Lenovo
ThinkShield
Security Solutions

ThinkShield Secure Wipe

HARDWARE BASED SECURITY PROTECTS "BELOW-THE-OS" LAYER

Technical Whitepaper

ThinkShield Secure Wipe is Lenovo's solution for securely and completely erasing all data from the embedded storage device. It complies with NIST SP 800-88 Revision 1 - Guidelines for Media Sanitization.

ThinkShield Secure Wipe is a utility program embedded in ThinkPad BIOS aimed to be a part of PC Lifecycle Management (PCLCM) during the retirement phase, preventing any data breaches.

TABLE OF CONTENTS

The purpose of this document is to provide guidelines for users on how to use ThinkShield Secure Wipe on ThinkPad products.

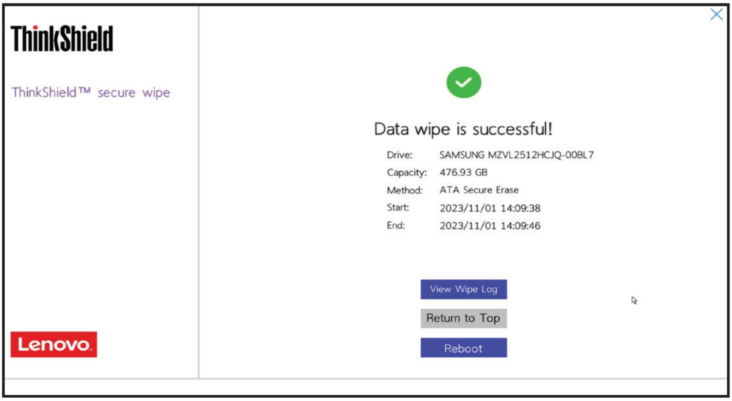
What is ThinkShield Secure Wipe

There have been reports indicating instances in which critical data has been extracted from retired PCs or disposed storage devices. As public awareness of data security and privacy continues to increase, PC manufacturers are required to provide the means to securely and completely erase the data on the storage devices embedded in the PC.

ThinkShield Secure Wipe is a utility program integrated into the BIOS. It offers the functionality to erase all contents stored on drives attached to the system internally. Users can select an erase algorithm from the list, depending on their needs. ThinkShield Secure Wipe comply with NIST SP 800-88 Revision 1 - Guidelines for Media Sanitization.

ThinkPad Products Supporting ThinkShield Secure Wipe

Most of the ThinkPad products shipped after 2019 support ThinkShield Secure Wipe.
This whitepaper is based on the latest version of the ThinkShield Secure Wipe.
Older versions may have different functionalities or a different user interface.

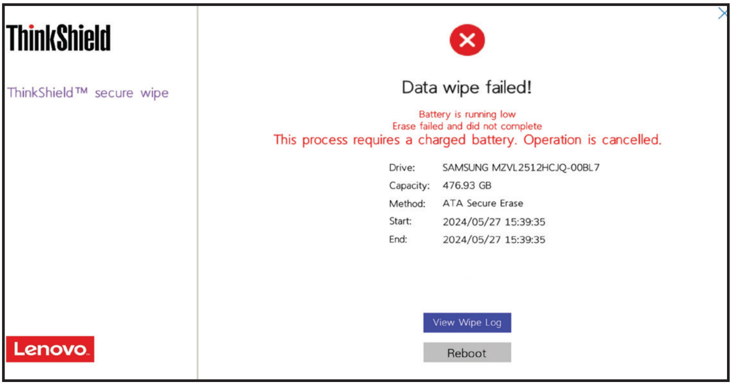


Data wipe is successful!

Drive: SAMSUNG MZVL2512HCJQ-00BL7
Capacity: 476.93 GB
Method: ATA Secure Erase
Start: 2023/11/01 14:09:38
End: 2023/11/01 14:09:46

Note

To proceed with the ThinkShield Secure Wipe, the remaining battery capacity must be greater than 25%.
The following error message will appear if you attempt to perform the secure wipe while the battery level is low:



Data wipe failed!

