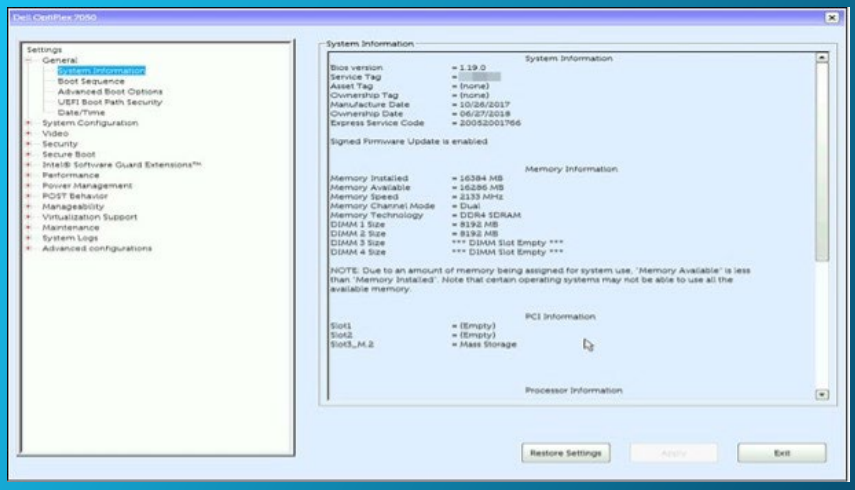
SOLUTION BRIEF

FirmGuard® SecureConfig

REMOTE BIOS CONFIGURATION

Introduction

Changing or conguring the BIOS settings of an endpoint is something most IT administrators can do if they are in front of the endpoint. It usually requires pressing some function key before Windows boots up and then navigating a menu such as in the graphic shown below. But what if you don't have direct, physical access to the endpoint and you need to make a change? Well, in that case, you might have to get on the phone and talk your client (who is often not very technical) through the process and that can be downright painful. There must be a better way!



DELL BIOS configuration screen

With FirmGuard SecureConfig, an administrator can remotely configure any BIOS parameter on any Windows endpoint just as if they were sitting in front of the computer. Because FirmGuard operates at the firmware level, it exposes every available BIOS parameter to the administrator.

If the manufacturer (e.g., Dell, HP, Lenovo) allows configuration of a given parameter, then FirmGuard will as well. Simply put, SecureConfig greatly streamlines and consolidates administration of BIOS settings across an entire organization.

phoenix technologies

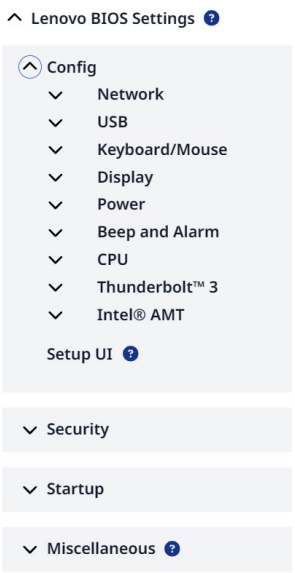
SecureConfig

How does it work?

With SecureConfig an administrator can easily configure any BIOS parameter that is available on the endpoint from the FirmGuard portal. The configuration screen will vary depending upon the make and model of the endpoint, but as an example, (on the right) here is a graphic showing some of the available parameters in a Lenovo laptop.

Here are some representative examples of configuration settings, changes or adjustments that might be needed from time to time:

- Enable/disable I/O firmware settings such as USB, Bluetooth or camera
- Set/update boot order sequence
- Enable Wake-on-LAN, change power plan (to save battery) etc.



FirmGuard SecureConfig BIOS configuration screen for Lenovo endpoint

HTS Case Study Summary

Healthy Technology Solutions (HTS), a FirmGuard customer since 2022, had a local client that had recently established an overseas office that was nearly 7,600 miles and 13 time zones away from their offices in Las Vegas. The local client had purchased two new laptops and an HTS technician followed the New Computer Setup form to configure the laptops. During setup, he was unable to enable BitLocker because the TPM (Trusted Platform Module) hardware was showing as "unavailable." The fix was obvious, enable TPM in UEFI BIOS firmware settings, however that would require coordination with the local client and with the 13 time zone difference that was going to be complicated.

> **"In a matter of 15 minutes what we thought was going to be a headache turned out to be something simple, thanks to FirmGuard SecureConfig!!"**
>
> *- Ben Gilbertson*
> *Executive Vice President of Healthy Technology Solutions*

Fortunately, HTS had access to SecureConfig which made the process almost trivial. An HTS technician logged into the FirmGuard portal from Las Vegas, pushed the FirmGuard agent to both laptops and then browsed the available BIOS settings via SecureConfig. He quickly drilled down and under "Security" found a setting to "Enable" the TPM security chip. After pressing the save button, the endpoint rebooted, and upon restart the drive started encrypting with BitLocker, as expected. What they thought was going to be a time-consuming headache turned out to only take 15 minutes to resolve, thanks to SecureConfig!

READ THE CASE STUDY

SEE THE TESTIMONIAL

phoenix technologies

SecureConfig helps maintain ISO and NIST compliance

SecureConfig helps FirmGuard customers, and their clients comply with a variety of industry standards. The list below provides a detailed breakdown of compliance with specific standards including individual clauses within the standard.

ISO 27001 Clause 12.1.1 (Documented Operating Procedures)	**SecureConfig** enables consistent enforcement of BIOS settings across all systems, aligning with operational security requirements.
ISO 27001 Clause 12.5.1 (Installation of Software on Operational Systems)	**SecureConfig's** remote management capabilities ensures BIOS Configuration compliance during software installation processes.
ISO 27001 Clause 12.6.1 (Management of Technical Vulnerabilities)	**SecureConfig** can be used to standardize and maintain BIOS settings are consistent across the entire software environment.
ISO 27001 Clause 16.1.4 (Assessment of and Decision on Information Security Events)	**SecureConfig** allows for quick adjustments to BIOS settings in response to security events, aiding in timely resolution of incidents.
ISO 27001 Clause 18.1.1 (Identication of Applicable Legislation and Contractual Requirements)	**SecureConfig** helps ensure compliance with laws and regulations that require standardized security Configurations across an organization's systems.
NIST SP 800-53 AC-19 (Access Control for Portable and Mobile Devices)	**SecureConfig** ensures that mobile and portable device BIOS settings are secured and standardized.
NIST SP 800-53 CM-2 (Baseline Configuration)	**SecureConfig** maintains baseline Configurations and ensure uniform application across devices, supporting compliance with NIST guidelines.
NIST SP 800-53 CM-6 (Configuration Settings)	Enforce least functionality by managing BIOS Configurations to comply with the strictest security settings recommended by NIST.
NIST Cybersecurity Framework ID.AM-3 (Resource Management)	**SecureConfig** can be utilized to ensure BIOS Configurations adhere to the organization's security policies, facilitating effective resource management.
NIST Cybersecurity Framework PR.PT-1 (Security Protections)	**SecureConfig** ensures security protections are uniformly applied at the BIOS level, enhancing overall cybersecurity measures.

Learn how FirmGuard can help you remotely secure, configure and update UEFI BIOS firmware. Book your 15 minute demo today.

firmguard.com/demo

phoenix technologies

rev. 02.10.25