TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

THUNDERBOLT™ DMA ATTACK MITIGATIONS

OBJECTIVE

The objective of this paper is to discuss the risks associated with USB Type-C™ Thunderbolt™ capable ports and to summarize the mitigations that are available to manage the associated risks. The majority of this paper assumes Windows 10 as the operating system.

ABOUT THUNDERBOLT™

Thunderbolt™ provides the highest bandwidth possible via a USB Type-C™ connection and enables use cases not otherwise possible via a single USB Type-C™ connection. Thunderbolt™ connections are capable of direct memory access (DMA) via a Peripheral Component Interconnect Express (PCIe) connection, and Thunderbolt™ ports are the only externally accessible ports on modern PCs that offer this capability.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

DMA RISKS

DMA capability via an externally accessible port increases the available attack surface versus non-DMA capable ports. DMA capability enables a peripheral device to read and write the main memory of the OS directly without any dependency on the main CPU processor. DMA also bypasses access restrictions enforced by the Memory Management Unit (MMU) that the OS configures to restrict de-privileged software SW running on the CPU from accessing privileged OS memory.

However, while Thunderbolt™ DMA capability does present some unique risks, it is important to understand that even for non-DMA capable ports, there are inherent risks associated with connecting any untrusted external peripheral to the PC, including standard USB devices.

GENERAL RISK MITIGATION STRATEGIES

Regardless of the type of peripheral, it is recommended that users connect only trusted peripherals procured from trusted sources to their PC. If this is not always possible, there are several strategies that can be used to provide increased levels of protection against malicious peripheral devices.

A good practice is to be logged into a non-administrative account if connecting untrusted peripherals, or if the PC is being used in an environment where there are no physical access controls in place to prevent a bad actor from plugging in an external peripheral device. As an example, consider a malicious device that mimics a USB keyboard when plugged in and can inject keystrokes just as if they were typed by the local user. Using a non-administrative account limits the ability of an attacker to install malicious software or modify other security critical settings in such a scenario, although it does not eliminate the ability of an attacker to exfiltrate data surreptitiously to the peripheral device.

It is also recommended to enable Bitlocker full drive encryption in Windows 10 (which is not enabled by default). This will help with mitigating attacks that are attempting to boot the PC to an alternative environment contained on a USB flash drive that could then mount the internal drive to potentially copy personal or confidential information off the internal drive or even modify the state of the drive to enable the attacker to bypass the user login screen on the next boot. The optional BITLOCKER group policy option (GPO) policy that requires the user to enter a unique PIN on each boot before the TPM will release the bitlocker drive encryption key is also recommended to block from some advanced attacks against bitlocker that are possible with physical access.

Limit boot devices to only the internal boot drive. In the BIOS menu, there is an option to disable types of boot devices, such as USB and network boot options. By restricting USB boot devices, you will deter attackers from authorizing malicious PCI devices on the host system through an image in an external drive as well as a variety of other attacks that may be possible if the system is booted to an OS that is on an attacker's external storage device.

Ensure Secure Boot is enabled. Enabling the Secure Boot feature of the BIOS will ensure BIOS performs a digital signature check of the OS boot loader, Secure Boot does not check key operating system files, and option UEFI device drivers ROMs by validating their digital signatures. The mechanism is intended to prevent passing execution control to malicious code such as a rootkit during the OS boot process.

Configuring a BIOS administrator password to prevent unauthorized changes to BIOS settings is also crucial. An attacker that is able to change BIOS setting can disable BIOS-based capabilities that are critical to maintaining the security posture of the platform.

Also note that most desktops have a "Clear Passwords" jumper on the system board and that the default behavior of the BIOS is that it will clear the BIOS administrator password on the next boot after the jumper is installed. Unless the desktop in question has some physical access controls in place to prevent access to the system board such as the HP hood lock, it is recommended to also enable the "Stringent Mode" setting when the BIOS admin password is set, as this setting will cause BIOS to ignore the state of the "Clear Passwords" jumper.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

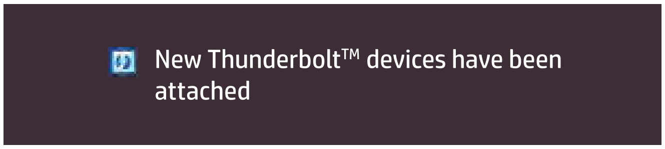
THUNDERBOLT™ DMA RISK MITIGATION BIOS POLICIES

BIOS shipping defaults

HP Thunderbolt commercial PCs released in 2018 or before are configured by default to block DMA access until an authenticated Windows user approves the connection of a Thunderbolt™ device via the Thunderbolt™ dialog box that pops up within the OS when a new Thunderbolt™ device is inserted.

