

知 HPE Gen10 服务器TPM Mode Switch Operation选项重启后是No action, 不是TPM2.0

BIOS 吕飞 2023-04-26 发表

问题描述

服务器BIOS中Server Security选项中的TPM Mode Switch Operation选项需要锁定2.0而不是No action, 当前每次重启后都是变成no action

过程分析

TPM Mode Switch Operation的选项功能是切换TPM模式的选项，此选项可切换TPM1.2或者TPM2.0。切换后Current TPM Type会改变为TPM2.0或1.2。

解决方法

TPM Mode Switch Operation此选项重启后为No action为正常现象，此选项可切换TPM模式。
切换后Current TPM Type会为：TPM2.0或者TPM1.2。