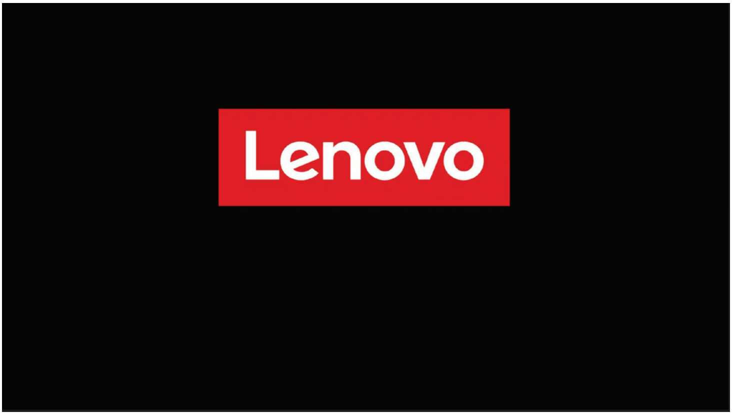
Battery is running low
Erase failed and did not complete
This process requires a charged battery. Operation is cancelled.

Drive: SAMSUNG MZVL2512HCJQ-00BL7
Capacity: 476.93 GB
Method: ATA Secure Erase
Start: 2024/05/27 15:39:35
End: 2024/05/27 15:39:35

Invoking ThinkShield Secure Wipe

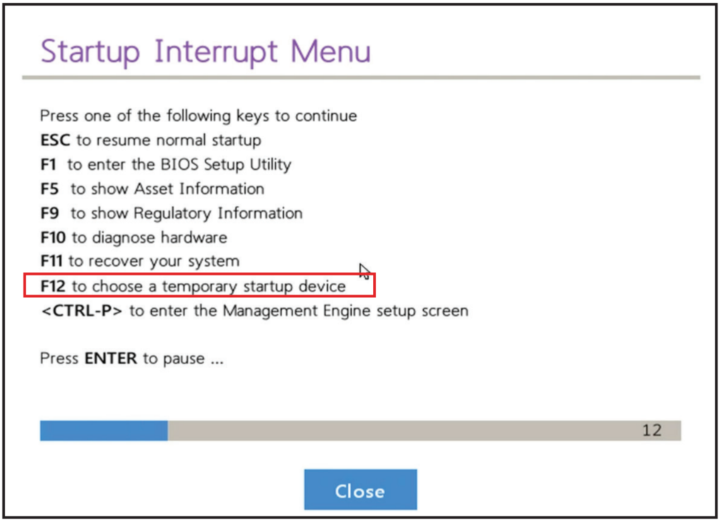
Step 1

Press the [Enter] key rapidly when the Lenovo logo appears on the screen at startup to launch the Startup Interrupt Menu.



Step 2

Press the [F12] key at the Startup Interrupt Menu to make the Boot Menu / App Menu appear.



Startup Interrupt Menu

Press one of the following keys to continue

ESC to resume normal startup

F1 to enter the BIOS Setup Utility

F5 to show Asset Information

F9 to show Regulatory Information

F10 to diagnose hardware

F11 to recover your system

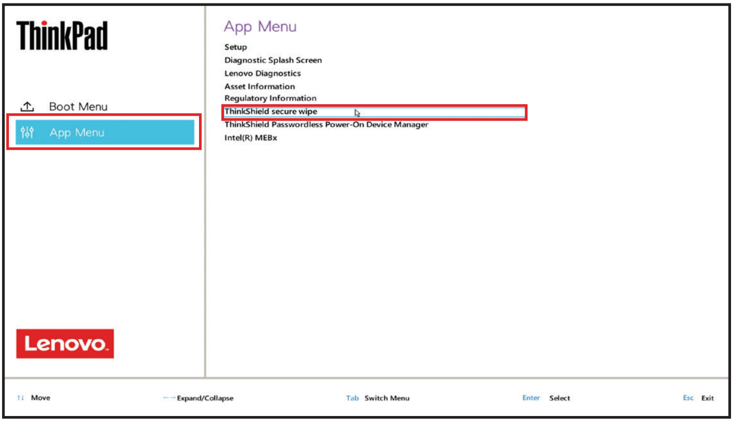
F12 to choose a temporary startup device

<CTRL-P> to enter the Management Engine setup screen

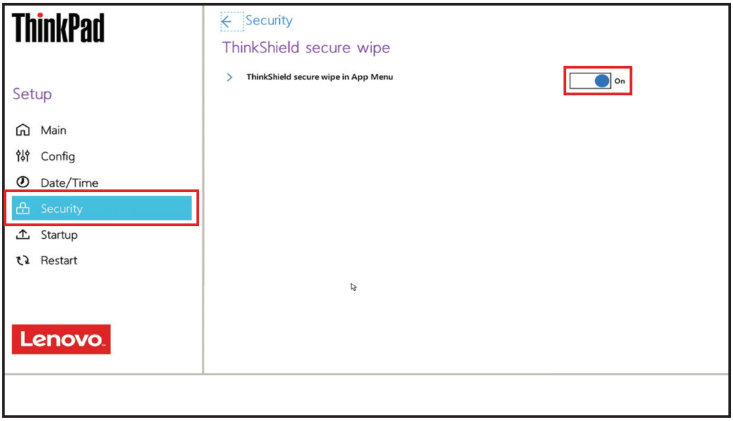
Press **ENTER** to pause ...