1. When connecting a new HP Thunderbolt Dock G2 to your notebook for the first time you may need to authorize the Thunderbolt™ Device. When the dialog that appears, click on the pop up. A dialog will appear each time a new Thunderbolt™ dock/device is attached. See Figure A.

NOTE: You must be logged on as an administrator of the local computer. In some Thunderbolt™ security level settings the dialog may not appear (see Thunderbolt™ Security level section).

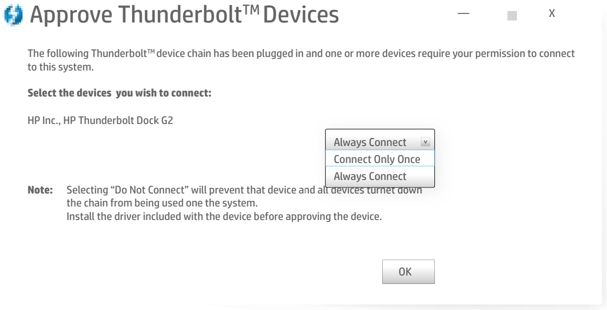


New Thunderbolt™ devices have been attached

Figure A. Dialog box requesting administrative approval of a new Thunderbolt™ device.

2. A second dialog opens. See Figure B. Select one of the following options:

- *Do Not Connect*—prevents the dock from connecting to the notebook.
- *Connect Only Once*—allows the dock to connect to the notebook until it is disconnected. Each time the dock is disconnected and reconnected, you must be logged on as an administrator to allow access to the dock.
- *Always Connect*—allows the dock to connect to the notebook. The dock can connect to the computer automatically after it is disconnected and reconnected, even if you are not logged on as an administrator



Approve Thunderbolt™ Devices

The following Thunderbolt™ device chain has been plugged in and one or more devices require your permission to connect to this system.

Select the devices you wish to connect:

HP Inc., HP Thunderbolt Dock G2

Always Connect

Note: Selecting "Do Not Connect" will prevent that device and all devices turnet down the chain from being used one the system.
Install the driver included with the device before approving the device.

Figure B. Dialog box to configure connection settings of a new Thunderbolt™ device.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

More recent platforms, beginning with HP EliteBook 800 G6, include BIOS and OS support for selectively blocking DMA access using the I/O Memory Management Unit (IOMMU) hardware. This approach is commonly referred to as DMA remapping (DMAr) support. In the BIOS menu, the option is referred to as DMA Protection.

The table below shows the shipping default settings for various generations of commercial notebook products.

Default Thunderbolt™ Security settings in BIOS	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2016**	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2017**	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018***	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2019***
User Authorization Required (SL1)	Supported (Default = Enabled)	Supported (Default = Enabled)	Supported (Default = Enabled)	Supported (Default = Disabled)
DMA Protection	Not Supported	Not Supported	Not Supported	Supported (Default = Enabled)

* HP EliteBook x360 830 G5 has the same Thunderbolt™ security features as HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018.

These settings are controlled by BIOS settings and can therefore be disabled in F10 BIOS setup. As mentioned previously, it is critical to block access to F10 BIOS by configuring a BIOS Administrator password to keep an attacker with physical presence from disabling these security policies.

