USER GUIDE

Solidigm™ Storage Tool - GUI

September 2022

SOLIDIGM™

Revision History

Document Revision	Description	Revision Date
001	• Initial release for Software version 1.0	March 2022
002	• Added HMC Feature	September 2022

Contents

1   Introduction

1.1   About Solidigm™ Storage Tool

The Solidigm™ Storage Tool (SST) is available in two interface types:

- Command line interface (CLI) tool; available in Windows, Linux, and ESXi.
- Graphical user interface (GUI) tool; available in Windows.

This document focuses on usage of the GUI interface version.

The SST (GUI) is drive management software that enables you to view the following information for Intel®/Solidigm™ SSDs:

- View:
  - o   Drive Health
  - o   Estimated Life Remaining
  - o   SMART attributes (also available for non-Intel®/non-Solidigm™ SSDs)
  - o   Drive Details (also available for non-Intel/non-Solidigm™ SSDs)
  - o   View your system information and hardware configuration, such as central processing unit (CPU), chipset, controller name and driver versions
- Features:
  - o   Update the firmware on supported SSDs
  - o   Run Secure Erase on a secondary SSD
  - o   Run Quick and Full diagnostic scans to test the read and write functionality of an SSD

1.2   Using the Tool

The initial screen shows Summary of the drives attached to the system.

GUI is split into 3 panels.:

- Top panel lists Tool Name and Tool settings.
- Left Panel lists tasks (Feature) that can be performed by the tool.
- Right Panel lists drives in separate tiles.

Note: For Identify and Smart tasks, select the drive from Top right corner if the system as multiple drives.

To perform a task, select Feature from left panel, select desired drive tile from the right panel. View data/information or Perform tasks available for that tile.

Slim vertical bar on the left side of drive tile indicates status of the drive as follows:

- Green: No special attention is needed for this drive
- Yellow: Firmware Update is available for this drive
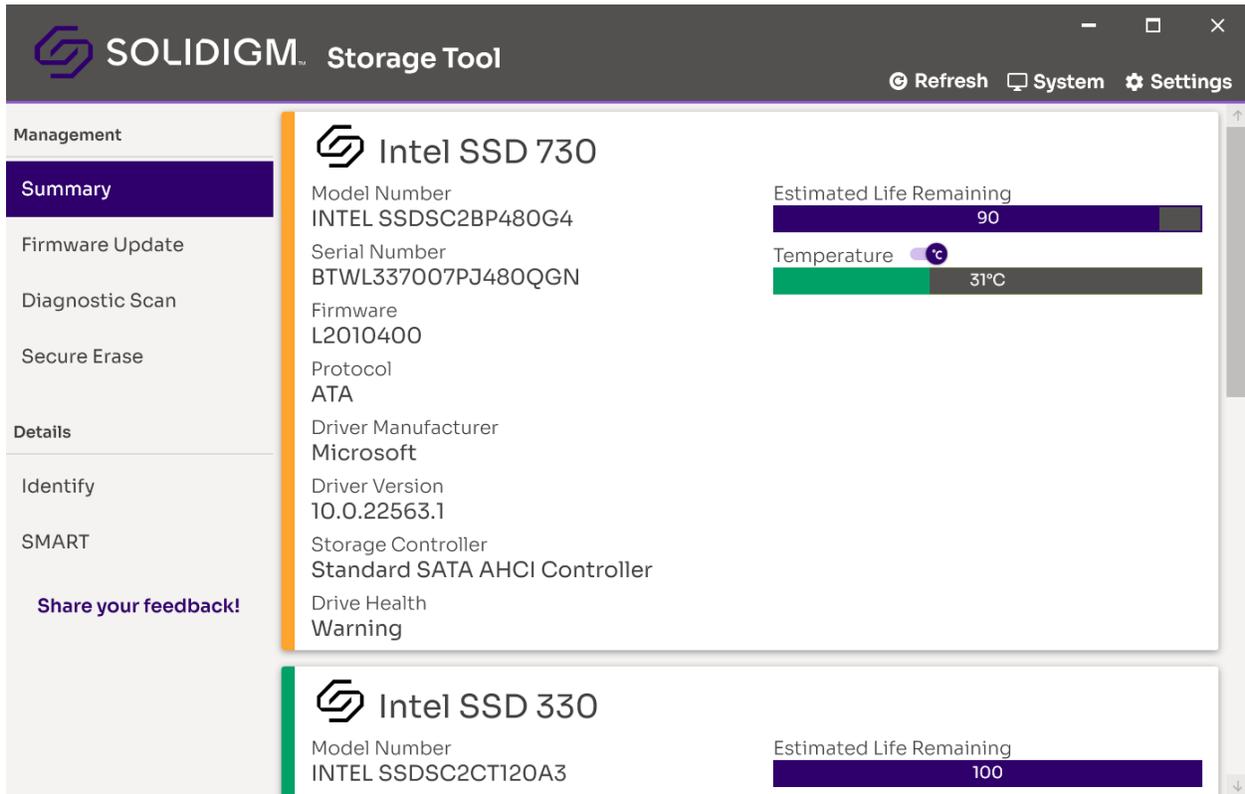
Summary page displaying drive tiles.

1.2.1   Drive Summary

Each summary tile will show the following information. Information varies depending on the device.

- Model Number
- Serial Number
- Firmware Version
- Protocol
- Driver Manufacturer
- Drive Capacity
- Drive Health
- Estimated Life Remaining
- Partitions

1.2.2   Feature Options

To run a task on the selected drive, select an option from the left panel. Then select the desired drive tile. (Available tasks vary depending on the type of drive.)

