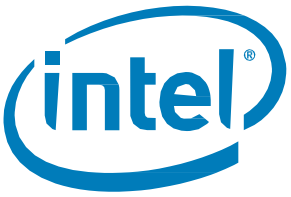
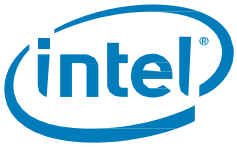


The Intel® SSD Pro 2500 Series Guide for Microsoft eDrive* Activation

Solutions Blueprint

January 2015

Order Number: 330880-002US



Contents

Revision History

Revision Number	Description	Revision Date
001	• Initial release.	August 2014
002	• Added NOTE in Section 2.3	January 2015

§

1 Introduction

With security breaches continually on the rise, data protection is more essential than ever. At Intel, we realize how important it is to provide security capabilities for PC storage devices. We build the Intel® SSD Professional Family with data protection in mind – delivering security and manageability features designed to help protect important data. With the growing use of Microsoft's eDrive* solution Intel has built eDrive support into our Intel® SSD Pro 2500 Series.

In order to effectively utilize any collaborative solution between the host platform, software and SSD, it is important to understand how the components work together. In this blueprint, we define:

- How to enable eDrive support on the Intel SSD Pro 2500 Series (Pro 2500 Series) using Intel SSD Pro Administrator Tool
- How to activate eDrive on the Pro 2500 Series with Windows OS*
- How to recover if something does not work properly with eDrive activation

1.1 Terminology

Term	Description
SED	Self-Encrypting Drive
BitLocker*	Microsoft's security software included in Windows 7* and Windows 8*
PBA	Pre-Boot Authentication – environment setup by system security software that requires a user to authenticate, typically with a passphrase or password, to start the OS boot process.
Opal*	A Trusted Computing Group* (TCG) standard that defines an interface for managing a Self-Encrypting Drive (SED).
eDrive	Microsoft specification for a drive that complies with the TCG* Opal 2.0 and IEEE 1667* standards
MBAM*	Microsoft BitLocker Administration and Monitoring
PSID	Physical presence Security ID
PSID Revert	Opal Revert using PSID value printed on drive label used in the event all Opal passwords have been lost.

1.2 Reference Documents

Document	Document No./Location
Trusted Computing Group Opal Storage Security Subsystem Class Specification, Version 2.0	www.trustedcomputinggroup.com
Microsoft TechNet site on eDrive Requirements	http://technet.microsoft.com/en-us/library/hh831627.aspx

2 Blueprint Elements

2.1 Intel SSD Pro 2500 Series

The Pro 2500 Series is a self-encrypting drive (hardware encryption) and provides security and manageability features, including support for TCG* Opal SSC* version 2.0 and Microsoft eDrive requirements.

2.2 TCG Opal SSC Version 2.0

TCG's Opal security standard is designed to secure at rest data, primarily in the business computing environment. Opal helps protect data stored on a computer's primary storage drive in the event the machine is lost or stolen. Access to stored data is protected using robust authentication methods and data encryption algorithms. Access control is managed with passwords or alternate authentication methods, depending on the software that manages the drive and the policies implemented by the administrator. The Opal solution addresses threats by combining a Professional Family Opal-enabled drive with a management software solution from a third party vendor. For more information on Opal, go to www.trustedcomputinggroup.com.

2.3 Microsoft eDrive

The Pro 2500 Series also adds Microsoft eDrive support. eDrive builds on the Opal 2.0 security features and has additional security protocol based on IEEE 1667 to enable drive locking and provisioning. For more information, start with http://technet.microsoft.com/en-us/library/hh831627.aspx.

Microsoft eDrive works in conjunction with the familiar Windows BitLocker application to manage the security policies and keys of the drive's secure partitions. With eDrive compatibility, BitLocker will offload the data encryption from the host to the storage drive – referred to as hardware encryption – freeing up the processor for other tasks.

NOTE: The Intel SSD Pro 2500 Series supports four locking ranges with hardware-based 256-bit AES encryption. Additional ranges are encrypted using BitLocker* software encryption. Because the default installation of Windows 8.1 uses three of the locking ranges for system partitions, only a single locking range remains available to be used as a hardware-based encrypted partition for the user, i.e. "C:". For the case where additional user partitions are defined, i.e. "D:", BitLocker software encryption will be automatically applied to those additional partitions.