Step 3

Click [App Menu] from left column and choose [ThinkShield Secure Wipe] from the right column.



If the 'ThinkShield Secure Wipe' selection does not appear in the App menu, confirm whether ThinkShield Secure Wipe is enabled in the Security options within the BIOS Setup Utility. The default setting is 'On' (enabled).

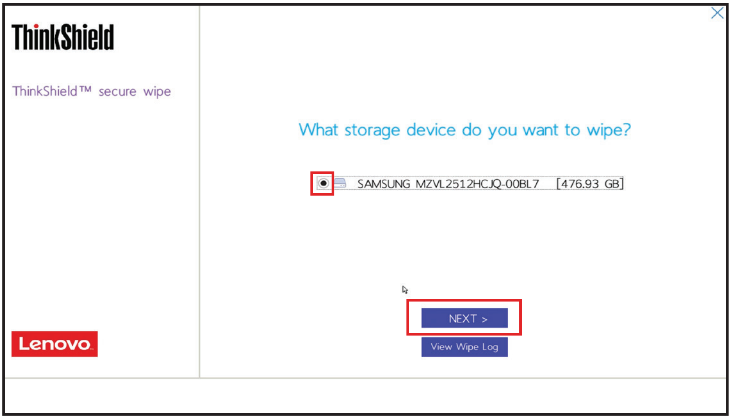


ThinkShield secure wipe in App Menu On

Method to Wipe the Storage Device

Step 1

Select the storage device to be erased. Please note that the selection is based on the entire storage unit, not on a partition basis. After confirming the storage device to be erased, click [NEXT >] at the bottom.

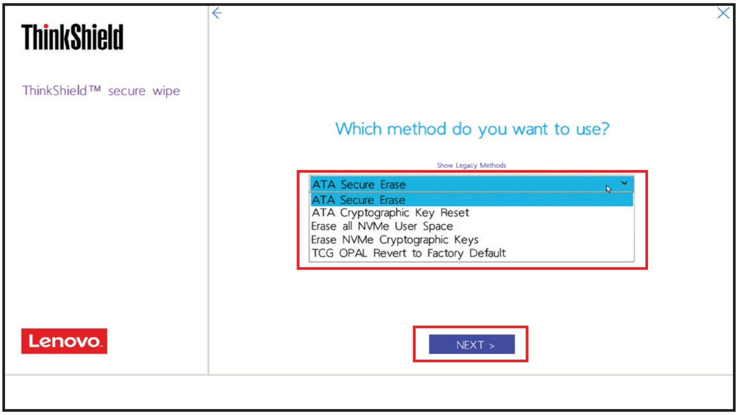


What storage device do you want to wipe?

● SAMSUNG MZVL2512HCJQ-00BL7 [476.93 GB]

Step 2

Select an erase method and click [NEXT >]. You can choose from erasure methods(*), including those commonly used for data deletion - ATA Secure Erase (Secure Erase) and Enhanced Secure Erase. The erase methods available for selection may vary depending on the type and condition of the installed storage.



Which method do you want to use?

ATA Secure Erase

- ATA Secure Erase
- ATA Cryptographic Key Reset
- Erase all NVMe User Space
- Erase NVMe Cryptographic Keys
- TCG OPAL Revert to Factory Default

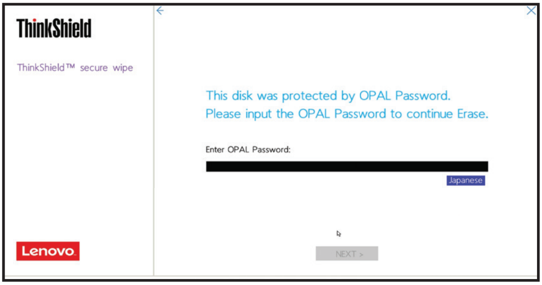
* Refer the "Wipe methods" table on page 8