- Management:
  - Summary
  - Firmware Update
  - Diagnostic Scan
  - Secure Erase
  - LED Color
  - Performance Booster
- Details:
  - Identify
  - SMART

Related Sections

Scanning for Drives

Identifying a Drive

1.3   Drive List

Click the **Refresh** button to rescan for drives and refresh all information displayed in the Tool.

1.3.1   Scanning for Drives

Upon startup, the SST scans for all available devices installed in the system including Intel/Solidigm SSDs, non-Intel/non-Solidigm SSDs, and hard disk drives (HDDs). Icons for all located drives will appear on the home screen.

If your system contains multiple drives, a separate tile is displayed for each drive.

Select the **Refresh** button on the top section to rescan the system for devices or exit the tool by clicking the X in the upper-right corner and start the program again.

If an installed device does not appear on the home screen, see Troubleshooting Drives.

Related Sections

Identifying a Drive

Viewing Drive Health

Viewing Estimated Drive Life Remaining

1.3.2   Identifying a Drive

Left panel of the tool displays each drive that was recognized. Identify the drive with Product Family and Model Number.

Information displayed for a drive may include:

- Assigned drive letter (Drive partitions, and drives installed as cache devices, appear as separate drives and may contain assigned drive letters)

- Usable capacity

Note: The total usable capacity of an SSD may be less than the total physical capacity because a small portion of the capacity is used for NAND flash management and maintenance purposes.

If an installed drive does not appear on the home screen, see Troubleshooting – Drives.

Drives listed on Right Panel

Drive Summary containing partitions.

If a drive contains multiple partitions, partitions are displayed on a single tile. See example below:
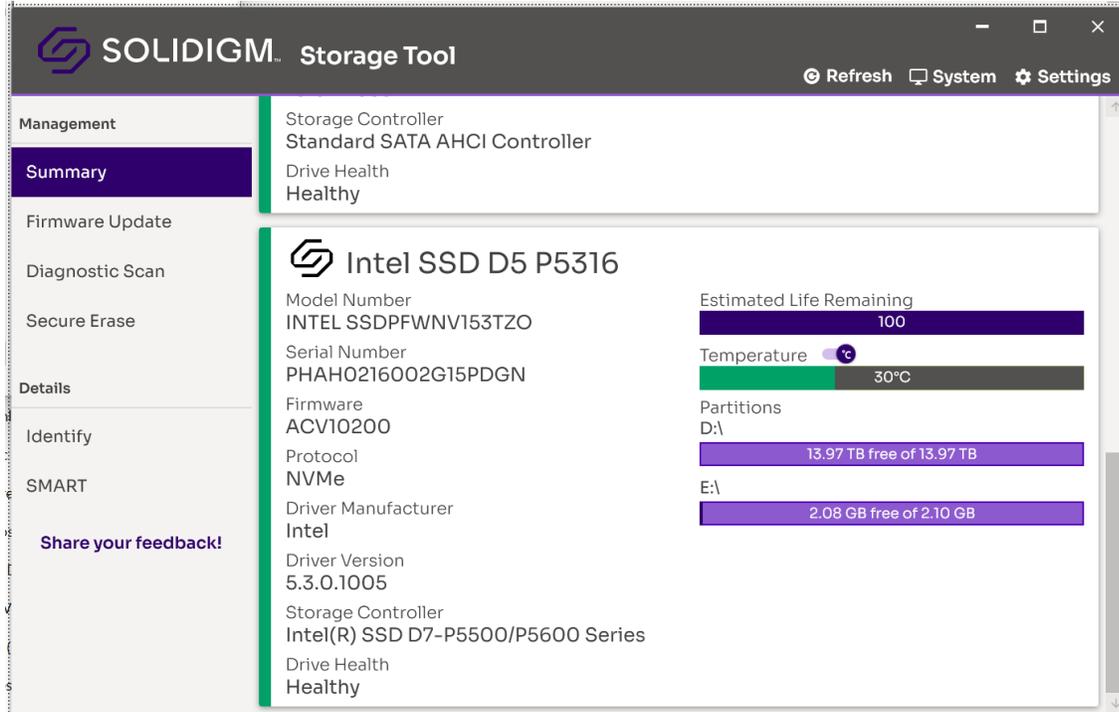
Additional Notes of Drives listings:

- Drives installed as cache devices using Intel® Rapid Storage Technology (Intel® RST)

- If a drive is installed as a cache device using Intel® RST, the drive appears as a separate drive on the home screen without an assigned drive letter. SST tool identifies this type of drive as a RAID volume member (a specific drive in a RAID volume).

- Drives part of a RAID array using Intel® RST

- If a drive is installed as part of a RAID array using Intel® RST, the drive appears as a separate drive on the home screen. Move the mouse over the drive to identify if it is the RAID volume (all drives in the RAID array) or a RAID volume member (a specific drive in a RAID volume).

Note: RAID volumes and RAID volume members have limited functionality in the Solidigm Storage Tool.

Drives part of dynamic partitions.

If a drive is part of a dynamic partition, the drive appears as a separate drive on the home screen.

Related Section

Identifying Security State of an SSD

§

2 Basic Drive Information: Summary

2.1 Model Information

Model information, such as device type, bus architecture, controller mode, form factor, and capacity is available for each drive on the home screen.

The model number, firmware version and the serial number are always displayed for the selected drive in the Drive Summary section.

2.2 Firmware Version

On the Summary screen, the Drive Summary section shows the version of firmware currently on each drive.

If the selected SSD contains an older version of firmware than what is included with this version of the SST Tool, "Update" button will appear next to the Firmware and vertical bar will be yellow next to the SSD.

To check if a newer firmware version is available for your SSD, see Checking for Firmware Updates.

Note: If you purchased your SSD from an OEM, your firmware version may have a different naming convention. The SST does not support updating firmware on OEM drives, contact your local OEM representative or support site for latest firmware revisions.

