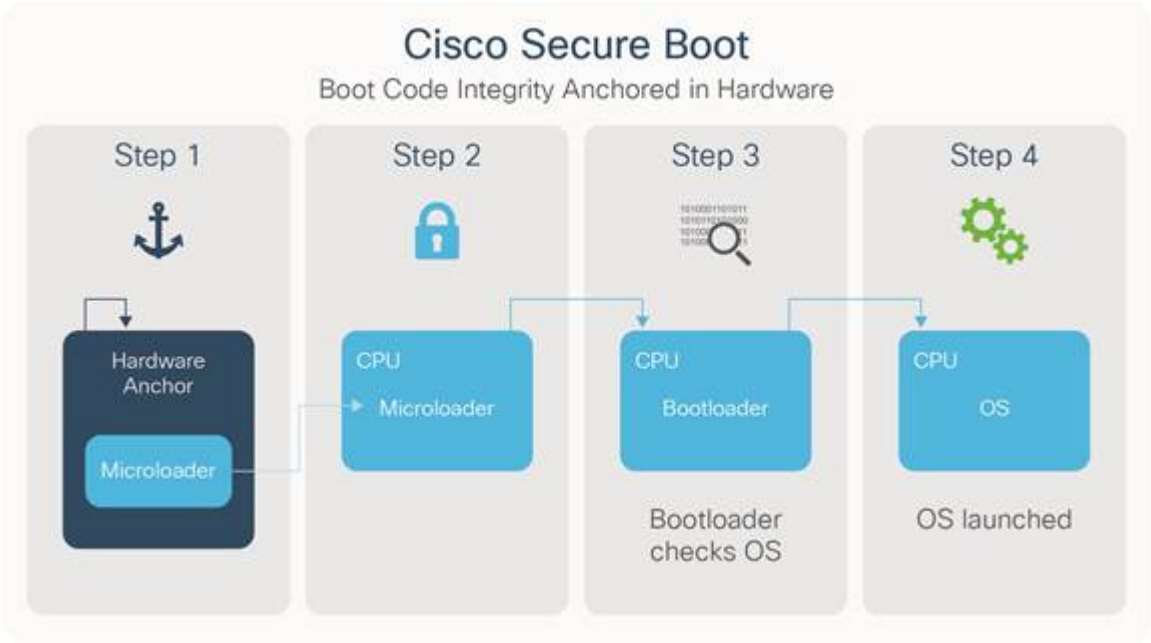
# Information About Cisco Secure Boot

Cisco Secure Boot support is introduced in the Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module, Cisco MDS 9132T Fibre Channel Switch, Cisco MDS 9396T Fibre Channel Switch, and Cisco MDS 9148T Fibre Channel Switch from Cisco MDS NX-OS Release 8.1(1) and later.

Cisco Secure Boot ensures that the first code executed on a Cisco hardware platform is authentic and unmodified. Cisco Secure Boot anchors the microloader in immutable hardware, establishing a root of trust and preventing Cisco network devices from executing tampered network software. It protects the boot code in the hardware, shows the image hashes, and provides the secure unique device identification (SUDI) certificate for the device. During the bootup process, if the authentication of the secure key fails, the line card module fails to bootup preventing the tampering of BIOS. Secure boot is enabled by default.

During a software authentication, Cisco is differentiated by anchoring the secure boot process in the hardware, thus providing the most robust security. It is robust because a hardware modification is difficult, expensive, and not easy to conceal even if hackers have physical possession of the device.

### Cisco Secure Boot Workflow




1. In the context of genuine hardware-anchored secure boot, the first instructions that run on a CPU are stored in immutable hardware.
2. When the device boots up, the microloader verifies whether the next set of instructions are from Cisco by validating the Cisco digital signature on that set of instructions.
3. The bootloader validates the operating system is from Cisco by checking whether it is digitally signed by Cisco.
4. The operating system is launched, if all the checks are passed. If any of the digital signature checks fail, the Cisco device will not let that software to boot, thus ensuring that malicious code does not run on the device.

# Information About Anti-counterfeit Measures

From Cisco MDS NX-OS Release 8.1(1), Anti-counterfeit measures are introduced on the Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module, Cisco MDS 9132T Fibre Channel Switch, Cisco MDS 9396T Fibre Channel Switch, and Cisco MDS 9148T Fibre Channel Switch.

The Anti-counterfeit measures ensure that the Cisco hardware platform with a Cisco NX-OS software image is genuine and unmodified, thereby establishing a hardware-level root of trust and an immutable device identity for the system to build on.

The Cisco MDS switch is built with ACT2-enabled ASIC. This embeds a corresponding SUDI X.509v3 certificate into the hardware. The SUDI certificate, the associated key pair, and the entire certificate chain is stored in the tamper-resistant Cisco Trust Anchor chip. The key pair is bound to a specific chip and the private key is not exported. These features make cloning or spoofing of identity information impossible.

The SUDI is permanently programmed into Trust Anchor module (TAm) and logged by Cisco during the closed, secured, and audited manufacturing processes of Cisco. This programming provides strong supply chain security, which is important for embedded systems such as routers and switches.

If an ACT2 authentication failure occurs, the following error message is displayed:

```
ACT2_AUTH_FAIL: ACT2 test has failed on module 9 with error : ACT2 authentication failure
```

For assistance with ACT2 authentication failure, contact the Cisco Technical Assistance Center (TAC).