Lenovo ThinkShield Secure Wipe on Workstation

ThinkStation: PX-P7-P5-P3-P360-P358-P350

ThinkPad P-Series Workstations



Table of Contents

Overview	. 3
Section 1 – Prepare Drive(s) for Secure Wipe	. 4
Section 2 – Secure Wipe on ThinkStation	. 9
Section 4 – Secure Wipe on ThinkPad	14
Section 5 – Revision History	.19

Overview

The purpose of this document is to provide guidelines for users on how to securely erase SATA and M.2 drives in select Lenovo ThinkStations and ThinkPads using the built-in ThinkShield Secure Wipe feature. Secure Wipe is available for drives utilizing the onboard controller. Secure Wipe for drives utilizing external controllers is not currently supported.

Some last generation and legacy ThinkStation platforms utilize Secure Erase instead of Secure Wipe. For more information on that feature, please see the ThinkStation Secure Erase whitepaper.

Section 1 – Prepare Drive(s) for Secure Wipe

The following instructions will cover the steps required to use ThinkStation BIOS to securely erase SATA HDD/SSD and M.2 NVMe drives.

To avoid erasing incorrect drives, Lenovo recommends users remove any drives not targeted for erasure to ensure only the intended drive is erased. If the user does not wish to remove any drives from the system, it is <u>highly</u> recommended to externally back up data from non-targeted drives to avoid accidental loss of data.

The ThinkShield Secure Wipe feature works best when erasing single drives rather than an entire RAID array or its members sequentially. It is recommended to switch the system's storage setting to AHCI and erase each drive individually.

Magnetic rotating drives will take significantly longer to erase compared to M.2 and SSD drives due to the nature of the older technology. Using legacy erasure methods may also increase the process duration for any drive type. Large capacity HDDs may take hours to complete, and the system cannot be used while the process is occurring.

 With the target drive connected to the system, power on the system and press "F1" at the Lenovo splash screen to enter the BIOS setup. Navigate to the "Devices" tab and select the "Storage Setup". This may appear as "ATA Drive Setup" on some systems. Press enter.

ThinkStation	USB Setup Select this option to configure your system's USB port. Storage Setup Color this configure way system's dependence
Start Menu Main Pevices Advanced Power Security Startup Exit Exit	 > Video Setup Select this option to configure your system's video. > Audio Setup Select this option to configure your system's audio. > Network Setup Select this option to configure your system's network. > PCIe Setup Select this option to configure your system's PCIe slot.
F1 Help ESC Exit	1 Select Item +/- Change Values F9 Setup Defaults ↔ Select Menu Enter Select > Sub-Menu F10 Save and Exit
	Version 2.21.0052. Copyright (C) 2023 AM1

2. Make sure the "Configure SATA as" option is set to "AHCI".

I IIIIIKƏLALIVII.	SATA Controller Select whether to enable or disable SATA controller.	Enabled 🗸
	SATA Drive 1 Select whether to enable or disable SATA drive 1.	Enabled 🗸
G Main	SATA Drive 2 Select whether to enable or disable SATA drive 2.	Enabled 🗸
🖞 Devices	SATA Drive 3 Select whether to enable or disable SATA drive 3.	Enabled 🗸
求 Advanced	M.2 Drive 1 Select whether to enable or disable M.2 drive 1.	Enabled 🗸
A Security	M.2 Drive 2 Select whether to enable or disable M.2 drive 2.	Enabled
🚣 Startup [→ Exit	MCIO Drive Select whether to enable or disable MCIO drive.	Enabled 🗸
Lenovo.	Configure SATA as Select AHCI/RAID Mode. NOTE: Device driver support is required for AHCI or RAID. Depending on how the hard disk image was installed, changing this setting may prevent the system from booting.	AHCI V
F1 Help ESC Exit	1↓ Select Item +/- Change Values €→ Select Menu Enter Select > Sub-Menu	F9 Setup Defaults F10 Save and Exit

3. Some platforms' RAID options may be listed under Advanced→"Intel® VROC SATA Controller" (for SATA RAID) or "Intel® Virtual RAID on CPU" (for M.2 NVMe VMD RAID). These titles may vary by platform. RAID arrays can be deconstructed in these menus.