2.3 Serial Number

On the Summary screen, the Drive Summary section shows the Serial Number of the drive. This information can be useful when contacting technical support.

2.4 Drive Health

On the Summary screen, the drive health information of the SSD as measured by supported SMART attributes is displayed.

- Good (green) - All SMART attributes are above their threshold levels.

- Warning (orange-red) - One or more SMART attribute has moved beyond the threshold level and reached the final value. Solidigm recommends you back up all data and consider replacing the SSD.

- Critical (red) – A SMART critical warning has been triggered or the drive has encountered a critical error related to drive degradation. Solidigm recommends you back up all data and consider replacing the SSD.

Related Section

Viewing Estimated Life Remaining

2.5   Estimated Life Remaining

On the Summary screen, the Estimated Life Remaining of the selected SSD is displayed.

Endurance calculations are estimated and may vary. The estimation shown is based on the applied workload and is not accurate if the workload changes. Estimates are based on your usage to date and will not extend or reduce the SSD warranty period.

Estimated Life Remaining is reported for SSDs only with SMART enabled or with a SMART health log available.

Related Section

Viewing Drive Health

2.6   Drive Capacity

On the Summary screen, the capacity bar graph reports the amount of used and free space available on the SSD.

The capacity bar graph appears for SSDs with valid partitions only. The bar graph is empty for SSDs without a valid partition or for SSDs installed as a cache.

Note: The total usable capacity may be less than the total physical capacity because a small portion of the capacity is used for NAND flash management and maintenance purposes.

Related Sections

Viewing Drive Health

Viewing Estimated Life Remaining

§

3   Obtaining Drive, SMART, and System Information

Identify and SMART tabs allows the user to view and export (XML, JSON) the following details

- Identify Details
- SMART Details

Identify and Smart Details can also be exported to XML/JSON file. To export data, select the desired drive and click the export icon ⬛ on the top menu bar.

3.1   Drive Details: Identify

Click on Identify and select the appropriate drive from the drive list dropdown on top right corner. Identify information will show data for the selected drive.

Example of drive list dropdown (right side) on Identify Tab.

The Identify feature displays standard identification data for the drive. The information displayed is generated by an ATA IDENTIFY DEVICE or NVMe IDENTIFY command, depending on the attached drive.

Scroll down to view all values on the screen. Details shown for each value include:

- **Word**: Identifies the word(s) assigned to a specific value.
- **Description**: Provides the name and bit information (if needed) for each value.
- **Hex value**: Reports the hexadecimal value for each piece of drive information.

The following are commonly referenced values. For complete descriptions of all values, see the ATA specifications.

- **Serial Number** (Word 10-19): Identifies production information about the selected drive.
- **Firmware Version** (Word 23-26): Version of firmware installed on the selected drive.
- **Model Number** (Word 27-45): Model of the selected drive.

For SSDs, the model number contains reference to the NAND lithography.

- **Security Status** (Word 128): Security state of the selected drive.
    - Bit 0 indicates the Security Mode feature set supported. If set to one, security is supported.
    - Bit 1 indicates security enabled. If set to one, the security is enabled.
    - Bit 2 indicates security locked. If set to one, the security is locked.
    - Bit 3 indicates security frozen. If set to one, the security is frozen.

See the ATA-7 Specification or the NVMe 1.3 Specification for more information.

Note: To reissue the ATA IDENTIFY DEVICE or NVMe IDENTIFY command and display updated information for the drive, click the **refresh** ⟳ icon.

Related Sections

Exporting Drive Details

Reference Documents

3.1.1   Exporting Drive Details

To **Export** drive details for the drive to XML, JSON file, select the SSD, and click the export icon 📄 on the top menu bar.

Related Section

Viewing Drive Details

3.2   Drive Details: SMART Attributes

Click on Smart option on the left side and select the appropriate drive from the drive list dropdown on top right corner. Smart data will be displayed for the selected drive.
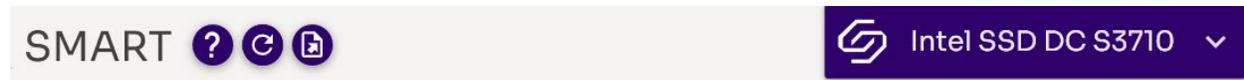
Example of drive list dropdown (right side) on Smart Tab.

The SMART Details screen shows Self-Monitoring, Analysis, and Reporting Technology (SMART) attributes and/or SMART Health Info attributes on the selected drive. Recommended actions (if any) appear next to each attribute.

Each drive operates under a predefined set of SMART attributes and corresponding threshold values, of which the drive should not pass during normal operation[1]. Each attribute has a *raw* value (defined by the manufacturer) and a *normalized* value[1]. See the ATA specifications and NVMe specifications for a complete description of each SMART attribute.

Scroll down to view the SMART attributes supported by the selected ATA or NVMe drive.

Details shown for each SMART attribute include:

- **ID:** The hexadecimal name of the SMART attribute.

- **Description:** The name of the SMART attribute.

- **Raw:** The raw value assigned to the SMART attribute by the drive manufacturer.

- **Normalized[1]:** The value of an attribute adjusted to a scale spanning typical increments of 100 to 1, or 200 to 1.

- **Threshold[1]:** The lowest acceptable normalized value for the drive.

- **Action:** Identifies whether the system can use the drive for processing.

Descriptions of some SMART attributes are shown in the following table. These attributes vary depending on the SSD or other drive selected. Your SSD or drive may not support some of these attributes. For more details on each attribute, see the ATA specifications and NVMe specifications.

Note: To reissue the ATA IDENTIFY DEVICE command or the NVMe IDENTIFY command and refresh the SMART information for the selected drive, click the **Refresh** button.

