Technical white paper

Device Guard Support on HP Desktop Workstations

Table of contents

Executive summary

This white paper describes current and planned support for Microsoft Windows 10 Enterprise Device Guard on HP Desktop Workstations.

Overview of Device Guard Support on HP Desktop Workstations

Microsoft has introduced a new security feature for Windows 10 Enterprise called Device Guard. Device Guard uses a combination of hardware and software to lock down devices, so that they can only run trusted (whitelisted) applications. Device Guard makes it much more difficult to run malicious executable code, even in the presence of issues allowing kernel-level access. Device Guard will evolve over time as more hardware and software components are hardened.

Device Guard support on HP Desktop Workstations is evolving to keep up with these changing requirements. HP Z2 Mini/ Z240/Z440/Z640/Z840 Desktop Workstations currently meet Windows 10 Redstone-1 (1607) level of Device Guard support in limited configurations. Credential Guard is a related feature (not part of Device Guard) that aims to isolate and harden key system and user secrets against compromise. This white paper also provides limited information regarding Credential Guard support on HP Desktop Workstations.

Microsoft Windows 10 Enterprise and Device Guard are only available for installation through HP Custom Integration Services to enterprise customers with a volume license to use Microsoft Windows 10 Enterprise. Device Guard is not available with Microsoft Windows 10 Pro or other operating systems.

Support Matrix

Table 1. Device Guard and Credential Guard Support/Availability Matrix

	October 2016	February/March 2017	May 2017
Device Guard Compliance	Redstone-1 (1607)		
System BIOS	Single-signed support HP Z240 v1.29 HP Z440/Z640/Z840 v2.26	Dual-signed support HP Z240/Z2 Mini v1.50 (March) HP Z440/Z640/Z840 v2.31 (Feb)	HP Z240/Z2 Mini vTBD HP Z440/Z640/Z840 vTBD
DG-signed Video BIOS (Not required for systems with Integrated Graphics)	NVIDIA® K620, M5000, M6000 (24G) AMD W2100 **(HP-Single-signed,** by request**)**	NVIDIA® K620, M4000, M5000, M6000 (12G), M6000 (24G), AMD W2100 **(HP-Dual-signed, Softpaq only** by request**)**	
DG-compliant Graphics Driver (Hypervisor based Code Integrity /H.V.C.I.)	AMD 16.40.2501 (or newer) NVIDIA® 369.09 (or newer)		
Hardware Security Test Interface (HSTI)			Limited support on HP Z240/Z2 Mini Not supported on HP Z440/Z640/ Z840 (Intel® does not support HSTI on Xeon® E5 Processors)
Windows SMM Security Mitigations Table (WSMT)			Supported
No-Execute (NX) Protection			Work in progress, no commit date

Support Matrix

Table 1. Device Guard and Credential Guard Support/Availability Matrix (Continued)

	October 2016	February/March 2017	May 2017
	Additional requirement needed for Credential Guard		
Trusted Platform Module (TPM 2.0)	Available as Factory Option		
Secure MOR	Secure MOR 1		Secure MOR 2

Disabling the Microsoft UEFI CA Key

The Microsoft UEFI CA key is used to sign third-party UEFI code for Secure Boot compliance, including non-Microsoft OS loaders and UEFI device drivers. Disabling the Microsoft UEFI CA key is a requirement for full Redstone-1 Device Guard support. However, disabling this key will cause the system to **abort booting** if the graphics card is not compatible with Device Guard (in the same way that a system would abort booting if Secure Boot was enabled and a non-Secure Boot-capable graphics card was used). Specifically, to fully support Redstone-1 Device Guard in HP Desktop Workstations, the graphics card UEFI device driver (part of the video BIOS) must be signed by the HP CA key. If the Microsoft UEFI CA Key is disabled and the graphics card video BIOS is not signed by the HP CA key, the system will be unable to boot and will halt with a 6 beep/blink pattern (3.3 pattern on Z240). Recovering from this situation requires pushing the "Clear CMOS" button (or jumper) on the motherboard. BIOS versions released in February and March 2017 include safeguards to avoid entering a non-bootable state.

Future support

HP Workstations Device Guard support will continue to improve with increased features and additional supported configurations. Additional Device Guard video BIOS will be dual-signed with the Microsoft UEFI CA key and the HP CA key. These will work in Secure Boot or Device Guard modes on the listed platforms. These are available for specific cards by engineering request. Eventually, video BIOS for graphics cards and Option ROMs for selected non-graphics cards will be widely available in Production and After Market Option kits. In the future, HP Workstations will continue to add support as possible for future Microsoft requirements including Redstone-2 compliance.