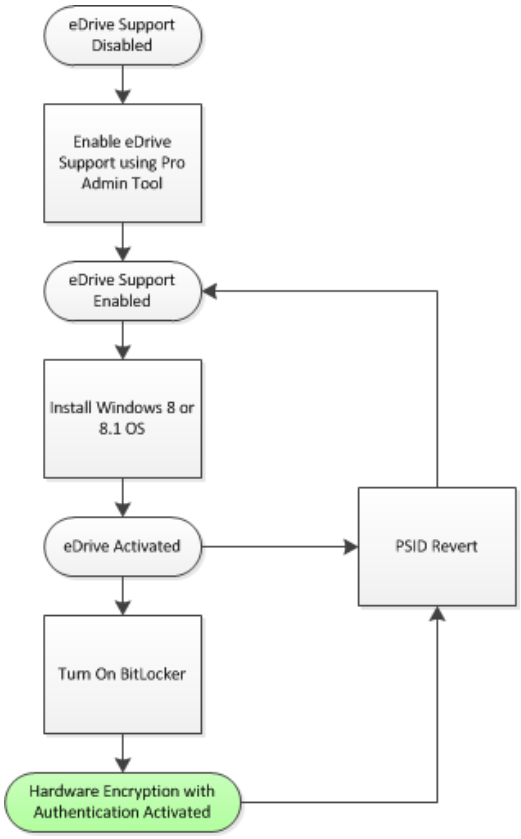
2.4 Intel SSD Pro Administrator Tool

Intel SSD Pro Administrator Tool (Pro Admin Tool) is a command line based tool that allows the user to check the security status and manage Intel® Professional Family of SSDs. Pro Admin Tool contains functions that support the user enabling eDrive, perform "PSID Revert", Secure Erase an Intel SSD, and view drive information on Pro 2500 Series drives.

3 The Solution

Enabling eDrive support on the Pro 2500 Series is simple with the new Intel SSD Pro Admin Tool. Once eDrive support is enabled on the Pro 2500 Series, Windows 8 makes the activation of eDrive simple with automatic provisioning during the OS install process.

Support flow:



3.1 System Requirements

3.1.1 Hardware

- The Pro 2500 Series is an SED and supports the TCG Opal 2.0 and IEEE 1667 specifications.
  NOTE: The Pro 2500 Series supports various configurations of security features. By default, the Pro 2500 Series ships with eDrive support disabled. Please make sure to check supported features on the Pro 2500 Series drive you are working with.
- TPM and UEFI support as required by Microsoft BitLocker.
  See http://technet.microsoft.com/en-us/library/hh831713.aspx for more info.

3.1.2 Software

- Windows 8 or Windows 8.1* Pro and Enterprise versions
- ATA Security must not be enabled – no drive password (ATA user password) should be set
- Intel RST storage driver does not support eDrive at this time

3.2 Enabling eDrive on the Pro 2500 Series

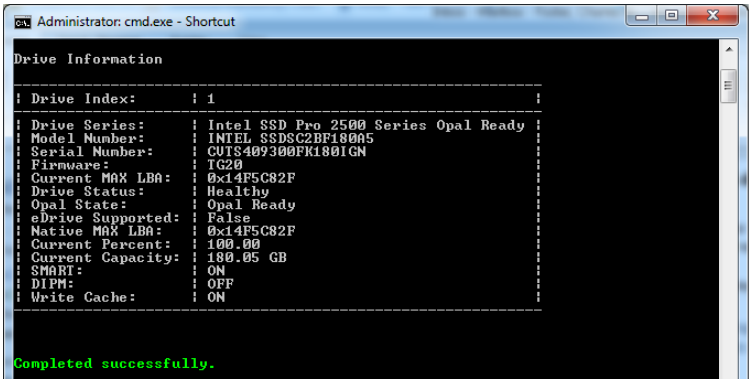
If eDrive requirements are met, Windows automatically performs the secure provisioning for eDrive during the OS installation. To meet eDrive requirements you'll want to verfiy and enable eDrive support prior to OS install.

Note: At this time, Intel SSD Pro Admin Tool only supports enabling eDrive. Users should enable eDrive if the support is needed for hardware encryption with Windows BitLocker. Enabling eDrive cannot be accomplished with ATA Security enabled (ATA user password set). Disable user password prior to running Intel SSD Pro Admin Tool to enable eDrive support.

3.2.1 Check the Current Configuration

Plug the drive into a system that supports the Intel SSD Pro Admin Tool. Version 1.1.0 supports eDrive enabling on the Pro 2500 Series. Download the Pro Admin Tool from www.intel.com/ssd under the Tools pull-down. Pro Admin Tool is a stand-alone command line executable, so all you need to do is place the executable in a familiar folder for execution.

1. Pro Admin Tool can only be run as administrator, so open an elevated command prompt.
2. Execute Pro Admin Tool with "-drive_list" option to see what drives are on the system and what index is assigned to each.
   - C:\> SSDProAdminTool_1.1.0_win64.exe –drive_list
3. Once drive index is known, then execute tool with "-drive_index X" (where X is drive index number) option to make sure Opal support is enabled on the Pro 2500 Series drive. The "-drive_index" info shows Opal and eDrive status. (See below.) Opal is supported if status is "Opal Ready".
   - C:\> SSDProAdminTool_1.1.0_win64.exe –drive_index 1



3.2.2 Enable eDrive support

If Opal is supported and eDrive support is False, then enable eDrive.