Note: 1. Threshold and Normalized values not applicable to NVMe drives unless defined in spec.

Please refer to SMART Attributes Lookup table for specific data.

3.2.1   Exporting SMART Attributes

To **Export** SMART Attributes for the drive to XML, JSON file, select the SSD, and click the export icon on the top menu bar

Related Sections

Viewing SMART Attributes

3.3   System Information

The System Information screen (found under System on top panel) shows details about your computer's operating system and hardware configuration, such as central processing unit (CPU), chipset, and controller name and driver version.

This information can be useful for troubleshooting purposes.

Related Sections

Viewing Drive Details

Viewing SMART Details

§

4   Updating Firmware

4.1   Checking for Firmware Updates

If the SSD contains an older version of firmware than the version included with this release of the SST Tool, Update button on the Summary page will be displayed.

Vertical bar will be yellow next to the drive tile that has outdated firmware.
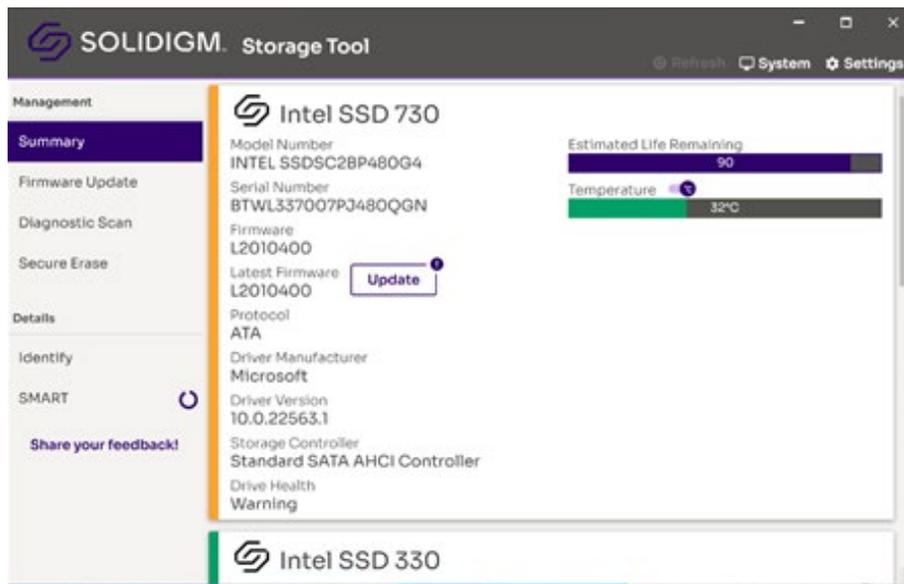
Summary tile indicating Update is available,
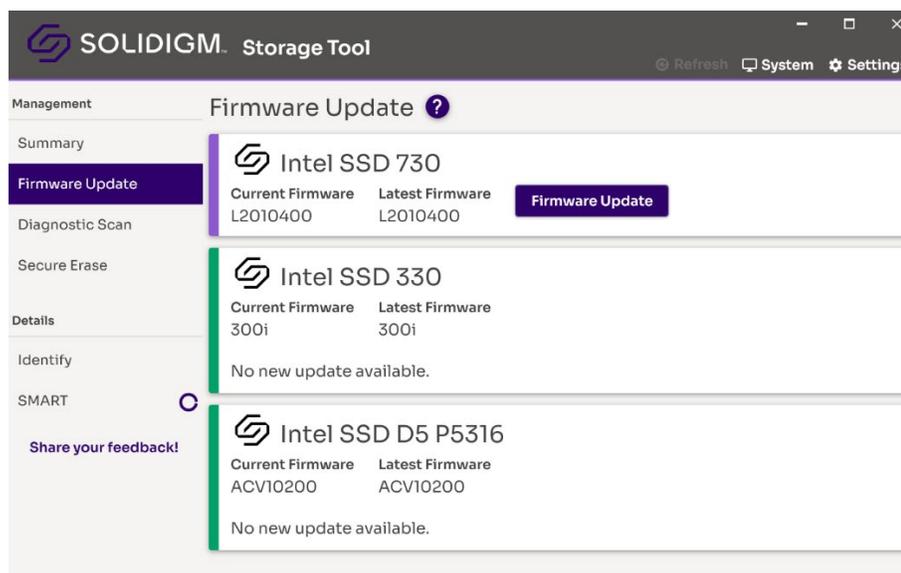
Firmware Update Tile indicating Firmware Update available

To manually check for a newer version:

1. Note the firmware version of the drive (on the Summary screen).

2. Select Firmware Update tab from left tab.

3. Click Check for Updates to open the Download Center to verify if there is a new version of the tool.

4. Confirm in the Release Notes or here for the latest firmware versions available for non-OEM Products.

5. Update the firmware following the instructions in Using Firmware Update.

Related Sections

Using Firmware Update

4.2   Using Firmware Update

The Firmware Update option updates the selected drive to the latest firmware available with this version of the tool.

Note: The firmware update functionality is not available if ATA Security is enabled on the selected SSD—whether it is locked or unlocked. Please ensure that ATA Security (also known as HDD or SSD Password) is disabled before proceeding. See your computer's documentation for instructions.

To update the firmware on supported SSD:

1. Back up the drive.

2. Perform a complete system backup on the drive to make sure no data is lost during the firmware update process. Solidigm is not responsible for any data loss that might occur during or after a firmware update on a drive.

3. Close all open applications except SST Tool.

4. Select **Firmware Update** tab from the left section.

5. Scroll to the drive you want to update.

6. Click **Firmware Update** to update the SSD with the firmware version included with this release of SST Tool. Minimize system use during this operation.

