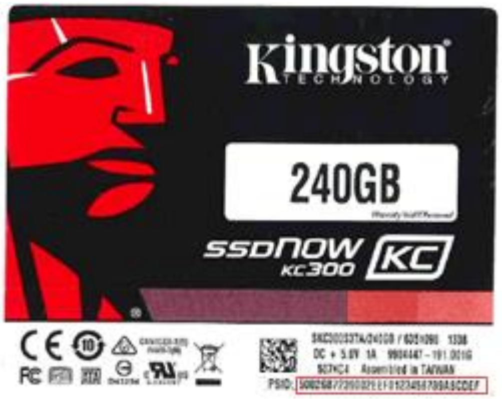
Intended for:

SKC300S37A/60G
SKC300S37A/120G
SKC300S37A/180G
SKC300S37A/240G
SKC300S37A/480G

Firmware Rev. 600ABBF0

The PSID Revert and the Enable/Disable IEEE1667 (or Microsoft eDrive) operations described in this document will only work on Kingston KC300 drives that support TCG Opal 2.0 and IEEE1667.

Please check the KC300 SSD label to ensure that it includes the 32-character PSID value (Older KC300 drives that do not include the PSID number do not support these features).



System Requirements

Platform

- PC with SATA II or SATA III interface
- Kingston SandForce-based SSD

OS Support

- Windows® 8, 8.1
- Windows® 7 (SP1)

System Preparation

- The SSD MUST be mounted as a secondary drive not as a boot drive
- You must be running Windows 8.1, 8, or 7 SP1 in AHCI mode in BIOS
- **Intel RST driver and AMD AHCI** users must switch to the standard Microsoft AHCI driver
- Use only native SATA ports for connecting the SSD

Contents:

Revert Utility

About

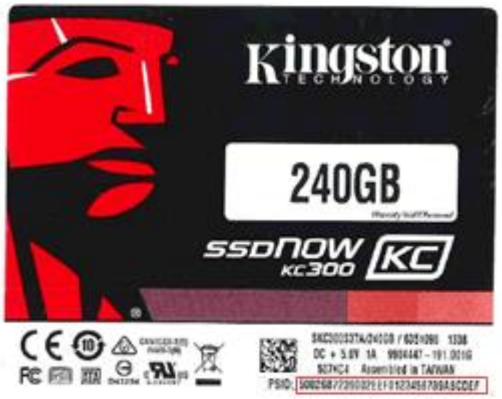
The Revert Utility is used when the KC300 SSD is in a locked state and it is unable to communicate with the system in order to unlock the drive and access the data. In this scenario, the Administrator must use the Revert Utility to reset the drive back to its factory state. In doing so, ALL DATA on the drive is lost and no data recovery can be completed; this is for security reasons and is normal behavior.

Getting Started

These instructions are designed to walk you through the revert procedure.

Step 1: Write Down the 32 Character PSID Value

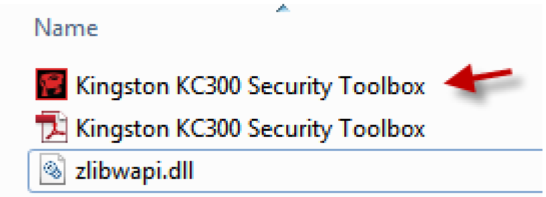
You can find this information on the SSD label.
See image provided.



Step 2: Launching the Utility

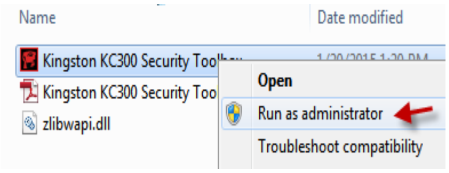
First, locate your download, double-click the zip file then extract it to your preferred location.

You will see the security toolbox, the instructions in .pdf form and a .dll file.



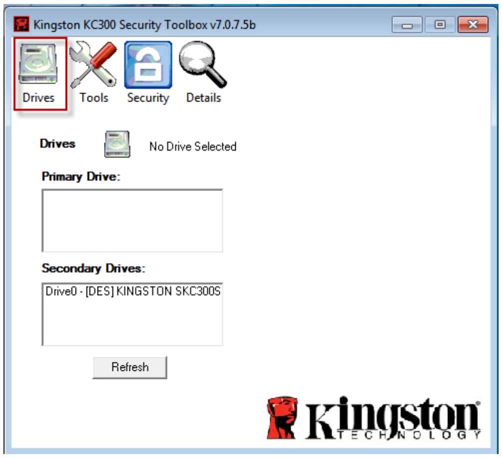
Name
Kingston KC300 Security Toolbox
Kingston KC300 Security Toolbox
zlibwapi.dll

If you are using Windows® 8 or 7 SP1 right click the Kingston KC300 Security Toolbox and select "Run as Administrator" to launch the application.


