#### Lenovo Secure Erase on ThinkStation

ThinkStation: P920-P720-P620-P520-P520c-P340-P348-Other Legacy Platforms





### **Table of Contents**

Overview	3
Section 1 – Prepare Drive for Secure Erase on ThinkStation	4
Section 2 – Secure Erase on ThinkStation	10
Section 3 – Revision History	14

#### Overview

The purpose of this document is to provide guidelines for users on how to securely erase SATA and M.2 drives in Lenovo ThinkStation P920, P720, P620, P520, P520c, P340, P330 and other legacy platforms. Certain other legacy platforms may not have the Secure Erase feature.

Images in this document were taken from the latest platforms with graphical BIOS setup screens. BIOS interfaces on older platforms may appear different than the images shown.

ThinkStation users can find Secure Erase by looking in BIOS under the Security tab and entering the Hard Drive Password feature. Secure Erase is available for drives utilizing the onboard controller.

ThinkStation	← Hard Disk Password	
Start Menu 유 Main Ƴ Devices ※ Advanced	M.2 Drive 1 Password [User] Hand Disk Password prevents unauthorized users from accessing the data on the Hard Disk. In addition to the User Password, an optional Master 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.	
Power Security Startup	Require HDP on System Boot [Auto] - Hard Disk Password (HDP) will be required if the Hard Disk is in lock status when the system stars from the full off, hibemate or restart state. [No] - HDP will not be required. Noweer, HDP will be required when the hard disk is attached to a different system.	Auto 🗸
Exit Lenovo.	<ul> <li>Security Erase HDD Data Select this option to security erase HDD data. The items are only available when corresponding hard disk password is present.</li> </ul>	
F1 Help ESC Exit	1↓         Select Item         •/-         Change Values           ↔         Select Menu         Enter         Select >Sub-Menu	F9 Setup Defaults F10 Save and Exit

# Section 1 – Prepare Drive for Secure Erase on ThinkStation

The following instructions will cover the steps to prepare SATA HDDs/SSDs and M.2 drives for secure erasure.

To use the Secure Erase feature, any drive the user wishes to be erase must be installed in the system either through onboard ports or add-in expansion card.

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 highly recommended to externally back up data from non-targeted drives to avoid accidental loss of data.

Lenovo recommends setting the system's storage mode to AHCI when performing Secure Erase. Complications may arise while attempting to erase RAID array member drives. For this reason, targeted drives should be removed from their RAID arrays and the system set to AHCI mode before beginning the Secure Erase Procedure. Secure Erase is available for drives utilizing the onboard controller.

 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 "ATA Drive Setup". This may appear as "PCH SATA Configuration" on some systems. Press enter.



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

	×.	
	ATA Drive Setup	
tart Menu	SATA Controller Select whether to enable or disable SATA controller.	Enabled
🛱 Main	SATA Drive 1 Select whether to enable or disable SATA drive 1.	Enabled
P Devices	SATA Drive 2 Select whether to enable or disable SATA drive 2.	Enabled
D Power	SATA Drive 3 Select whether to enable or disable SATA drive 3.	Enabled
A Security	SATA Drive 4 Select whether to enable or disable SATA drive 4.	Enabled
Exit	SATA Drive 4 Hot-Plug Support Select whether to enable or disable hot-plug for this port.	Disabled
Lenovo.	Configure SATA as Select AHC(#AID/Intel(R) RST with Intel(R) Optane Mode. NOTE Device driver support is required, for AHCI or BAID or Intel(R) DBT with Intel(R) Optane. Dependence on the part dick image was installed reparating this setting	AHCI
F1 Help ISC Exit	14 Select Item +/- Change Values 43 Select Menu Enter Select 5 Sub-Menu	F9 Setup Defaults F10 Save and Exit

3. [P620] P620 users will also need to navigate to the "Devices" tab and select the "NVMe Setup".

ThinkStation	<ul> <li>Serial Port Setup</li> <li>Select this option to configure your system's serial por</li> <li>USB Setup</li> </ul>	L.		
Start Menu	Select this option to configure your system's USB port.			
Main	Select this option to configure your system's ATA drive			
4 Devices	> NVMe Setup Select this option to configure your system's NVMe driv	re.		
<ul><li>☆ Advanced</li><li>○ Power</li></ul>	<ul> <li>Video Setup</li> <li>Select this option to configure your system's video.</li> </ul>			
🕂 Security	> Audio Setup Select this option to configure your system's audio.			
Exit	> Network Setup Select this option to configure your system's network.			
Lenovo	> Thunderbolt Setup Select this option to configure your system's Thunderb	olt.		
	> RAIDXpert2 Configuration Utility			~
F1 Help ESC Exit	↑↓         Select Item         +/-           ←>         Select Menu         Enter	Change Values Select > Sub-Menu	F9 Setup Defaults F10 Save and Exit	

4. [P620] Make sure the "NVMe RAID Mode" is set to "Disabled".

