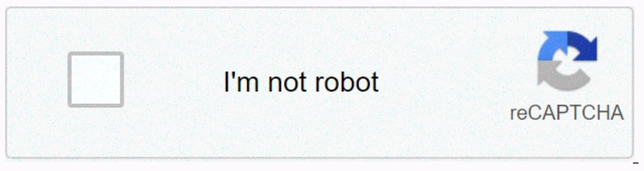

Continue

Bitlocker performance impact

I turn on BitLocker on a tablet and laptop with Windows 10. On tablet: HDD: SEAGATE Barracuda with 1TB power and 7200rpm, the specific type is ST1000DM010, 64MB cache. Processor: Intel Pentium CPU G4400, dual core dual core, 3MB cache, clocked at 3.3GHz. The CPU specification lists the new guidelines for the technology that supports AES. Laptop: SSD: TOSHIBA Q200EX, 240G storage capacity, SATA3 port. Processor: Intel Core i5-2430M CPU frequency 2.40GHz, the largest Turbo frequency is 3.0G, dual-core four-threaded, 3MB cache. BitLocker causes 50% - 60% loss of performance on the tablet, while not affecting the laptop. To find out if processor effects are or not, turn on BitLocker on a Windows 7 tablet. Here are the details: HDD: SEAGATE Barracuda ST1000DM003, 1TB power and 7200rpm, 64Mb cache. Processor: Intel Xeon E3-1203 v3, quad-core eight themes, 8MB cache, 3.3GHz clock speed and Intel Turbo Boost allows users to increase clock speed to 3.70 GHz. CPU specification lists technology that supports AES new guidelines. As a result, this is still a 50% writing rate decrease. Therefore, the processor does not affect performance at all. Then I will conduct an in-depth study of how BitLocker effects read-write performance. Turning on BitLocker would have less impact on the SSD with the AES chip. Closed. This question is based on opinion. Right now, he doesn't accept the answers. Do you want to correct this question? Update the question to be answered with facts and quotes by editing this post. Closed four years ago. I'ASP.NET a developer/ C# developer. I use VS2010 all the time. I mean allowing BitLocker to protect content on my laptop, but I'm concerned about the performance deteriorating. Developers who use IDs like Visual Studio work on many and many files at once. More than a regular office worker, I guess. So I was curious if there are other developers out there who develop BitLocker enabled. How'd the show go? Is that noticeable? If so, is that bad? My laptop has a 2.53GHz Core 2 Duo 4GB RAM and Intel X25-M G2 SSD. It's pretty cheeky, but I want it to stay that way. When I hear some bad stories about BitLocker, I keep doing what I do now, which keeps the stuff RAR'ed password when I'm not actively working, and then SDeleting it when I'm done (but it's kind of pain). Update 2015: I have used Visual Studio 2015 when traveling to my Surface Pro 3 that has BitLocker enabled by default. It looks pretty much like my desktop, which is i7-2600k @ 4.6 GHz. I think that modern hardware good for the SSD, you do not notice! Some SSDs advertise support for hardware encryption. If you enable BitLocker in Windows, Microsoft trusts your SSD and does nothing. But researchers have found that many SSDs do a terrible job, which means BitLocker doesn't provide secure encryption. Update: Microsoft has released a security bulletin for this issue. This includes: you can check whether you are using hardware or software encryption. Update: Almost a year later, BitLocker no longer trusts your SSD, so you can trust it again. Many SSDs don't apply encryption correctly even if you enable BitLocker encryption on your system, Windows 10 may not actually encrypt your data. Instead, Windows 10 can rely on your SSD to do this and your SSD encryption can be easily broken. That's the conclusion from a new paper by researchers at Radbound University. They reverse engineered firmwares for many solid state-drives and found various issues with hardware encryption found in many SSDs. The researchers tested the hard drives of Important and Samsung, but we certainly wouldn't be surprised if other manufacturers had big problems. Even if you don't have any of these specific drives, you should be worried. For example, an important MX300 contains a default empty base password. Yes, that's right — it has a basic password that's set to nothing, and this blank password gives you access to the encryption key that encrypts your files. It's crazy. Encrypted SSD is the basic password that is set. But don't worry, customers, you can turn it off! It's going to be okay. pic.twitter.com/hSlPCMyHsi — Matthew Green (@matthew_d_green) 5. Windows users would use BitLocker instead. BitLocker encrypts the files before they're stored in the SSD, right? Wrong. If your computer has a solid state drive that says it can handle hardware encryption, BitLocker does nothing. BitLocker simply trusts the SSD to encrypt files by waiing all responsibility. And as researchers have found, SSD manufacturers have some serious problems with implementing encryption properly. Even if you choose to encrypt your laptop's hard drive with BitLocker, you're now relying on what company did on your laptop SSD. Do you believe that the manufacturer of the drive laptop did a good job? Do you even know what the company did on your laptop internal SSD? Did the laptop manufacturer think about it before choosing a hard disk supplier? BitLocker in Windows 7 does not support encryption for encrypted hard disks, as the Microsoft documentation says. In other words, it's a new feature of Windows 10, so Windows 7 systems don't have the same problem. Using BitLocker Software Encryption If you use BitLocker encryption in SSD, you can tell BitLocker to avoid hardware-based encryption and software-based encryption. However, this requires Group Policy. Group Policy is only available in Windows 10 Professional, but then there's the standard version of BitLocker. On one computer, open the local Group Policy Editor by pressing Windows+R, typing the Run