Instant Secure Erase

Instant Secure Erase (ISE) is a feature on many Ultrastar HDDs & SSDs. The feature is included in newer capacity enterprise drives: Ultrastar® DC HC520 (12TB) and Ultrastar DC HC510 (10TB/8TB). It provides several benefits, and is available in both SATA and SAS configurations.

Drives with the ISE feature allow users to instantly erase the drive by using industry-standard commands and options. This feature is beneficial compared to the alternative of overwriting a drive with new data, which can take hours, especially for higher capacity hard drives.

Another benefit of using the new feature is that it can effectively erase both user accessible data, as well as potentially hidden user data that the drive maintains, but the user cannot easily access, such as re-allocated blocks, spare blocks, etc.

How Does Instant Secure Erase Work?

In order to securely erase the data, the drive first creates an internal cipher key that is used to cryptographically scramble (or unscramble) the data as it is written to (or read from) the disk. During normal drive operation, all data is scrambled (or unscrambled) using that internal key. When the operator uses Instant Secure Erase to wipe the drive clean, the HDD deletes the internal key, rendering all user data unreadable.

It is important to note that while Instant Secure Erase uses cryptographic techniques to securely erase data, it does not offer data encryption to protect data at rest.

Data Encryption

Western Digital offers comprehensive data encryption solutions on many Ultrastar SATA and SAS drives.

- Bulk Data Encryption (BDE) is offered as an option on some SATA HDDs.
- TCG Encryption (TCG) is offered as an option for SAS HDDs and SSDs.

Western Digital also offers FIPS 140–2 Level 2 validation, a U.S. government security standard which includes tamper-evidence protection, on certain TCG drive models (TCG-FIPS).

Neither Instant Secure Erase (ISE) nor Secure Erase (SE) drive models provide encryption, but ISE functionality is included on all BDE, TCG and TCG-FIPS HDDs and SSDs from Western Digital.

Implementation

Instant Secure Erase is Western Digital's implementation of the industry standard T10/T13 SANITIZE command. The host can determine if the feature is available in SATA drives by calling Identify Device to determine if the SANITIZE device feature set is supported, and what optional features are supported. With SAS drives, the Sanitize Service Action Codes can be used to determine features. Refer to the Ultrastar HDD and SSD OEM specification for specific bit/byte assignments.

The SANITIZE command supports three options:

1. Crypto Scramble (SATA)/ Crypto Erase (SAS)
2. Overwrite (for HDDs)
3. Block Erase (for SSDs)

Crypto Scramble/Erase uses cryptographic techniques to securely erase the drive.

- T13 SATA specification uses the term Crypto Scramble.
- T10 SAS specification uses the term Crypto Erase.

Both features are similar. To simplify things, both are used interchangeably in this document to describe the same feature. When the drive is SANITIZED (wiped clean) using the Crypto Erase option, the HDD deletes the internal key, rendering data unreadable.

Overwrite is a secondary erasure method for HDDs. It erases the drive by overwriting existing data with a bit pattern. This method erases the existing magnetic bits by overwriting them with new data. The host can provide a specific bit pattern to use for overwriting.

Block Erase is the secondary erasure method for SSDs. SSDs can be erased by performing a block erase, which "electrically" erases each block by using internal SSD functions.

In normal operation, the host can query the device to determine if SANITIZE is supported, and if so, which of the three options (Crypto Erase, Overwrite, Block Erase) are supported.

With ISE HDDs, both Crypto Erase and Overwrite are supported. Block Erase does not apply to HDDs.

With ISE SSDs, both Crypto Erase and Block Erase are supported. Overwrite does not apply to SSDs.

Secure Erase

Secure Erase (SE) is a subset of Instant Secure Erase, where the Crypto Erase option has been disabled. Thus, there is no longer an "instant" option. The SANITIZE command is still supported, but only with "Overwrite" or "Block Erase" options. The SE feature provides an advantage over a "manual overwrite" by ensuring that any current non-accessible user data areas are also overwritten.

Western Digital provides Instant Secure Erase (ISE) as a standard feature in many of our enterprise-class HDD and SSD products. Secure Erase (SE) drives provide an option for customers who do not want the Crypto Erase option, but still desire to support the SANITIZE Feature with Overwrite only (or Block Erase only for SSDs).

With SE HDDs, Overwrite is supported. With SE SSDs, Block Erase is supported.

More Information

For more information on the SANITIZE command, please refer to the OEM Specifications for the specific drive of interest.

OEM Specifications can be found on our website for the following products:

Ultrastar DC HC520
http://www.wdc.com/dc-hc520

Ultrastar DC HC510
http://www.wdc.com/dc-hc510

SATA: See manual sections titled "SANITIZE Device Feature Set". This section explains the command parameters as well as the state machine for various conditions that occur when using the SANITIZE command. Do not confuse "Instant Secure Erase" using the SANITIZE command (what we are describing in this document) with the similarly named "SECURITY ERASE Unit" which is part of the Security Mode Feature Set found on Ultrastar SATA HDDs & SSDs.

SAS: See sections titled "SANITIZE (48)"

Industry Standards

The T10/T13 technical committees define the SAS/SATA drive standards respectively, and the technical committees publish these specifications. The SANITIZE feature is one of the commands available within the specification. More information can be found at the links below:

www.T13.org (SATA)

www.t10.org (SAS)

Western Digital.

5601 Great Oaks Parkway
San Jose, CA 95119, USA
US (Toll-Free): 800.801.4618
International: 408.717.6000

www.westerndigital.com