7. Reboot your system once the update is complete.

Related Sections

Checking for Firmware Updates

Troubleshooting – Firmware Update

§

5   Running Diagnostic Scans

5.1   Quick Diagnostic Scan

Run the Quick Diagnostic scan to test the basic functionality of the selected drive. The scan takes approximately three minutes to complete and performs two tests:

- Read Scan – checks 1.5 GB of the SSD for READ errors.

- Data Integrity Scan – creates 1 GB of random data, writes the data to unused areas of the SSD, and then compares it for data integrity *(Note: The Data Integrity Scan cannot be run on a Windows 8, Windows 8.1, Windows 10 or Windows Server 2012 Storage Space, nor on any individual SSD that is a member of a Storage Space)*.

The scan requires:

- A minimum of 5 GB of free space to run.

- A partitioned area to create and validate random data.

Note: Other tool options (such as the Summary screen or SMART Details screen) may be accessed while the scan is running, but no other tests (such as Full Diagnostic Scan) may be started.

1. Click **Run**.
2. View the progress on the screen.

To stop the scan, click **Cancel**.

5.2   Full Diagnostic Scan

Run the Full Diagnostic scan to perform an overall health evaluation on the selected drive.

The scan performs two tests:

- Read Scan – checks every logical block address (LBA) for READ errors.

- Data Integrity Scan – uses free space to write random data and read it back to ensure data integrity *(Note: The Data Integrity Scan cannot be run on a Windows 8, Windows 8.1, Windows 10 or Windows Server 2012 Storage Space, nor on any individual SSD that is a member of a Storage Space)*.

The scan can take an hour or more to complete (depending on the amount of free space on the SSD). The test can run in the background.

The scan requires:

- A minimum of 5 GB of free space to run.

- A partitioned area to create and validate random data.

Note: Other tool options (such as the Smart screen or SMART Details screen) may be accessed while the scan is running, but no other tests (such as Quick Diagnostic Scan) may be started.

1. Click **Run**.

2. View the progress on the screen.

To stop the scan, click Cancel.

6   Host Memory Cache

Host Memory Cache (HMC) feature is only available for selected drives. If the feature is supported, the feature tab will be show in left menu.
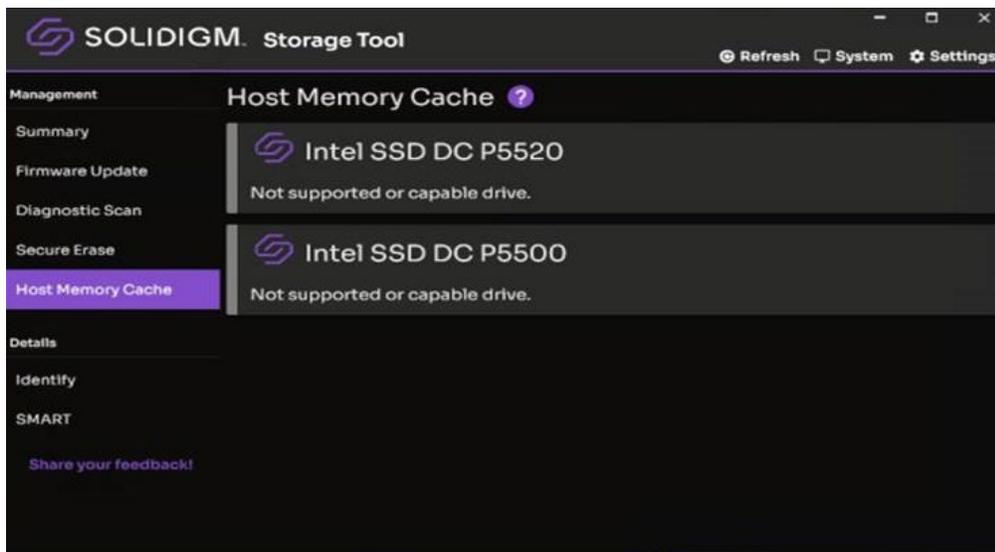
HMC feature requires supporting driver as well. When all conditions are met, Enable or Disable options will be available.

§

7   Tuning Your System

7.1   Tips for Optimizing Performance

Optimizer

Uses Microsoft Windows built in Optimizer service to optimize the drives

SST Tool provides shortcut to Windows Optimizer. Click on System->Optimizer.

Intel® Rapid Storage Technology (Intel® RST) Write Cache

For best performance, Solidigm recommends enabling Write Back cache in Intel® RST/Intel® Matrix Storage Manager console.

Superfetch/Prefetch

In Microsoft Windows 8 and newer, Superfetch functions differently than in previous versions of Windows, and should not be disabled for the SSD.

Device Initiated Power Management (DIPM)

For SSDs installed in mobile systems, DIPM is the most efficient power management method for managing SATA link power. With DIPM, link management is handled by the SSD (the SSD knows best how long a specific command might take to complete and is best equipped to request a link power management state change while processing the command). DIPM should be enabled on the SSDs for optimal performance.

Additionally, depending on your system configuration and operating system, perform these tasks to optimize performance:

- [Mobile systems with shock sensor](#)
- [SSDs in RAID Configurations Using Intel® Rapid Storage Technology Driver](#)
- [Mobile systems without Intel® Rapid Storage Technology or Intel® Matrix Storage Manager](#)

Related Sections

[Additional Tips for Optimizing Performance](#)

[Changing System Tuner Settings](#)

7.2   Additional Tips for Optimizing Performance

In addition to running the System Tuner, perform these tasks (depending on your system configuration and operating system) to optimize the performance of the SSD:

- [SSDs in RAID Configurations](#)
- [Mobile systems without Intel Rapid Storage Technology or Intel Matrix Storage Manager](#)

7.2.1 SSDs in RAID Configurations Using Intel® Rapid Storage Technology Driver

To obtain higher performance from RAID configurations consisting of SSDs and Intel® Rapid Storage Technology (Intel® RST), make sure Intel® RST Write Back Cache is enabled.