ThinkStation	$\leftarrow$
	NVMe Setup
Start Menu	NVMe RAID Mode Disabled VMe RAID mode.
A Main	NOTE: Device driver support is required for NVMe RAID.Depending on how the hard disk image was installed, changing this setting may prevent the
A Devices	system from booting. System should be installed on First array if the system is booted from AMD-RAID Array.
Advanced	
D Power	
🔒 Security	
📩 Startup	
→ Exit	
Lenovo	
F1 Help ESC Exit	Image         etc         Change Values         F9         Setup Defaults           Image         Select Menu         Enter         Select > Sub-Menu         F10         Save and Exit
	Version 2.21.0052. Copyright (C) 2022 AM1

5. Navigate the "Security" tab. Select the "Hard Disk Password" option, then press enter.

Thinl/Ctation	Power-On Password	Not Installed	î
I IIIIIKƏLALIVII.	System Management Password	Not Installed	
	Set Supervisor Password		
Start Menu	Select this line to set, change, or delete the Supervisor Passwor NOTE:	d.	
Main	To delete Supervisor Password, enter blank fields for each new line item.	password	
俗 Devices	Set Power-On Password		
Advanced	Select this line to set, change, or delete the Power-On Passwore NOTE:	1.	
Power	To delete Power-On Password, enter blank fields for each new p line item.	bassword	
A Security	Set System Management Password		
	Select this line to set, change, or delete the System Manageme (SMP).	nt Password	
💑 Startup	NOTE: To delete Sustem Management Password, onter black fields for	and new	
→ Exit	password line item.	each new	
	> System Management Password Access Control		
	System Management Password prevents unauthorized user fro BIOS Setup in default.	m accessing	
Lenovo	> Hard Disk Password		
	Configure hard disk password.		
F1 Help	↑↓ Select Item +/- Chang	e Values F9 Setup Defaults	
ESC Exit	€→ Select Menu Enter Select	> Sub-Menu F10 Save and Exit	

6. To perform Secure Erase, a password must be assigned to the drive. If a password is already assigned to the drive, <u>the rest of this Section can be skipped</u>. Otherwise, highlight "SATA Drive X Password" or "M.2 Drive X Password" (Where X = drive number to be erased, based on the port where it is installed) and press enter.

ThinkStation	<i></i>	
	Hard Disk Password	
Start Menu 슈 <sup>Main</sup> 谷 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.	
<ul> <li>৵ Advanced</li> <li>O Power</li> <li>G Security</li> <li>▲ Startup</li> <li>→ Exit</li> </ul>	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 of for 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	Use is a studied us an interior system. Biock SID Authentication [Enabled] - TCG Storage device will block attempts to authenticate the SID authority until a subsequent device power cycle occurs. [Disabled] - Aliow SID authentication in TCG Storage device at the next system boot only, not all subsequent boots.	Enabled 🗸
F1 Help ESC Exit	♣↓         Select Item         +/-         Change Values           ♠→         Select Menu         Enter         Select > Sub-Menu	F9 Setup Defaults F10 Save and Exit

7. 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 Erase feature.

INNKSTATION	÷		
	Hard Disk Password		
Start Menu 슈 <sup>Main</sup> 俗 Devices			
🖗 Advanced	Setup Confirmation		
D Power			
A Security	Select "Single Password" only or "Dual Password (Admin+User)"		~
🖧 Startup	[Single Password] [Dual Password (Admin+User)] Cancel		
⊖ Exit	[No] HDP will not be required. However, HDP will be required when the hard disk is attached to a different system.		
Lenovo	Block SID Authentication [Enabled] - TCG Storage device will block attempts to authenticate the SID authenty until 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	~

8. Choose a 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.

ThinkStation	. ← Hard Disk Passw	ord		
Start Menu	NVMe 1 Password			
<ul> <li>Main</li> <li>☆ Devices</li> <li>☆ Advanced</li> <li>↔ Power</li> </ul>	Enter New Password		Show Password Off Keyboard Layout	
🔒 Security	*****		English	~
🚵 Startup [→ Exit			-	~
Lenovo.	↑↓ Select Item	Yes No	es F9 Setur	) Defaults
	←→ Select Menu	Enter Select > Sub-	Menu F10 Save	

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

<b>ThinkStation</b>	← Hard Disk Password		
Start Menu 슈 Main 俗 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.		
桨 Advanced	Setup Notice		
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.		
Fl Help ESC Exit	Select Item         +/-         Change Values           ↔         Select Menu         Enter         Select > Sub-Menu	F9 Setur F10 Save	Defaults and Exit
	Version 2.21.0052. Copyright (C) 2023 AMI		

10. 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 hinkStation	← Hard Disk Password	
Start Menu	M.2 Drive 1 Password [Single Password] Hard Disk Password prevents unauthorized users from accessing th on the Hard Disk. In addition to the User Password, an optional Ad Password can be used to recover the disk if the User Password is lo	
Main	NOTE: If several di same. Save & reset	
梁 Advanced	? Save configuration and reset?	
Power		
A Security	(Auto) Hard	Auto 🗸
🖧 Startup	status when [Power On]	
Exit	starts from [No] HDP wi disk is attac Yes	No
Lenovo	Block SID [Enabled] - TCG Storage device will block attempts to authenticate authority until a subsequent device power cycle occurs. [Disabled] - Allow SID authentication in TCG Storage device at the system boot only, not all subsequent boots.	the SID Finabled
F1 Help	ty Select Item +/- Change Va	alues F9 Setup Defaults