ThinkStation	Common RefCode Configuration Displays and provides option to change the Common RefCode Settings. Intel(R) Manageability Contains Intel vPro features.	
Start Menu		
에 Main 谷 Devices	> Intel(R) Total Memory Encryption Contains Intel(R) Total Memory Encryption features.	
Advanced Power Security	 Intel(R) VROC SATA Controller This formset allows the user to manage RAID volumes on the Intel(R) RAID Controller 	
	Intel(R) Virtual RAID on CPU This formset allows the user to manage Intel(R) Virtual RAID on CPU	
_	BIOS Self-healing [Enabled] Enable BIOS Self-healing feature [Disabled] Disable BIOS Self-healing feature	Enabled
Lenovo	BIOS Never Crash [Enabled] Enable BIOS Never Crash feature [Disabled] Disable BIOS Never Crash feature	Enabled
F1 Help	Select Item +/- Change Values Select Select > Sub-Menu	F9 Setup Defaults

4. For all systems, to perform Secure Wipe, a password must be assigned to the drive. If a password is not assigned now, the user will be prompted later in the Secure Wipe process to assign one. To do this, navigate to Security→Hard Disk Password. Highlight "SATA Drive # Password" or "M.2 Drive # Password" and press enter.

ThinkStation.	← Hard Disk Password	
Start Menu 命 ^{Main} 완 Devices	M.2 Drive 1 Password [Disabled] Hard Disk Password prevents unauthorized users from accessing the data on the Hard Disk. In addition to the User Password, an optional Admin Password can be used to recover the disk if the User Password is lost. NOTE: If several disks are present, suggest to set all Hard Disk Passwords to the same.	
 ※ Advanced > Power Security ▲ Startup → Exit 	Require HDP on System Boot [Auto] Hard Disk Password (HDP) will be required if the Hard Disk is in lock status when the system starts from the full off, hibernate or restart state. [Power On] Hard Disk Password (HDP) will be required when the system starts from the full off or hibernate state. [No] HDP will not be required. However, HDP will be required when the hard disk is attached to a different system.	Auto 🗸
Lenovo.	Block SID Authentication [Enabled] - TCG Storage device will block attempts to authenticate the SID authority unit a subsequent device power cycle occurs. [Disabled] - Allow SID authentication in TCG Storage device at the next system boot only, not all subsequent boots.	Enabled 🗸
F1 Help ESC Exit	All Select Item +/- Change Values ↔ Select Menu Enter Select > Sub-Menu	F9 Setup Defaults F10 Save and Exit

5. A "Setup Confirmation" box will appear. Select "User" or "Single Password" and press enter. The dual password option may also be selected, however only the single user password is required for the Secure Wipe feature.

In the Disk Password [Disabled] Drive 1 Password [Disabled] Disk Password prevents unauthenized users from accessing the data he Hand Disk. In addition to the User Password, an optional Admin word can be used to recover the disk if the User Password is lost. Event disks are present, suggest to set all Hard Disk Passwords to the e.		
tup Confirmation		
lect "Single Password" only or "Dual Password (Admin+User)"		~
[Single Password] [Dual Password (Admin+User)] Cancel		
HDP will not be required. However, HDP will be required when the bard is attached to a different system.	and the second s	
	Enabled	~
bled] - TCG Storage device will block attempts to authenticate the SID only until a subsequent device over cycle occurs. abled] - Allow SID authentication in TCG Storage device at the next im boot only, not all subsequent boots.		
	tup Confirmation ect "Single Password" only or "Dual Password (Admin+User)" [Single Password] [Dual Password (Admin+User)] Cancel HDP will not be required However, HDP will be required when the bard is attached to a different system. k SID Authentication leed] -TGS Storage device will block attempts to authenticate the SID only until a subsequent device power cycle occurs. bled] -Allow SID authentication in TGS Storage device at the next in boot only, and all subsequent boots.	tup Confirmation ect "Single Password" only or "Dual Password (Admin+User)" [Single Password] [Dual Password (Admin+User)] Cancel HDP will not be required. However, HDP will be required when the hard is attached to a different system: k SID Authentication Enabled led] TGS Storage device will block attempts to authenticate the SID only until a subsequent device power cycle occurs. ubed] - Allow SID authentication in TGS Storage device at the next in boot only, not all subsequent tools.