Wipe Methods

Wipe Method	Target storage device	Command used	Sanitization method defined in the NIST SP 800-88 Rev.1
TCG Opal Revert to Factory Default	Opal SSD	**TCG Opal Revert command** on the Admin SP	Purge
TCG Opal PSID Revert	Opal SSD	**TCG Opal Revert command** with the PSID (Physical Presence SID)	Purge
Erase NVMe Cryptographic Keys	NVMe SSD	**NVMe Format NVM command** (Cryptographic Erase)	Purge
Erase all NVMe User Space	NVMe SSD	**NVMe Format NVM command** (User Data Erase)	Purge
ATA SECURE ERASE	ATA SSD	**ATA SECURITY ERASE UNIT** (normal erase mode)	Clear
ATA Cryptographic Key Reset	ATA SSD	**ATA SECURITY ERASE UNIT** (enhanced erase mode)	Clear
ATA Cryptographic Key Reset	ATA HDD	**ATA SECURITY ERASE UNIT** (enhanced erase mode)	Purge

Step 3

If the hard disk password has been set, you will be prompted to enter the password. If you enter the wrong password three times, ThinkShield Secure Wipe will be terminated.

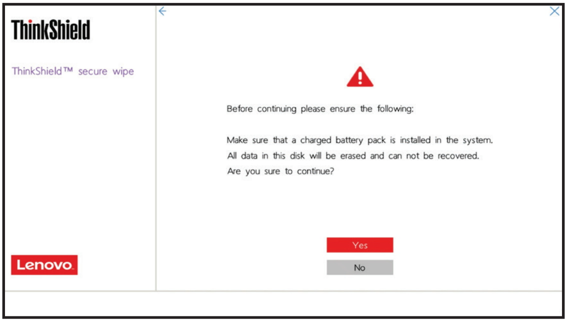


This disk was protected by OPAL Password.
Please input the OPAL Password to continue Erase.

Enter OPAL Password: [redacted]

Step 4

Once you choose the wipe-out method, the following warning message is displayed before proceeding to wipe out. Please carefully read it and ensure that power loss will not occur during the wipe-out process.

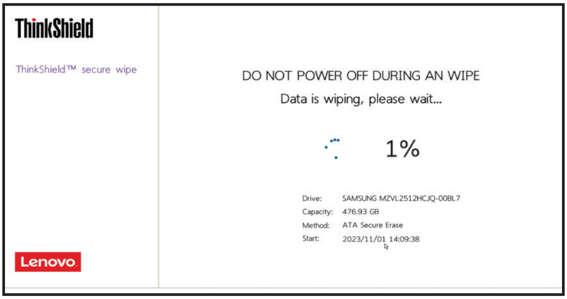


Before continuing please ensure the following:

Make sure that a charged battery pack is installed in the system.
All data in this disk will be erased and can not be recovered.
Are you sure to continue?

Step 5

If everything is OK, the ThinkShield Secure Wipe starts with the progress indication as below. Do not power off the system during the wipe. The time required to complete the secure wipe varies depending on the storage type, size, and wipe method.



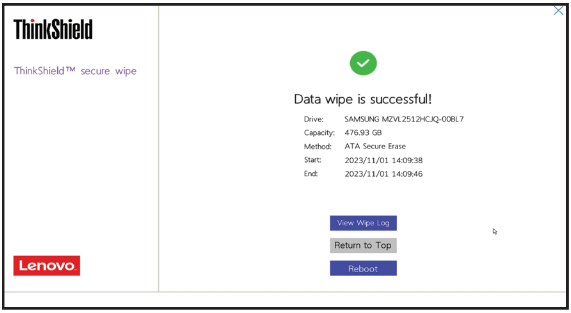
DO NOT POWER OFF DURING AN WIPE
Data is wiping, please wait...

1%

Drive: SAMSUNG MZVL2512HCJQ-00BL7
Capacity: 476.93 GB
Method: ATA Secure Erase
Start: 2023/11/01 14:09:38

Step 6

When the wipeout completes successfully, the following message appears with some information such as drive information, start time, and end time.



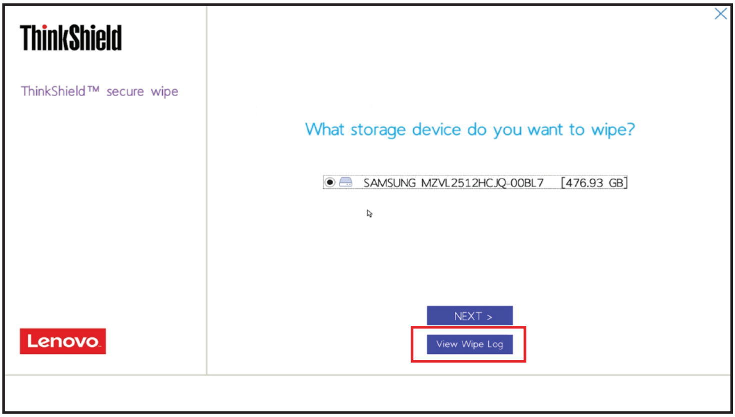
Data wipe is successful!

