Technical Note

Installing Micron SEDs in Windows 8 and 10

Introduction

Self-encrypting drives (SEDs) can provide an effective way of protecting sensitive data from falling into the wrong hands. This technical note describes the proper installation and operation of Windows BitLocker in hardware encryption mode. In some configurations it is possible for BitLocker to run in software encryption mode, but this can slow the performance of the SED and the overall system. Proper installation will help maximize the performance and data security of Micron's SEDs, which are designed for desktop computing.

Beginning with the M500 and continuing with the latest SED generations, Micron has provided AES-256-bit hardware encryption as a standard option on our SEDs. AES-256 is state-of-the-art data encryption and is generally considered unbreakable by known decryption techniques (within reasonable time scales).

Micron's SEDs conform to both the Trusted Computing Group (TCG) Security Subsystem Class (SSC) Opal Specification 2.0 and the IEEE-1667 specification, "Standard Protocol for Authentication in Host Attachments of Transient Storage Devices." In satisfying both of these specifications, Micron's SEDs conform to Microsoft's specification for "eDrive" under Windows 8 and Windows 10. The eDrive functionality enables the management of hardware-encrypted storage devices under the versions of BitLocker found in the Windows8 and 10 Enterprise and Professional editions.

Note: For simplicity, references to "Windows 8" should be understood to apply to either Windows 8 or Windows 8.1. This document describes Windows 8 or 10 installation from media (DVD or USB thumb drive) or via disk duplication. Deployment from a network or server is not discussed; that information can be found at www.microsoft.com, using the keyword search "encrypted hard drives."

Micron SSD Models

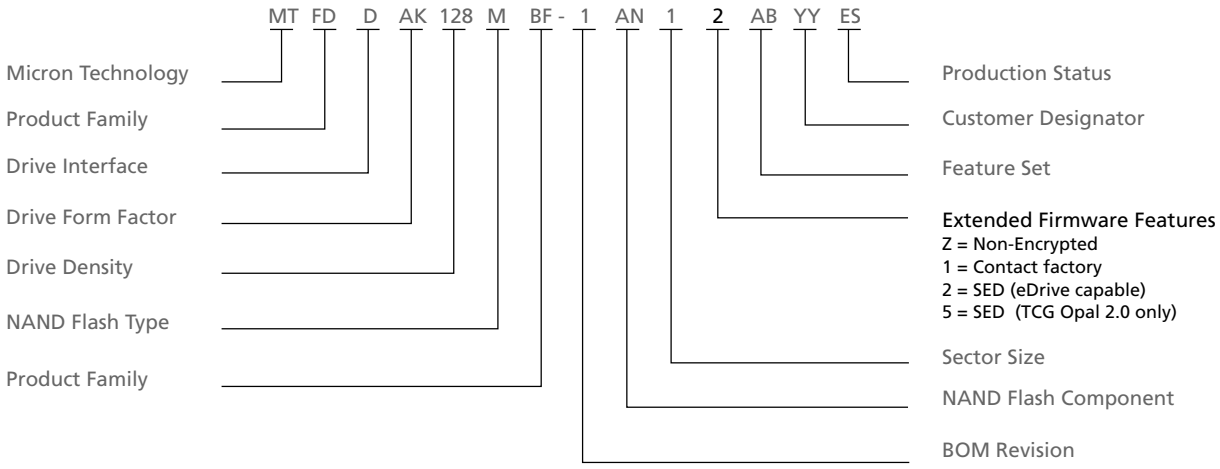
Some Micron SSD models do not include encryption at all, in which case BitLocker will implement software encryption. Other Micron SEDs comply only with the TCG Opal 2.0 protocol. If this is the case, then there are encryption management solutions from Independent Software Vendors (ISV) which can address your data security concerns in place of BitLocker. If BitLocker is used, these Opal-only SEDs will be software encrypted because they do not fully comply with the eDrive protocol.

Micron C400 SEDs are not compatible with the eDrive protocol, but are TCG Opal 1.0 compatible.

Micron SSDs, which are included as original equipment in a computer system, may meet specific design requirements by the PC manufacturers. Such SSDs or SEDs may not be covered by this technical note.

Micron data center and enterprise-class SSDs follow a different encryption protocol, and are not discussed here.

Figure 1: Part Marking for Encryption Devices (Example)



The Role of Hardware Encryption in Data Security

Hardware encryption of data on a storage device is only part of an overall data security regime. Hardware encryption can protect "data at rest" on a storage device, especially when the device is lost or stolen and in a powered-off or hibernate mode. However, when the host computer is operating, all data are "in the clear" and vulnerable to intrusion. Consequently, hardware encryption at the drive level is a complement to, rather than a substitute for, firewalls, virus protection software, and other methods of protecting against data intrusion.

