SA UEFI Secure-Boot Server Provisioning

The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between personal-computer operating system and platform firmware. UEFI replaces the Basic Input/ Output System (BIOS) firmware interface present in all IBM PC-compatible personal computers.

The interface consists of data tables that contain platform-related information, plus boot and runtime service calls that are available to the operating system and its loader. Together, these provide a standard environment for booting an operating system and running pre-boot applications. In practice, most UEFI images provide legacy support for BIOS services. UEFI can support remote diagnostics and repair of computers, even without another operating system.

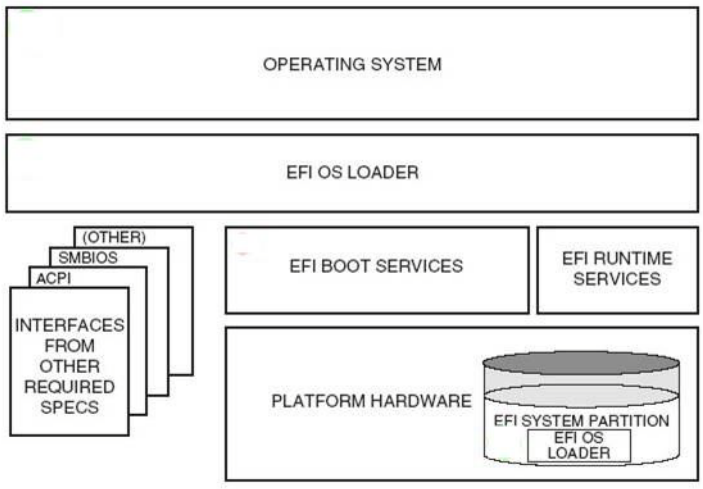
For more information, see *http://www.uefi.org/*.

UEFI Overview

UEFI encourages code reuse, modularization, flexibility and modernization. UEFI specifications contain interfaces that streamline and aid in firmware innovation by promoting interoperability between devices, software and systems. UEFI supports diagnostics and repair, even without an installed operating system. UEFI also supports more secure systems, faster boot times, extensibility and modularity.

Figure 1 shows the UEFI architecture.

figure 1 UEFI Architecture



UEFI Secure Boot

UEFI Secure Boot improves security in the pre-boot environment and provides firmware, operating system and hardware a defense against potential malware attacks. UEFI Secure Boot uses signed components that are started by the system firmware and requires signed fw-drivers for the components (for example NIC,HD or RAID-like SmartArray, etc.) as well as signed boot loaders, OS kernels and OS drivers.

Supported UEFI capable Hardware

SA supports UEFI and UEFI Secure Boot on the Gen8 HP ProLiant DL580 including legacy BIOS and UEFI boot modes.

- LEGACY: the server behaves like a standard BIOS based machine (secure boot not available)
  - Boot Mode: “Legacy”
- UEFI: Secure Boot can be enabled/disabled
  - Boot Mode: UEFI_OPTIMIZED

    The default mode of operation
  - Boot Mode: UEFI_OPTIMIZED_SECURE

    Secure Boot enabled UEFI boot mode
  - Boot Mode: UEFI

    UEFI - “optimized mode” disabled - fallback mode for older Windows OSes (for example, Windows Server 2008) which require special interrupt handling.

Supported Operating Systems

Secure Boot is supported in P79 1.00 ROM and later. HP highly recommends that you use the latest firmware update. See the HP ProLiant Support Page:

http://h20565.www2.hp.com/portal/site/hpsc/public/psi/home/

- Windows Server 2012 r2 x64
- Supported boot loader: pxelinux
- Supported SOS: WinPE 2.1 (32bit) / 3.1 (64bit), Gaius Linux, Gaius WinPE

Provisioning an HP ProLiant DL580 and Enabling Secure Boot

1. Install Windows Server 2012 R2x64 using a standard SA OS Provisioning build plan (*ProLiant OS - Windows 2012 R2 Standard x64 Scripted Install*) on a server that has UEFI Secure Boot disabled. See also the *User Guide: Provisioning* for more information about running Build Plans.
2. Enable Secure Boot from the server’s **System Utilities Menu** (see Enabling/Disabling UEFI Secure Boot).
3. Reboot the server into Secure Boot mode.

Enabling/Disabling UEFI Secure Boot

Enabling/disabling UEFI Secure Boot requires manual changes using the device's ROM firmware or using iLO.

To enable/disable UEFI Secure Boot, perform the following tasks:

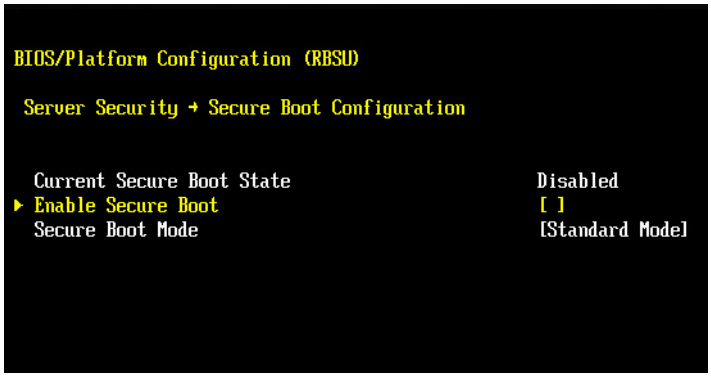
1 Boot the server and access the **System Utilities Menu** by pressing **F9.**

2 Select **System Configuration** from the Options menu.

3 Select **BIOS/Platform Configuration (RBSU)** from the Options menu.

4 Select **Server Security** from the Options menu.

5 Select **Secure Boot Configuration** from the Options menu



6 Press Enter to enable or disable (toggle) UEFI Secure Boot.

Provisioning a Non-ProLiant UEFI Capable Server and Enabling Secure Boot

See the *User Guide: Provisioning* for information about provisioning a non-ProLiant UEFI capable server and running Build Plans.

See your hardware vendor's documentation for information about enabling secure boot after deployment in non-secure mode.