Drive: SAMSUNG MZVL2512HCJQ-00BL7
Capacity: 476.93 GB
Method: ATA Secure Erase
Start: 2023/11/01 14:09:38
End: 2023/11/01 14:09:46

Viewing The Wipe Log

In some series of products, it is possible to accumulate logs of wipe results and display detailed information. To view the log, select [View Wipe Log] on the storage selection screen after launching the ThinkShield Secure Wipe, or on the wipe completion screen.

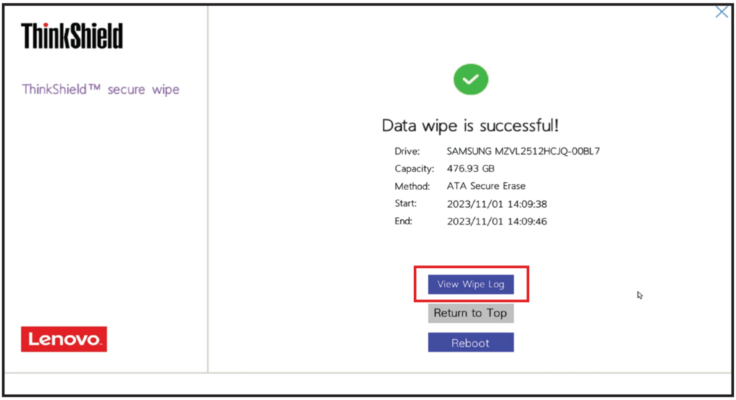
From the storage device selection screen right after involving the ThinkShield Secure Wipe



What storage device do you want to wipe?

● SAMSUNG MZVL2512HCJQ-00BL7 [476.93 GB]

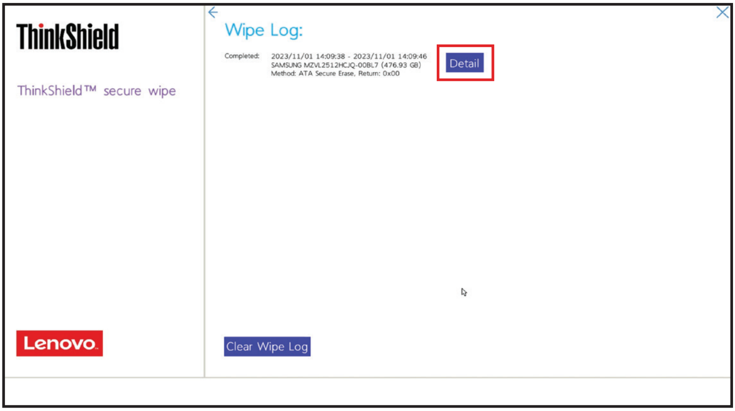
From the wipe completion screen



Data wipe is successful!

Drive: SAMSUNG MZVL2512HCJQ-00BL7
Capacity: 476.93 GB
Method: ATA Secure Erase
Start: 2023/11/01 14:09:38
End: 2023/11/01 14:09:46

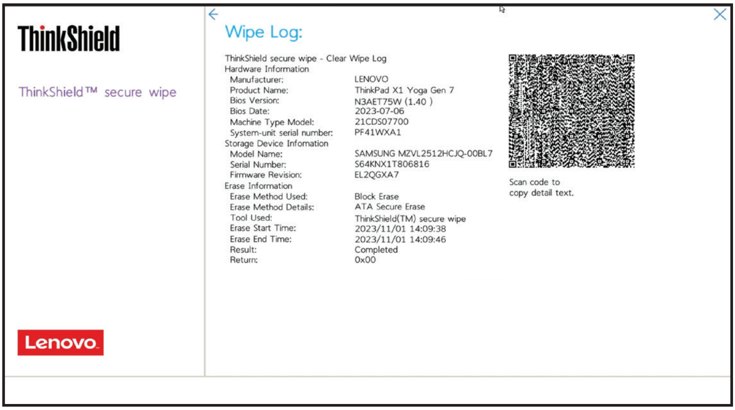
On the Wipe Log screen, accessible from the [View Wipe Log] button, you can view a list of wipe logs. In some product series, you can display detailed logs by clicking the [Detail] button shown on the right side of each row. Up to 10 logs are kept per device.



```
Completed:   2023/11/01 14:09:38 - 2023/11/01 14:09:46
             SAMSUNG MZVL2512HCJQ-00BL7 (476.93 GB)
             Method: ATA Secure Erase, Return: 0x00
```

If a Supervisor Password or System Management Password is set, entering the password is required to clear the wipe log (by pressing the [Clear Wipe Log] button at the bottom of the screen).