6. Choose a simple, temporary password and confirm it. <u>Write down this</u> <u>password as it will be needed later.</u> Select "Yes" to continue. This password will also be erased alongside all data on the drive.

i iiiiik9fgfif	Hard Disk Pass	sword		
Start Menu	NVMe 1 Password			
Main C Devices	Enter New Password		Show Password	
* Advanced	Confirm New Password		Keyboard Layout	~
 Becurity ▲ Startup → Exit 			51 <u>6</u> 131	
Lenovo		Yes No	=	~
F1 Help	1↓ Select Item	+/- Change Valu	es F9 Setup	Defaults

7. A "Setup Notice" box will be prompted, displaying that the changes have been saved. Press "Continue".

ThinkStation	Hard Disk Password M.2 Drive 1 Password [Disabled]	
Start Menu	Hard Disk Password prevents unauthorized users from accessing the data on the Hard Disk. In addition to the User Password, an optional Admin Password, an optional Admin	
🔂 Main		
삼 Devices		
₩ Advanced	Setup Notice	
O Power		
	Changes have been saved.	~
🝰 Startup	Continue	
⇒ Exit	[No] HDP will not be required. However, HDP will be required when the hard disk is attached to a different system.	
		Enabled 🗸
Lenovo	[Enabled] - TGG Storage device will block attempts to authenticate the SID authority until a subsequent device power cycle occurs. [Disabled] - Allow SID authentication in TGG Storage device at the next system boot only, not all subsequent boots.	
	Select Item +/- Change Values Select > Select > Sub-Manu	
	Enter Select > Sub-Menu	

8. At this point, the system needs to be rebooted for the changes to take effect. Press "F10" function key to save and exit the BIOS setup.

I UIUK2(ALION	← Hard Disk Password	
Start Menu	M.2 Drive 1 Password [Single Password] Hard Disk Password prevents unauthorized users from accessing the on the Hard Disk. In addition to the User Password, an optional Admi Password can be used to recover the disk if the User Password is lost	
Main A Devices	NOTE: If several di same. Save & reset	
₩ Advanced	? Save configuration and reset?	
O Power		
🔒 Security	Require H [Auto] Hard	Auto
📩 Startup	status when [Power On] state from	
⊨ Exit	[No] HDP wi disk is attac Yes N	lo
Lenovo	Block SID [Enabled] - TCG Storage device will block attempts to authenticate th authonity until a subsequent device power cycle occurs. [Disabled] - Allow SID authentication in TCG Storage device at the ne system boot only, not all subsequent boots.	Enabled V
	ty Select Item +/- Change Value	

9. Once the system starts to reboot, press "F1" at Lenovo splash screen to enter the BIOS setup again. If the system prompts to enter the "Hard Disk Password", enter the assigned password.

Section 2 – Secure Wipe on ThinkStation

This section covers performing the Secure Wipe function for ThinkStation. The tables below list methods found on most systems. Some methods may appear/disappear depending on system model, drive type, and RAID status. Secure Wipe is available for drives utilizing the onboard controller. Secure Wipe for drives utilizing external controllers is not currently supported.

Erase Method	Description
ATA Secure Erase	This method resets all data on the drive in the standard way.
ATA Cryptographic Key Reset	For Full Disk Encrypted drives only. This method resets the internal encryption key, making the drive data completely unreadable.

Legacy Methods – These methods are not guaranteed to fully erase a modern hard drive.

Legacy Erase Method
US DoD 5220.22-M
Single Pass Zeros
US Navy & Air Force
CSE Canada ITSG-06 (Unclassified)
British HMG Infosec Standard 5, Enhanced
German VSITR
Russian GOST P50739-95 Level 1
Russian GOST P50739-95 Level 4
RCMP TSSIT OPS-II

1. Enter BIOS and navigate to "Secure Wipe" under the Security tab. Set to "Enabled". Press F10 to save the setting and reboot the system.