gpedit.msc dialog, and then pressing Enter. In the right pane, double-click Configure Hardware-Based Encryption for Fixed Data Drives in the right pane\ Select Disabled, and then click OK. Microsoft says you need to decrypt and recrypt the drive before the change takes effect. You can also use the Open Source VeraCrypt tool to encrypt a Windows system drive or any other drive using BitLocker SSD encryption, instead of relying on bitlocker. It is based on TrueCrypt software, which may have been heard. Unlike BitLocker, VeraCrypt is also available for Windows 10 Home and Windows 7 Home users. You don't have to pay $100 for encryption. VeraCrypt never relies on SSDs that the encryption job does – VeraCrypt always handles encryption itself. Warning: Some major Windows 10 updates have caused problems with VeraCrypt in the past. We recommend life-saving equipment at hand just in case. If you stay with BitLocker, we don't have any problems with bitlocker and disable hardware encryption. RELATED: How to encrypt your Windows system drive veracrypt Why BitLocker Trust SSD? If available, hardware-based encryption may be faster than software-based encryption. Therefore, if the SSD had a solid hardware-based encryption technology based on this SSD, it would lead to better performance. Unfortunately, it seems that many SSD manufacturers cannot trust it to be implemented properly. If you need encryption, you'd better use BitLocker software-based encryption so you don't have to trust your SSD security. In a perfect world, accelerated hardware encryption is definitely better. That's one reason Apple includes a T2 security chip on its new Macs. The T2 chip uses a hardware accelerated encryption engine to quickly encrypt and decrypt data stored on a Mac's internal SSD. However, your Windows PC doesn't use this technology— it has a manufacturer's SSD, which probably didn't spend much time thinking about security. And that's not good. Some people often store important or private folders, files, and data on their hard disk. In the meantime, they're also afraid of unauthorized people accessing these important things. Therefore, to protect important data and file security, people tend to use BitLocker to encrypt and maintain disk partitions. However, it is also suspected that using BitLocker to encrypt your hard disk will affect disk read and write performance. Anyway, I'll test you if it has any effect, if so, how much? Tips 1: Different encryption algorithms supported by BitLocker BitLocker support AES 128-bit and 256-bit encryption algorithms. By the way, the longer the key, the greater the security, the harder it is to break through, but the longer the key, the longer it takes to encrypt and decrypt data. By default, BitLocker is encrypted using AES in Windows 7 diffuser and Windows 10 encryption is XTS-AES 128-bit. However, which algorithm to use and whether to use the diffuser, you can open the local Group Policy Editor and navigate to the computer configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption. In the right panel, double-click Select Drive Encryption Method and Cipher Strength to select the encryption algorithms you want to change. Tips 2: Encryption and non-encryption You can test reading and writing speed in unencrypted situations before encryption. Use BitLocker to encrypt the hard disk you're testing, and if your hard disk is encrypted, you can test the reading and write speed of encryption. Does BitLocker encryption affect your disk performance? Let's get to the point. Since my all partitions on the hard drive are encrypted to complete BitLocker before, I intend to use windows 10 E cup desktop and Windows 10 D cup laptop test target using ATTO Disk Benchmark v3.05 according to test SSD / HDD read and write performance encrypted and unencrypted. Please watch carefully the following two tests: Test 1: SSD bitLocker VS SSD without BitLocker Test 2: HDD bitLocker VS HDD without BitLocker Test 1: SSD without BitLocker VS SSD BitLocker Testing Environment Testing Tool: ATTO Disk Benchmark. Encryption methods: 1. non-encryption; 2. XTS-AES 128-bit (default); 3. XTS-AES 256-bit. SSD: TOSHIBA Q200EX, 240G storage capacity, SATA3 port. Processor: Intel Core i5-2430M CPU frequency 2.40GHz, the largest Turbo frequency is 3.0G, dual-core four-threaded, 3MB cache. Windows system: Windows 10 Enterprise 64-bit operating system, 1703 version. Test result 1. Different BitLocker encryption algorithms have a slight impact on SSD reading and writing performance. (See comparison below) Test 2: HDD without BitLocker VS HDD BitLocker Testing Environment Testing Tool: ATTO Disk Benchmark. Encryption methods: 1. non-encryption; 2. AES-CBC 128-bit; 3. AES-CBC 256-bit. HDD: SEAGATE Barracuda 1TB capacity and 7200rpm, specific type is ST1000DM010, 64MB cache. Processor: Intel Pentium CPU G4400, dual-threaded, 3MB cache, clocked at 3.3GHz. The CPU specification lists the new guidelines for the technology that supports AES. Windows system: Windows 10 Enterprise, 64-bit version 1709. Test result 1. You can use different encryption methods to verify that it affects hdd reading and writing performance. (See following images) Conclusion As you can see from the results, the test results, after HDD/SSD encryption with different encryption methods and then testing encrypted and unencrypted disks, have obvious differences. Test 1, performance loss writing is about 5%, read performance loss is less than 1%. Test 2 does not have a very large impact on hdd reading results, but there are obvious differences in data writing and writing results 50% - 62%. Related Articles