HP EliteBook and ZBook default configurations align with the rest of the industry to provide the best balance of security versus compatibility for the typical user. HP highly recommends that the end user/adminstrator review these settings versus their threat models and risk profile to determine if more aggressive security policy settings are appropriate.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

SUMMARY OF BIOS THUNDERBOLT™ SECURITY SETTINGS

Thunderbolt™ Security Setting	Description	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2016	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2017	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018*	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2019*
No Security (SL0)	In this mode, the Thunderbolt™ host controller will connect the PCIe fabric to the external Thunderbolt™ devices as soon as they are connected which can result in that external device performing DMA if there is no other mechanism configured to prevent it.	Y	Y	Y	Y
Authorization required (SL1)	This mode requires an authenticated user to first approve a Thunderbolt™ connection in the Windows environment via the Thunderbolt™ software before the external device is connected to the internal PCIe fabric. If the user chooses to "always connect" for that device, on each subsequent insertion, the device will auto-connect PCIe in OS environment. The device will also auto-connect in the Pre-OS boot environment on HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018 or later.	Y	Y	Y	Y
Secure Connect (SL2)	This option is very similar to SL1, but with an enhancement that is applicable to the "always connect" scenario only. In the SL1 auto-connect case, Secure Connection provides a mitigation against an attack, which involves cloning the unique device ID of attack by dynamically generating a unique secret key on the initial connection that is stored by the peripheral and the host. On subsequent connections the device that claims to be a previously connected unique ID, the host will perform a challenge/response protocol with the peripheral, and it must prove it is in possession of the secret key before the host will allow the DMA connection. If Pre-boot support is not required and DMA Protection setting is not available or is disabled, it is recommended using SL2 for enhanced assurance of the auto-connect option and future proofing against advancing attacker capabilities in the future. **Note:** User Authorization / Secure Connect (SL2) BIOS options is unavailable with the DMA Protection setting enabled. Intel® Thunderbolt™ SW does not support this combination. Also, note that in SL2 mode, the Intel® Thunderbolt™ controller will not auto-connect devices in the Pre-boot environment that the user has specified as "always connect."	Y	Y	Y	Y

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

SUMMARY OF BIOS THUNDERBOLT™ SECURITY SETTINGS (CONTINUED)

Thunderbolt™ Security Setting	Description	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2016	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2017	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018*	HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2019*
DisplayPort™ and USB (SL3)	When this option is selected, the port will provide USB functionality, power delivery, and DisplayPort™. When a Thunderbolt™ device is attached, a Thunderbolt™ link will be established, but PCIe will NOT be tunneled through that link, which can result it either no functionality or limited functionality for an attached Thunderbolt™ device. Recommend using this mode only when there is no requirement to support Thunderbolt™ peripherals, or Thunderbolt™ peripherals that only require the DisplayPort™ interface to be fully functional.	Y	Y	Y	Y
Daisy Chaining Disabled (SL4)	This mode uses an Intel® proprietary approach to terminate the PCIe interface within the first Thunderbolt™ peripheral bridge chip connected to a Thunderbolt™ host port. This may be a mechanism to provide protection against DMA attacks involving daisy chaining a malicious PCIe device to a Thunderbolt™ peripheral chip in an external device.	N	N	N	Y

* HP EliteBook x360 830 G5 has the same Thunderbolt™ security features as HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018.

Because the Thunderbolt™ Security setting SL1 and SL2, described in the table above, require an authenticated user to approve connection of a Thunderbolt™ device before it is able to perform DMA, they help prevent an attacker with physical access to the system from compromising it when the authorized user is not logged in, but some risks remain if we consider a scenario where the malicious DMA device is inadvertently, unknowingly, or unwittingly authorized to connect by the user.

Note that although the BIOS default options do not enable Thunderbolt™ user authorization when DMA Protection is enabled, it is possible to require User Authorization (SL1) in conjunction with DMA Protection for an additional layer of security.

DMA Protection

When DMA Protection is enabled in BIOS, versions of Windows 10 that support Kernel DMA protection to Thunderbolt™ will enable that capability within the OS.

Additionally, when this setting is enabled, the BIOS (UEFI) pre-boot environment blocks DMA from ALL DMA-capable devices (not just Thunderbolt™) to critical memory used by that environment.

This BIOS setting is recommended to be enabled on all platforms that support it. Refer to the table above to determine which platforms it is supported on.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3–6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

Disabling Thunderbolt™ Capability

For those organizations in which any DMA from an external port is above their risk-tolerance threshold, there are additional options available, assuming that Thunderbolt™ capability is not required in those environments.

On HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018 or later have a BIOS (F10) setup option that allows for disablement of the Thunderbolt™ capability of all Type-C connections on the system that support Thunderbolt™. With this policy configured, Charging, Power, USB, and DisplayPort™ capability of the Type-C ports are still available via those ports even though the Thunderbolt™ capability is disabled. Also, note that, since the HP Thunderbolt Dock G2 is designed as a universal dock, the majority of its functionality is available when connected via a Thunderbolt™-disabled port.

For HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2017 or earlier, the BIOS Thunderbolt™ Security = DisplayPort™ and USB (SL3) can be used for a similar result. The major differences are that Thunderbolt™ devices that require the DisplayPort™ interface only will function as expected and the HP Thunderbolt Dock G2 will NOT connect in universal mode and will have very limited functionality.

WINDOWS 10 POLICIES

Disable new DMA devices when this computer is locked

Windows 10 (1703 or higher) includes a Group Policy Option (GPO) that can be used that, when enabled **and bitlocker is enabled**, will block DMA access from any new Thunderbolt™ peripheral that is attached while the screen is locked. DMA from this new device will only be enabled once an authorized user has successfully logged in to that machine. This GPO is not enabled by default but can be enabled and will co-exist with the user approval prompting by the Thunderbolt™ software described above.
Link to GPO: **https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings#disable-new-dma-devices-when-this-computer-is-locked**

NOTE: It is not recommended to use this GPO in lieu of the Thunderbolt™ prompting control in F10 BIOS setup since disabling Thunderbolt™ security in F10 BIOS setup will allow DMA-capable devices access to memory in the Pre-OS environment with no user authorization required.

Blocking Thunderbolt™ controllers to reduce Thunderbolt™ DMA threats to BitLocker

This optional group policy to block DMA capable devices attached to the Thunderbolt™ port from being enabled has drawbacks and could lead to undesirable results.
Link to GPO: **https://support.microsoft.com/en-us/help/2516445/blocking-the-sbp-2-driver-and-thunderbolt-controllers-to-reduce-1394-d**.

This approach is not recommended. The recommended alternative approach is to either disable Thunderbolt™ capabilities in BIOS on platforms that support this setting, or alternatively change the BIOS Thunderbolt™ security level to DisplayPort™ and USB (SL3) on those systems that do not support disablement of the Thunderbolt™ capability in BIOS settings.

Microsoft Windows Kernel DMA protection for Thunderbolt™

This link has more details on the Microsoft implementation of this feature:
https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt

Be aware that, in order to provide the best compatibility in Windows 10 1803, this feature does not enforce any restrictions on DMA devices for which the applicable drivers do not support DMAr. In RS5 and greater, there is a new OS policy for the feature that can be used to modify this behavior and increase the security posture of the platform at the expense of breaking compatibility with any devices which do not have drivers that support DMAr.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3–6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIe based Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

Enumeration policy for external devices incompatible with Kernel DMA Protection

It is recommended that the following policy be changed to “Block all” (Most restrictive): Devices with DMA remapping compatible drivers will be allowed to enumerate at any time. Devices with DMA remapping incompatible drivers will never be allowed to start and perform DMA at any time.

The policy can be enabled by using either:

Group Policy: Administrative Templates\System\Kernel DMA Protection\Enumeration policy for external devices incompatible with Kernel DMA Protection.

Mobile Device Management (MDM): DmaGuard policies (**https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-dmaguard#dmaguard-policies**)

USING PCIE BASED THUNDERBOLT™ DEVICES IN BIOS PRE-OS ENVIRONMENT

Some users will have Pre-OS use cases for externally attached Thunderbolt™ devices. Example use cases include:

- Booting from an external PCIe Based storage controller
- Booting from an external PCIe Based NIC
- Using Thunderbolt™ connected external graphics solution where the user requires screen output before the OS starts

Pre-Boot PCIe device support (with default BIOS settings) varies based on notebook generation.