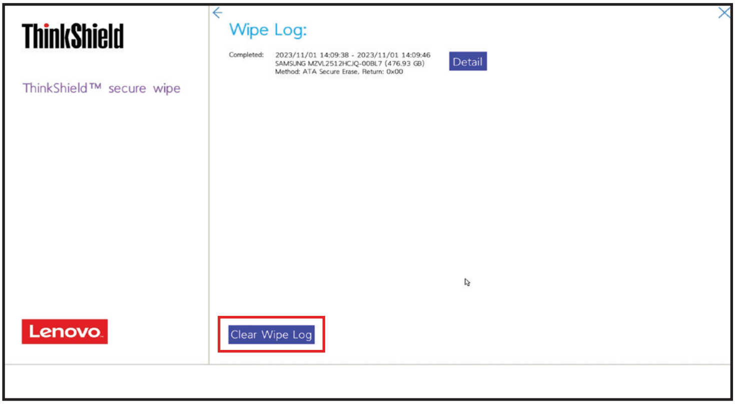
From the [Wipe Log] screen, you can view information such as the device's MTM (Machine Type and Model), serial number, storage device information, erase details including the erase method, and time. Additionally, in some product series, the log can be exported through a displayed QR code.



```
ThinkShield secure wipe - Clear Wipe Log
Hardware Information
  Manufacturer:                 LENOVO
  Product Name:                 ThinkPad X1 Yoga Gen 7
  Bios Version:                 N3AET75W (1.40 )
  Bios Date:                    2023-07-06
  Machine Type Model:           21CDS07700
  System-unit serial number:    PF41WXA1
Storage Device Infomation
  Model Name:                   SAMSUNG MZVL2512HCJQ-00BL7
  Serial Number:                S64KNX1T806816
  Firmware Revision:            EL2QGXA7
Erase Information
  Erase Method Used:            Block Erase
  Erase Method Details:         ATA Secure Erase
  Tool Used:                    ThinkShield(TM) secure wipe
  Erase Start Time:             2023/11/01 14:09:38
  Erase End Time:               2023/11/01 14:09:46
  Result:                       Completed
  Return:                       0x00
```

Clearing The Wipe Log

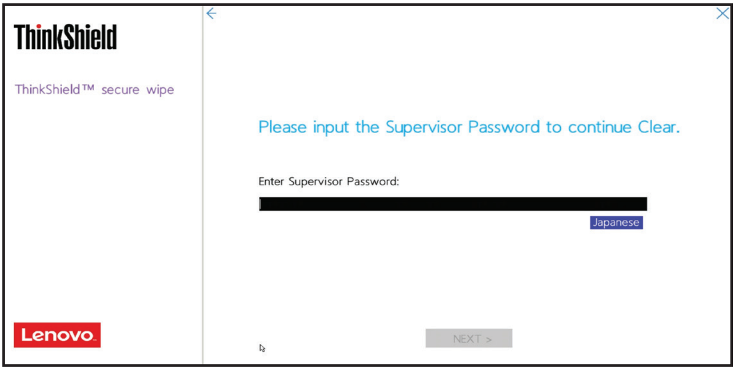
Click the [Clear Wipe Log] button to clear the stored wipe logs.



Wipe Log:

Completed: 2023/11/01 14:09:38 - 2023/11/01 14:09:46
SAMSUNG MZVL2512HCJQ-00BL7 (476.93 GB)
Method: ATA Secure Erase, Return: 0x00

If Supervisor Password or System Management Password is set, password authentication is required to proceed.



Please input the Supervisor Password to continue Clear.

Enter Supervisor Password:

Wipe Log Format

Category	Item	Information Displayed
Hardware Information	Manufacture	LENOVO
	Product Name	Example: ThinkPad X1 Yoga Gen 7
	BIOS Version	Example: N3AET75W (1.40)
	BIOS Date	YYYY-MM-DD
	Machine Type Model	XXXXXXXXXX
	System-Unit Serial Number	XXXXXXXX
Storage Device Information	Model Name	Identify Device Word27-46 (40 bytes) (SATA) Identify Device Byte 24-63 (20 bytes) (NVMe)
	Serial Number	Identify Device Word10-19 (20 bytes) (SATA) Identify Device Byte 4-23 (40 bytes) (NVMe)
	Firmware Revision	Identify Device Word23-26 (8 bytes) (SATA) Identify Device Byte 64-71 (8 bytes) (NVMe)
Erase Information	Erase Method Used	Erase Method
	Erase Method Details	Erase Method Detail
	Tool Used	ThinkShield(TM) secure wipe
	Erase Start Time	YYYY/MM/DDHH:MM:SS
	Erase End Time	YYYY/MM/DDHH:MM:SS
	Result	Completed/Incompleted/Failed
	Return	EFI Return Code