Name
Date modified
Kingston KC300 Security Toolbox
1/20/2015 1:20 PM
Kingston KC300 Security Too
zlibwapi.dll
Open
Run as administrator
Troubleshoot compatibility

The toolbox application interface will appear and default to the "Drives" window.

Note: If your drive does not appear within the window, confirm that you have adhered to the requirements located within the "System Preparation" section at the start of this document.



Drives: No Drive Selected

Primary Drive:

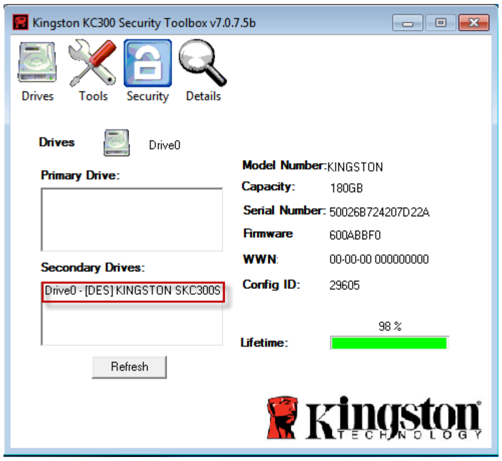
Secondary Drives: Drive0 - [DES] KINGSTON SKC300S

Step 3: Identifying your Secondary Drive to be Reverted

Select the drive you wish to Revert from "Secondary Drive".

Once you have selected the drive you wish to revert, the drive information including Model Number, Capacity, Serial Number, Firmware, WWN, and Config ID will appear on the right.

Note: If you attempt to Revert on your PRIMARY DRIVE, the utility will display a popup box stating, "Operation cannot be done on a primary drive."



Drives: Drive0

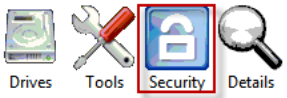
Primary Drive:

Secondary Drives: Drive0 - [DES] KINGSTON SKC300S

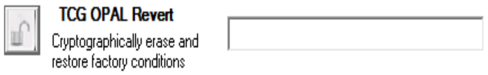
Model Number: KINGSTON
Capacity: 180GB
Serial Number: 50026B724207D22A
Firmware 600ABBF0
WWN: 00-00-00 000000000
Config ID: 29605
Lifetime: 98 %

Step 4: Selecting the "Security" Window and Reverting your SSD

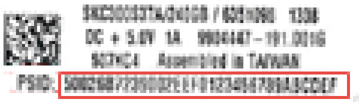
Select the "Security" tab located at the top of the application interface.



Proceed to the "TCG OPAL Revert" section. If you are ready to revert your drive, click in the box and type the 32-character value following the “PSID” label.



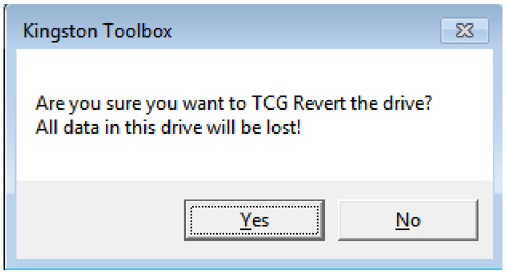
TCG OPAL Revert
Cryptographically erase and restore factory conditions



This is the value you should have written down in Step 1. Press the “Enter” key once you have entered in your PSID value.

Note: All data will be wiped from drive when the revert process completes.

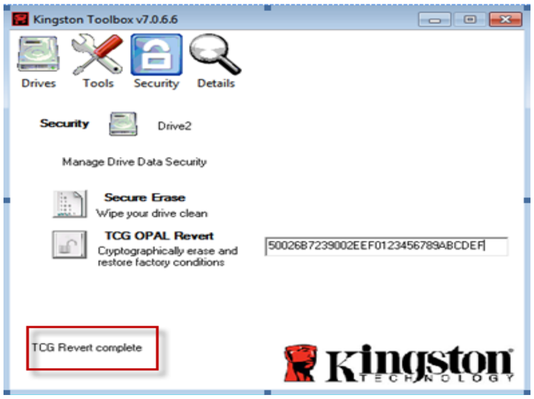
If you are ready to revert, click “Yes” to continue.



Kingston Toolbox

Are you sure you want to TCG Revert the drive?
All data in this drive will be lost!

When the revert is successful, "TCG Revert Complete" will appear in the lower left corner of the application window.