Default Thunderbolt™ Security settings in BIOS	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2016**	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2017**	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018***	**HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2019***
User Authorization Required (SL1)	Supported (Default = Enabled)	Supported (Default = Enabled)	Supported (Default = Enabled)	Supported (Default = Disabled)
DMA Protection	Not Supported	Not Supported	Not Supported	Supported (Default = Enabled)
Pre-boot Support	No Support with Defaults (PCIe interface from Thunderbolt™ will not be enabled)	No Support with Defaults (PCIe interface from Thunderbolt™ will not be enabled)	Device MUST first be authorized by authenticated user in Windows to “always connect”. Thereafter if that specific device is present, Thunderbolt™ controller will auto-connect PCIe interface in Preboot	All DMA from Thunderbolt™ devices are blocked by default. UEFI device driver support is required to request memory buffer from UEFI environment and UEFI will allocate a buffer and reconfigure IOMMU to allow DMA to that region only

* HP EliteBook x360 830 G5 has the same Thunderbolt™ security features as HP EliteBooks and ZBooks (with Thunderbolt™ support) released in 2018.

With DMAr support enabled, any Thunderbolt™ device requiring DMA that has a UEFI driver that does not request allocation of a memory buffer using the UEFI protocol will not be operable.

User Authorization (SL1) can be used in conjunction with DMA Protection which provides multiple layers of protection:

1. User must first approve in Windows and choose “always connect” before the device will be connected in the BIOS Pre-OS environment
2. Once connected, the device will be subject to DMA Protection restrictions

Note that “Secure Connect” (SL2) is not compatible with Pre-boot use cases for Thunderbolt™ devices that require a PCIe interface.

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIebased Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