Security Modes

Micron's SEDs support either the TCG Opal 2.0 specification or the ATA SECURITY FEATURE SET. The ATA security modes are generally initiated by system BIOS or by some universal extensible firmware interface (UEFI)-based systems in legacy mode. By specification from the associated industry standards organizations, TCG Opal and ATA security are mutually exclusive. In other words, if one is enabled, the other is disabled. Thus, if the ATA SECURITY FEATURE SET is enabled by BIOS, then Windows will not be able to properly engage Micron's SED as a hardware-encrypted device. Instead, in this mode, software encryption may be engaged by BitLocker.

For many systems, the ATA SECURITY FEATURE SET is an effective means of managing encryption without having to acquire an encryption management software package.

Note: In the case of Micron's legacy C400 SED, TCG Opal 1.0 is supported, but the ATA security encryption functions are not.

TCG Hardware Encryption in Windows 7

Micron's SEDs can be effectively deployed in Windows 7. Note that Windows 7 BitLocker does not support hardware-encrypted devices. However, Micron has worked with several independent software vendors to ensure compatibility, including Wave Systems (www.wave.com) and WinMagic (www.winmagic.com).

Physical Security ID

All form factors of the M500 and newer SEDs provide what is known as a physical security ID (PSID) code on the serial number label of every SED. The PSID is a 32-character code which can be used to initiate an operation known as PSID REVERT. PSID REVERT may be used to recover the use of an SED when a password or authentication key is lost; however, PSID REVERT cannot be used to recover data from such a drive. PSID REVERT will initiate a cryptographic erase on the target SED, which changes the 256-bit encryption key resident in hardware on the drive. This renders all of the user data on the drive unreadable. The process will then reset the drive to a factory new state, from which a new OS can be installed.

Micron's Storage Executive software package includes a PSID REVERT function. Please see the User Guide for Storage Executive for more specific instructions. Additionally, several third-party tools are available which perform PSID REVERT, including tools from Wave Systems and WinMagic. The PSID, as printed on the Micron serial number label, includes several hyphens (-) for human readability. Do not include these hyphens when entering the PSID code into the revert tool.

When doing an OS reinstall on a drive which had a previous installation of Window 8 or Windows 10, it may be necessary to execute a PSID REVERT command on the drive be-

fore proceeding to the following steps, in order to reinitialize the SED to a state where the new OS can be successfully installed.

Windows 8 or 10 Installation

Requirements

The setup and installation steps are the same for Windows 8 and Windows 10.

Micron's SEDs meet the device requirements for implementing a hardware encryption system, but there are also requirements at the host computer. When the SED is configured as an operating system drive, the following preconditions must be met:

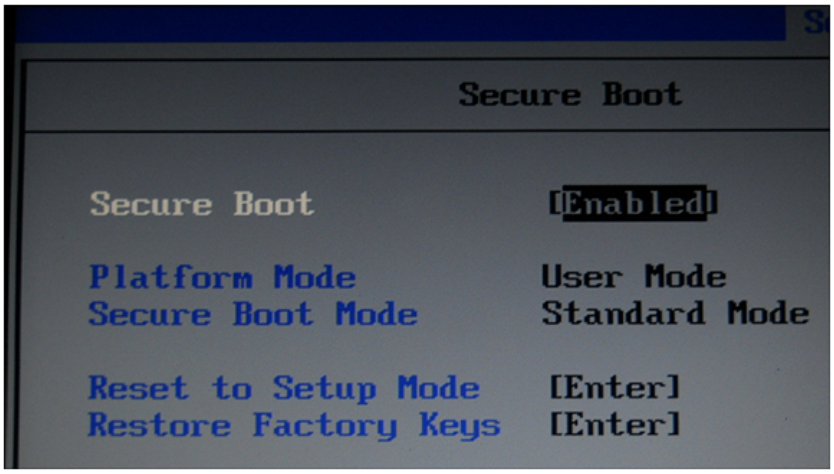
- The host computer should be at a minimum of UEFI 2.3.1 and should have the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined. This enables security protocol commands to be sent to and from the SED. Please contact the manufacturer of your host computer to ensure that this requirement is met.
- Secure Boot must be enabled.
- The host computer must always boot from UEFI. Any “compatibility” or “legacy” boot mode must be disabled. We recommend putting the system in UEFI-only mode before installing the Micron SED.
- The compatibility support module (CSM) must be disabled, if it is available.
- The drive must be in an uninitialized state with all security modes inactive. (This refers to the security state of the SED under the TCG and ATA protocols.) If the drive has been previously initialized, you may need to refer to instructions from the BIOS maker or any previous encryption software which may have been used in order to return the SED to an uninitialized state. The PSID REVERT function may also be needed to reinitialize the SED.
- Windows 8 and 10 cannot manage encryption on SEDs that are attached to the host computer via a RAID controller.
- A trusted platform module (TPM) on the host computer is not required in order to run hardware encryption. However, a TPM can provide additional data security functions, such as mating the SED to the host system so it cannot be operated in any other host computer. Instructions for using a TPM should be obtained from the manufacturer of the host computer. Installation on a host computer without a TPM may require using a USB thumb drive as a key. (See Microsoft's Windows documentation for more details.)