Kingston Toolbox v7.0.6.6

Security Drive2

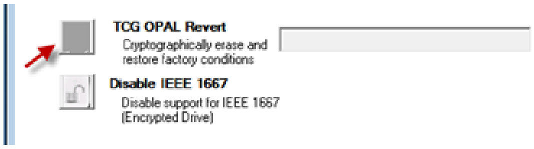
Manage Drive Data Security

Secure Erase
Wipe your drive clean

TCG OPAL Revert
Cryptographically erase and restore factory conditions
50026B7239002EEF0123456789ABCDEF

TCG Revert complete

If the TCG OPAL Revert screen is greyed out, it means the LockingEnabled flag is not active and you will not be able to perform a Revert.



TCG OPAL Revert
Cryptographically erase and restore factory conditions

Disable IEEE 1667
Disable support for IEEE 1667 (Encrypted Drive)

Note: The LockingEnabled flag is active when a drive has been authenticated by via 3rd party ISV (ex: Wave®, WinMagic®, McAfee® etc).

Enable/Disable IEEE1667

About

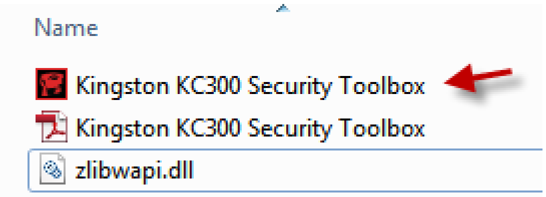
The Enable/Disable IEEE 1667 section will allow you to set the Word 69 bit to 0 or 1. “0” represents that it is set to Disable and “1” represents that it is set to Enable. If Enable is set, the LockingEnabled flag is automatically switched from “N” to “Y” during the fresh install of Windows 8, 8.1, or Server 2012 R2. This will prevent the drive from being managed or initialized with other 3rd party ISV (ex: Wave®, WinMagic®, McAfee® etc). It is to be used with Windows® eDrive (Bitlocker) during activation to utilize AES 256 Hardware Encryption Engine from the SSD controller to improve performance.

Getting Started

Step 1: Launching the Utility

First, locate your download, double-click the zip file , then extract it to your preferred location.

You will see the security toolbox, the instructions in .pdf form and a .dll file.



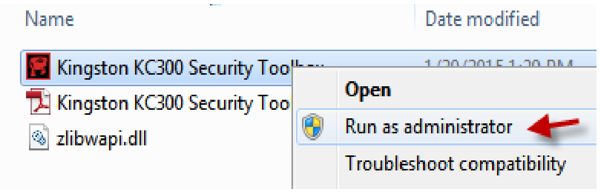
Name

Kingston KC300 Security Toolbox

Kingston KC300 Security Toolbox

zlibwapi.dll

If you are using Windows® 8 or 7 SP1 right click the Kingston KC300 Security Toolbox and select "Run as Administrator" to launch the application.



Name | Date modified

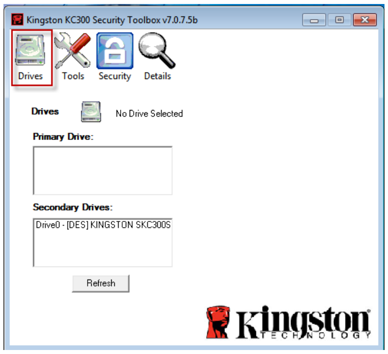
Kingston KC300 Security Too

Kingston KC300 Security Too

zlibwapi.dll

The toolbox application interface will appear and default to the "Drives" window.

Note: If your drive does not appear within the window, confirm that you have adhered to the requirements located within the "System Preparation" section at the start of this document.



Kingston KC300 Security Toolbox v7.0.7.5b

Drives No Drive Selected

Primary Drive:

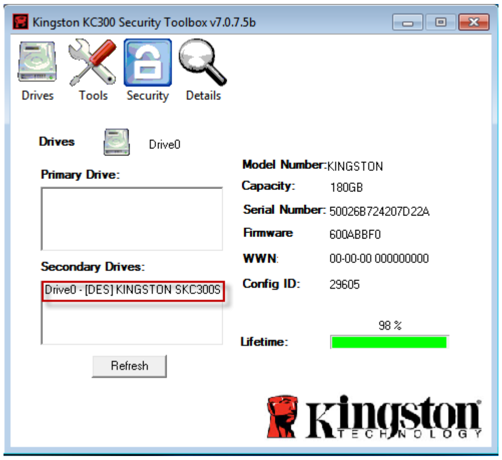
Secondary Drives:

Drive0 - [DES] KINGSTON SKC300S

Step 2: Identifying your Secondary Drive

Select the "Secondary Drive".