Sample of Wipe Log Read Through QR Code

```
ThinkShield secure wipe - Clear Wipe Log
Hardware Information
Manufacturer:LENOVO
Product Name:ThinkPad X1 Yoga Gen 7
Bios Version:N3AET75W (1.40 )
Bios Date:2023-07-06
Machine Type Model:21CDS07CTO
System-unit serial number:PF4ZZZZZ
Storage Device Infomation
Model Name:SAMSUNG MZVL2512HCJQ-00BL7
Serial Number:S64KNX1T00000
Firmware Revision:EL2QGXA7
Erase Information
Erase Method Used:Block Erase
Erase Method Details:ATA Secure Erase
Tool Used:ThinkShield(TM) secure wipe
Erase Start Time:2023/11/01 14:09:38
Erase End Time:2023/11/01 14:09:46
Result:Completed
Return:0x00
```

Performing ThinkShield Secure Wipe by WMI

Note

When performing the ThinkShield Secure Wipe with WMI (Windows Management Instrumentation), it is necessary to pre-set either a Supervisor Password, System Management Password, or Hard Disk Password. If none of these are set, the ThinkShield Secure Wipe cannot be executed with WMI commands.

Additionally, when executing a secure wipe remotely via WMI, user authentication is required. There are also erasure methods, such as TCG Opal PSID Revert, that cannot be executed remotely.

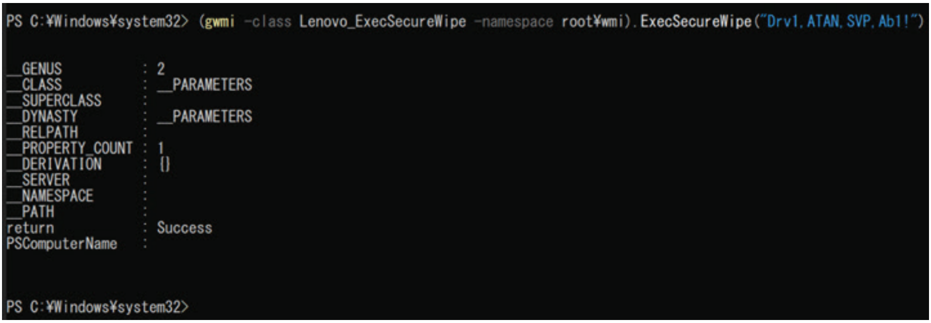
After issuing a ThinkShield Secure Wipe via WMI command, it will be performed at the next boot of the PC.

After executing a ThinkShield Secure Wipe via WMI, the operating system will also be erased, resulting in the inability to connect to the internet. Therefore, it is not possible to send back the execution results.

WMI Command

(gwmi -class Lenovo_ExecSecureWipe -namespace root\wmi).ExecSecureWipe(“Target drive,Erase method,
Password type,Password”)

Example



```
PS C:¥Windows¥system32> (gwmi -class Lenovo_ExecSecureWipe -namespace root¥wmi).ExecSecureWipe("Drv1,ATAN,SVP,Ab1!")


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
return           : Success
PSComputerName   :



PS C:¥Windows¥system32>
```

Parameters Of The WMI Command

ITem	Parameter	Note
Target Drive	Drv1	
	Drv2	
	Drv3	
	...	
Erase Method	ATAN	ATA Secure Erase (Recommended)
	ATAC	ATA Cryptographic Key Reset (Recommended)
	DOD	US DoD 5520.22-M
	SPZ	Single Pass Zeros
	USNAF	US Navy & Air Force
	CCI6	CSE Canada ITSG-06
	BHI5	British HMB Infosec Standard 5, Enhanced
	GV	German VSITR
	RGP1	Russian GOST P50739-95 Level 1
	RGP4	Russian GOST P50739-95 Level 4
	RTOII	RCMP TSSIT OPS-II
	OPALPASS	TCG Opal Revert to Factory Default
	NVMEC	Erase NVMe Cryptographic Keys
	NVMEU	Erase all NVMe User Space
Password Type	SVP	Supervisor Password
	SMP	System Management Password
	UHDP	User Hard Disk Password
	MHDP	Master Hard Disk Password
	UDRP	User Password
	ADRP	Admin Password

Appendix: Legacy Wipe Methods

Legacy Wipe

The legacy wipe method is executed by the software using a standard write command. According to the definition of the erase algorithm, defined data is written to all sectors for defined times. Note that this method may not wipe out all data, even when writing to all sectors from LBA 0 to max LBA, because some physical sectors may not be mapped to logical sectors due to wear leveling. The completion time varies according to the storage capacity and the algorithm.

