Table of Contents

1. Introduction ................................................................................................................................. 1

2. Installing the SanDisk Crypto Erase Tool.................................................................................... 2
   System Pre-requisites .................................................................................................................. 2
   Supported Operating Systems .................................................................................................... 2
   Supported Drives ....................................................................................................................... 2
   Procedure .................................................................................................................................. 2

3. Crypto Erase on a Secondary SSD ............................................................................................... 4

4. Crypto Erase on a Primary SSD ................................................................................................... 8

5. Getting Help ............................................................................................................................... 12

6. FAQs .......................................................................................................................................... 13
List of Pictures

Figure 1: Launch the Crypto Erase installer ................................................................. 2
Figure 2: Verify installation settings .............................................................................. 3
Figure 3: Crypto Erase successfully installed on the system ........................................... 3
Figure 4: Crypto Erase for secondary SanDisk SSD ...................................................... 4
Figure 5: Crypto Erase disabled for an OPAL-deactivated SSD ..................................... 5
Figure 6: PSID entry for performing Crypto Erase .......................................................... 5
Figure 7: Warning message before Crypto Erase ........................................................... 6
Figure 8: Successful Crypto Erase on a secondary SSD ................................................ 7
Figure 9: Drive in uninitialized state after a successful crypto erase .............................. 7
Figure 10: Crypto Erase for a Primary Drive using a bootable USB ............................... 8
Figure 11: Warning to backup contents of USB .............................................................. 9
Figure 12: Bootable crypto erase USB drive successfully created ................................. 9
Figure 13: Crypto Erase USB lists all connected secure drives at boot-up ...................... 10
Figure 14: Entering PSID of selected drive ................................................................... 10
Figure 15: Successful Crypto erase using bootable USB method ................................. 11
Figure 16: Get help for Crypto Erase tool ..................................................................... 12
Figure 17: About page of Crypto Erase tool ................................................................. 12
1. **Introduction**

The SanDisk Crypto Erase tool is a Windows application, which can be used to revert an OPAL-activated or eDrive-activated SanDisk SSD back to its factory default state. After a Crypto Erase, all security keys will be deleted; therefore, user data will be destroyed. Also, OPAL or eDrive will be deactivated, and the drive can then be reused with any compatible security application. Crypto Erase is only supported on security enabled SSDs. The drive's unique Physical Security ID (PSID), which is printed on the drive's label, is required to perform a Crypto Erase. The Crypto Erase process is often referred to as a PSID Revert.

**Note:** It is not possible to perform a Crypto Erase on an SSD which does not have OPAL or eDrive activated on it.

The SanDisk Crypto Erase tool can perform a Crypto Erase on primary as well as secondary SSDs. Secondary SSDs can easily be erased using the Windows GUI by selecting the SSD and providing the correct PSID. For primary SSDs, a bootable USB drive must be created, which can then be used as the boot drive on the target system. For detailed instructions, please refer to Section 4: [Crypto Erase on a Primary SSD](#).
2. Installing the SanDisk Crypto Erase Tool

System Pre-requisites

The SanDisk Crypto Erase tool is a Windows application. It can be installed on 32 or 64 bit Windows 7, 8, or 8.1 environments. For systems that have SanDisk secure SSDs installed in them but are not running Windows, please use the bootable USB drive method (as described in section 4: Crypto Erase on a Primary SSD) to perform Crypto Erase on the SSDs.

Supported Operating Systems

- Windows 7 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows 8.1 (32/64 bit)

Supported Drives

- SanDisk Self-Encrypting Drives (SED)

Procedure

The SanDisk Crypto Erase download consists of a Windows installer. This installer can be used to install the Crypto Erase tool on target systems that meet the system pre-requisites outlined above. To install the tool, please follow the instructions below.

1. Download and save the SanDisk Crypto Erase installer (CryptoEraseSetup.exe) in a folder or directory on the target system.
2. Double click on the CryptoEraseSetup.exe file to launch the installer. Administrator rights will be required to perform this step. Click Next to continue.

Figure 1: Launch the Crypto Erase installer
3. Verify the installation settings, and click on Install to begin installation.

![Verify installation settings](image)

**Figure 2: Verify installation settings**

4. Click on Finish to complete installation.

![Finish](image)

**Figure 3: Crypto Erase successfully installed on the system**
3. **Crypto Erase on a Secondary SSD**

Any drive that is not the primary boot drive of that system is referred to as a secondary drive. The SanDisk Crypto Erase tool can be installed on a system whose primary operating system is Windows and contains secondary SSDs which need to be erased. The procedure for performing the crypto erase is outlined below:

1. Install the Crypto Erase tool on the desired system. (See Section 2: [Installing the Crypto Erase Tool](#) for detailed instructions.)
2. Launch the Crypto Erase tool.
3. The tool will scan the system and list all detected secure SanDisk SSDs in the left panel. If an SSD is not listed, click on the Refresh icon to rescan the system. If a Refresh fails to detect the SSD, check the SATA connection, and try again.