Configuring the Host System

It is recommended that the host system UEFI be configured to properly accept the SED before physically installing it, as outlined in the example below. Details of the system setup will vary from system to system, as will the names of various functions. However, they are similar enough that a single example should be sufficient. For details on specific UEFI setups, contact your computer's manufacturer.

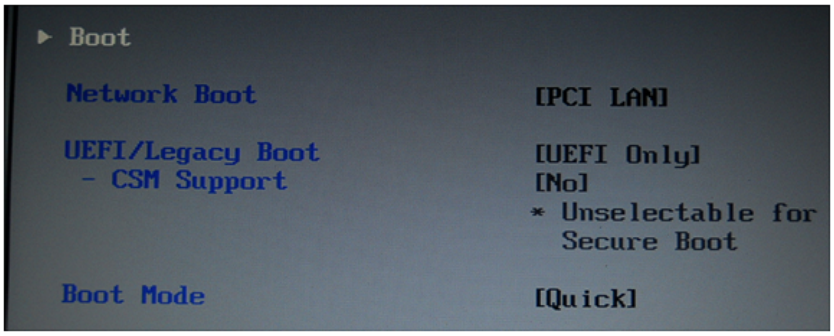
Enabling Secure Boot

Microsoft Secure Boot is a requirement to run any Windows 8 or 10 system. Any computer that has been configured from the factory for Windows 8 or 10 will already have Secure Boot enabled. If the host system was originally configured for Windows 7 or a previous operating system, check to ensure that Secure Boot is enabled, as shown below.



UEFI Boot Mode/CSM Support

The host computer system must be in UEFI-only mode, as shown below. Typically, the CSM will be automatically disabled in UEFI-only mode; however, this should be verified and the CSM should be disabled if necessary.



Installing Windows 8 or 10

The most straightforward method of implementing hardware encryption is to perform a clean, new installation of the operating system. BitLocker versions in the Enterprise and Professional editions of Windows 8 or 10 support hardware encryption on SEDs. No special steps are needed for this function; simply follow the normal OS installation process described by Microsoft.

After the OS is installed, proceed to the Enable BitLocker section.

System Cloning

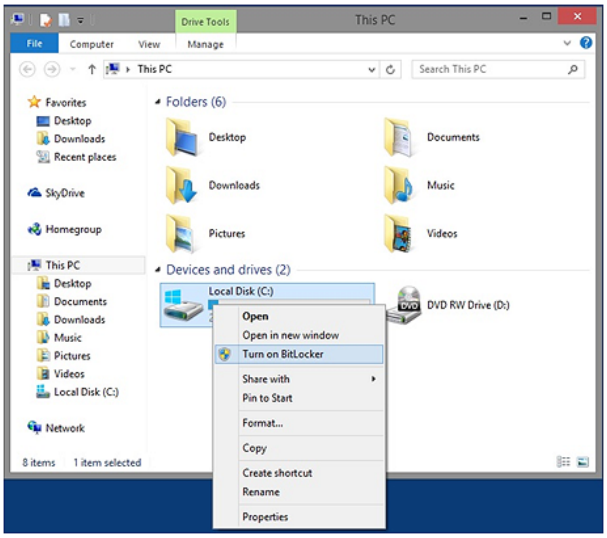
Because Micron SEDs support eDrive, activating BitLocker creates special partitions, which are required to put the eDrive features in effect. When an eDrive-activated SSD is cloned, these special partitions may not be properly copied to the target drive. The target drive may function, but this is not considered a valid process and it may cause latent performance problems.

If the source disk has been encrypted using software encryption in Bitlocker, first ensure that BitLocker is turned off before initiating the image clone to a Micron SED. If using BitLocker in software encryption mode on the source system, a decryption process will be required to turn off BitLocker. This can take several hours, depending on the amount of user and OS data on the drive.