Note: Enabling Write Back Cache increases the chance of system data loss during a power-loss event. (However, all data written to the SSD will be committed to NAND during a power-loss event.) See your system documentation for information on enabling or disabling this feature.

7.2.2 Mobile Systems without Intel® Rapid Storage Technology or Intel® Matrix Storage Manager

To obtain higher performance on mobile systems with an SSD without Intel Rapid Storage Technology, enable DIPM (Device Initiated Power Management) on your mobile system. See your system documentation for instructions.

§

8   Performing a Secure Erase

8.1   About Secure Erase

Secure Erase permanently deletes all data on a SSD. To run Secure Erase, the SSD must be installed as a secondary SSD in your system.

⚠️ **CAUTION:** Secure Erase is an unrecoverable operation that permanently deletes all data on the SSD. Secure Erase eliminates not only the user data section of the SSD, but also the reserve data area, rendering data remnants virtually unrecoverable. Secure Erase is an addition to the existing *format drive* command available in computer operating systems. Once you run Secure Erase on an SSD, there is no possibility to recover data from the SSD.

On SSDs containing 25nm and later NAND Flash Memory, retired blocks are also erased.

- On SSDs supporting encryption, the encryption key used in randomizing data is re-generated after Secure Erase

- Secure Erase is blocked by the Windows 8.1, Windows 10, and Windows Server operating systems on SATA drives

- Secure Erase is not available if ATA Security is enabled on the selected SSD—whether it is locked or unlocked.

Related Sections

Secure Erase Requirements

Running Secure Erase

8.2   Secure Erase Requirements

- Secure Erase is blocked by the Windows 8.1, Windows 10 and Windows Server operating systems on SATA drives

To run Secure Erase on an SSD:

- Back up any data onto another drive if you want to keep any of the data on a SSD.

- The SSD must be the secondary drive in the system. Secure Erase cannot be run from a bootable SSD or on an SSD with a partition.

- All drive passwords (ATA Security) must be disabled for the SSD[8]. See your computer's documentation for instructions.

  o Some systems provide the ability to password-protect their drives. If your system has password protection enabled, the SSD may reject any requests from the host to update the firmware. Turn off the drive password protection prior to beginning the Firmware update process.

  o Although it varies from system to system, you can usually find the Drive Password Protection feature located in the BIOS. Consult your system documentation for the BIOS settings and passwords.

  o If you need help disabling the drive password protection feature, contact Customer Support.

- The system must allow access to the SATA power cable connected to the SSD.

- All partitions must be removed from the SSD.

- Back up any data onto another drive if you want to keep any of the data on the SSD.

Related Sections

Deleting a Partition

Running Secure Erase

8.3   Deleting a Partition

Follow the Operating System instructions on how to delete a partition on the SSD.

After deleting the partition, click **Refresh** on the SST tool home screen.

Related Sections

Running Secure Erase

8.4   Running Secure Erase

Run Secure Erase to permanently delete all data on a secondary SSD installed in your system.

⚠️ **CAUTION:** Secure Erase is an unrecoverable operation that permanently deletes all data on the SSD. Secure Erase eliminates not only the user data section of the SSD, but also the reserve data area, rendering data remnants virtually unrecoverable. Secure Erase is an addition to the existing *format drive* command available in computer operating systems. Once you run Secure Erase on the SSD, there is no possibility to recover data from the SSD.

1. Review the requirements before running Secure Erase.

2. Delete all partitions on the SSD to be erased.

3. Select the SSD on the home screen and view the Drive Summary information to verify the SSD is the drive you want to erase.

4. Select **Secure Erase** from left section

5. Click **Erase**.

If a Secure Frozen Warning message appears:

A Secure Frozen Warning message indicates the SSD is in the SECURITY FREEZE LOCK state. Secure Erase cannot be performed on an SSD when it is in this state. To prepare the SSD for the removal of the SECURITY FREEZE LOCK state, the SST tool sends the STANDBY IMMEDIATE command to the SSD, which results in the warning message.

To remove the SECURITY FREEZE LOCK state and continue with the Secure Erase process:

a. Power-cycle the SSD by removing the SATA power cable from the SSD and quickly reconnecting it while the tool is running. Depending on your system configuration, this may require that you physically remove the SSD from the system.

Note: Solidigm recommends performing this process quickly to make sure the system continues to recognize the SSD.

b. After unplugging and plugging in the SSD, click OK.

The tool rescans the system for the SSD. Once the SSD is detected, continue with Step 6.

If the SSD is not detected, click **OK** on the Selected Drive Not Found message. The tool home screen appears and scans the system for drives. Once the SSD is detected, select the SSD on the home screen and click **Secure Erase**.

If the Security warning message appears again, repeat the power-cycling process (steps a and b), making sure to quickly remove and reconnect the SATA power cable. If the Secure Frozen Warning message continues to appear, this indicates that power-cycling the drive is not removing the SECURITY FREEZE LOCK state on this system. If this is the case, the tool cannot run Secure Erase on this system. Solidigm recommends obtaining a drive utility with Secure Erase and running Secure Erase from that utility.

If the SSD is not detected and does not appear on the home screen, open the Windows Device Manager and rescan the system for drives (right-click the Windows Key and select **Device Manager**, then right-click **Disk Drives > Scan for hardware changes**).

After scanning the system, click **Refresh** on the SST tool and try the Secure Erase procedure again, making sure to quickly remove and reconnect the SATA power cable.