ChinkStation	Secure Roll Back Prevention [Yes] - Flash BIOS to a previous or current version is not allowed. This is the default setting. [No! - Flash BIOS to a previous or current version is allowed.	Yes 🗸
Start Menu 命 ^{Main}	Mindows UEFI Firmware Update This option enables or disables windows UEFI firmware update feature. [Enabled] Allow windows UEFI firmware update. [Disabled] BIOS will siki pindows UEFI firmware update. Smart USB Protection	Enabled V
谷 Devices 梁 Advanced ① Power	Smart USB Protection could block copying data from the computer to the USB storage device in Window: Read Only mode: the user can copy data from USB storage device to the Computer but cannot copy data from the computer to USB storage device No Access mode: the user cannot use USB storage device in Windows	U.Subcu V
 Control Security Startup → Exit 	Secure Wipe [Enabled] Display the "secure wipe" option on the F12 BIOS Startup Menu. Users can select this option to securely erase HDD data. [Disabled] Hidden the "secure wipe" option on the F12 BIOS Startup Menu. NOTE: Some HDD will meet install error after erase, please use the "clean" command of "diskpart" to clean the HDD.	Disabled V Enabled Disabled
Lenovo	> TCG Feature Setup Contains TCG security features.	
F1 Help FSC Evit	↑ Select Item +/- Change Values	F9 Setup Defaults

2. On the Lenovo splash screen, press F12 to enter the Boot Menu. Navigate to the App Menu and select "ThinkShield secure wipe".

ThinkStation	App Menu			
💩 Boot Menu	Lenovo Diagnostics Asset Information ThinkShield secure wipe Intel Management Engine B	OS Extension		
Lenovo				
↑↓ Select Item	€Э Select Menu	Enter	Select > Sub-Menu	ESC Exit

3. ThinkShield will load and list available drives in the system that can be wiped. Click "NEXT" to proceed.

ThinkShield	×
ThinkShieldTM secure wipe - v1.9.1 -	
	What storage device do you want to wipe?
	€ 🚍 SAMSUNG HZVLBITOHBLR-000L7
	P1
Lenovo.	NEXT >

4. Select the preferred erasure method. "ATA Secure Erase" will be used in this example. Click "NEXT".

Thinkshield TM secure wipe - v1.9.1 - Which method do you want to use? Show Legacy Methods This method resets all data on the drive in the standard way. Completion time: varies according to storage capacity.	ThinkShield	÷	×
Hick method do you want to use?	ThinkShieldTM secure wipe – v1.9.1 –		
blow Legacy Methods		Which method do you want to use?	
		Show Legacy Methods ATA Secure Erase This method resets all data on the drive in the standard way. Completion time: varies according to storage capacity.	
	Lenovo	NEXT >	

5. This is the final warning to the user that all data will be erased. Once acknowledged, click "OK".



6. If the user forgot to assign a password on the drive, ThinkShield will prompt at this step to assign one to the drive.

ThinkShield	×
ThinkShieldTM secure wipe - v1.9.1 -	
	This disk wasn't protected by HDD Password. Please set the HDD Password to continue Erase.
	Enter New Password:
	Confirm New Password:
	₽.
Lenovo"	NEXT >

7. The wiping process will now start. Once concluded the system will need to be rebooted. The temporary password set on the drive is now erased. Once the reboot is concluded, the system can be powered down, and the drive can safely be removed from the system. Repeat the process for any additional drives that might need to be securely wiped.

ThinkShield	×
ThinkShieldTM secure wipe - v1.9.1 -	
	Data wipe is successful!
	Drive: SAMSUNG MZVLBITOHBLR-000L7
	Capacity: 953.86 GB
	Method: ATA Secure Erase
	Start: 03/01/2023 at 09:05:04
	End: 03/01/2023 at 09:05:05
	View Wipe Log Go
Lenovo	Return to Top Reboot

Section 4 – Secure Wipe on ThinkPad

The following instructions will cover the steps required to use ThinkShield feature in ThinkPad BIOS to securely erase storage drives.