![List of SanDisk secure SSDs](image)

**Figure 4:** Crypto Erase for secondary SanDisk SSD

4. Choose the drive that needs to be erased by clicking on the drive name.
5. Details about the drive will be shown on the right panel. Crypto Erase is only allowed on SSDs in an *Activated* (security) state, i.e., on SSDs which have OPAL or eDrive enabled on them. If the drive’s Security State is *Deactivated*, Crypto Erase will be disabled for it.

![Figure 5: Crypto Erase disabled for an OPAL-deactivated SSD](image)

6. Confirm that the selected drive is correct, and provide the PSID in the boxes provided. The PSID can be found on the drive’s label as a 32-character string and a 2D barcode. **Note:** The PSID can only be alphanumeric. Special characters will be rejected.

![Figure 6: PSID entry for performing Crypto Erase](image)
7. Confirm the PSID typed into the boxes. If any errors are detected in the typed PSID, use the Clear All button to clear the PSID boxes and start again.

8. If the PSID is correct, continue with the Crypto Erase, by clicking on the Erase Now button.

9. **Warning**: All user data will be destroyed after a Crypto Erase. To initiate Crypto Erase on the selected drive, accept the warning by clicking Yes on the pop-up. Clicking No will cancel the Crypto Erase on the SSD.

![Figure 7: Warning message before Crypto Erase](image-url)
10. After a successful Crypto Erase, the SSD security state will change to *Deactivated*, and all user data will be destroyed. The drive will be in an uninitialized state and will need to be initialized and reformatted for reuse.

![Figure 8: Successful Crypto Erase on a secondary SSD](image)

![Figure 9: Drive in uninitialized state after a successful crypto erase](image)
4. **Crypto Erase on a Primary SSD**

To erase a primary boot drive or to perform a Crypto Erase on non-Windows systems, a Crypto Erase bootable USB drive must be created. The USB drive will contain a bootable Linux kernel with the Crypto Erase utility installed on it. The system can be booted to this USB drive to perform Crypto Erase on the target SSD(s). To create a bootable Crypto Erase USB drive and use it to perform Crypto Erase on SanDisk SSDs, please follow these steps:

1. Install the Crypto Erase tool on any compatible Windows system. (See Section 2: [Installing Crypto Erase Tool](#) for detailed instructions.)
2. Launch the Crypto Erase tool.
3. Click on the **Create Crypto Erase Bootable USB Drive** button.
4. The tool will scan the system and display a list of available USB drives. If the desired USB drive is not shown on the list, unplug and re-plug in the USB drive, then click on the refresh icon to see an updated list of USB drives.

![Crypto Erase Tool](image)

*Figure 10: Crypto Erase for a Primary Drive using a bootable USB*
5. Select the correct USB drive from the drop down list, and click on the Create Crypto Erase USB button to create a bootable Crypto Erase USB drive. **Note:** The USB must have at least 50MB of free space to perform this operation. If enough free space is not available, the contents of the USB may be deleted. To prevent loss of data, it is recommended to backup the contents of the USB drive before proceeding.

![Image of the Crypto Erase Tool with a warning message]

**Figure 11: Warning to backup contents of USB**

6. The tool will display a confirmation when the bootable USB drive is ready to use.

![Image of the Crypto Erase Tool with a successful creation message]

**Figure 12: Bootable crypto erase USB drive successfully created**
7. Connect the bootable Crypto Erase USB drive to the target system.
8. If needed, change the boot priority in the BIOS settings on the target system to allow booting to USBs.
9. Boot the target system to the Crypto Erase USB.
10. The Crypto Erase Utility on the USB will launch automatically and display a list of all connected SanDisk secure SSDs.

![SanDisk Crypto Erase Utility 1.04](image)

`Crypto Erase is used to revert an OPAL- or eDrive-activated SanDisk SSD back to its factory default state. After a Crypto Erase, all security keys will be deactivated. Therefore, user data will be destroyed. Also, OPAL or eDrive will be and the drive can then be reused with any compatible security application. Crypto Erase is only supported on security-enabled SSDs. The drive’s unique Physical Security ID (PSID), which is printed on the drive’s label, is required to perform a Crypto Erase.

Warning: This utility will permanently erase all data on the selected drive. This data cannot be recovered.

```
/dev/sdb  SanDisk SSD X300s
Serial Number  Size  Security Protocols  Activation Status  Lock status
13389401458  512.10 GB  TCG OPAL,eDrive  Activated  Unlocked
```

Enter the Device Name (e.g. /dev/sda) : /dev/sdb

![Figure 13: Crypto Erase USB lists all connected secure drives at boot-up](image)

11. The utility will prompt to select the SSD for performing a Crypto Erase. Enter the name of the drive to select. (Drive name will be in the format /dev/sdX, where X can be a, b, c, etc.)

12. Enter the PSID of the selected drive. While entering the PSID, please ignore any spaces or hyphens, which may be printed on the label.

![Warning: This utility will permanently erase all data on the selected drive. This data cannot be recovered.](image)

```
/dev/sdb  SanDisk SSD X300s
Serial Number  Size  Security Protocols  Activation Status  Lock status
13389401458  512.10 GB  TCG OPAL,eDrive  Activated  Unlocked
```

Enter the Device Name (e.g. /dev/sda) : /dev/sdb

Crypto Erase for /dev/sdb

Please enter your PSID (please ignore any spaces printed in the PSID on the drive label): AAAAAAAAAAAAAAAAAA

Are you sure you want to continue (Y/N)?