6. Click **Run**.

Secure Erase starts on the selected SSD. A progress bar shows the status of the operation. The process can take 1 to 2 minutes, depending on the capacity of the SSD.

⚠ **CAUTION:** Your system may appear to stop responding during this operation. Do not power off or disconnect power from your system during the operation, as this can damage the SSD.

7. When complete, create an active partition and format the SSD

8. Click **Refresh** on the home screen to view the SSD.

Related Sections

[Secure Erase Requirements](#)

§

9   Performance Booster Feature

9.1   Solid State QLC and Hybrid Drive

Solidigm™ QLC QLC-based SSDs, such as 660p series are equipped with a cache architecture to boost performance. This feature will move and clear the contents of the available cache and boost the performance of the SSD. The following section describes how to run performance boost feature.

Select the device connected to your system:

1. Select the Performance Booster tab from the left section.
2. Click the "Run" button.
3. If user decides to cancel, the progress bar will show the percentage of cache that's been cleared. For example, refer to the image below.
4. Once the entire cache is clear the progress bar should show 100 percent.

§

10   Troubleshooting

10.1 Troubleshooting – Drives

Drive does not appear on the home screen.

If a drive installed in the system does not appear on the home screen:

- Check power to the drive.

- For SATA drives, check the SATA cable connection and make sure the cable is properly connected to the drive and the host system.

- For NVMe drives, check that the drive is properly socketed in the CPU direct attached PCIe slot.

- Click **Refresh** on the home screen.

- Reboot the system and restart the SST Tool.

If the problem persists, contact Support.

SMART information does not appear for a selected drive.

If the SMART Details option is not available for a selected drive, make sure SMART is enabled on the drive.

Drive Health or Estimated Life Remaining does not appear for a selected drive.

Drive Health and Estimated Life Remaining information appears for SSDs only with SMART enabled.

10.2 Troubleshooting – Firmware Update

If you encounter an issue updating the firmware on the SSD or if the firmware update fails, use the bootable Firmware Update Tool.

NOTES:

- Firmware update for the Solidigm™ SSD 750 Series on Windows 7 and 8.1 requires the NVMe Drivers for Solidigm™ SSDs. For Windows 10, the Microsoft Native NVMe driver may be used.

- The Firmware Update option in the SST tool can be used to update the firmware on Supported SSDs only. All SSDs are supported except:

  o   Intel® X25-E Solid State Drive

  o   Intel® Solid State Drive 510 Series

For these SSDs, use the Firmware Update Tool mentioned above.

§

11 SMART Attributes Lookup table

Table of SMART Attribute IDs and their description.

ID	Attribute and Description (SATA)
03	**Spin Up Time** For SSDs, reports a fixed value of zero (0). The average time it takes the spindle to spin up. (Since an SSD has no moving parts, this attribute reports a fixed Raw value of zero (0) and a fixed Normalized value of 100.)
04	**Start/Stop Count** For SSDs, reports a fixed value of zero (0). This type of event is not an issue for SSDs. However, hard disk drives can experience only a finite number of these events, and therefore, must be tracked.
05	**Re-allocated Sector Count** The raw value shows the number of retired blocks since leaving the factory (grown defect count).
09	**Power-On Hours Count** The raw value reports the cumulative number of power-on hours over the life of the device. *Note:* The On/Off status of the Device Initiated Power Management (DIPM) feature affects the number of hours reported. • If DIPM is turned on, the recorded value does not include the time that the device is in a slumber state. • If DIPM is turned off, the recorded value should match the clock time, as all three device states are counted: active, idle, and slumber.
0C	**Power Cycle Count** The raw value reports the cumulative number of power-cycle events (power on/off cycles) over the life of the device.
AA	**Available Reserved Space** Reports the number of reserve blocks remaining. The normalized value begins at 100 (64h), which corresponds to 100 percent availability of the reserved space. The threshold value for this attribute is 10 percent availability.
AB	**Program Fail Count** The raw value shows total count of program fails. The normalized value, beginning at 100, shows the percent remaining of allowable program fails.

ID	Attribute and Description (SATA)
AC	**Erase Fail Count** The raw value shows total count of erase fail. The normalized value, beginning at 100, shows the percent remaining of allowable erase fails.
AE	**Unexpected Power Loss** Reports number of unclean shutdowns, cumulative over the life of the SSD. An "unclean shutdown" is the removal of power without STANDBY IMMEDIATE as the last command (regardless of PLI activity using capacitor power). Also known as "Power-off Retract Count" per magnetic-drive terminology.
B8	**End-to-End Error Detection Count** Reports number of errors encountered during Logical Block Address (LBA) tag checks within the SSD data path. The normalized value begins at 100 and decrements by 1 for each LBA tag mismatch detected. The threshold value is 90.
BB	**Uncorrectable Error Count** The raw value shows the count of errors that could not be recovered using Error Correction Code (ECC).
BE	**Temperature - Airflow (Case)** Reports the SSD case temperature in degree Celsius. The raw value is as follows: • Byte 0 = Current case temperature (° C) • Byte 2 = Recent minimum case temperature (° C) • Byte 3 = Recent maximum case temperature (° C) The normalized value is 100. Case temperature is calculated based on an offset from internal temperature sensor.
C0	**Unsafe Shutdown Count (Power-off Retract Count)** The raw value reports the cumulative number of unsafe (unclean) shutdown events over the life of the device. An unsafe shutdown occurs whenever the device is powered off without STANDBY IMMEDIATE being the last command.
C2	**Temperature - Device Internal** Reports internal temperature of the SSD. Temperature reading is the value direct from the internal sensor. The raw value is the current temperature. The normalized value is the results equation min (150-current temp, 100).
C7	**CRC Error Count** The total number of encountered SATA interface Cyclic Redundancy Check (CRC) errors.
E1	**Host Writes** The raw value reports the total number of sectors written by the host system. The raw value increases by 1 for every 65,536 sectors written by the host.