Enabling Device Guard

Enabling Device Guard support requires multiple changes to BIOS and Operating System settings. Following are the high level steps required to enable Device Guard.

1. Update Operating System, System BIOS, Video BIOS and Graphics Driver to the desired levels based on the Support Matrix above. Note that Device Guard is only supported on Windows 10 Enterprise.

2. Previous Device Guard BIOS - Provision BIOS settings to support Device Guard:

The following are for earlier BIOS (released prior to February 2017)

	HP Z440/Z640/Z840 v2.26+	HP Z240 v1.29+/Z2 Mini v1.04+
Disable TXT	Security > System Security > Intel TXT (LT) Support set to **Disable**	Security > Trusted Execution Technology (TXT) **(unchecked)**
Enable VT-x	Security > System Security > Virtualization Technology (VT-x) set to **Enable**	Advanced > Virtualization Technology (VTx) **(checked)**
Enable VT-d	Security > System Security >Intel VT for Directed I/O (VT-d) set to **Enable**	Advanced > Virtualization Technology for Directed I/O (VTd) **(checked)**
Enable Secure Boot	Advanced > Secure Boot Configuration > Configure Legacy Support and Secure Boot set to **Disable Legacy Support and Enable Secure Boot**	Advanced> Secure Boot Configuration > Configure Legacy Support and Secure Boot set to **Legacy Support Disable and Secure Boot Enable**
Disabling MS UEFI CA KEY	**Redstone -1 and Later Only** Advanced > Secure Boot Configuration > MS UEFI CA key set to **Disable**	**Redstone -1 and Later Only** Advanced > Secure Boot Configuration > Enable MS UEFI CA key **(uncheck)**

Note 1: If full Redstone-1 Device Guard compliance is desired (see Support Matrix for Redstone-1 requirements) and a Device Guard compatible graphics card is installed, disable the Microsoft UEFI CA key. **Caution:** disabling this key will cause the system to abort booting if the graphics card is not compatible with Device Guard.*

3. Future Device Guard BIOS - Provision BIOS settings to support Device Guard.

The following are for current BIOS (released February 2017 or later)

	HP Z440/Z640/Z840 v2.31+	HP Z240/Z2 Mini v1.50
Disable: TXT Enable: VT-x, VT-d	Advanced > Secure Boot Configuration > Ready BIOS for Device Guard Use set to **"On Next Boot"**	Same as Previous BIOS
Enable Secure Boot	Same as Previous BIOS	Same as Previous BIOS
Disabling MS UEFI CA KEY	**Redstone -1 and Later Only** Advanced > Secure Boot Configuration > MS UEFI CA key set to **Disable** Note: The menu will only be available if all graphic cards are compatible with Device Guard	

These settings can be modified programmatically using the integrated "Replicated Setup" menu in Computer Setup (F10), using the HP BIOS Configuration Utility (BCU), or using WMI-capable scripting tools such as PowerShell or Windows Script Host.

4. Provision the Operating System to support Device Guard:

– Microsoft TechNet provides a Device Guard deployment guide at https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide

Additional Information

Additional details on Device Guard features and enablement are available directly from Microsoft.

Note that Device Guard support on HP Desktop Workstations is continually evolving. This document will be updated to reflect these changes. Please contact your HP Sales Representative or HP Workstation Support with any questions regarding Device Guard.

Disclaimer

The information contained within this white paper, including URL, other web site references, and other specification documents are subject to change without notice and are provided for informational purposes only. No licenses with respect to any intellectual property are being granted, expressly or impliedly, by the disclosure of the information contained in this document. Furthermore, neither HP Inc. nor any of its subsidiaries makes any warranties of any nature regarding the use of the information contained within this document, and thus the entire risk, if any, resulting from the use of information within this document is the sole responsibility of the user. In addition, the names of the technologies, actual companies, and products mentioned within this document may be trademarks of their respective owners. Complying with all applicable copyright and trademark laws is the sole responsibility of the user of this document. Without limiting any rights under copyright, no part of this document may be reproduced, stored, or transmitted in any form or by any means without the express written consent of HP Inc. HP Inc. or its subsidiaries may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this document. Except where expressly provided in any written license from HP Inc. or its subsidiaries, the furnishing of this document, or any ideas contained within, does not grant any license to these ideas, patents, trademarks, copyrights, or other intellectual property.

4AA6-9621ENW, March 2017