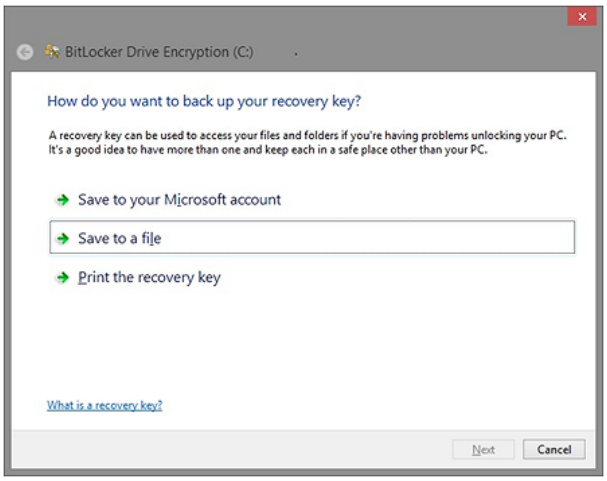
Enable BitLocker

Follow the steps below to enable BitLocker.

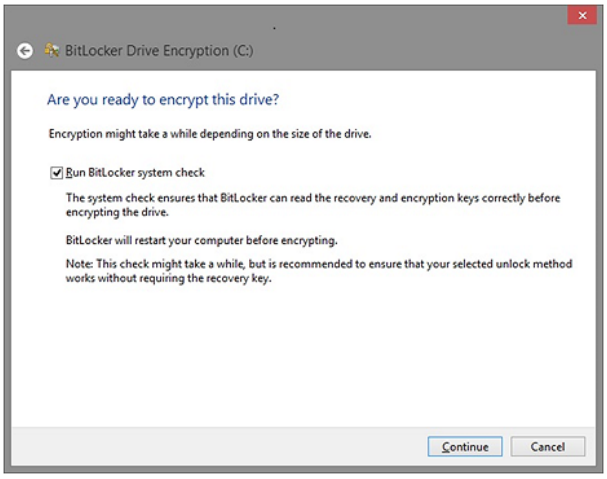
- Press the **Windows** key (usually between <Ctrl> and <Alt>); then type **This PC** and press **Enter**.
- Right-click on the icon for the system drive and select **Turn on BitLocker** from the pop-up menu. (Note that Windows 10 displays will look slightly different, but are functionally the same.)



- Next, a status box confirming that BitLocker is configuring will display, along with a status bar. This will complete momentarily.
- Select one of Microsoft's options for saving your recovery key. While Micron has no preferred option here, do not neglect this step. In some circumstances, this may be the only way to recover data from your SSD. Micron has no factory backdoor methods by which to recover data if an authentication key or password is lost. Once the key is saved, select **Next** to continue.



- BitLocker will ask, "Are you ready to encrypt this drive?" After you click **Continue**, a system restart will be required to complete the process.



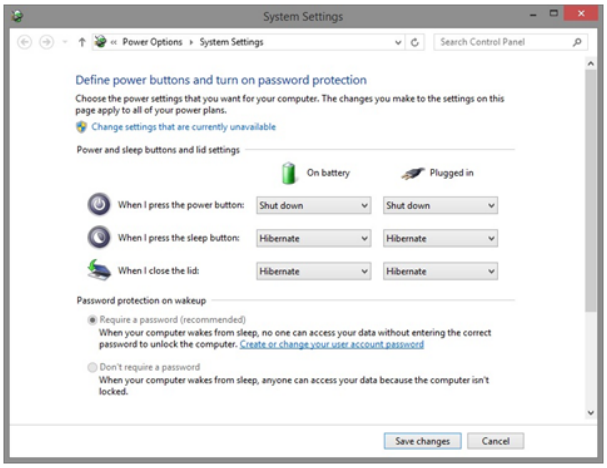
- After the reboot is complete, you will see from the BitLocker padlock icon on your system drive that BitLocker is enabled.

WARNING: After this first reboot, if a status window with a progress bar indicating that encryption is underway displays, then the system is most likely in software encryption mode, which means one of the preceding steps was not correctly completed. In particular, double-check that the pre-boot settings for Secure Boot and UEFI-Only Boot are enabled and that the CSM is disabled.

Recommended Settings

Micron recommends that the system be placed in hibernate mode when the system is not in use, in particular, when the notebook computer's lid is closed. This ensures that the SED fully enters the locked mode. To do so, follow these steps:

- Press the **Windows** key and then type **Change what the power buttons do**; then press **Enter**.
- Select the power-down options as shown below.



- Hibernate is preferred over sleep mode for both security and power consumption purposes. Recovery time may be compromised a bit, but SSDs can recover from hibernate significantly faster than HDDs. In fact, after a clean shutdown, a Micron drive will typically recover from hibernate and be ready to compute in under 0.2 seconds.

Conclusion

When installed properly and operated in hardware encryption mode, Windows 8 and 10 BitLocker enables nearly seamless and transparent management of Micron's M500 and newer SEDs.

Revision History

Rev. A – 08/15

- Updated to include Windows 10 information

Rev. A – 07/14

- Initial release

8000 S. Federal Way, P.O. Box 6, Boise, ID 83707-0006, Tel: 208-368-4000
www.micron.com/products/support Sales inquiries: 800-932-4992