![Figure 14: Entering PSID of selected drive](image)

13. Confirm the PSID, and hit Enter to issue a Crypto Erase to the selected SSD.

14. **Warning:** All user data will be destroyed after a Crypto Erase. To initiate the Crypto Erase, type Y or y at the prompt. Entering N or n will cancel the Crypto Erase on the SSD.

15. After a successful Crypto Erase, the SSD security state will change to *Deactivated*, and all user data will be destroyed. The drive will be in an uninitialized state and will need to be initialized and reformatted for reuse.
16. Repeat steps 10-14 for any other secure SanDisk SSDs in the system that need to be erased.

![Image of SSD serial number and activation status]

**Figure 15: Successful Crypto erase using bootable USB method**

17. The same USB can be used on any target platform to perform Crypto Erase on SanDisk secure SSDs.
5. Getting Help

The Options menu on the SanDisk Crypto Erase tool provides links for getting help for the tool. Selecting Help & Support from this menu will redirect the user to the help page of the SanDisk Crypto Erase tool. More information about the tool and SanDisk secure SSDs can be found there. The system must be connected to the Internet for this option to work.

Figure 16: Get help for Crypto Erase tool

More information about the tool such as application revision, legal disclaimers, etc... can be found on the About page.

Figure 17: About page of Crypto Erase tool
6. FAQs

1. **What is Crypto Erase?**
   Crypto Erase is the process of reverting an OPAL-activated or eDrive-activated SSD back to its factory default state. After a Crypto Erase, all security keys are deleted; therefore, user data is destroyed. Also, OPAL or eDrive is deactivated, so the drive can then be reused with any compatible security application. The drive’s unique Physical Security ID (PSID), which is printed on the drive’s label, is required to perform a Crypto Erase. This process is also referred to as PSID Revert.

2. **Can user data be recovered after a Crypto Erase?**
   No, user data is permanently destroyed after a Crypto Erase.

3. **Can I re-use the SSD after a Crypto Erase?**
   Yes, the SSD will return to a factory default state after a Crypto Erase. It can then be re-initialized and formatted like any other SSD. Any compatible security application can be used to re-activate OPAL or eDrive on the SSD after a Crypto Erase.

4. **Can I perform Crypto Erase on a non-secure SSD? What will happen if I run this application on a non-secure SSD or non-SanDisk SSD?**
   No, Crypto Erase is only supported on OPAL-activated or eDrive-activated SSDs. The application scans the local system and lists all security capable SanDisk SSDs. Crypto Erase will be disabled for SSDs that are security capable but are not OPAL-activated or eDrive-activated. To activate OPAL or eDrive on a security capable SSD, use a security application, such as Microsoft Bitlocker.

5. **When will I need to use the SanDisk Crypto Erase Tool?**
   The SanDisk Crypto Erase tool should be used for an OPAL-activated or eDrive-activated SanDisk SSD if the password has been forgotten or lost. It can also be used to wipe user data before returning a drive for an RMA.

6. **When should I use the “Create Crypto Erase Bootable USB Drive” option?**
   This option is typically used for performing Crypto Erase on a primary boot drive.

7. **Are there any size limitations for the USB, when choosing the “Create Crypto Erase Bootable USB Drive” option?**
   The minimum free-space requirement for the USB is 50MB. It must be formatted as a FAT/NTFS drive.

8. **What is a PSID? Where can I find it?**
   PSID stands for Physical Security ID. It is a unique 32-character alphanumeric identifier for security-capable SSDs, which is required for a Crypto Erase. It is printed on the drive’s label as both a 32-character string and a 2D barcode.
9. What is TCG OPAL?
   TCG stands for Trusted Computing Group. OPAL is a security specification, for storage devices, defined by TCG.

10. What is eDrive?
    eDrive is a security storage specification defined by Microsoft. It is based on the TCG OPAL and IEEE 1667 specifications.

11. What does the “Activated” or “Deactivated” status mean?
    An “Activated” SanDisk SSD refers to a security capable SSD which has OPAL or eDrive enabled on it. OPAL or eDrive may be enabled by security applications, such as Microsoft Bitlocker. When no security application has been used to enabled OPAL or eDrive on the SSD, it remains in a “Deactivated” state. A secure SSD will also get “Deactivated” after a Crypto Erase operation.

12. How do I know if my SSD is a secure drive?
    The SanDisk Crypto Erase tool will scan the local system and list all security capable SanDisk SSDs in the left panel. If your SSD is displayed in the list after the scan, it is a secure drive.

13. Why is my SSD not listed in this application?
    The SanDisk Crypto Erase tool will only list SanDisk secure SSDs. All other drives on the system will be ignored.

14. Will the Crypto Erase Tool work on any platform?
    The Crypto Erase tool is a Windows application. To perform an erase on other operating systems, it is recommended to use the “Create Crypto Erase Bootable USB Drive” option.