

# Modify System Image, Technique T1601 - Enterprise

Archived: 2026-04-05 16:08:23 UTC

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves. On such devices, the operating systems are typically monolithic and most of the device functionality and capabilities are contained within a single file.

To change the operating system, the adversary typically only needs to affect this one file, replacing or modifying it. This can either be done live in memory during system runtime for immediate effect, or in storage to implement the change on the next boot of the network device.

---

Source: <https://attack.mitre.org/techniques/T1601>