

Secure Boot

[Main Page](#) > [FAQ](#) > [Security](#) > **Secure Boot**



Contents

- [1 How secure boot works?](#)
- [2 Why you should use secure boot?](#)
- [3 Limitations](#)
- [4 Compatibility](#)

How secure boot works?

A secure boot system adds cryptographic checks to each stage of the system boot process. Cryptographic processing verifies the authenticity of all of the protected software images that are executed by the devices. Routers with a secure boot protection mechanism allows loading firmware released only by Teltonika



Why you should use secure boot?

This additional check prevents unauthorized images from running on the router. This way, it secures the router from any unwanted "guests" loading malicious software versions.

Limitations

Devices that do have the Secure Boot will not allow uploading modified firmware images based on Teltonika software development kit(SDK)

Compatibility

At this moment secure boot is compatible only with certain RUT950 and RUT955 versions (without any additional configuration):

* **RUT950U072C0**

* **RUT955T073B0**