1. Boot into BIOS by pressing function "F1" key at the Lenovo splash screen.



2. Once inside the BIOS setup, navigate to the "Security" menu and select "ThinkShield secure wipe".

ThinkPad	Security		
i iiiiini uu	→ Password		î
C .	→ Fingerprint		
Setup	→ Security Chip		
🛱 Main	→ UEFI BIOS Update Option		
 فاغ Config	→ Memory Protection		
	→ Virtualization		
O Date/Time	→ I/O Port Access		
🗄 Security	→ Internal Device Access		
⊥ Startup	→ Absolute Persistence® Module		
Restart	→ Secure Boot		
	→ Intel® SGX		
	→ Device Guard		
Leriovo.	ThinkShield secure wipe		·
F1 General Help	F9 Setup Defaults	Esc Back	F10 Save and Exit

3. Confirm the "ThinkShield secure wipe in App Menu" is set to enabled.

ThinkPad	 ← Security ThinkShield secure wipe 	
Setup	ThinkShield secure wipe in App Menu [On] Enable the ThinkShield secure wipe in the App Menu invoked by F12.	On
🔂 Main	[Off] Disable the ThinkShield secure wipe in the App Menu invoked by F12.	
않 Config		
O Date/Time	N	
🗄 Security	10	
🛧 Startup		
رع Restart		
Lenovo.		
F1 General Help	F9 Setup Defaults Esc Back	F10 Save and Exit

4. Save and exit the BIOS setup by pressing the "F10" function key.

On reboot, load the "Boot Menu" by pressing the "F12" function key at the Lenovo splash screen. Tab over to the "App Menu" and select "ThinkShield secure wipe" option.

ThinkPad	App Menu Setup Diagnostic Splash Screen Lenovo Diagnostics Regulatory Information ThinkShield secure wipe			
የያ App Menu				
Lenovo.		lş.		
11 Move	Expand/Collapse	Tab Switch Menu	Enter Select	Esc Exit

5. Select the storage device to be erased and press "Next".

ThinkShield	>
ThinkShield™ secure wipe	
	What storage device do you want to wipe?
	• 🚍 WD PC SN810 SDCQNRY-512G-1001 [476.93 GB]
Lenovo	NEXT >

6. Select an appropriate method from the dropdown menu to securely erase the chosen drive and press "Next". "ATA Secure Erase" will be used in this example.

ThinkShield	<	×
ThinkShield™ secure wipe		
	Which method do you want to use?	
	ATA Secure Erase	
	For SSD drives only.	
	This method resets all data on the drive in the standard way.	
	Completion time: varies according to storage capacity.	
Lenovo.	NEXT >	

7. A warning will appear to confirm if the user wants to continue with the secure erase process. Select "Yes" to proceed.



8. A progress window will appear displaying the data wiping process. Do not power off until the process is complete.

ThinkShield	
ThinkShield™ secure wipe	DO NOT POWER OFF DURING AN WIPE Data is wiping, please wait
	:: 2%
Lenovo	Drive:WD PC \$N810 SDCQNRY-512G-1001Capacity:476.93 GBMethod:ATA Secure EraseStart:2023/06/08 11:23:28
	4

9. On completion of the process, a confirmation message will be displayed. At this time, drives are wiped successfully, and the system should be rebooted for the changes to take effect. Select "Reboot".

ThinkShield ThinkShield™ secure wipe	×
	Data wipe is successful!
	Drive: WD PC SN810 SDCQNRY-512G-1001 Capacity: 476.93 GB Method: ATA Secure Erase Start: 2023/06/08 11:23:28 End: 2023/06/08 11:23:35
Lenovo.	View Wipe Log Return to Top Reboot

10. At this point, the erase procedure is complete. The temporary password on the drive is now erased. Repeat the process for any additional drives that might need to be securely erased.

Section 5 – Revision History

Version	Date	Author	Updates
1.0	7/26/2023	Chris C.	Initial Release