1. Execute the tool by using the "-drive_index X -enable_eDrive" option to turn on support for eDrive. User will be prompted to determine if enabling eDrive is desired; type "Y" to proceed.
   - C:\> SSDProAdminTool_1.1.0_win64.exe –drive_index 1 –enable_eDrive
2. To confirm eDrive is enabled, use the "-drive_index X" option again to check status. Status should be "True".
   - C:\> SSDProAdminTool_1.1.0_win64.exe –drive_index 1

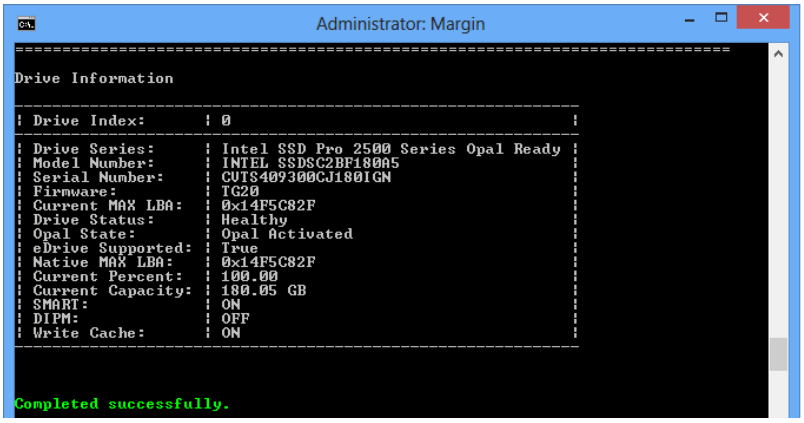
3.3 eDrive Activation

Now that eDrive is enabled on the Pro 2500 Series drive, the next step is to install Windows and activate security capabilities with eDrive.

1. On Windows Install, the OS recognizes the drive supports eDrive features and sets up the admin authority to take control of the drive's security. eDrive requires secure partitioning at the time of the OS install to allow BitLocker to make use of drive's HW encryption.

Note: At this point using ATA security is no longer an option because Opal activation does not support ATA security functions; all authentication (passwords) is managed by Microsoft and BitLocker.

2. BitLocker can now be enabled to enforce PBA. (Even with BitLocker enabled and allowing HW encryption, there is no PBA if user does not have password set.) BitLocker can now be quickly enabled for a volume on the drive without the long wait for software encryption.
3. Depending on how the IT administrator has set policies on the system, the password credentials (keys) may be managed with a secondary secure device connected to system, or may be remotely managed by way of an enterprise IT database like Microsoft's MBAM*.
4. Confirm that eDrive is activated by using the Pro Admin Tool "-drive_index" option. Opal State will show "Opal Activated" since admin authority is now setup.
    - C:\> SSDProAdminTool_1.1.0_win64.exe –drive_index 0



5. Microsoft also provides a tool to check status of BitLocker. From command prompt, execute:
    - C:\> manage-bde –status

    If BitLocker is configured appropriately to work with HW encryption on the Pro 2500 SSD, then the "Encryption Method" will be shown as "Hardware Encryption".

3.4 Security Feature Set Interactions

When eDrive is activated on the Pro 2500 Series drive, several ATA security features will not be available. ATA Security and Santize Device Features are not supported as the Opal feature set is activated. Be aware that an ATA password cannot be set, Secure Erase cannot be performed and the Sanitize Device features will not work.

4 Drive Revert

If problems occur during installation, or if eDrive isn't setup correctly, the system should be returned to the pre-install state and the install process repeated.

4.1 PSID Revert Using Intel SSD Pro Admin Tool.

During operating system installation, on eDrive capable systems, Windows sets up and activates secure partitions on the drive. Microsoft only allows the drive to be returned to the pre-activated state by performing a hardened physical (or presence) revert. To return the drive to the pre-activated state, execute the PSID Revert function.

1. The PSID Revert function removes all secure partitions activated on the drive and removes any admin authorities set on the drive. The function also erases and resets the encryption keys, so all user data is inaccessible.
2. To perform the PSID Revert function, the PSID value that is printed on the label of the drive is required. For this reason, and because the operating system will be destroyed, PSID Revert must be performed with the drive plugged into a secondary port of a computer. This will allow the PSID value to be read from the label and the Pro Admin tool to execute the function.
3. Intel provides the Intel SSD Pro Admin Tool which performs the PSID Revert function on the Intel SSD Professional Family of drives. To perform the PSID Revert, execute the Pro Admin Tool with the "-drive_index X -psid_revert" option and follow instructions on the screen. As eDrive no longer "owns" drive security, ATA security will again be supported following the PSID Revert.

4.2 Secure Erase

The PSID Revert function performs a cryptographic erase of user data, meaning it erases and resets the encryption keys on the drive. If the user wants to perform a block erase of data in the drive, then an additional Secure Erase step must be performed using the Pro Admin Tool. Simply execute the tool with the "-secure_erase" option.

§