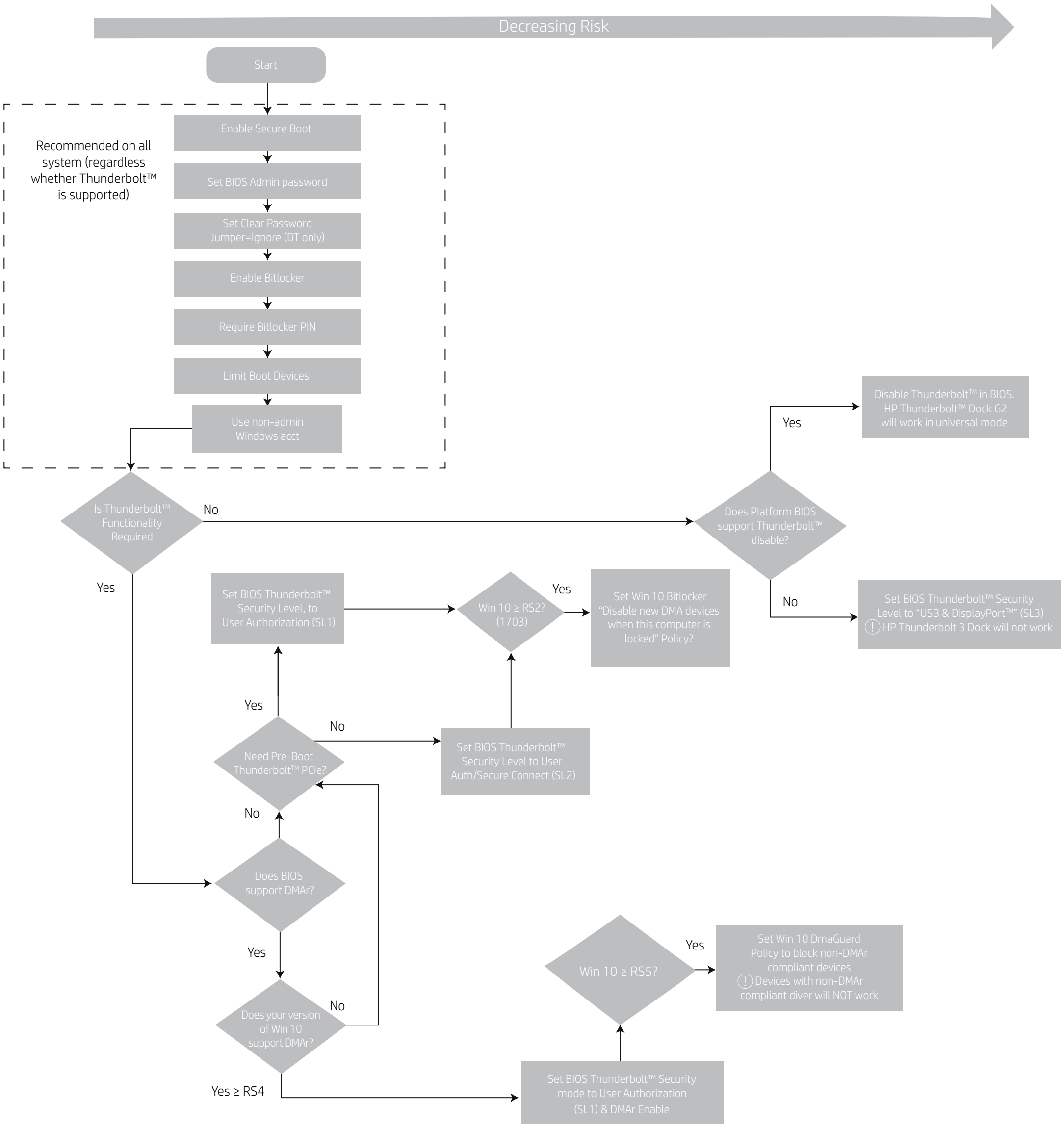
10
Additional Resources

SUMMARY OF SECURITY OPTIONS

The diagram below summarizes the various topics discussed in this paper and provides guidance on the options available for a given OS and Hardware capabilities as well as customer environment requirements. The further to the right side of the page that the final solution terminates, the higher the level of protection.

There are 3 types mitigations at a high level

1. Disable Thunderbolt™ PCIe connections (and thus completely block DMA).
2. Block new DMA capable Thunderbolt™ device until an authenticated user explicitly approves the connection.
3. Use of IOMMU Hardware to restrict the memory range each DMA capable device can access.


Decreasing Risk
Start
Recommended on all system (regardless whether Thunderbolt™ is supported)
Enable Secure Boot
Set BIOS Admin password
Set Clear Password Jumper=Ignore (DT only)
Enable Bitlocker
Require Bitlocker PIN
Limit Boot Devices
Use non-admin Windows acct
Is Thunderbolt™ Functionality Required
No
Yes
Does Platform BIOS support Thunderbolt™ disable?
Yes
Disable Thunderbolt™ in BIOS. HP Thunderbolt™ Dock G2 will work in universal mode
No
Set BIOS Thunderbolt™ Security Level to "USB & DisplayPort™" (SL3)
! HP Thunderbolt 3 Dock will not work
Set BIOS Thunderbolt™ Security Level, to User Authorization (SL1)
Win 10 ≥ RS2? (1703)
Yes
Set Win 10 Bitlocker "Disable new DMA devices when this computer is locked" Policy?
Yes
No
Need Pre-Boot Thunderbolt™ PCIe?
Set BIOS Thunderbolt™ Security Level to User Auth/Secure Connect (SL2)
No
Does BIOS support DMAr?
Yes
Does your version of Win 10 support DMAr?
No
Yes ≥ RS4
Set BIOS Thunderbolt™ Security mode to User Authorization (SL1) & DMAr Enable
Win 10 ≥ RS5?
Yes
Set Win 10 DmaGuard Policy to block non-DMAr compliant devices
! Devices with non-DMAr compliant diver will NOT work

1
Objective
About Thunderbolt™

2
DMA Risks
General Risk Mitigation Strategies

3-6
Thunderbolt™ DMA Risk Mitigation BIOS Policies

7
Windows 10 Policies

8
Using PCIebased Thunderbolt™ devices in BIOS Pre-OS environment

9
Summary of Security Options

10
Additional Resources

ADDITIONAL RESOURCES

HP

HP Thunderbolt Dock G2 Technical Whitepaper
http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-3384ENW&doctype=Technical%20white%20paper&doclang=EN_US&searchquery=&cc=us&lc=en

HP Elite Dock with Thunderbolt™ & HP ZBook Dock with Thunderbolt™ Whitepaper
http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA6-5088ENW

MICROSOFT

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures#protecting-thunderbolt-and-other-dma-ports).

https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune#protect-against-direct-memory-access-dma-attacks

INTEL®

Thunderbolt™ and Security on Microsoft Windows 10 Operating System
https://thunderbolttechnology.net/security/Thunderbolt%203%20and%20Security.pdf

LET US HELP YOU CREATE SOME AMAZING BUSINESS SOLUTIONS TODAY

CONTACT US

4AA7-5807ENW, April 2020