ID	Attribute and Description (SATA)
E2	**Timed Workload, Media Wear** Measures the wear seen by the SSD (since reset of the Timed Workload Timer, attribute E4), as a percentage of the maximum rated cycles.
E3	**Timed Workload, Host Read/Write Ratio** The percentage of I/O operations that are read operations (since reset of the Timed Workload Timer, attribute E4).
E4	**Timed Workload Timer** Measures the elapsed time (number of minutes) since starting this workload timer.
E8	**Available Reserved Space** Reports the number of reserve blocks remaining. The normalized value begins at 100 (64h), which corresponds to 100 percent availability of the reserved space. The threshold value for this attribute is 10 percent availability.
E9	**Media Wearout Indicator** Reports the number of cycles the NAND media has undergone. The normalized value declines linearly from 100 to 1 as the average erase cycle count increases from 0 to the maximum rated cycles. Once the normalized value reaches 1, the number will not decrease, although it is likely that significant additional wear can be put on the device.
F1	**Total LBAs Written** Counts sectors written by the host.
F2	**Total LBAs Read** Counts sectors read by the host.

Scroll down to view the SMART Health Info attributes supported by the selected NVMe drive.

Details shown for each SMART Health Info attribute include:

- **ID:** The byte offset value of the SMART Health Info.

- **Description:** The name of the SMART Health Info.

- **Raw:** The raw value assigned to the SMART Health Info by the drive manufacturer.

- **Threshold[1]:** (If defined) The lowest acceptable normalized value for the drive.

- **Action:** Identifies whether the system can use the drive for processing.

Descriptions of some SMART Health Info attributes are shown in the following table. These attributes vary depending on the SSD or other drive selected. Your SSD or drive may not support some of these attributes. For more details on each attribute, see the NVMe specification.

ID	Attribute and Description (NVMe)
1	**Temperature** Reports overall Device current temperature in Kelvin.
3	**Available Spare** Contains a normalized percentage (0 to 100%) of the remaining spare capacity available. Starts from 100 and decrements.
4	**Available Spare Threshold** Threshold is set to 10%.
5	**Percentage Used Estimate** (Value allowed to exceed 100%) A value of 100 indicates that the estimated endurance of the device has been consumed but may not indicate a device failure. The value is allowed to exceed 100. Percentages greater than 254 shall be represented as 255. This value shall be updated once per power-on hour (when the controller is not in a sleep state).
32	**Data Units Read (in LBAs)** Contains the number of 512 byte data units the host has read from the controller; this value does not include metadata. This value is reported in thousands (i.e., a value of 1 corresponds to 1000 units of 512 bytes read) and is rounded up. When the LBA size is a value other than 512 bytes, the controller shall convert the amount of data read to 512 byte units.
48	**Data Units Write (in LBAs)** Contains the number of 512 byte data units the host has written to the controller; this value does not include metadata. This value is reported in thousands (i.e., a value of 1 corresponds to 1000 units of 512 bytes written) and is rounded up. When the LBA size is a value other than 512 bytes, the controller shall convert the amount of data written to 512 byte units. For the NVM command set, logical blocks written as part of Write operations shall be included in this value. Write Uncorrectable commands shall not impact this value.
64	**Host Read Commands** Contains the number of read commands issued to the controller.
80	**Host Write Commands** Contains the number of write commands issued to the controller.
96	**Controller Busy Time (in minutes)** Contains the amount of time the controller is busy with I/O commands. The controller is busy when there is a command outstanding to an I/O Queue (specifically, a command was issued by way of an I/O Submission Queue Tail doorbell write and the corresponding completion queue entry has not been posted yet to the associated I/O Completion Queue). This value is reported in minutes.

ID	Attribute and Description (NVMe)
112	**Power Cycles** Contains the number of power cycles
128	Power On Hours Contains the number of power-on hours. This does not include time that the controller was powered and in a low power state condition.
144	**Unsafe shutdowns** Contains the number of unsafe shutdowns. This count is incremented when a shutdown notification (CC.SHN) is not received prior to loss of power.
160	Media Errors Contains the number of occurrences where the controller detected an unrecovered data integrity error. Errors such as uncorrectable ECC, CRC checksum failure, or LBA tag mismatch are included in this field.
176	**Number of Error Information Log Entries** Contains the number of Error Information log entries over the life of the controller.
192	Warning Composite Temperature Time Contains the amount of time in minutes that the controller is operational, and the Composite Temperature is greater than or equal to the Warning Composite Temperature Threshold (WCTEMP) field and less than the Critical Composite Temperature Threshold (CCTEMP) field in the Identify Controller data structure.
196	Critical Composite Temperature Time Contains the amount of time in minutes that the controller is operational, and the Composite Temperature is greater the Critical Composite Temperature Threshold (CCTEMP) field in the Identify Controller data structure.
0	Critical Warning These bits if set, flag various warning sources. • Bit 0: Available Spare is below Threshold • Bit 1: Temperature has exceeded Threshold • Bit 2: Reliability is degraded due to excessive media or internal errors • Bit 3: Media is placed in Read- Only Mode • Bit 4: Volatile Memory Backup System has failed (e.g., enhanced power loss capacitor test failure) • Bits 5-7: Reserved Any of the critical warning can be tied to asynchronous event notification.

§

12   Additional Information

12.1   Related Publications

For more information on Intel Solid State Drives, go to http://www.intel.com/ssd.

12.2   Reference Documents

Document	Document No./Location
ATA Specification	http://www.t13.org/
SATA Specification	http://www.sata-io.org
NVMe Specification	http://www.nvmexpress.org

§