Once you have selected the drive, the drive information including Model Number, Capacity, Serial Number, Firmware, WWN, and Config ID will appear on the right.



Kingston KC300 Security Toolbox v7.0.7.5b

Drives Drive0

Primary Drive:

Secondary Drives:

Drive0 - [DES] KINGSTON SKC300S

Model Number: KINGSTON

Capacity: 180GB

Serial Number: 50026B724207D22A

Firmware 600ABBF0

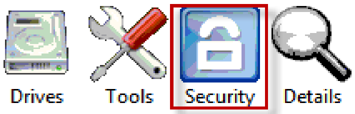
WWN 00-00-00 000000000

Config ID: 29605

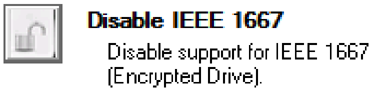
Lifetime: 98 %

Step 3: Selecting the “Security" Window

Select the "Security" tab located at the top of the application interface.



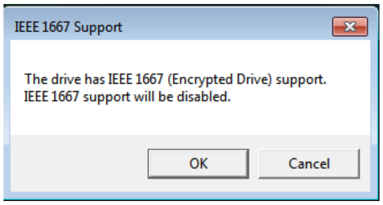
At the bottom of the screen, you will see a section for the Enable/Disable IEEE 1667. The following shows that it is currently Enabled. Click on the lock and you will be presented with the following screen.



Disable IEEE 1667

Disable support for IEEE 1667 (Encrypted Drive).

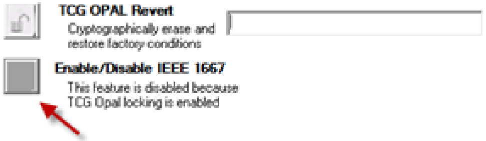
After selecting OK, the Word 69 bit will now be changed from “1” to “0”. To confirm this, proceed to Step 5.



IEEE 1667 Support

The drive has IEEE 1667 (Encrypted Drive) support.
IEEE 1667 support will be disabled.

Note: If the IEEE1667 box is greyed out, it means the Locking Enabled flag is active. You will need to perform a PSID Revert before attempting this process. To do this, please review the revert procedure at the top of this document.



TCG OPAL Revert

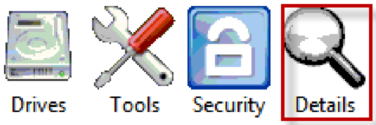
Cryptographically erase and restore factory conditions

Enable/Disable IEEE 1667

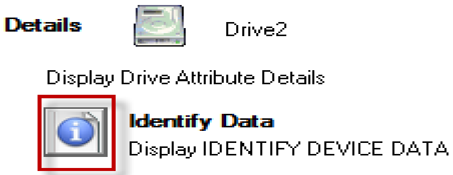
This feature is disabled because TCG Opal locking is enabled

Step 5: Selecting the Details Screen to Verify

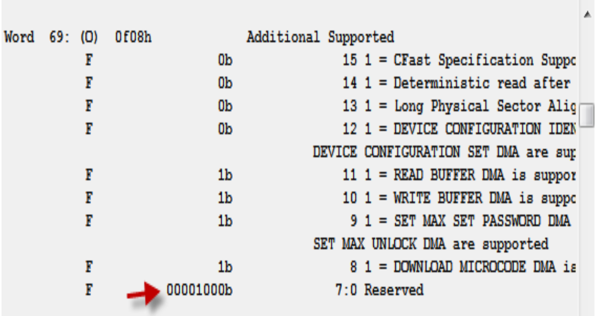
Select the "Details" tab located at the top of the application interface.



Click the “Identify Data” button as seen in the image and look for the following screen image below.



Scroll down to find Word 69. The first numerical value right of the red arrow (as depicted in the image) should show 0 for Disabled.



```
Word  69: (O)  0f08h          Additional Supported
          F            0b            15 1 = CFast Specification Suppc
          F            0b            14 1 = Deterministic read after
          F            0b            13 1 = Long Physical Sector Alig
          F            0b            12 1 = DEVICE CONFIGURATION IDEN
                                 DEVICE CONFIGURATION SET DMA are sup
          F            1b            11 1 = READ BUFFER DMA is suppor
          F            1b            10 1 = WRITE BUFFER DMA is suppc
          F            1b             9 1 = SET MAX SET PASSWORD DMA
                                 SET MAX UNLOCK DMA are supported
          F            1b             8 1 = DOWNLOAD MICROCODE DMA is
          F      00001000b          7:0 Reserved
```

For additional support information, please contact Kingston Technical Support @ http://www.kingston.com/support