Use of the legacy methods is not recommended as it does not guarantee to fully erase all the data of a modern drive, and you use it at your own risk.

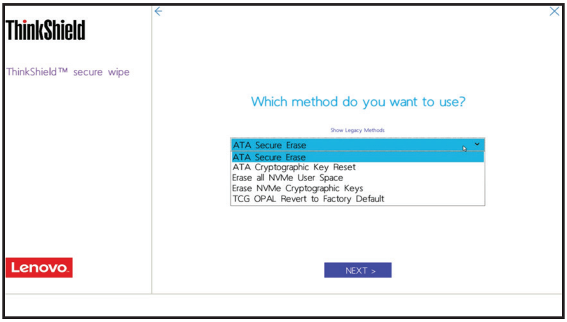
List of the Legacy Wipe Methods

Following table shows the list of the supported legacy wipe methods. Note that supporting legacy wipe methods may be terminated without notice.

Feature Set	Erase method	Erase Method Details
ATA	Overwrite	US DOD 5520.22M
ATA	Overwrite	Single Pass Zeros
ATA	Overwrite	US Navy & Air Force
ATA	Overwrite	CSE Canada ITSG06
ATA	Overwrite	British HMB Infosecs Standard 5, Enhanced
ATA	Overwrite	German VSITR
ATA	Overwrite	Russian GOST P50739 Level 1
ATA	Overwrite	Russian GOST P50739 Level 4
ATA	Overwrite	RCMP TSSIT OPSII

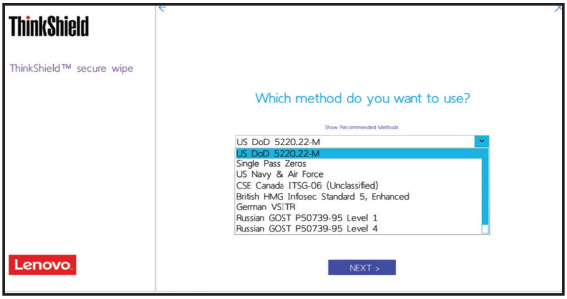
Using Legacy Wipe Out Methods

By clicking the ‘Show Legacy Methods’ button, you are navigated to see the list of legacy wipe methods. It flips back to the secure wipe methods by clicking the ‘Show Recommended Method’ button.


ThinkShield
ThinkShield™ secure wipe
Lenovo
Show Legacy Methods
ATA Secure Erase
ATA Secure Erase
ATA Cryptographic Key Reset
Erase all NVMe User Space
Erase NVMe Cryptographic Keys
TCG OPAL Revert to Factory Default
NEXT >

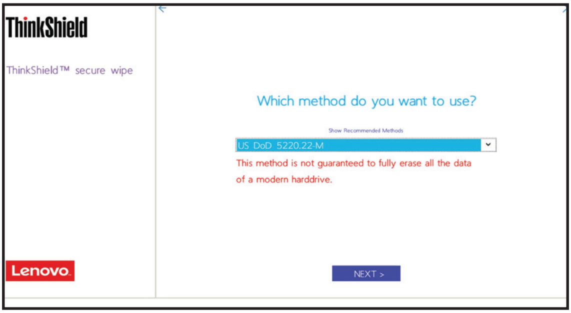
Which method do you want to use?

Choose one of the legacy method you prefer to use.



Which method do you want to use?

If the legacy method is selected, a warning message is displayed.
Use of the legacy methods is not recommended as it does not guarantee to fully erase all the data of a modern drive, and you use it at your own risk.



Which method do you want to use?

This method is not guaranteed to fully erase all the data of a modern harddrive.

Contact one of our business experts and tell us about your challenges and goals.

We'll work together to customize a technology package tailored to your business.

The information in this document is as of February29, 2024.
The implementation of features varies depending on the product series and model.
Changes may be made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice. Any performance data contained herein was determined in a controlled environment; therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems, and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment. Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Lenovo, the Lenovo logo, ThinkSystem, are trademarks of Lenovo in the United States, other countries, or both.

Smarter
technology
for all

Lenovo