11. 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 Erase on ThinkStation

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

1. In the BIOS setup, navigate to the "Security" tab and open "Hard Disk Password" option.

[hinkStation]	Power-On Password System Management Password	Not Installed Not Installed
itart Menu	Set Supervisor Password           Select this line to set, change, or delete the Supervisor Password.           NOTE:           To delete Supervisor Password, enter blank fields for each new passworline item.           Set Power-On Password           Select this line to set, change, or delete the Power-On Password.           NOTE:           To delete Power-On Password, enter blank fields for each new passworline item.           Select this line to set, change, or delete the System Management Password           Select this line to set, change, or delete the System Management Password, (SMP).           NOTE:           To delete System Management Password, enter blank fields for each new password line item.           NOTE:           To delete System Management Password, Setter Management Password, SMP).           NOTE:           To delete System Management Password, enter blank fields for each ne password line item.	rd d word ew
Lenovo.	System Management Password prevents unauthorized user from access BIOS Setup in default.  Hard Disk Password Configure hard disk password.   the Select Item the Select Menu fore: Select Menu fore: Select Menu	sing s F9 Setup Defaults denu F10 Save and Exit

2. Highlight the "Security Erase HDD Data" and press enter. Select "Erase SATA Drive X Data" to wipe the drive.

ThinkStation.	← Hard Disk Password	
Start Menu Gi Main 솬 Devices 윤 Advanced	M.2 Drive 1 Password [User] Hard Disk Password prevents unauthorized users from accessing the data on the Hard Disk. In addition to the User Password, an optional Master 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.	
Power           Becurity           Association           Association           Association           Association           Association	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. [No] - HDP will not be required. However, HDP will be required when the hard disk is attached to a different system.	Auto 🗸
E> exit Lenovo.	<ul> <li>Security Erase HDD Data</li> <li>Select this option to security erase HDD data. The items are only available when corresponding hard disk password is present.</li> </ul>	
F1 Help ISC Exit	↑↓     Select Item     +/-     Change Values       ♦→     Select Menu     Enter     Select > Sub-Menu	F9 Setup Defaults F10 Save and Exit

ThinkStation	← Security Erase HDD	Data		
Start Menu	Erase M.2 Drive 1 Data			
Main	Select this option to security erase H	DD data.		
来 Advanced				
Power				
🗄 Security				
[→ Exit				
Lenovo				
F1 Help	L Select Item	+/- Change Values	F9 Setue Defaulte	
ESC Exit	↔ Select Menu	Enter Select > Sub-Menu	F10 Save and Exit	
	Version 2.21.005/J. Copyright (C) 2022 AMI			

3. A "Setup Warning" box will appear as a final warning to the user before erasing the data from the drive permanently. Select "Yes" to proceed.

Start Menu	Erase M.2 Drive 1 Data The time of the control erase HOO data. Setup Warning All HDD data will be erased and the hard disk password will be deleted. Do you really want to continue? No	
	14         Select Item         +/-         Change Values           €→         Select Menu         Enter         Select > Sub-Menu	

4. Input the temporary password, and press enter.

Warning: Proceeding with this step will erase all data from the selected drive and cannot be undone.

	Security Erase HDD	Data	
tart Menu	Please Input User HDP		
🛱 Main	Please Input User HDP		
🕆 Devices			
₩ Advanced			
Dewer			
🔒 Security			
🖧 Startup			
🔁 Exit			
		(as No	
Lenovo			

5. A progress bar will appear to display the secure erase progress. The process should be relatively quick for M.2 and SATA SSDs. Spinning HDDs will take much longer. Total capacity of the drive will also affect duration.

Note: Users should not unplug the system during this process.

ThinkStation.	← Security Erase HDD Data	
Start Menu Main Devices Advanced Power Security Startup Exit Exit	Erase SATA Drive 1 Data Select this a Warning Security erase is in progress, please don't turn off the computer! Process: 7%	
F1 Help ESC Exit	No.         Figure 10         Figure 10         Figure 10         Figure 10         Defaults           €⇒         Select Menu         Figure 10         Save and Exit         Figure 10         Save and Exit	

6. Once the Secure Erase process completes, a new confirmation box will be prompted stating "System will reset to make changes take effect". Press "Continue" to reboot the system.

	← Security Erase HDD Data	
Start Menu	Erase M2 Drive 1 Data Confirmation M M System will reset to make changes take effect. [Continue]	
EEL Help ESC Exit	14         Select Item         -/-         Change Values           €→         Select Menu         Enter         Select > Sub-Menu	

7. At this point, the erase procedure is complete. The temporary password on the drive is now erased. 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 erased.



## Section 3 – Revision History

Version	Date	Author	Updates
1.0	03/22/2021	SP	Initial launch release
1.1	7/26/2023	Chris C.	Updated information